Articles / News

Security Experts Battle Hackers, COVID-19 Cyberattacks

Jessica Lyons Hardcastle | Managing Editor
March 27, 2020 8:18 PM

Threat researchers at Microsoft, ClearSky Cyber Security, and Okta are among the hundreds of security experts helping the medical community fight COVID-19 cyberattacks through the COVID-19 CTI League.

Ohad Zaidenberg, lead cyber intelligence researcher at ClearSky Cyber Security, founded the group this week (CTI stands for cyber threat intelligence). And in just nine days, the league counts more than 450 members from more than 35 countries worldwide, he said.

“Since the corona crisis came out, I started to notice more and more hackers use it to gain profit,” he told SDxCentral. “When the pandemic became a global crisis, I understood these malicious activities can cause

Justice League

It's important to note that these volunteers aren't quitting their day jobs, which have also become busier than usual as cyber criminals try to exploit the virus for financial gain — and at the expense of the businesses and individuals that the volunteers' companies secure.

Nate Warfield, who manages Windows, Azure, and Hyper-V vulnerabilities for Microsoft and also helped start the COVID-19 CTI League, says between the two there's little time for sleep.

"I, like most of the members of CTI League, have full time jobs in InfoSec," he said. "I saw this as an opportunity to donate my spare time, skills, and experience to help our brothers and sisters in the medical field who may not have the funding those of us in tech companies do."

The league's volunteers identify, analyze, and neutralize threats that look to exploit the pandemic. While the group's management team won't elaborate on what exactly that looks like or give specifics about their successes, "we're here to support the medical sector, to prevent attacks, to help them handle and mitigate attacks," Zaidenberg said.

"Moreover, the community allows us to create a network of goodwill — a network of people that want to share information and help each other during this crisis," he added. "In such days that every country closes its borders, we open it virtually."

COVID-19 Cyberattacks

And there's definitely no shortage of COVID-19 threats these days. Cisco Talos' latest threat report says the team continues to see malware and phishing campaigns using coronavirus-themed lures along with fraud and disinformation campaigns and attacks against medical and research organizations performing COVID-19 work.

"Talos has not yet observed any new techniques during this event. Rather, we have seen malicious actors shift the subject matter of their attacks to focus on COVID themes," it said. The Cisco threat intelligence team recommends that businesses protect against these threats using "the same strong security

As a growing number of employees work from home, and use software-as-a-service (SaaS) and cloud-based remote connectivity services, attackers will try to collect credentials that potentially allow them to access these SaaS accounts and companies' data, warns Adam Meyers, who oversees all of CrowdStrike's intelligence gathering and cyber-adversarial monitoring activities.

"The eCrime big game hunting (BGH) ransomware industry in particular leverages Remote Desktop Protocol (RDP) brute forcing or password spraying for initial entry," Meyers wrote in a blog. "As many sophisticated BGH actors remain highly active at present, they will likely attempt to capitalize on possible staffing disruptions COVID-19 may bring to organizations, as well as attempt to compromise employee devices while they work remotely.

100,000+ Coronavirus Domains Registered

Unit 42, the Palo Alto Networks threat intelligence team, notes that over the past few weeks more than 100,000 of domains have been registered containing terms like "covid," "virus," and "corona." While not all are malicious, "all of them should be treated as suspect," wrote Ryan Olson, VP of threat intelligence at Unit 42 in a threat briefing. "Whether they claim to have information, a testing kit, or a cure, the fact that the website didn't exist until the pandemic became news should make you very skeptical of their validity."

Additionally, VMware Carbon Black calls out masquerading as one of the biggest cyber threats associated with the pandemic. "Cybercriminals are now most commonly masquerading fake VPNs, remote meeting software and mobile apps," according to its latest Technical Analysis.

Ultimately, hackers want to profit off of the pandemic, Zaidenberg said. "It can be phishing attacks with social engineering methods playing on the fear of people or their wish to find a vaccine, it can be ransomware attacks against hospitals, it can be wipers. Every attack has its cases, and in some cases, the causes might be death."

Read Next

Samsung stumped by AT&T's 5G open RAN plan

Interview | **Dan Meyer** | December 12, 2023

VMware integration to cost Broadcom $1B, Carbon Black goes on the block

Interview | **Dan Meyer** | December 12, 2023

Kinetica aims to enable telcos to converse with their data

Analysis | **Taryn Plumb** | December 11, 2023

Security shakeup — Palo Alto Networks, Cato, Crowdstrike, Zscaler take the lead

Opinion | **Matthew Palmer** | December 11, 2023

BT betting big on a smarter SD-WAN approach

Popular News

1 **Versa Networks brings SD-WAN, zero trust to the Thunderdome**

2 **Will Apple Vision Pro unlock private 5G potential?**

3 **Fortinet augments cybersecurity operations with genAI**

Trending Companies

VMware

Broadcom

Palo Alto Networks

Cato Networks

Zscaler

CrowdStrike Inc

Accenture

Fortinet

Study Up

1 **Exclusive Dell'Oro SASE Market Report**

2 **What is multifactor authentication?**

3 **What is software defined networking (SDN)? Definition**

4 **What is zero-trust security?**

5 **What is zero-trust network access (ZTNA)?**

Product News

AFL-CIO and Microsoft announce new tech-labor partnership on AI and the future of the workforce

Intel Labs to present industry-leading AI research at NeurIPS 2023

Armada raises more than $55M to bridge the digital divide

Rambus protects data center infrastructure with Quantum Safe Engine IP

10% of organizations surveyed launched genAI solutions to production in 2023

Sponsored Content

Latest from SDxCentral

Samsung stumped by AT&T's 5G open RAN plan

Interview | **Dan Meyer** | December 12, 2023

"I don't know that the way they've chosen to do it is necessarily what I've seen work in the past," Samsung VP Alok Shah said.

VMware integration to cost Broadcom $1B, Carbon Black goes on the block

Interview | **Dan Meyer** | December 12, 2023

Broadcom is also killing VMware's perpetual licensing option in favor of a subscription model.

Kinetica aims to enable telcos to converse with their data

Analysis | **Taryn Plumb** | December 11, 2023

Kinetica’s real-time GPU database was built for spatial and time-series workloads. With its telecommunications platform, users can ask complex questions and visualize and interact with billions of data points.

Security shakeup — Palo Alto Networks, Cato, Crowdstrike, Zscaler take the lead

Opinion | **Matthew Palmer** | December 11, 2023

To get a pulse on the changing security market, we analyzed over 750K pageviews. Our data reveals a major shift in how readers secure their IT infrastructure.