CTI League Darknet Report 2021

Exposing Criminal Activity Targeting the Healthcare Industry During COVID-19

The healthcare industry has been bombarded with concurrent cyber threats over the last 12 months as they are on the front lines of the COVID response. Caregivers have faced many challenges during this period, including workforce shortages, overcrowded facilities, and the lack of personal protective equipment (PPE) to name a few. Ransomware however, poses the greatest cyber security threat facing the healthcare industry and caused several directly related deaths during this pandemic.

In a report released by the CTI League earlier today, many points of interest have been covered in detail. In this article, we'll cover some of the key insights and you can read the full report below.

What is the CTI League?

The CTI League is a collective of cyber security professionals who work together with law enforcement organizations to identify and collect CTI (Cyber Threat Intelligence) to prevent ransomware from gaining access. Within the CTI League, there's an entire team of security researchers who monitor cybercriminal underground networks within the Darknet and Deep/Dark web, called CTIL-Dark. CTIL-Dark's goal is to reduce the likelihood and impact of cyber threats so these organizations can continue to provide care to the public consistently.

CTIL-Dark Insights and Assessments

CTIL Dark found that the top five ransomware variants that impacted healthcare in 2020 were Maze, Conti, Netwalker, REvil, and Ryuk. In total so far, attacks from these groups have affected more than 100 organizations.

Recent Posts

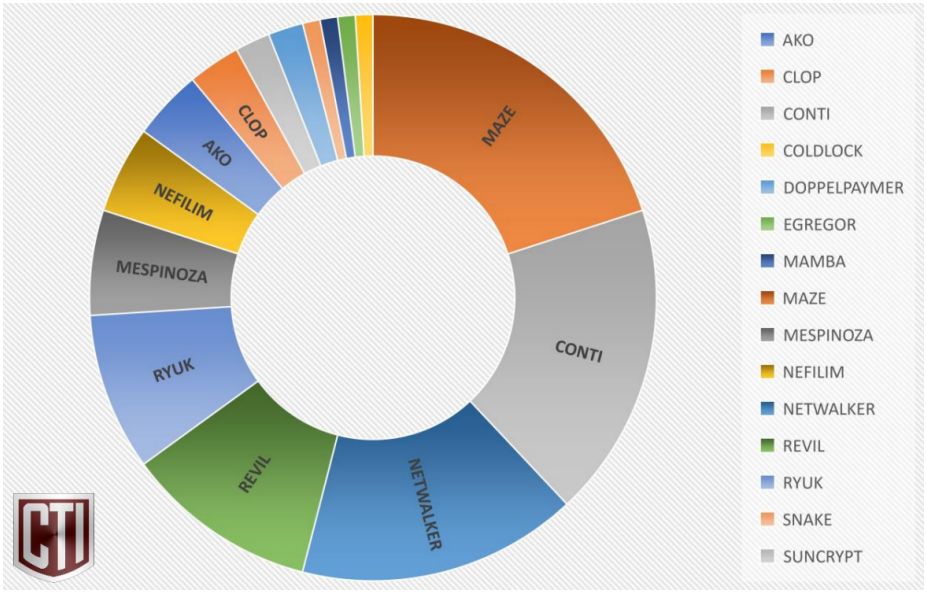
The Risks of DCE/RPC Service Enumeration (https://www.criticalpathsecurity.com/the-risks-of-dce-rpc-service-enumeration/)

Stop Sending Sensitive Data with Cleartext Protocols (https://www.criticalpathsecurity.com/stop-sending-sensitive-data-with-cleartext-protocols/)

SNMP GetBulk Reflected Distributed Denial of Service Attack (https://www.criticalpathsecurity.com/snmp-getbulk-reflected-distributed-denial-of-service-attack/)

Patrick Kelley interviewed by 11Alive/NBC regarding NameDrop (https://www.criticalpathsecurity.com/patrick-kelley-interviewed-by-11alive-nbc-regarding-namedrop/)

Holiday Turkey With A Side Of Scam (https://www.criticalpathsecurity.com/holiday-turkey-with-a-side-of-scam/)



(https://www.criticalpathsecurity.com/wp-content/uploads/2021/02/46ccd9b0-f5e4-410e-bfca-f40cfa8b6100.png)

Nearly two-thirds of healthcare cybercrime victims were in North America and Europe, with victims in every populated continent. They also found that the proliferation of dark markets and supply chains significantly lowered the barrier to entry for cybercriminals to affect healthcare.

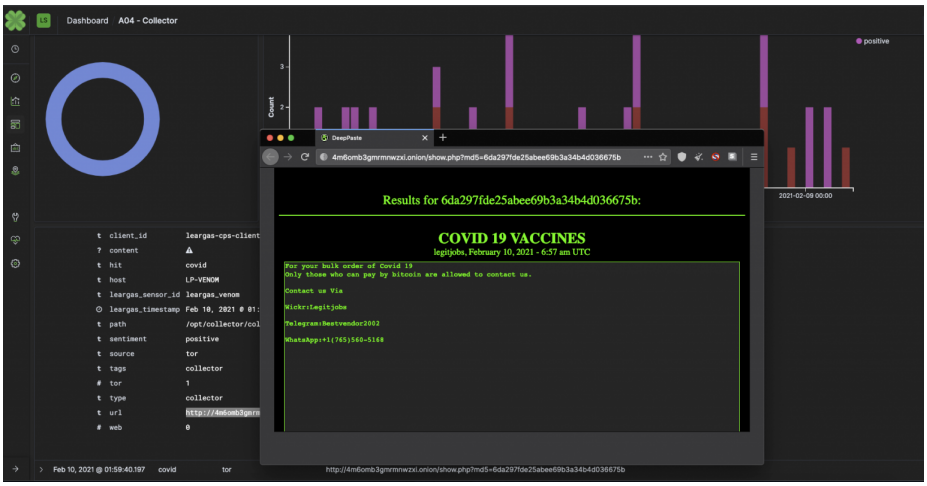
(https://www.criticalpathsecurity.com/wp-content/uploads/2021/02/b4b0e221-7607-4476-b9c5-3db6337644c1.png)

Democratized Intelligence: Critical Path Security observed fake Vaccine and PPE vendors on the Darknet seeking not only to rip off those desperate to protect themselves, but also to gain foothold on networks--wreaking havoc on operations. This intelligence was shared with CTIL Dark and their law enforcement partners to further advance our common objectives.

Email

Name

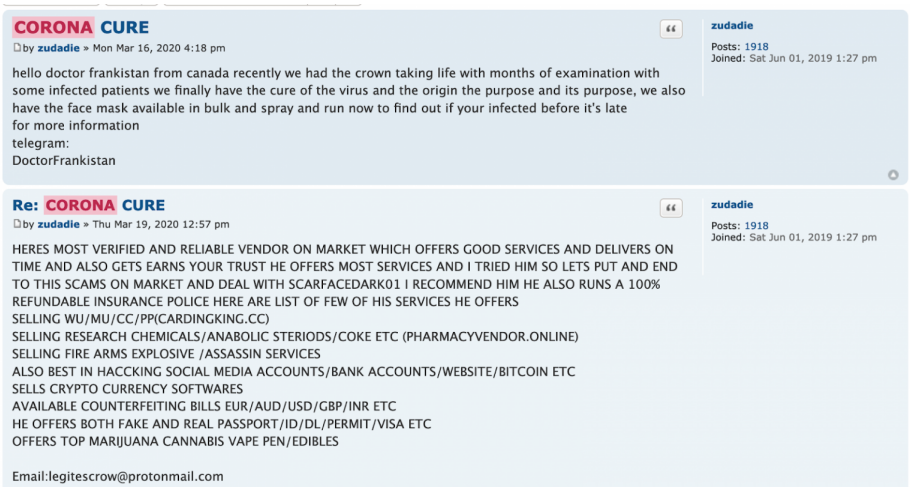
JOIN NOW



(https://www.criticalpathsecurity.com/wp-content/uploads/2021/02/00424f09-0955-4364-916f-1391d968273c.png)

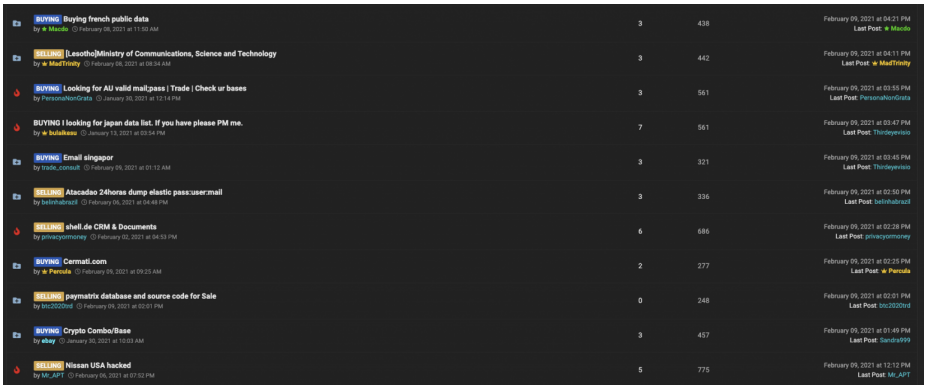
Threat actors that deploy ransomware as part of their attack method will almost certainly increasingly target the healthcare industry as they are most vulnerable during the pandemic.

Threat groups will continue to leverage underground message boards and other Chan forums as a way to test out different COVID-themed conspiracies before launching their surface web disinformation campaigns.



(https://www.criticalpathsecurity.com/wp-content/uploads/2021/02/d488f7eb-07fd-42ca-981a-12a4f33f49a1.png)

Threat actors will continue to leak, trade, and sell databases containing Protected Health Information (PHI) obtained through targeted breaches.



(https://www.criticalpathsecurity.com/wp-content/uploads/2021/02/0a0bd41f-0d84-438a-8813-ca307a197251.png)

Critical Path Security is proud to be a part of this global effort and will continue to work diligently to identify and notify authorities of new findings. We must all do our part to fight these types of attacks if we are to fully overcome this pandemic. With your help, we will win this fight.

Those who want to help or to benefit from the CTI-League's efforts, particularly healthcare organizations, are encouraged to join via the website at https://cti-league.com/join (https://cti-league.com/join)

Read the Full Report

Darknet Report 2021 Download (https://www.criticalpathsecurity.com/wp-content/uploads/2021/02/CTI-League-Darknet-Report-2021.pdf)

Darknet

202

YOU MIGHT ALSO LIKE

Phishing: What you should know! (https://www.criticalpathsecurity.com/phishing-what-you-should-know/)

January 30, 2020

Wanted: Women to Work in Male-Dominated Fields (https://www.criticalpathsecurity.com/wanted-women-to-work-in-male-dominated-fields/)

February 28, 2018

The Importance of Cybersecurity for CEOs: Lessons and Recommendations (https://www.criticalpathsecurity.com/the-importance-of-cybersecurity-for-ceos-lessons-and-recommendations/)

September 25, 2023

(https://www.linkedin.com/company/critical-path-security/)

(https://twitter.com/criticalpathsec)

(https://www.facebook.com/criticalpathsec)
