telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

May 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

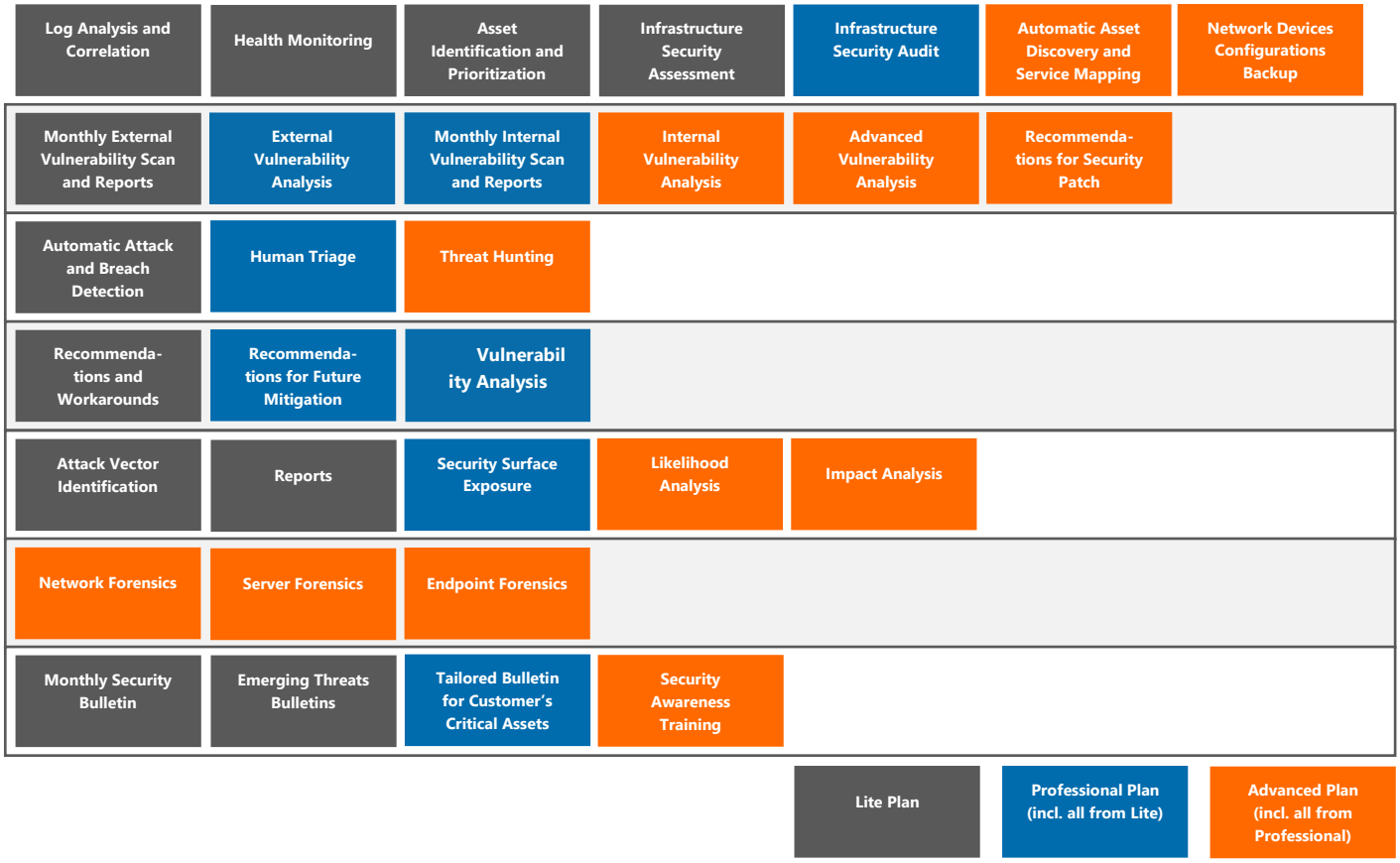
Start to mitigate cyber threats and minimize the risk!

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!



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

1. Microsoft warned of ongoing human-operated ransomware campaigns targeting healthcare organizations and critical services, and shared tips on how to block new breaches by patching vulnerable Internet-facing systems. Many such attacks start with the human operators first exploiting vulnerabilities found in internet-facing network devices or by brute-forcing RDP servers and then deploying the ransomware payloads. →

2. A new Windows malware has emerged that makes disks unusable by overwriting the master boot record (MBR) - the same trick that the infamous NotPetya wiper malware used in 2017. This malware takes its cue from the COVID-19 pandemic, calling itself simply "Coronavirus." →

3. With growing the volume and complexity of attacks, high-quality threat intelligence can offer immediate network protection, provide visibility to known threats and significantly reduce the time required for situational investigation or incident response. See how relevance scoring (correlation of the properties of security analysts' threat intelligence and those of their organization) can help. →

4. Attacks using new card-harvesting code from the prolific Magecart Group and is targeting small- to medium-sized businesses, claiming 19 sites so far. →

5. 44 Million of IDs, charge cards, loyalty cards, gift cards, medical marijuana ID cards and personal information was left exposed to the open Internet by Key Ring, creator of a digital wallet app used by 14 million people across North America. →

6. Many companies are now holding daily meetings using videoconferencing services from Zoom. But without the protection of a password, there's a decent chance your next Zoom meeting could be "Zoom bombed" — attended or disrupted by someone who doesn't belong – an action aided by new automated Zoom meeting discovery tool dubbed "zWarDial,". →

7. More than 350,000 of all Microsoft Exchange servers (80% of all)currently exposed on the Internet haven't yet been patched against the CVE-2020-0688 RCE vulnerability affecting all supported Microsoft Exchange Server versions via turned on by default Exchange Control Panel (ECP) component, allowing attackers to take over vulnerable Microsoft Exchange servers using any previously stolen valid email credentials. →

8. According to Microsoft, the volume of malicious attacks hasn't increased, but instead, threat actors have repurposed infrastructure used in previous attacks and rethemed attack campaigns to exploit fears surrounding the COVID-19 pandemic. →

9. A malicious, copycat Malwarebytes website serves up the Raccoon information stealer malware to unsuspecting visitors was set up in March and is being used in a malvertising campaign via the PopCash ad network. →

10. As reported by Wall Street Journal, Travelex, an company that provides foreign-exchange services in 70 countries across more than 1,200 retail branches, has paid out $2.3 million in Bitcoin to hackers to regain access to its global network after a malware attack at the new year knocked the global currency exchange offline and crippled its business during the month of January. →

11. With the release of the April 2020 security updates, Microsoft has released fixes for 113 vulnerabilities in Microsoft products. Out of all these vulnerabilities, 15 are classified as Critical, 93 as Important, 3 as Moderate, and 2 as Low. Within these of particular interest are four zero-day vulnerabilities, with two of them being seen actively exploited in attacks. →

12. Active GitHub users are currently being targeted by a phishing campaign specifically designed to collect and steal their credentials via landing pages mimicking GitHub's login page. After taking over their accounts, the attackers are also immediately downloading the contents of private repositories, including but not limited to "those owned by organization accounts and other collaborators." →

13. As per Bill Bonney article in Information Security magazine companies need to adopt a digital trust mindset, invest in system hygiene and commit to a high-performing security function that can provide flexibility in business and protect the products and services that their customers rely on. →

14. Microsoft has released an out-of-band security update for Microsoft Office, Office 365 ProPlus and Paint 3D. The applications are affected by multiple Autodesk vulnerabilities that, if exploited, could enable remote code execution. →

15. Threat actors with varying motivations are actively exploiting the current pandemic and public fear of the coronavirus and COVID-19 and are creating malware distribution campaigns. Check the article for several samples, involving malicious MS Office and Open Office documents. →

16. Twitter announced that it has turned off the Twitter via SMS service because of security concerns, a service which allowed the social network's users to tweet using text messages since its early beginnings. →

17. A sophisticated, ongoing espionage campaign, Dubbed PhantomLance by Kaspersky is aimed at Android users in Asia and is likely the work of the OceanLotus advanced persistent threat (APT) actor. The campaign is distributed via dozens of apps within the Google Play official market, as well as other outlets like the third-party marketplace known as APKpure. →

18. Check interview of four of Fortinet's Field CISOs – Courtney Radke, Renee Tarun, Joe Robertson, and Alain Sanchez, discussing the value of Secure SD-WAN in today's evolving threat landscape. →

1. Microsoft releases guidance on blocking ransomware attacks

Microsoft warned today of ongoing human-operated ransomware campaigns targeting healthcare organizations and critical services, and shared tips on how to block new breaches by patching vulnerable internet-facing systems.

Many such attacks start with the human operators first exploiting vulnerabilities found in internet-facing network devices or by brute-forcing RDP servers and then deploying the ransomware payloads.

For instance, Pulse VPN devices have been targeted by threat actors in the past, with one such vulnerable device thought to be behind the Travelex ransomware attack by Sodinokibi (REvil).

Other ransomware gangs such as DoppelPaymer and Ragnarok Ransomware also exploited the Citrix ADC (NetScaler) CVE-2019-1978 vulnerability to get a foothold on the edge of their victims' networks.

As Microsoft details, the final stage of deploying the ransomware and encrypting the systems is normally preceded by a reconnaissance stage where the attackers steal data they can later use for blackmail, as well as harvest credentials and move laterally throughout their victims' networks.

To prevent all of this from happening, Microsoft advises potential victims to prevent threat actors behind ransomware campaigns from being able to exploit the weaknesses they usually abuse to launch their attacks.

Reduce the risk of being a ransomware victim

"Applying security patches for internet-facing systems is critical in preventing these attacks," the Microsoft Threat Protection Intelligence Team explains.

From data acquired by Microsoft following recent ransomware attacks, the malicious actors commonly take advantage of these security gaps:

• Remote Desktop Protocol (RDP) or Virtual Desktop endpoints without multi-factor authentication (MFA)

• Older platforms that have reached end of support and are no longer getting security updates, such as Windows Server 2003 and Windows Server 2008, exacerbated by the use of weak passwords

• Misconfigured web servers, including IIS, electronic health record (EHR) software, backup servers, or systems management servers

• Citrix Application Delivery Controller (ADC) systems affected by CVE-2019-19781

• Pulse Secure VPN systems affected by CVE-2019-11510

While Microsoft hasn't observed any recent attacks exploiting the CVE-2019-0604 (Microsoft SharePoint), CVE-2020-0688 (Microsoft Exchange), CVE-2020-10189 (Zoho ManageEngine) vulnerabilities, based on historical signals they will eventually be exploited to gain access within victims' networks, so they are also worth reviewing and patching.

Detecting and responding to ongoing attacks

Organizations should also hunt for signs of an active ransomware attack within their environments like tools that help the attacks blend in with red team activities (e.g., Malicious PowerShell, Cobalt Strike, and other penetration-testing tools), credential theft activities, or security logs tampering.

Once any such signs are detected, orgs' security operations teams should immediately take the following actions to assess the security impact and prevent the payloads from being deployed:

- Investigate affected endpoints and credentials
- Isolate compromised endpoints
- Inspect and rebuild devices with related malware infections

Addressing internet-facing weaknesses by searching for and identifying any perimeter systems the attackers could have used as a stepping stone to gain access to their networks is another important measure to defend against ransomware attacks.

Systems that ransomware attackers might try to abuse during their attacks:

- RDP or Virtual Desktop endpoints without MFA
- Citrix ADC systems affected by CVE-2019-19781
- Pulse Secure VPN systems affected by CVE-2019-11510
- Microsoft SharePoint servers affected by CVE-2019-0604
- Microsoft Exchange servers affected by CVE-2020-0688
- Zoho ManageEngine systems affected by CVE-2020-10189

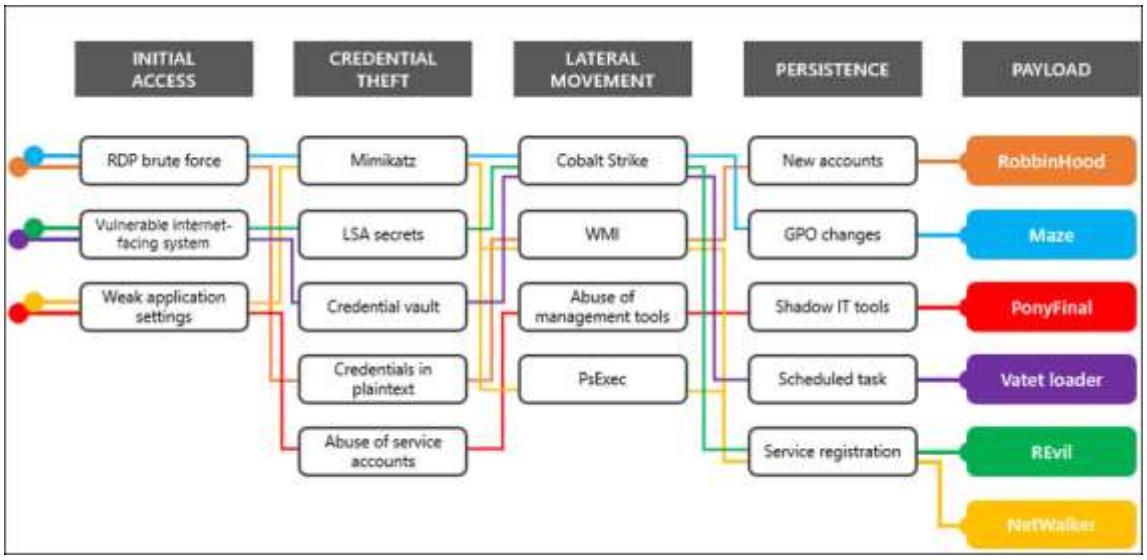
Ransomware gangs maintain access to victims' networks for months

"Multiple ransomware groups that have been accumulating access and maintaining persistence on target networks for several months activated dozens of ransomware deployments in the first two weeks of April 2020," Microsoft says.

"So far the attacks have affected aid organizations, medical billing companies, manufacturing, transport, government institutions, and educational software providers, showing that these ransomware groups give little regard to the critical services they impact, global crisis notwithstanding."

Furthermore, healthcare orgs and critical services are not the only ones targeted by ransomware gangs so all government and private organizations should take pre-emptive measures to mitigate such risks and be ready to react at any time.

As Microsoft's threat intelligence data shows, the initial date of infiltration within the ransomed orgs' networks dates to the beginning of 2020, with the attackers waiting to deploy the ransomware payloads at the perfect moment that gets them the most financial gain.



Attack techniques used by ransomware gangs (Microsoft)

"In stark contrast to attacks that deliver ransomware via email—which tend to unfold much faster, with ransomware deployed within an hour of initial entry—the attacks we saw in April are similar to the Doppelpaymer ransomware campaigns from 2019, where attackers gained access to affected networks months in advance," Microsoft adds.

"They then remained relatively dormant within environments until they identified an opportune time to deploy ransomware.

"On networks where attackers deployed ransomware, they deliberately maintained their presence on some endpoints, intending to reinitiate malicious activity after ransom is paid or systems are rebuilt.

"In addition, while only a few of these groups gained notoriety for selling data, almost all of them were observed viewing and exfiltrating data during these attacks, even if they have not advertised or sold yet."

During early March, Microsoft shared information on the various entrance vectors and post-exploitation techniques used by the operators behind DoppelPaymer, Dharma, and Ryuk, showing that there's an overwhelming overlap in the security misconfigurations these threat actors abuse as part of their devastating ransom attacks.

Microsoft is also alerting hospitals regarding vulnerable public-facing VPN devices and gateways located on their networks starting with April 1.

As a glimpse at the actual impact ransomware attacks have on the victims, after analyzing collected cryptocurrency wallets and ransomware ransom notes, the FBI said at this year's RSA security conference that victims paid more than $140 million to ransomware operators during the past six years.

Source: https://www.bleepingcomputer.com/news/security/microsoft-releases-guidance-on-blocking-ransomware-attacks/

2. Wiper Malware Called “Coronavirus” Spreads Among Windows Victims

Like NotPetya, it overwrites the master boot record to render computers "trashed."

A new Windows malware has emerged that makes disks unusable by overwriting the master boot record (MBR). It takes its cue from the COVID-19 pandemic, calling itself simply “Coronavirus.”

Overwriting the MBR is the same trick that the infamous NotPetya wiper malware used in 2017 in a campaign that caused widespread, global financial damage.

Worryingly, according to the SonicWall Capture Labs Threat Research team, the fresh malware strain is also a destructive trojan — though not as destructive as other wipers. And like its namesake, there’s no obvious cure. In a posting on Tuesday, researchers explained that victims of the Coronavirus trojan find themselves with a gray screen and a blinking cursor with a simple message, “Your computer has been trashed.”

The novel coronavirus, and the disease it causes, COVID-19, has provided a depth of fodder for cybercriminals looking to capitalize on the global concern around the pandemic. For instance, a recent spate of phishing attacks has used the promise of financial relief due to the disease as a lure. However, the operator behind this malware takes it one step further, going so far as to take the coronavirus as its name and infection theme.

As far as that infection routine, the malware can be delivered in any of the usual ways – as a malicious email attachment, file download, fake application and so on.

Upon execution, the malware starts its process by installing a number of helper files, which are placed in a temporary folder. The malware cleaves tight to its pandemic theme: An installer (a helper file named “coronavirus.bat”) sets up the attack by creating a hidden

folder named "COVID-19" on the victim machine. The previously dropped helper files are then moved there, in an effort to go unnoticed until its goal is achieved.

After that, the installer disables Windows Task Manager and User Access Control (UAC) in a further stab at obfuscation, according to the analysis. It also changes the victim's wallpaper, and disables options to add or modify that wallpaper after the change is made. It also adds entries in registry for persistence, and then sets about rebooting to finish the installation.

The process run.exe creates a batch file named run.bat to ensure the registry modifications done by "coronavirus.bat" are kept intact during the reboot process, according to SonicWall.

After reboot, the infection executes two binaries. One, "mainWindow.exe," displays a window with a picture of the coronavirus itself, with two buttons. At the top of the window, the victim is notified that "coronavirus has infected your PC!"

The two buttons read "Remove virus" and "Help." The former does nothing when clicked; the latter brings up a pop-up that tells victims to "not wast [sic] your time" because "you can't terminate this process!"

The other binary carries out the meat of the attack: It's responsible for overwriting the MBR.

"The original MBR is first backed up in the first sector before it is overwritten with new one, [and the] MBR is overwritten with the new code," according to the researchers.

Once the overwrite is complete, the victim's display is changed to a simple grey screen delivering the bad news:

SonicWall told Threatpost in an email interview that it was able to analyze the sample after it was uploaded to VirusTotal. Thus, so far, there haven't been many instances of "Coronavirus" observed in the wild, and little in known in terms of targeting or what the spreading mechanisms are for the mysterious new malware.

The team also told Threatpost that the good news is that this is not as dangerous as other wiper strains.

"Even if the MBR is not restored…data can still be accessed/recovered by mounting the drive," the firm noted. "The MBR [also] can be potentially restored, but it is not easy and requires deep technical knowledge."

Source: https://threatpost.com/wiper-malware-coronavirus-windows-victims/154368/

3. How Relevance Scoring Can Make Your Threat Intell More Actionable

As businesses around the world become more global, the volume and complexity of attacks continue to grow. Protecting a company in today's environment has become more difficult. For example, securing an organization with offices in London, Hong Kong and Santa Cruz represents a challenge of both scale and complexity for security analysts. In addition, the number of companies affected by data breaches, destructive malware and ransomware is growing at a rapid pace.

High-quality threat intelligence can offer immediate network protection, provide visibility to known threats and significantly reduce the time required for situational investigation or incident response.

Security analysts, whether performing incident response or general threat research, need automated tools with intelligent rules to help find, organize and filter the most relevant information for their primary task. Within the security operations center (SOC), analysts and incident response engineers use threat intelligence to quickly isolate the signal from the noise, identify real problems and their fixes, and prioritize remediation efforts.

Speed is imperative. More specifically, time to decision is everything.

Challenges Facing Security Analysts

In order to shorten their time to decision, security analysts need to quickly answer key questions, such as:

- Do I understand the situation?
- Is the threat real?
- What is its potential impact on my organization?
- How do I prioritize it against my backlog?
- What evidence do I have to support my position?
- What do I do next?

Threat intelligence can help answer those questions. It can provide context to the situation being investigated. Indicator-based threat intelligence can corroborate internal sightings, and vulnerability-based threat intelligence can help illuminate potential exposures and consequences for the organization.

However, a key problem for analysts, assuming they have quality threat intelligence, is relevance. How do you know if *that* threat intelligence is relevant to *this* situation?

How Relevance Scoring Can Help

Relevance scoring is a technique that correlates the properties of security analysts' threat intelligence and those of their organization, such as the industry and region. By identifying indicators associated with one or more of the organization's properties, analysts can place more weight on those specific to the organization compared to other indicators, especially when correlating against traffic they are investigating. Wouldn't it be better if analysts' automated tool sets understood and could use relevance scoring to provide more relevant insights automatically?

These techniques yield a relevance scoring system that is specific to the user's organization, industry and region. Embedding relevance scoring in security tools provides professionals with the right data at the right time, contextualized to their situation. Organizations that share their sightings with other threat sharing organizations and threat intelligence vendors who accept direct or anonymized user sightings containing local properties can enrich their threat intelligence, benefiting the larger communities these organizations are a part of.

Quality threat intelligence combined with local relevance scoring can go directly to the bottom line in the form of faster incident investigation, determination, prioritization and remediation.

Learn how the X-Force Threat Score brings relevance scoring to IBM Security Threat Intelligence Insights

The post How Relevance Scoring Can Make Your Threat Intelligence More Actionable appeared first on Security Intelligence.

Source: http://feedproxy.google.com/~r/SecurityIntelligence/~3/NhPGN6rYv5k/

4. Emerging MakeFrame Skimmer from Magecart Sets Sights on SMBs

Attacks using a brand-new card-harvesting code is targeting small- to medium-sized businesses, claiming 19 sites so far.

Researchers have observed a new skimmer from the prolific Magecart Group that has been actively harvesting payment-card data from 19 different victim websites, mainly belonging to small- and medium-sized businesses (SMBs), for several months.

RiskIQ researchers first discovered the skimmer, dubbed MakeFrame for its use of iframes to skim data, on Jan. 24. Since then, they've captured several different versions of the skimmer with "various levels of obfuscation," researchers Jordan Herman and Mia Ihm wrote in a blog post published Thursday.

The versions range from from development versions in clear code to finalized versions using encrypted obfuscation, they wrote.

"This version of the skimmer is the classic Magecart blob of hex-encoded terms and obfuscated code," Herman and Ihn wrote. "It is nestled in amongst benign code to blend in and avoid detection."

MakeFrame also leeches off the compromised site for its functionality, a technique that in particular alerted researchers that MakeFrame is most likely the work of Magecart Group 7. And, targeting SMB sites, as MakeFrame does, also is indicative of Magecart Group 7 activity, researchers said.

"In some cases, we've seen MakeFrame using compromised sites for all three of its functions — hosting the skimming code itself, loading the skimmer on other compromised websites and exfiltrating the stolen data," Herman and Ihm wrote.

Indeed, Magecart Group 7 typically uses victim sites for skimmer development, which was also observed when the group compromised OXO in 2017 and in activity by the group in 2018, researchers wrote.

"In all of these cases, the skimmer is hosted on the victim domain," according to the analysis. "The stolen data is posted back to the same server or sent to another compromised domain."

Another aspect of MakeFrame that links the new skimmer back to Magecart Group 7 is its method of exfiltration of data once it's stolen, Herman and Ihm noted. The skimmer sends stolen data in the form of .PHP files to other compromised sites for exfiltration, they said.

"Each compromised site used for data exfil has also been injected with a skimmer and has been used to host skimming code loaded on other victim sites as well," the researchers added.

Magecart Group 7 is one of a number of threat actors operating under the Magecart umbrella, which includes several different groups who all use a similar attack vector. Magecart attacks compromise websites — principally built on the Magento e-commerce platform – to inject card-skimming scripts on checkout pages to steal customer payment-card details and other data entered on the page's fields.

The group has been active since 2016 and consistently switches tactics to target e-commerce platforms to steal people's payment and other credentials.

Skimmers are the primary weapons of choice for the various Magecarts groups, but they have also engaged in other nefarious activities such as brute-forcing passwords, spoofing third-party payment sites and even targeting Wi-Fi routers with malicious code to steal customer data.

The latest skimmer uncovered by RiskIQ shows the group's "continued evolution, honing tried-and-true techniques and developing new ones all the time," researchers wrote.

The onset of stay-at-home orders amid the COVID-19 pandemic also seems to have inspired Magecart to bolster activity as more people conduct business online, with many brick-and-mortar shops and shopping malls closed, researchers noted.

"RiskIQ data shows Magecart attacks have grown 20 percent amid the COVID-19 pandemic," Herman and Ihm wrote. "With many home-bound people forced to purchase what they need online, the digital-skimming threat to e-commerce is as pronounced as ever."

Source: https://threatpost.com/emerging-makeframe-skimmer-magecart-smbs/154374/

5. 44M Digital Wallet Items Exposed in Key Ring Cloud Misconfig

Millions of IDs, charge cards, loyalty cards, gift cards, medical marijuana ID cards and personal information was left exposed to the open internet.

Key Ring, creator of a digital wallet app used by 14 million people across North America, has exposed 44 million IDs, charge cards, loyalty cards, gift cards and membership cards to the open internet, researchers say.

The Key Ring app allows users to upload scans and photos of various physical cards into a digital folder on a user's phone. While Key Ring is primarily designed for storing membership cards for loyalty programs, users also store more sensitive cards on the app. According to the research team at vpnMentor, it found 44 million scans exposed in a misconfigured cloud database that included: Government IDs, retail club membership and loyalty cards, NRA membership cards, gift cards, credit cards with all details exposed

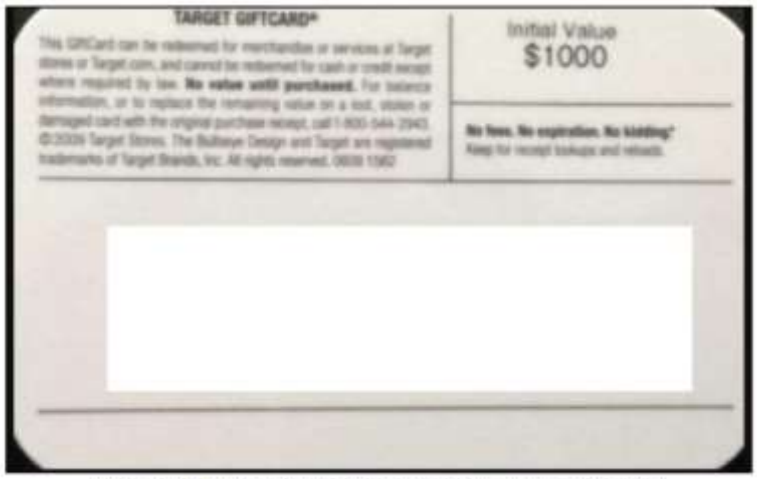
(including CVV numbers), medical insurance cards and medical marijuana ID cards, among others.

vpnMentor said that it found a total of five misconfigured Amazon Web Services (AWS) S3 cloud databases owned by the company. These could have revealed millions of these uploads to anyone with a web browser, thanks to a lack of password-protection on the buckets, the company said. Also, every file could also be downloaded and stored offline.

Threatpost reached out to Key Ring's media team multiple times over the last few days for a comment or reaction to the findings, with no response — and will update this post with any additional information should the company eventually respond.

Five Databases of Information

According to the research, launched Thursday and shared with Threatpost ahead of publication, vpnMentor came across indicators of an initial exposed bucket in January, which contained the scanned card information. However, that wasn't the extent of the exposed data.



***Example 1:** A Target gift card with a value of $1,000*

The researchers also said that they found older, brand-specific loyalty-card lists sorted by retail company, including CSV databases detailing various reports on customers of Walmart, Footlocker and other big brands. vpnMentor said that the lists contained personally identifiable information (PII) data for millions, including full names, emails, membership ID numbers, dates of birth, physical addresses and ZIP codes. The firm also said that the data set stretched back in some cases to 2014.

Examples of the number of people exposed in these lists include 16 million for Walmart, 64,000 for the Kids Eat Free Campaign, 6,600 for La Madeleine and 2,000 for Mattel, among others, it said.

Also, as the firm was looking into the situation, it said that it found four additional unsecured S3 buckets belonging to Key Ring, which the company said contained even more sensitive data.

vpnMentor said that these additional four storage units each contained a different snapshot of Key Ring's internal database of users, containing emails, home addresses, device and IP address info, encrypted passwords and the "salt" randomized data used to encrypt them and more.

Disclosure and Exposure

Once the details of the leak were confirmed, the vpnMentor team said that it contacted Key Ring and AWS to disclose the discovery on February 18 – and the buckets were secured two days later.

However, Key Ring itself never responded to the firm's findings.

"We reached out to them but didn't get any reply," Noam Rotem, lead of vpnMentor's research team, told Threatpost. "At the same time, we reached out to Amazon, who (we believe) reached out to them too in order to secure the data. As we haven't been in touch with them, we don't know if they're going to notify their users."

The research team is unsure of how long the data was exposed prior to the discovery.

"In fact, we can't say for certain that nobody else found these S3 buckets and downloaded the content before we notified Key Ring," according to the analysis shared with Threatpost. "If this happened, simply deleting the exposed data and securing the S3 buckets might not be enough. Hackers would still have access to all the data, stored locally, offline and completely untraceable."

vpnMentor said that the team did not reach out to the third parties (Walmart, et al) about the data exposure: "It doesn't seem related to data sharing, as data sharing is supposed to be related to the PII provided by their customers, and not the cards [that individuals] scan and save in their wallet," Rotem said.

Potential Fallout

Key Ring's databases, if they've been stolen, could facilitate massive fraud and identity theft schemes targeting millions of people in America and Canada, according to the analysis.

Any cybercriminal that accessed the databases could sell the information on the criminal underground, or use it themselves, vpnMentor pointed out. Potential attacks include identity theft; the ability to file fraudulent tax returns and claim refunds in victims' names; credit-card fraud and online shopping fraud; account takeovers; stealing and using

accrued loyalty points; and even "loan stacking" where criminals take out multiple loans in a person's name, from automated lenders, with numerous payouts made before the victim becomes aware. Plus, the wealth of information opens victims up to phishing and convincing email scams.

"What's most notable about this incident is that people would trust companies to secure their data, and hence share with them everything, including their credit cards (both sides), without fearing that this could be exploited," Rotem told Threatpost. "Needless to list the risks related to a clear credit-card picture leaking."

vpnMentor pointed out that the company itself could also be in danger if the database has been downloaded by criminal hackers.

"Aside from losing users and partners, Key Ring would have been vulnerable to legal action, fines and intense scrutiny from government data privacy groups," the research noted. "Key Ring is already no longer operating in the EU due to the inability to comply with GDPR. With California enacting its data privacy law in January 2020 – the CCPA – Key Ring could still have faced investigation and fines from the state's legislative bodies. Given the scale and seriousness of this leak, the impact on the company's finances, reputation and market share would be unmeasurable."

The company's privacy policy was last updated in March 2015 and states: "We may encrypt certain sensitive information using Secure Socket Layer (SSL) technology to ensure that your Personally Identifiable Information is safe as it is transmitted to us."

It adds: "However, no data transmission can be guaranteed to be 100 percent secure. As a result, while we employ commercially reasonable security measures to protect data and seek to partner with companies that do the same, we cannot guarantee the security of any information transmitted to or from the Website or via the Key Ring Service, and are not responsible for the actions of any third parties that may receive any such information."

Cloud misconfigurations are all too common, with businesses both large and small inadvertently exposing users' personal data. In fact, a recent Unit 42 report found that more than half (60 percent) of breaches occur in the public cloud due to misconfiguration.

Rotem told Threatpost that "we're not here to judge how these companies are managing their customers' data." However, he added that "too many companies are failing at protecting their data…the way they react to such leaks, fix and respond is what would distinguish a company that cares about its security and customers, from a company that doesn't."

Threatpost also reached out to Key Ring for more details on its disclosure policies and how it has handled this incident.

Source: https://threatpost.com/44m-digital-wallet-key-ring-cloud-misconfig/154260/

6. ‘War Dialing’ Tool Exposes Zoom’s Password Problems

As the Coronavirus pandemic continues to force people to work from home, countless companies are now holding daily meetings using videoconferencing services from **Zoom**. But without the protection of a password, there’s a decent chance your next Zoom meeting could be “Zoom bombed” — attended or disrupted by someone who doesn’t belong. And according to data gathered by a new automated Zoom meeting discovery tool dubbed “**zWarDial**,” a crazy number of meetings at major corporations are not being protected by a password.

zWarDial, an automated tool for finding non-password protected Zoom meetings. According to its makers, zWarDial can find on average 110 meetings per hour, and has a success rate of around 14 percent.

Each Zoom conference call is assigned a Meeting ID that consists of 9 to 11 digits. Naturally, hackers have figured out they can simply guess or automate the guessing of random IDs within that space of digits.

Security experts at **Check Point Research** did exactly that last summer, and found they were able to predict approximately four percent of randomly generated Meeting IDs. The Check Point researchers said enabling passwords on each meeting was the only thing that prevented them from randomly finding a meeting.

Zoom responded by saying it was enabling passwords by default in all future scheduled meetings. Zoom also said it would block repeated attempts to scan for meeting IDs, and that it would no longer automatically indicate if a meeting ID was valid or invalid.

Nevertheless, the incidence of Zoombombing has skyrocketed over the past few weeks, even prompting an alert by the FBI on how to secure meetings against eavesdroppers and mischief-makers. This suggests that many Zoom users have disabled passwords by default and/or that Zoom's new security feature simply isn't working as intended for all users.

New data and acknowledgments by Zoom itself suggest the latter may be more likely.

Earlier this week, KrebsOnSecurity heard from Trent Lo, a security professional and co-founder of SecKC, Kansas City's longest-running monthly security meetup. Lo and fellow SecKC members recently created **zWarDial**, which borrows part of its name from the old phone-based war dialing programs that called random or sequential numbers in a given telephone number prefix to search for computer modems.

Lo said zWarDial evades Zoom's attempts to block automated meeting scans by routing the searches through multiple proxies in Tor, a free and open-source software that lets users browse the Web anonymously.

"Zoom recently said they fixed this but I'm using a totally different URL and passing a cookie along with that URL," Lo said, describing part of how the tool works on the back end. "This gives me the [Zoom meeting] room information without having to log in."

Lo said a single instance of zWarDial can find approximately 100 meetings per hour, but that multiple instances of the tool running in parallel could probably discover most of the open Zoom meetings on any given day. Each instance, he said, has a success rate of approximately 14 percent, meaning for each random meeting number it tries, the program has a 14 percent chance of finding an open meeting.

Only meetings that are protected by a password are undetectable by zWarDial, Lo said.

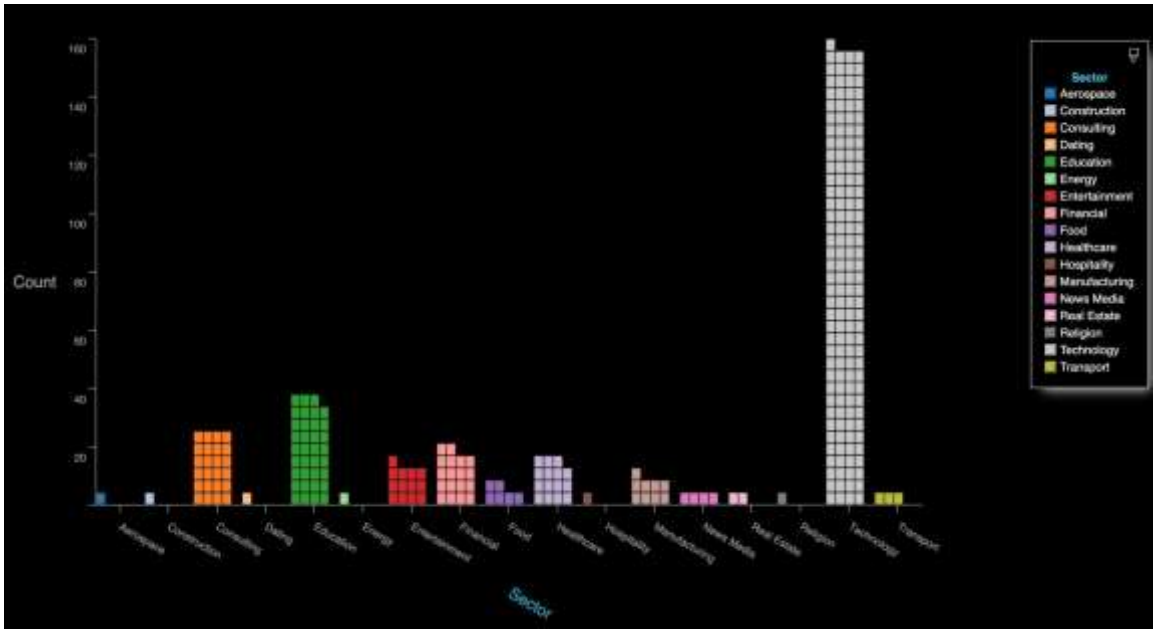
"Having a password enabled on the meeting is the only thing that defeats it," he said.

Lo shared the output of one day's worth of zWarDial scanning, which revealed information about nearly 2,400 upcoming or recurring Zoom meetings. That information included the link needed to join each meeting; the date and time of the meeting; the name of the meeting organizer; and any information supplied by the meeting organizer about the topic of the meeting.

The results were staggering, and revealed details about Zoom meetings scheduled by some of the world's largest companies, including major banks, international consulting firms, ride-hailing services, government contractors, and investment ratings firms.

KrebsOnSecurity is not naming the companies involved, but was able to verify dozens of them by matching the name of the meeting organizer with corporate profiles on LinkedIn.

By far the largest group of companies exposing their Zoom meetings are in the technology sector, and include a number of security and cloud technology vendors. These include at least one tech company that's taken to social media warning people about the need to password protect Zoom meetings!



The distribution of Zoom meetings found by zWarDial, indexed by industry. As depicted above, zWarDial found roughly 2,400 exposed meetings in less than 24 hours. Image: SecKC.

A GREMLIN IN THE DEFAULTS?

Given the preponderance of Zoom meetings exposed by security and technology companies that ostensibly should know better, KrebsOnSecurity asked Zoom whether its approach of adding passwords by default to all new meetings was actually working as intended.

In reply, Zoom said it was investigating the possibility that its password-by-default approach may fail under certain circumstances.

"Zoom strongly encourages users to implement passwords for all of their meetings to ensure uninvited users are not able to join," the company said in a written statement shared with this author.

"Passwords for new meetings have been enabled by default since late last year, unless account owners or admins opted out," the statement continues. "We are looking into unique edge cases to determine whether, under certain circumstances, users unaffiliated with an account owner or administrator may not have had passwords switched on by default at the time that change was made."

The acknowledgment comes amid a series of security and privacy stumbles for Zoom, which has seen its user base grow exponentially in recent weeks. Zoom founder and chief executive **Eric Yuan** said in a recent blog post that the maximum number of daily meeting participants — both paid and free — has grown from around 10 million in December to 200 million in March.

That rapid growth has also brought additional scrutiny from security and privacy experts, who've found plenty of real and potential problems with the service of late. TechCrunch's **Zack Whittaker** has a fairly comprehensive breakdown of them here; not included in that list is a story he broke earlier this week on a pair of zero-day vulnerabilities in Zoom that were publicly detailed by a former NSA expert.

Zoom CEO Yuan acknowledged that his company has struggled to keep up with steeply growing demand for its service and with the additional scrutiny that comes with it, saying in a blog post that for the next 90 days all new feature development was being frozen so the company's engineers could focus on security issues.

Dave Kennedy, a security expert and founder of the security consultancy TrustedSec, penned a lengthy thread on Twitter saying while Zoom certainly has had its share of security and privacy goofs, some in the security community are unnecessarily exacerbating an already tough situation for Zoom and the tens of millions of users who rely on it for day-to-day meetings.

"What we have here is a company that is relatively easy to use for the masses (comes with its challenges on personal meeting IDs) and is relatively secure," Kennedy wrote. "Yet the industry is making it out to be 'this is malware' and you can't use this. This is extreme. We need to look at the risk specific applications pose and help voice a message of how people can leverage technology and be safe. Dropping zero-days to the media hurts our credibility, sensationalizes fear, and hurts others."

"If there are ways for a company to improve, we should notify them and if they don't fix their issues, we should call them out," he continued. "We should not be putting fear into everyone, and leveraging the media as a method to create that fear."

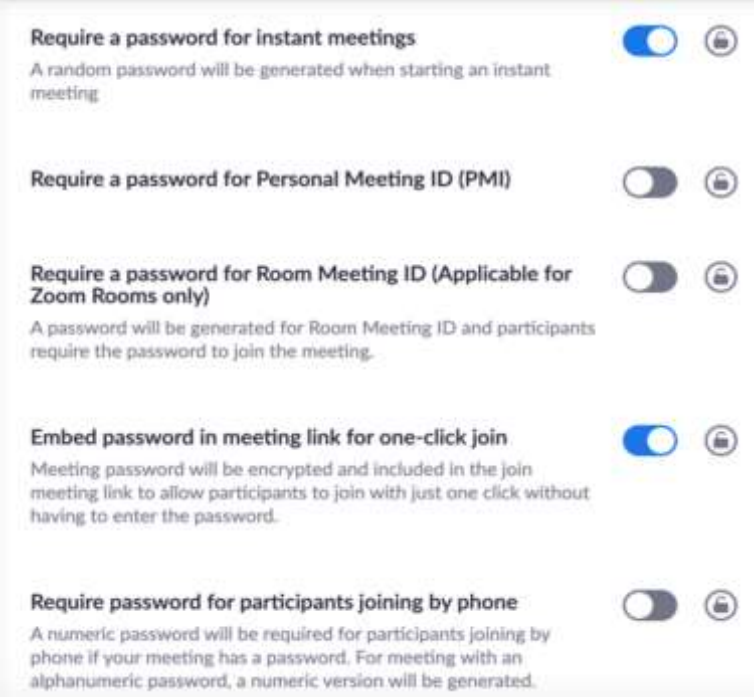
Zoom's advice on securing meetings is here. SecKC's Lo said organizations using Zoom should avoid posting the Zoom meeting links on social media, and always require a meeting password when possible.

"This should be enabled by default as a new customer or a trial user," he said. "Legacy organizations will need to check their administration settings to make sure this is enabled.

You can also enable 'Embed password in meeting link for one-click join.' This prevents an actor from accessing your meeting without losing the usability of sharing a link to join."

In addition, Zoom users can disable "Allow participants to join the meeting before the host arrives."

"If you have to have this feature enabled at least enable "notify host when participants join the meeting before them," Lo advised. "This will notify you that someone might be using your meeting without your knowledge. If you must keep your meeting unprotected you should enable 'Mask phone number in the participant list.' Using the waiting list feature will prevent unwanted participants from accessing your meeting but it will still expose your meeting details if used without a password."



Some of the security settings available to Zoom users. These and others can be found at https://www.zoom.us/profile/settings/

Source: https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/

7. 80% of all exposed Exchange servers still unpatched for critical flaw

More than 350,000 of all Microsoft Exchange servers currently exposed on the Internet haven't yet been patched against the CVE-2020-0688 post-auth remote code execution vulnerability affecting all supported Microsoft Exchange Server versions.

This security flaw is present in the Exchange Control Panel (ECP) component —on by default— and it allows attackers to take over vulnerable Microsoft Exchange servers using any previously stolen valid email credentials.

Microsoft patched this RCE bug on the February 2020 Patch Tuesday and tagged it with an "Exploitation More Likely" exploitability index assessment, hinting at the vulnerability being an attractive target for attackers.

Cyber-security firm Rapid7, the one behind the Metasploit penetration testing framework, added a new MS Exchange RCE module to the pen-testing tool on March 4, following multiple proof-of-concept exploits having surfaced on GitHub.

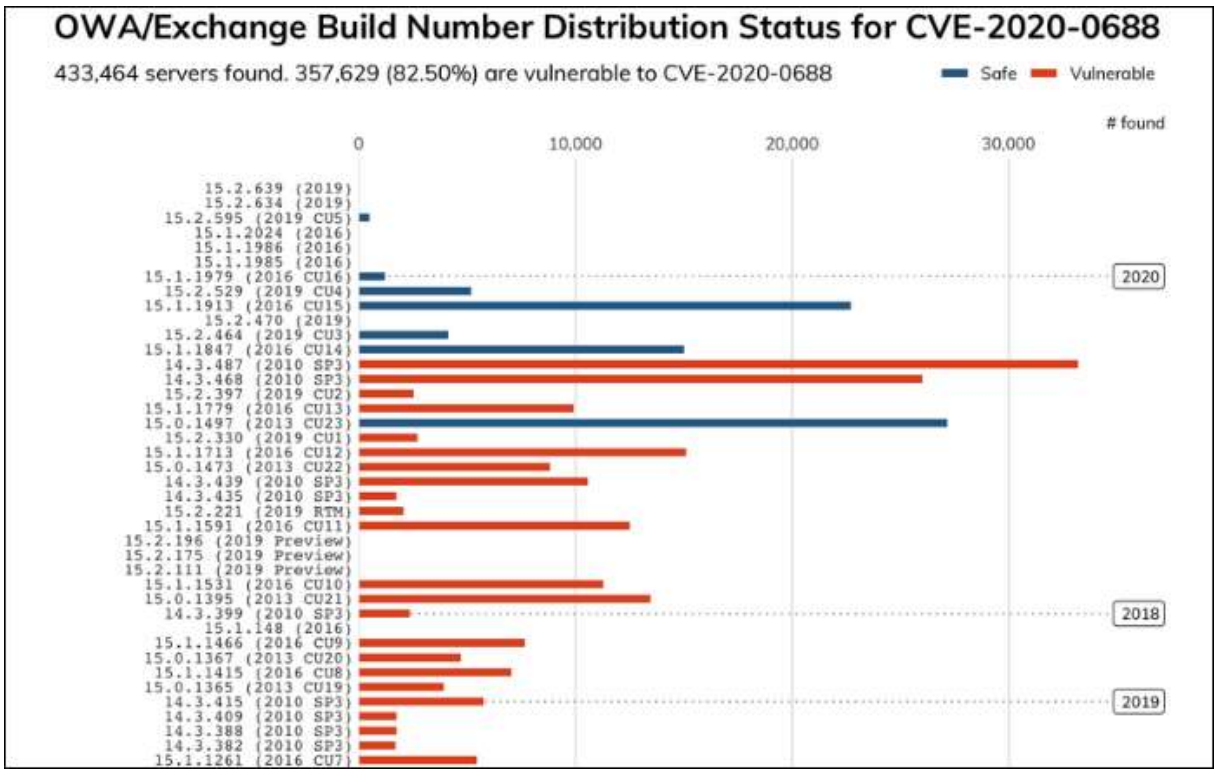
Both the NSA and CISA later issued warnings that urged organizations to patch CVE-2020-0688 as soon as possible seeing that multiple APT groups have already started exploiting it in the wild.

82.5% of all found Exchange servers not yet patched

Starting March 24, Rapid7 used its Project Sonar internet-wide survey tool to discover all publicly-facing Exchange servers on the Internet and the numbers are grim.

As they found, "at least 357,629 (82.5%) of the 433,464 Exchange servers" are still vulnerable to attacks that would exploit the CVE-2020-0688 vulnerability.

To make matters even worse, some of the servers that were tagged by Rapid7 as being safe against attacks might still be vulnerable given that "the related Microsoft update wasn't always updating the build number."



Part of Rapid7's CVE-2020-0688 scan (Rapid7)

Furthermore, "there are over 31,000 Exchange 2010 servers that have not been updated since 2012," as the Rapid7 researchers observed. "There are nearly 800 Exchange 2010 servers that have never been updated."

They also found 10,731 Exchange 2007 servers and more than 166,321 Exchange 2010 ones, with the former already running End of Support (EoS) software that hasn't received any security updates since 2017 and the latter reaching EoS in October 2020.

Rapid7's results line up with a report from Kenna Security from March 13 saying that only 15% of all Exchange servers they found were patched for CVE-2020-0688 until March 11.

Patch against CVE-2020-0688 ASAP

"There are two important efforts that Exchange Administrators and infosec teams need to undertake: verifying deployment of the update and checking for signs of compromise," Rapid7 Labs senior manager Tom Sellers further explained.

User accounts compromised and used in attacks against Exchange servers can be discovered by checking Windows Event and IIS logs for portions of encoded payloads including either the "Invalid viewstate" text or the __VIEWSTATE and __VIEWSTATEGENERATOR string for requests to a path under /ecp.

Since Microsoft says that there are no mitigating factors for this vulnerability, the only choice left, as Rapid7 also advises, is to patch your servers before hackers find them and fully compromise your entire network — unless you're willing to reset all user accounts' passwords to render previously stolen credentials useless.

Download links to security updates for vulnerable Microsoft Exchange Server versions needed to deploy the update and related KB articles are available in the table below:

Product	Article	Download
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 30	4536989	Security Update
Microsoft Exchange Server 2013 Cumulative Update 23	4536988	Security Update
Microsoft Exchange Server 2016 Cumulative Update 14	4536987	Security Update

Microsoft Exchange Server 2016 Cumulative Update 15	4536987	Security Update
Microsoft Exchange Server 2019 Cumulative Update 3	4536987	Security Update
Microsoft Exchange Server 2019 Cumulative Update 4	4536987	Security Update

Source: https://www.bleepingcomputer.com/news/security/80-percent-of-all-exposed-exchange-servers-still-unpatched-for-critical-flaw/

8. Microsoft: No surge in malicious attacks, just more COVID-19 lures

Microsoft says that the volume of malicious attacks hasn't increased but, instead, threat actors have repurposed infrastructure used in previous attacks and rethemed attack campaigns to exploit fears surrounding the COVID-19 pandemic.

"Attackers don't suddenly have more resources they're diverting towards tricking users; instead, they're pivoting their existing infrastructure, like ransomware, phishing, and other malware delivery tools, to include COVID-19 keywords that get us to click," Microsoft 365 Security Corporate Vice President Rob Lefferts said.

"Once we click, they can infiltrate our inboxes, steal our credentials, share more malicious links with coworkers across collaboration tools, and lie in wait to steal information that will give them the biggest payout."

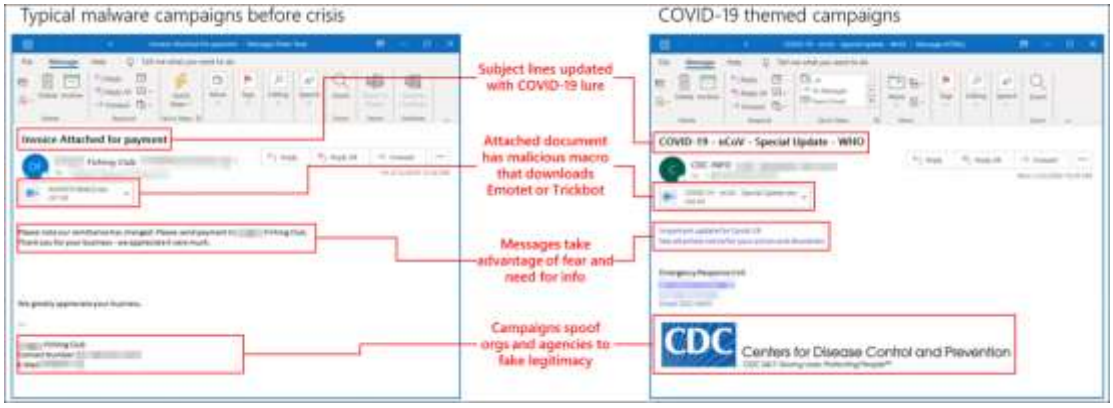
The United States' Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) have also issued a joint alert today about ongoing COVID-19 exploitation.

No surge attacks, just an influx of rethemed attack campaigns

Lefferts explains that Microsoft's data clearly shows that attackers have just re-themed their previous campaign using COVID-19 lures to take advantage of the high-stress levels affecting potential victims during the SARS-CoV-2 outbreak.

This translates into malicious actors switching their bait and not into a surge of attacks as many previously believed after being flooded with COVID-19 themed attacks since the start of the outbreak.

"Our intelligence shows that these attacks are settling into a rhythm that is the normal ebb and flow of the threat environment," Lefferts added.



Malware campaigns adapted to the pandemic (Microsoft)

Based on Microsoft's telemetry, all countries have already been targeted by some type of pandemic-themed attack, with the US, China, and Russia having been the ones threat actors have focused most of their attacks.

Since these attacks have started, Microsoft has already spotted 76 threat variants abusing COVID-19 themed lures, with the Trickbot and Emotet malware families being very active and making use of such lure to exploit the outbreak.

Around 60,000 attacks out of millions of targeted messages feature COVID-19 related malicious attachments or URLs according to Microsoft, based on data collected from thousands of email phishing campaigns every week.

"In a single day, SmartScreen sees and processes more than 18,000 malicious COVID-19-themed URLs and IP addresses."

Impact of COVID-109 themed attacks around the world (Microsoft)

"While that number sounds very large, it's important to note that that is less than two percent of the total volume of threats we actively track and protect against daily, which

reinforces that the overall volume of threats is not increasing but attackers are shifting their techniques to capitalize on fear," Lefferts explains.

Nation-state actors using COVID-19 lures in attacks targeting healthcare have also been spotted by Microsoft security researchers since the start of the pandemic.

Microsoft is sending notifications to dozens of hospitals affected by such attacks and about vulnerable exposed VPN devices and gateways on their networks.

Redmond shares news and guidance related to the pandemic on the company's COVID-19 response page.

CISA and NCSC joint alert on COVID-19 exploitation

Both cybercriminal and advanced persistent threat (APT) groups are actively exploiting the COVID-19 global pandemic in attacks targeting individuals, small and medium enterprises, as well as government agencies and large organizations according to CISA and NCSC.

Furthermore, "both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors," the alert says.

"At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations."

Threats observed so far by CISA, NCSC, and the security industry at large include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure,
- Malware distribution, using coronavirus- or COVID-19- themed lures,
- Registration of new domain names containing wording related to coronavirus or COVID-19, and
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

CISA and NCSC in collaboration with industry partners and law enforcement agencies also provide non-exhaustive lists of COVID-19-related IOCs in CSV and STIX formats.

Guidance to mitigate the risk posed by COVID-19 themed attack campaigns to organizations and individuals is available via the following CISA and NCSC resources:

- CISA guidance for defending against COVID-19 cyber scams
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), which provides guidance for executives regarding physical, supply chain, and cybersecurity issues related to COVID-19
- CISA Alert: Enterprise VPN Security
- CISA webpage providing a repository of the agency's COVID-19 guidance

- NCSC guidance to help spot, understand, and deal with suspicious messages and emails
- NCSC phishing guidance for organizations and cyber security professionals
- NCSC guidance on mitigating malware and ransomware attacks
- NCSC guidance on home working
- NCSC guidance on end user device security

Source: https://www.bleepingcomputer.com/news/security/microsoft-no-surge-in-malicious-attacks-just-more-covid-19-lures/

9. Copycat Site Serves Up Raccoon Stealer

Visitors to the fake site expecting antivirus offerings will instead encounter the Fallout exploit kit and a possible malware infection.

Someone is targeting web denizens with a malicious, copycat Malwarebytes website, which serves up the Raccoon information stealer malware to unsuspecting visitors.

According to the security firm itself, the attackers set up the domain "malwarebytes-free[.]com" with a domain registrar in Russia in late March. "We don't expect to hear from either the registrar or hosting provider," Malwarebytes researchers told Threatpost, noting that the website is still active.

"Examining the source code, we can confirm that someone stole the content from our original site but added something extra," according to a posting from the security firm this week. "A JavaScript snippet checks which kind of browser you are running, and if it happens to be Internet Explorer, you are redirected to a malicious URL belonging to the Fallout exploit kit."

Further, the fake Malwarebytes site is being used in a malvertising campaign via the PopCash ad network, researchers added. Fake Malwarebytes ads served up by the PopCash network on adult websites take visitors to the watering-hole site. The firm said that it contacted PopCash to report the malicious advertisements.

Whether they arrive via organic means or via an ad, once visitors hit the site, the Fallout exploit kit (EK) is used to infect vulnerable machines with the Raccoon data-harvesting malware. Raccoon scours systems for credit card information, cryptocurrency wallets, passwords, emails, cookies, system information and data from popular browsers (including saved credit-card info, URLs, usernames and passwords), and then sends that data back to its operator.

The fake site. Click to enlarge.

Raccoon is a relatively new malware that is under active development by the hackers behind it, according to a previous analysis from Cofense. It's sold on underground forums as a malware-as-a-service offering in both Russian and English, and includes around-the-clock customer support.

First spotted in April of 2019, Raccoon has been leveraged in several different campaigns since then. Cofense for instance saw a campaign in November where scurried past Microsoft and Symantec anti-spam messaging gateways, by using .IMG files hosted on a hacker-controlled Dropbox account.

According to additional research, the malware had infected hundreds of thousands of Windows systems as of last October.

Interestingly, the Malwarebytes analysts also found that the operators of the fake-site campaign appear to have tried similar tactics with other security firms – notably Cloudflare. That effort used a similar copycat site that was disseminated via malvertising.

"We believe this may be the same threat actor already involved in ongoing adult malvertising campaigns and using the Fallout exploit kit," researchers at Malwarebytes told Threatpost. "The attacks are not sophisticated but the spread among various ad platforms is fairly wide. Typically we see malvertising via one or two ad networks simultaneously, but this threat actor has diversified his traffic leads."

Malwarebytes researchers believe that the targeting of security firms could be a deliberate tactic meant as payback for revealing malvertising activity.

"The few malvertising campaigns that remain are often found on second- and third-tier adult sites, leading to the Fallout or RIG exploit kits, as a majority of threat actors have moved on to other distribution vectors," Malwarebytes said in its post. "However, we believe this faux Malwarebytes malvertising campaign could be payback for our continued work with ad networks to track, report, and dismantle such attacks."

Users can protect themselves by keeping their systems fully patched, and by double-checking the identity of any website before clicking on an ad or a link.

Source: https://threatpost.com/malwarebytes-copycat-site-raccoon-stealer/154638/

10. Travelex Pays $2.3M in Bitcoin to Hackers

The payout stems from a system-wide attack that knocked global networks offline on New Year's Eve and reflects a shift in thinking about ransom payouts

Travelex has paid out $2.3 million in Bitcoin to hackers to regain access to its global network after a malware attack at the new year knocked the global currency exchange offline and crippled its business during the month of January.

The move—reported by the Wall Street Journal—may seem counterintuitive, as experts in the past have typically recommended that companies refrain from paying threat actors ransom when such scenarios occur.

However, this mindset has been shifting as attacks become more and more sophisticated and paying ransoms to hackers has less of a detrimental financial effect on a business than continuing to be locked out of systems.

Travelex said in this case it was experts who advised the company pay those responsible for the New Year's Eve attack, which forced the company to shut down its online services and its mobile app. The attack left retail locations to carry out tasks manually and many customers stranded without travel money, while global banking partners also were left adrift with no way to buy or sell foreign currency.

Image courtesy of Travelex

Travelex is a ubiquitous fixture at airports, providing foreign-exchange services in 70 countries across more than 1,200 retail branches. The attack resulted in Travelex websites in at least 20 countries going offline, which hamstrung the company's business as well as caused major problems for banking partners like Barclays, First Direct, HSBC, Sainsbury's Bank, Tesco and Virgin Money.

Travelex has kept partners and regulators apprised of the situation since the attack, which was blamed on a Sodinokibi ransomware strain. The criminals demanded a six-figure payout in return for the decryption key and directed the company to a payment website hosted in Colorado, Travelex revealed about a week after the attack.

A recent report found that while payouts like the one Travelex made are not always made public, the majority of companies these days that are hit with ransomware attacks end up paying the hackers to spare themselves the hassle and financial penalty of the damage—financial and otherwise–having their networks shut down can cause.

The "2020 Cyberthreat Defense Report" from security firm PerimeterX found that 62 percent of the 1,200 IT security decision makers and practitioners who responded to the survey said their networks had been compromised by ransomware, with most of those paying the ransom in the end to free networks from the hands of hackers.

A report last year from Forrester Research also suggested that paying a ransom could be a good business practice alongside other efforts recovery efforts, as it's typically

impossible to completely recover data and systems even in an organization's best-case scenario of having good back-ups.

"Forrester's guidance is not a recommendation of whether or not to pay a ransom but to recognize paying the ransom as a valid recovery path that should be explored in parallel with other recovery efforts to ensure that you're making the best decision for your organization," Forrester Principal Analyst Josh Zelonis wrote in the report.

Organizations are clearly beginning to take this advice, especially those that don't have a raft of security or technical support to recover systems once they've been compromised. Local governments in particular are vulnerable to more financial debt to try to recover systems if they don't pay ransoms than if they do, researchers said.

A city in Florida last June paid $600,000 to hackers to recover data after a ransomware attack, a move criticized by security experts. However, the city of Baltimore experienced a highly publicized ransomware attack last year with a financial impact estimated at $18.2 million versus the $76,000 of bitcoin the hacker demanded, making the decision not to pay "shortsighted," Zelonis noted in his report.

Indeed, as the cost of not paying ransom continues to become higher than just giving in to hackers' demands, it's likely going forward that high-profile ransomware payouts like the one Travelex made will happen more often.

Source: https://threatpost.com/travelex-pays-2-3m-in-bitcoin-to-hackers-who-hijacked-network-in-january/154666/

11. Microsoft April 2020 Patch Tuesday fixes 4 zero-days, 15 critical flaws

With the release of the April 2020 security updates, Microsoft has released fixes for 113 vulnerabilities in Microsoft products. Of these vulnerabilities, 15 are classified as Critical, 93 as Important, 3 as Moderate, and 2 as Low.

Of particular interest, Microsoft patched three zero-day vulnerabilities, with two of them being seen actively exploited in attacks.

Users should install these security updates as soon as possible to protect Windows from known security risks.

Zero-day vulnerabilities fixed in April 2020

Microsoft has stated that two zero-day vulnerabilities have been publicly disclosed and two have been known to be exploited in the wild.

The publicly released vulnerabilities are:

- CVE-2020-0935 - OneDrive for Windows Elevation of Privilege Vulnerability
- CVE-2020-1020 - Adobe Font Manager Library Remote Code Execution Vulnerability

The publicly exploited vulnerabilities are:

- CVE-2020-0938 - Adobe Font Manager Library Remote Code Execution Vulnerability
- CVE-2020-1020 - Adobe Font Manager Library Remote Code Execution Vulnerability

Patch released for Adobe Font Manager zero-day vulnerabilities

The two zero-day remote code execution vulnerabilities in the Windows Adobe Font Manager Library were previously announced by Microsoft as they were seen being exploited in limited attacks.

These vulnerabilities are known as the CVE-2020-0938 and CVE-2020-1020 "Adobe Font Manager Library Remote Code Execution Vulnerability" and has the following description:

> A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.
>
> For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
>
> There are multiple ways an attacker could exploit the vulnerability, such as convincing a user to open a specially crafted document or viewing it in the Windows Preview pane.

Previously, various workarounds were released, such as disabling preview panes, various services, and registry modifications to reduce the security risks or block attacks.

With this security update installed, these workarounds are no longer necessary, and users who have applied them should undo them as they are no longer needed.

The April 2020 Patch Tuesday Security Updates

Below is the full list of resolved vulnerabilities and released advisories in the April 2020 Patch Tuesday updates. To access the full description of each vulnerability and the systems that it affects, you can view **the full report here**.

Update 4/14/20: Microsoft made a correction to CVE-2020-0968 and changed it to not being exploited. So only three zero-days this Patch Tuesday.

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2020-patch-tuesday-fixes-4-zero-days-15-critical-flaws/

12. GitHub accounts stolen in ongoing phishing attacks

GitHub users are currently being targeted by a phishing campaign specifically designed to collect and steal their credentials via landing pages mimicking GitHub's login page.

Besides taking over their accounts, the attackers are also immediately downloading the contents of private repositories, including but not limited to "those owned by organization accounts and other collaborators."

"If the attacker successfully steals GitHub user account credentials, they may quickly create GitHub personal access tokens or authorize OAuth applications on the account in order to preserve access in the event that the user changes their password," GitHub's Security Incident Response Team (SIRT) says.

GitHub's SIRT published information on this ongoing phishing campaign dubbed Sawfish to increase awareness and allow users that might be targeted to protect their accounts and repositories.

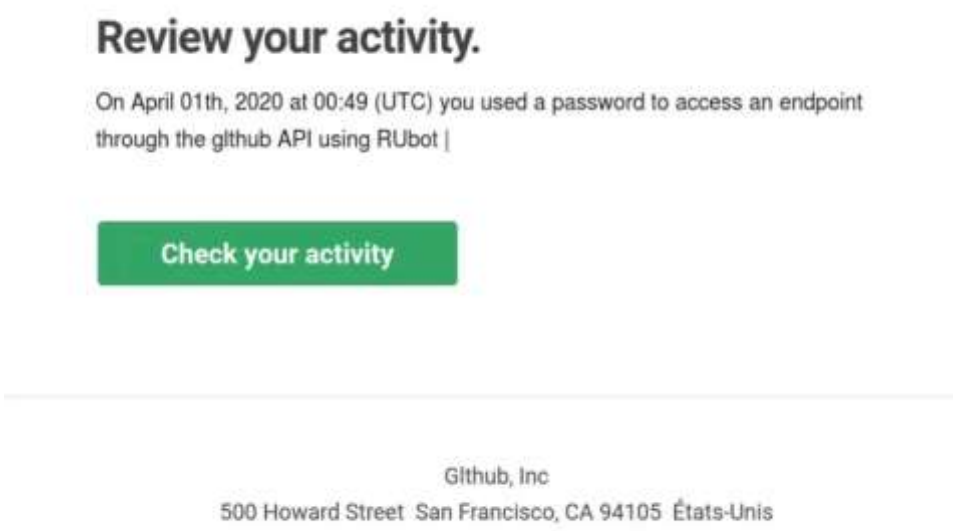
Phishing attack targets active GitHub accounts

The phishing emails use various lures to trick targets into clicking the malicious link embedded in the messages: some say that unauthorized activity was detected, while others mention repository or settings changes to the targeted user's account.

Users who get tricked and click to check their account's activity are then redirected to a fake GitHub login page that collects their credentials and sends them to attacker-controlled servers.

The phishing landing page will also exfiltrate the victims' 2FA codes in real-time if they're using a time-based one-time password (TOTP) mobile app, making it possible for the attackers behind this campaign "to break into accounts protected by TOTP-based two-factor authentication."

However, "[a]ccounts protected by hardware security keys are not vulnerable to this attack," the Git repository hosting service's SIRT explains.



Phishing email sample (GitHub)

This ongoing phishing campaign targets currently-active GitHub users working for tech companies from multiple countries using email addresses obtained from public commits.

The phishing emails are delivered from legitimate domains, either using previously-compromised email servers or with the help of stolen API credentials for legitimate bulk email service providers.

Attackers behind this campaign also make use of URL-shortening services designed to hide the landing pages' URLs and have also been observed while chaining multiple URL-shortening services for enhanced obfuscation.

To further help them make the malicious links used in the attack look less suspicious, the threat actors also use PHP-based redirectors on compromised sites.

How to defend against these phishing attacks

Users that haven't configured two-factor authentication for their GitHub accounts using a security key are advised by the Microsoft-owned company to:

- Reset their password immediately.
- Reset their two-factor recovery codes immediately.

- Review their personal access tokens.
- Take additional steps to review and secure their accounts.

"In order to prevent phishing attacks (which collect two-factor codes) from succeeding, consider using hardware security keys or WebAuthn two-factor authentication," GitHub also advises users. "Also consider using a browser-integrated password manager."

"These provide a degree of phishing protection by auto-filling or otherwise recognizing only a legitimate domain for which you have previously saved a password.

"If your password manager doesn't recognize the website you're visiting, it might be a phishing site."

One year ago, attackers were using GitHub's platform to host their phishing kits by abusing the service's free repositories to deliver them via github.io pages.

Source: https://www.bleepingcomputer.com/news/security/github-accounts-stolen-in-ongoing-phishing-attacks/

13. Business Flexibility Through Digital Trust and Risk Management

I grew up watching professional football back in the 70s, when defenses were so good they had their own nicknames. The Pittsburgh Steelers had the "Steel Curtain," the Miami Dolphins had the "No-Name Defense" and the Dallas Cowboys had the "Doomsday Defense." The Cowboys' defense was based on a newfangled concept called the flex defense, which their coach, Tom Landry, introduced in 1964 and the team perfected over the next decade.

The flex defense used gap assignments to define player's roles and relied on reading "keys" to determine what the offense was likely going to do. Players trusted each other to mind their gap, and each learned to read and react to the keys that would predict what was to come and were trained to continually read changes and alter the plan of attack as the play unfolded.

The Role of Security in Business Flexibility

Flexibility in business, like business continuity planning, is a core competency. Much like the Cowboys' flex defense, information security teams can amplify this competency by creating a trusted foundation that generates goodwill and engenders confidence, and by continually sharpening their risk management skills so the business can experiment, adapt to customers' evolving needs and remain secure.

The cumulative effect of the data breaches that started to become commonplace at the beginning of the last decade has taken a toll on both the cybersecurity community's confidence in our own abilities to detect and prevent breaches and data loss and also on the consumer's overall belief that their private data will remain private. At the same time, because trust matters greatly to consumers, it can also yield extremely positive results.

To leverage the value of trust as a source of goodwill, companies need to adopt a digital trust mindset, invest in system hygiene and commit to a high-performing security function that can provide flexibility in business and protect the products and services that their customers rely on.

Engender Digital Trust in Your Organization

Digital trust can be defined as a measure of confidence in an organization's ability to protect and secure data, as well as safeguard the privacy of individuals. By aligning privacy controls and privileges around the customer's data experience, you can leverage your investment in system hygiene to go beyond business continuity and create customer goodwill and peace of mind for the organization. Your customers will have confidence that their data is secure and their privacy is protected, and you will have confidence in your ability to protect their data and minimize the impact of cyber intrusions.

Achieving this requires diligence around system hygiene and an emphasis on identity, authentication, and the granularity of privileges for your workforce and customers. This, in turn, can give you confidence about the activity on your network and make it easier to provide the privacy controls required by regulations like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR).

In addition to developing trust by emphasizing data security at the systems level, the flexible security organization needs to have a high-caliber team that is continually investing in skills development. To return to the flex defense analogy, Dallas was known for drafting fast, strong and smart players, and for training constantly on the flex. So too should the security function place a high value on learning agility and keeping team members in constant learning mode. While there is no getting around the time investment required for always being in learning mode, the resulting combination of trustworthy systems and finely honed security skills is worth the investment.

Work Backward to Manage Cyber Risk

Finally, as I discussed in an article about diversity of thought in security, we often don't have enough security personnel to meet all of our security requirements and, therefore, may not be able to promise the needed flexibility in business for our internal customers. We can't just embed personnel; we need to teach security thinking.

I like an effective and straightforward risk management technique that can be taught through example and used in a wide variety of scenarios: The idea is to visualize the ideal

state of control or "security" for a product, service, function or process that we're implementing — that ideal state would be when security is fully implemented and would represent the fully risk-mitigated state.

While we're getting to that ideal state, our task is to design and implement compensating and detective controls. Depending on the background of the members of the team, rather than talking about compensating controls, we might ask how we can protect this process in the meantime. Likewise, instead of discussing detective controls, we might challenge the team to come up with ways of determining whether there is a problem we need to respond to.

This technique fosters brainstorming and teamwork by acknowledging an ideal state in the future while keeping the focus on the here and now. It can be applied anywhere, and it can be employed repeatedly as circumstances change.

Foster Innovation and Adaptability Throughout Your Business

By establishing digital trust, we are buying goodwill. By investing in a well-trained security team, we are creating a legion of teachers that can take a simple risk management technique and deliver flexibility in business, so we can innovate and give customers the products they need and want.

So how good was the flex defense? If the New England Patriots, the football team that has dominated the whole 21st century, and possibly the last true American sports dynasty, have one more winning season before experiencing a tie or losing season, it'll be their 20th in a row and will just tie the Dallas record from 1966 to 1985. The flex defense and its offshoots and imitations were so effective at allowing defenses to dominate football that the only real solution was to alter the playbook to open up the game. Flexibility matters.

Source: http://feedproxy.google.com/~r/SecurityIntelligence/~3/Ne5k3tMO8Dc/

14. Microsoft Issues Out-Of-Band Security Update For Office, Paint 3D

Microsoft has released an out-of-band security update for Microsoft Office, Office 365 ProPlus and Paint 3D. The applications are affected by multiple Autodesk vulnerabilities that, if exploited, could enable remote code execution.

The flaws, all rated "important" in severity, are tied to six CVEs stemming from Autodesk's library for FBX, a popular file format format that supports 3D models. This library is integrated into certain Microsoft applications.

"Remote code execution vulnerabilities exist in Microsoft products that utilize the FBX library when processing specially crafted 3D content," according to Microsoft's Tuesday advisory.

Affected products include Office 365 ProPlus (for 32- and 64-bit systems), which is Microsoft's subscription that comes with premium apps like Word, Excel, PowerPoint, Outlook and Teams; as well as Paint 3D (formerly known as Microsoft Paint), Microsoft's 3D modeling and printing application. Microsoft Office 2016 (Click-to-Run for 32- and 64-bit editions) and Microsoft Office 2019 (for 32- and 64-bit editions) are also impacted.

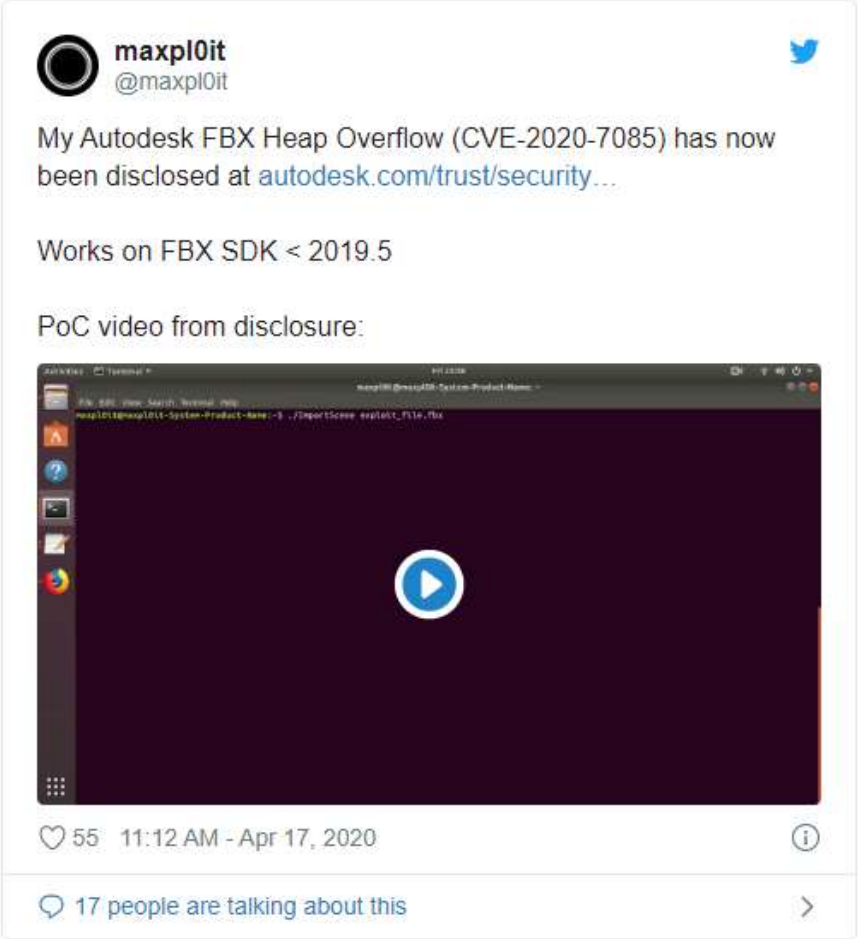
The Flaws

The Autodesk flaws all stem from FBX's software development kit (SDK). They include a high-severity buffer overflow flaw (CVE-2020-7080) that could enable an attacker to run arbitrary code, a type confusion vulnerability (CVE-2020-7081) that could allow an attacker to read/write out-of-bounds memory location or run arbitrary code on the system or lead to denial-of-service (DoS), and a use-after-free glitch (CVE-2020-7082) that could cause an application to reference a memory location controlled by an unauthorized third party – allowing them to run arbitrary code on the system.

Other flaws include an integer overflow vulnerability (CVE-2020-7083) that could be abused to cause the application to crash (leading to DoS), and a Null Pointer Dereference vulnerability (CVE-2020-7084) that could enable a DoS attack.

Finally, a high-severity heap overflow flaw in vulnerable FBX parsers (CVE-2020-7085) can be abused to obtain a limited code execution by altering certain values in a FBX file, causing the application to run arbitrary code on the system.

The latter flaw was reported by F-Secure security researcher Max Van Amerongen, who demonstrated his proof-of-concept (PoC) exploit for the flaw on Twitter.



Real Life Attack

In a real life scenario, an attacker would need to send a specially crafted file (containing 3D content) to a user and convince them to open it in order to exploit the flaws.

An attacker who successfully exploited these vulnerabilities could gain the same user rights as the local user, according to Microsoft.

"Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights," it said.

The security updates addresses these vulnerabilities by correcting the way 3D content is handled by Microsoft software.

The patches were out-of-band, meaning they were outside of Microsoft's regularly scheduled Patch Tuesday updates. For its April 2020 Patch Tuesday updates, Microsoft disclosed 113 vulnerabilities – including 19 rated as critical, and 94 rated as important, and three being exploited in the wild.

Source: *https://threatpost.com/microsoft-issues-out-of-band-security-update-for-office-paint-3d/155016/*

15. Social Engineering Based on Stimulus Bill and COVID-19 Financial Compensation Expected to Grow

Given the community interest and media coverage surrounding the economic stimulus bill currently being considered by the United States House of Representatives, we anticipate attackers will increasingly leverage lures tailored to the new stimulus bill and related recovery efforts such as stimulus checks, unemployment compensation and small business loans. Although campaigns employing themes relevant to these matters are only beginning to be adopted by threat actors, we expect future campaigns—primarily those perpetrated by financially motivated threat actors—to incorporate these themes in proportion to the media's coverage of these topics.

Threat actors with varying motivations are actively exploiting the current pandemic and public fear of the coronavirus and COVID-19. This is consistent with our expectations; malicious actors are typically quick to adapt their social engineering lures to exploit major flashpoints along with other recurrent events (e.g. holidays, Olympics). Security researchers at FireEye and in the broader community have already begun to identify and report on COVID-19 themed campaigns with grant, payment, or economic recovered themed emails and attachments.

Example Malware Distribution Campaign

On March 18, individuals at corporations across a broad set of industries and geographies received emails with the subject line "COVID-19 Payment" intended to distribute the SILENTNIGHT banking malware (also referred to by others as Zloader). Despite the campaign's broad distribution, a plurality of associated messages were sent to organizations based in Canada. Interestingly, although the content of these emails was somewhat generic, they were sometimes customized to reference a payment made in currency relevant to the recipient's geography and contextually relevant government officials (Figure 1 and Figure 2). These emails were sent from a large pool of different @gmx.com email addresses and had password protected Microsoft Word document attachments using the file name "COVID 19 Relief.doc" (Figure 3). The emails appear to be auto generated and follow the format <name>.<name><SevenNumberString>@gmx.com. When these documents were opened and macros enabled, they would drop and execute a .JSE script crafted to download and execute an instance of SILENTNIGHT from http://209.141.54[.]161/crypt18.dll.

An analyzed sample of SILENTNIGHT downloaded from this URL had an MD5 hash of 9e616a1757cf1d40689f34d867dd742e, employed the RC4 key 'q23Cud3xsNf3', and was associated with the SILENTNIGHT botnet 'PLSPAM'. This botnet has been seen loading configuration files containing primarily U.S.- and Canada financial institution webinject

targets. Furthermore, this sample was configured to connect to the following controller infrastructure:

- http://marchadvertisingnetwork4[.]com/post.php
- http://marchadvertisingnetwork5[.]com/post.php
- http://marchadvertisingnetwork6[.]com/post.php
- http://marchadvertisingnetwork7[.]com/post.php
- http://marchadvertisingnetwork8[.]com/post.php
- http://marchadvertisingnetwork9[.]com/post.php
- http://marchadvertisingnetwork10[.]com/post.php

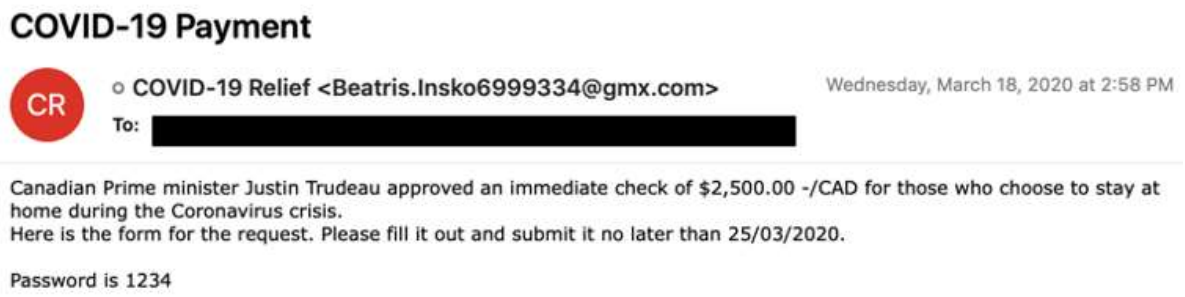


Figure 1: Example lure using CAD

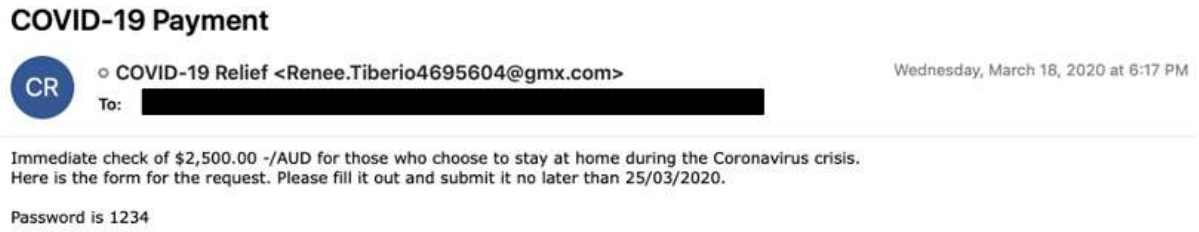


Figure 2: Example lure using AUD

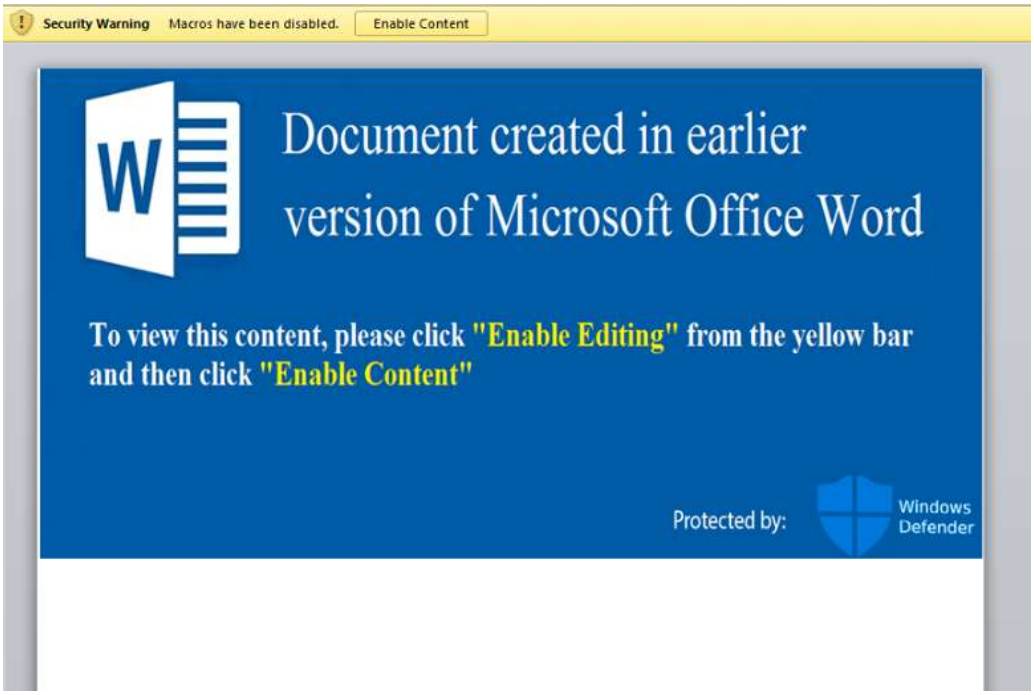


Figure 3: Malicious Word document

Example Phishing Campaign

Individuals at financial services organizations in the United States were sent emails with the subject line "Internal Guidance for Businesses Grant and loans in response to respond to COVID-19" (Figure 4). These emails had OpenDocument Presentation (.ODP) format attachments that, when opened in Microsoft PowerPoint or OpenOffice Impress, display a U.S. Small Business Administration (SBA) themed message (Figure 5) and an in-line link that redirects to an Office 365 phishing kit (Figure 6) hosted at https://tyuy56df-kind-giraffe-ok.mybluemix[.]net/.

Figure 4: Email lure referencing business grants and loans

Figure 5: SBA-themed message

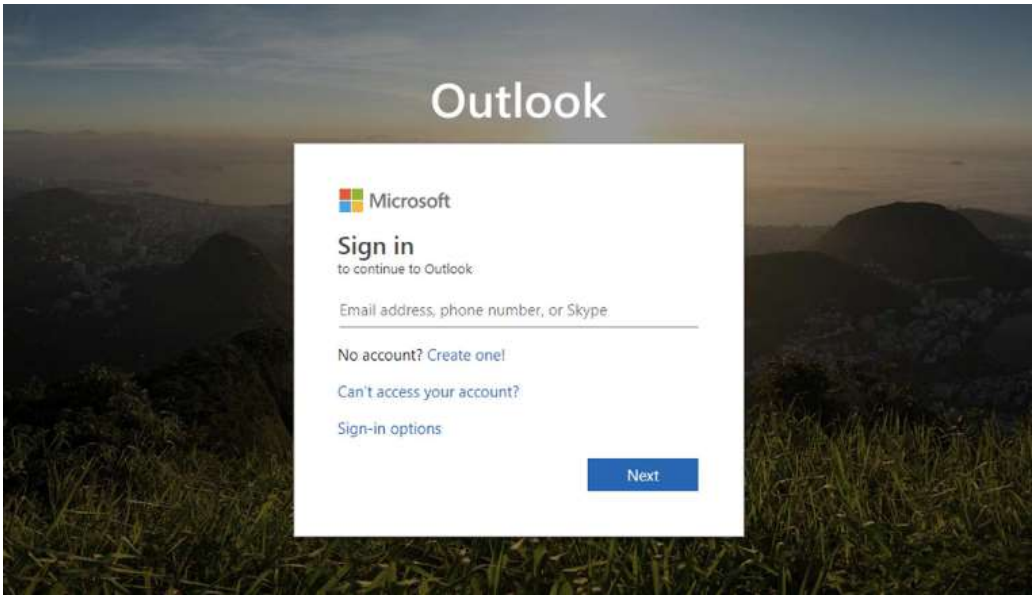


Figure 6: Office 365 phishing page

Implications

Malicious actors have always exploited users' sense of urgency, fear, goodwill and mistrust to enhance their operations. The threat actors exploiting this crisis are not new, they are simply taking advantage of a particularly overtaxed target set that is urgently seeking new information. Users who are aware of this dynamic, and who approach any new information with cautious skepticism will be especially prepared to meet this challenge.

Source: http://www.fireeye.fr/blog/threat-research/2020/03/stimulus-bill-social-engineering-covid-19-financial-compensation-schemes.html

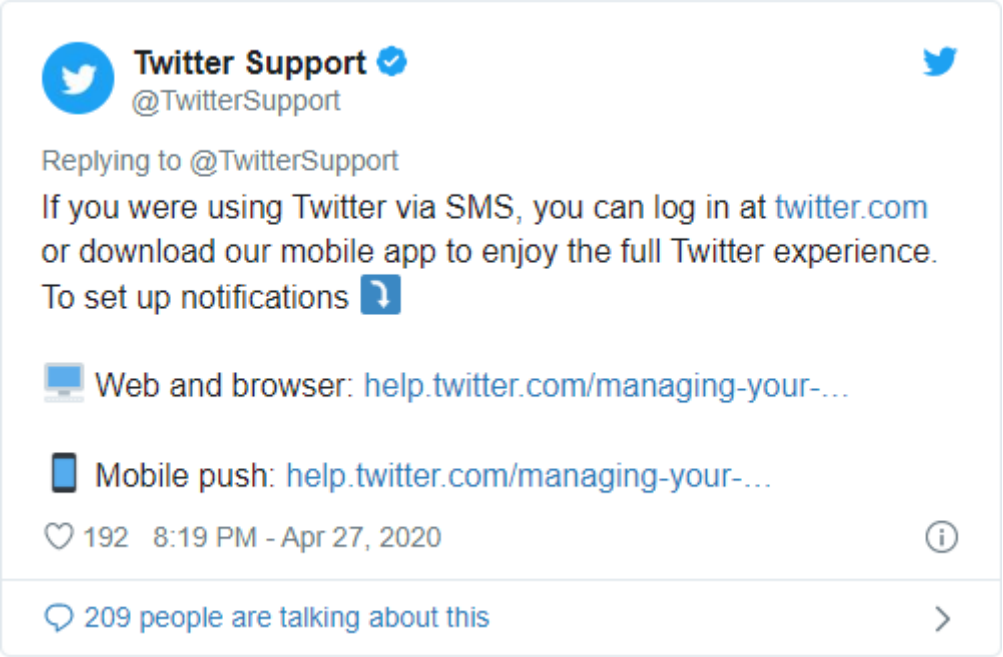
16. Twitter kills SMS-based tweeting in most countries

Twitter announced today that it has turned off the Twitter via SMS service because of security concerns, a service which allowed the social network's users to tweet using text messages since its early beginnings.

"We want to continue to help keep your account safe," the company's support account tweeted earlier today.

"We've seen vulnerabilities with SMS, so we've turned off our Twitter via SMS service, except for a few countries."

However, as the company added, Twitter users will still be able to use "important SMS messages" to log in onto the platform and to manage their accounts.



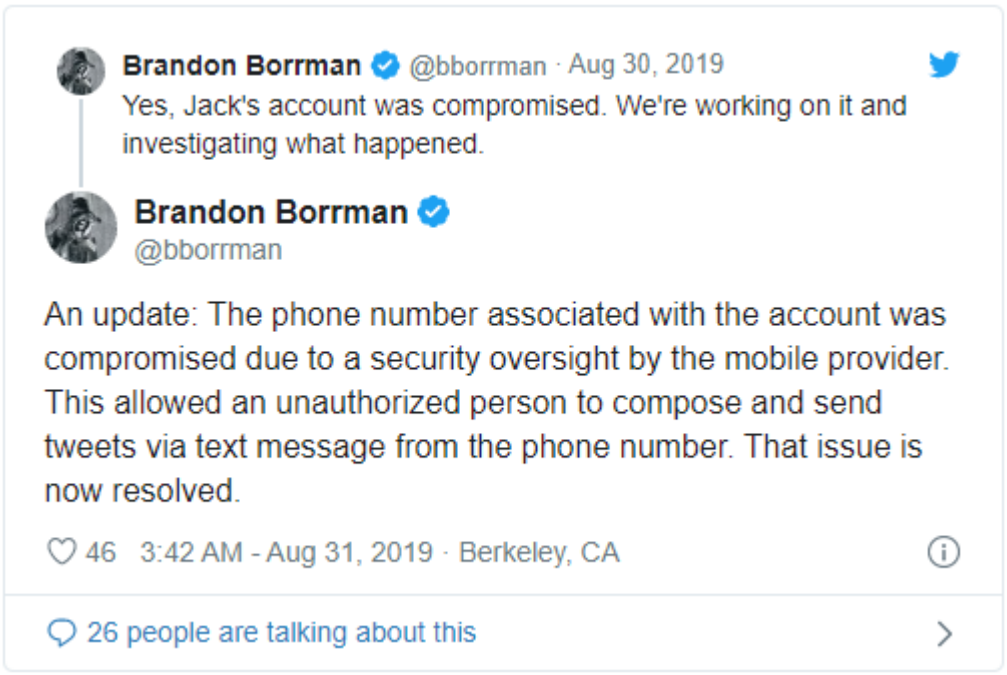
Users who were using Twitter over SMS are advised to transition to the social network's web platform or to the Twitter mobile app "to enjoy the full Twitter experience."

For the time being, Twitter has also decided not to kill SMS-based two-factor authentication (2FA) and password verification.

Twitter previously temporarily turned off the users' ability to tweet via text messages between September 4 and September 5, 2019, to protect their accounts after Jack Dorsey's Twitter account, the company's CEO, got hacked.

"We've now turned this feature back on for a few locations that depend on SMS to Tweet," Twitter said. "It remains turned off for the rest of the world."

As Twitter's Communications team tweeted and Brandon Borrman, Vice President Global Communications at Twitter said at the time, "the phone number associated with the account was compromised due to a security oversight by the mobile provider" which allowed the attackers to compose and send tweets via SMS using Dorsey's phone number.



In February, Twitter discovered and fixed an issue actively exploited by attackers to match specific phone numbers to their corresponding Twitter accounts using a large network of fake accounts.

During October 2019, Twitter also revealed that some users' phone numbers and email addresses provided for account security like 2FA may have been used accidentally for ad targeting.

"No personal data was ever shared externally with our partners or any other third parties," Twitter said at the time. "As of September 17, we have addressed the issue that allowed this to occur and are no longer using phone numbers or email addresses collected for safety or security purposes for advertising."

Source: https://www.bleepingcomputer.com/news/security/twitter-kills-sms-based-tweeting-in-most-countries/

17. Sophisticated Android Spyware Attack Spreads via Google Play

The PhantomLance espionage campaign is targeting specific victims, mainly in Southeast Asia -- and could be the work of the OceanLotus APT.

A sophisticated, ongoing espionage campaign aimed at Android users in Asia is likely the work of the OceanLotus advanced persistent threat (APT) actor, researchers said this week.

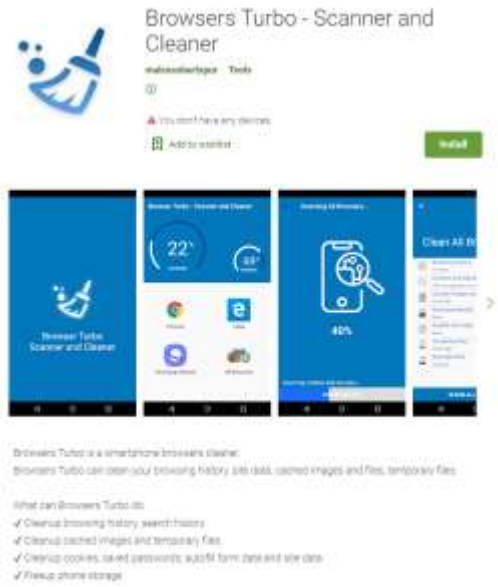
Dubbed PhantomLance by Kaspersky, the campaign is centered around a complex spyware that's distributed via dozens of apps within the Google Play official market, as well as other outlets like the third-party marketplace known as APKpure.

The effort, though first spotted last year, stretches back to at least 2016, according to findings released at the SAS@home virtual security conference on Tuesday.

A Sophisticated Campaign

The spyware is fairly narrow in its focus when it comes to functionality, researchers said. It can gather geolocation data, call logs and contacts, and can monitor SMS activity; the malware can also gather a list of installed applications, as well as device information, such as the model and OS version.

Multiple versions of the malware have been found in various applications since being flagged back in July 2019, albeit all with the same basic tool set. All of the samples uncovered, researchers said, are connected by multiple code similarities. Once a rogue application is installed on a device, it vets the victim's device environment, such as which Android version the person is using and the apps that are installed on the device – and then, the payload is adapted accordingly.



"This way, the actor was able to avoid overloading the application with unnecessary features and at the same time gather the desired information," according to Kaspersky.

In the latest Google Play sample observed by Kaspersky, there is a clear payload; other versions use an interim step that drops an additional executable file.

"Our main theory about the reasons for all these versioning maneuvers is that the attackers are trying to use diverse techniques to achieve their key goal, to bypass the official Google marketplace filters," the firm explained. "And achieve it they did, as even this version passed Google's filters and was uploaded to Google Play Store in 2019."

The latest version also hides its suspicious permission requests; they are requested dynamically and hidden inside the dex executable.

"This seems to be a further attempt at circumventing security filtering," according to Kaspersky. "In addition to that, there is a feature that we have not seen before: if the root privileges are accessible on the device, the malware can use a reflection call to the undocumented API function 'setUidMode' to get permissions it needs without user involvement."

"In order to evade filtering mechanisms employed by marketplaces, the first versions of the application uploaded by the threat actor to marketplaces did not contain any malicious payloads," Kaspersky researchers explained in the analysis. "However, with later updates, applications received both malicious payloads and a code to drop and execute these payloads."

Kaspersky's report follows previous research from BlackBerry, which connected OceanLotus to a trio of fake apps for Android last year. One of those apps supposedly provided support for high-resolution graphics on the phone (e.g. for use in games), while another purported to block ads on a phone, and a third presented itself as a browser and cache cleaner. The apps were distributed through phishing, but also to a wider set of targets via third-party app stores as well as the official Google Play Store.

BlackBerry researchers also dug into how the apps made it into the Google Play Store itself – "finding that OceanLotus went to the trouble establishing an entire fake backstory to give its malicious apps an air of legitimacy," a spokesperson told Threatpost.

In behavior also seen by Kaspersky, the threat actor created a fake developer profile on an associated GitHub account for each app.

"They created modified GitHub repositories that theoretically showed evidence of the developers' code for each app, complete with public facing 'contact us' email addresses to answer any questions that might arise about their 'products,'" according to the BlackBerry research. "They even went to lengths to concoct entire privacy policies for their apps, which few people tend to actually read, but nevertheless was ironic, given that OceanLotus' entire premise was to spy on its targets."

A Targeted Attack

Interestingly, researchers observed that the malware's operators don't seem interested in widescale infection. In fact, according to the firm's telemetry, since 2016, only around 300 infection attempts were observed on Android devices — mainly in India, Vietnam,

Bangladesh and Indonesia. Other infections, however, were found in Algeria, Iran and South Africa. And, several infections were found in Nepal, Myanmar and Malaysia.

"Usually if malware creators manage to upload a malicious app in the legitimate app store, they invest considerable resources into promoting the application to increase the number of installations and thus increase the number of victims," explained the researchers in the writeup. "This wasn't the case with these newly discovered malicious apps. It looked like the operators behind them were not interested in mass spread. For the researchers, this was a hint of targeted APT activity."

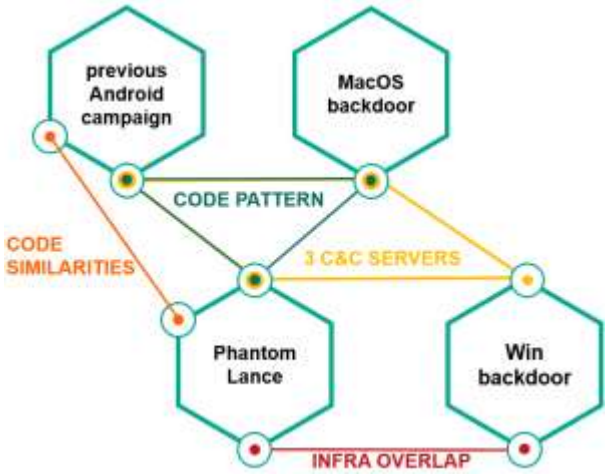
The types of applications that the malware mimics include Flash plugins, cleaners and updaters.

An example of a Vietnam-focused PhantomLance app.

Vietnam in particular saw a large number of attempted attacks; and, some malicious applications used in the campaign were also made exclusively in Vietnamese. These include "Tim quan nhau | Tìm quán nhậu" ("Find each other | Find pubs" in Vietnamese); and "Địa Điểm Nhà Thờ" ("Church Place").

The OceanLotus Connection

Kaspersky researchers determined in their research that the PhantomLance payloads were at least 20 percent similar to those used in an older Android campaign associated with OceanLotus. Also, there were several other overlaps with OceanLotus activity that has been seen targeting Windows and MacOS users. The firm is assessing with "medium confidence" that PhantomLance could be the work of the cyber-espionage group.



Links to prior OceanLotus activity.

OceanLotus is a Vietnam-linked APT that has been in operation since at least 2013, also known as APT32. Its targets are mostly located in Southeast Asia. Recently, from at least January to April, the FireEye Mandiant researchers have seen the group attacking China's Ministry of Emergency Management, as well as the government of Wuhan province, in an apparent bid to steal intelligence regarding the country's COVID-19 response.

Kaspersky reported all discovered PhantomLance samples to the owners of legitimate app stores in which they were found, and Google Play has removed the known apps, but the campaign is ongoing, according to the firm.

"This campaign is an outstanding example of how advanced threat actors are moving further into deeper waters and becoming harder to find," said Alexey Firsh, security researcher at Kaspersky's GReAT division, who delivered a session at the SAS@home virtual summit on the campaign. "PhantomLance has been going on for over five years and the threat actors managed to bypass the app stores' filters several times, using advanced techniques to achieve their goals. We can also see that the use of mobile platforms as a primary infection point is becoming more popular, with more and more actors advancing in this area."

Source: https://threatpost.com/sophisticated-android-spyware-google-play/155202/

18. Leveraging Secure SD-WAN to Meet Security and Network Reqs

Evolving beyond the traditional WAN architecture with SD-WAN enables organizations to move past MPLS services and open their networks to direct internet access. SD-WAN solutions not only allow organizations to reap the rewards of Software-as-a-Service (SaaS) applications, applications in public clouds, and unified communications, but it ultimately delivers a lower total cost of ownership (TCO).

With Secure SD-WAN, security leaders can meet both business and customer needs to simplify the management and operation of a WAN and deliver multiple real-world business benefits.

Fortinet digitally met with four of Fortinet's Field CISOs – Courtney Radke, Renee Tarun, Joe Robertson, and Alain Sanchez – to discuss the value of Secure SD-WAN in today's evolving threat landscape.

Q: Why are security and networking critical to be considered together and integrated today? Why the urgency?

Courtney - Businesses have been challenged with finding and retaining talent on technology teams, particularly in specialized network and security roles. This global skills gap underlines the capacity and capability proficiencies, which are the two base pillars of 'The Five Constraints of Organizational Proficiency.' These guidelines, adopted by Verizon, are a good way for companies to determine their overall cyber maturity and spell out some of the challenges the businesses encounter when not managed appropriately. One of the biggest, being network and security teams operating independently from each other. When network and security teams are setup in silos, without tight integrations and coordination, it becomes difficult to allocate resources (people, funding, or tools) or prioritize initiatives to reduce risk. This reduces the overall competency of both teams and makes the business more vulnerable.

Renee - Security and networking need to go hand in hand. When building and designing your network, you need to ensure that it is built with security in mind. Otherwise, poorly configured networks increase your risk of exposing your data and systems to a breach. In addition, when doing incident response, you don't always immediately know if the issue is a security problem like a breach or a performance issue like a failing hard drive. Speed is of the essence when doing incident response to minimize damage and outages. Therefore, it is imperative that the security and networking teams have a strong working relationship to troubleshoot these issues together as quickly as possible.

Joe - I have always thought that the split between networking and security was not necessary; it really is just an artifact of the history of IT. For at least the last twenty years, since the real rise of the internet as a tool of mass utilization, the network has been the route for bad actors to find and attack their targets. With rare exceptions, every probe, every threat, every malware, every attack, crosses the network. So, the network is the logical place for cybersecurity, but not just as a gate or a door where you hope to recognize the bad guy as he tries to sneak in. Security and the network should be conceived together, managed together, and work together. No one can afford a network without security these days, and cybersecurity without a network is an oxymoron. As attackers get better and better at what they do and the sophistication of their attacks grows, it is urgent for the organizations that still have silos between the networking and security teams to tear them down and get everyone cross trained and working together.

Alain - Let's remember that SD-WAN is primarily a network concept; it means Software-Defined Wide Area Network. In other words, the routing tables are ruled by a policy that is established and updated elsewhere. Despite the enormous benefits of this feature, you end up executing orders that make sense from a performance standpoint, such as send this traffic to this leased line and that one to this public address, but that can rise significantly your exposure if only network criteria are considered. Hence the imperious necessity to run simultaneously a security stack that supports segmentation criteria, traffic analysis, VPN, IPSec to name a few, and enforces the same security policy across all your company. The moment the network tasks prevail, you're at risk and the security prevails, you reduce performance. From the beginning, Fortinet solved this dilemma by dedicating high performing ASICs to the security stack, enabling sophisticated security tasks to be conducted with marginal loss of performance. This is the exact definition of security-driven networking, the merger of the networking domain with the security domain with no compromise.

Q: What have you heard about, or do you think some CISOs have learned when it comes to SD-WAN in regards to securing remote work?

Renee - Like many people, I think many CISOs and IT leaders weren't necessarily prepared for the major shift to remote working that has occurred over the last few months. That has meant looking at technology that can not only scale to accommodate the entire organization but also how to do securely. As CISOs and IT teams look at SD-WAN solutions, they may find that some solutions don't have the security built in or the basic firewall and VPN solution that is included isn't sufficient enough from a security perspective. This results in not only additional cost to buy add-on solutions, but also creates an additional management burden for the already overworked IT and security staff. Therefore, it is imperative that they look at solutions that have integrated security features such as next-gen firewalls, intrusion prevention, and encryption.

Joe - Of course, SD-WAN and remote teleworking are not the same thing, but there are strong similarities in the thinking that goes into them. Organizations that I have dealt with that had made a conscious decision to implement Secure SD-WAN seem to most often be those that put security at the top of their remote access to-do lists. In many cases, I have seen the Secure SD-WAN project be the driver for the breaking down of silos that we were just talking about. Where the security and networking teams are integrated, remote teleworking is set up from the get-go with security. It isn't left to a later date.

Alain - They certainly have learned but sometimes in a hard way. It's fair to say that remote access architectures were never designed to take on an entire country. Not only business critical applications were accessed from many different places and heterogeneous networks, but also video conferencing, database synchronization, and infrastructure management significantly made the traffic patterns more complex and difficult to predict. We have learned to segment traffic and user privileges in a different way. In this context,

automation is becoming more important than ever. Redesigning the authorization levels or enforcing a more granular segmentation are not easy tasks, but they become nightmares when you do not have the ability to fully automate its enforcement across the entire infrastructure. Integration also enabled to load balance dynamically to the traffic and ensure business continuity at critical times. We have also learned to make quick decisions, interact more directly, and as a result the decision that are emerging now empower the edge more, both from a human and machine perspective. Going forward, organizations will have leaner decision processes and more direct engagement practices. Digital innovation is accelerating.

Q: What do you see as the role around SD-WAN and critical applications?

Courtney - The ability to create application specific policies ensures business critical applications both reach their intended destinations over the most appropriate link while also avoiding impact during network events as businesses continue to shift to commodity broadband to reduce cost. These capabilities are crucial any time but especially right now as on-premise work has switched to remote work. Not only is it important to have specific policies based on applications but the ability for application signatures to be "aware" and update when changes are made, such as IP ranges for Microsoft/Office 365, is equally important.

Renee - Organizations are increasingly moving to cloud services. SD-WAN enables direct cloud access at the remote locations, therefore enabling workers to directly access cloud applications regardless of location without burdening the core network with additional traffic to manage and secure. In addition, SD-WAN improves cloud application performance by prioritizing business critical applications and enabling branches to directly communicate to the Internet.

Joe - To me, one of the biggest benefits of SD-WAN has not gotten as much attention as it should: local breakout. SD-WAN is the perfect tool for giving access to SaaS applications to a workforce distributed across many branch offices. Why backhaul all of that Salesforce or Office 365 traffic back to the data center just to head out to the internet? Giving local branch users high-speed broadband into the SaaS's local access points makes them happy, because they get good response times. It makes the finance folks happy because that's probably a lot cheaper than sending that traffic across an MPLS network. And if the solution has sufficient cybersecurity safeguards to be a Secure SD-WAN, it makes the security team happy. Everybody wins. Well, everyone except the hackers.

Alain – From a user standpoint, ramping-up the cloud and empowering remote sites are the two sides of one coin. CISOs understand the need to embrace security as one, in the cloud, in the core, and at the edge. You cannot afford to lose visibility of the applications just because they're running as SaaS across a multi-cloud architecture and you can't let the cloud provider security policy prevail on your own. Deciding which pattern of

prioritization serves your specific business objectives is your responsibility. In this context, a holistic vision of cybersecurity that enables visibility, but also orchestrates the response across hybrid cloud architectures is paramount. Not only does the integrated fabric allow you to see, secure, and act, but it also preserves your freedom of choice. You can always adopt a new cloud provider, repatriate some components in-house, or accelerate your cloud adoption without affecting your ability to designs a cybersecurity strategy of your own.

Q: Why is SD-WAN such a business driver for SPs around the world?

Courtney - Service providers are in a unique position to utilize SD-WAN as a new business driver and as a business enabler for existing customers. Many service providers were already performing internet/telecom management, hardware procurement, and field service/installation roles for their customers in conjunction with traditional management of network and security operations. This means that many providers were already equipped to enable SD-WAN services for their customers, and those that weren't could quickly pivot or expand services to do so. The addition of SD-WAN to a service provider's portfolio opens up the door for other opportunities aimed at ensuring ease of cloud on-ramp, application assurance, and better business continuity without forcing the customer to choose cost over capability.

Renee - Businesses strive for increased performance, better security, and ease of management when it comes to their architectures. SD-WAN can provide all of that with a lower total cost of ownership. In addition, as remote access and cloud adoption become part of the new norm in how we operate, SD-WAN with built in security becomes an important piece of the infrastructure for network and security teams.

Joe - SD-WAN is a natural business for all types of service providers. A large percentage of customers want their SD-WAN to be run as a managed service. This makes sense for two reasons:

- WANs have traditionally been managed services, whether MPLS, Frame Relay, ATM, X.25, or leased lines, so SD-WAN simply follows in this.
- The complexity of managing connectivity and policies at tens, hundreds, or thousands of sites requires a networking team that many organizations simply do not have. So, the opportunity for SPs is enormous, and many of them have taken advantage of this. There are, however, even further opportunities around SD-WAN for creative service providers. Bundling multiple services is an area where SPs have a great deal of experience and which allows fine-tuned offerings that match customer requirements. Furthermore, SD-WAN is closely tied to digital innovation projects, which require good networking to be effective. Tying into this dynamic, SPs can develop different consulting practices to improve the business outcomes of their customers.

Alain - SD-WAN solves the performance-security dilemma, but traditional SD-WAN needs to evolve to integrate security into the equation natively. As the threat becomes more sophisticated, no service provider can afford to trade security against performance or cost. The new SD-WAN has to be secure and advanced. I also certainly do see these as a foundational opportunity for SPs and other types of partners if they integrate superior security to their SD-WAN capabilities.

Source: http://feedproxy.google.com/~r/fortinet/blogs/~3/iHX1mI2QK-A/leveraging-secure-sd-wan-to-meet-todays-security-and-network-requirements.html

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.