telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

January 2021

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

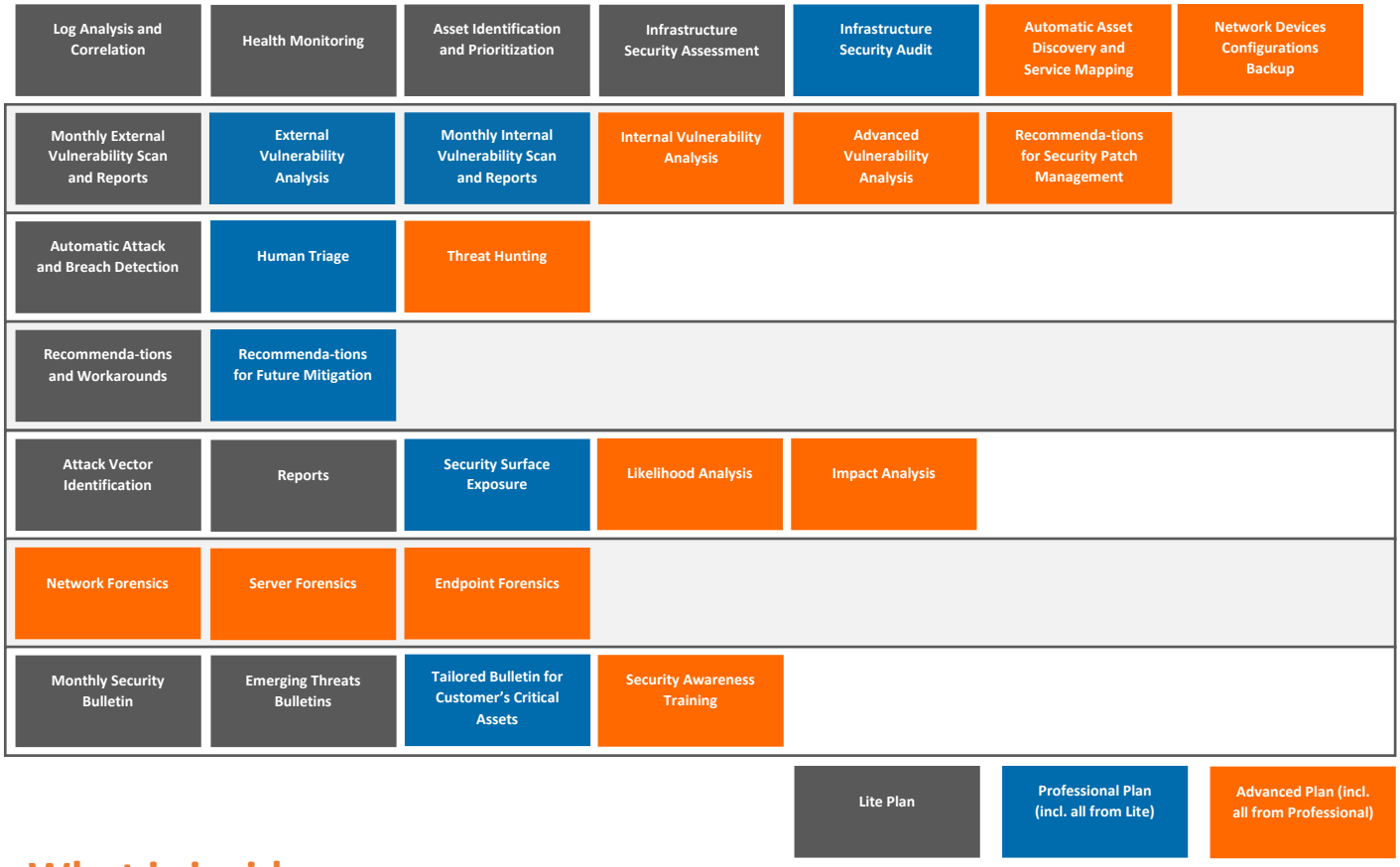
Start to mitigate cyber threats and minimize the risk!

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

1. 2020 Work-for-Home Shift: What We Learned

Threatpost explores 5 big takeaways from 2020 -- and what they mean for 2021.

Goodbye, 2020 — and good riddance, right? Most of us don't want to take too much from this year into the next — but let's make an exception for what we learned about security in the wake of the COVID-19 pandemic. In 2021 after all, more enterprises will permanently downsize their physical spaces and give employees the flexibility to continue working from home.

In an effort to have a safer 2021, Threatpost takes a look at the top five biggest takeaways of the remote-work shift for security teams going forward.

Cybercriminals Are No Dummies

This one seems obvious, but for too long security teams have ignored the danger that comes from offering attackers low-hanging fruit.

As soon as businesses made the transition to work-from-home, cyberattackers got busy capitalizing on it. Researchers saw a near-immediate 131-percent increase in malware infections and about 600 new phishing attacks per day when the pandemic and remote working started in earnest in March. And according to a recent Acronis Cyberthreat Report, 31 percent of global companies reported daily cyberattacks in 2020, mainly targeted at remote workers. Clearly, threat actors know that home networks are typically less secure than corporate infrastructure, and saw an opportunity to ramp up their attacks accordingly.

Credit: Acronis

Since cybercriminals are pretty savvy (and quick-moving), defenders need to be too. The mad scramble to get employees connected from home is over; and now, security practices need to be hardened.

"2021 will be the year of 'working from anywhere' and it is very much a moving target for security and privacy professionals," Yossi Naar, chief visionary officer and co-founder at Cybereason, told Threatpost. "Coupled with a challenging home environment where devices are often shared with family members and the rapid change that occurred, there

was little time to prepare and that fact has been exploited widely by hackers leveraging phishing attacks and known exploits to penetrate and maintain their hold on the remote environment. In 2021, enterprises need to focus on patching the holes in their security defenses as the majority of their workers continue to operate remotely."

Bitdefender researchers noted that home routers and computers will continue to be seen as weak links, so endpoint security will become a bigger focus in 2021 even as attackers evolve and mature.

"Threat actors specialized in hijacking devices will either rent access to other groups seeking distributed command-and-control capabilities or sell them in bulk to underground operators to reuse as proxy nodes to conceal malicious activity," they said.

Collaboration: The New Chink in the Armor

When companies went to a decentralized footprint, they also turned in droves to cloud applications and collaboration services to support the new, borderless, virtual office. In short order, Zoom, Microsoft Teams and Slack became household words, video calls became the default for meetings, and the resources that are connected to, shared and exposed in the cloud were suddenly being used by tens of millions of workers.

A recent Fortune CEO survey showed that 77 percent of CEOs reported that the COVID-19 crisis accelerated their digital transformation plans, while 40 percent are spending more on IT infrastructure and platforms. Security, however, largely remained an afterthought as companies prioritized productivity over vetting the security for these products.

As a result, it was open season on collaboration. Last month for instance, attackers were seen using ads for fake Microsoft Teams updates to deploy backdoors, which used Cobalt Strike to infect companies' networks with malware.

On a related note, cybersecurity will move up the food chain to become a business differentiator for collaboration platforms and cloud apps, researchers said — which will spur innovation in the space.

Going forward, "[security] needs a category disruptor," Nico Popp, chief product officer at Forcepoint, told Threatpost. "The need for a converged, digital, cloud-delivered platform means we'll see the emergence of the 'Zoom of Security' – a high-tech system that 'just works' and is easily accessible for the everyday consumer."

Zero-Trust Has a Moment

As employees were sent home and forced to connect to precious corporate resources using potentially insecure devices, home networks and new cloud apps, the focus on authentication ramped up for security teams. The problem, of course, is that password

hygiene isn't good in the best of times, let alone in an environment of massive change and new platform adoption.

As a result, zero-trust frameworks gained a little buzz in 202o. "Zero trust" means that all users, inside and outside of an organization's enterprise network, are inherently not trusted and must be authenticated and authorized before being able to access apps and data. In order to do this, systems must evaluate the safety of a user's device, verify transport/session information and general identity, and take into account the application being used (is it allowed?) and the data being accessed (how sensitive is it?).

It works, according to those in the trenches. "Our adoption of zero-trust network access technologies and a cloud-based end user security stack made the transition of 95 percent of our workforce from relatively secure corporate networks to relatively unsecure home networks virtually seamless for the end user, but comparatively safe," said Bradley Schaufenbuel, vice president and CISO at Paychex, via email.

Zero-trust frameworks have a reputation for being expensive and complicated, but in 2021, they will no longer be optional for enterprise, according to Jasen Meece, CEO of Cloudentity.

"There's no doubt that COVID-19 and the shift to remote work have accelerated zero-trust adoption in the enterprise," he told Threatpost. "In 2021 and the following years, implementing a zero-trust approach will become essential to protecting every enterprise, regardless of industry. Roughly one-quarter of all data breaches are caused by human error, with the average cost of $3.92 million for each breach, according to a report from the Ponemon Institute. As a result of this growing issue, the zero-trust model will become the new standard."

A Mobile-Focused Security Policy is a Must

As workers went home, mobile devices became more ascendant, with many of the new go-to collaboration and cloud services offering mobile apps designed to boost productivity and allow multitasking. This resulted in rafts of personal devices suddenly being used to access corporate resources — and true to form, cybercriminals followed the trend lines.

For instance, 2020 saw mobile messaging becoming a growing vector for phishing attacks (often called smishing). In fact, in September, the FTC issued a warning about phishing campaigns involving text messages with false delivery notices that included a link to validate the delivery.

"Across any chat medium on mobile, phishing attacks seek to trick users into clicking links to expose personal and work credentials, and even download mobile surveillanceware," Chris Hazelton, director of security solutions at Lookout, told Threatpost.

But threat actors are building more advanced phishing campaigns beyond just credential harvesting, according to Hank Schless, senior manager for security solutions at Lookout.

"Through the first 9 months of 2020, almost 80 percent of phishing attempts intended to get the user to install a malicious app on their mobile device," he said. "Threat actors have [also] learned how to socially engineer at scale by creating fake influencer profiles with massive followings that encourage followers to download malicious apps. Personal apps on devices that can access corporate resources pose serious risk to enterprise security posture."

Criminals are also targeting weaknesses in mobile apps. For instance, WhatsApp in February disclosed a vulnerability in its iOS app that was exploited by Pegasus surveillanceware to gather intelligence from targets.

"While there are security vulnerabilities in all operating systems, including iOS and Android, it is less understood that vulnerabilities in mobile apps can be used in attacks," Schless said.

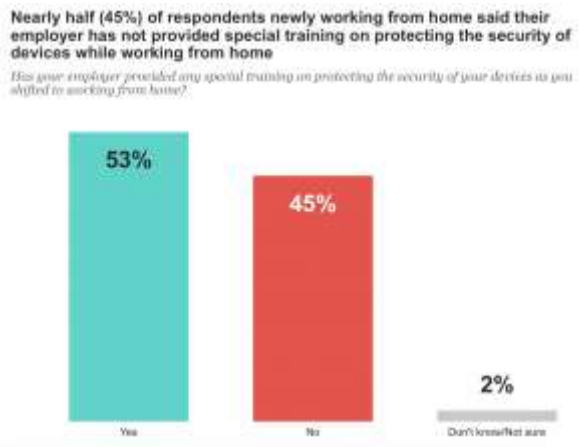
The Rise of New Insider Threats

Remote employees have been thrust into new working environments, with no face-to-face supervision and little to no training for handling new security risks. And, they are also facing more distractions from their home settings, as well as new emotional stresses tied to COVID-19 and less job satisfaction. All of these factors created a ticking time bomb for insider-threat risks in 2020, researchers said.

According to a report from Tessian, insider-caused security incidents already increased by 47 percent since 2018. Worse, security experts warn that organizations aren't ready for this influx of remote work-induced challenges.

"The [work from home] trend due to the COVID-19 pandemic has significantly increased insider threats from employees taking risks with company assets, such as stealing sensitive data for personal use or gain as employers have less visibility to what employees are doing or accessing," Joseph Carson, chief security scientist and advisory chief information security officer at Thycotic, told Threatpost.

Insider threats can stem from either "negligent insiders," or malicious insiders, who intentionally steal data or company secrets. The "negligent insiders" are the bigger threat, according to Proofpoint. They account for 62 percent of insider-threat incidents.



Security training stats. Source: IBM Security.

A survey from IBM Security in June found that more than half surveyed had yet to be given any new security policies on how to securely work from home. Also, more than half surveyed had not been provided with new guidelines on how to handle personal identifiable information (PII) while working from home, despite more than 42 percent newly being required to do so as consumers lean on customer service representatives for a variety of services.

Going forward, awareness of insider threats must take on more importance, researchers noted — especially as the pandemic grinds on and layoffs/workplace dissatisfaction rises.

"One area that organizations need to deal with is the rise of the insider threat, with so many unhappy employees who have been furloughed, or let go, from their jobs," Steve Durbin, managing director of the Information Security Forum, told Threatpost.

"The insider threat is one of the greatest drivers of security risks that organizations face as a malicious insider utilizes credentials to gain access to a given organization's critical assets. Many organizations are challenged to detect internal nefarious acts, often due to limited access controls and the ability to detect unusual activity once someone is already inside their network. The threat from malicious insider activity is an increasing concern, especially for financial institutions, and will continue to be so in 2021."

Overall, the trust that organizations must place on their workers has grown with rapid digital transformation, increasing information risk and changing work environments — and there's no sign of this changing. Taking the lessons of 2020 will be critical for a safer and happier 2021.

Source: https://threatpost.com/2020-work-for-home-shift-learned/162595/

2. Ransomware in 2020: A Banner Year for Extortion

From attacks on the UVM Health Network that delayed chemotherapy appointments, to ones on public schools that delayed students going back to the classroom, ransomware gangs disrupted organizations to inordinate levels in 2020.

Remote learning platforms shut down. Hospital chemotherapy appointments cancelled. Ransomware attacks in 2020 dominated as a top threat vector this past year. Couple that with the COVID-19 pandemic, putting strains on the healthcare sector, and we witnessed ransomware exact a particularly cruel human toll as well. Attacks had an impact on nearly all sectors of the global economy – costing business $20 billion collectively and creating major cybersecurity headaches for others.

Below are the most impactful ransomware stories of 2020.

250K Databases For Sale: MySQL Ransomware Disaster

In December, researchers warned of an active ransomware campaign that plagued MySQL database servers. The ransomware, called PLEASE_READ_ME, not only breached at least 85,000 servers worldwide over the past year – but the attackers behind the malware gave the campaign a double-extortion twist, posting at least 250,000 stolen databases on a website for sale.

Garmin Haggles Over Evil Corp Ransom

In August, GPS and aviation tech specialist Garmin reportedly negotiated with Evil Corp for an decryption key to unlock its files in the wake of a WastedLocker ransomware attack. The attack, which occurred on July 23, knocked out Garmin's fitness-tracker services, customer-support outlets and commercial aviation offerings such as flight-plan filing, account-syncing and database-concierge capabilities.

U.S. Gov Mulls Ransomware Sanctions, Restrictions – To Dismay of Some

ransomware alert

Over the past year, U.S. local and federal governments have increasingly looked at regulatory efforts regarding ransomware payments. In January, New York State mulled banning municipalities from paying ransomware demands in the event of a cyberattack. Meanwhile, in October, the U.S. Department of the Treasury said that companies that facilitate ransomware payments to cyber-actors on behalf of victims may face sanctions for encouraging crime and future ransomware payment demands.

These efforts have generated mixed reviews from the security space: While the feds have always recommended not paying ransoms, in reality, the decision to pay up or to not is an individual choice that has to be made given the context of any given situation, researchers argue.

IoT Chipmaker Reels From $14M Conti Ransom Demand

In November, chip manufacturer Advantech confirmed that it received a ransom note from a Conti ransomware operation on Nov. 26 demanding 750 Bitcoin, which translates into about $14 million, to decrypt compromised files and delete the data they stole. The scammers behind the attack published a list of files from a stolen .zip archive on their leak site. The ransom note claimed that the 3.03GB of data posted on the leak site accounted for about 2 percent of the total amount of data lifted ripped off from Advantech.

Ransomware Election Woes: Georgia Voter Database Hit

With the 2020 November U.S. presidential elections this year, the security space braced for an onslaught of cyberattacks targeting election infrastructure. In October, reports emerged of one of the first breaches of the voting season, on Hall County, Ga. The county's database of voter signatures was impacted in the attack along with other government systems. Although the county said the voting process wasn't impacted by the ransomware attack, the incident served as a warning to other municipalities to lock down their systems, particularly in these last days leading up to the election.

U.S. Pipeline Downed For Two Days

Operational Technology (OT) continued to worry security experts from a ransomware attack perspective in 2020. In February, feds warned that a ransomware attack hit a natural gas compression facility in the U.S.

The attack resulted in a two-day pipeline shutdown as the unnamed victim worked to bring systems back online from backups. The attackers were able penetrate the IT portion of the facility's network, and then move beyond that to eventually infiltrate the control and communication assets on the OT side of the house.

Double Extortion: A Growing Ransomware Threat

Cybercriminals this past year increasingly relied on a ransomware tactic, called "double extortion," where they increasingly inflict more pain on ransomware victims by threatening to leak compromised data or use it in future spam attacks, if ransom demands aren't met.

Double extortion first emerged in late 2019 by Maze operators – but has been rapidly adopted over the past year by various cybercriminals behind the Clop, DoppelPaymer and Sodinokibi ransomware families, who have set up websites as a way to leak data when their ransom demands were not met.

Ransomware: The New "Snow Day"

Forget snow days – ransomware attacks are the new cause of schools being shut down for days in 2020, with a slew of cyberattacks plaguing back-to-school plans. In September, attacks in Hartford, Conn. and Clark County, Nev. forced public schools to postpone the first day of school, while an attack against the Newhall School District in Valencia closed down remote learning for 6,000 elementary school students. Also in September, personal data for students in the Clark County School District (which includes Las Vegas) reportedly turned up on an underground forum, after a ransomware attack linked to the Maze gang.

Ransomware Shake Up TTPs During Strange Times

Overall, COVID-19 reshaped the ransomware landscape and how organizations were affected by ransomware. Cybercriminals, for their part, stepped up their game this past year, with ransomware attacks more than doubling year-over-year (up 109 percent). Many ransomware attacks utilized COVID-19 related lures in spear phishing attacks.

Hospitals Face Disruption, Appointment Reschedules

While ransomware gangs initially pledged not to hit hospitals during the COVID-19 pandemic, these promises turned out to be empty. The UVM Health Network, Universal Health Services and University of California, San Francisco (UCSF) medical school were only a few medical entities to be hit by ransomware attacks in 2020.

The increase in attacks – and the consequential impact not just on patient data, but access to healthcare resources during a pandemic – caused U.S. feds to warn of "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."

Source: https://threatpost.com/ransomware-2020-extortion/162319/

3. Unauthorized Access of FireEye Red Team Tools

Overview

A highly sophisticated state-sponsored adversary stole FireEye Red Team tools. Because we believe that an adversary possesses these tools, and we do not know whether the attacker intends to use the stolen tools themselves or publicly disclose them, FireEye is releasing hundreds of countermeasures with this blog post to enable the broader security community to protect themselves against these tools. We have incorporated the countermeasures in our FireEye products—and shared these countermeasures with partners, government agencies—to significantly limit the ability of the bad actor to exploit the Red Team tools.

You can find a list of the countermeasures on the FireEye GitHub repository found HERE.

Red Team Tools and Techniques

A Red Team is a group of security professionals authorized and organized to mimic a potential adversary's attack or exploitation capabilities against an enterprise's security posture. Our Red Team's objective is to improve enterprise cyber security by demonstrating the impacts of successful attacks and by showing the defenders (i.e., the Blue Team) how to counter them in an operational environment. We have been performing Red Team assessments for customers around the world for over 15 years. In that time, we have built up a set of scripts, tools, scanners, and techniques to help improve our clients' security postures. Unfortunately, these tools were stolen by a highly sophisticated attacker.

The stolen tools range from simple scripts used for automating reconnaissance to entire frameworks that are similar to publicly available technologies such as CobaltStrike and Metasploit. Many of the Red Team tools have already been released to the community and are already distributed in our open-source virtual machine, CommandoVM.

Some of the tools are publicly available tools modified to evade basic security detection mechanisms. Other tools and frameworks were developed in-house for our Red Team.

No Zero-Day Exploits or Unknown Techniques

The Red Team tools stolen by the attacker did not contain zero-day exploits. The tools apply well-known and documented methods that are used by other red teams around the world. Although we do not believe that this theft will greatly advance the attacker's overall capabilities, FireEye is doing everything it can to prevent such a scenario.

It's important to note that FireEye has not seen these tools disseminated or used by any adversaries, and we will continue to monitor for any such activity along with our security partners.

Detections to Help the Community

To empower the community to detect these tools, we are publishing countermeasures to help organizations identify these tools if they appear in the wild. In response to the theft of our Red Team tools, we have released *hundreds* of countermeasures for publicly available technologies like OpenIOC, Yara, Snort, and ClamAV.

A list of the countermeasure is available on the FireEye GitHub repository found here. We are releasing detections and will continue to update the public repository with overlapping countermeasures for host, network, and file-based indicators as we develop new or refine existing detections. In addition, we are publishing a list of CVEs that need to be addressed to limit the effectiveness of the Red Team tools on the GitHub page.

FireEye Products Protect Customers Against These Tools

Teams across FireEye have worked to build the countermeasures to protect our customers and the broader community. We have incorporated these countermeasures into our products and shared these countermeasures with our partners, including the Department of Homeland Security, who have incorporated the countermeasures into their products to provide broad coverage for the community.

More information on the detection signatures available can be found in the GitHub repository.

Source: http://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

4. The SolarWinds cyberattack: The hack, the victims, and what we know

Since the SolarWinds supply chain attack was disclosed last Sunday, there has been a whirlwind of news, technical details, and analysis released about the hack. Because the amount of information that was released in such a short time is definitely overwhelming, we have published this as a roundup of this week's SolarWinds news.

The information is distilled into a format that will hopefully explain the attack, who its victims are, and what we know to this point.

The SolarWinds supply chain attack

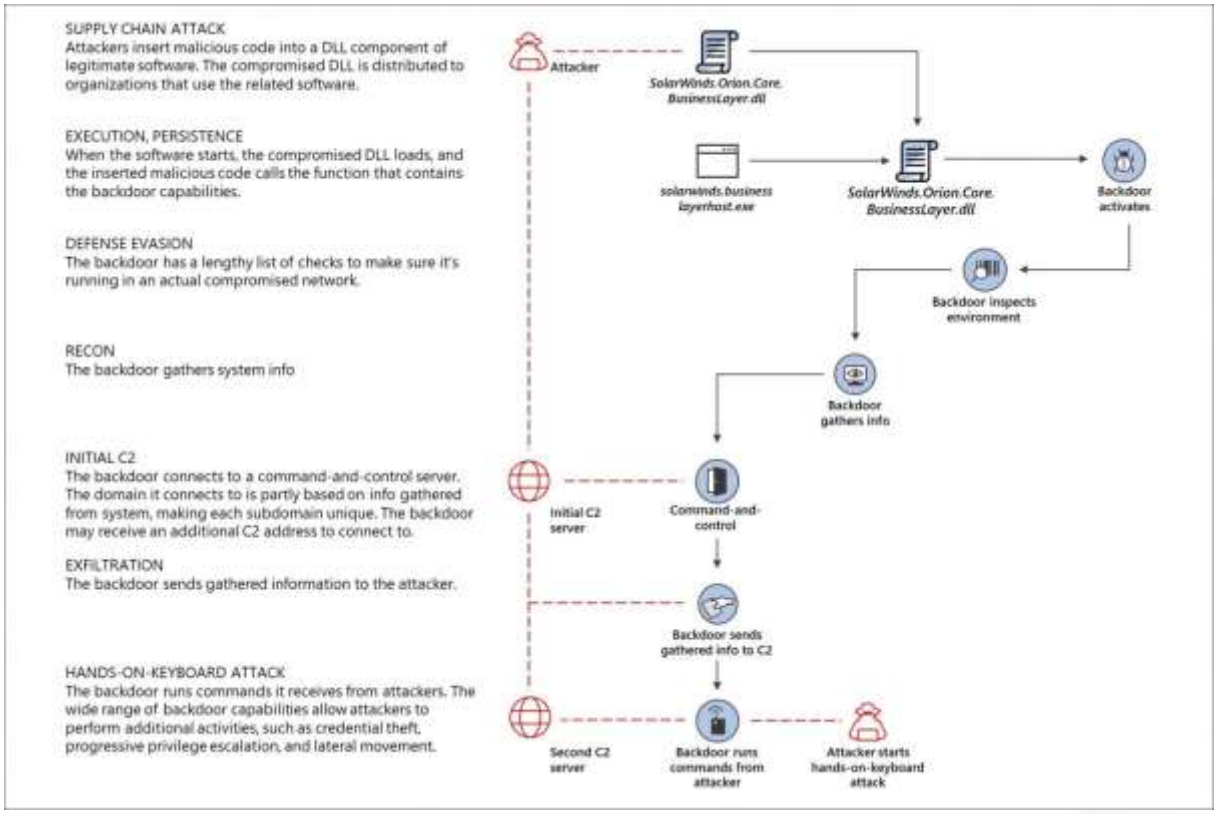
While we learned of SolarWind's attack on December 13th, the first disclosure of its consequence was made on December 8th when leading cybersecurity firm FireEye

revealed that it was hacked by a nation-state APT group. As part of this attack, the threat actors stole Red Team assessment tools that FireEye uses to probe its customers' security.

It was not known how the hackers gained access to FireEye's network until Sunday, December 13th, 2020, when Microsoft, FireEye, SolarWinds, and the U.S. government issued a coordinated report that SolarWinds had been hacked by state-sponsored threat actors believed to be part of the Russian S.V.R.

One of SolarWinds' customers who was breached in this attack is FireEye.

As part of the attack, the threat actors gained access to the SolarWinds Orion build system and added a backdoor to the legitimate **SolarWinds.Orion.Core.BusinessLayer.dll** DLL file. This DLL was then distributed to SolarWinds customers in a supply chain attack via an automatic update platform used to push out new software updates.



SolarWinds supply chain attack
Source: Microsoft

This DLL backdoor is known as SunBurst (FireEye) or Solarigate (Microsoft) and is loaded by the **SolarWinds.BusinessLayerHost.exe** program. Once loaded, it will connect back to the remote command & control server at a subdomain of **avsvmcloud[.]com** to receive "jobs," or tasks, to execute on the infected computer.

The backdoor's command control server's DNS name is created utilizing a domain generation algorithm (DGA) to create an encoded subdomain of **avsvmcloud[.]com**. FireEye states that the subdomain is created by "concatenating a victim userId with a reversible encoding of the victims local machine domain name," and then hashed. For

example, a subdomain used in this attack is '1btcr12b62me0buden60ceudo1uv2f0i.appsync-api.us-east-2[.]avsvmcloud.com.'

It is unknown what tasks were executed, but it could be anything from giving remote access to the threat actors, downloading and installing further malware, or stealing data.

Microsoft published a technical writeup on Friday for those interested in the technical aspects of the SunBurst backdoor.

A report by Kim Zetter released Friday night indicates that the threat actors may have performed a dry run of the distribution method as early as October 2019. During this dry run, the DLL was distributed without the malicious SunBurst backdoor.

After the threat actors began distributing the backdoor in March 2020, researchers believe that the attackers have been silently sitting in some of the compromised networks for months while harvesting information or performing other malicious activity.

Zetter's report stated that FireEye eventually detected they were hacked after the threat actors registered a device to the company's multi-factor authentication (MFA) system using stolen credentials. After the system alerted the employee and the security team of this unknown device, FireEye realized that they had been compromised.

The hackers behind the SolarWinds attack

FireEye is currently tracking the threat actor behind this campaign as UNC2452, while Washington-based cybersecurity firm Volexity has linked this activity to a threat actor it tracks under the Dark Halo moniker.

Volexity says that Dark Halo actors have coordinated malicious campaigns between late 2019 and July 2020, targeting and successfully compromising the same US-based think tank three times in a row.

"In the initial incident, Volexity found multiple tools, backdoors, and malware implants that had allowed the attacker to remain undetected for several years," the company said.

In the second attack, after being cast out from the victim's network, Dark Halo leveraged a newly disclosed Microsoft Exchange server bug that helped them to circumvent Duo multi-factor authentication (MFA) defenses for unauthorized email access via the Outlook Web App (OWA) service.

During the third attack targeting the same think tank, the threat actor used the SolarWinds supply chain attack to deploy the same backdoor Dark Halo used to breach FireEye's networks and several U.S. government agencies.

Unconfirmed media reports have also cited sources linking the attacks to APT29 (aka Cozy Bear), a state-sponsored hacking group associated with the Russian Foreign Intelligence Service (SVR).

Researchers, including FireEye, Microsoft, or Volexity, have not attributed these attacks to APT29 at this time.

The Russian Embassy in the USA reacted [1, 2] to these media reports saying that they were an "unfounded attempt of the U.S. media to blame Russia for hacker attacks on U.S. governmental bodies."

"Russia does not conduct offensive operations in the cyber domain," the Embassy added.

While Russia continues to deny these attacks, Secretary of State Mike Pompeo stated in an interview released Friday night that it is "pretty clear" that Russia was behind that attack.

"This was a very significant effort, and I think it's the case that now we can say pretty clearly that it was the Russians that engaged in this activity," Pompeo told radio host Mark Levin.

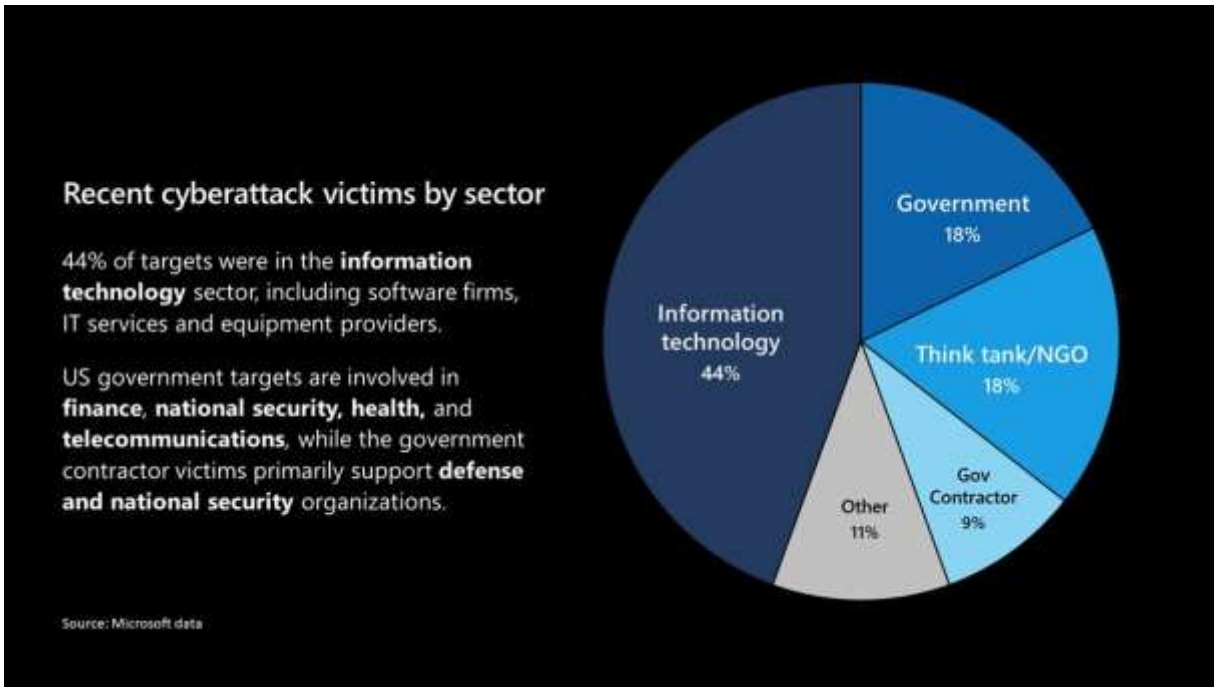
The victims of the attack

Researchers believe that the malicious DLL was pushed out to approximately 18,000 customers as part of this attack. The threat actors, though, only targeted organizations that they perceived as 'high value,' so even though some of these customers may have received the DLL, it is unknown if they were actively targeted in further attacks.

The currently known list of organizations that were hit by the SolarWinds supply chain attack include:

- FireEye
- U.S. Department of the Treasury
- U.S. National Telecommunications and Information Administration (NTIA)
- U.S. Department of State
- The National Institutes of Health (NIH) (Part of the U.S. Department of Health)
- U.S. Department of Homeland Security (DHS)
- U.S. Department of Energy (DOE)
- U.S. National Nuclear Security Administration (NNSA)
- Some US states (Specific states are undisclosed)
- Microsoft
- Cisco

Microsoft has also identified and notified more than 40 of its customers affected by this attack but has not disclosed their names. They state that 80% of the victims were from the U.S., and 44% were in the IT sector.



SunBurst victims by sector

Based on the [decoding of subdomains] generated by the malware domain generation algorithm (DGA), many well-known companies may disclose targeted attacks at a later date.

```
q1b01c6fdd7q4td50rswoiou0govirsv.appsync-api.us-east-1.avsvmcloud.com        servitia.intern
q3b8h31m9q7eoqa56260kun0e6iuir0e.appsync-api.us-east-2.avsvmcloud.com        sos-ad.state.
q3vcrhhcmddh7rl5oi602ou6iuir0grn.appsync-api.us-east-2.avsvmcloud.com        its.lastate.ed
q80cgv4eolosbfo4tvef0t12eu1.appsync-api.us-east-1.avsvmcloud.com          gncu.local
q882csbrq5oa58d4r6eud012st.appsync-api.us-east-1.avsvmcloud.com       escap.org
q8bps26mucuq6re4dutru70ct2w.appsync-api.us-east-1.avsvmcloud.com        pagewz.gov
q8gl1thobvg6d004tvef0b12eu1.appsync-api.us-east-1.avsvmcloud.com        gncu.local
sf0q84qduth323q6eo6e202e2h.appsync-api.us-east-1.avsvmcloud.com       cisco.com
q8vmaeii8n3dpeui5vr2d3212voe60be2.appsync-api.us-east-1.avsvmcloud.com          neophotonics.co
qb9tt88vftrj6v84euheoip0e12eu1.appsync-api.us-west-2.avsvmcloud.com       camcity.local
qbj2615jokrqdac5wh602un0twusouv0.appsync-api.us-west-2.avsvmcloud.com        vms.ad.varian
1cmge6dsclrtfejc6e0gdohu0et2w.appsync-api.us-east-1.avsvmcloud.com        sc.pima.gov
qfnf6ab6u28je4d5un0b2di0ho7r1p0b.appsync-api.us-east-2.avsvmcloud.com        ad.optimizely.
qfnf6ab6u28je415un0c2di0ho7r1p0c.appsync-api.us-east-2.avsvmcloud.com        ad.optimizely.
qg1e4bcthk3gdkr4e2sd0bdieo0be2h.appsync-api.us-east-1.avsvmcloud.com        corp.ptci.com
qgc2gj97t3sop415uhs8be2sd0govir1.appsync-api.us-east-1.avsvmcloud.com        amr.corp.intel
qg6ubroda1vp0414srd6su0oe2h.appsync-api.us-east-1.avsvmcloud.com       repsrv.com
qipptpf1jic4gav5oi60eou6iuir0grn.appsync-api.us-east-2.avsvmcloud.com        its.lastate.ed
qit0415tqf2j9mq5wo11r02irssrc2vv.appsync-api.us-east-2.avsvmcloud.com        ville.terrebonn
qj1bggoa06prfj646d6n0g6j02eu.appsync-api.us-east-1.avsvmcloud.com       spsd.sk.ca
qj82njdvtfuoi455uhs0be2sd0govir1.appsync-api.us-east-1.avsvmcloud.com        amr.corp.intel
qo046rspifbl4k04e2mvr10ge2m0te2h.appsync-api.us-east-2.avsvmcloud.com        coxnet.cox.com
qr1ao21mr659tfk5uh601un0hwusouv0.appsync-api.us-west-2.avsvmcloud.com        vms.ad.varian
qrjtdj3almlcj0k4urso2ve2sd00e2h.appsync-api.us-west-2.avsvmcloud.com        aerioncorp.com
qvot463cl5rcg5r4urso2ve2sd02e2h.appsync-api.us-west-2.avsvmcloud.com        aerioncorp.com
r14ptgk17qacucu5chsv0ee2h.appsync-api.us-west-2.avsvmcloud.com       hmrn.com
r1q6arhpujcf6jb6ervisu10odohu0it.appsync-api.us-west-2.avsvmcloud.com        central.pima.g
r1qshofj05j105ac6eolp02jovt612v0c.appsync-api.us-west-2.avsvmcloud.com        city.kingston.
r60ncekf5j1kkrboi602ou6iuir02rn.appsync-api.us-east-2.avsvmcloud.com        its.lastate.ed
r6b5cj43deojp665u30c2st.appsync-api.us-east-2.avsvmcloud.com       ah.org
r74br8r0cce4m6r6o160eou6iuir0trn.appsync-api.us-east-2.avsvmcloud.com        its.lastate.ed
r75n0q055j7bl6nvboi60cou6iuir0orn.appsync-api.us-east-2.avsvmcloud.com        its.lastate.ed
r7kqk893t5lu82j6uhs0ie2sd0iovir1.appsync-api.us-east-2.avsvmcloud.com        amr.corp.intel
```

Decoded backdoor command & control server subdomains
Source: RedDrip Team

What are security firms doing to protect victims

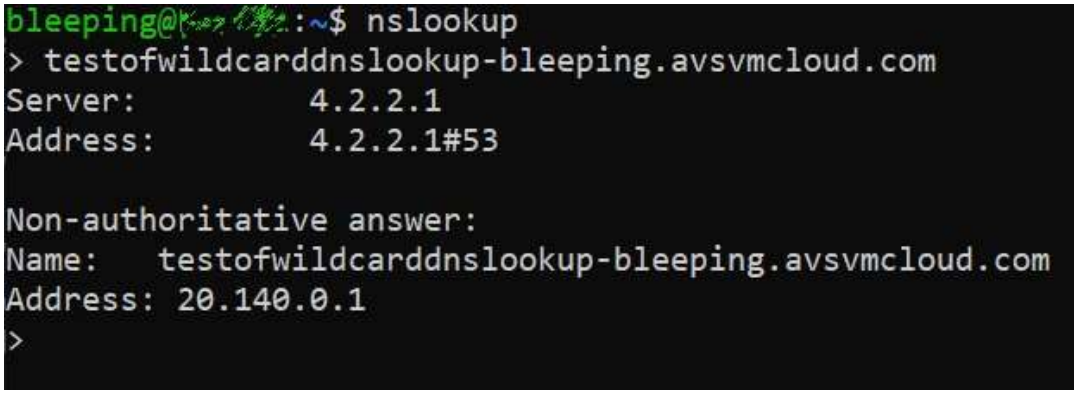
Since the cyberattack has been disclosed, security firms have been adding the malicious SunBurst backdoor binaries to their detections.

While Microsoft was already detecting and alerting customers of malicious SolarWinds binaries, they were not quarantining them out of concern it could affect an organization's network management services. On December 16th, at 8:00 AM PST, Microsoft Defender began quarantining detected binaries even if the process is running.

Microsoft, FireEye, and GoDaddy also collaborated to create a kill switch for the SunBurst backdoor distributed in the SolarWinds hack.

When the malicious binaries attempt to contact the command & control servers, they will perform DNS resolution to get the IP address. If this IP address is part of certain IP ranges, including ones owned by Microsoft, the backdoor will terminate and prevent itself from executing again.

To create the kill switch, GoDaddy created a wildcard DNS resolution so that any subdomain of avsvmcloud[.]com resolves to the IP address 20.140.0.1, which belongs to Microsoft and is on the malware's blocklist. This wildcard resolution is illustrated by a DNS lookup for a made-up subdomain, as shown below.



Wildcard DNS resolution

As this IP address is part of the malware's blocklist, when it connects to any subdomain of avsvmcloud[.]com, it will unload and no longer execute.

While this kill switch will disable SunBurst backdoor deployments connecting the command & control servers, FireEye has stated the threat actors may have deployed other backdoors.

"However, in the intrusions FireEye has seen, this actor moved quickly to establish additional persistent mechanisms to access to victim networks beyond the SunBurst backdoor. This killswitch will not remove the actor from victim networks where they have established other backdoors. However, it will make it more difficult to for the actor to

leverage the previously distributed versions of SunBurst," FireEye warned about the kill switch," FireEye told BleepingComputer in a statement.

How to check if you were compromised

If you are a user of SolarWinds products, you should immediately consult their advisory and Frequently Asked Questions as it contains necessary information about upgrading to the latest 'clean' version of their software.

Microsoft has also published a list of nineteen malicious SolarWinds.Orion.Core.BusinessLayer.dll DLL files spotted in the wild.

This list, shown below, contains a file's SHA256 hash, the file version, and when it was first seen.

SHA256	File Version	Date first seen
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d	2020.2.100.11713	February 2020
a58d02465e26bdd3a839fd90e4b317eece431d28cab203bbdde569e11247d9e2	2020.2.100.11784	March 2020
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77	2019.4.5200.9083	March 2020
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b	2020.2.100.12219	March 2020
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed	2020.2.100.11831	March 2020
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77	Not available	March 2020
ffdbdd460420972fd2926a7f460c198523480bc6279dd6cca177230db18748e8	2019.4.5200.9065	March 2020
b8a05cc492f70ffa4adcd446b693d5aa2b71dc4fa2bf5022bf60d7b13884f666	2019.4.5200.9068	March 2020
20e35055113dac104d2bb02d4e7e33413fae0e5a426e0eea0dfd2c1dce692fd9	2019.4.5200.9078	March 2020
0f5d7e6dfdd62c83eb096ba193b5ae394001bac036745495674156ead6557589	2019.4.5200.9078	March 2020
cc082d21b9e880ceb6c96db1c48a0375aaf06a5f444cb0144b70e01dc69048e6	2019.4.5200.9083	March 2020
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c	2020.4.100.478	April 2020
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134	2020.2.5200.12394	April 2020

ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6	2020.2.5300.12432	May 2020
2b3445e42d64c85a5475bdbc88a50ba8c013febb53ea97119a11604b7595e53d	2019.4.5200.9078	May 2020
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690	2020.4.100.751	May 2020
a3efbc07068606ba1c19a7ef21f4de15d15b41ef680832d7bcba485143668f2d	Not available	Not available
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc	2019.4.5200.8890	October 2019
d3c6785e18fba3749fb785bc313cf8346182f532c59172b69adfb31b96a5d0af	2019.4.5200.8890	October 2019

Finally, security researchers have released various tools that allow you to check if you were compromised or what credentials were stored in your SolarWinds Orion installation.

- SolarFlare Release: Password Dumper for SolarWinds Orion
- SpearTip's SolarWinds' Orion Vulnerability Tool SunScreen – SPF 10

The source code for both projects is published to GitHub. You are strongly encouraged to review the source code, if available, of any program you plan to run on your network.

Second SUPERNOVA malware found

During the investigation into the SolarWinds hack, Palo Alto Networks and Microsoft found an additional malware named SUPERNOVA distributed using the **App_Web_logoimagehandler.ashx.b6031896.dll** DLL file.

This malware is a backdoor that allowed the threat actors to send C# code that would be compiled and executed by the malware.

SUPERNOVA code

This malware is not believed to be related to the **SolarWinds.Orion.Core.BusinessLayer.dll** supply chain attack. It does, though, indicate that the SolarWinds Orion platform was used in two different attacks, and possibly by different groups, to distribute malware.

Last week, SolarWinds released an update advisory that advises all Orion Platform customers to upgrade to the latest versions to be protected from not only the SUNBURST vulnerability but the SUPERNOVA malware as well.

Source: https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

5. Russia's SolarWinds Attack

Recent news articles have all been talking about the massive Russian cyberattack against the United States, but that's wrong on two accounts. It wasn't a cyberattack in international relations terms, it was espionage. And the victim wasn't just the US, it was the entire world. But it was massive, and it is dangerous.

Espionage is internationally allowed in peacetime. The problem is that both espionage and cyberattacks require the same computer and network intrusions, and the difference is only a few keystrokes. And since this Russian operation isn't at all targeted, the entire world is at risk — and not just from Russia. Many countries carry out these sorts of operations, none more extensively than the US. The solution is to prioritize security and defense over espionage and attack.

Here's what we know: Orion is a network management product from a company named SolarWinds, with over 300,000 customers worldwide. Sometime before March, hackers working for the Russian SVR — previously known as the KGB — hacked into SolarWinds and slipped a backdoor into an Orion software update. (We don't know how, but last year the company's update server was protected by the password "solarwinds123" — something that speaks to a lack of security culture.) Users who downloaded and installed that corrupted update between March and June unwittingly gave SVR hackers access to their networks.

This is called a supply-chain attack, because it targets a supplier to an organization rather than an organization itself — and can affect all of a supplier's customers. It's an increasingly common way to attack networks. Other examples of this sort of attack include fake apps in the Google Play store, and hacked replacement screens for your smartphone.

SolarWinds has removed its customer list from its website, but the Internet Archive saved it: all five branches of the US military, the state department, the White House, the NSA, 425 of the Fortune 500 companies, all five of the top five accounting firms, and hundreds of universities and colleges. In an SEC filing, SolarWinds said that it believes "fewer than 18,000" of those customers installed this malicious update, another way of saying that more than 17,000 did.

That's a lot of vulnerable networks, and it's inconceivable that the SVR penetrated them all. Instead, it chose carefully from its cornucopia of targets. Microsoft's analysis identified 40 customers who were infiltrated using this vulnerability. The great majority of those were in the US, but networks in Canada, Mexico, Belgium, Spain, the UK, Israel and the UAE were also targeted. This list includes governments, government contractors, IT companies, thinktanks, and NGOs — and it will certainly grow.

Once inside a network, SVR hackers followed a standard playbook: establish persistent access that will remain even if the initial vulnerability is fixed; move laterally around the network by compromising additional systems and accounts; and then exfiltrate data. Not being a SolarWinds customer is no guarantee of security; this SVR operation used other initial infection vectors and techniques as well. These are sophisticated and patient hackers, and we're only just learning some of the techniques involved here.

Recovering from this attack isn't easy. Because any SVR hackers would establish persistent access, the only way to ensure that your network isn't compromised is to burn it to the ground and rebuild it, similar to reinstalling your computer's operating system to recover from a bad hack. This is how a lot of sysadmins are going to spend their Christmas holiday, and even then they can&;t be sure. There are many ways to establish persistent access that survive rebuilding individual computers and networks. We know, for example, of an NSA exploit that remains on a hard drive even after it is reformatted. Code for that exploit was part of the Equation Group tools that the Shadow Brokers — again believed to be Russia — stole from the NSA and published in 2016. The SVR probably has the same kinds of tools.

Even without that caveat, many network administrators won't go through the long, painful, and potentially expensive rebuilding process. They'll just hope for the best.

It's hard to overstate how bad this is. We are still learning about US government organizations breached: the state department, the treasury department, homeland security, the Los Alamos and Sandia National Laboratories (where nuclear weapons are developed), the National Nuclear Security Administration, the National Institutes of Health, and many more. At this point, there's no indication that any classified networks were penetrated, although that could change easily. It will take years to learn which networks the SVR has penetrated, and where it still has access. Much of that will probably be classified, which means that we, the public, will never know.

And now that the Orion vulnerability is public, other governments and cybercriminals will use it to penetrate vulnerable networks. I can guarantee you that the NSA is using the SVR's hack to infiltrate other networks; why would they not? (Do any Russian organizations use Orion? Probably.)

While this is a security failure of enormous proportions, it is not, as Senator Richard Durban said, "virtually a declaration of war by Russia on the United States." While

President-elect Biden said he will make this a top priority, it's unlikely that he will do much to retaliate.

The reason is that, by international norms, Russia did nothing wrong. This is the normal state of affairs. Countries spy on each other all the time. There are no rules or even norms, and it's basically "buyer beware." The US regularly fails to retaliate against espionage operations — such as China's hack of the Office of Personal Management (OPM) and previous Russian hacks — because we do it, too. Speaking of the OPM hack, the then director of national intelligence, James Clapper, said: "You have to kind of salute the Chinese for what they did. If we had the opportunity to do that, I don't think we'd hesitate for a minute."

We don't, and I'm sure NSA employees are grudgingly impressed with the SVR. The US has by far the most extensive and aggressive intelligence operation in the world. The NSA's budget is the largest of any intelligence agency. It aggressively leverages the US's position controlling most of the internet backbone and most of the major internet companies. Edward Snowden disclosed many targets of its efforts around 2014, which then included 193 countries, the World Bank, the IMF and the International Atomic Energy Agency. We are undoubtedly running an offensive operation on the scale of this SVR operation right now, and it'll probably never be made public. In 2016, President Obama boasted that we have "more capacity than anybody both offensively and defensively."

He may have been too optimistic about our defensive capability. The US prioritizes and spends many times more on offense than on defensive cybersecurity. In recent years, the NSA has adopted a strategy of "persistent engagement," sometimes called "defending forward." The idea is that instead of passively waiting for the enemy to attack our networks and infrastructure, we go on the offensive and disrupt attacks before they get to us. This strategy was credited with foiling a plot by the Russian Internet Research Agency to disrupt the 2018 elections.

But if persistent engagement is so effective, how could it have missed this massive SVR operation? It seems that pretty much the entire US government was unknowingly sending information back to Moscow. If we *had* been watching everything the Russians were doing, we would have seen some evidence of this. The Russians' success under the watchful eye of the NSA and US Cyber Command shows that this is a failed approach.

And how did US defensive capability miss this? The only reason we know about this breach is because, earlier this month, the security company FireEye discovered that it had been hacked. During its own audit of its network, it uncovered the Orion vulnerability and alerted the US government. Why don't organizations like the Departments of State, Treasury and Homeland Security regularly conduct that level of audit on their own systems? The government's intrusion detection system, Einstein 3, failed here because it doesn't detect new sophisticated attacks — a deficiency pointed out in 2018 but never fixed. We shouldn't have to rely on a private cybersecurity company to alert us of a major nation-state attack.

If anything, the US's prioritization of offense over defense makes us less safe. In the interests of surveillance, the NSA has pushed for an insecure cell phone encryption standard and a backdoor in random number generators (important for secure encryption). The DoJ has never relented in its insistence that the world's popular encryption systems be made insecure through back doors — another hot point where attack and defense are in conflict. In other words, we allow for insecure standards and systems, because we can use them to spy on others.

We need to adopt a defense-dominant strategy. As computers and the internet become increasingly essential to society, cyberattacks are likely to be the precursor to actual war. We are simply too vulnerable when we prioritize offense, even if we have to give up the advantage of using those insecurities to spy on others.

Our vulnerability is magnified as eavesdropping may bleed into a direct attack. The SVR's access allows them not only to eavesdrop, but also to modify data, degrade network performance, or erase entire networks. The first might be normal spying, but the second certainly could be considered an act of war. Russia is almost certainly laying the groundwork for future attack.

This preparation would not be unprecedented. There's a lot of attack going on in the world. In 2010, the US and Israel attacked the Iranian nuclear program. In 2012, Iran attacked the Saudi national oil company. North Korea attacked Sony in 2014. Russia attacked the Ukrainian power grid in 2015 and 2016. Russia is hacking the US power grid, and the US is hacking Russia's power grid — just in case the capability is needed someday. All of these attacks began as a spying operation. Security vulnerabilities have real-world consequences.

We're not going to be able to secure our networks and systems in this no-rules, free-for-all every-network-for-itself world. The US needs to willingly give up part of its offensive advantage in cyberspace in exchange for a vastly more secure global cyberspace. We need to invest in securing the world's supply chains from this type of attack, and to press for international norms and agreements prioritizing cybersecurity, like the 2018 Paris Call for Trust and Security in Cyberspace or the Global Commission on the Stability of Cyberspace. Hardening widely used software like Orion (or the core internet protocols) helps everyone. We need to dampen this offensive arms race rather than exacerbate it, and work towards cyber peace. Otherwise, hypocritically criticizing the Russians for doing the same thing we do every day won't help create the safer world in which we all want to live.

This essay previously appeared in the *Guardian*.

Source: https://www.schneier.com/blog/archives/2020/12/russias-solarwinds-attack.html

6. TrickBot's new module aims to infect your UEFI firmware

TrickBot malware developers have created a new module that probes for UEFI vulnerabilities, demonstrating the actor's effort to take attacks at a level that would give them ultimate control over infected machines.

With access to UEFI firmware, a threat actor would establish on the compromised machine persistence that resists operating system reinstalls or replacing of storage drives.

Malicious code planted in the firmware (bootkits) is invisible to security solutions operating on top of the operating system because it loads before everything else, in the initial stage of a computer's booting sequence.

Bootkits enable control over an operating systems' boot process and allow sabotaging defenses at a higher level. Because the code runs at the earliest stage, the Secure Boot mechanism does not help, since it depends on the integrity of the firmware.

The implications associated with a threat actor obtaining this sort of permanent presence on a machine are tremendous, all the more in the case of TrickBot, whose average daily infections can get as high as several thousand.

Targeting Intel platforms

In a joint report today, cybersecurity boutique Advanced Intelligence (AdvIntel) and researchers at hardware and security firm Eclypsium provide technical details on TrickBot's new component.

TrickBoot acts as a reconnaissance tool at this stage, checking for vulnerabilities in the UEFI firmware of the infected machine. For now, the verification targets only Intel platforms (Skylake, Kaby Lake, Coffee Lake, Comet Lake). Nevertheless, the module also includes code to read, write, and erase firmware so it can be used for significant damage.

It checks if the UEFI/BIOS write protection is active using the RwDrv.sys driver from RWEverything, a free utility that allows access to hardware components such as the SPI flash memory chip that stores a system's BIOS/UEFI firmware.

If the name of the tool rings a bell it's because it was used by LoJax, the first UEFI rootkit discovered in the wild, in an attack from Russian hackers known as APT28 (Fancy Bear, Sednit, Strontium, Sofacy).

"All requests to the UEFI firmware stored in the SPI flash chip go through the SPI controller, which is part of the Platform Controller Hub (PCH) on Intel platforms. This SPI controller includes access control mechanisms, which can be locked during the boot process in order to prevent unauthorized modification of the UEFI firmware stored in the SPI flash memory chip" - joint report (Eclypsium, AdvIntel)

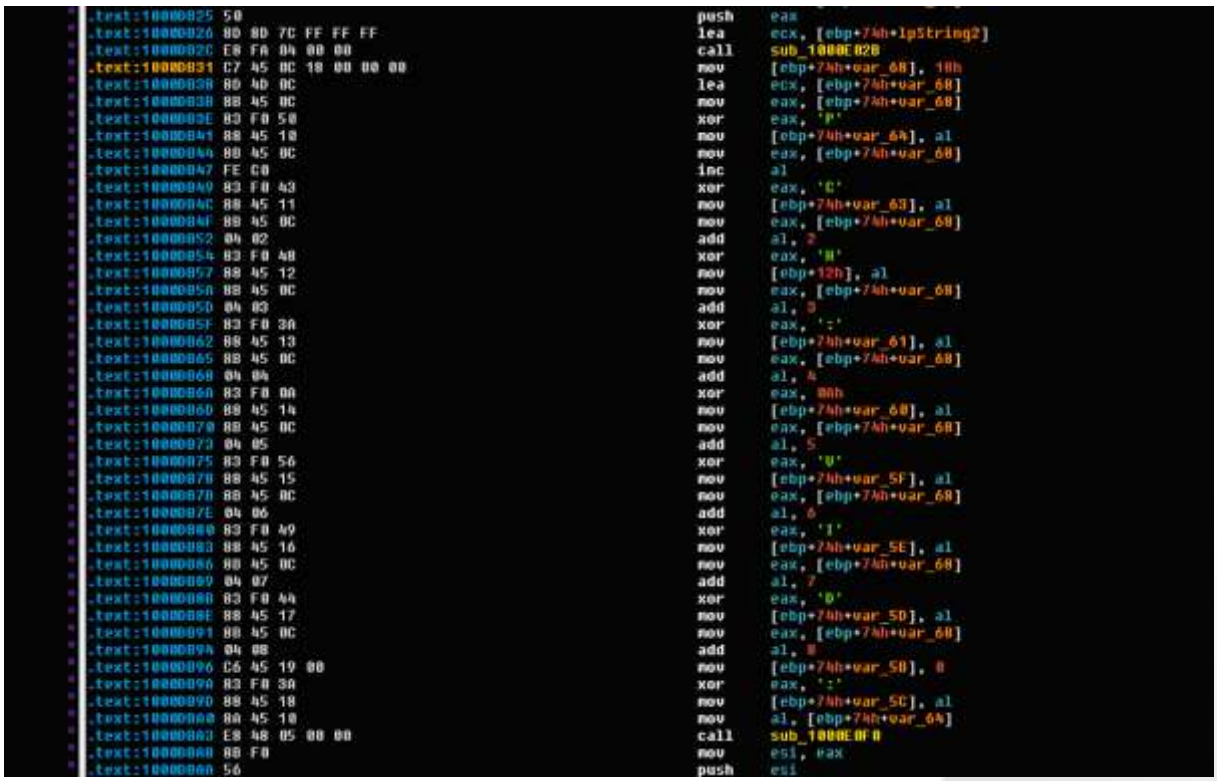
The researchers say that BIOS/UEFI write protection is available on modern systems but this feature is often not active or misconfigured, allowing attackers to modify the firmware or delete it to brick the device.

The researchers discovered the module on October 19 and named it TrickBoot, a pun on its functionality and the name of the botnet malware that deploys it.

In a sample analyzed by Advanced Intelligence, the researchers spotted the name "PermaDll" associated with the file "user_platform_check.Dll" in a new TrickBot sample.

Investigating the file with Eclypsium revealed that the threat actor had implemented a mechanism that checked the single-chip chipset on the compromised system.

The researchers discovered that the role of the module was to run PCH queries to determine the specific model of PCH running on the system, thus identifying the platform. This information also allows the attacker to check if the platform is vulnerable or not.



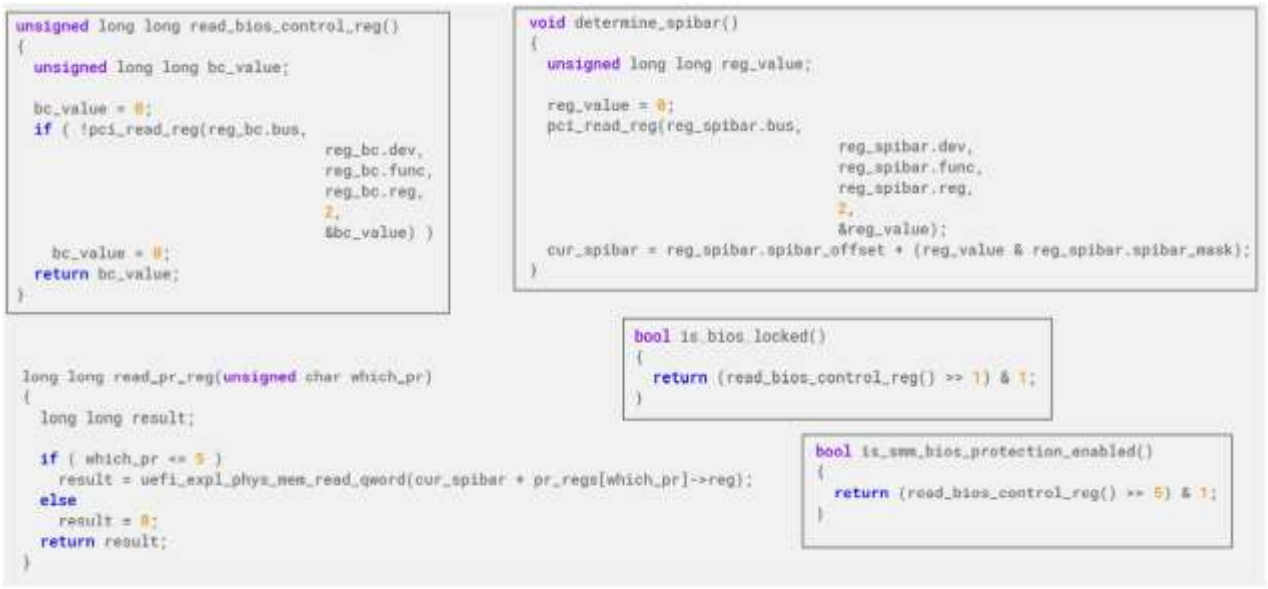
The researchers also found that the actor relies on functions from a known firmware exploitation tool and library called [fwexpl](#) For the following purposes:

- read data from hardware IO ports

- call the rwdrv.sys driver to write data to hardware IO ports
- call the rwdrv.sys driver to read data from physical memory addresses
- call the rwdrv.sys driver to write data to physical memory addresses

The researchers note that if TrickBoot is running on a platform not present in its lookup table, it activates a function with a pre-Skylake set of default values for operations requiring hardware access.

After identifying the platform, TrickBoot accesses paths related to reading registers for the flash memory (SPIBAR, PRO-PR4) and BIOS control (BC - contains write-protect lock bits for BIOS access at hardware level).



```
unsigned long long read_bios_control_reg()
{
  unsigned long long bc_value;

  bc_value = 0;
  if ( !pci_read_reg(reg_bc.bus,
                     reg_bc.dev,
                     reg_bc.func,
                     reg_bc.reg,
                     2,
                     &bc_value) )
    bc_value = 0;
  return bc_value;
}
```

```
void determine_spibar()
{
  unsigned long long reg_value;

  reg_value = 0;
  pci_read_reg(reg_spibar.bus,
               reg_spibar.dev,
               reg_spibar.func,
               reg_spibar.reg,
               2,
               &reg_value);
  cur_spibar = reg_spibar.spibar_offset + (reg_value & reg_spibar.spibar_mask);
}
```

```
bool is_bios_locked()
{
  return (read_bios_control_reg() >> 1) & 1;
}
```

```
long long read_pr_reg(unsigned char which_pr)
{
  long long result;

  if ( which_pr <= 5 )
    result = uefi_expl_phys_mem_read_qword(cur_spibar + pr_regs[which_pr]->reg);
  else
    result = 0;
  return result;
}
```

```
bool is_smm_bios_protection_enabled()
{
  return (read_bios_control_reg() >> 5) & 1;
}
```

An interesting find in the function that attempts to disable BIOS write protection is that it contains a bug that reads from the wrong offset in the BIOS Control register to check if the BIOS Write Protection Disable bit is set. This results in the code interpreting that write protection is active and tries to disable it.

```
unsigned int try_disable_bios_write_protection()
{
  unsigned int result;
  unsigned long long bc_val;

  // BUG HERE: Trying to read BIOS Control offset
  // from SPIBAR instead of PCI Config Space
  if ( uefi_expl_phys_mem_read_byte(cur_spibar + 0xDC) & 0x20 )
    goto LABEL_10;
  // BUG HERE: Trying to write BIOS Control offset
  // via SPIBAR instead of PCI Config Space
  uefi_expl_phys_mem_write_byte_or_with_old(cur_spibar + 0xDC, 1u);
  bc_val = 0;
  // Read BIOS Control register and check if WPD bit is already set
  if ( pci_read_reg(reg_bc.bus,
                    reg_bc.dev,
                    reg_bc.func,
                    reg_bc.reg,
                    2,
                    &bc_val) && !(bc_val &  ) )
    // Try to set the WPD (Write Protect Disable) bit
    // in BIOS Control register
    pci_write_reg(
      reg_bc.bus,
      reg_bc.dev,
      reg_bc.func,
      reg_bc.reg,
      2,
      bc_val | 1);
  // Check if we were able to set the WPD bit
  pci_read_reg(reg_bc.bus,
               reg_bc.dev,
               reg_bc.func,
               reg_bc.reg,
               2,
               &bc_val);
  if ( !(bc_val & 1) )
LABEL_10:
    result = 15;
  else
    result = 0;
  return result;
}
```

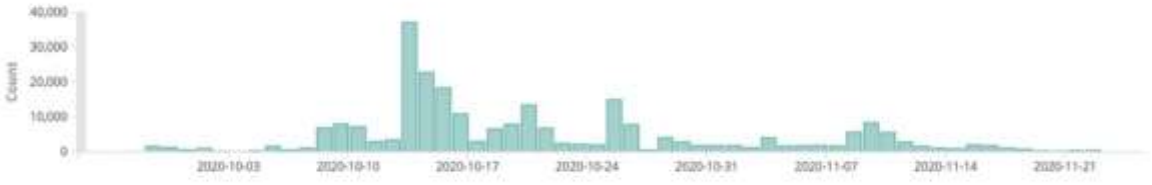
commented by Eclypsium

Major implications

TrickBot developing such a module is a clear indication that the actor is making an effort to expand its grip on compromised systems. The botnet already has thousands of infected machines from which the actor can select the most valuable targets.

AdvIntel's telemetry shows that daily TrickBot infections between October 3 and November 21 peaked at 40,000, with a daily average between 200 and 4,000. These figures are conservative since it does not count infected computers on private networks, which communicate externally using the gateway's IP address.

Selecting the most profitable victims is done manually based on data pulled through reconnaissance scripts that extract information from victim networks, hardware, and software.



The operators are financially motivated and use the botnet to deliver Ryuk and Conti ransomware on high-value machines. Since 2018, they made at least $150 million. From one recent victim alone, they took 2,200 BTC (valued at $34 million at the time).

TrickBot is truly a cybercriminal enterprise involved in multiple money-making schemes, including bank fraud and financial/personal information stealing.

Gaining UEFI-level persistence on the high-value machines could maximize the actor's profits as they could use this advantage in several ways.

Apart from using UEFI implants as leverage in negotiations to drive up the ransom price, the cybercriminals could maintain access to the machines even after the victim pays them to release systems from TrickBot control.

Later on, after victims complete the cleaning and recovery processes, the actor can take advantage of their continued presence in the UEFI code to run a new attack. They could also collect the newly set access credentials and sell them to a different gang.

Moreover, this could be used in operations that have a purely destructive goal as it can impact large operational environments and critical infrastructure. Another effect of bricking the devices is that it makes forensic investigation much more difficult, considerably slows down the recovery process, and breaks other layers of security.

Defense action is tough

Jesse Michael, principal researcher at Eclypsium told BleepingComputer that determining if a system has been compromised at UEFI firmware level is a tough job.

A more thorough method is to read the content on the SPI memory chip when the system is powered down by physically attaching an SPI flash programming device. This solution, though, involves not only expertise but also extended downtime for the company since in some cases the chip is soldered to the motherboard and this comes with the risk of reading problems.

Another method is to use open-source tools (CHIPSEC) or Eclypsium's platform that looks for low-level weaknesses at the hardware and firmware level and can also determine if BIOS write protection is active or not.

Checking firmware hashes also helps determine if the code has been tampered with. Furthermore, updating the firmware is a good way to make sure that it is not affected by known vulnerabilities.

UEFI-level compromise is a rarity even these days, more than five years since Hacking Team's VectorEDK UEFI implant code has been leaked and publicly available.

At the moment, publicly documented attacks of this kind come from highly advanced, state-backed threat actors - Lojax from Russian hackers and MosaicRegressor from Chinese hackers, which uses VectorEDK code.

However, attacks from these adversaries are highly targeted, unlike TrickBot's, which aims to infect as many systems as possible and pick the valuable targets (large companies from any sector) from that pool.

From the analysis of the TrickBoot sample, the module only identifies the hardware and checks if the BIOS region is writable. But this can easily change to allow writing to the SPI flash memory and modify the system firmware.

The technical report from AdvIntel and Eclypsium provides indicators of compromise for TrickBoot along with a Yara rule created by Vitali Kremez for this new module.

Source: https://www.bleepingcomputer.com/news/security/trickbots-new-module-aims-to-infect-your-uefi-firmware/

7. Microsoft issues guidance for DNS cache poisoning vulnerability

Microsoft issued guidance on how to mitigate a DNS cache poisoning vulnerability reported by security researchers from the University of California and Tsinghua University.

Successfully exploiting the vulnerability could allow attackers to use modified DNS records to redirect a target to a malicious website under their control as part of DNS spoofing (also known as DNS cache poisoning) attacks.

The end goal of such attacks is to either exploit device or software vulnerabilities to infect the target with malware or to harvest sensitive information via a phishing landing page.

Impacts multiple Windows server platforms

The addressing spoofing vulnerability — tracked as CVE-2020-25705 and nicknamed SAD DNS (Side-channel AttackeD DNS) — exists in the Windows DNS Resolver software component that comes bundled with the Windows Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

"Microsoft is aware of a vulnerability involving DNS cache poisoning caused by IP fragmentation that affects Windows DNS Resolver," the company explains in a security advisory published as part of this month's Patch Tuesday.

"An attacker who successfully exploited this vulnerability could spoof the DNS packet which can be cached by the DNS Forwarder or the DNS Resolver."

SAD DNS is rated by Microsoft as 'Important' severity and it impacts only Windows server platforms, between Windows Server 2008 R2 and Windows 10, version 20H2 (Server Core Installation).

CVE-2020-25705 mitigation

To mitigate this vulnerability, Windows administrators can alter the Registry to change the maximum UDP packet size to 1,221 bytes which would block any DNS cache poisoning attacks attempting to exploit it on vulnerable devices.

To do that, admins are required to go through the following procedure:

- Run **regedit.exe** as Administrator.
- In Registry Editor, navigate to the `HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters` subkey and set the following parameters:
  - Value: MaximumUdpPacketSize
  - Type: DWORD
  - Data: 4C5 Hexadecimal or 1221 Decimal
- Close Registry Editor and restart the DNS service.

After the registry update, the DNS resolver will now switch to TCP for all responses larger than 4C5 or 1221, automatically blocking any CVE-2020-25705 attacks.

According to researchers who discovered SAD DNS, CVE-2020-25705 also impacts other operating systems besides Windows including Linux, macOS, and FreeBSD, as well as other DNS resolvers including but not limited to BIND, Unbound, and dnsmasq.

Microsoft has also released security updates today to fix 58 vulnerabilities as part of December 2020 Patch Tuesday, nine classified as Critical, 48 as Important, and two as Moderate severity.

Source: https://www.bleepingcomputer.com/news/security/microsoft-issues-guidance-for-dns-cache-poisoning-vulnerability/

8. How Open Security Can Make Threat Management More Efficient

Security operations center (SOC) teams struggle with an array of challenges. Too many tools can make the work too complex; and recruiting and retaining personnel can be hard amidst a skills shortage. Experts need to focus on using their skills to their fullest. But, an open approach can improve threat management in a way that makes all of these things easier.

All these challenges complicate some aspect of threat management. Complex tools make it harder for SOCs to gain insight into their landscapes and detect threats. Solving cases thoroughly and responding to incidents quickly is difficult when staff are overwhelmed.

Making tools simpler and connecting teams — both to each other and to threat intelligence landscapes — can help ease these challenges. By allowing everyone in the SOC to access the same data, threat intelligence feeds and workflows create strength in

numbers. It also breaks down silos. Teams can be more efficient and work with other departments more easily.

Here's how an open approach to security draws connections that can benefit team leaders, analysts and incident responders.

For Security Leaders: Connecting Tools and Teams

In light of the skills shortage, leaders are focused on retaining their staff and using their skills to their full potential. Providing everyone on the team insight over data and access to threat intelligence helps break down any silos that might exist. It also improves the way the SOC can detect and respond to threats.

Connecting not just teams, but also tools to each other can help meet work goals. Reducing complex processes keeps teams from having to switch between tools and integrate point products, which take up time. With a more condensed view over the threat management life cycle, leadership can get the high-level overview they need.

An open security landscape also reduces vendor lock-in. Connecting the people and tools of a SOC to third-party threat intelligence feeds and partners gives them more choices.

Providing clarity, triaging workloads and focusing on what you're trying to protect can help to reduce workloads and dissipate personnel burnout. This also helps the security leaders retain and get the most out of the skilled individuals on their elite team.

Security Analysts: Augmenting End-to-End Hunting

Analysts need practical, trustworthy, insightful intelligence in context to gain insight and assess risk. Providing access to third-party threat intelligence makes ad hoc threat hunting, incident response and threat investigation more effective. With the context provided by that data, analysts have more confidence and clues when they triage alerts.

In addition to opening the SOC to external intelligence feeds, analysts can be more efficient when internal processes are more connected in a threat management workflow. Connecting security intelligence to a SOAR solution, for example, makes incident response workflows more direct.

Automation can also connect different parts of the process. Now, analysts are flooded with alerts flowing into the SOC. Automation can improve the alert triage process, connecting analysts with priority alerts while reducing the need for some manual processes.

Incident Responders: Work Together

Similar to analysts, incident responders need to work with large volumes of data — most of which is noise — and a growing set of different tools to build context. A common set

of tools can help analysts and incident responders work with each other, making the SOC more efficient.

Dynamic playbooks, which consist of single or multiple discrete workflows, are one such example. These step-by-step guided response playbooks can enable responders to follow a smart course of action, while allowing them to pivot as events unfold. Having the right procedures in place helps give the incident response team the guidance they need to get started when working to resolve an incident spotted by the analyst team.

Incident responders often need to work through the largely manual process of action and evidence tracking. A SOAR tool can timestamp and log every action throughout an incident response for reporting and auditing purposes. Key metrics help inform strategic decisions and generate reports that can be shared with both their managers and the wider business.

Addressing Threat Intelligence Challenges

One way to achieve open security and connection is with a security platform. With a security platform, you'll have a set of modules that share common services and user experiences to provide more complete insights and streamlined workflows. The common services share data and information. They encourage reuse across the security team, regardless of role, seniority or niche. This helps to scale the team and let them work efficiently rather than uncovering the same things in parallel workflows.

In the security industry, 'platform' is a term sometimes incorrectly used to refer to portfolios — suites of products with some integration — or ecosystems. A platform that offers a set of modular security capabilities can help teams shift away from solving individual use cases.

The sharing of insights across apps and services brings together existing tooling and investments. And it does so without creating vendor lock-in. With a security platform, it's possible to infuse threat intelligence across use cases like incident response and threat hunting. At the same time, you can enhance end-to-end threat management workflows alongside united searches.

As entities manage hybrid multicloud environments, a platform enables a holistic view across the entire enterprise — on cloud and on premise. This doesn't just provide confidence through clarity; it also improves on existing investments. A platform can enable those tools that have already been deployed and configured to be connected and infused with threat intelligence. This connection encourages team members to be more productive and provides a more meaningful return on investment.

United Threat Management

As entities evolve to this hybrid multicloud posture, providing everyone in the SOC the same access to more data via connected tools paves the way for more efficient threat management. Rather than making things more complex, the goal of an open approach is to leverage what you have: the skills of your staff, the threat intelligence of your industry peers and the existing tooling of your SOC. Bringing all these elements together with a vendor-agnostic platform can help unite your team against cybersecurity threats.

Source:https://securityintelligence.com/posts/how-open-security-makes-threat-management-efficient/

9. 45 Million Medical Images Left Exposed Online

A six-month investigation by CybelAngel discovered unsecured sensitive patient data available for third parties to access for blackmail, fraud or other nefarious purposes.

More than 45 million medical images—and the personally identifiable information (PII) and personal healthcare information (PHI) associated with them–have been left exposed online due to unsecured technology that's typically used to store, send and receive medical data, new research has found.

A team from CybelAngel Analyst Team uncovered sensitive medical records and images–including X-rays CT scans and MRI images—that anyone can access online in a six-month investigation researchers conducted into network attached storage (NAS) and Digital Imaging and Communications in Medicine (DICOM).

NAS is an inexpensive storage solution used mainly by small companies or individuals to store data rather than paying for more expensive dedicated servers or virtual cloud servers, while DICOM is a global standard used by healthcare professionals to transmit medical images.

"CybelAngel Analyst Team detected medical devices leaking more than 45 million unique imaging files on unprotected connected storage devices with ties to hospitals and medical centers worldwide," David Sygula, senior cybersecurity analyst at CybelAngel, said in the report Full Body Exposure, adding that leaks were found in data across 67 countries.

The findings are concerning for a number of reasons. Threat actors can violate people's privacy by selling the data on the dark web, where it is a valuable commodity, researchers said. They also can use the images and data to blackmail patients or to scam the medical system by using patient data to set up "ghost clinics" and "ghost patients" to commit fraud.

Moreover, privacy concerns over patient data are especially critical as the world is currently in the midst of a pandemic in which PII and PHI can have major implications for patient lives and the lives of those they've been in contact with. Threat actors or those with bad intentions also can use access to the data to modify someone's medical records with ill intent, researchers noted.

CybelAngel tools scanned approximately 4.3 billion IP addresses to discover the images, which were left exposed on more than 2,140 unprotected servers across 67 countries including the United States, United Kingdom, France and Germany, according to the report.

Images typically included up to 200 lines of metadata per record which included the name, birth date and address of the patient as well as his or her height, weight, diagnosis and other PHI. Anyone could access the images and data without the need for a username or password; in fact, in some cases, login portals to the systems storing the info accepted blank usernames and passwords, researchers said.

"The fact that we did not use any hacking tools throughout our research highlights the ease with which we were able to discover and access these files," Sygula said in a press statement. "This is a concerning discovery and proves that more stringent security processes must be put in place to protect how sensitive medical data is shared and stored by healthcare professionals."

Researchers investigated the route medical images and data take from devices such as MRI, CT scanners and X-rays using DICOM through to a centralized Picture Archiving and Communication System (PACs), which stores and distributes the images.

The PACS workstations usually include DICOM viewers, which can exist in the form of web applications, as well as organizational and collaborative tools. While these means of communication and transfer are meant to be secure, researchers discovered that security was "insufficient," at best.

"To make matters worse, the existing DICOM application security measures are not mandatory and are not implemented by default," Sygula wrote.

In most cases, the leak involved a NAS device that would expose data in a number of ways. These include unsecured ports allowing FTP and SMB protocols to provide unauthorized third parties access to devices and their data, as well as Dynamic DNS (DDNS) granting outsiders access to unsecured web services.

CybelAngel provided some simple advice for healthcare facilities to avoid exposing sensitive data to those unauthorized to view it. Researchers suggest they ensure that pandemic response not exceed current security policies, as well as maintain proper network segmentation of connected medical imaging equipment.

CybelAngel also suggests that healthcare facilities conduct real-world audit of third-party partners to ensure that they also are in compliance with protocols so data isn't leaked inadvertently in transit, according to the report.

Source: https://threatpost.com/million-medical-images-online/162284/

10. Top Ten Tips for Protecting Your Identity, Finances, and Security Online

Whether you're working, banking, shopping, or just streaming a few shows online, these quick tips will make sure you're more secure from hacks, attacks, and prying eyes.

1 – Protect your computers

Start with the basics: get strong protection for your computers and laptops. And that means more than basic antivirus. Using a comprehensive suite of security software like McAfee® Total Protection can help defend your entire family from the latest threats and malware, make it safer to browse, help steer you clear of potential fraud, and look out for your privacy too.

2 – Protect your phones and tablets too!

Aside from using it for calls and texting, we use our smartphones for plenty of things. We're sending money with payment apps. We're doing our banking. And we're using them as a "universal remote control" to do things like set the alarm, turn our lights on and off, and even see who's at the front door. Whether you're an Android owner or iOS owner, get security software installed on your smartphones and tablets so you can protect all the things they access and control.

3 – Create new passwords

Get a fresh start with strong, unique passwords for all your accounts using a strong method of password creation. And keep those passwords safe—don't store them in an unprotected file on your computer, which can be subject to a hack or data loss. Better yet, instead of keeping them on a notebook or on sticky notes, consider using a password manager. It can actually create strong passwords for you, store them as you create them, and automatically use them as you surf, shop, and bank.

4 – Keep updated

Make sure you have the latest software updates for your computers, laptops, phones, tablets, and apps, and internet of things (IoT) devices like camera and alarm systems. Updates are important for two reasons: one, they'll make sure you're getting the latest functionality from your app or device; and two, they often contain security upgrades. If there's a setting that lets you receive automatic updates, enable it so that you always have the latest.

5 – Beware of what you share

Hackers love playing the role of imposters to get a hold of sensitive info and account logins—because it's often so effective. If you get what appears to be a suspicious request from a recruiter, co-worker, vendor, friend, or family member, verify the message with that person directly before opening or responding. Remember that an employer will never request sensitive information such as social security numbers or bank routing numbers over email or text.

6 – Watch out for phony web addresses

When searching, give the results a good look before clicking. Ask yourself if the website you want to click is legitimate—are there any red flags, like a strange URL, an unfamiliar name, a familiar brand name with an unusual addition to it, or a description that simply doesn't feel right when you read it. If so, don't click. They could be malware sites. Better yet, use a built-in browser advisor that helps you search and surf safely. It'll call out any known or suspected bad links clearly before you click.

7 – Make your meetings password protected

To ensure that only invited attendees can access your video or audio conference call, make sure your meeting is password protected. For maximum safety, activate passwords for new meetings, instant meetings, personal meetings, and people joining by phone. To keep users (either welcome or unwelcome) from taking control of your screen while you're video conferencing, select the option to block everyone except the host (you) from screen sharing.

8 – Watch out for phishing scams

If you receive an email asking to confirm your login credentials or that's asking for any personal info, go directly to the company's website or app—even if the email looks legitimate. Phishing attacks are getting more and more sophisticated, meaning that hackers are getting pretty good at making phishing emails look real. Don't open any attachments or click any links in these emails. Instead, check the status of your account at the site or in your app to determine the legitimacy of the request.

9 – Use two-factor authentication

Our banks, many of the online shopping sites we use, and numerous other accounts use two-factor authentication to make sure that we're logging in we really are who we say we are. In short, a username and password combo is an example of one-factor authentication. The second factor in the mix is something you, and only you, own, like your mobile phone. Thus when you log in and get a prompt to enter a security code that's sent to your mobile phone, you're taking advantage of two-factor authentication. If your IoT device supports two-factor authentication as part of the login procedure, put it to use and get that extra layer of security.

10 – Use a VPN

Another line of defense you can use to hamper hackers is a virtual private network (VPN), which allows you to send and receive data while encrypting your information so others can't read it. When your data traffic is scrambled that way, it's shielded from prying eyes, which helps protect your network and the devices you have connected to it. If you're working from home, check with your employer to see if they have a corporate VPN that you can use.

Stay even more secure with these free resources

Find out plenty more about working and schooling from home, health and well-being, in addition to articles on healthcare and dating online too. Drop by McAfee's Safer Together site for a wealth of free articles and resources.

Source: https://www.mcafee.com/blogs/consumer/top-ten-tips-for-protecting-your-identity-finances-and-security-online/

11. Twitter fined by EU data protection watchdog for GDPR breach

Ireland's Data Protection Commission fined Twitter €450,000 (~$550,000) for failing to notify the DPC of a breach within the 72-hour timeframe imposed by European Union's General Data Protection Regulation (GDPR) and to adequately document it.

The GDPR is a user and data privacy regulation that came into effect in the EU on May 25, 2018, and was quickly put to use following four separate complaints against Google, Facebook, Instagram, and WhatsApp on the same day over their use of "forced consent."

Based on GDPR rules, EU data regulators can impose maximum fines of up to €20 million (about $24.3 million) or 4% of the infringing company's annual global turnover – whichever is greater – for violations.

"The DPC's investigation commenced in January 2019 following receipt of a breach notification from Twitter and the DPC has found that Twitter infringed Article 33(1) and 33(5) of the GDPR in terms of a failure to notify the breach on time to the DPC and a failure to adequately document the breach," the Irish DPC said.

"The DPC has imposed an administrative fine of €450,000 on Twitter as an effective, proportionate, and dissuasive measure."

Breach caused by an Android app bug

The breach that led to Twitter getting fined today was caused by a four-year-old bug in the Twitter Android app responsible for the inadvertent exposure of protected accounts' private tweets.

"On 26 December 2018, we received a bug report through our bug bounty program that if a Twitter user with a protected account, using Twitter for Android, changed their email address the bug would result in their account being unprotected," the breach notification sent to the DPC on January 2019 said.

"This would render their previously protected Tweets (Tweets viewable by only approved followers of the account) public and viewable to anyone. The bug in the code was traced back to a code change made on 4 November 2014."

Twitter said that it didn't realize the severity of the issue and the breach until January 3, 2019, which is when the incident response process was activated.

However, as the EU watchdog underlined, even after this, Twitter failed to report the breach on time — within the 72-hour timeframe — given that it was only sent to the Commission on January 8.

The final decision, including details on Article 65 (dispute resolution) process leading to consultations with "all EU supervisory authorities were consulted as Concerned

Supervisory Authorities" (the first time since the GDPR was introduced), was published by the European Data Protection Board on its website [PDF].

Twitter fully supported the investigation

Twitter said today that it closely collaborated with the Irish DPC during the investigation which is probably one of the reasons behind why the data watchdog considered the €450,000 fine as "effective, proportionate and dissuasive."

"Twitter worked closely with the Irish Data Protection Commission to support their investigation," the company said today. "We have a shared commitment to online security and privacy, and we respect their decision, which relates to a failure in our incident response process."

"We appreciate the clarity this decision brings for companies and the public around the GDPR's breach notification requirements. As always, our approach to these incidents will remain one of committed transparency and openness."

In contrast with today's decision, Google was fined €100 million last week by the French data protection authority (CNIL) for "advertising cookies on the computers of users of the search engine google.fr, without obtaining prior consent and without providing adequate information."

Google was also fined €50 million in January 2019 for "lack of transparency, inadequate information and lack of valid consent regarding the ads personalization."

Source: https://www.bleepingcomputer.com/news/technology/twitter-fined-by-eu-data-protection-watchdog-for-gdpr-breach/

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

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.