


by Cynthia Brumfield
Contributing Writer

Legions of cybersecurity volunteers rally to protect hospitals during COVID-19 crisis

News Analysis

Apr 23, 2020 • 6 mins

Cyberattacks Healthcare Industry Security

The COVID-19 Cyber Threat Intelligence League and other groups cooperate with the industry, law enforcement, and the government to prevent attacks on healthcare providers.



Credit: inkoly / Getty Images

Last month, some of the usual cast of online scammers and malware miscreants **promised to refrain** from attacking healthcare organizations or exploiting them during the COVID-19 crisis, showing a sense of honor unexpected from **ransomware** attackers and cryptocurrency thieves.

However, this ceasefire turned out to be a head-fake. Within a week of those vows, **malware** purveyors and con artists rushed to send out **phishing** emails while masquerading as healthcare organizations and even launched attacks against hospitals and other critical facilities. Last week, **Google alone** was blocking 18 million COVID-19 phishing or malware-delivery emails per day.

One group of esteemed hackers and cybersecurity experts couldn't stand idly by and watch cybercriminals take advantage of this unprecedented crisis or, even worse, damage overtaxed and much-needed healthcare facilities. So, Marc Rogers, head of sec ops for DEF CON and VP of cybersecurity strategy for Okta; Nate Warfield, senior security program manager at Microsoft; Chris Mills, also a key security player at Microsoft; and Ohad Zaidenberg, lead cyber intelligence researcher at Clearsky Cyber Security, formed the COVID-19 Cyber Threat Intelligence League (CTI League).

Early success at disrupting threat actors

This invitation-only group, which [one industry publication](#) called a cyber version of the Justice League, began work about a month ago seeking to mitigate threats and protect the digital well-being of the global healthcare system during the pandemic. Since **March 14**, the League's ranks of volunteers has skyrocketed with more than 1,400 vetted members in 76 countries spanning 45 different sectors, including cybersecurity, healthcare, technology, telecommunications, computer emergency response teams (CERTs), government, and law enforcement.

The organization's members have helped to lawfully take down 2,833 cybercriminal assets on the internet, including 17 designed to impersonate government organizations, the United Nations, and the World Health Organization. Moreover, the League has identified more than 2,000 vulnerabilities in healthcare institutions in more than 80 countries, notifying those organizations directly or through escalation to appropriate government or industry bodies, according to its [just-released inaugural report](#).

"I knew I had to do something to help" Zaidenberg tells CSO. "There is a really strong appetite for doing good in the community," Rogers said during [a webinar hosted by the Aspen Institute](#). "If we can't go out and have a beer, the next best thing is opening our laptop."

Hospitals are a particular worry for the group. "After [WannaCry](#) and [NotPetya](#), we realized hospitals were vulnerable to malware," Rogers said during the webinar. "Our idea was to find these vulnerabilities ...using tools like [Shodan](#)."

Coordination with healthcare, law enforcement

League members work through healthcare organizations' CISOs and suppliers and other key players as channels to the institutions to inform the hospitals of what they've discovered. Some of the vulnerabilities, however, are serious enough to get kicked up to the FBI or the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ([CISA](#)).

"We have seen, and are likely going to continue to see, an increase in bad guys taking advantage of the COVID-19 pandemic to target businesses, governments and individuals alike," Christopher C. Krebs, director of CISA tells CSO. "CISA is working around the clock with our public and private sector partners to combat this threat. This includes longstanding partnerships, as well as new ones that have formed as a direct result of COVID-19, including the COVID-19 Cyber Threat Intelligence League."

The CTI League also works with other organizations to help reach out to healthcare organizations, including the Health-ISAC (Health Information Sharing and Analysis Center.) "We were involved with them very early on," Errol Weiss, CSO for the Health-ISAC tells CSO. "We look to them for two pieces of information sharing. One is that they're doing a great job of collecting threat actor information and indicators of compromise. We're grabbing that information and sharing it with all our members," Weiss says.

"Then number two is where we've got these small organizations who are probably running vulnerable VPNs and don't know it or they've got RDP [remoted desktop protocol] open and don't know it. So, folks on the CTI League are doing the scanning and the sharing of that information and grabbing that. We're also notifying healthcare organizations who are not necessarily Health-ISAC members and try to convince them to take a look at that and take it seriously."

One of the goals of the CTI League is to help law enforcement, particularly if they find malware or situations that they believe are driven by nation-states. "If we can just help our law enforcement partners by cleaning the field, removing the low-hanging fruit...then that empowers the agency to focus on the bigger threats...the really bad guys," Rogers said during the webinar.

Number of cybersecurity volunteer groups growing

The CTI League is not alone in rounding up cybersecurity volunteers to help organizations, particularly healthcare organizations, during the coronavirus crisis. Another group called the COVID-19 [Cyber Threat Coalition](#) consists of several thousand volunteer security experts who are tracking online cybercriminal activity, particular the rise in new health-related domains that appear ripe for malicious activity.

Weiss says his team plans to work this group and other ad hoc emerging volunteer groups in much the same way his ISAC is working with the CTI League, namely by grabbing the indicators they have and sharing them with the group's members.

Yet another group, [Cyber Volunteers 19](#), was set up in the UK by Lisa Forte, founder of RedGoatCyber, along with cybersecurity practitioners Daniel Card and Radoslaw Gnat. CV19 says its primary purpose is to facilitate and enable a volunteer matchmaking that gives healthcare services access to a pool of cybersecurity experts.

As the number of volunteer efforts grow to help tackle COVID-19 threats and scams, it's clear the current crisis has brought many members of the industry together with a sense of common purpose. "We've never seen this level of collaboration across the board for all

aspects of the problems that are cropping up due to the pandemic,” Rogers said.

Krebs says his agency is finding it easy to work with groups like CTI League. “The voluntary nature of our work with stakeholders and our longstanding role facilitating coordinated vulnerability disclosure efforts allows us to easily collaborate with groups like this, which share threat information and mitigation techniques in near real time,” he says. “We look forward to continuing to work with the CTI League and all our partners to combat malicious cyber targeting during this complex and evolving situation.”

by **Cynthia Brumfield**
Contributing Writer




Cynthia Brumfield is a veteran communications and technology analyst who is currently focused on cybersecurity. She runs a cybersecurity news destination site, Metacurity.com, consults with companies through her firm DCT-Associates, and is the author of the book published by Wiley, Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework.

More from this author



Most popular authors

Jon Gold
Senior writer

 **Shweta Sharma**
Senior Writer

 **Joe Sullivan**
Contributor

Show me more

Popular Articles Podcasts Videos

01

Feature

Accenture takes an industrialized approach to safeguarding its cloud controls

By Aimee Chanthadavong
Dec 11, 2023 • 8 mins

Application Security Cloud Security Compliance

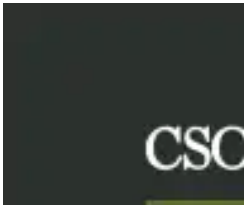
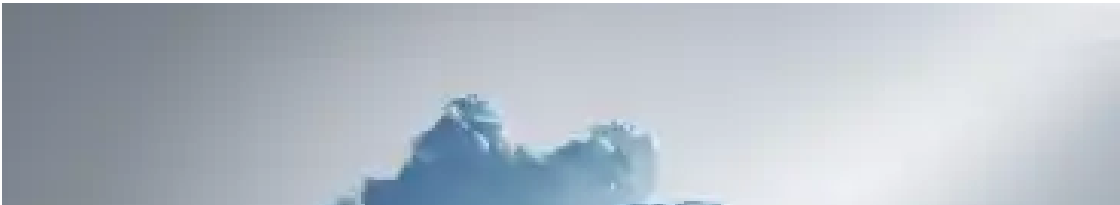
02

Podcast

CSO Executive Sessions Australi

Nov 20, 2023 • 15 mins

CSO and CISO



About



About Us

Advertise

Contact Us

Foundry Careers

Reprints

Newsletters

Brandposts

Policies



Privacy Policy

Cookie Policy

Copyright Notice

Member Preferences

About AdChoices

E-commerce Links

Your California Privacy Rights

Privacy Settings

Our Network



CIO

Computerworld

Infoworld

Network World

