



PRIVACY

Volunteer cybersecurity pros say they've stymied hacks against health care organizations

The group say it's dismantled nearly 3,000 malicious domains and identified more than a 2,000 software vulnerabilities.

BY SEAN LYNKAAS • APRIL 21, 2020



(Getty Images)

SHARE



volunteer group of cybersecurity professionals formed to protect computer networks during the coronavirus pandemic says it has helped dismantle nearly

Subscribe to our daily newsletter.

SUBSCRIBE



“The threats are coming in like a firehose; as fast as we can take things down, there are new [threats] there,” said Marc Rogers, who is an executive with cybersecurity company Okta and one of the founders of the volunteer group.

Known as the Cyber Threat Intelligence (CTI) League, the group’s membership has soared from a few dozen since its [founding](#) last month to some 1,400 people in 76 countries today. Security specialists from technology giants like [Microsoft](#) are members, and the group says it has formed close connections with law enforcement agencies.

Their services are in high demand as health care organizations strain to deal with COVID-19, which has killed more than 175,000 people worldwide. Spies and criminal groups have looked to exploit the pandemic, adapting their phishing and impersonation attempts to fears around the virus.

Some of the software vulnerabilities that the volunteers are finding at [health care](#) organizations have long been identified as popular with hackers. That includes a flaw in the [virtual private network](#) software Pulse Secure, which allows hackers to gain remote access to an organization’s server and steal credentials. Although disclosed last year, many private and public-sector organizations have yet to apply the software update. Last week, the U.S. Department of Homeland Security [said](#) its cybersecurity wing had seen hackers exploit the vulnerability to deploy [ransomware](#) on hospital IT systems and U.S. government agencies.

“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,” Chris Krebs, head of DHS’s [cybersecurity division](#), said Tuesday, touting his agency’s work with the CTI League.

In a [report](#) released Tuesday, the CTI League also said it was scouring the dark web for stolen login credentials used at medical organizations. “A large amount of the credentials reported by CTI League volunteers was stolen from breached sites, which we see hundreds each week,” the volunteers wrote.

The group has notched some early wins in its anti-hacking efforts. Last month, it helped the U.S. [Department of Health and Human Services](#) fix a flaw in its website that redirected visitors to a data-stealing web domain.

A far more serious threat has emerged in the [Czech Republic](#), where authorities last week

Subscribe to our daily newsletter.

[SUBSCRIBE](#)

A spearphishing campaign against numerous health care organizations that preceded the attacks was a cleverly crafted attempt to fool the targets, a Czech official told CyberScoop.

“The situation is very dynamic,” the official, who spoke on the condition of anonymity, said of the malicious cyber campaign. “It’s still ongoing. We’re sharing information on the threat with our partners and allies.

It remains to be seen how the CTI League can help the Czechs deal with the cyberthreat. The volunteers said they are closely monitoring the situation and trying to help where they can.



Written by Sean Lyngaas

Sean Lyngaas is CyberScoop’s Senior Reporter covering the Department of Homeland Security and Congress. He was previously a freelance journalist in West Africa, where he covered everything from a presidential election in Ghana to military mutinies in Ivory Coast for The New York Times. Lyngaas’ reporting also has appeared in The Washington Post, The Economist and the BBC, among other outlets. His investigation of cybersecurity issues in the nuclear sector, backed by a grant from the Pulitzer Center on Crisis Reporting, won plaudits from industrial security experts. He was previously a reporter with Federal Computer Week and, before that, with Smart Grid Today. Sean earned a B.A. in public policy from Duke University and an M.A. in International Relations from The Fletcher School of Law and Diplomacy at Tufts University.

In This Story

[INTERNATIONAL](#)[MARC ROGERS](#)[CTI LEAGUE](#)[CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY \(CISA\)](#)[DEPARTMENT OF HOMELAND SECURITY \(DHS\)](#)[CHRIS KREBS](#)[DOMAINS](#)[SPEARPHISHING](#)[CZECH REPUBLIC](#)[CYBERTHREATS](#)[DEPARTMENT OF HEALTH AND HUMAN SERVICES \(HHS\)](#)[VULNERABILITIES](#)

Subscribe to our daily newsletter.

[SUBSCRIBE](#)

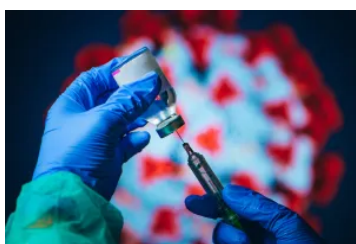
More Scoops



Conti ransomware gang victimized US health care, first-responder networks, FBI says

The Conti ransomware gang is behind the attack on Ireland's health care system, too.

BY TIM STARKS



COVID-19 hacking extends to supply chain for controlling vaccine temperature, IBM says

BY SEAN LYNGAAS



Health sector mobilizes defenses following Ryuk ransomware warning

BY SEAN LYNGAAS

Subscribe to our daily newsletter.

SUBSCRIBE

BY SEAN LYNKAAS

CISA turns to security experts with street cred to protect health sector

BY SEAN LYNKAAS

US cyber officials try to channel Liam Neeson in responding to coronavirus threats


BY SEAN LYNKAAS

Philadelphia-area health system says it 'isolated' a malware attack

BY SEAN LYNKAAS

Latest Podcasts



 How Troy Hunt knows if you've been hacked and Washington tries to understand AI



 Why pig butchering is the worst kind of online scam

Subscribe to our daily newsletter.

SUBSCRIBE



 **How the FBI fights ransomware**



 **Iranian attacks on U.S. water systems and the data broker economy**

Technology

DHS seeks information for CISA analytics and machine learning project

US and UK release guidelines for secure AI development

Microsoft upgrades security for signing keys in wake of Chinese breach

White House executive order on AI seeks to address security risks

Subscribe to our daily newsletter.

SUBSCRIBE

Coker tells Senate committee that he'd follow ONCD's current path if confirmed to top cyber position

CISA budget cuts would be "catastrophic," official says

DC Board of Elections breach may include entire voter roll

Threats

North Korean hacking ops continue to exploit Log4Shell

LogoFAIL vulnerabilities impact vast majority of devices

Dangerous vulnerability in fleet management software seemingly ignored by vendor

Feds: Iran-linked hacking campaign a 'clarion call' for digital defenses

Policy

~~CISA's Goldstein wants to ditch 'patch faster, fix faster' model~~

Subscribe to our daily newsletter.

SUBSCRIBE

Senate panel advances Coker's nomination to head ONCD

Reform bill would overhaul controversial surveillance law

SEC sues SolarWinds and CISO for fraud



ABOUT US

FEDSCOOP

DEFENSESCOOP

STATESCOOP

EDSCOOP

CYBERSCOOP

WORKSCOOP

Subscribe to our daily newsletter.

SUBSCRIBE

ADVERTISE WITH US

AD SPECS

(202) 887-8001

HELLO@CYBERSCOOP.COM

FB TW LINK IG

Subscribe to our daily newsletter.

SUBSCRIBE