



# Darknet Report 2021

This publication would not be possible without the tireless dedication of those who remain in the shadows to provide these details at risk to their own identities, employers, and personal safety.

Thank you for shining your lights in the darkest of places.

CTI League Team Leaders

## Letter from the team leaders

Welcome to the CTI League's first darknet activity report.

COVID has changed the very fabric of our society: from how we live to how we work. For many people worldwide, the new normal of 2021 includes working from home, schooling from home, and telemedicine. Doctors work to manage patients and a pandemic simultaneously.

The effects of COVID have been felt everywhere, including the cyber threat landscape. Criminals did not hesitate or waste time when it came to taking advantage of the pandemic. While the world was focused on health outcomes, threat actors exploited the new conditions. While some criminals promised not to capitalize on COVID, they did so anyway.

Criminals increased their targeting of healthcare organizations, including hospitals at the front lines of care delivery. Governments and critical infrastructure were not spared either, as attacks on those segments spiked in the early days of the pandemic.

Promises of treatments, testing, and critical medical supplies filled the internet, acting as a front for malware distribution and data collection. Additionally, evidence of 'Disinformation as a Service' (DaaS) and critical elements of disinformation itself also appeared at an escalated rate. As members of our societies grew increasingly concerned, adversaries grew bolder.

The CTIL Dark team within the CTI League has spent countless hours volunteering their time to assist law enforcement, administrators, business leaders, and the general public. Their dedication to helping protect these entities and individuals against emerging threats, cannot be understated. We are eternally grateful for their support. CTIL Dark's efforts have not gone unnoticed, so the CTI League saw it fit to publish this report to showcase a few of their many success stories.

This report serves as a breakdown of some of the CTIL Dark's findings to what the criminal element was doing during the first half of the year. We're proud to present their efforts to the public and encourage you to reach out should you have any questions or comments.

CTIL Dark Team Leads, CTI League

## Table of Contents

Letter from the team leaders .....	3
Executive Summary .....	5
Key Insights .....	7
Key Assessments .....	7
Threats.....	8
Ransomware.....	9
Initial Access Brokers .....	13
Opportunistic Cybercriminals.....	14
Disinformation Campaigns.....	16
Scammers.....	19
Phishing .....	21
Databases.....	22
CTIL Dark in Action .....	23
Polish nationwide hospital alerting .....	23
Pre-empting access to large Catholic Healthcare Organization .....	24
Summary .....	25
About the CTI League.....	26

## Executive Summary

The healthcare sector faces many threats, including those from supply chain shortages, spikes of severe illness, and adversaries willing to do harm. While this report focuses on only one of these, we expect it will be read in context of these other risks and acknowledging the superhuman efforts of so many in healthcare during this impossible time.

The CTI League aims to create a safer cyberspace for the healthcare industry worldwide from cyber-attacks by supplying reliable information, reducing the risk of compromise, supporting security departments, and neutralizing cyber threats. Within the CTI League there is an entire team of security researchers and law enforcement personnel who monitor various cybercriminal underground networks within the Darknet and Deep/Dark web. We have termed 'CTIL Dark'. Their days are spent looking for signs of data breaches, targeted attacks, and any other cybercriminal activity that may impact the medical industry or general public health. CTIL Dark focuses on three different aspects of threats:

- Threats on the healthcare industry - CTIL Dark focuses on discovering emerging threats to healthcare organizations. CTIL Dark provides an overview of the risks that can affect these organization's networks and disrupt their ability to save lives. Data breaches, network access, and compromised assets offered for sale in the darknet are examples of these threats.
- Threat actors operating in the darknet – CTIL Dark provides actionable threat intelligence to our law enforcement partners on the specific threat actor Personas of Interest (POI) who are targeting the healthcare industry.
- Threats to Public Health and Safety – CTIL Dark is focused on finding cyber threats to public health and safety, such as purchasing fake COVID vaccines, which can result in a fatal infection or even death. The CTI League escalates the threats discovered to inform our associates and law enforcement partners for the next steps.

The report will be the first in a series exposing what CTIL Dark has discovered and how it has responded. From participating in operations in concert with law enforcement to collecting evidence on COVID cure scams to a HUMINT (human intelligence) operation that prevented threat actors from gaining access to a European hospital chain in less than 8 hours. CTIL Dark's efforts have not gone unnoticed. The CTI League recognizes there is value in greater understanding and awareness among the public and is revealing some of the behind-the-scenes activities that keep them safe from adversaries, whether criminal, ideological, or state-sponsored. Readers of this report will:

- Learn about ransomware groups and campaigns targeting healthcare organizations during the COVID pandemic, broken down by region and by threat group.
- Explore of dark markets and sellers of COVID-themed medical products.
- Understand the supply chains and dark markets for access to compromised healthcare environments.
- See examples of the CTIL Dark in action during 2020.

This report exists in two forms. A general version of the information will be released to the public. A more detailed description will be made available to law enforcement agencies and government entities by request only.

Please contact a CTI League administrator for more information – [le@cti-league.com](mailto:le@cti-league.com).

---

### Key Insights

---

- CTIL Dark found that the top five ransomware variants that impacted healthcare in 2020 are Maze, Conti, Netwalker, REvil, and Ryuk, affecting over 100 organizations.
- CTIL Dark found that nearly two-thirds of healthcare cybercrime victims were in North America and Europe, with victims in every populated continent.
- CTIL Dark found that threat actors moved to target the healthcare industry with ransomware because of their increased prominence during the pandemic and their high susceptibility.
- CTIL Dark found that demand for backdoor access to healthcare networks increased significantly from prior years, as did the number of criminals acquiring and selling that access.
- CTIL Dark found that the proliferation of dark markets and supply chains significantly lowered the barrier to entry for cybercriminals to affect healthcare.

---

### Key Assessments

---

- CTIL Dark assesses that the threat actors that deploy ransomware as part of their attack method will almost certainly increasingly target the healthcare industry as they have emerged as most vulnerable during the pandemic.
- CTIL Dark assesses that as global work-from-home numbers continue to rise, threat actors will increasingly exploit vulnerable remote access platforms as organizations implement them to support work from home.
- CTIL Dark assesses that 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.
- CTIL Dark assesses that phishing from targeted and opportunistic threat actors and from scammers will adapt to emerging COVID-themed trends to exploit target fear and curiosity.
- CTIL Dark assesses that threat actors will continue to leak, trade, and sell databases containing Protected Health Information (PHI) obtained through targeted breaches.

## Threats

Since the initial standup CTIL Dark has seen and mapped many trends and threats related to our mission of stopping threat actors from taking advantage of the healthcare system in a world stretched thin by COVID. We have found that there are a number of different types of threats exploiting the COVID pandemic. Some of these threats include opportunistic cybercriminals, scammers, Nation-state disinformation campaigns, initial access brokers, targeted ransomware, phishing, and the hybrid/other threats.

**Opportunistic cybercriminals within darknet marketplaces have mirrored the pandemic from the very start.** When there was a shortage of masks and COVID test kits, darknet vendors started selling them. When the United States president embraced Hydroxychloroquine as a way to treat COVID, the darknet vendors who once sold cocaine and other illicit drugs shifted to selling the anti-malaria medicine. The United States passed the COVID Relief Bill and immediately following there was an increase in tax identity theft for stimulus relief fraud.

**Disinformation campaigns organized by Nation-state threat actors and Conspiracy-based groups have been observed** on darknet Chan forums and other underground message platforms before dissemination via automated scripted bot programs and fake medical personnel personas on social media.

**Initial Access Brokers (IABs) seek out vulnerable networks, and once they have access, they then resell that information to the highest bidder.** In many cases these IABs will sell victim access to ransomware groups through cybercriminal forums. In other cases, the IABs become ransomware operators themselves by joining a Ransomware-as-a-Service affiliate program.

**Ransomware and the groups that deploy them have become one of most sophisticated and well-funded and fastest-growing cybersecurity threats.** As the '2020 year of ransomware' continues, the attacks are only getting more extensive, targeted and more coordinated. Using malware to infiltrate a victim's network to encrypt their data and restrict access until payment is made (often through the form of cryptocurrency), the cybercriminals will often then decrypt the victim's systems and show proof that they have deleted the victim's data.

**Scammers are individuals or small groups with short term goals of cheating the end-user out of money or information.** CTIL Dark has interacted with scammers whose entire purpose was to sell a COVID cure that they didn't have to unsuspecting people in fear of the pandemic and the third-order effects that came with it.

## Ransomware

CTIL Dark found that perimeter vulnerabilities were the most common entry point in the healthcare-related Ransomware cases we examined. Adversaries leveraged unpatched vulnerabilities and weak, reused, or default passwords in remote connectivity systems, such as Remote Desktop Protocol (RDP) servers, to gain access to these servers and pivot farther into victim networks. This finding is surprising, as prevailing wisdom holds that most Ransomware stems from phishing or social engineering attacks. One reason for this may be that many organizations deployed remote connectivity hastily because of time-sensitive work from home mandates.

Part of the CTIL Dark capabilities involves tracking ransomware groups and instantaneous alerting if they pose a threat to the healthcare industry overall. Early on in the COVID pandemic, the CTIL Dark team collectors saw signs that multiple RaaS (ransomware as a service) groups would respect the healthcare groups' need to preserve operations during a global pandemic. The truce limited the threats and risks to hospitals and possibly showed some collaboration among these groups.

### Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus

*Figure 1 - Maze announces they will not target medical organizations during the pandemic*

The truth is that there is no honor among thieves, and as soon as the truce was broken by one, they all began to plunder any targets they could. The top five ransomware variants that have impacted the healthcare industry the most in the year 2020 are Maze, Conti, Netwalker, Revil and Ryuk, making up approximately 75% of all successful attacks tracked. From October to December the CTI League observed a dramatic uptick in focused attacks against healthcare entities, particularly small and medium sized hospitals and clinics, which impacted clinical workflows at hundreds of healthcare providers.

### **Why the CTI League Prioritizes Ransomware**

In 2020, the incidence of cyber attacks against healthcare organizations increased dramatically, and we believe that this trend will continue or accelerate. Unlike the majority of cyber attacks, Ransomware impairs an organization's ability to operate normally and can be destructive.

Cybersecurity issues that delay, degrade, or deny access to patient care can be deadly. Although no deaths have been conclusively linked solely to Ransomware, its impacts can impact patient care. For instance:

- In 2020 the CTI League learned of a cancer center Ransomware victim where staff and patients had to try rebuilding treatment regimen from memory.
- Diagnostic imaging techniques greatly improve outcomes in cases such as strokes and trauma, so loss of these systems from Ransomware denies these benefits.
- Delays in acute cardiac care, such as those when hospitals divert incoming ambulances to other facilities, lead to a significant increase in mortality rate.

Ransomware during the COVID pandemic can impact healthcare across a city or a region. Under normal conditions, a single hospital affected by ransomware can divert patients to other local facilities which can absorb the additional load. Under COVID, many hospitals are already near or at capacity and face workforce shortages, making it more likely that other facilities would reach or exceed capacity from a single hospital going on diversion. A Ransomware attack, such as the one in late 2020 in New England that hobbled over 100 facilities, could trigger a region-wide cascade.

The effects on patient care from a city-wide or regional care delivery overload can be dire and heartbreaking. Stories have recently emerged from Los Angeles where the pandemic circumstances, even without Ransomware, caused hospitals to stop taking in patients, and tied up ambulances for hours waiting in line at emergency rooms across the city. Ransomware could make similar situations more likely and more common.

At the same time, capabilities to prepare for and respond to Ransomware improve defenses against other cybersecurity issues. Organizations can decrease their likelihood of becoming a victim and reduce cost and time to recover. When adversaries exert more effort for a lesser impact, they tend to focus elsewhere, deterring future attacks against the sector and allowing healthcare organizations to continue delivering patient care to those who need it.

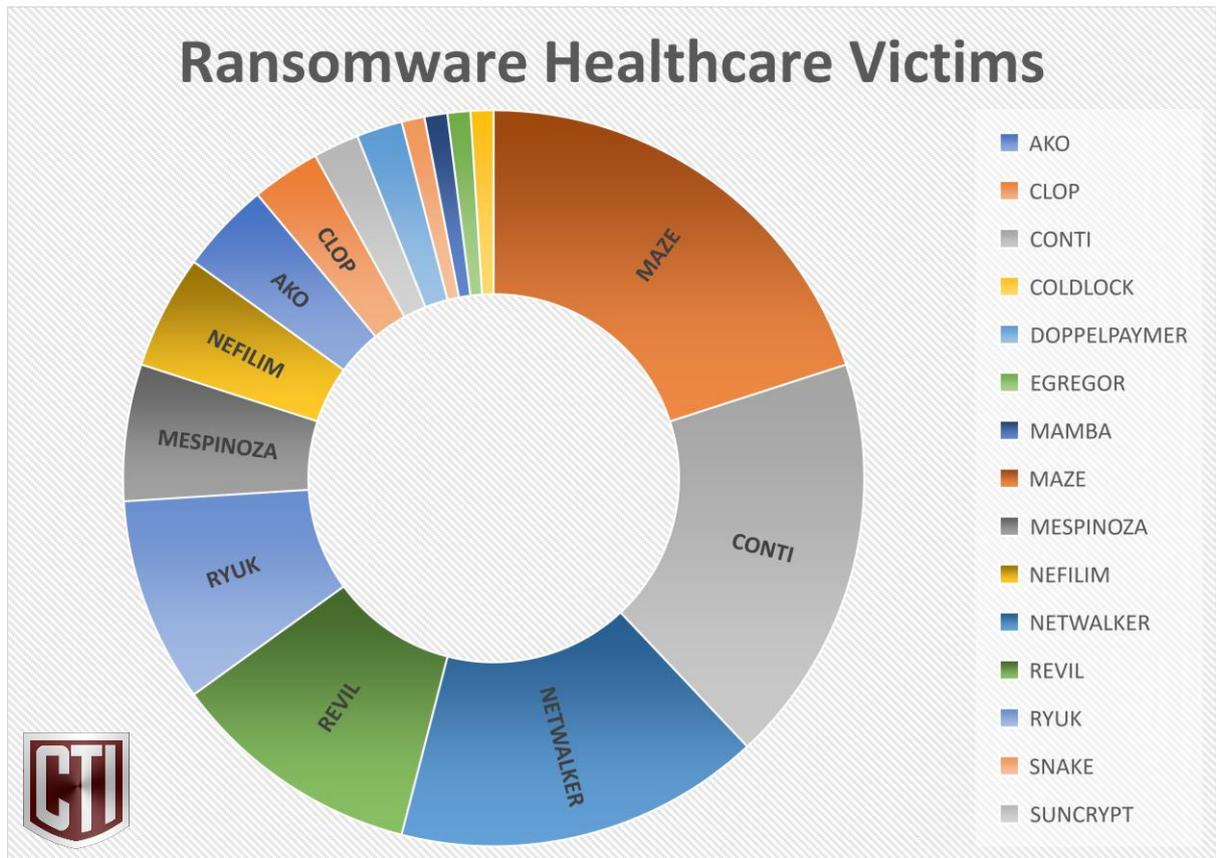


Figure 2 - Ransomware families by the number of healthcare organizations they have victimized

In March 2020, it is believed to have started with the hacking of Hammersmith Medicines Research in London by the Maze ransomware group, who likely targeted Hammersmith because they were researching a cure for COVID. CTIL Dark began extensive link analysis, intelligence collection, and general forensics in coordination with strategic partners and international law enforcement to uncover the actors' actual identities to assist in criminal justice. Our analysts conducted extensive link analysis, intelligence collection, and general forensics to help build a bigger picture. One of our analysts tracked the threat actor back to suspected Command and Control (C2) nodes or proxies located in Russia. The CTI League was able to share this information with Hammersmith IT teams, through our trust network, so they could block communications with the suspicious infrastructure.

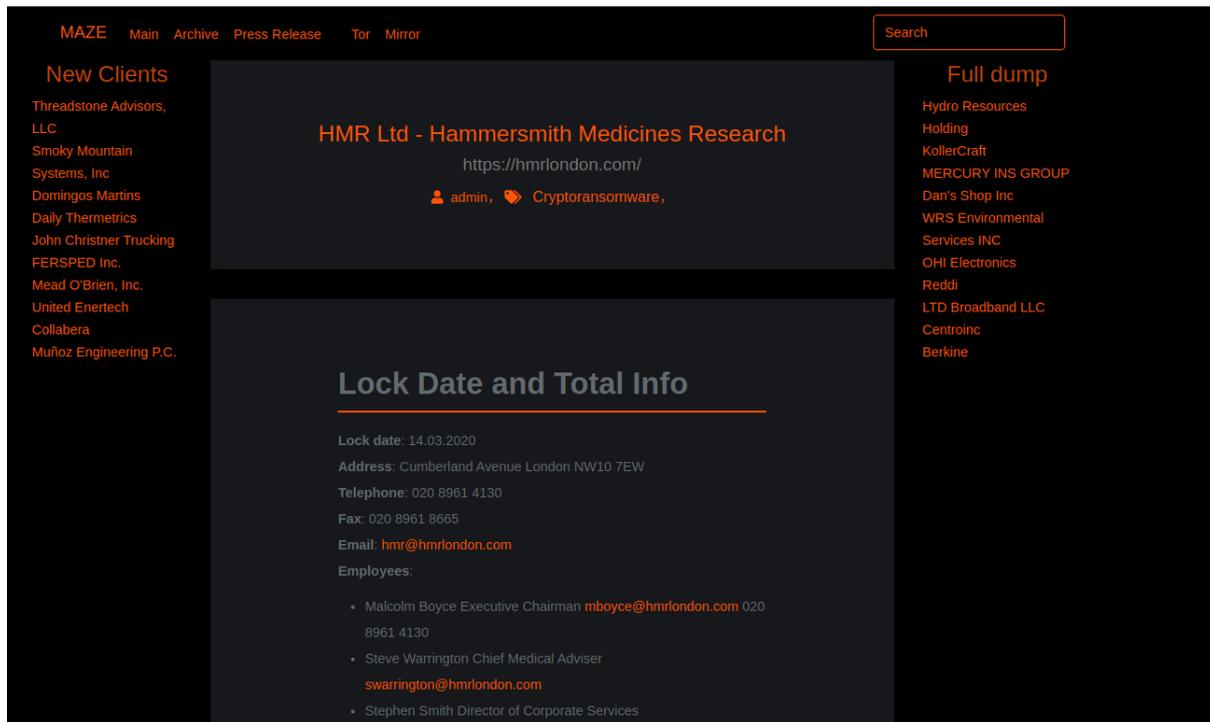


Figure 3 - Maze leaks data belonging to Hammersmith Medicines Research

Since the launch of the CTI League, the threat group that operates Maze ransomware shut down their operations. CTIL Dark assess that the threat group is now operating the Egregor ransomware. CTIL Dark assesses that the volume of ransomware attacks will continue into 2021. The actions of ransomware groups will not slow down nor stop at the door of the healthcare industry. The CTI League continues to pursue these groups and keep our healthcare and law enforcement partners apprised of our findings.

The CTI League assesses that Ransomware will remain one of the largest threats to healthcare delivery. Threat actors are likely to continue increasing their attack sophistication and volume, across the sector and their supply chain. The CTI League will continue to develop our tools to help our members track and counter this threat.

## Initial Access Brokers

With the increase in the number of employees working from home due to mandatory social distancing, the business of Initial Access Brokers (IAB) has boomed in the year 2020. An IAB is someone who gains access into a victim's network through several vectors, with the most common being through Remote Desktop Protocol (RDP) and then selling that access to the highest bidder. RDP is consistently compromised through a mix of open-source reconnaissance to find email formats and basic credential stuffing attacks to uncover passwords without tipping off internal detection methods.

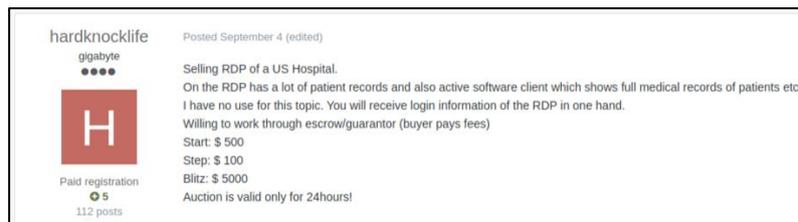


Figure 4 - Cybercriminal persona "hardknocklife" advertises RDP access to a US Hospital

In most cases, IABs sell directly to ransomware groups or become affiliates of Ransomware-as-a-Service programs to ensure they get highly compensated for the victim access they acquire. From Q2 2020 to Q4 2020, the number of IABs compromising and selling access to Healthcare and other lifesaving organizations has more than doubled. The highest impacted regions by IABs targeting the healthcare industry are North America, Europe, Asia, and the Middle East.



Figure 5 - Initial Access Brokers targeting Healthcare industry by Region

## Opportunistic Cybercriminals

CTIL Dark have observed opportunistic cybercriminals within darknet marketplaces exploiting the fears of individuals impacted by the COVID pandemic. This first became evident towards the end of Q2 when there was a global supply chain shortage in PPE, COVID test kits, and other critically needed medical items, which were observed advertised on multiple darknet marketplaces. One example observed was the rapid increase in Hydroxychloroquine sales postings to treat the COVID virus shortly after the United States president was shown on news media endorsing its use.

From Q2 to Q3 2020, the highest COVID-themed items advertised on darknet marketplaces were Hydroxychloroquine and COVID test kits. CTIL Dark discovered that many vendors that changed to advertising Hydroxychloroquine and other medical supplies on darknet marketplaces who previously sold or were still selling illegal drugs such as heroin, fentanyl, and cocaine.

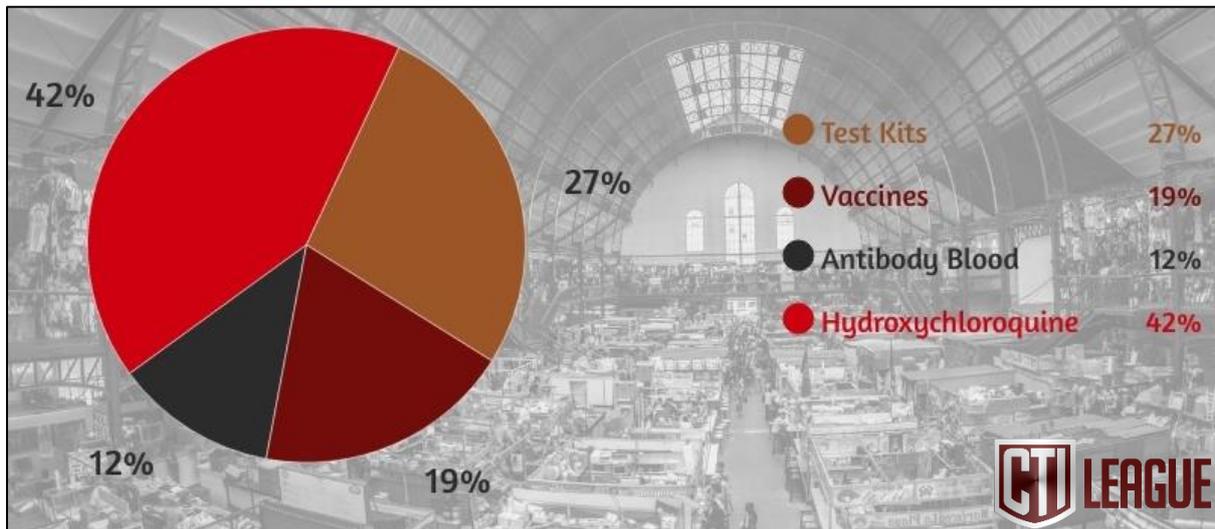
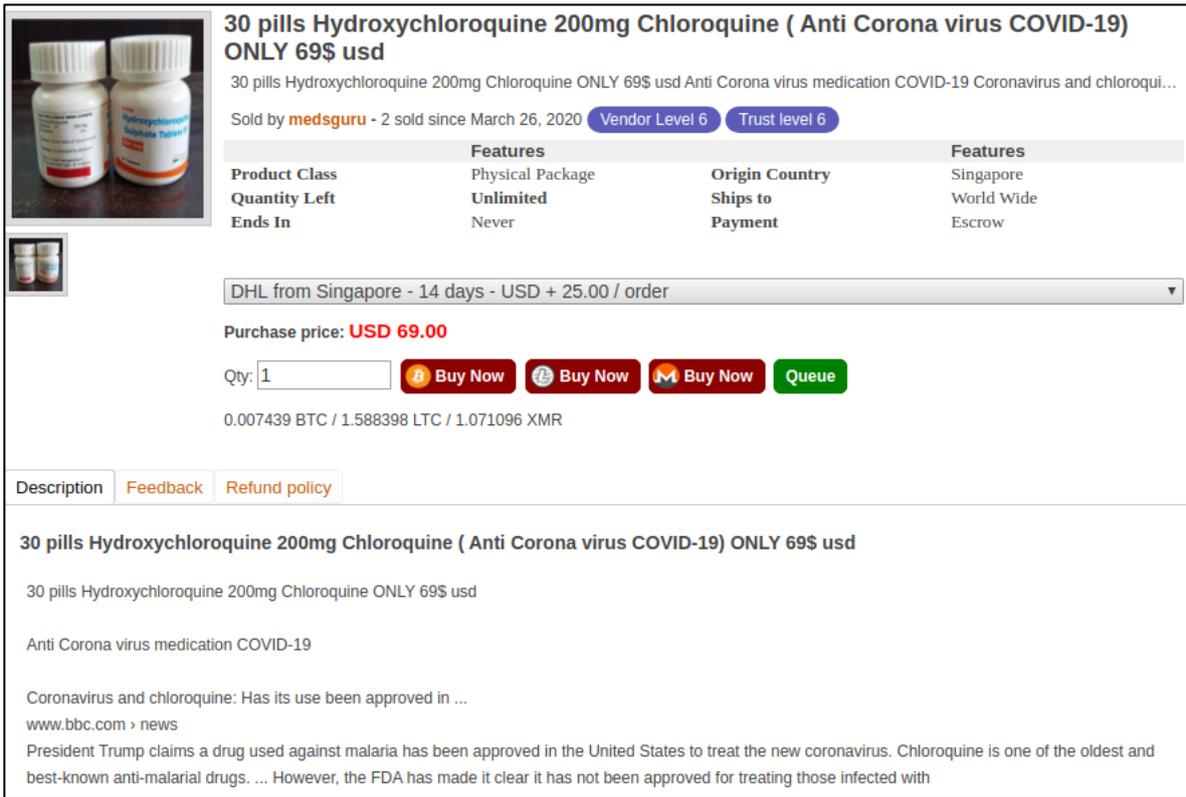


Figure 6 - COVID-themed medical advertisements in the cybercriminal underground

An example of an opportunistic cybercriminal is a darknet marketplace vendor using the pseudonym "medsguru" who advertised the sale of 200mg of Hydroxychloroquine, citing a BBC article that quoted President Trump's claims that the drug was approved in the US to treat the coronavirus. The use of referencing legitimate media articles when advertising the sale of COVID-themed products was a repeatable tactic observed by the CTIL Dark researchers during our monitoring of opportunistic cybercriminals.



**30 pills Hydroxychloroquine 200mg Chloroquine ( Anti Corona virus COVID-19) ONLY 69\$ usd**

30 pills Hydroxychloroquine 200mg Chloroquine ONLY 69\$ usd Anti Corona virus medication COVID-19 Coronavirus and chloroqui...

Sold by **medsguru** - 2 sold since March 26, 2020 Vendor Level 6 Trust level 6

	Features	Origin Country	Features
Product Class	Physical Package	Singapore	Singapore
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

DHL from Singapore - 14 days - USD + 25.00 / order

Purchase price: **USD 69.00**

Qty:  Buy Now Buy Now Buy Now Queue

0.007439 BTC / 1.588398 LTC / 1.071096 XMR

**Description** Feedback Refund policy

**30 pills Hydroxychloroquine 200mg Chloroquine ( Anti Corona virus COVID-19) ONLY 69\$ usd**

30 pills Hydroxychloroquine 200mg Chloroquine ONLY 69\$ usd

Anti Corona virus medication COVID-19

Coronavirus and chloroquine: Has its use been approved in ...  
[www.bbc.com](http://www.bbc.com) > news  
 President Trump claims a drug used against malaria has been approved in the United States to treat the new coronavirus. Chloroquine is one of the oldest and best-known anti-malarial drugs. ... However, the FDA has made it clear it has not been approved for treating those infected with

Figure 7 - Cybercriminal persona "medsguru" advertises Hydroxychloroquine for sale on a darknet market

CTIL Dark assess that these opportunistic cybercriminals will continue to monitor and respond accordingly to the general public's needs of the COVID pandemic. Like the Hydroxychloroquine trend, several other public trends emerge as long as the COVID virus remains a priority of concern to the general public. These trends can emerge through media reports, public and political figures making claims, and the spread of disinformation campaigns started by Nation-state threats.

## Disinformation Campaigns

CTIL Dark has assessed during our research that disinformation, misinformation, and conspiracy theories of COVID is one of the biggest threats to the general public's health and safety. For context, we have defined the topic as follows:

- *Misinformation* is false or misleading information that's potentially harmful. For example, a claim that COVID doesn't exist. This is spread directly or indirectly by unsuspecting individuals – often times through sharing posts in social media.
- *Disinformation* is the deliberate promotion of false, misleading, or misattributed information, usually designed to change the beliefs or actions of large numbers of people. This is usually created and initially spread deliberately, often by government or intelligence agencies through the use of personas carefully crafted to appear to have credentials of authority (Medical Doctors or PhD credentials) or through the use of social media amplification technology ("bots").
- *Conspiracy Theories* are misinformation which, in context, is beyond reasonable credibility. Conspiracy theories can be part of Disinformation campaigns.

Collection and analysis within select Tor Markets and fringe social media platforms revealed indications that adversaries used strategic narratives to create tactical messaging. The COVID campaigns appeared to fall within three common misinformation themes: 1) Receiving the vaccine resulted in significant neurological side effects (specifically Bell's Palsy), 2) All COVID vaccines have a hidden intention of global depopulation, and 3) The vaccine is not needed because other medications such as Niacin are more medically effective. These narratives received ongoing discussions within messaging platforms known to incubate misinformation, such as 4Chan and 8Kun. At the same time, engagement of established personas and imposter websites would move to target the more widely used social media platforms.



Figure 8 - Twitter post from Disinformation Persona using Bell's Palsy photo from Medical Journal and citing imposter news site to imply the first UK Health Workers to receive the Pfizer vaccine experienced the side effect

**Structural similarity between HIV-1 gp41 and SARS-CoV S2 proteins suggests an analogous membrane fusion mechanism\***

Xue Wu Zhang<sup>1</sup>, Yee Leng Yap<sup>1</sup>

**THEO CHEM**

**DEPOPULATION VACCINE!**

**mRNA COVID VACCINE = CUSTOM DNA SPECIFIC AIDS WITH NO CURE!! DEAD IN 5 YEARS!!**

**AI SOFTWARE TOOL TO PSYOP THE MASSES WHEN FULL BLOWN HIV/AIDS SIDE EFFECTS**

**II.1) Scope of the procurement**

**II.1.1) Title:** SafetyConnect – AI

**II.1.2) Main CPV code:** 48000000 Software package and information systems

**II.1.3) Type of contract:** Supplies

**II.1.4) Short description:** The MHRDA currently seeks an Artificial

**Legal Basis:** Directive 2014/24/EU

**Section I: Contracting authority**

**I.1) Name and addresses**

Official name: MHRA Buyer Organisation  
 Town: London  
 NUTS code: UK UNITED KINGDOM  
 Postal code: E14 4PU  
 Country: United Kingdom  
 E-mail: [purchasing@mhra.gov.uk](mailto:purchasing@mhra.gov.uk)  
 Telephone: +44 2030806000  
 Internet address(es):

Figure 9 – Message board image related to campaign of hidden vaccine purpose of global depopulation

The third campaign of note: the use of Niacin, was observed to be referenced and promoted highly by the conspiracy theory group QAnon and later promoted by the same community on Twitter<sup>1</sup>. The self-proclaimed medical expert, “Dmitry Kats, PhD, MPH” was observed to have written several preprint medical journals, citing them as established medical fact. This individual was observed to have created an elaborate backstop persona<sup>2</sup> that included a Google Scholar account.

**IN A NUTSHELL:** Research here: [gofile.io/d/TVaYAu](https://gofile.io/d/TVaYAu)

If we had a daily recommended value for niacin at 1 gram (/day), rather than say the legit only 15-20 mg FDA has it set at (don't ask me why that is), then NO ONE WOULD HAVE EVER HAD COVID-19!

Even after the fact, we can still COMPLETELY ERADICATE it and overnight in those who do have it!!!

My point is that we don't have a healthy immune system

Characteristic	Value	Importance	Score
Age	30-40	High	0.8
Gender	Male	Medium	0.6
Body Mass Index (BMI)	20-25	Low	0.4
Current medications	None	High	0.9
Current smoking status	None	Medium	0.7
Previous hospitalizations	None	High	0.8
Previous surgeries	None	Medium	0.6
Cardiovascular disease	None	High	0.9
Diabetes	None	Medium	0.7
Hypertension	None	High	0.8
Respiratory disease	None	Medium	0.6
Chronic kidney disease	None	High	0.9
Autoimmune disease	None	Medium	0.7
Other chronic conditions	None	High	0.8
Overall Health Score	High	Low	0.2

Figure 10 - False Persona promoted by QAnon about the use of Niacin

<sup>1</sup> Noting for this report that all findings and research mentioned regarding the conspiracy theory group QAnon was collected and analyzed prior to account removals as a result of the recent January 6<sup>th</sup>, 2021 Washington DC Capitol Building insurrection

<sup>2</sup> “The act of creating other assets/dossier/cover/fake relationships and/or connections or documents, sites, bylines, attributions, or establish/augment/inflate credibility/believability” Technique 0030, from AMITT, an information security-based framework for responding to disinformation. AMITT is available at <https://github.com/cogsec-collaborative/AMITT>

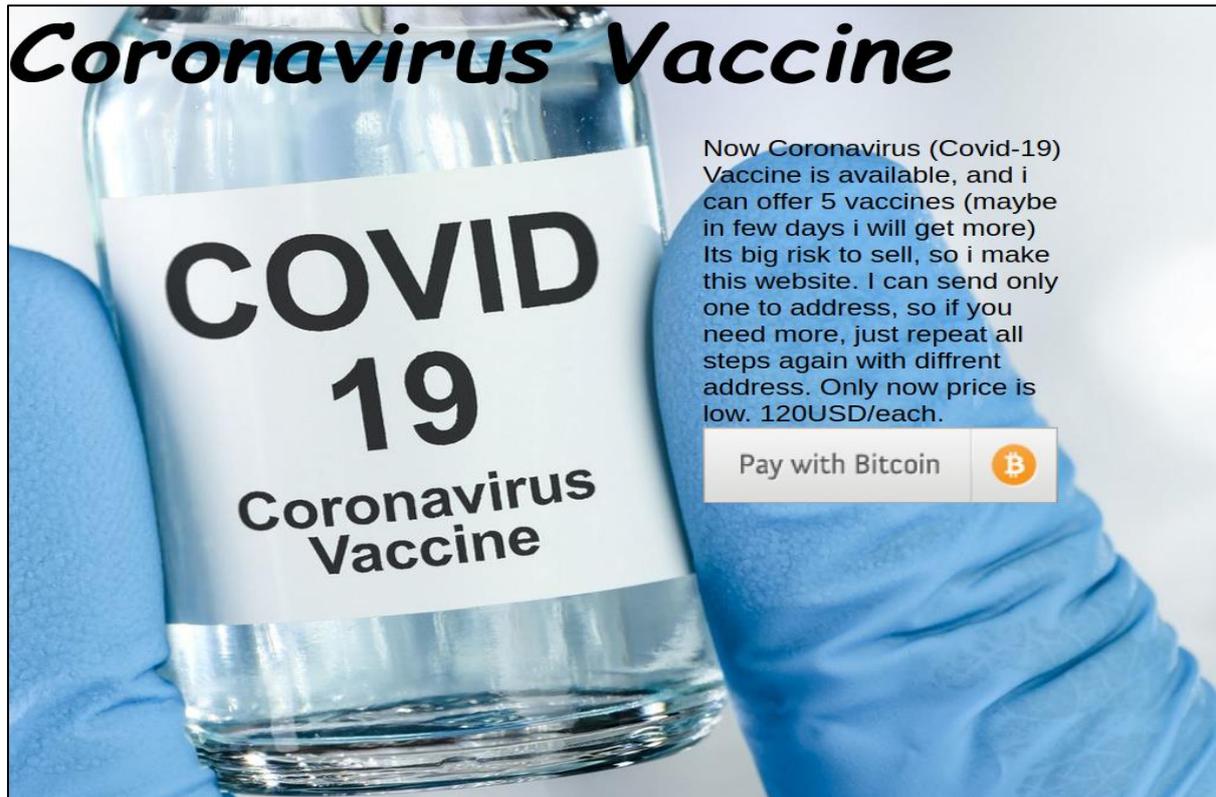
Misinformation and Disinformation are likely to continue as growing concerns for healthcare and public perception of COVID. Medical disinformation with narratives around Covid19, personal protection measures including masks, and anti-vaccination narratives continue. Groups like QAnon are likely to continue and to be joined by more groups and new groups. Since January 2021, more groups are focused on disinformation mitigation and countermeasures, but despite that, disinformation is likely to continue as a technique in cyber-cognitive and physical-cognitive hybrid attacks.<sup>3</sup>

---

<sup>3</sup> Credibility Coalition: Misinformation Working Group. (2019, July). Building standards for misinfosec: Applying information security principles to misinformation response. <https://github.com/cogsec-collaborative/documentation/blob/master/Publications/MisinfosecWG-2019-1.pdf>

## Scammers

The emergence of individuals and groups looking to scam people out of money in a pandemic is nothing new and was something CTIL Dark expected. As was widely reported, the COVID miracle cure sites came first. Scammers set these up to exploit fears and influence the individuals to click phishing links. Then came the Tor-based COVID vaccine scam sites that urged their victims to pay in Bitcoin for their miracle cures



*Figure 11 - Tor-based scam site advertising COVID vaccines for \$120 in Bitcoin*

The CTI league was instrumental in taking down more than 2,000 of these scam sites since the pandemic began. CTIL Dark tracked the threat actors coordinating their setup on criminal forums, monitoring which domains they were setting up to host their fraudulent sites and reporting to the domain hosting companies of the violations. Our observation is that sites ending in .info were often the preferred domain choice, as it gave the perception of the legitimacy of passing factual information on the pandemic.



*Figure 12 - Product image for fake COVID treatment*

CTIL Dark also took an active role in gathering intelligence and information on named threat actors. One example is a UK national who advertised a COVID cure. CTIL Dark Intelligence Collectors reached out to the individual to gather more information. Starting in a public forum and moving the conversations to a more secure direct messaging, the actor provided enough personal information that CTIL Dark could uncover his real identity and location. CTIL Dark gave the relevant evidence to law enforcement for further action.

Scams tracked COVID-themed trends alongside stages of the pandemic to exploit target fear and curiosity. From miracle cures when the virus effects were not clear, into vaccine scamming now. Therefore, the CTIL Dark assesses that scammers will continue to adapt to emerging COVID-themed trends in 2021.

## Phishing

Since the beginning of the pandemic there have been a number of different COVID-themed phishing campaigns preying on the fears of the general public. These campaigns have included the COVID vaccine, the John Hopkins Coronavirus map and various other tempting lures to target fearful individuals. CTIL Dark assesses with that these COVID-themed phishing campaigns will continue so long as the Coronavirus is relevant to the general public.



Figure 13 - Fake COVID map used in phishing to deliver malware

Most are aware of the fake COVID map that a cybercriminal group made to mimic the original Johns Hopkins map. The original map was crucial in disseminating information in the opening days of the crisis. This fake map looked the same but would infect users who

visited with AZORult malware that steals browsing history, cookies, ID/passwords, cryptocurrency information, and other techniques. Some people may not have known about the creators' presence on the Darkweb and their attempts to resell the map and malware in various forms.

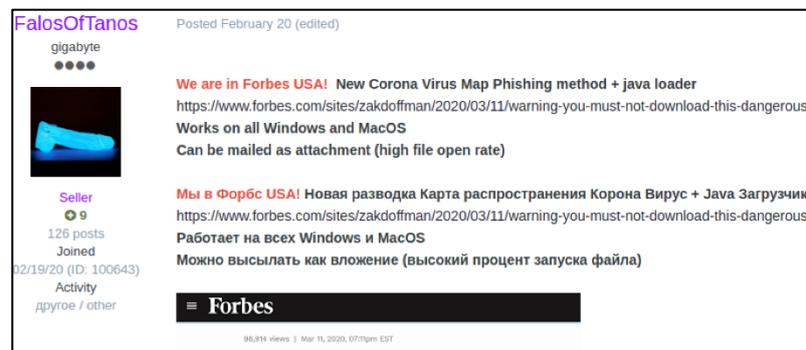


Figure 14 - Threat actor bragging about success of their malware campaign

CTIL Dark discovered the creators of the map in underground forums were ecstatic that their malware-infected Coronavirus map was making its round in Forbes and actively bragging about it. CTIL Dark Human Intelligence (HUMINT) collectors engaged with the malware creators by fueling their ego to exchange for valuable intelligence. The actors bragged about who was interested in purchasing the map, where they were from, and what they intended to do with the malware. Throughout these discussions, the CTIL Dark HUMINT collectors shared the information with global Law Enforcement partners and Hospital IT teams.

## Databases

In Q2, CTIL Dark identified an increase in medical Databases containing PHI being advertised within several underground forums and marketplaces. These databases were all obtained at one point or another through a malicious actor stealing the contents of the database after initially breaching a medical organization. The information within these databases can be used by threat actors in targeted attacks on the patients themselves.

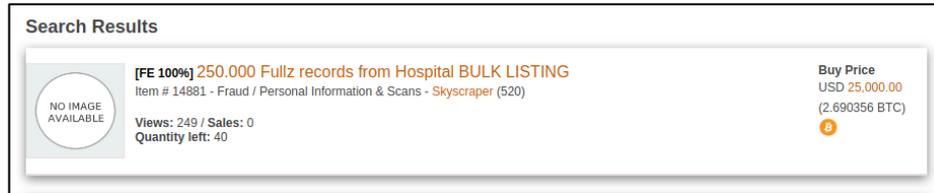


Figure 15 - Cybercriminal persona "Skyscraper" advertises a database with 250,000 hospital records

In other cases, threat actors will consolidate multiple hospital employees' data obtained from several databases and then sell it as one database to threat actors who may want to breach hospitals in a particular region in the world. Malicious actors can use hospital employee information to target each employee from many different hospitals simultaneously until they find the one that will help them gain access to their hospital's network.

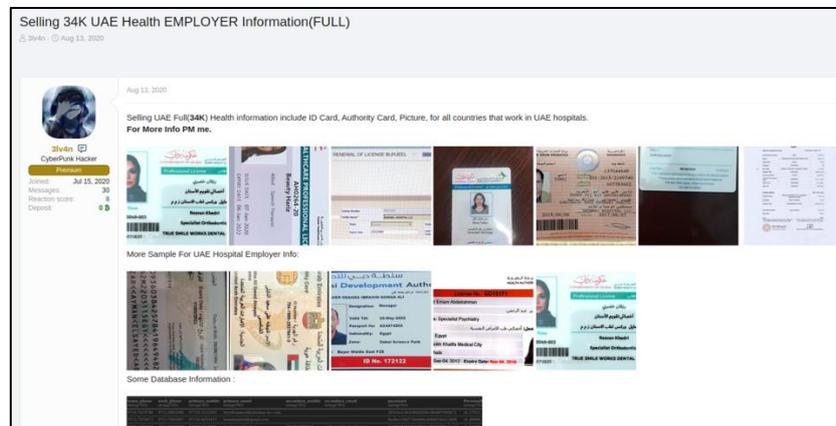


Figure 16 - Cybercriminal persona "3lv4n" advertises a database with 34,000 UAE hospital employee data

CTIL Dark assesses that the buying, selling, leaking and trading of healthcare databases that include PHI and other sensitive information on patients and medical staff will continue in 2021. Threat Actors may use this information for immediate financial gain or as a way to find a target entry point into another more lucrative victim organization.

## CTIL Dark in Action

CTIL Dark has been called into action on numerous occasions. Two incidents resulted in major wins for the CTIL Dark team, our Law Enforcement partners, and the victim organizations who were able to mitigate these threats before major damage was done. These efforts directly resulted in actionable intelligence that allowed for Law enforcement and local CERTs to assist the victim organizations that were impacted.

### Polish nationwide hospital alerting

In early June, around 1:00 a.m. Eastern Time, a CTIL Dark intelligence collector had a source contact them regarding the sale of RDP access to a state-run hospital in Eastern Europe on the dark web for \$1000. As the researcher alerted the other team members, they set forth on corroborating the threat via other methods. Multiple sources of information were collected quickly to substantiate the Polish hospital's vulnerability and confirm the findings. Simultaneously, a CTI League partner with the Polish Computer Emergency Response Team (CERT.PL) analyzed the data and escalated an alert to every hospital in Poland for their internal IT teams to harden the identified vulnerabilities to disrupt the RDP access.

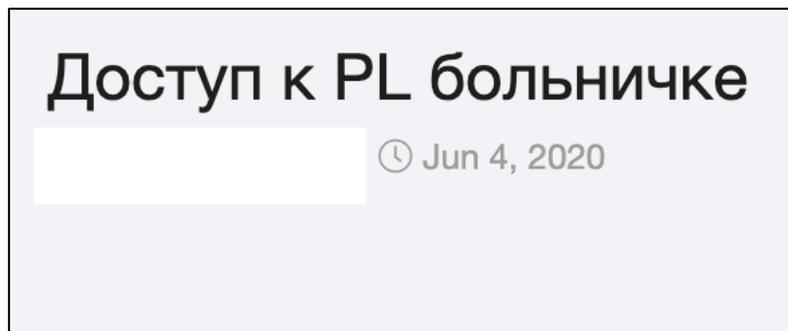


Figure 17 - Cybercriminal persona (redacted) advertising RDP access to a Polish hospital

From the initial report to disseminating the information to every state hospital in Poland, the international team of CTI league members took 3 hours, including finding multiple sources and intelligence types to corroborate the initial claim.

## Pre-empting access to large Catholic Healthcare Organization

CTIL Dark identified a Russian-speaking threat actor on an underground fraud forum selling Remote Desktop Protocol access to one of the largest Catholic healthcare systems in the United States. The threat actor claims that the institution has an annual revenue of \$18 Billion and 86,000 employees. The advertisement is listed at \$5,000. The screenshots reveal that the threat actor could be reached via XMPP, an instant messaging platform for encrypted communications.

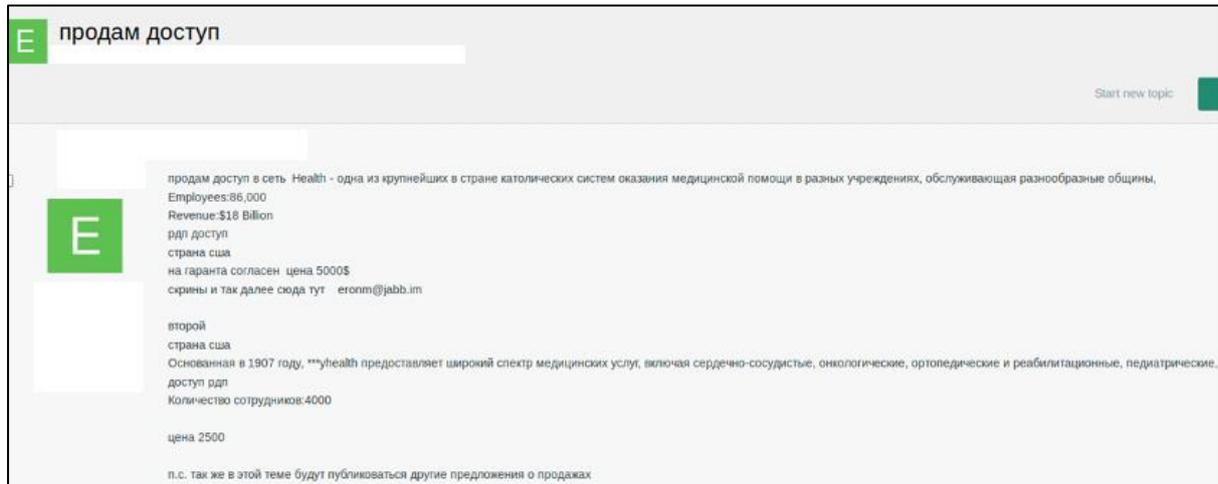


Figure 18 - Cybercriminal persona (redacted) advertises RDP access to a Catholic healthcare system

CTIL Dark submitted this alert to authorities and organizations affiliated with the Catholic Archdiocese and the top three Catholic healthcare organizations that matched the threat actor's description.

## Summary

CTIL Dark, the CTI League participants, strategic partners, and law enforcement members worldwide have created through the shared values of trust a community in which we dedicated our skills to providing healthcare organizations worldwide with real-time intelligence on cyber threats to their infrastructures. The CTI League is proud of our members, the contributions they have made, and we will continue to work with law enforcement to protect healthcare organizations worldwide in their ongoing battle with cyber threats.

In 2020, threat actors firmly fixated on the healthcare sector. Their increased attention led to a largescale rise in harmful and disruptive effects on the global COVID pandemic response. As with many of the risks it faced in the past hear, healthcare was simply overwhelmed and unable to cope with the volume of cyber threats.

Attack trends are rising as we enter 2021, and so the healthcare community will have to improve even farther, even faster if it wants to keep pace. This will take a whole of society effort, among government, citizens, industry, and communities such as the CTI League.

If you work in law enforcement, healthcare organization, or the cybersecurity community, we encourage you to join our community to protect society against COVID. Apply at <https://cti-league.com/join>.

A more detailed analysis of information discussed in this report is available to law enforcement. Please contact [le@cti-league.com](mailto:le@cti-league.com).

## About the CTI League

The CTI League is a global non-profit organization derived by a community, with the vision of creating a safer cyberspace for healthcare/public health and emergency services organizations worldwide from cyber-attacks. Established in March 2020, the CTI League's community of professionals has more than 1,500 vetted volunteer cybersecurity experts and collaborates with government agencies, law enforcement, healthcare, telecommunications, and technology companies globally. CTI League volunteers prevent harm to human life and COVID response by supplying reliable information about cyberattacks, threat actors, and vulnerabilities to our stakeholders.

The CTI League believes in collective actions, contribution and facilitating the resources of each member of the community to maximum. Within the CTI League there is an elite team of security researchers and law enforcement personnel who monitor cybercriminal underground networks within the Darknet and Deep/Dark web. Their days are spent looking for signs of data breaches, targeted attacks, and any other cybercriminal activity that may impact the medical industry or general public health.

**We call this team CTI League Dark.** This multidisciplinary team empowers each member and builds goodwill through collaboration, working as a united group to protect the healthcare sector. CTIL Dark focuses on three different aspects of threats:

- Threats on the health ecosystem – CTIL Dark focuses on discovering emerging threats to organizations providing life-saving care and in the health supply chain. CTIL Dark provides an overview of the risks that can affect an organization's networks and disrupt their ability to save lives. Data breaches, network access, and compromised assets offered for sale in the darknet are examples of these threats.
- Threat actors operating in the darknet – CTIL Dark provides actionable threat intelligence to our law enforcement partners on the specific threat actor Personas of Interest (POI) who are targeting the health ecosystem.
- Threats to Public Health and Safety – CTIL Dark is focused on finding cyber threats to public health and safety such as the purchase of fake COVID vaccines. These fake vaccines can result in a fatal infection or even death. The CTI League escalates the threats discovered to inform our associates and law enforcement partners for the next steps.