



The Cyber Threat Impact of COVID-19 to Global Business

Introduction

The COVID-19 pandemic has altered the way business is done around the world. With predominantly remote workforces operating on unsecured home networks, corporate security teams are struggling to gain control of rapidly expanding attack surfaces.

Cybercriminals and state-sponsored advanced threat groups are exploiting the COVID-19 pandemic to attack networks around the world for both financial and strategic gain. Between January and March, coronavirus-themed phishing lures, malware infections, network intrusions, scams, and disinformation campaigns have become rampant across the clear, deep, and dark web.

IntSights researchers put together this report to explore the most prevalent COVID-19 cyber threats: phishing websites and emails, fake coronavirus mobile apps, malware, ransomware, fraud, and disinformation. We also address the criminal and state-sponsored threat actors behind these campaigns, the most common types of targets, and network indicators of compromise.

What started as simple phishing attacks and hand sanitizer scams now involves several well-known threat actors. APT36, FIN7, the Maze ransomware group, and several other nation state actors are now behind attacks related to the coronavirus pandemic. As sophisticated threat actors enter this ring, both the volume and sophistication of the attacks will likely increase.

IntSights recommends the following steps for defense against these threats:

- Update the current threat landscape risk assessment based on new emerging threats to remote workers.
- Closely monitor collaboration and remote working tools.
- Strictly enforce the use of VPNs, encryption, and endpoint security.
- Enforce strong password policy and 2FA.
- Educate end users on the new threat landscape.

Tactics, Tools, Procedures

Phishing Domain Registrations

IntSights has been monitoring the registration of domains that include the words 'corona' and 'covid.' While some of these domains were registered for legitimate uses, others now host phishing attacks. The graph below shows the exponential rise in the number of domains registered. In 2019, only 190 domains using the worlds 'corona' and 'covid' were registered. In January of 2020 alone, that number was over 1400, and during February, it soared to over 5000 before topping 38,000 in March.

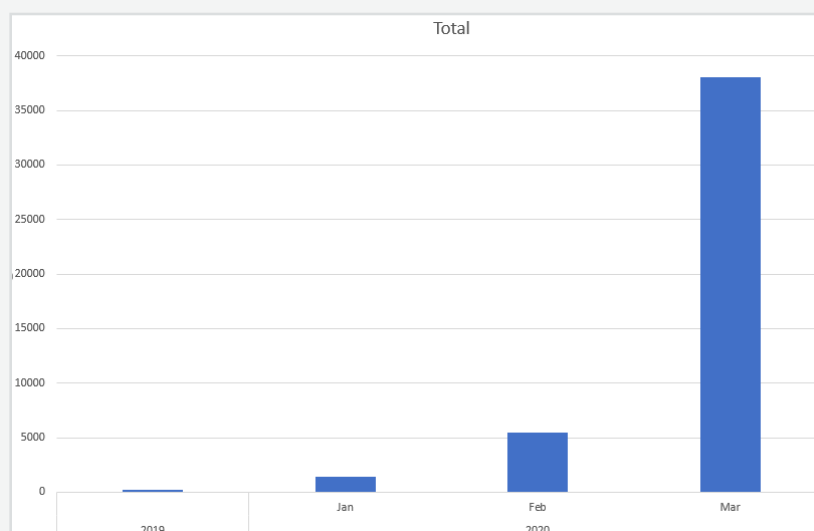


Figure 1: Graph showing the increase in phishing domain registrations related to COVID-19 between December 2019 and March 2020. Source: IntSights Threat Command

Phishing Emails

There are many phishing emails currently in circulation that use the pandemic as their theme. The example in Figure 2 (below) includes a phishing email that impersonates DHS and redirects victims to a malware download address. This will result in an installation of an information stealer malware on the victim's device.

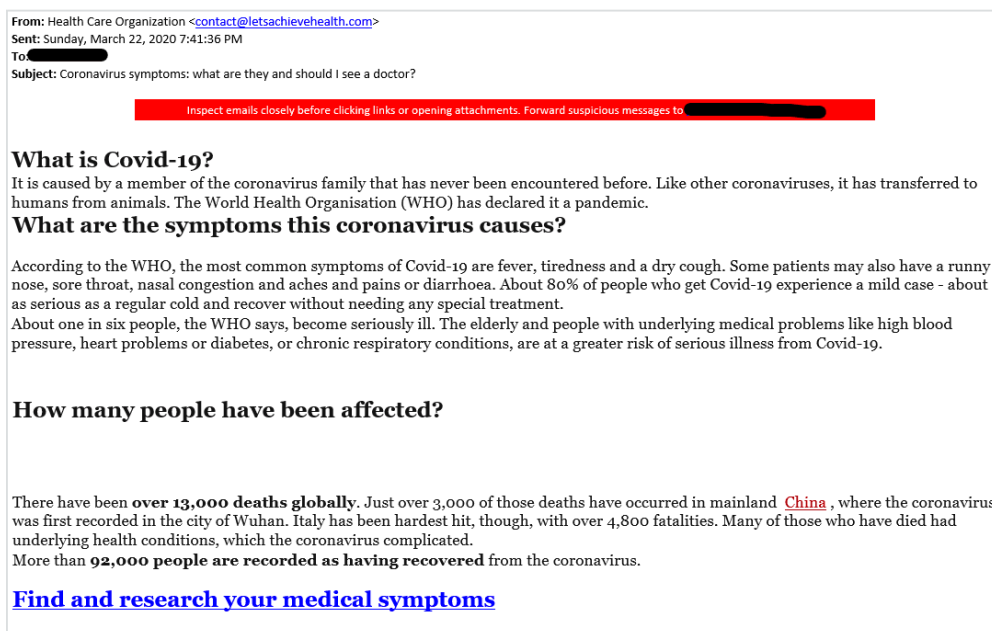


Figure 2: A phishing email that impersonates DHS and redirects victims to a malware download address

Malware

AZORult Malware

In our recent [blog](#), we described a Russian underground vendor offering a malware that looks like the Johns Hopkins coronavirus outbreak map, which pulls real-time data from the legitimate site. The map is a JAVA-based malware deployment that installs the AZORult credential stealer malware. The kit costs \$200 if the buyer has a Java code certificate, or \$700 if the buyer wishes to purchase the seller's certificate. The map mimics the real Johns Hopkins map, hosted at coronavirus.jhu.edu, and features live, real-time data (see Figure 3 below).

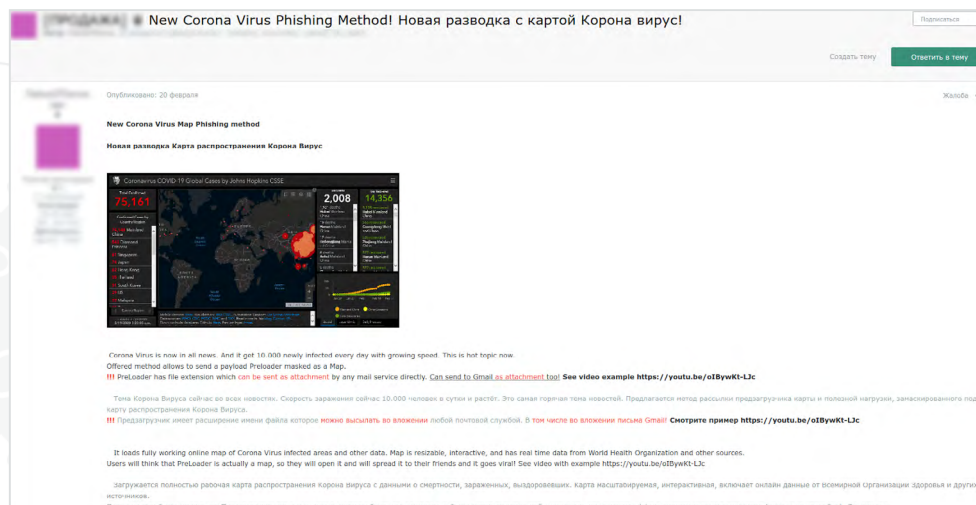


Figure 2: A phishing email that impersonates DHS and redirects victims to a malware download address

Remcos RAT Malware

The Remcos RAT malware is spreading through unknown infection vectors to drop an executable file called "CoronaVirusSafetyMeasures_.pdf[.]exe." The file is an obfuscated dropper that would install the executable on the compromised computer with a VBS file specifically designed to run the RAT. The malware is capable of persistence through a startup key, which allows the malware to restart when the victim's device is restarted. After installation is complete, the malware then logs the users keystrokes and exfiltrates the data to its command and control IP, 66[.]154.98.108. The process is shown in Figure 4, below:

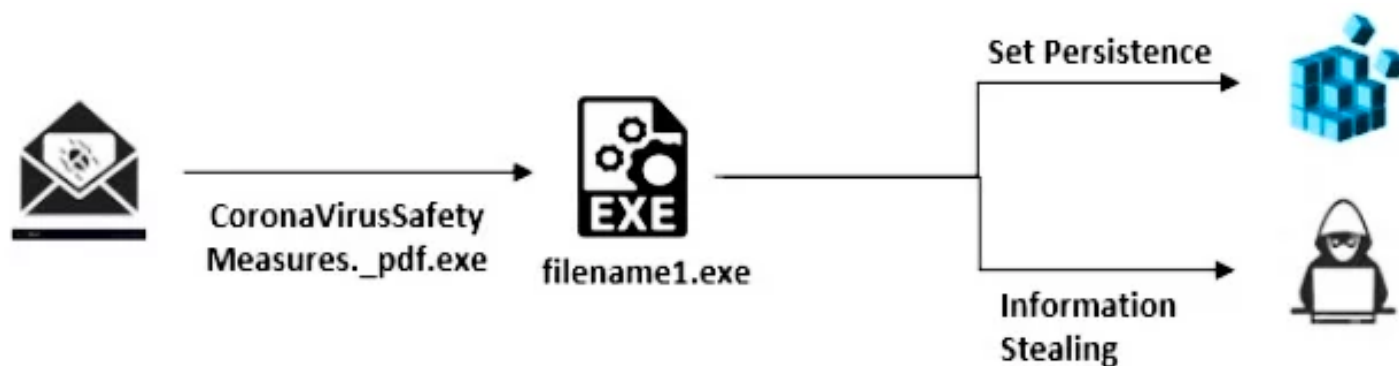


Figure 4: Remcos RAT execution process

Emotet + Lokibot Malware

Earlier this month, researchers discovered an Emotet phishing email circulating, designed to look like it is from China's Ministry of Health (Figure 5, below). The email detailed official emergency coronavirus regulations, suspiciously in the English language.

Natural language analysis reveals that the English was a very poor translation, reflecting incorrect grammar and including odd phrases, such as "As we work hard to kicking away the virus." This indicates that the email was written by a non-English speaker. Attached to the email is an .arj file called "Emergency Regulation Ordinance," which is a Windows RAR file. When unpacked, a Windows Batch file called "Emergency Regulations" executes and proceeds to exfil the victim's user credentials to the Command and Control IP.



Figure 5: Phishing email purporting to be from China's Ministry of Health



Figure 6: [Source](#)

Ransomware

Maze Ransomware

While some cybercrime groups vouched to not attack medical facilities during the outbreak, others had no such intentions. The Maze ransomware group, which has previously targeted everything from small US law firms to the German government, targeted HMR, a company that performs clinical tests for drugs and vaccines. HMR has recently taken an active role in developing tests and vaccines for COVID-19. The company was attacked on March 14th, with medical records of over 2,300 patients and employees leaked on March 21st (Figure 7).

NetWalker Ransomware

In early March 2020, the Champaign Urbana Public Health District (CHUPD) in Illinois was [attacked by the NetWalker ransomware group](#), which became very active early this year. The campaign started with a coronavirus-themed phishing email loaded with a malicious attachment named "CORONAVIRUS_COVID-19.vbs." The file contains an embedded NetWalker ransomware executable file and obfuscated code to extract and launch it on the victim's device.

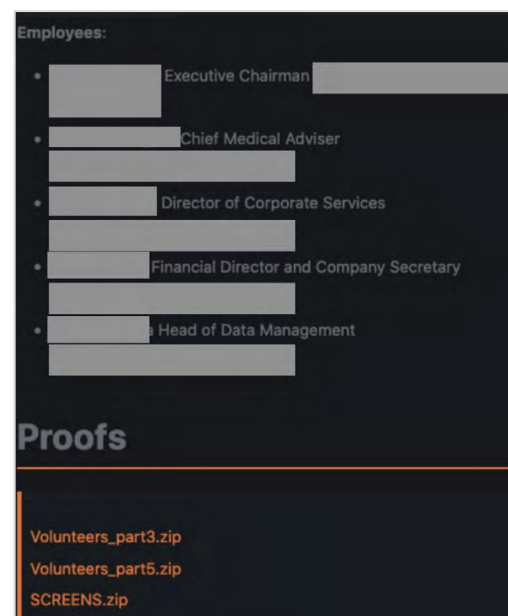


Figure 7: Leaked data of DHS employees

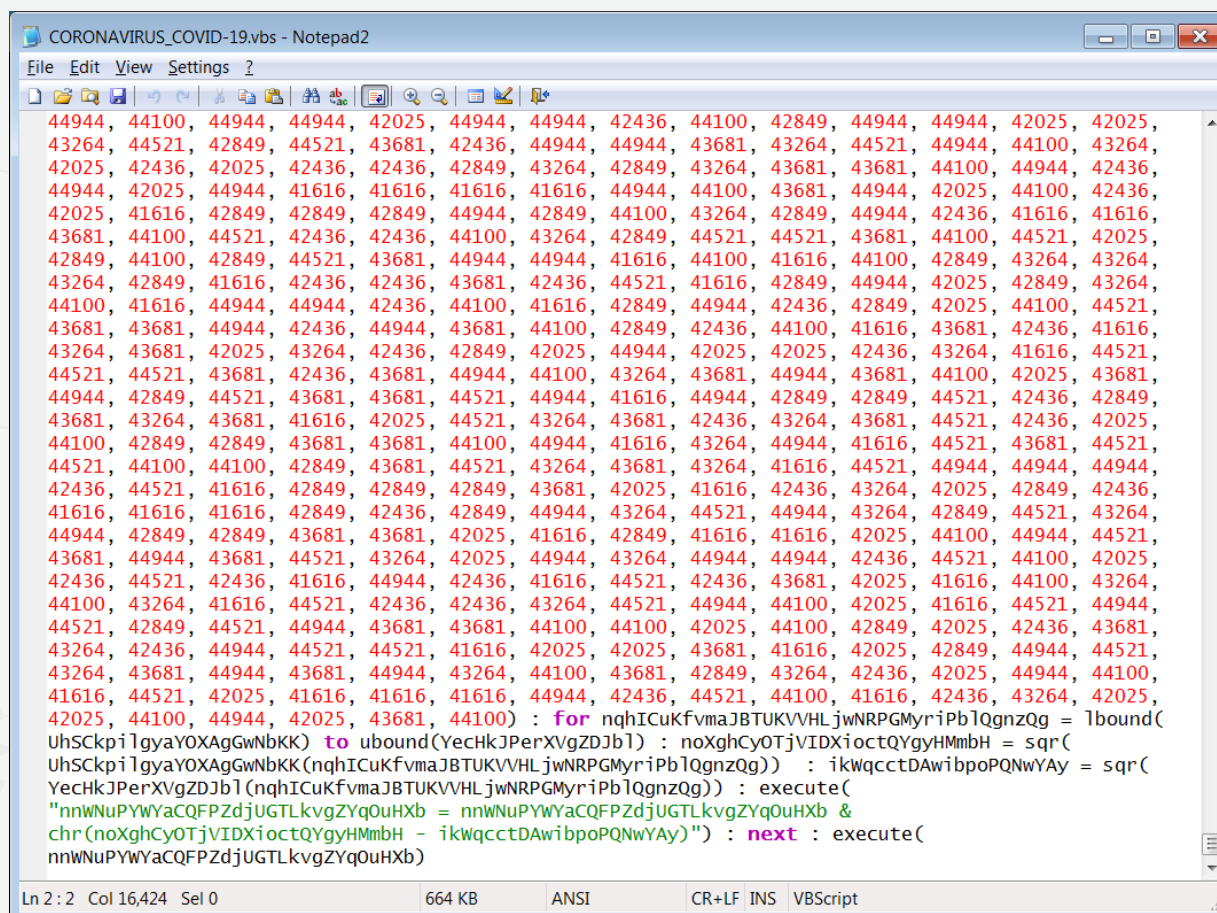


Figure 8: NetWalker ransomware VBS attachment observed in March 2020 campaign against healthcare

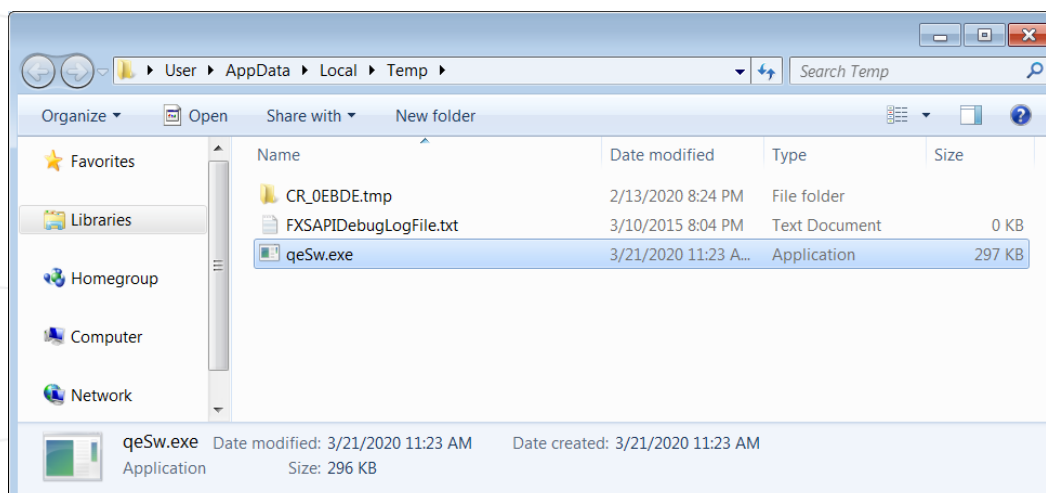


Figure 9: NetWalker executable saved to %Temp%\qeSw.exe

The NetWalker ransom letter, seen in Figure 10 below, taunts the victim by insisting he or she move away from the computer and let the malware finish its encryption process, emphasizing there is nothing the victim can do to stop it.

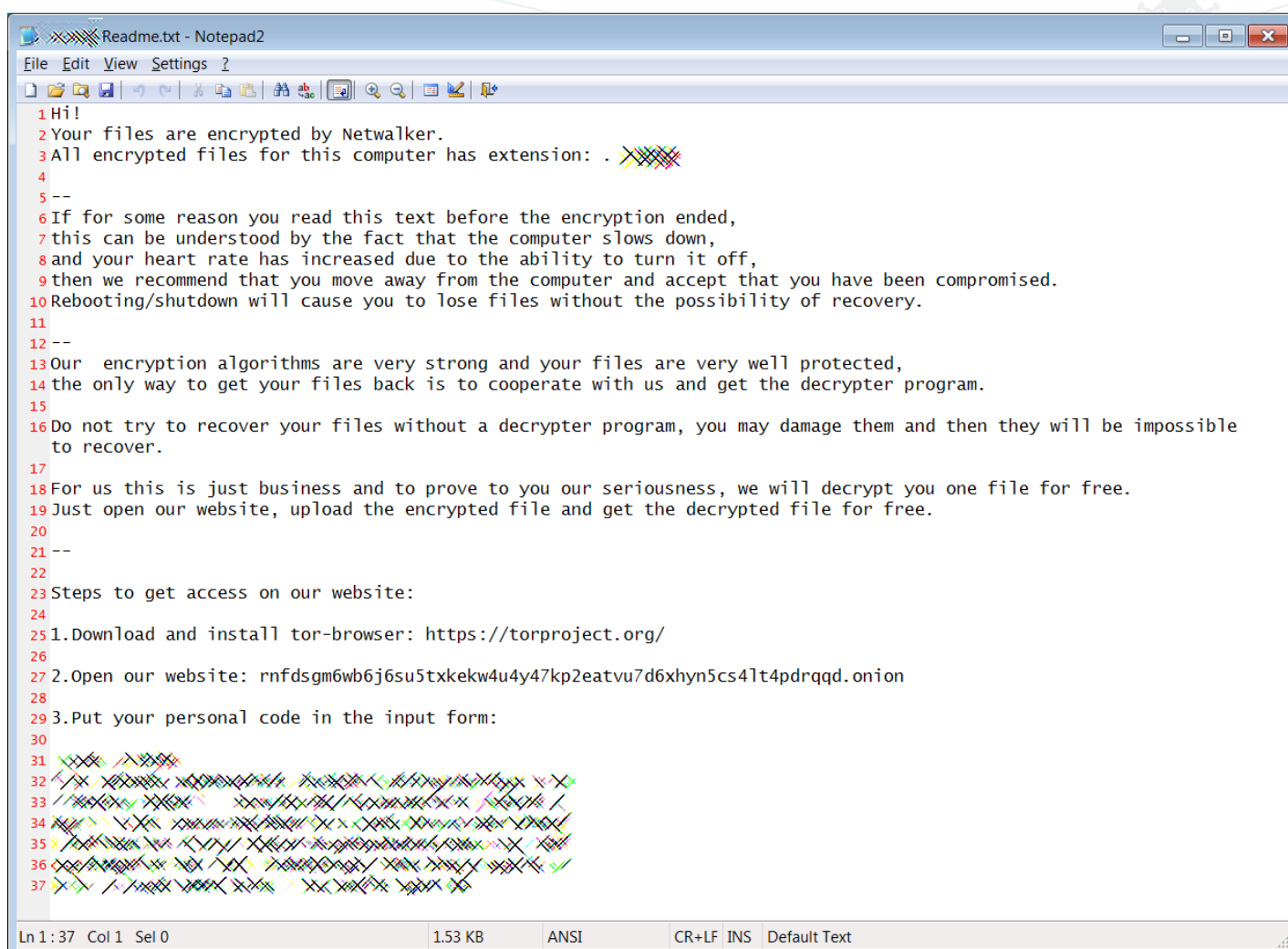


Figure 10: NetWalker ransom letter instructs victims to download TOR browser and visit a .onion site to pay the ransom

Extortion and Fear Tactics Through Ransomware

Threat actors all over the world are exploiting people's fears around COVID-19 in order to make money. The ransomware letter below tells the victim that not only did they encrypt all of their data, but they can also "infect your whole family with the Coronavirus." These types of fear tactics work on a vulnerable population of people during a frightening pandemic. Threat actors use these fear tactics because they work. We have also observed similar psychological tactics used in sextortion scams, in which the threat actor tells the victim that he has access to the victim's camera or photos with evidence of wrongdoing. The bad actor threatens to extort the victim's "sins" to family and friends if the ransom is not paid.

What do I know about you?
 To start with, I know all of your passwords. I am aware of your whereabouts, what you eat, with whom you talk, every little thing you do in a day.

What am I capable of doing?
 If I want, I could even infect your whole family with the CoronaVirus, reveal all of your secrets. There are countless things I can do.

What should you do?
 You need to pay me \$4000. You'll make the payment via bitcoin to the below-mentioned address. If you don't know how to do this, search "how to buy bitcoin" in Google.

Bitcoin Address:
 [REDACTED]
 (It is cAsE sensitive, so copy and paste it)

You have 24 hours to make the payment. I have a unique pixel within this email message, and right now, I know that you have read this email.

If I do not get the payment:
 I will infect every member of your family with the CoronaVirus. No matter how smart you are, believe me, if I want to affect, I can. I will also go ahead and reveal your secrets. I will completely ruin your life.

Nonetheless, if I do get paid, I will erase every little information I have about you immediately. You will never hear from me again. It is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Figure 11: [Source](#)

Fraud and Hoaxes

There has been a surge in COVID-19 related products, scam templates, and hoaxes on deep and dark web markets. The sellers seek to exploit public fear by offering products that could allegedly serve as virus tests or vaccines. The limited availability of coronavirus testing – especially in countries like the United States – leads to demand for such products in black markets. In all likelihood, however, these "products" are in no way real, and buyers would be scammed out of their money.

Other > Drug Test Kits

New rapid test kit to detect COVID-19

Vendor: [CannaCare](#) (99.3)

The test kit, which has been developed and is manufactured by Cetus? strategic partner BGI in Shenzhen, China, enables diagnostic laboratories to test for SARS-CoV2, the virus causing COVID-19, in only a matter of hours.

The kit contains enough reagents and controls to test up to 48 patients in just a few hours

wick id: CannaCare79

Price: \$ 0.123476 (600.00000000 USD)

S & H:

- priority shipping
\$ 0.002315 (15.00000000 USD)
- express mail
\$ 0.003087 (20.00000000 USD)
- 24hour overnight delivery
\$ 0.009946 (45.00000000 USD)

Accepted Crypto Currencies:

 Bitcoin

Ships From:  United States

Ships To:  Worldwide

[View](#)

Figure 12: Source – <http://agarthafcidkiwas.onion/item/431752006584450143>

FAST CORONAVIRUS DETECTOR \$400

Vendor: [Rodrigomendez](#) (82.9)

WICKR.....

RODRIG45
RODRIG45
RODRIG45

FAST DETECTOR OF CORONAVIRUS
YOU NEED EVEN FOR YOUR HOME USE OR MORE

FOR FASTER RESPONDS AND MORE INFO'S ABOUT PRODUCT ... CONTACT

WICKR.....

RODRIG45
RODRIG45
RODRIG45

Price: \$ 0.061738 (400.00000000 USD)

S & H:

- fedex




Figure 13: Source – <http://agarthafcidkiwas.onion/item/4763580630124718721>

GET THAT VACCINE FOR THE MOST VIRAL CORONA VIRUS

Vendor: Legalshop (98.4)

PROMOTION... PROMOTION... PROMOTION...

Welcome Valued Clients Buy tested and trusted corona vaccine against the wide spread deadly pandemic virus called corona virus putting threads on lives at comfortable and affordable prices 100% DELIVERY GUARANTEE WITH UPS DHL USPS. FAST DISCREET OVERNIGHT DELIVERY WITHIN THE USA AND STEALTH DELIVERY WORLDWIDE. WE ALSO DO PROVIDE TRACKING DETAILS ONCE PACKAGE IS REGISTER. WE ARE AVAILABLE 24/7.

CUSTOMERS SATISFACTION IS OUR TOP PRIORITY AS WE LOOK FORWARD TO BUILD AND DO LONG TERM BUSINESS.

PLEASE all new clients do contact us through our wickr app or whatsapp number below for FAST AND EASY Communication

Wickr ID... legalshop247







Whatsapp number ... +14089091479


Price: ₪ 0.069455 (450.00000000 USD)


S & H:

- UPS
₪ 0.003859 (25.00000000 USD)
- DHL
₪ 0.003859 (25.00000000 USD)
- USPS
₪ 0.003859 (25.00000000 USD)


Accepted Crypto Currencies:

 Bitcoin,  Dash,  Litecoin,  BitcoinCash,  Vertcoin,  Monero

Ships From:  United States

Ships To:  Worldwide

BUY


Figure 14: Source – <https://agarthafcidkiwas.onion/item/6590149416587138941>

phpBB® Piazza
Large & flexible & accessible - [Help/FAQ/Howto/Support](#) - [Help/FAQ/Howto/Support](#)

Quick links: [FAQ](#) [Register](#) [Login](#)

Home Board index Personal Words

Search:

buy your coronavirus antidotes and vaccines now! Protect your family!

Post Reply

buy your coronavirus antidotes and vaccines now! Protect your family!

by darknetmarketnews - Sun Mar 15, 2020 10:58 am

buy your coronavirus antidotes and vaccines now! Protect your family!

MIGAL is a research organization located in Galilee, Israel and specialized in fields of biotechnology
MIGAL already created a vaccine against avian Coronavirus Infectious Bronchitis Virus (IBV) and we have a limited number of one thousand of samples to sell to interested persons
 Take this information seriously because it'll be months before they are allowed to be sold to you

SERIOUS BUYERS ONLY
CONTACT US NOW
 Contact us via darknetmarketnews@protonmail.com
 General support darknetmarketnews@protonmail.com
 Text: +972 414-2670
 WhatsApp: +972 414-2670
 Telegram: @legitshopcompany
 Wickr ID: @legitshop008

Re: buy your coronavirus antidotes and vaccines now! Protect your family!
 by darknetmarketnews - Sun Mar 15, 2020 3:00 pm

Hello, If you're interested in our products or services hit me up for more info at:


Contact us via darknetmarketnews@protonmail.com
 General support darknetmarketnews@protonmail.com
 Text: +972 414-2670
 WhatsApp: +972 414-2670
 Telegram: @legitshopcompany
 Wickr ID: @legitshop008

Figure 15: Source – <https://ferkey4nox6vbwqr.onion/viewtopic.php?f=12&t=66260>

OWN SHOP
Best Marketplaces to Buy & Sell Online

Shop Checkout My account Become a Vendor Vendor Dashboard Checkout Contact us \$0.00 0 items

Home Products/Services Coronavirus - COVID-19

 **Coronavirus – COVID-19**

\$1,000.00

I was infected with Coronavirus – COVID-19!!!

I sell my infected blood and saliva.

I do this to provide for my family financially.

Indicate how you prefer to get after purchase (Order notes (optional)).

Add to cart

Sold by: E0K0D-19
 Category: Products/Services
 Tags: Corona, Coronavirus, COVID-19, virus

Product categories:

- Advertising
- All Shipping
- Coining
- Counterfeits
- Digital Downloads
- Documents
- Drugs
- Electronics
- Gift Cards
- Mask
- Page 19
- Poisons - Viruses
- Satanic Box
- Sex Dolls Hologram
- Shop Store

Figure 16: Source – <https://ownshopfar25ghcs.onion/?product=coronavirus-covid-19>

One particularly bleak offering, seen below in Figure 16, claims to offer blood and saliva from a coronavirus survivor. In theory, this blood and saliva could be immune to the virus, having developed the antibodies to fight it off.

Fake Mobile Apps

People around the world are desperate to find out how many coronavirus cases there are, and how severe the threat is in their regions. Cybercriminals wasted no time exploiting this fear, creating a plethora of fake mobile apps claiming to provide such data. IntSights monitors multiple online app stores for fake apps, and while some of the fake apps that have been created are benign, others have malicious capabilities such as ransomware, trojans, spyware, and more.

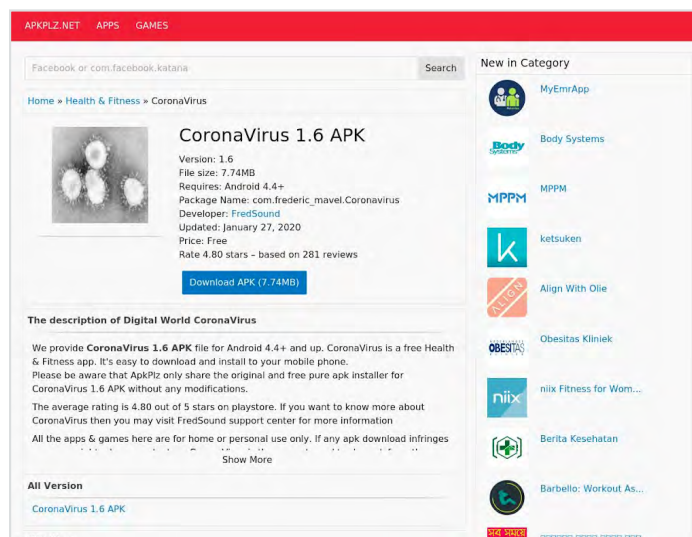


Figure 17: One example of a malicious coronavirus mobile application found in an app store through IntSights Threat Command

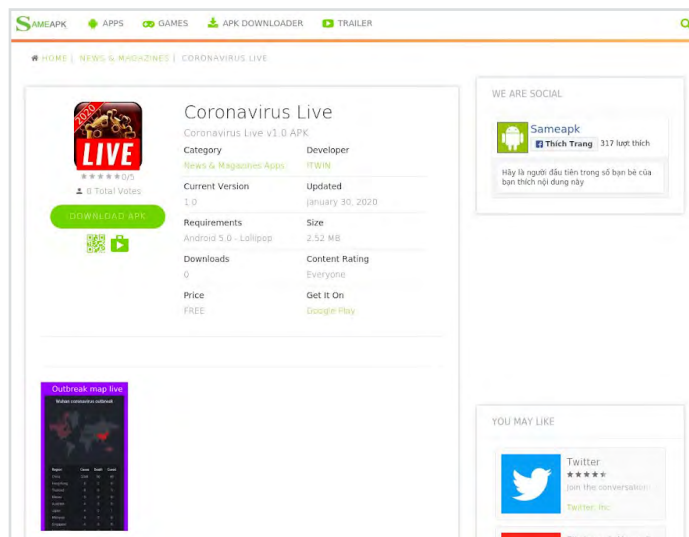


Figure 18: Another example of a malicious coronavirus mobile app in an Android app store, discovered through IntSights Threat Command

Remote Work Vulnerabilities

While phishing and malware attacks have always been around, what has significantly changed due to the COVID-19 pandemic is how employees communicate and access data. There is a significant increase in the usage of online meeting platforms, and the cybercriminals are paying attention. A quick look at IntSights Vulnerability Risk Analyzer (VRA) shows that cybercriminals are discussing different online platform vulnerabilities and exploits. With the majority of the workforce working from home and utilizing these platforms (sometimes on their personal computers as well), it is imperative to make sure these systems are secure and patched. The graphs below show clear, deep, and dark web mentions of specific CVEs per month.

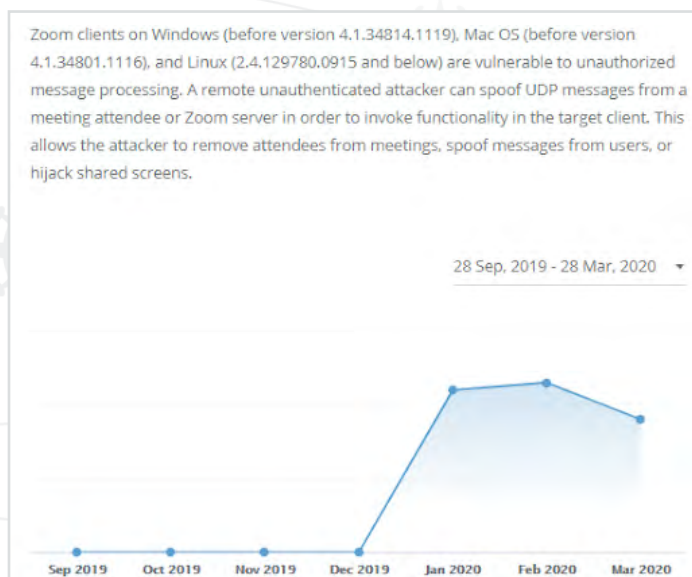


Figure 19: Increase in vulnerabilities in Zoom application between Dec 2019 and Mar 2020. Source: IntSights Vulnerability Risk Analyzer

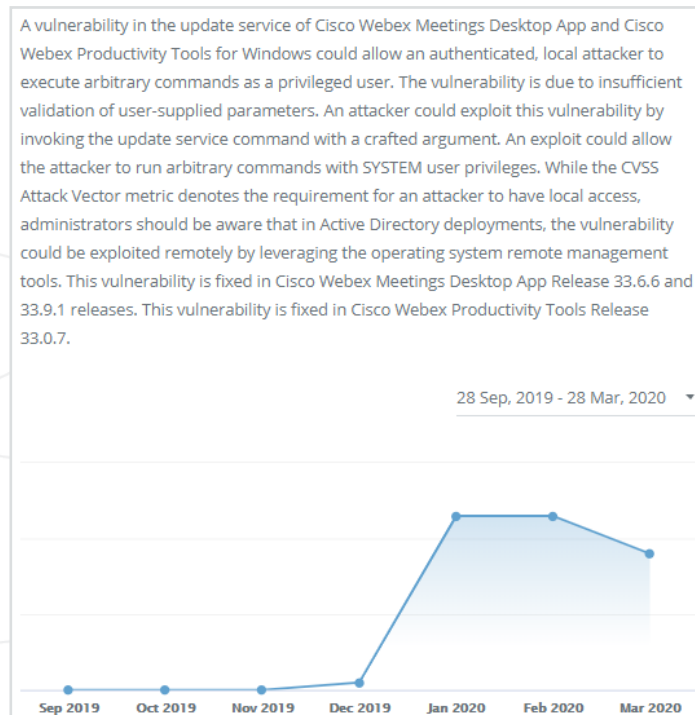


Figure 20: Increase in vulnerabilities in Cisco Webex Meetings desktop app between Dec 2019 and Mar 2020. Source: IntSights Vulnerability Risk Analyzer

Disinformation

Information about COVID-19 is pouring into the internet from every country and from various outlets, including governments, press, social media, healthcare professionals, and cybercriminals. As with any crisis, war, or other opportunity, threat actors are using the novel coronavirus to create panic, confusion, and distrust. Criminals have found ways to exploit human ignorance about coronavirus detection, testing, and treatment by selling various products and services that claim to help or heal people. Social media is teeming with hoaxes, myths, and conspiracy theories about where the virus originated, who is to blame for its global spread, how it spreads among the population, and how it can be detected. One example is a text message chain that started in the United States claiming that the federal government was going to shut down the whole country with a mandatory quarantine and implement martial law to enforce it (Figure 21).

The US government immediately denied that it sent out the message and [claimed the information was false](#). In the UK, a text message that appeared to be from the government said "You have been outside of your house 3 times today, you are in breach of government guidelines. Your £30 fine will be added to your bill." While the UK government did send one prior text to those with UK phone numbers, the text about the fine was false and caused panic among the population.

Just got this from a reliable source.

Please be advised, within 48 to 72 Hours it is very probable the president will evoke what is called the Stafford act. Just got off the phone with some of my military friends up in DC who just got out of a two-hour briefing. The president will order a two week mandatory quarantine for the nation. Stock up on whatever you need to make sure you have a two week supply of everything. Please forward to your network.

Figure 21: A viral text message spreading false news

Of greater concern is the spread of disinformation by state-sponsored operations to create dissent and disrupt world markets, elections, and authorities. Politicians and militaries alike are employing psychological operations on adversary populations to cause conflict, division, and dissent around this pandemic. However, this tactic is not new. Russia has been [conducting disinformation campaigns around healthcare](#) crises since 1983 with the AIDS crisis. Whether it is a [lie about an opponent in an election](#) and how he is governing during this crisis, an authoritarian party [censoring information to control the narrative](#), or a foreign nation trying to influence the world by placing blame for the origination of the virus, the tactics are difficult to detect and track.

Threat Actors

Criminals are capitalizing on people worldwide who are hungry for information about this virus and how it affects their daily lives. They are making huge profits selling fake products and vaccines, and price gouging medical supplies. Hackers are hijacking routers to spread coronavirus-themed malicious applications, disseminate malware, and conduct large-scale phishing campaigns. Some hackers have claimed they will righteously avoid hacking healthcare systems and hospitals out of mercy, yet hospitals all over the world are still suffering from crippling ransomware attacks. Meanwhile, underground hacking forums are ripe with opportunities related to coronavirus-themed attacks. Combine that with an internet-connected workforce that was rushed home with very little security preparation, and it makes for a perfect recipe for cybercrime profit.

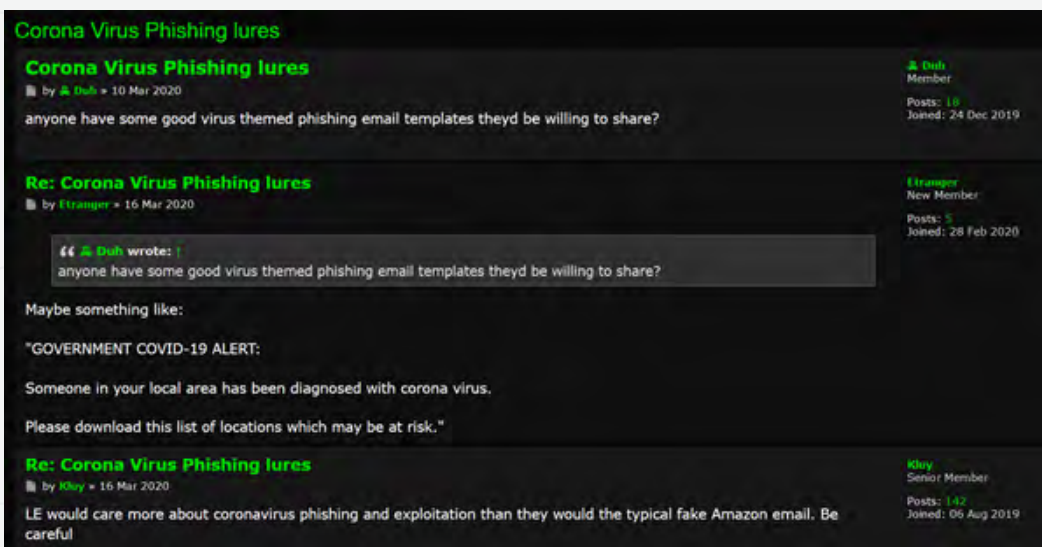


Figure 22: Criminals use dark web forums to advise each other on coronavirus-themed phishing lures that work

State-sponsored attackers thrive on global crises as a distraction from their “business as usual.” So far in the COVID-19 pandemic, three major state-sponsored campaigns have stood out to researchers:

Russia

In mid-February, a Russian state-sponsored hacking group known as “Hades” was observed targeting Ukraine with a multifaceted campaign, including malware and disinformation, designed to create panic and confusion around the novel coronavirus. The campaign started with a specially crafted phishing email (Figure 23, below) appearing to be from the Center for Public Health of the Ministry of Health of Ukraine and containing a bait document with fake information about COVID-19.

A malicious macro in the document drops a hidden C# backdoor trojan that grants the attackers remote control of the victim’s device. The second stage of the attack was a disinformation campaign, launched via social media in Ukraine, claiming that many people in Ukraine were infected with coronavirus. This fake news coincided with the arrival of a flight of evacuees from China. The combination of the events [incited riots and looting](#) across the country.

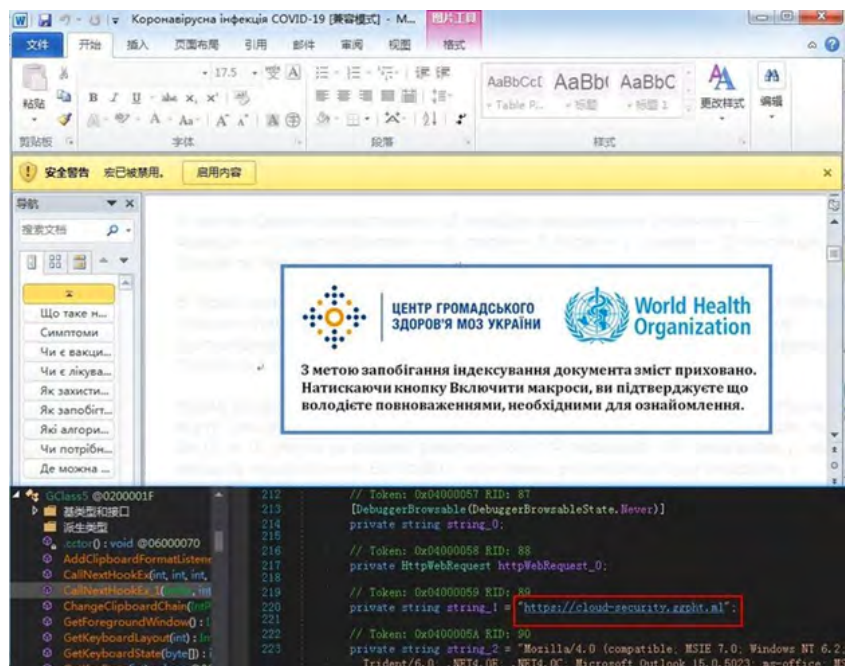


Figure 23: Maldoc opened through phishing campaign targeting Ukraine

North Korea

In late February, South Korean government officials received phishing emails with malicious documents attached that claimed to provide information on how the South Korean government planned to deal with the COVID-19 situation. Although not as sophisticated as the Russian campaign, the phishing campaign aimed at South Korea delivered BabyShark, a malware strain previously utilized by a North Korean hacker group known as Kimsuky.

China

The time period of March 1 through March 13, 2020, revealed that the largest number of targeted spear phishing campaigns [came from China](#). Advanced Persistent Threat (APT) groups such as “MUSTANG PANDA” and “VICIOUS PANDA” were discovered targeting people in Vietnam and Mongolia with phishing emails loaded with malicious .rar files. When the victim unzips the file, a backdoor trojan is installed on the machine.

Pakistan

APT36, also known as Transparent Tribe, ProjectM, Mythic Leopard, and TEMP.Lapis, is a state-sponsored threat actor attributed to Pakistan. APT36 was recently observed spreading a malicious Office document spoofed to look like it came from Indian government websites. The document appears to be a health advisory related to coronavirus and lures victims to enable macros, which then executes the Crimson RAT payload.

URLs ⓘ			
Scanned	Detections	URL	
2020-01-16	0 / 72	http://email.gov.in.maildrive.email/?att=1579160420	
2020-03-12	2 / 71	http://email.gov.in.maildrive.email/?att=1581914657	
2020-02-27	0 / 71	http://email.gov.in.maildrive.email/	
Downloaded Files ⓘ			
Scanned	Detections	Type	Name
2020-03-11	33 / 59	MS Excel Spreadsheet	36978_1582552996_NHQEncl1.xls1
2020-03-11	35 / 60	MS Excel Spreadsheet	2020-21.xls

Figure 24: VirusTotal view of malicious APT36 filenames. [Source](#)

Targets

While most hackers are likely to aim at easy targets, such as vulnerable technologies, internet-exposed networks and devices, and the general population's email accounts, more sophisticated threat actors are targeting the most vulnerable entities during this pandemic, including healthcare organizations, government agencies, and remote workers.

The **World Health Organization (WHO)** and other global health authorities are under heavy fire from cyber threat actors right now. As the whole world looks to the WHO for recommendations and guidance during this global crisis, hackers are launching destructive attacks to take them offline and disrupt operations. The World Health Organization's CISO, Flavio Aggio, said that cyberattacks have [doubled against the WHO](#) since the pandemic began. One recent campaign is thought by researchers to be attributed to an elite hacking group called DarkHotel. The group registered a fake WHO email website and went live on March 13th, after several failed attempts to steal employee credentials.

No industry is suffering more right now than the **healthcare industry**. Hospitals all over the world are overwhelmed with COVID-19 patients, are working hard to gather medical supplies, and are struggling to maintain qualified employees to assist in the pandemic. In the midst of all of this, hackers are relentlessly targeting healthcare networks, endpoints, and IOT devices in hopes to make a bitcoin--or several. Ransomware is still running rampant in the industry, shutting down entire hospitals and disabling life-saving medical devices.

Remote workers are easy targets right now. Within a few months time, thousands of office employees have been sent home to quarantine themselves against the spreading coronavirus. With little preparation and very little cybersecurity awareness, companies are scrambling to provide employees with devices, remote tools, and video conferencing applications. Many organizations are simply resorting to allowing employees to use their home computers and cell phones to conduct work unencrypted and unsecured. This situation has expanded the threat surface exponentially, and threat actors are looking to target the most popular platforms: email, messaging, video, VPNs, and home networks.

Recommendations

With most employees currently working from home, it is essential to make sure they operate in a secure environment. Threat actors are looking to take advantage of the remote workforce, knowing some people will make mistakes, such as:

- Not using provided security tools
- Performing physical and logical bridging of networks
- Using home computers for work
- Using corporate credentials for private business
- Using vulnerable software

In addition, attackers may target employees with phishing and malware that are not direct attacks against the company. The attacks mentioned in the TTPs section use the COVID-19 theme but ultimately aim to steal usernames and passwords to enterprise resources or collect PII.

In addition to everyday security hygiene and best practices, IntSights recommends:

- Assessing new risks based on threat intel. Known threat actors, such as Maze and FIN7, have stepped into the "corona-themed" attack scene. These are well-organized and experienced actors, and we can expect a rise in the sophistication of tools and tactics.
- Continuous monitoring of newly adopted remote access and collaboration technologies and their vulnerabilities. This also includes public code repositories that may be used more frequently now.
- Monitoring and enforcement of strong passwords, along with mandating 2FA for any access to corporate resources.
- Ensure the use of VPNs and encryption for communication and file sharing.
- Educating end users on the current threat landscape and the types of attacks deployed by different threat actors, including phishing, malware, social engineering, fake mobile apps, and more.



About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on [LinkedIn](#), [Twitter](#), and [Facebook](#).

