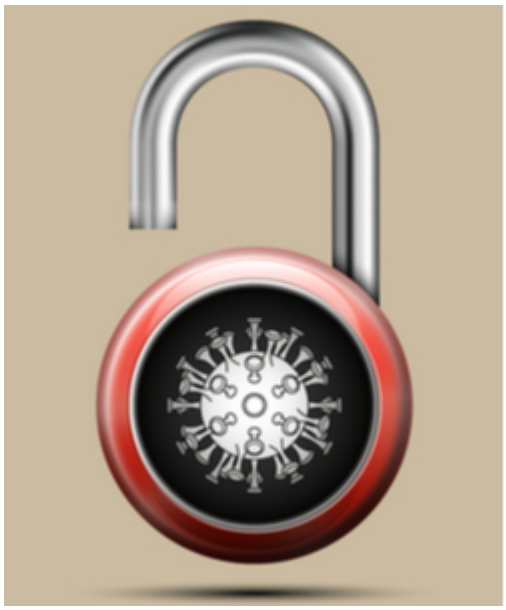
KrebsonSecurity
In-depth security news and investigation

COVID-19 Has United Cybersecurity Experts, But Will That Unity Survive the Pandemic?

April 15, 2020 28 Comments

The Coronavirus has prompted thousands of information security professionals to volunteer their skills in upstart collaborative efforts aimed at frustrating cybercriminals who are seeking to exploit the crisis for financial gain. Whether it's helping hospitals avoid becoming the next ransomware victim or kneecapping new COVID-19-themed scam websites, these nascent partnerships may well end up saving lives. But can this unprecedented level of collaboration survive the pandemic?



At least three major industry groups are working to counter the latest cyber threats and scams. Among the largest in terms of contributors is the COVID-19 Cyber Threat Coalition (CTC), which comprises rough 3,000 security professionals who are collecting, vetting and sharing new intelligence about new cyber threats.

Nick Espinosa, a self-described "security fanatic," author and public speaker who's handling communications for the CTC, said the group does most of its work remotely via a dedicated Slack channel, where many infosec professionals seem eager to counter the gusto with which the cybercriminal community has sought to profit by exacerbating an already difficult situation.

"A nurse or doctor can't do what we do, and we can't do what they do," Espinosa said. "We've seen a massive rise in threats and attacks against healthcare systems, but it's worse if someone dies due to a malicious cyberattack when we have the ability to prevent that. A lot of people are involved because they're emotionally attached to the idea of helping this critical infrastructure stay safe and online."

Using threat intelligence feeds donated by dozens of cybersecurity companies, the CTC is poring over more than 100 million pieces of data about potential threats each day, running

those indicators through security products from roughly 70 different vendors. If at least 10 of those flag a specific data point — such as a domain name — as malicious or bad, it gets added to the CTC's blocklist, which is designed to be used by organizations worldwide for blocking malicious traffic.

"For possible threats, meaning between five and nine vendors detect an indicator as bad, our volunteers manually verify that the indicator is malicious before including it in our blocklist," Espinosa said.

Another Slack-based upstart coalition called the COVID-19 CTI League spans more than 40 countries and includes professionals in senior positions at such major companies as Microsoft Corp and Amazon.com Inc.

Mark Rogers, one of several people helping to manage the CTI League's efforts, told Reuters the top priority of the group is working to combat hacks against medical facilities and other frontline responders to the pandemic, as well as helping defend communication networks and services that have become essential as more people work from home.

"The group is also using its web of contacts in internet infrastructure providers to squash garden-variety phishing attacks and another financial crime that is using the fear of COVID-19 or the desire for information on it to trick regular internet users," wrote Reuters' **Joe Menn**.

"I've never seen this volume of phishing," Rogers told Reuters. "I am literally seeing phishing messages in every language known to man."

Among the more mature organizations working to counter the threat from COVID-19 scammers is the Cyber Threat Alliance, a industry group founded in 2017 that counts among its members more than two dozen major cybersecurity firms that are all required to regularly share threat intelligence with other members.

"One thing we're paying attention to in addition to phishing and malware attacks is anything targeting stuff involved in the pandemic response, such as the manufacturers of protective gear, testing kits, or hospitals," **CTA President Michael Daniel** told KrebsOnSecurity. "One of those organizations getting hit with ransomware now would be really bad, and we want to make sure if we see that we're alerting and working with law enforcement."

Earlier this month, the international police network INTERPOL issued a warning to law enforcement in nearly 200 member countries, saying it had detected "a significant increase in the number of attempted ransomware attacks against key organizations and infrastructure engaged in the virus response."

The alert came after several top ransomware gangs pledged a moratorium on attacking hospitals and other care centers for the near future. Nevertheless, these group have continued to target companies on the periphery of the pandemic response, including virus testing labs, N95 mask production facilities, and companies engaged in vaccine research.

The CTC's Espinoza said it would be a potentially fatal mistake to assume all cybercriminal groups might observe such a cease-fire.

"We might have independent criminal groups saying they won't hit hospitals but they'll hit everyone else, but that doesn't prevent them from sending phishing emails and masquerading as the World Health Organization or the Centers for Disease Control," he said. "These are people who have no problems locking out little old ladies out of their computers for 800 bucks, and of course there are state-sponsored hackers who love any opportunity to sow discord and disrupt things."

SURVIVING THE PANDEMIC

The CTA's Daniel said while it's great to see so much voluntary collaboration between the cybersecurity industry, governments and law enforcement, he's been thinking a lot lately about how to sustain these relationships and networks once the urgency of the pandemic subsides.

Formerly special assistant to President Obama and cybersecurity coordinator on the National Security Council, Daniel said he sees preserving and enhancing this information sharing effort post-COVID as one of the biggest policy issues facing the federal government over the next few years.

"Information sharing is easy to talk about, and hard to do in practice," Daniel said. "I don't use the term 'public-private partnership' because it's been bandied about so much over the years that I don't know what it means anymore. It's probably best described as 'working together on an operation.'"

What prevents private companies from working more closely and frequently with governments on operations to target cybercrime organizations and networks? Daniel said on the government side, there are real concerns that working with one or two particularly clueful or effective companies (versus all of them) might give the impression that the government is showing favoritism, or picking winners and losers in the market.

"But you have to do that to some extent because the truth is some companies matter in this space, and a lot don't," Daniel said. "The government has to accept that, determine what are the objective rules, and establish transparency so that [their efforts] aren't seen as some secret club but as part of a normal process."

Daniel said governments in general also need to get more comfortable sharing information about operations targeting specific crime groups in advance of those actions.

"The government has to figure out how to let the private sector in on some of the planning and preparation," he said. "If you want [the cybersecurity industry's] help against certain targets, you have to tell us who they are ahead of time. But this goes against how governments operate in almost every way."

On the private sector side are issues of how for-profit companies can closely collaborate with the government without being perceived as potentially compromising the privacy and security of their customers, or as simply an agent of the government.

"For companies, the question is how do you deal with the liability and other questions that come with that," Daniel said. "These are very real impediments, and why I think we need to get

past the endless discussions of public-private partnerships and start talking about what we can do to coordinate actions against these groups so we can have a more strategic impact on the adversary."

This entry was posted on Wednesday 15th of April 2020 11:28 AM

THE COMING STORM

COVID-19 CYBER THREAT COALITION CYBER THREAT ALLIANCE JOE MENN MARK ROGERS MICHAEL DANIEL NICK ESPINOSA

28 thoughts on "COVID-19 Has United Cybersecurity Experts, But Will That Unity Survive the Pandemic?"

ALC MBCP

April 15, 2020

Excellent to see this level of collaboration!

markson

April 15, 2020

We will definitely go through this period of Covid-19. thanks for sharing.

Sharon FIles

April 15, 2020

way to rain on our parade, Brian. The goodwill I've seen is the only inspiring thing about this.

MoreDThanU

April 15, 2020

Super Nerds, Assemble!

Drone

April 15, 2020

When your assets are tightly grouped, you become a target that is much much easier to obliterate. A scattered thousand dedicated citizen-soldiers each armed with only a trusted rifle and a store of tack, will eventually win over a thousand battle tanks.

Andy

April 15, 2020

Cyber like any field is fiercely competitive

I'll help my customers but not the mass of jokers who pretend they have a place in our business! The majority of 'experts' are a bunch of pretenders who didnt get into these businesses for the passion but rather for a profitable occupation. If there's any amount of intellectual labor in this you're a fakin'!

The Sunshine State

April 16, 2020

Down with the miscreants !

Jim

April 16, 2020

Good write-up. Interesting sounding group.
But, the commenters, snarfed my coffee. Durn well up the nose. You thought everyone would go honest in time of an emergency? You never will see that, remember, they have to make a living also. So they widen their target zone. They spray a little more. It's never going to be " oh, where are my Nigerian princes".

Rosemary

April 16, 2020

Great reporting and so thorough. Thank you for sharing.

Rosemary Valdez

April 16, 2020

Thank you for the info Brian.

dead link

April 16, 2020

CTC link seems dead.

- BrianKrebs Post author

-

April 16, 2020

Which link? They both work for me.

Robert Scroggins

April 16, 2020

Good topic, Brian. I fervently hope that the IT security industry can use the cooperation that is developing to a significant advantage after the Coronavirus pandemic is under control.

Regards,

Tom Stockmeyer

April 16, 2020

We're glad to be helping CISA out Chris!

kindDave

April 16, 2020

there should be a law somewhere in the books to prosecute folks who cripple hospitals with cyber attacks, resulting in death of patients, for manslaughter or murder since it is intentional.

KoSReader600000

April 17, 2020

Are there any browser expert who care tell us honestly how to step-by-step load cybertreats rather long block list in the major browsers or any major browser? That would include, Firefox, Chrome, Chromium, Edge, Microsoft's adoption of the Chromium engine browser and so on?

I notice the cybertreats list removes the dot and just spells "dot" it for safety. Are there any, quick work arounds for that problem on a long list?

See blocklist:

ht tps://blacklist.cyberthreatcoalition.org/vetted/domain.txt

MikeOh Shark

-

April 17, 2020

I only saw a few occurrances of dot. Perhaps they belong in the urls that have it.

You can always open the txt file in something like LibreOffice and do a find and replace if the list has really been massaged to render it less useful.

You could make the list into a hosts file or import it into an ipset if you use a netfilter type firewall.

KoSReader600000

-

April 18, 2020

Hi MikeOh Shark

Thanks for do a find and replace idea. Yes, it does work. And, your host file idea is OK but a bit harder to implement. I see both Firefox and Chrome have the Enterprise Policy Generator add on that could also work. Also, Noscript, uMatrix, and Adblock plus have somewhat contorted methods of achieving the blocking list – some by blocking all scripts and others by blocking the whole URL.

I did find Hold Security in Brian's next post that has the block list with the actual URLs (with the normal dot) in a cvs format. It also could work will most of the above add ons. I need to test all of the ideas first to find a fairly easy implementation.

- BrianKrebs Post author

-

April 18, 2020

As far as I know, the Hold Security link refers to ALL domains registered with certain key words like "Coronoavirus" and "COVID". As I said in the story, there is NO scoring attached to those domains, so those daily and weekly lists should NOT be considered block lists. I only referenced them because no one else had published the entire corpus from which the suspected bad domains were being pulled.

KoSReader600000

-

April 18, 2020

Thank you Brian. I did not know those were just key words to construct a list. I did download the current list or over 100,000 domains from covid dot holdintegrity dot com and did tests to block all of them. The test produced extreme long times trying to get to other domains (maybe a problem with hold security an their long list).

Is this just a fact of domain running by major domain providers who also do ddos protection via sub-domains to avoid ddos attacks?

I don't know what to say except I though Hold Security was selective about the domains they listed. Oh well, it's back to other domain blocking lists.

irving roberts

April 17, 2020

what about domain resellers, are they the bigger problem? registrars not policing their customers

small business

April 19, 2020

This website was… how do you say it? Relevant!! Finally
I've found something which helped me. Many thanks!

David Walker

April 19, 2020

Respectfully @BrianKrebs calling Nick Espinosa "… a self-described 'security fanatic' …" is a little dismissive.

Nick Espinosa and my other cyber security colleagues, yourself included, are voices of reason with positive attitudes that resonate in working the problems. Finding solutions. Staying vigilant.

If I did not have colleagues like you, Nick Espinoza and support from the cyber security professionals on LinkedIN, I think I would have stuck my head in a gas oven with the pilot light shut off a long time ago.

Dealing with cyber security and cyberwarfare takes thick skin, a sense of humor and support.

I do hereby attest without any reservation that Nick Espinoza "Is a Cyber Security Fanatic." There you go, Nick's not self-proclaimed anymore.

Tom Trottier

April 25, 2020

I just added
https://blacklist.cyberthreatcoalition.org/vetted/domain.txt
to my HOSTS file like I do with MVPS
http://winhelp2002.mvps.org/hosts.htm
See instructions there for your OS

Tom Trottier

April 25, 2020

FWIW, the covid blocklist has 7412 entries. My HOSTS file now has 35k lines (incl comments) and i don't experience much slowdown accessing websites. I am using W10 on an i7 3612 and using 0.0.0.0 as my black hole for references to bad sites.

Jorden Hussey

May 6, 2020

I have read your post!

Bob Patterson

May 7, 2020

Great post!

Rev. Dave

May 8, 2020

great article, very helpful.

Comments are closed.