telelink
BUSINESS SERVICES

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

Monthly Security Bulletin

September 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

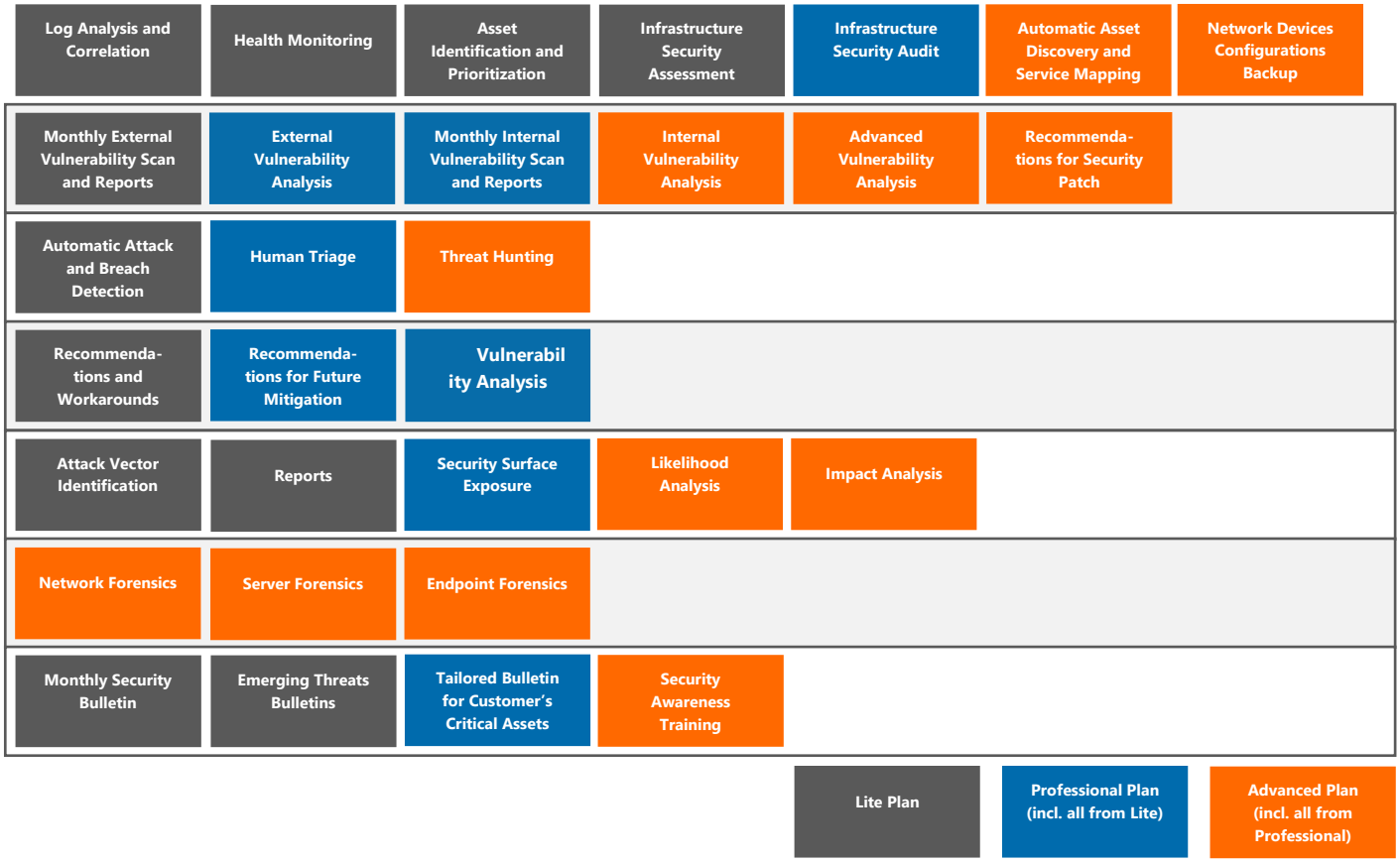
Start to mitigate cyber threats and minimize the risk!

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

1. Do You Have Enough Cloud Security? Use CIS Controls to Assess Yourself

Clients often ask me, "How do I know if I have 'enough' security in the cloud?" This is a great question because it shows a willingness to learn. The truth is that there is no right answer.

However, a simple place to begin is the basics. You should be sure you're covering the basics well and tracking them closely. This is why I am a huge fan of standards. While they are not the be-all and end-all for security, they give you an excellent place to start. One common set of standards are the Center for Internet Security's (CIS) top 20 controls, a prioritized list of 20 best practices that help organizations improve cybersecurity.

CIS Controls: Benchmarks for Cloud

Threat research shows that 65% of cloud security incidents are the result of customer misconfigurations. Why is this number so high? Because organizations are not getting the security basics right. This is where standards like

the CIS controls can provide an excellent benchmark for those foundations.

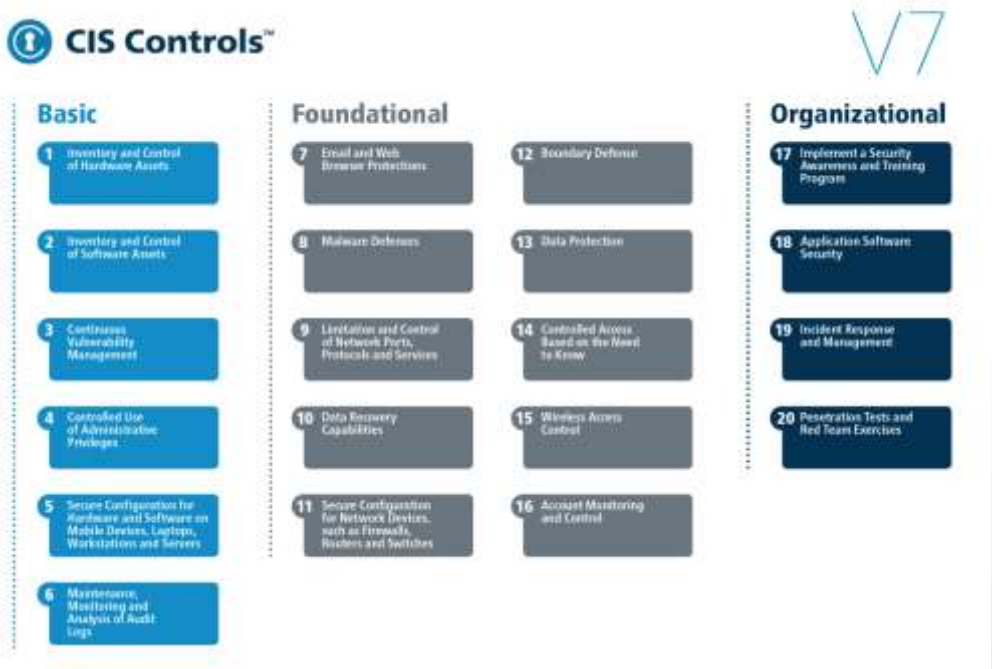


Figure 1: CIS 20 Critical Controls
Source: Center for Internet Security

This chart displays the top 20 CIS controls, divided into basic, foundational and organizational categories.

A great exercise for your cloud program is to map these 20 controls against what you have in place today. With the exception of control 15, Wireless Access Control, these are all relevant to varying degrees across infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) platforms.

Measure a Complete View of Cloud Security Using CIS 20

The trick for your security program is to measure as many of the 20 controls as possible using cloud native tooling. By cloud native, I mean platforms that integrate with multiple cloud service providers (CSPs), hybrid-cloud environments and common software development tools like CircleCI, GitHub and Jenkins.

Most security teams think of only the attack surface on the CSP, however the entire CI/CD pipeline is just as critical. This is why it's important to use security platforms that are completely integrated across all the major public cloud providers and development pipelines. Otherwise, you are only seeing a part of the picture. See figure 2 below.

This chart shows the role that a cloud native security platform plays in the full development lifecycle, providing visibility, help with compliance and governance, compute security, network protection and identity security.

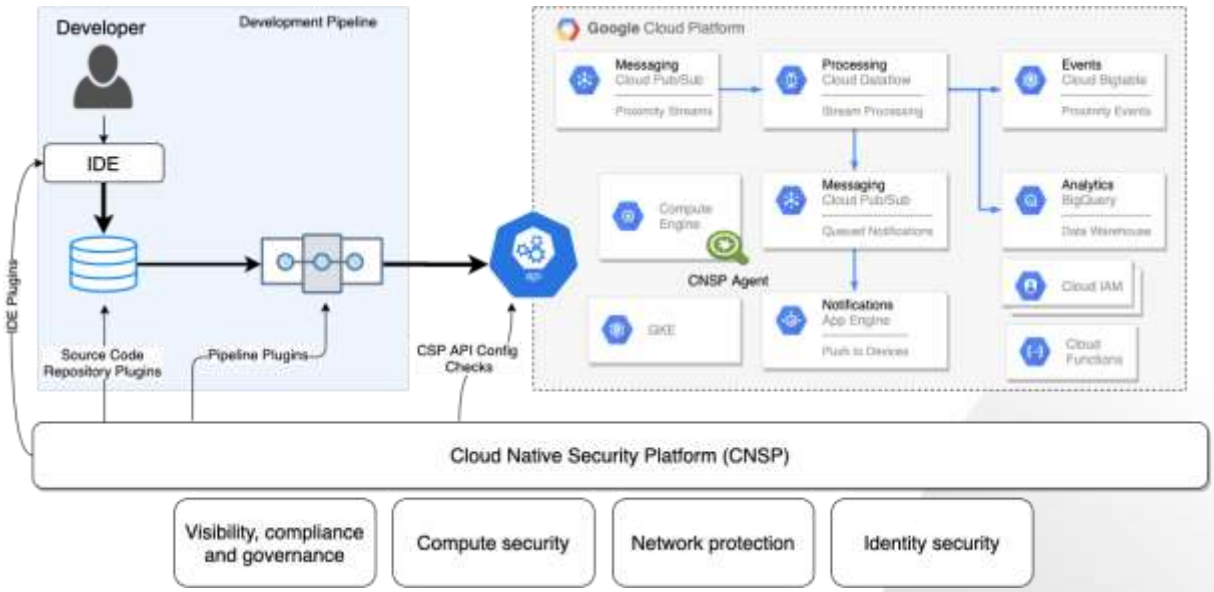


Figure 2: Full lifecycle, full stack and multi-cloud coverage from cloud native tooling

We know that most security programs lack this holistic view into the development pipeline thanks to the Spring 2020 Cloud Threat Report from Unit 42. Researchers analyzed hundreds of thousands of infrastructure as code (IaC) templates and came up

with some interesting findings. The most pertinent: nearly 200,000 insecure templates in use, 43% of cloud databases not being encrypted and 60% of cloud storage services with logging disabled. These numbers illustrate why it's important to examine your entire cloud stack when assessing your cloud security.

Figure 3: Lack of visibility into the development pipeline
Source: unit42.paloaltonetworks.com/cloud

The chart displays key figures from the Spring 2020 Cloud Threat Report from Unit 42: Nearly 200K insecure templates in use, 43% of cloud databases not encrypted, 60% of cloud storage services have logging disabled.

How to Apply CIS Controls to Cloud Development

So how do you apply the CIS 20 to your entire cloud stack? The first thing I recommend is reading through the CIS Controls Cloud Companion Guide. The guide will help you create metrics for each control, decide what end result you're looking for and begin to work backward to determine where and how to collect data.

Figure 4: Example of a spreadsheet for tracking the CIS 20 in the Cloud

This spreadsheet shows an example of how you might translate the top 20 CIS controls into metrics you can track within your organization.

Again, it's important to keep the entire cloud stack in mind. Don't just focus on the CSP but be sure to include your entire development pipeline. These 20 critical controls should evenly apply across the stack.

Don't expect to have this process perfect overnight. A great way to test this out would be to make these metrics a key requirement for any proofs of concept your team is likely running on cloud native security platforms (CNSPs). **The key question is will the CNSP enable you to track these metrics over time and take corrective action when necessary?**

How Much Is Enough Cloud Security?

In my view, you can only begin to answer the question of whether you have "enough" cloud security by first covering the basics. Step number two – and the key to long term success in the cloud – then comes by measuring the controls consistently over time across the entire stack. Combined, these give you a better sense of your overall posture, and can inform whether your current controls are enough.

You can see real-world data on how thousands of other companies are securing their cloud native stacks in the State of Cloud Native Security 2020 survey.

The post Do You Have Enough Cloud Security? Use CIS Controls to Assess Yourself appeared first on Palo Alto Networks Blog.

Source: https://blog.paloaltonetworks.com/2020/08/cloud-cis-controls/

2. Copying a Key by Listening to It in Action

Researchers are using recordings of keys being used in locks to create copies.

Once they have a key-insertion audio file, SpiKey's inference software gets to work filtering the signal to reveal the strong, metallic clicks as key ridges hit the lock's pins [and you can hear those filtered clicks online here]. These clicks are vital to the inference analysis: the time between them allows the SpiKey software to compute the key's inter-ridge distances and what locksmiths call the "bitting depth" of those ridges: basically, how deeply they cut into the key shaft, or where they plateau out. If a key is inserted at a nonconstant speed, the analysis can be ruined, but the software can compensate for small speed variations.

The result of all this is that SpiKey software outputs the three most likely key designs that will fit the lock used in the audio file, reducing the potential search space from 330,000 keys to just three. "Given that the profile of the key is publicly available for commonly used [pin-tumbler lock] keys, we can 3D-print the keys for the inferred bitting codes, one of which will unlock the door," says Ramesh.

Source: https://www.schneier.com/blog/archives/2020/08/copying_a_key_b.html

3. Vaccine for Emotet Malware

Interesting story of a vaccine for the Emotet malware:

Through trial and error and thanks to subsequent Emotet updates that refined how the new persistence mechanism worked, Quinn was able to put together a tiny PowerShell script that exploited the registry key mechanism to crash Emotet itself.

The script, cleverly named EmoCrash, effectively scanned a user's computer and generated a correct -- but malformed -- Emotet registry key.

When Quinn tried to purposely infect a clean computer with Emotet, the malformed registry key triggered a buffer overflow in Emotet's code and crashed the malware, effectively preventing users from getting infected.

When Quinn ran EmoCrash on computers already infected with Emotet, the script would replace the good registry key with the malformed one, and when Emotet would re-check the registry key, the malware would crash as well, preventing infected hosts from communicating with the Emotet command-and-control server.

The Binary Defense team quickly realized that news about this discovery needed to be kept under complete secrecy, to prevent the Emotet gang from fixing its code, but they understood EmoCrash also needed to make its way into the hands of companies across the world.

Compared to many of today's major cybersecurity firms, all of which have decades of history behind them, Binary Defense was founded in 2014, and despite being one of the industry's up-and-comers, it doesn't yet have the influence and connections to get this done without news of its discovery leaking, either by accident or because of a jealous rival.

To get this done, Binary Defense worked with Team CYMRU, a company that has a decades-long history of organizing and participating in botnet takedowns.

Working behind the scenes, Team CYMRU made sure that EmoCrash made its way into the hands of national Computer Emergency Response Teams (CERTs), which then spread it to the companies in their respective jurisdictions.

According to James Shank, Chief Architect for Team CYMRU, the company has contacts with more than 125 national and regional CERT teams, and also manages a mailing list through which it distributes sensitive information to more than 6,000 members. Furthermore, Team CYMRU also runs a biweekly group dedicated to dealing with Emotet's latest shenanigans.

This broad and well-orchestrated effort has helped EmoCrash make its way around the globe over the course of the past six months.

Either by accident or by figuring out there was something wrong in its persistence mechanism, the Emotet gang did, eventually, changed its entire persistence mechanism on Aug. 6 -- exactly six months after Quinn made his initial discovery.

EmoCrash may not be useful to anyone anymore, but for six months, this tiny PowerShell script helped organizations stay ahead of malware operations -- a truly rare sight in today's cyber-security field.

Source: https://www.schneier.com/blog/archives/2020/08/vaccine_for_emo.html

4. Drovorub Malware

The FBI and NSA have published today a joint security alert containing details about a new strain of Linux malware that the two agencies say was developed and deployed in real-world attacks by Russia's military hackers.

The two agencies say Russian hackers used the malware, named Drovorub, was to plant backdoors inside hacked networks.

Based on the evidence the two agencies have collected, FBI and NSA officials claim the malware is the work of APT28 (Fancy Bear, Sednit), a codename given to the hackers operating out of military unity 26165 of the Russian General Staff Main Intelligence Directorate (GRU) 85th Main SpecialService Center (GTsSS).

Through their joint alert, the two agencies hope to raise awareness in the US private and public sectors so IT administrators can quickly deploy detection rules and prevention measures.

Drovorub: APT28's swiss-army knife for hacking Linux

Per the two agencies, Drovorub is a multi-component system that comes with an implant, a kernel module rootkit, a file transfer tool, a port-forwarding module, and a command-and-control (C2) server.

"Drovorub is a 'swiss-army knife' of capabilities that allows the attacker to perform many different functions, such as stealing files and remote controlling the victim's computer," McAfee CTO, Steve Grobman, told ZDNet in an email today.

"In addition to Drovorub's multiple capabilities, it is designed for stealth by utilizing advanced 'rootkit' technologies that make detection difficult," the McAfee exec added. "The element of stealth allows the operatives to implant the malware in many different types of targets, enabling an attack at any time."

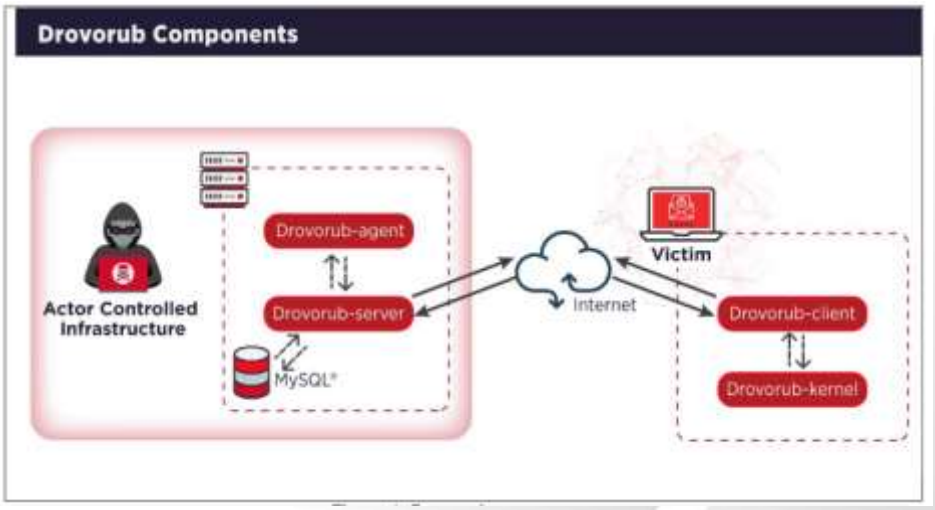


Image: FBI and NSA

"The United States is a target-rich environment for potential cyber-attacks. The objectives of Drovorub were not called out in the report, but they could range from industrial espionage to election interference," Grobman said.

"Technical details released today by the NSA and FBI on APT28's Drovorub toolset are highly valuable to cyber defenders across the United States."

To prevent attacks, the agency recommends that US organizations update any Linux system to a version running kernel version 3.7 or later, "in order to take full advantage of kernel signing enforcement," a security feature that would prevent APT28 hackers from installing Drovorub's rootkit.

The joint security alert [PDF] contains guidance for running Volatility, probing for file hiding behavior, Snort rules, and Yara rules -- all helpful for deploying proper detection measures.

Some interesting details we gathered from the 45-page-long security alert:

The name Drovorub is the name that APT28 uses for the malware, and not one assigned by the NSA or FBI.

The name comes from drovo [дрово], which translates to "firewood," or "wood" and rub [руб], which translates to "to fell," or "to chop."

The FBI and NSA said they were able to link Drovorub to APT28 after the Russian hackers reused servers across different operations. For example, the two agencies claim Drovorub connected to a C&C server that was previously used in the past for APT28 operations targeting IoT devices in the spring of 2019. The IP address had been previously documented by Microsoft.

Source: https://www.zdnet.com/article/fbi-and-nsa-expose-new-linux-malware-drovorub-used-by-russian-state-hackers/

5. Don't Remove Stalkerware Before Reading This Article

Stalkerware is technically software with malicious intent, but security professionals should treat it as a different beast from other malware.

Stalkerware is an app or apps that someone else can install on your device to intercept text messages and phone calls, send call logs, record web browsing activity and keystrokes and even access your location. And stalkerware — a tool often associated with abuse and domestic violence — can be a risk to enterprise data and security in general. Given the difficult nature of detecting stalkerware, and the risk of retaliation by abusers, what can an employer do to protect their employees as well as their company's data?

How is Stalkerware Unique?

Stalkerware isn't usually thought of as a major risk to an enterprise. However, it is considered a major threat because it can extract sensitive data from an individual or an enterprise without their consent or knowledge. Plus, anyone with access to commercially available spyware can partake in stalkerware activities.

Stalkerware isn't as clearly defined as other traditional forms of malware, such as phishing, and, it is difficult to detect. Confusion over the legality of stalkerware has also made it difficult to prosecute, partially because there is no steadfast, legitimate way to obtain forensic evidence that it is happening. Abuse and harassment are hazier from a legal perspective, and what counts as breaking the law can differ from one jurisdiction to the next. Proving harm based on these in a court of law can be a much more difficult task than proving harm in the case of financial crimes.

Adding to the problem, victims are frequently blamed for being a target of abuse.

Shades of Grayware

With the blurry legal lines around abuse and harassment, what counts as stalkerware is equally fuzzy. Many of the tools abusers use to control their victims are hijacked accounts and legitimate software. This activity isn't something you can detect with traditional anti-malware software. As an employer, there is little you can do to identify or protect employees from this.

Misuse of legitimate software is not the only way abusers can spy on victims through their devices. Applications that straddle the border of being legitimate are considered tools rather than weapons. This grayware is often detected as potentially unwanted software by anti-malware vendors.

Many of these stalkerware apps are advertised as services for 'employee monitoring.' Because personal monitoring software is not illegal in most jurisdictions, it's very easy to find apps that market themselves in this way. And it's not just shadowy corners of the web where you can find these things; a quick internet search shows how easily they can be found on the official Apple and Google app stores.

Detection of these 'potentially unwanted' stalkerware apps can be difficult. Users need to turn on specific settings on their devices that are not enabled by default in order for malware to flag them. Confusingly, as this Wired post notes, some anti-malware software refers to items detected with these settings as 'not a virus' or something similarly ambiguous. This vague wording may lead people to ignore the warning.

Listen to Employees

How best to protect employees and company data from this can differ depending on whether or not the company has provided the device. More than anything, it's critical to remember that this is a very personal and possibly violent crime. The safety of your employee is the ultimate goal.

Remember, it's not the victim's fault they were targeted. The abuser may have forced or coerced them into sharing their password, or into giving them access to the compromised device. Asking a victim to do security training is not going to correct this, as it is not a lack of knowledge that caused the problem.

Questions to Ask If You Find Stalkerware

Whereas with regular malware you can simply remove or quarantine a malicious file, with stalkerware you'll need to take a more hands-on approach. What should happen next will depend on the answer to a couple of questions:

Is it the employee's device or the company's?

If the device was provided by your company, you can proactively prevent some stalkerware installation by allowing only pre-approved software. If stalkerware is detected on a company device, you'll still need to talk with the employee about what you've found. You may wish to offer the option of a replacement device that has been locked down to prevent re-infection, keeping the affected device powered down and in a safe place.

If the device belongs to your employee, you must speak with the employee before performing removal actions. Listen carefully to them, and work with them to find a safe and secure way to proceed.

Is the detection before or after installation?

If the detection was before installation, you can safely quarantine the file. Keep in mind that this file and detection logs may be considered evidence that must be kept if the victim chooses to pursue legal action.

If the detection was after installation, whether or not it was on a company device, you need to speak with the employee in person first. Do not notify them in a way that could be intercepted on the compromised device. If the employee feels that removing the stalkerware app may put them in greater danger, do not remove it without their permission.

While you may be worried about the risks to data security with regards to stalkerware, this is minor compared with the physical safety risk to the person being targeted. It's possible to work with your employee to address these concerns in a way that protects their safety as well.

The post Don't Remove Stalkerware Before Reading This Article appeared first on Security Intelligence.

Source: https://securityintelligence.com/articles/stalkerware-apps-employee/

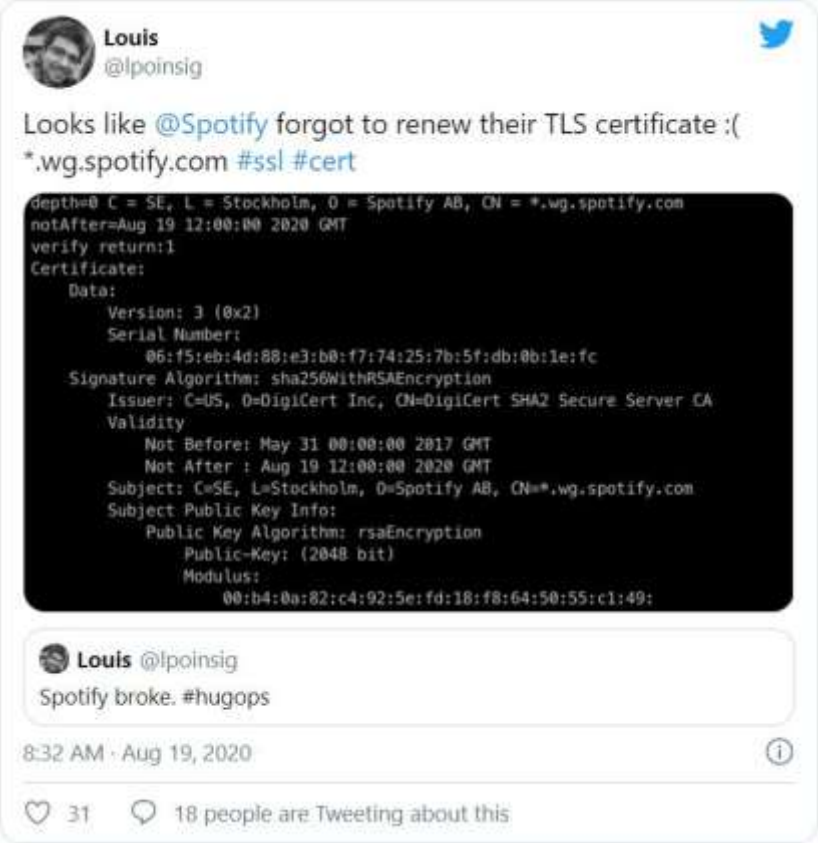
6. Spotify hit with outage after forgetting to renew a certifficate

Spotify was hit with a brief outage today after they forgot to renew a certificate used as part of their service.

At approximately 8 AM EST today, Spotify users began to report on Twitter that they were unable to connect to the service and it would just display an error stating it "Couldn't load the page".

According to Cloudflare network engineer Louis Poinsignon, a wildcard certificate for the Spotify hostname *.wg.spotify.com had not been renewed and expired.

The expired certificate would cause Spotify services that communicate with these hosts to have issues, which likely led to the outage.



An hour later, Poinsignon stated that the certificate was renewed again, and at that same time, Spotify's official support account tweeted that the service had been restored.

Unfortunately, outages and problems caused by expired certificates are becoming more common as most services have switched over to secure connections.

Earlier this month, a certificate expired for California's CalREDIE infectious disease reporting and monitoring system that led to an underreporting of COVID-19 cases in the state.

In the past, we have also seen expired certificates affect services such as Facebook's Tor server, Microsoft Teams, and IoT devices.

Source: https://www.bleepingcomputer.com/news/technology/spotify-hit-with-outage-after-forgetting-to-renew-a-certifficate/

7. Lucifer cryptomining DDoS malware now targets Linux systems

A hybrid DDoS botnet known for turning vulnerable Windows devices into Monero cryptomining bots is now also scanning for and infecting Linux systems.

While the botnet's authors named it Satan DDoS, security researchers are calling it Lucifer to differentiate it from Satan ransomware.

Besides adding Linux targeting support, Lucifer's creators have also expanded the Windows version's capabilities to steal credentials and escalate privileges using the Mimikatz post-exploitation tool.

When it was first spotted by Palo Alto Networks Unit 42 researchers in May, the malware was deploying an XMRig miner on Windows computers infected using weaponized exploits targeting high and critical severity vulnerabilities or by brute-forcing machines with TCP ports 135 (RPC) and 1433 (MSSQL) open.

Similar capabilities to the Windows version

As detailed in a report published today by researchers at NETSCOUT's ATLAS Security Engineering & Response Team (ASERT), the Linux port — uploaded on VirusTotal on July 9, 2020 — displays the same welcome message as the Windows variant.

The new Linux version comes with capabilities similar to the Windows counterpart, including modules designed for cryptojacking and for launching TCP, UCP, and ICMP-based flooding attacks.

Additionally, Lucifer-infected Linux devices can also be used in HTTP-based DDoS attacks (including HTTP GET- and POST-floods, and HTTP 'CC' DDoS attacks).

"The fact that it can run on Linux-based systems means that it can potentially compromise and make use of high-performance, high-bandwidth servers in internet data centers (IDCs), with each node packing a larger punch in terms of DDoS attack capacity than is typical of most bots running on Windows or IoT-based Linux devices," the NETSCOUT researchers explained.

The full list of DDoS attacks that can be launched using Lucifer infected devices is available in the table embedded below.

Attack type	DDoS attack
Volumetric	TCP_Flood - TCP packets with SYN and ACK bits set, source IP, and port spoofed

	UDPFlood - UDP packets with packet payload size set by the attacker
	DK_Flood - UDP packets with packet payload size set by the attacker
	WZUDP_Flood - UDP packets with source IP and port spoofed
	ICMPFlood - ICMP ping request packets with payload size set by the attacker
State Exhaustion	SYNFlood - TCP packets with SYN bit set, source IP, and port spoofed
	Tcp - TCP packets with SYN bit set
Application Level Attacks	Get_CC - HTTP GET request, URL, Referer, and Host headers set by attacker
	Post_CC - HTTP POST, URL, and Host header set by attacker
	postattack - HTTP POST, URL, and Host header set by attacker
	CCAttack - HTTP GET request, URL, and Host header set by attack
	MNAttack - HTTP GET request, URL, and Host header set by attack; REMOTE_ADDR, HTTP_CLIENT_IP, and HTTP_X_FOR headers are spoofed
	HEAD - HTTP HEAD request, URL, and Host header set by attacker; Referer is set by the bot.

Increasingly dangerous cross-platform botnet

By adding support for additional platforms, Lucifer's authors are making sure that they can expand the total number of devices controlled by their botnet.

This translates into a lot more cryptocurrency being mined by the botnet in the future — in May when it was first spotted, Lucifer's cryptocurrency wallets contained only $30

worth of Monero — , as well as more dangerous DDoS attacks being launched against potential targets.

"At first blush, a hybrid cryptojacker/DDoS bot seems a bit unusual. However, given the prevalence of DDoS attacks within the illicit cryptomining arena, it makes a weird kind of sense to have a 'one-stop' bot," the researchers concluded.

"This allows controllers to fulfill their needs in one fell swoop rather than forcing them to use booter/stresser services or other DDoS botnets to foil the progress of their rival miscreants."
Source: *https://www.bleepingcomputer.com/news/security/lucifer-cryptomining-ddos-malware-now-targets-linux-systems/*

8. FritzFrog Botnet Attacks Millions of SSH Servers

The unique, advanced worming P2P botnet drops backdoors and cryptominers, and is spreading globally.

A peer-to-peer (P2) botnet called FritzFrog has hopped onto the scene, and researchers said it has been actively breaching SSH servers since January.

SSH servers are pieces of software found in routers and IoT devices, among other machines, and they use the secure shell protocol to accept connections from remote computers. SSH servers are common in enterprise and consumer environments alike.

According to an analysis from Guardicore Labs, FritzFrog propagates as a worm, brute-forcing credentials at entities like governmental offices, educational institutions, medical centers, banks and telecom companies. FritzFrog has attempted to compromise tens of millions of machines so far, and has successfully breached more than 500 servers in total, Guardicore researcher Ophir Harpaz said. Victims include well-known universities in the U.S. and Europe, and a railway company; and the most-infected countries are China, South Korea and the U.S.

"FritzFrog executes a worm malware which is written in Golang, and is modular, multi-threaded and fileless, leaving no trace on the infected machine's disk," Harpaz explained, in a posting on Wednesday. Once the server is compromised, "the malware creates a backdoor in the form of an SSH public key, enabling the attackers ongoing access to victim machines."

It also can drop additional payloads, such as cryptominers.

Swimming in a Unique Pond

FritzFrog is a P2P botnet, meaning that it has greater resiliency than other types of botnets because control is decentralized and spread among all nodes; as such, there's no single point-of-failure and no command-and-control server (C2).

"FritzFrog is completely proprietary; its P2P implementation was written from scratch, teaching us that the attackers are highly professional software developers," Harpaz said. She added, "The P2P protocol is completely proprietary, relying on no known P2P protocols such as µTP."

As far as the other technical details go, Guardicore analyzed the botnet by injecting its own nodes into the mix, giving researchers the ability to participate in the ongoing P2P traffic and see how it was built.

They discovered that almost everything about FritzFrog is unique when compared with past P2P botnets: Harpaz noted that it doesn't use IRC like IRCflu; it operates in-memory unlike another cryptomining botnet, DDG; and runs on Unix-based machines unlike others like the InterPlanetary Storm botnet.

Additionally, its fileless payload is unusual. Harpaz wrote that files are shared over the network to both infect new machines and run new malicious payloads on compromised ones – and that this is accomplished completely in-memory using blobs.

"When a node A wishes to receive a file from its peer, node B, it can query node B which blobs it owns using the command getblobstats," according to the researcher. "Then, node A can get a specific blob by its hash, either by the P2P command getbin or over HTTP, with the URL http://:1234/. When node A has all the needed blobs – it assembles the file using a special module named Assemble and runs it."

One the malware is installed on a target by this method, it begins listening on port 1234, waiting for initial commands that will sync the victim with a database of network peers and brute-force targets. Once this initial syncing is finished, FritzFrog gets creative on the evasion-detection front when it comes to further communication from outside the botnet: "Instead of sending commands directly over port 1234, the attacker connects to the victim over SSH and runs a netcat client on the victim's machine," according to the analysis. "From this point on, any command sent over SSH will be used as netcat's input, thus transmitted to the malware."

Meanwhile, the botnet constantly updates itself with databases of targets and breached machines as it worms through the internet - "Nodes in the FritzFrog network keep in close contact with each other," Harpaz noted. "They constantly ping each other to verify connectivity, exchange peers and targets and keep each other synced. The nodes participate in a clever vote-casting process, which appears to affect the distribution of brute-force targets across the network. Guardicore Labs observed that targets are evenly

distributed, such that no two nodes in the network attempt to 'crack' the same target machine."

Further, it was built with an extensive dictionary of breached names and passwords for brute-forcing purposes, making it highly aggressive ("By comparison, DDG, a recently discovered P2P botnet, used only the username 'root,'" said Harpaz).

The malware also spawns multiple threads to perform various tasks simultaneously. For instance, an IP address in the target queue will be fed to a Cracker module, which in turn will scan the machine attached to the IP address and try to brute-force it; a machine which was successfully breached is queued for malware infection by the DeployMgmt module; and a machine which was successfully infected will be added to the P2P network by the Owned module.

In the event of a reboot of the compromised system, the malware leaves a backdoor behind, whose login credentials are saved by the network peers.

"The malware adds a public SSH-RSA key to the authorized_keys file," according to the research. "This simple backdoor allows the attackers – who own the secret private key – for passwordless authentication, in case the original password was modified."

The malware also monitors the file system state on infected machines, periodically checking for available RAM, uptime, SSH logins and CPU-usage statistics. Other nodes take this information and uses it to determine whether to run a cryptominer or not.

If it decides to run a cryptominer, the malware runs a separate process called "libexec" to mine the Monero cryptocurrency with an XMRig spinoff. Though this secondary infection is what the botnet has so far been used for, its architecture means that it could also install any other type of malware on infected nodes, should its authors decide to do so.

In all, FritzFrog is highly advanced, Harpaz said, but there's a simple way to ward off a compromise: "Weak passwords are the immediate enabler of FritzFrog's attacks," she said. "We recommend choosing strong passwords and using public key authentication, which is much safer."

Admins should also remove FritzFrog's public key from the authorized_keys file, preventing the attackers from accessing the machine, she said. And, "routers and IoT devices often expose SSH and are thus vulnerable to FritzFrog; consider changing their SSH port or completely disabling SSH access to them if the service is not in use."

Source: https://threatpost.com/fritzfrog-botnet-millions-ssh-servers/158489/

9. Stolen Data: The Gift That Keeps on Giving

Users regularly reuse logins and passwords, and data thieves are leveraging that reality to breach multiple accounts.

By now, we have all received at least one email disclosing to us that the personal information we provided to an organization was leaked or stolen. It could have been a social media platform, a bank, or a fast-food chain (Drizly, an alcohol delivery service, was one of the latest to announce a breach). Seemingly no industry has been exempt from data breaches, inadvertent leaks, or misconfigurations by the governing body to date.

Since LinkedIn's notable 2012 breach affecting 170 million users, we have seen many other significant security incidents exposing massive amounts of user data. Sometimes it's billions of accounts — billions! For example, in 2019, researcher Bob Diachenko discovered an unsecured Elasticsearch server that leaked records related to 1.2 billion people.

Considering the amount of publicity these incidents receive, does the data from well-known mega-breaches have any value within the underground economy, and do end users continue to be affected today? Many people may be surprised by the answer.

In most scenarios, organizations follow guidelines of responsible disclosure in the event of a data breach or cybersecurity incident. This may look like offering complimentary breach remediation, perhaps by third-party remediation or credit-monitoring services such as Tri-Credit bureau organizations. This is typically followed up with recommendations for end users to change the credentials affected. And then the organization itself resets, locks, or removes the impacted leaked data rendering it unusable, and end users reset their own passwords … right?

Data from Highly Publicized Breaches Are Valuable Today

Remember these?

- 2014: Yahoo (3 billion)
- 2017: Equifax (163 million)
- 2018: Under Armour (150 million), Panera Bread (37 million)
- 2019: Verifications.io (200 million), Canva (140 million), Zynga (173 million)

A majority of this leaked data, and more, continues to be readily available for little to no cost, found within commodity-based threat actor forums or open source intelligence environments, or recycled in forums and sold as smaller unique datasets, pivoting off the original leaked datasets, and leveraging the users' password reuse on other third-party accounts.

For example, researchers at Vigilante obtained 100 Citibank user accounts — completely valid credentials — belonging to valid Citibank customers. These credentials

are directly from well-known breaches not related to a Citibank breach. In other words, threat actors took data from well-known, highly commoditized leaks and targeted other possible accounts those users might have, such as Citibank, by testing the credentials for a match.

This is easily accomplished via well-known and easy-to-obtain cybercrime tools such as Private Keeper. This tool is touted as requiring no knowledge of programming skills and uses a simple and intuitive graphical user interface, highly capable of brute-forcing credentials. With such ease of use and lowered technological sophistication, this certainly broadens the threat-actor population who are willing to engage in cybercrime activity in order to turn a buck — most certainly endangering all online brands.

The Elephant in the Room

Today, there may be a lack of collaboration between organizations that represent midsize to large ecosystems of users, for example. That is to say, it does not appear that third-party organizations unrelated to a mega-breach are monitoring for leaks, cross-comparing their user base, or identifying their own users of the mega-breach and forcing password resets of their own user, considering the high probability of password reuse.

When mega-leaks occur, many other ecosystems become endangered due to the tendency of users to reuse the same credentials on other sites. Not only well-known brands but even small to midsize organizations with an online presence should consider the issue of password reuse stemming from previous mega-leaks as a primary threat vector.

While I do believe organizations that are breached continue to monitor for attribution around the leak, and they work to remediate their own users to the best of their ability, other satellite organizations may not confirm if their end users have reused the credentials of their infrastructure.

How We Shift Away from Account Takeovers Due to Breaches

We know that threat actors tend to leverage the simplest threat vectors and unsophisticated password-reuse campaigns, which tend to be the most successful and profitable campaigns for cybercriminals. Despite this, most end users have stopped paying much attention to new data breaches. Individuals are not proactively working to protect their accounts in the easiest ways possible.

This means that when mega-breaches occur, the leak affects not only the breached organization but all other online ecosystems that share the same user base. And threat actors will continue to leverage massive data leaks to compromise user accounts at other online ecosystems, in addition to reselling it.

My vision for the future is that organizations with personal data should work as a collective. When a breach occurs at one organization, all organizations should be

enforcing new credentials and rejecting known compromised credentials. This can help to curb account takeover, fraud, and misrepresentation. We have seen that account credentials from eight years ago are being reused today. Organizations should potentially consider evaluating well known breaches of correlations between their own ecosystem and well-known breaches, remediating matches, not only enforcing step-up authentication challenges in the login process but also enforce users of formerly known data leaks to leverage two-factor authentication.

Source: https://www.darkreading.com/attacks-breaches/stolen-data-the-gift-that-keeps-on-giving/a/d-id/1338645

10. ICS Vulnerability Reports Rapidly Rise

More scrutiny of products for industrial control systems is expected to expose even more weaknesses in devices that run critical infrastructure.

It started in January with an industrial control systems (ICS) hacking contest in Miami amid a sudden cold front that literally paralyzed and felled some of the city's tree-clinging iguana population. Inside a room adjacent to the lobby of South Beach's historic Fillmore theatre and safe from the elements (and falling lizards), security researchers hacked SCADA gateways, control servers, human-machine interfaces (HMIs), an engineering workstation, and other ICS software in the first-ever ICS Pwn2Own contest.

That the 25 ICS product entries were successfully hacked came as no big surprise since many ICSs, especially products from newcomer vendors, notoriously lack security features and contain insecure software. The event, run by Trend Micro's Zero-Day Initiative (ZDI) as part of the annual S4x20 ICS conference, had been expected to open the floodgates for more researcher scrutiny of ICS products - and new data published today shows that's exactly what ensued.

In the first half of 2020, there were 10.3% more ICS vulnerabilities reported in the National Vulnerability Database (NVD) and an increase of 32.4% of ICS-CERT advisories for vulns compared with one year earlier. More than 75% of the ICS flaws reported this year were rated high or critical, according to a report from ICS security firm Claroty. More than 70% of ICS flaws reported in the first half of 2020 are remotely exploitable, 365 ICS flaws landed in the NVD, and 139 advisories came via ICS-CERT, the data shows.

This is just the tip of the iceberg now that more researchers are training their hacking chops on ICS products in the wake of the January contest, while more new ICS vendors are entering the market, according to Amir Preminger, vice president of research at Claroty, who also competed in the ICS Pwn2Own. The contest awarded a total of $280,000 in prize money to the winning teams.

Preminger expects many more ICS vulns to be reported publicly by the end of the year.

"We are going to witness a bigger spike as we go because of COVID," he says, which leaves critical infrastructure systems more at risk of attack given the heavier reliance on those systems as more people stay at home and work from home in the pandemic. Attention has also gone to helping OT organizations better secure their critical infrastructure systems, with the recent joint advisory from the US Department of Homeland Security's CISA and the National Security Agency, as well as an executive order issued by the White House earlier this year, he notes.

Look for more vulnerabilities and fixes in the second half, Preminger says.

The ICS flaws exposed this year were found in products used in critical infrastructure: The report shows that of the 385 flaws included in the security advisory, 236 affect the energy sector, 197 affect critical manufacturing, and 171 affect water and wastewater. That's an increase of 58.9% for energy, 87.3% for critical manufacturing, and 122% for water and wastewater over the same period in 2019.

"When you see so many remote control execution [flaws], that actually correlates with the fact you have a lot of newcomers [vendors]," Preminger says. Some of these vendors have no secure development life cycle program, and "some of these products never undergo any security review before releasing," he adds.

Dale Peterson, CEO of Digital Bond and head of the S4 conference, also points out that the data in Claroty's report mainly reflects researchers' intensified efforts in finding flaws in ICS systems.

"It's not reflecting risk to the ICS community, not reflecting that things are being more or less vulnerable," he says. "It doesn't change the risk profile or what asset owners do."

Just how a product gets remediated for a security flaw depends on whether fixing it would break a function or disrupt an industrial process.

"There are cases where vulnerabilities are in some isolated part of the application and you change [fix] it and it doesn't affect anything," Peterson explains. "There are other issues buried down deep so that if you make that change, a bunch of things are not going to work, so you can't just out a patch without breaking the system."

It can take anywhere from a month to a three months for a researcher to achieve remote code execution exploiting an ICS vulnerability, Preminger says. "It's not an 'if' but a 'when'" for an attacker to do the same, he notes.

"The bigger risk of COVID is ... what we saw in remote access vulns in ICS products," he says.

For industrial organizations, it's all about awareness of their ICSs' security holes and ensuring they are sitting securely on the network and not inadvertently exposed to the public Internet.

"Unfortunately, you still see a lot of them directly connected to the Internet," Preminger says. "Some of them are old and they just leave it on the Internet, and some are new and should not be connected, even if that device doesn't have a CVE. Attackers could use it for a botnet" or as a way to break into the network.

Patching isn't always the solution for OT organizations, of course, so it's matter of mapping out risk to the network.

"We're trying to advise customers how to better build their networks in terms of segmentation or layers," Preminger says. "Leveraging this [vuln] data, they can better design what they have up front or [determine] where to thicken their security layer against other vulnerabilities. They can better prioritize."

Of the 365 ICS vulns reported in the first half of 2020, 26 were discovered by Claroty, and more than half of those flaws are remotely exploitable.

Source: https://www.darkreading.com/risk/ics-vulnerability-reports-rapidly-rise/d/d-id/1338699

11. Newly Patched Alexa Flaws a Red Flag for Home Workers

Alexa could serve as an entry point to home and corporate networks. Security experts point to the need for manufacturers to work closely with enterprise security teams to spot and shut down IoT device flaws.

A trio of vulnerabilities recently found in Alexa devices that could have led to broader attacks on home and corporate networks have been patched in a software update by Amazon.

The vulnerabilities, which were made public last week by researchers at Check Point, raised red flags given the many millions of people now working from home because of the pandemic.

More than 200 million Alexa smart-home devices have shipped to date, according to multiple sources. The vulnerabilities, which could be exploited by clicking on a bad link filled with malicious code, could have exposed personal user info, including banking data histories, usernames, phone numbers, and home addresses.

Oded Vanunu, head of Check Point's product vulnerability research, says security pros should be concerned about the Alexa vulnerabilities because most home users don't have basic network security, such as network segmentation, in place.

"An Alexa account can serve as a gateway to the home network and be used as a base to launch other attacks," Vanunu says. "While segmenting the network is a good idea, it's a lot to ask of the typical home user."

Brandon Hoffman, CISO at Netenrich, agrees that placing the onus on consumers to do more extensive management of the network doesn't make sense.

"Rather, device manufacturers have to recognize that the work-from-home shift puts a greater focus on home equipment, and they have a responsibility to the consumer base to take proper measures in closing vulnerabilities and providing security guidance along with more robust security options for savvy users," Hoffman says.

Hank Schless, senior manager of security solutions at Lookout, says security teams need to understand that traditional tools do not protect their employees from this type of attack. Even if security pros deploy a VPN, multifactor authentication, and mobile device management, none of that will stop an employee from tapping on a convincing phishing link and giving up their corporate login credentials or introducing malware into the corporate infrastructure.

"In the case of a consumer app, app developers need to integrate security into their app to protect their customers from malware," Schless says. "App developers and security teams need to work together to integrate security measures into their mobile apps that protects the user."

Check Point presented the vulnerabilities to Amazon in June. The company was receptive to the research and patched the vulnerabilities right away, Vanunu says. In recent months, Check Point has also conducted security research on TikTok, WhatsApp, and Fortnite.

"Alexa has concerned us for a while now, given its ubiquity and connection to IoT devices," Vanunu says. "We hope manufacturers of similar devices will follow Amazon's example and check their products for vulnerabilities that could compromise users' privacy."

The Vulns

Check Point's researchers found that certain Amazon/Alexa subdomains were vulnerable to Cross-Origin Resource Sharing (CORS) misconfigurations and Cross Site Scripting (XSS). Using XSS, the researchers were also able to get the cross-site request forgery (CSRF) token and perform actions on the victim's behalf.

Vanunu said a single click by a victim triggers the three vulnerabilities: First, the XSS vulnerability in one of Amazon's subdomains enables access to the victims' identification cookies. Second, once access is gained, both the CORS misconfiguration and the CSRF token can be exploited, and, third, actions can be performed on behalf of victims on their Alexa accounts.

A CSRF token is a unique, secret, unpredictable value that's generated by the server-side application and transmitted to the client in such a way that it's included in a subsequent HTTP request made by the client. Vanunu says these exploits could let an attacker remove or install Alexa skills (apps) on a targeted victim's Alexa account, access the person's voice history, and acquire personal information.

While Vanunu reiterated that prevention was mostly the burden of the manufacturer, users can take certain steps to protect their Alexa accounts. For starters, he says, users should not install unfamiliar apps to their systems. They should also think twice before sharing password or bank account information.

"People should also delete their voice histories and know how many apps they've installed," Vanunu added.

Netenrich's Hoffman says while hackers have been prying into home automation equipment for a long time, the real value of penetrating into home networks initially had limited value to cybercriminals. However, the paradigm has changed now that more people work from home.

"The most dangerous consideration of the work-from-home shift is the idea that vulnerable home networks create a bridge into highly valuable corporate networks," Hoffman says. "While the recent example of Alexa-based vulnerabilities is interesting in terms of highlighting the capability, the actual data accessed is of low or very little value to cybercriminals unless obtained on a massive scale. On the other hand, moving laterally or escalating access to machines on the network shared with a device like Alexa has massive appeal."

Chris Morales, head of security analytics at Vectra, says security teams need to finally understand that IoT attacks are real and here for the long-term. He says large-scale DDoS attacks – the original use of IoT botnets – are difficult to combat for even the largest, most prepared businesses.

"An even greater danger is when IoT devices start snooping around corporate networks and can pivot to more critical systems," he says. "Devices, such as virtual assistants, printers, cameras and even advanced devices like MRI scanners, can pose an alarming cybersecurity risk. While they don't fit the bill of a traditional network host, they represent fruitful targets and vectors for cyberattackers."

Source: https://www.darkreading.com/iot/newly-patched-alexa-flaws-a-red-flag-for-home-workers/d/d-id/1338700

12. Attackers Use Unicode & HTML to Bypass Email Security Tools

Researchers spot cybercriminals using new techniques to help malicious phishing emails slip past detection tools.

Cybercriminals have been spotted using HTML/CSS and Unicode tricks to bypass tools meant to block malicious emails, marking a new twist in phishing techniques, security researchers report.

Attackers are continuously testing enterprise security systems and exploring new ways to get through. Some rely on hidden text and zero-font attacks, in which they put invisible characters between the letters of an email so it doesn't trigger email defenses with phrases like "password expired" or "Office 365." These malicious emails appear legitimate to any unsuspecting user.

Security firm Inky noticed a new twist on this technique in which attackers use their knowledge of HTML/CSS and Unicode to disguise phishing emails. The company began to investigate when a customer reported a suspicious message disguised as a "password expired" email from Office 365. Researchers loaded the raw text into text editor Emacs and found a few interesting traits.

One of these is the Unicode "soft hyphen," also known as "syllable hyphen." In typesetting, this is used to tell the renderer where to safely break a line and insert a visible hyphen. The soft hyphen normally renders as invisible; however, it will appear as a Unicode character to security software scanning emails for malicious content. To a security tool, it may as well be an "X".

When the Inky team scanned the malicious email for phrases like "change your password," they didn't receive results because the attacker had written such phrases as "c-h-a-n-g-e- -y-o-u-r- -p-a-s-s-w-o-r-d-." To a user they appear as normal; to a scanner they may not raise any flags because its pattern-matching settings aren't configured to look for this type of content.

"The fact that they render invisible is this weird quirk of Unicode," says Dave Baggett, founder and CEO at Inky. "Clearly, the attacker knows a lot about Unicode and is being quite smart in crafting this." He notes there were about 10 Unicode characters included in this email alone.

This wasn't the only new technique seen in this Office 365 phishing email, a type of malicious message Baggett describes as "rampant." When the attacker typed "Office 365," for example, they used the HTML <font> to make it look like logotype. This big red text in the upper left corner is common in Office 365 phishing, he says, and people often register the text as a logo.

Attackers also used the "display:none" setting, an element of CSS that tells a browser to render text as invisible. The phisher made the error of putting text they wanted the user to see within a span element, even though the CSS was written to render spans as hidden. The attacker used the invisible span trick to hide repeating text "40008" between words of the phrase "Password for user[@]example[.]com," a move Baggett says was intended to hide the malicious text from security tools.

"If you're a developer, it's useful to temporarily hide things to test, but here, they're using it to make every span 'display:none,' which is very weird," he notes. "You would never do this on a webpage." He hypothesizes the idea was to fool security tools into thinking the text was visible.

The "40008" text could be another tactic to bypass the pattern-matching in security tools, Baggett adds. If there is a random number generated for every email, there's less of a chance tools will associate them with the same phishing kit.

"This looks like someone took an existing template they'd been using and modified it to use this new trick," he says.

The technique used here is similar to steganography, or the practice of hiding surreptitious messages in text by using invisible or hard-to-see space, Baggett explains. Steganography is another common technique among cybercriminals who want to conceal malicious text. An attacker could also use zero-width Unicode characters to transmit messages in this manner.

A challenge in defending against this technique is there are different kinds of soft hyphens, he points out. It's in the attacker's interest to use several unique Unicode characters to slip past security defenses; however, the more Unicode characters a company adds to its security tool, the slower it will be. Even if you could capture all the many ways an attacker can bypass defenses, it may not necessarily scale well.

"It's in the attacker's best interest to use more characters," Baggett says. "It's in the SEG [Secure Email Gateway]'s interest to have fewer characters in their matching patterns."

Source: https://www.darkreading.com/attacks-breaches/attackers-use-unicode-and-html-to-bypass-email-security-tools/d/d-id/1338739

13. MITRE Releases 'Shield' Active Defense Framework

Free knowledge base offers techniques and tactics for engaging with and better defending against network intruders.

MITRE Corp. has released a new guide cataloging measures that organizations can take to actively engage with and counter intruders on their networks.

Like MITRE's widely used ATT&CK framework, which offers a comprehensive listing of attacker behavior, the federally funded organization's new Shield is a publicly availably knowledge base, this time of tactics and techniques for proactive defense.

The core focus is on informing security practitioners about adversary engagement — or interacting with cyber intruders and figuring out how to mount a more active defense against them, says Bill Hill, CISO at MITRE.

"When noninteractive defenses like patching, firewalls, IDSs, etc., fail or are completely circumvented, what can we learn and how can we improve?" he says. Adversary engagement is "learning about how our adversaries attack us, what tools they use, what they will do after they establish a beachhead on our systems, maybe even what they want from us."

MITRE's new Shield framework presents information in a matrix format, in similar fashion as ATT&CK. The matrix consists of eight columns, each one listing different tactics — such as detect, disrupt, contain, and collect — that security practitioners can use to defend against intruders on the network. The hyperlinked data in the rows or each of the cells describes the actual techniques that defenders can use to implement each of these tactics.

For instance, the techniques listed in the individual cells under the "detect" column include API monitoring, behavioral analytics, email manipulation, and the creation of decoy accounts, networks, and credentials. Similarly, MITRE's recommended techniques for containing an adversary include baselining systems, system isolation and hardware, and software manipulation. By clicking on each of the cells, security professionals can then get more information on each technique, including the use cases for them.

MITRE's new Shield active defense framework identifies the opportunities for learning that defenders have from actively taking on and engaging with intruders on the network. "We believe that adversary actions not only present challenges, they also present opportunities to the defender," Hill says. "We consider these opportunities to be instances where the defender can take 'active' defense measures in order to change the game."

For example, by creating a decoy account, an organization could entice an adversary to take some action that would reveal information about their tactics and tools. Similarly,

by seeding a target system with decoy credentials — such as fake usernames, passwords, and browser tokens — defenders can get alerts when an adversary accesses a particular resource or uses a specific technique, according to MITRE.

MITRE has mapped the post-compromise adversary behavior contained in its ATT&CK framework to the relevant defensive techniques in Shield. So by clicking on a particular adversary behavior in ATT&CK, defenders can quickly pull up MITRE's recommended tactic and technique for dealing with that specific behavior.

"Consider the techniques in Shield as active defense building blocks," says Christina Fowler, chief cyber intelligence strategist at MITRE. Some of them are basic and approachable, while some others are more sophisticated. "Each building block can be used alone or added to other building blocks to achieve something more elaborate. Defenders can begin with the basics, and go as far as their desire and resources take them."

Fowler says the creation of the Shield framework was prompted by MITRE's positive experience using active defense techniques over the past 10 years. "Thinking that nothing works with practitioners like details learned through experience," Fowler says, "we've put Shield together to see if we can really get a conversation started about the benefit of active defense."

Source: https://www.darkreading.com/attacks-breaches/mitre-releases-shield-active-defense-framework-/d/d-id/1338741

14. Sendgrid Under Siege from Hacked Accounts

Email service provider **Sendgrid** is grappling with an unusually large number of customer accounts whose passwords have been cracked, sold to spammers, and abused for sending phishing and email malware attacks. Sendgrid's parent company **Twilio** says it is working on a plan to require multi-factor authentication for all of its customers, but that solution may not come fast enough for organizations having trouble dealing with the fallout in the meantime.

Many companies use Sendgrid to communicate with their customers via email, or else pay marketing firms to do that on their behalf using Sendgrid's systems. Sendgrid takes steps to validate that new customers are legitimate businesses, and that emails sent through its platform carry the proper digital signatures that other companies can use to validate that the messages have been authorized by its customers.

But this also means when a Sendgrid customer account gets hacked and used to send malware or phishing scams, the threat is particularly acute because a large number of

organizations allow email from Sendgrid's systems to sail through their spam-filtering systems.

To make matters worse, links included in emails sent through Sendgrid are obfuscated (mainly for tracking deliverability and other metrics), so it is not immediately clear to recipients where on the Internet they will be taken when they click.

Dealing with compromised customer accounts is a constant challenge for any organization doing business online today, and certainly Sendgrid is not the only email marketing platform dealing with this problem. But according to multiple emails from readers, recent threads on several anti-spam discussion lists, and interviews with people in the anti-spam community, over the past few months there has been a marked increase in malicious, phishous and outright spammy email being blasted out via Sendgrid's servers.

Rob McEwen is CEO of Invaluement.com, an anti-spam firm whose data on junk email trends are used to improve the spam-blocking technologies deployed by several Fortune 100 companies. McEwen said no other email service provider has come close to generating the volume of spam that's been emanating from Sendgrid accounts lately.

"As far as the nasty criminal phishes and viruses, I think there's not even a close second in terms of how bad it's been with Sendgrid over the past few months," he said.

Trying to filter out bad emails coming from a major email provider that so many legitimate companies rely upon to reach their customers can be a dicey business. If you filter the emails too aggressively you end up with an unacceptable number of "false positives," i.e., benign or even desirable emails that get flagged as spam and sent to the junk folder or blocked altogether.

But McEwen said the incidence of malicious spam coming from Sendgrid has gotten so bad that he recently launched a new anti-spam block list specifically to filter out email from Sendgrid accounts that have been known to be blasting large volumes of junk or malicious email.

"Before I implemented this in my own filtering system a week ago, I was getting three to four phone calls or stern emails a week from angry customers wondering why these malicious emails were getting through to their inboxes," McEwen said. "And I just am not seeing anything this egregious in terms of viruses and spams from the other email service providers."

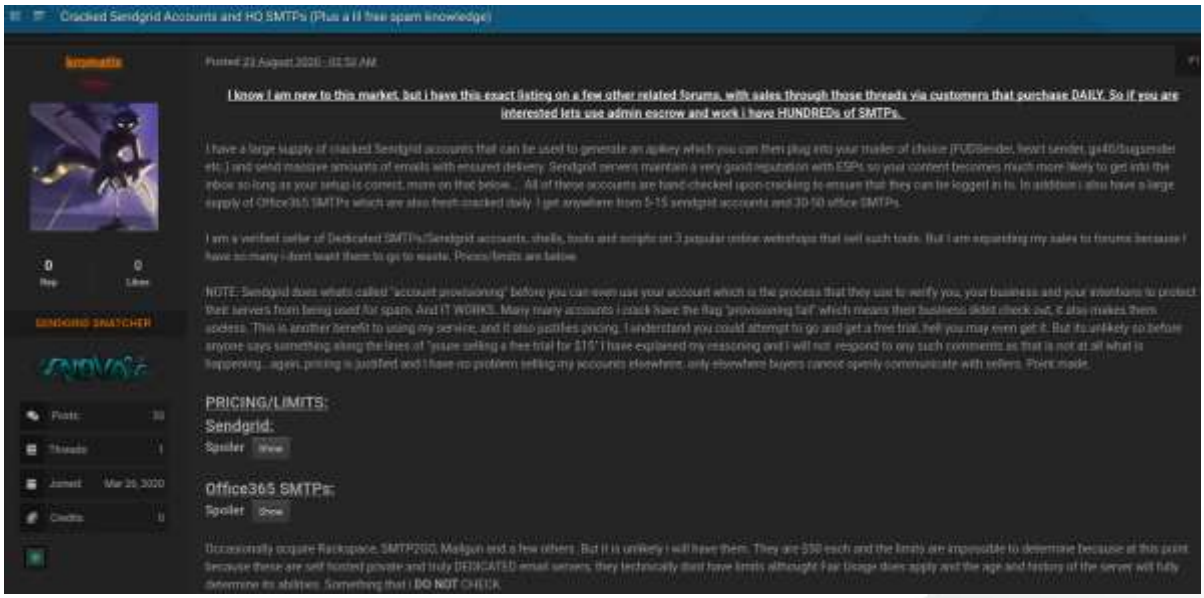
In an interview with KrebsOnSecurity, Sendgrid parent firm Twilio acknowledged the company had recently seen an increase in compromised customer accounts being abused for spam. While Sendgrid does allow customers to use multi-factor authentication (also known as two-factor authentication or 2FA), this protection is not mandatory.

But **Twilio Chief Security Officer Steve Pugh** said the company is working on changes that would require customers to use some form of 2FA in addition to usernames and passwords.

"Twilio believes that requiring 2FA for customer accounts is the right thing to do, and we're working towards that end," Pugh said. "2FA has proven to be a powerful tool in securing communications channels. This is part of the reason we acquired Authy and created a line of account security products and services. Twilio, like other platforms, is forming a plan on how to better secure our customers' accounts through native technologies such as Authy and additional account level controls to mitigate known attack vectors."

Requiring customers to use some form of 2FA would go a long way toward neutralizing the underground market for compromised Sendgrid accounts, which are sold by a variety of cybercriminals who specialize in gaining access to accounts by targeting users who re-use the same passwords across multiple websites.

One such individual, who goes by the handle "Kromatix" on several forums, is currently selling access to more than 400 compromised Sendgrid user accounts. The pricing attached to each account is based on volume of email it can send in a given month. Accounts that can send up to 40,000 emails a month go for $15, whereas those capable of blasting 10 million missives a month sell for $400.



"I have a large supply of cracked Sendgrid accounts that can be used to generate an API key which you can then plug into your mailer of choice and send massive amounts of emails with ensured delivery," Kromatix wrote in an Aug. 23 sales thread. "Sendgrid servers maintain a very good reputation with [email service providers] so your content becomes much more likely to get into the inbox so long as your setup is correct."

Neil Schwartzman, executive director of the anti-spam group CAUCE, said Sendgrid's 2FA plans are long overdue, noting that the company bought Authy back in 2015.

Single-factor authentication for a company like this in 2020 is just ludicrous given the potential damage and malicious content we're seeing

"Single-factor authentication for a company like this in 2020 is just ludicrous given the potential damage and malicious content we're seeing," Schwartzman said.

"I understand that it's a task to invoke 2FA, and given the volume of customers Sendgrid has that's something to consider because there's going to be a lot of customer overhead involved," he continued. "But it's not like your bank, social media account, email and plenty of other places online don't already insist on it."

Schwartzman said if Twilio doesn't act quickly enough to fix the problem on its end, the major email providers of the world (think Google, Microsoft and Apple) — and their various machine-learning anti-spam algorithms — may do it for them.

"There is a tipping point after which receiving firms start to lose patience and start to more aggressively filter this stuff," he said. "If seeing a Sendgrid email according to machine learning becomes a sign of abuse, trust me the machines will make the decisions even if the people don't."

Source: https://krebsonsecurity.com/2020/08/sendgrid-under-siege-from-hacked-accounts/

15. Microsoft Put Off Fixing Zero Day for 2 Years

A security flaw in the way **Microsoft Windows** guards users against malicious files was actively exploited in malware attacks for two years before last week, when Microsoft finally issued a software update to correct the problem.

One of the 120 security holes Microsoft fixed on Aug. 11's Patch Tuesday was CVE-2020-1464, a problem with the way every supported version of Windows validates digital signatures for computer programs.

Code signing is the method of using a certificate-based digital signature to sign executable files and scripts in order to verify the author's identity and ensure that the code has not been changed or corrupted since it was signed by the author.

Microsoft said an attacker could use this "spoofing vulnerability" to bypass security features intended to prevent improperly signed files from being loaded. Microsoft's

advisory makes no mention of security researchers having told the company about the flaw, which Microsoft acknowledged was actively being exploited.

In fact, CVE-2020-1464 was first spotted in attacks used in the wild back in August 2018. And several researchers informed Microsoft about the weakness over the past 18 months.

Bernardo Quintero is the manager at VirusTotal, a service owned by Google that scans any submitted files against dozens of antivirus services and displays the results. On Jan. 15, 2019, Quintero published a blog post outlining how Windows keeps the Authenticode signature valid after appending any content to the end of Windows Installer files (those ending in .MSI) signed by any software developer.

Quintero said this weakness would particularly acute if an attacker were to use it to hide a malicious **Java** file (.jar). And, he said, this exact attack vector was indeed detected in a malware sample sent to VirusTotal.

"In short, an attacker can append a malicious JAR to a MSI file signed by a trusted software developer (like Microsoft Corporation, Google Inc. or any other well-known developer), and the resulting file can be renamed with the .jar extension and will have a valid signature according Microsoft Windows," Quintero wrote.

But according to Quintero, while Microsoft's security team validated his findings, the company chose not to address the problem at the time.

"Microsoft has decided that it will not be fixing this issue in the current versions of Windows and agreed we are able to blog about this case and our findings publicly," his blog post concluded.

Tal Be'ery, founder of Zengo, and **Peleg Hadar**, senior security researcher at SafeBreach Labs, penned a blog post on Sunday that pointed to a file uploaded to VirusTotal in August 2018 that abused the spoofing weakness, which has been dubbed **GlueBall**. The last time that August 2018 file was scanned at VirusTotal (Aug 14, 2020), it was detected as a malicious Java trojan by 28 of 59 antivirus programs.

More recently, others would likewise call attention to malware that abused the security weakness, including this post in June 2020 from the **Security-in-bits** blog.

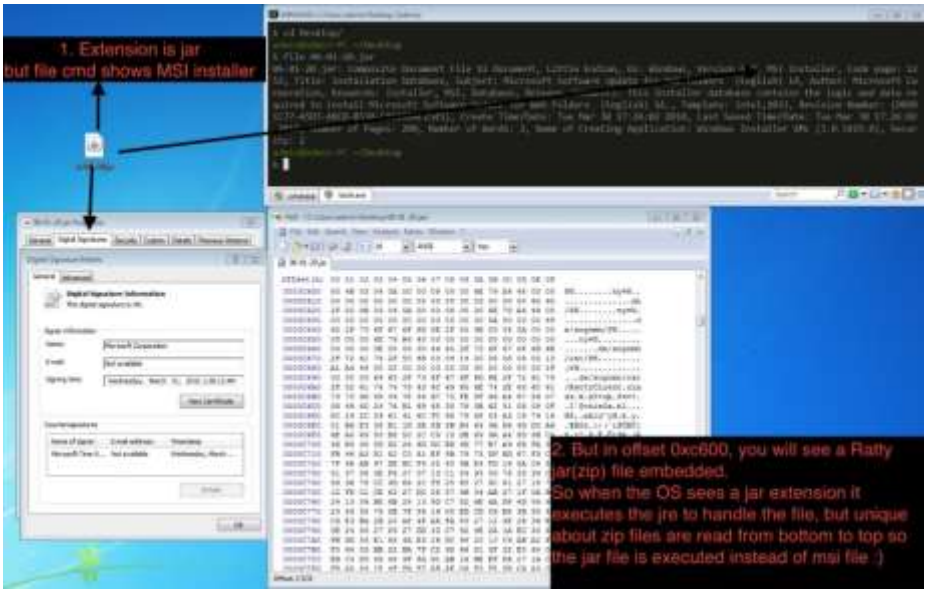


Image: Securityinbits.com

Be'ery said the way Microsoft has handled the vulnerability report seems rather strange.

"It was very clear to everyone involved, Microsoft included, that GlueBall is indeed a valid vulnerability exploited in the wild," he wrote. "Therefore, it is not clear why it was only patched now and not two years ago."

Asked to comment on why it waited two years to patch a flaw that was actively being exploited to compromise the security of Windows computers, Microsoft dodged the question, saying Windows users who have applied the latest security updates are protected from this attack.

"A security update was released in August," Microsoft said in a written statement sent to KrebsOnSecurity. "Customers who apply the update, or have automatic updates enabled, will be protected. We continue to encourage customers to turn on automatic updates to help ensure they are protected."

Source: *https://krebsonsecurity.com/2020/08/microsoft-put-off-fixing-zero-day-for-2-years/*

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.