telelink

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

Monthly Security Bulletin

October 2018

Table of Contents

Executive Summary 2

1. Google Adds New Rules To End Malicious Chrome Extensions 4
2. SMB Security Best Practices: Why Smaller Businesses Face Bigger Risks 5
3. Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad 8
4. Facebook Breach Sparks Concerns Around Third-Party Apps, Website Security 12
5. Sony Smart TV Bug Allows Remote Access, Root Privileges 13
6. Google+ Shutting Down After Bug Leaks Info of 500k Accounts 14
7. Vulnerability Spotlight: VMWare Workstation DoS Vulnerability 15
8. US Advanced Weaponry Is Easy to Hack, Even by Low-Skilled Attackers 16
9. Fake Adobe Flash Updates Hide Malicious Crypto Miners 18
10. Facebook States 30 Million People Affected by Last Month's "View As" Bug 19
11. Up to 35 Million 2018 Voter Records For Sale on Hacking Forum 20
12. In County Crippled by Hurricane, Water Utility Targeted in Ransomware Attack 22
13. As End of Life Nears, More Than Half of Websites Still Use PHP V5 23
14. Multiple D-Link Routers Open to Complete Takeover with Simple Attack 24
15. New Windows Zero-Day Bug Helps Delete Any File, Exploit Available 26
16. Debunking AI's Impact on the Cybersecurity Skills Gap 27
17. UK Slaps Facebook with $645K Fine Over Cambridge Analytica Scandal 29

Executive Summary

The below Monthly Security bulletin will cover greater detail the following topics:

- "Google has stated that they will no longer tolerate ones that ask for powerful permissions for no reason, use external scripts, or obfuscate their code". At the moment extensions have the ability to get full access to the users' information, but this about to change to Chrome 70. There users can restrict the degree of information that extensions can access. The new policy states that "starting on October 1st, Google is no longer allowing new extensions to use obfuscated JavaScript code or to utilize external scripts that are obfuscated. For any developers who currently utilize obfuscated code, they have until January 1st, 2019 to remove it." *Jump to article*
- Despite the popular belief that small and medium businesses (SMBs) are not of any interest for the hackers, the recent "Verizon's "2018 Data Breach Investigations Report" found that about 58 percent of all data breaches target small businesses" and the damages there are some of the most damaging. The trade-off of saving 500$ only to pay 8000$ in ransomware is hardly justifiable. That is why experts advise to have a holistic cyber security strategy and look for Managed Security Service Providers (MSSPs) who outsource their cybersecurity protections and expertise for a monthly fee. *Jump to article*
- Artificial Intelligence – is it the silver bullet everyone hopes about in the fight with cyber security or a two-edged dagger? When it comes to analyzing large amounts of data and finding relevant patterns, AI can be powerful tool, but companies need to understand that it still has its own limitations. Criminals understand the fact that they can leverage it too in their malicious favor. *Jump to article*
- Facebook acknowledged data breach of its platform that impacts around 50 million accounts and said that hackers exploited flaw in their platform. The concern is the debatable security levels of third-party apps that could give access to personal information. *Jump to article*
- The widespread use and availability of smart TVs has opened the door for remote access and root privileges exploits. "Sony Bravia smart TV models are vulnerable to 3 separate bugs, one rated as crucial." *Jump to article*
- Bad news for all Google+ lovers, the company has decided to shut down the platform due to limited usage and an API bug that leaked the personal information of up to 500 000 users. *Jump to article*
- "Cisco Talos disclosed a vulnerability in VMware Workstation that could result in denial of service. VMware Workstation is a widely used virtualization platform designed to run alongside a normal operating system, allowing users to use both virtualized and physical systems concurrently." *Jump to article*
- "Major weapon systems developed by the US Department of Defense are riddled with vulnerabilities that make them an easy target for adversaries trying to control them or disrupt their functions. Testing teams charged with probing the resilience to cyber-attacks were able to take control or disable the target using basic tools and techniques." *Jump to article*

- "A fake Adobe update actually updates victims' Flash – but also installs malicious cryptomining malware. While fake Flash updates that push malware have traditionally been easy to spot and avoid, a new campaign has employed new tricks that stealthily download cryptocurrency miners on Windows systems." *Jump to article*
- "Good news" coming from Facebook state that of the aforementioned 50 million affected accounts only 30 million of them had their access tokens stolen. The attackers had stolen various information such as names, contact information, gender etc., but did not however accessed services such as Messenger, Messenger Kids, Instagram, WhatsApp, Oculus, Workplace, Pages, payments, third-party apps, or advertising or developer accounts. *Jump to article*
- In light of the 2018 mid-term election in the US, up to 35 million voter records have been found up for sale on a popular hacking forum from 19 states. Researchers said that within hours of the initial advertisement, a "high-profile actor" organized a crowdfunding campaign to purchase each of the voter registration databases. *Jump to article*
- „The Emotet Trojan is behind a crippling ransomware attack that hit the Onslow Water and Sewer Authority. A "critical water utility" has been targeted in a recent ransomware attack, significantly impeding its ability to provide service in the week after Hurricane Florence hit the East Coast of the U.S. Regardless of its age, the Emotet is still being put into use". *Jump to article*
- "Support for PHP 5.6 drops on December 31 - but a recent report found that almost 62 percent of websites are still using version 5". Now what? *Jump to article*
- Eight D-Link routers in the company's small/home office "DWR" range are vulnerable to complete takeover – but the vendor said it is planning on only patching two, according to a researcher. However, only 2 of these 8 routers will be patched, since the rest will no longer be supported. *Jump to article*
- "Proof-of-concept code for a new zero-day vulnerability in Windows has been released by a security researcher before Microsoft was able to release a fix. The code exploits a vulnerability that allows deleting without permission any files on a machine, including system data, and it has the potential to lead to privilege escalation." Although deleting operating system files and the prospect of privilege escalation are serious threats, the bug is being described as "low quality" and a "pain to exploit". *Jump to article*
- "Artificial intelligence is the latest buzzword to take hold of the cybersecurity industry. It is being touted, among other things, as the ultimate solution to the cybersecurity skills gap." AI could be the answer to the shortage of right talent and skill in the field of cybersecurity but being still in its early life time. By processing large amounts of data and replacing manual tasks, researchers are hopeful that AI could be the bridge the cybersecurity gap and increase productivity. *Jump to article*
- The UK has fined Facebook $645,000 over Cambridge Analytica's data harvesting practices, which exploited the data of 87 million users of the social network. However, this is a barely slap on the wrist due to the fact that this is the maximum amount allowed in the pre-GDPR relegation. In comparison the GDPR rules stipulate a maximum fine of 4% of annual global turnover, which in the $1.6 billion Facebook's case isn't a chump change. *Jump to article*

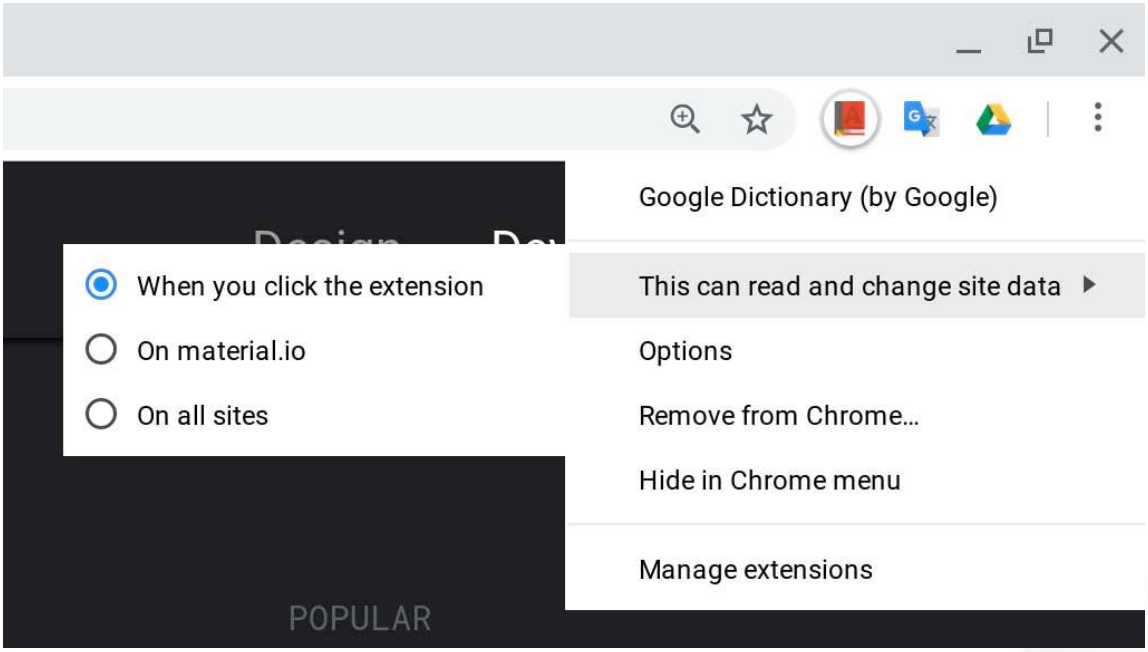
1. Google Adds New Rules To End Malicious Chrome Extensions

Google has stated that they will no longer tolerate ones that ask for powerful permissions for no reason, use external scripts, or obfuscate their code.

In the current version of Chrome, an extension has the ability to get full access to all of the data and content of a web site that you are visiting. This allows beneficial extensions to be created that modify the skin of a site, add extra features, or fix bugs on sites.

At the same time, this also allows extensions to inject advertisements, steal social profile information, inject in-browser miners, steal login information, access other web sites, and perform a variety of other malicious activities.

With Chrome 70, users will now have the ability to restrict the sites an extension has access. With this new setting, you can specify that the extension only has access to a site "When you click the extension, on a specific site, or on all sites.



Unfortunately, according to Google's User Controls For Host Permissions: Transition Guide it appears that users will need to make these changes themselves, rather than having them become restrictive by default.

New extension review policies

Extensions that request powerful permissions, or full access to sites, will now be subject to additional review. Google has also stated that they will be looking closely at extensions that utilize remotely hosted code and outgoing monitoring.

Whether this will include Google analytics, which is heavily used by new tab and search hijacking extensions to track users, is unknown. It also does not indicate whether search redirects for the sole purpose of tracking a user's activity will be allowed as well.

Overall, Google wants a tight package that makes it easier to perform a review and do not want to have to examine off site code that can easily be changed whenever a developer wishes.

Starting on October 1st, Google is no longer allowing new extensions to use obfuscated JavaScript code or to utilize external scripts that are obfuscated. For any developers who currently utilize obfuscated code, they have until January 1st, 2019 to remove it.

Analyzing extensions can be time consuming as most malicious Chrome extensions are obfuscated. This means the developers use special tools that make it harder to see what the extension's scripts are doing.

As Google is stepping up their review process, this means that they need to make it easier for them to review the code. This is a welcome change and one that will make it easier for not only Google but for people who commonly analyze Chrome extensions to look for malicious behavior.

This policy still allows developers to minify their extension's code with the following methods:

- Removal of whitespace, newlines, code comments, and block delimiters
- Shortening of variable and function names
- Collapsing the number of JavaScript files

2-Step verification required for devs

In the past, very popular extensions, such as MEGA, have been hacked and been replaced with a malicious variant. Due to this, in 2019 Google will require all Chrome extension developers to enable 2-Step verification on their Chrome Web Store developer accounts.

By doing so, it will make it much harder for an attacker to hack an account as they would need the developer's authentication device, such as their mobile phone, to do so.

Source: https://www.bleepingcomputer.com/news/google/google-adds-new-rules-to-end-malicious-chrome-extensions/

2. SMB Security Best Practices: Why Smaller Businesses Face Bigger Risks

Data breaches that compromise hundreds of thousands — or millions — of records tend to grab the most headlines, but small and medium-sized businesses (SMBs) are far from immune to cyberattacks.

SMB security is full of holes, and these vulnerabilities are often the most damaging, according to recent research. For example, Verizon's "2018 Data Breach Investigations Report" found that about 58 percent of all data breaches target small businesses. In addition, 60 percent of SMBs hit with a data breach close within six months, according to Switchfast Technologies, even though more than half of all small business leaders don't believe they're targets.

Small Businesses Are Easy Targets

"Think your business is too small to be targeted by a hacker? Think again," said Chris Stoneff, vice president of security solutions at secure remote access provider Bomgar. "If your business handles any financial information or valuable data about your customers, then guess what? You're a target for cyberattacks."

As large enterprises increasingly focus on improving cybersecurity, cybercriminals may take the path of least resistance.

"If that path is via a smaller business with tempting customers," Stoneff added, "you better believe they will take the easy route."

At the same time, many small businesses don't have a lot of money to spend on cybersecurity. In fact, nearly half of all small businesses fail within five years, according to the U.S. Small Business Administration, and cash flow problems account for a huge number of those closures.

Why You Shouldn't Skimp on SMB Security

Cybersecurity is not the place for SMBs to cut costs, said John Watkins, vice president and chief information officer (CIO) of inRsite IT Solutions, a cloud and security provider for SMBs.

"If you don't take cybersecurity seriously, and one day you're forced to pay $8,000 in bitcoin to — hopefully — unlock your QuickBooks data, just remember, you saved $500 by not getting a firewall," Watkins quipped.

Clearly, small businesses — even those with razor-thin profit margins — shouldn't skimp on their cybersecurity protections. But assuming budgets are tight, how can SMBs make the most of their spending?

Many cybersecurity experts still recommend the basics:

- Use multifactor authentication to sign on to company devices.
- Require strong passwords.
- Deploy antivirus, antispyware and firewall protection.
- Identify the sensitive data you hold and encrypt it.

- Regularly update software.
- Train employees on cybersecurity.

A business-grade firewall is one of the essential basics no SMB should ignore, Watkins said.

Building a Holistic Security Strategy

SMB cybersecurity efforts should focus on their people and processes, "coupled with the support of reliable, well-implemented tools and technologies," said Chris Duvall, senior director at The Chertoff Group, a company that advises clients on security and risk management.

Beyond the basics, Duvall urged SMBs to consider a virtual private network (VPN) to protect traffic in and out of their networks and a password management tool to help employees store their credentials in a single, secure location. Small businesses should also look into commercial products that package a number of security tools, such as intrusion detection and prevention systems, together.

What to Look For in an MSSP

Managed security service providers (MSSPs) enable small businesses to outsource their cybersecurity protections for a monthly fee. MSSPs can be useful for a resource-strapped SMB, Duvall noted, "but using the right MSSP and ensuring regular and detailed communication is key." He added that with managed service becoming a popular offering in the cybersecurity industry, some companies are "labeling themselves as MSSPs but are not capable of, or qualified to, manage the security of other organizations." SMBs should do their homework and request a "proof-of-concept" period before signing an MSSP contract.

Mike Baker, founder and principal of managed cybersecurity provider Mosaic451, agreed that outsourced services can help SMBs fight off attackers. An SMB's IT staff can "get bogged down by providing the basics — such as routine system monitoring, software upgrades, training on new systems and services, help desk support, and the seemingly endless number of meetings," he said. The best way to find a managed service provider, then, is through word of mouth.

"It's always better to go with an actual referral," Baker said. "Go with someone you know. Go with someone that a peer knows."

Online ratings, "random top-10 lists and whatnot are paid-for marketing," he added. "Trust them at your peril."

Why You Must Actively Manage Your Data

Watkins and other cybersecurity professionals also advised SMBs to frequently back up their data. A cloud service is a good way to make copies that are protected from direct attacks

on the business. Ransomware remains a serious threat, and some network-attached storage device makers include software to encrypt and replicate a business' data in the cloud.

SMBs should have at least three backups of their data, Watkins recommended.

"One of the most devastating things that can happen to an SMB is data loss," he said. "Whether caused by lightning frying your PC or cryptoware infecting your server, data loss can literally bring a business to the brink of closure."

Frequent backups, a managed security provider, a VPN, and a well-rounded package of antivirus and intrusion detection tools are among the protections SMBs should consider to better secure their data, but establishing these defenses is only the beginning. To sustain a successful enterprise security strategy, organizations must regularly audit the efficacy of each tool and team, establish a culture of security from the top down, and scale consistently through growth phases.

Source: https://securityintelligence.com/smb-security-best-practices-why-smaller-businesses-face-bigger-risks/

3. Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad

Attractive to both white-hats and cybercriminals, AI's role in security has yet to find an equilibrium between the two sides.

Artificial intelligence is the new golden ring for cybersecurity developers, thanks to its potential to not just automate functions at scale but also to make contextual decisions based on what it learns over time. This can have big implications for security personnel—all too often, companies simply don't have the resources to search through the haystack of anomalies for the proverbial malicious needle.

For instance, if a worker normally based in New York suddenly one morning logs in from Pittsburgh, that's an anomaly — and the AI can tell that's an anomaly because it has learned to expect that user to be logging in from New York. Similarly, if a log-in in Pittsburgh is followed within a few minutes of another log-in by the same user from, say, California, that's likely a malicious red flag.

So, at its simplest level, AI and "machine learning" is oriented around understanding behavioral norms. The system takes some time to observe the environment to see what normal behavior is and establish a baseline—so that it can pick up on deviations from the norm by applying algorithmic knowledge to a data set.

AI for security can help defenders in a myriad of ways. However, there are also downsides to the emergence of AI. For one, the technology has also been leveraged by cybercriminals, and it's clear that it can be co-opted for various nefarious tasks. These have include at-scale

scanning for open, and vulnerable ports – or automated composition of emails that have the exact tone and voice of the company's CEO, learned over time by 24-7 eavesdropping.

And in the not-too-distant future, that automatic mimicking could even extend to voice. IBM scientists for instance have created a way for AI systems to analyze, interpret and mirror users' unique speech and linguistic traits – in theory to make it easier for humans to talk to their technology. However, the potential for using this type of capability for malicious spoofing applications is obvious.

And meanwhile, the zeal for adopting AI across vertical markets – for cybersecurity and beyond – has opened up a rapidly proliferating new attack surface—one that doesn't always feature built-in security-by-design. AI has the capacity to revolutionize any number of industries: offering smarter recommendations to online shoppers, speeding along manufacturing processes with automatic quality checks or even tracking wildfire risk and monitoring, as researchers at the University of Alberta in Canada are doing.

This dual-nature aspect of AI – a force for good, a force for evil – has yet to find an equilibrium, but interest in AI for security continues to grow.

Fighting the Good Fight with AI

AI has received plenty of hype when it comes to its applicability to cybersecurity. Because AI relies on analyzing large amounts of data to find relevant patterns and anomalies, it can be asked to learn over time what constitutes a false positive and what doesn't within the context of a certain prescribed set of policies. As such, it can be an immeasurable boon for intrusion prevention and detection, for instance, along with fraud detection and rooting out malicious activities such as DNS data exfiltration and credential misuse.

AI algorithms can be applied to user and network behavior analytics. For instance, machine learning that looks at the activity of people, endpoints and network devices like printers in order to flag potential malicious activity of rogue insiders. Similarly, AI has a role to play in web behavior analytics, which examines user interactions with websites and acts as a complement to online fraud detection.

For instance, if a user logs into a retail application, searches around the site, finds a product to learn more about, and then either saves that product to a shopping cart or checks out. That user now fits a behavior profile as a buyer. In the future, if that user displays wildly different behavior on the same ecommerce site, it could be flagged for further investigation as a potential security event.

On the DNS front, an AI system can examine DNS traffic to track when DNS queries go to an authoritative server, but don't receive a valid response.

Identifying credential-stuffing and misuse is another good example. This type of attack is becoming more and more common as people's emails and passwords flow to the Dark Web from data breaches. The Equifax breach for instance resulted in millions of valid emails being

exposed; and in 2016, attackers made off with credentials for 500 million accounts in the massive Yahoo! data breach. Because people tend to re-use passwords, criminals will try different sets of emails and passwords on random machines in various contexts, hoping to get a hit. To identify this kind of attack, "AI is useful here because the users have been baselined," explained Jett. "Those users connect to and log in to a set number of devices each day. It's easy for a human to see when a credential is tried hundreds of times on a server, but it's hard to catch someone that tries to connect to 100 different machines on the network and only succeeds once."

AI also can be used to automatically evaluate open-source code for potential flaws. Cybersecurity firm Synopsys for example is using AI to automatically map publicly known vulnerabilities to open-source projects, and evaluating the risk impact for companies; for instance, it automatically analyzes hundreds of legal documents (licenses, terms of services, privacy statements, privacy laws such as HIPAA, DMCA, and others) to determine the compliance risks of any detected vulnerabilities.

Yet another application on the vulnerability front is for retrospection and prognostication. If a new vulnerability is announced, it becomes possible to go back through log data to see if it's been exploited in the past. Or, if it is indeed a new attack, the AI could evaluate whether the evidence deterministic enough to see what the next steps could be for an attacker.

AI also works very well for tedious, repetitive tasks – such as looking for specific patterns. As such, its implementation can alleviate the resource constraints faced by most security operations centers (SOCs), according to Greg Martin, CEO and co-founder of JASK. SOC personnel are fielding hundreds of security flags every day – not all of them actual attacks of course. This requires them to do things like alert triage, creating false negative/positive decision trees, swivel chair tool correlation, and implementing RSS and email list intelligence, he said.

"Security teams have always been overwhelmed by information," said Scott Crawford, a research director at 451 Research, in an interview. "Information about what adversaries are doing, the latest attacker tools, malware variations and the ton of information generated by internal resources. In the intrusion protection space along the amount of log data and alerts that are generated is overwhelming. The SIEM market arose in part to address this, surfacing stuff in principle only when there are things that actually need to be dealt with—but it hasn't been enough. So now we see the rise in new techniques for handling data at scale and getting meaning out of it with analytics and AI."

Not Perfect Yet

Despite all of its utility in the security space, companies should be careful to understand AI's limitations; these engines are only as good as the data that goes into them, and merely imputing data into an algorithm will tell an analyst what's unusual, but not if it matters. The data scientist that establishes the parameters for the AI needs to know how to ask the right questions to properly harness the AI's capabilities. What is the AI supposed to be looking for?

Once whatever that is found, what should the AI do with it? Often, complex flow charts are needed to program the AI for the desired results.

A Cyber-Attacker Bonanza

The other side of the AI story is that as these engines' capabilities become more powerful and widespread, cybercriminals have copped on to the fact that they, too, can leverage the technology — specifically to carry out cyber-attacks cheaper and easier than ever before.

For instance, AI can increase the effectiveness of attacks through, say, the automation of spear-phishing, using real-time speech synthesis for impersonation attacks and fraud, or for carrying out activities such as packet-sniffing and vulnerability-hunting at scale, according to the Malicious Use of Artificial Intelligence report. The report also noted that AI could also be used for exploiting existing software vulnerabilities on a mass level (e.g. automated hacking of tens of thousands of machines per day).

None of this is merely theoretical. In 2017, cybersecurity firm Darktrace an attack in India that used "rudimentary" AI to observe and learn patterns of normal user behavior inside the network, for reconnaissance. The activity could also start to parse specific users' communications patterns, to be able to mimic his or her tone and style. This could be used for the automated composition of business email compromise messages, for example, that would be much more effective and convincing than the standard social-engineering attempt.

On a similar note, the Malicious Use report also noted that AI can be used to automate tasks involved in analyzing mass-collected data, expanding threats associated with privacy invasion and social manipulation and more.

Another AI-driven development is the rise of botnet swarms, as seen with the recent Hide and Seek botnet. Hide and Seek is a self-learning cluster of compromised devices that is the world's first to communicate via a custom-built peer to peer protocol. Traditional botnets wait for commands from a bot herder; swarms are able to make decisions independently.

A Look to the Future

Perhaps to keep pace with the bad guys' efforts, AI is coming into its own from a security standpoint, and companies are building it into their security offerings more frequently. Going forward, the emphasis is on more fully applying it to a rapidly accelerating and complex threat landscape.

"What we've seen is continuing sophistication of attacks, coming from a backdrop of security departments being under-resourced and not really knowing where they should put their spend and their people," said Steve Durbin, managing director at the Information Security Forum, in an interview. "All of this is happening amidst an increasingly complex environment with more and more IoT devices taking feeds from various sources, plus there's often a hugely

complex third-party supply chain. AI is becoming necessary to get one's arms around all of this."

The Nirvana, he explained, is the capability to navigate this attack surface from end-to-end. From there, the goal is to anticipate attacks before they happen or proactively head off cybercriminals before they get to the network in the first place.

There is some evidence that this is starting to happen. For instance, IBM – which employs its Watson AI and advanced analytics to monitor 60 billion security events on a daily basis – has developed an AI-based "cognitive honeypot" to proactively bait hackers into spending valuable time and resources on nonexistent leads. The technology lures malicious hackers in with email exchanges and interactive websites that divert their attacks.

Source: https://threatpost.com/artificial-intelligence-a-cybersecurity-tool-for-good-and-sometimes-bad/137831/

4. Facebook Breach Sparks Concerns Around Third-Party Apps, Website Security

Days after Facebook acknowledged a data breach of its platform – impacting 50 million accounts – the company said it has found no evidence that attackers accessed any apps using Facebook Login. But security experts are still on edge that the breach could have let attackers access third-party apps and websites. That's in part due in part to the company's Single Sign-On feature API, which lets users log in to websites using their Facebook credentials- and can be obtained via access tokens.

The social media platform at the end of September said that hackers exploited a flaw in its platform that left the access tokens – the digital keys that keep users logged into Facebook – of almost 50 million accounts ripe for the taking. Guy Rosen, VP of product management at Facebook, stressed Tuesday that so far, there has been no evidence that the threat actors behind the breach have accessed apps via Facebook's login tool.

The vulnerability, which was discovered by Facebook engineers, existed in Facebook's "View As" feature, which let users see what their profiles look like from other account.

Facebook has since fixed the vulnerability and reset the access tokens for the 90 million total accounts subject to the "View As" look-up in the last year. But the possibility remains that the attackers could have used the access tokens to access APIs containing profile information, such as name or gender. And one of those APIs, the Single Sign-On API, is used by third-party apps or sites that users can log into using their Facebook credentials.

Source: https://threatpost.com/facebook-breach-sparks-concerns-around-third-party-app-website-security/137918/

5. Sony Smart TV Bug Allows Remote Access, Root Privileges

As the number of smart TVs grows, so does the number of vulnerabilities inside of them. On Thursday, security researchers revealed that eight Sony Bravia smart TV models are vulnerable to three separate bugs, one rated critical.

The flaws – a stack buffer overflow, a directory traversal and a command-injection bug – were found by Fortinet in March by its FortiGuard Labs team. The most serious of the vulnerabilities is the command-injection (CVE-2018-16593) bug, which is tied to a proprietary Sony application called Photo Sharing Plus. The app allows users to share multimedia content from their phones or tablets via Sony TVs.

"This application handles file names incorrectly when the user uploads a media file," wrote Fortinet's Tony Loi, who found the vulnerability. "An attacker can abuse such filename mishandling to run arbitrary commands on the system, which can result in complete remote code-execution with root privilege."

Fortinet researchers said a compromised TV could be recruited into a botnet or be used as springboard for additional attacks against devices that shared the same network. To be successful, an adversary would need to be on the same wireless network as the Sony TV.

Similar to the previous vulnerability, the other two Sony Bravia bugs are also tied to Sony's Photo Sharing Plus application, but are rated high severity. The stack buffer overflow (CVE-2018-16595) is a "memory corruption vulnerability that results from insufficient size checking of user input," Loi wrote in a technical write up.

The directory-traversal vulnerability (CVE-2018-16594**)** relates to the way the Photo Sharing Plus app handles file names. "An attacker can upload an arbitrary file with a crafted file name (e.g.: ../../) that can then traverse the whole filesystem," the researcher wrote.

Fortinet said Sony's over-the-air patch needs a user's approval and a network connection to work. In its security bulletin, Sony said that impacted televisions are set to automatically receive updates by default, and should have already. Affected Bravia models include: R5C, WD75, WD65, XE70, XF70, WE75, WE6 and WF6.

This attack surface is growing, too: According to market researchers at GFK, more than half of all 2017 TV sales in the U.S. were smart TVs.

Source: https://threatpost.com/sony-smart-tv-bug-allows-remote-access-root-privileges/138063/

6. Google+ Shutting Down After Bug Leaks Info of 500k Accounts

Google has announced that they are closing the consumer functionality of Google+ due lack of adoption and an API bug that leaked the personal information of up to 500,000 Google+ accounts.

While no evidence was found that indicates this bug was ever misused, it was determined that the complexity of protecting and operating a social network like Google+ was not a worthwhile endeavor when so few users actually used the service for any length of time.

"This review crystallized what we've known for a while: that while our engineering teams have put a lot of effort and dedication into building Google+ over the years, it has not achieved broad consumer or developer adoption, and has seen limited user interaction with apps," stated a blog post by Google regarding the Google+ closure. "The consumer version of Google+ currently has low usage and engagement: 90 percent of Google+ user sessions are less than five seconds."

The consumer functionality of Google+ will be closing over a 10 month period, while Google transitions the product to be used internally by the Enterprise.

API bug caused data leak

After performing a code review of the Google+ APIs, called Project Strobe, Google stated they discovered a bug that could leak the private information of Google+ accounts. This bug could allow a user's installed apps to utilize the API and access non-public information belonging to that user's friends. The non-public information that was accessible includes an account holder's name, email address, occupation, gender and age.

As Google only keeps two weeks of API logs for its Google+ service, it was impossible for them to determine if the bug was ever misused. They were able to determine that the bug was not misused during the two weeks that they had log data.

Google knew about leak in May but did not disclose

According to a report by the Wall Street Journal, the bug in the Google+ API existed between 2015 and March 2018, which was when Google discovered and fixed the bug. According to their reporting, an internal committee at Google decided not to disclose the bug even though they were not 100% sure that it was not abused.

The Wall Street Journal, reported that they have reviewed a memo prepared by Google's legal and policy staff, which indicated that disclosing the data breach could lead to scrutiny by government regulatory agencies.

In a statement to BleepingComputer, a Google Spokesperson said that their Privacy & Data Protection Office felt it was not necessary to disclose as it did not meet the threshold that would warrant it.

Source: https://www.bleepingcomputer.com/news/security/google-shutting-down-after-bug-leaks-info-of-500k-accounts/

7. Vulnerability Spotlight: VMWare Workstation DoS Vulnerability

Cisco Talos disclosed a vulnerability in VMware Workstation that could result in denial of service. VMware Workstation is a widely used virtualization platform designed to run alongside a normal operating system, allowing users to use both virtualized and physical systems concurrently.

TALOS-2018-0589

Discovered by Piotr Bania of Cisco Talos TALOS-2018-0589/CVE-2018-6977 is an exploitable denial-of-service (DoS) vulnerability in the VMware Workstation 14 software. The vulnerability lies in the pixel shader utilized by VMware Workstation and can be triggered by supplying a malformed pixel shader in either text or binary form inside a VMware guest operating system. This vulnerability can be triggered from VMware guest or VMware hosts and results in a process crashing leading to a DoS state. Additionally, it is possible to trigger the vulnerability through WEBGL, assuming the browser will not use ANGLE and will supply the malformed shader as intended.

Tested Software:

VMware Workstation 14 (14.1.1.28517)

Coverage

Talos has developed the following Snort rules to detect attempts to exploit this vulnerability. Note that these rules are subject to change pending additional vulnerability information. For the most current information, please visit your Firepower Management Center or Snort.org.

Source: https://blog.talosintelligence.com/2018/10/vuln-spot-vmware-dos.html

8. US Advanced Weaponry Is Easy to Hack, Even by Low-Skilled Attackers

Major weapon systems developed by the US Department of Defense are riddled with vulnerabilities that make them an easy target for adversaries trying to control them or disrupt their functions. As the DoD plans to spend about $1.66 trillion to advance its weapons arsenal, the US Government of Accountability Office (GAO) finds reports from various development stages of the systems showing that mission-critical vulnerabilities are a regular find in "nearly all weapon systems that were under development."

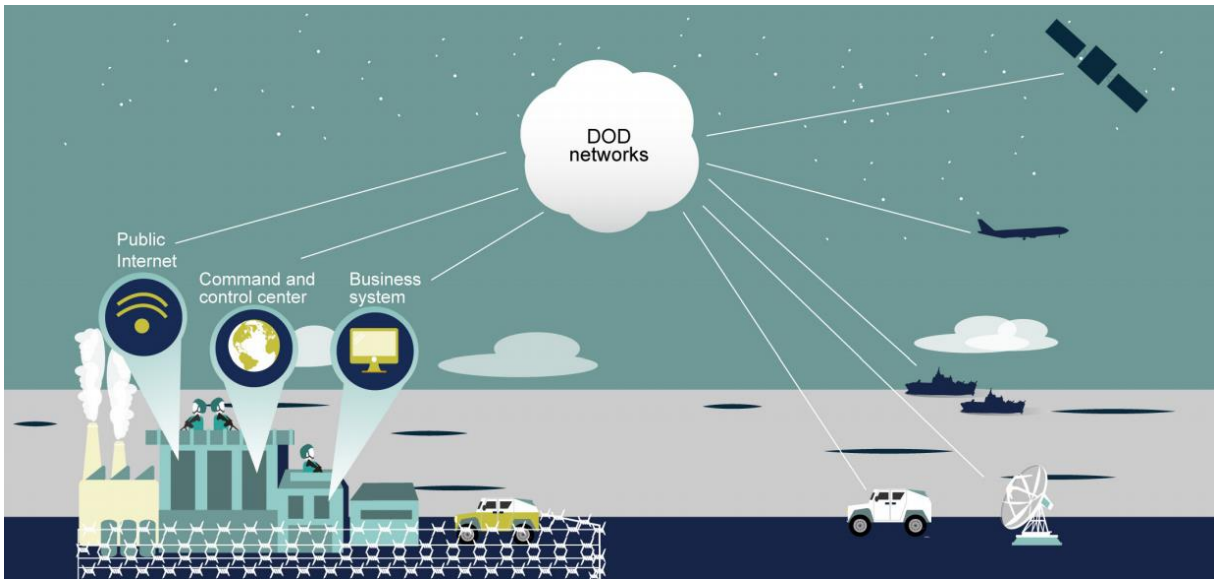
Testing teams charged with probing the resilience to cyber attacks were able to take control or disable the target using basic tools and techniques. Sometimes, just scanning the system caused parts of it to shut down. GAO says that it found test records about credentials management being so poor that one team was able to guess the admin password of a system in nine seconds. The most likely reason for this was that the administrators did not change the default passwords in the software installed on the weapon system.

The trouble runs deeper

Multiple factors allowed the intrusion of the red team to remain undetected, sometimes for several weeks. GAO officials learned about cases where the trespassers were deliberately loud in their actions, yet the operators of the system failed to see the signs of the suspicious activity.

Misconfiguration of alert systems is part of the problem as multiple reports indicated that the intrusion detection systems (IDS) raised the flag correctly, but the operators did not receive the alert. In another, the IDS showed a permanent alert status, making it undependable to the user.

"One test team emulated a denial of service attack by rebooting the system, ensuring the system could not carry out its mission for a short period of time. 41 Operators reported that they did not suspect a cyber attack because unexplained crashes were normal for the system," says the report from GAO.



System operators are also to blame

Some of the attacks went completely unnoticed despite evidence in the activity logs because the operators did not bother to check them.

Reports of tests revealed cases when intrusions were detected but the operator failed to deploy an effective counteraction. In one instance, the defense measures were easily bypassed by the test team. In another, outside assistance was necessary to restore the computer.

The red team having fun

Finding a way to gain access to the target and control it, fully or partially, was the main objective, but the teams assessing the vulnerable state of the weapon systems also had their fun.

Internal reports show that when they got a foothold on the system, the testers were able to escalate privileges and move around easily, even watch in real time every move of the operators of the target systems.

Copying, deleting or modifying data was just as regular an occurrence as the discovery of major vulnerabilities. One team even managed to steal 100GB of data.

Among the pranks they pulled on the defenders, the "attackers" displayed a pop-up message on the user's terminal, "instructing them to insert two quarters to continue operating," the GAO report notes.

Root cause analysis

GAO's audit lasted for over a year, from July 2017 until October 2018, and involved examining cybersecurity reports on selected weapons tested between 2012 and 2017.

The congressional watchdog also looked into the steps the DoD is taking to improve the security stance in the weapon systems, by analyzing acquisition, requirements, testing policies and guidance revised since 2014.

The conclusion is dire, though: the DoD is late to the game and missed important steps for the development of weapons capable to withstand cyber attacks.

The cyber defenses focused mostly on the infrastructure and the networks, not on the weapons themselves, which also evolved into computerized systems that require at least the same level of attention.

"Multiple factors contribute to the current state of DOD weapon systems cybersecurity, including: the increasingly computerized and networked nature of DOD weapons, DOD's past failure to prioritize weapon systems cybersecurity, and DOD's nascent understanding of how best to develop more cyber secure weapon systems," GAO officials conclude.

Despite loud warnings about cybersecurity risks, the DoD took its time making this aspect a priority. The result is a basic understanding of today's issues and how they can be exploited by a real adversary.

According to GAO, some program offices still struggle to recognize the cybersecurity implications as far as system design and connectivity are concerned.

Probably discounting the modern attack scenarios, there are officials that dismissed some of the test results as being unrealistic; they also showed a strong belief that the weapon systems were properly protected.

The current state discovered by GAO may be just the tip of the iceberg, as this is the agency's first audit of weapon systems acquisitions and it did not analyze the problems in a larger context that includes security of contractor facilities, Internet-of-Things devices or industrial control systems.

Source: https://www.bleepingcomputer.com/news/security/us-advanced-weaponry-is-easy-to-hack-even-by-low-skilled-attackers/

9. Fake Adobe Flash Updates Hide Malicious Crypto Miners

A fake Adobe update actually updates victims' Flash – but also installs malicious cryptomining malware.

While fake Flash updates that push malware have traditionally been easy to spot and avoid, a new campaign has employed new tricks that stealthily download cryptocurrency miners on Windows systems.

To the average user, the newly discovered samples, which have been active as early as August, seem legitimate. The samples act as Flash updates, borrowing pop-up notifications from the official Adobe installer, and even actually updating a victim's Flash Player to the latest version.

Unbeknownst to the victims, while the legitimate Flash update has occurred, a tricky XMRig cryptocurrency miner is quietly downloaded and runs in the background of the infected Windows computers.

"A recent type of fake Flash update has implemented additional deception," said Brad Duncan Threat Intelligence Analyst with Palo Alto Networks' Unit 42 group, in a post about the new campaign Thursday. "As early as August 2018, some samples impersonating Flash updates have borrowed pop-up notifications from the official Adobe installer. These fake Flash updates install unwanted programs like an XMRig cryptocurrency miner, but this malware can also update a victim's Flash Player to the latest version."

While searching for fake Flash updates, researchers noticed Windows executable file names starting with AdobeFlashPlayer, from non-Adobe, cloud-based web servers. The downloads always contain the string "flashplayer_down.php?clickid=" in the URL.

Network traffic during the infection process consists mainly of the Flash update. Interestingly, the infected Windows host generate an HTTP POST request to [osdsoft[.]com], a domain associated with updaters or installers pushing cryptocurrency miners.

But, the research team noticed that their infected systems soon generated traffic associated with the XMRig cryptocurrency mining over TCP port 14444 – as the malicious cryptominer began to take sway and utilize the systems' power for mining.

While the Adobe pop-up and update features make the fake installer seem more legitimate, potential victims will still receive warning signs about running downloaded files on their Windows computer, said Duncan.

"This campaign uses legitimate activity to hide distribution of cryptocurrency miners and other unwanted programs," the research team said. "Organizations with decent web filtering and educated users have a much lower risk of infection by these fake updates.

Source: https://threatpost.com/stealthy-fake-adobe-flash-updates-tout-malicious-crypto-miners/138199/

10. Facebook States 30 Million People Affected by Last Month's "View As" Bug

Remember that bug Facebook revealed a couple of weeks ago that may have affected 50 million users if not more? Well Facebook has stated that 30 million of those user had their access tokens stolen by attackers according to Facebook.

This bug was part of Facebook's "View As" tool, which allows you to view your profile as it would appear to someone else on Facebook. Attackers chained 3 vulnerabilities together to exploit a bug in this feature and steal a user's, and their friends, access tokens. These access tokens could then be used to login to the associated account and provide full access to everything on it.

In a blog post, Facebook has decided to downplay the attack to make it appear as less serious than it actually is.

"We now know that fewer people were impacted than we originally thought," stated the Facebook's update. "Of the 50 million people whose access tokens we believed were affected, about 30 million actually had their tokens stolen. Here's how it happened:"

Isn't that great? Only 30 million.

According to the update, using accounts they already controlled, the attackers exploited the bug to steal tokens from approximately 400,000 users. The attackers then used some of those 400,000 accounts to steal the access tokens from a total of 30 million users.

"The attackers used a portion of these 400,000 people's lists of friends to steal access tokens for about 30 million people," stated Facebook's blog post. "For 15 million people, attackers accessed two sets of information – name and contact details (phone number, email, or both, depending on what people had on their profiles). For 14 million people, the attackers accessed the same two sets of information, as well as other details people had on their profiles. This included username, gender, locale/language, relationship status, religion, hometown, self-reported current city, birthdate, device types used to access Facebook, education, work, the last 10 places they checked into or were tagged in, website, people or Pages they follow, and the 15 most recent searches. For 1 million people, the attackers did not access any information."

Facebook also stated that the attackers did not have access to information related to other Facebook services such as Messenger, Messenger Kids, Instagram, WhatsApp, Oculus, Workplace, Pages, payments, third-party apps, or advertising or developer accounts.

Source: https://www.bleepingcomputer.com/news/technology/facebook-states-30-million-people-affected-by-last-months-view-as-bug/

11. Up to 35 Million 2018 Voter Records For Sale on Hacking Forum

Up to 35 million voter records have been found up for sale on a popular hacking forum from 19 states, researchers discovered.

Researchers at Anomali Labs and Intel 471 on Monday said that they discovered Dark Web communications offering a large quantity of voter databases for sale – including valuable personally identifiable information and voter history.

This represents the first indication of 2018 voter registration data for sale on a hacking forum, said the researchers. The discovery comes weeks before the U.S. November mid-term elections.

"With the November 2018 midterm elections only four weeks away, the availability and currency of the voter records, if combined with other breached data, could be used by malicious actors to disrupt the electoral process or pursue large-scale identity theft,"researchers at Anomali Labs said in a Monday post. "Given the illicit vendor claims of weekly updates of voter records and their high reputation on the hacker forum, we assess with moderate confidence that he or she may have persistent database access and/or contact with government officials from each state."

Researchers did not post what the name of the hacking forum was, or the timeline of the sales.

The disclosure affects 19 states and includes 23 million records for just three of the 19 states, researchers said. Impacted states include: Georgia, Idaho, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Mississippi, Montana, New Mexico, Oregon, South Carolina, South Dakota, Tennessee, Texas, Utah, West Virginia, Wisconsin, and Wyoming.

No record counts were provided for the remaining 16 states, but they did include prices for each state. Each voter list ranges from $150 to $12,500, depending on the state, the research team said. These prices could be related to the number of voter records per database.

The records contain voter data including full name, phone numbers, physical addresses, voting history, and other unspecified voting data.

"We estimate that the entire contents of the disclosure could exceed 35 million records," the research team said. "Researchers have reviewed a sample of the database records and determined the data to be valid with a high degree of confidence."

Researchers said that within hours of the initial advertisement, a "high-profile actor" organized a crowdfunding campaign to purchase each of the voter registration databases.

"According to the actor, the purchased databases would be made available free of charge to all registered members of the hacker forum, with early access given to donors of the project," said researchers.

So far, of the 19 available databases, Kansas has been acquired and published as part of that crowdfunding campaign – and Oregon is in the lead as the second state to be published.

Concerns around voter data in the U.S. have continued to peak as the elections draw near.

In July, a misconfigured repository bucket was found leaking the information of U.S. voters. The information was exposed on a public Amazon S3 bucket by a Virginia-based political campaign and robocalling company called Robocent.

While voter lists are not permitted to be used for commercial purposes, "State voter registration lists can be obtained at varying costs established by each state," researchers said. Those lists could include registered voters and who has voted in specific elections – but, rules still remain governing which authorized persons (such as political campaigns, journalists or academic researchers) may retrieve and use the data.

"This type of information can facilitate criminal actions such as identity fraud or allow for false submissions of changes online to voter registrations, making some legitimate voters ineligible to cast ballots," researchers said. "In a voter identity theft scenario, fraudsters can cause disruptions to the electoral process through physical address changes, deletion of voter registrations or requests for absentee ballots on behalf of the legitimate voter."

Source: https://threatpost.com/up-to-35-million-2018-voter-records-for-sale-on-hacking-forum/138295/

12. In County Crippled by Hurricane, Water Utility Targeted in Ransomware Attack

The Emotet Trojan is behind a crippling ransomware attack that hit the Onslow Water and Sewer Authority.

A "critical water utility" has been targeted in a recent ransomware attack, significantly impeding its ability to provide service in the week after Hurricane Florence hit the East Coast of the U.S.

The Attack

On Oct. 4, ONWASA first saw indications of the virus known as Emotet, a well-known polymorphic malware that has been popping up in the news for years, on its network.

Emotet stands out in its ability to self-propagate, meaning that once it's on a computer, the malware downloads and executes a spreader module. That module has a password list that it uses to brute-force access to other machines on the same network. Emotet can also spread to additional computers using a spam module that it installs on infected victim machines.

Network-spreading particularly poses as a headache for organizations, because it means that victims can become infected without even needing to click on a malicious link or attachment.

While the utility said it has "multiple layers of computer protection in place" – including firewalls and AV software – they were unable to stop the penetration. And, while the virus was at first thought to be under control, it persisted.

Then, at what may have been a timed event, the malware launched a sophisticated virus known as RYUK at 3 a.m. on Oct. 13.

Emotet has been around for years – most recently, in early July, officials in Portsmouth, N.H. said that the malware cost them $156,000 to remove after spreading to the city's entire computer network via phishing emails.

Tricky Emotet first emerged targeting banking credentials; but lately, researchers have spotted the trojan changing its tactics and its targets, catching the eye of both researchers and law enforcement this week.

"Despite its age, Emotet is far from just barely alive," researchers with Check Point Research said in a report. "It spreads itself abundantly through spam emails, network shares and the Rig exploit kit. While some features have stayed constant, during the four years of Emotet's lifecycle, modules have come and gone."

While there was no indication of who the threat actors might be behind this particular incident, earlier this year, Symantec researchers linked Emotet to threat group Mealybug, a cybercrime actor that has been active since at least 2014.

Mealybug seems to have both expanded the trojan's capabilities and its targets to become what Symantec researchers call an "end-to-end service for delivery of threats."

"Mealybug's shift from distributing its own banking trojan to a relatively small number of targets, to acting primarily as a global distributor of other groups' threats, is interesting, and backs up an observation we made… that threat actors are evolving and refining their techniques and business model to maximize profits," Symantec researchers said in a blog post.

Source: https://threatpost.com/in-county-crippled-by-hurricane-water-utility-targeted-in-ransomware-attack/138327/

13. As End of Life Nears, More Than Half of Websites Still Use PHP V5

Support for PHP 5.6 drops on December 31 - but a recent report found that almost 62 percent of websites are still using version 5.

Almost 62 percent of all websites are still running PHP version 5 – even as version 5.6 of the server-side scripting language inches toward an ominous end-of-life.

Despite end-of-life in the horizon, a new report by Web Technology Surveys found that PHP version 5 is still used by 61.8 percent of all server-side programming language websites.

And, of those using version 5, 41.5 percent of websites are using version 5.6, the report said. What this means is, security patches, upgrades and bug fixes will cease for end-of-life technology – putting that percentage of PHP-based websites using PHP 7.0 and below at risk. Researchers and developers alike have called on these websites to update to newer, supported versions of PHP 7.2. It's particularly critical given the popularity of PHP: A full 78.9 percent of all websites use PHP overall, Web Technology Surveys' report found.

It's particularly critical given the popularity of PHP: A full 78.9 percent of all websites use PHP overall, Web Technology Surveys' report found.

And content management systems are doing nothing to help this cause – Drupal is the only CMS that has posted an official notice requiring an upgrade to PHP 7 by March (three months after the PHP 5.6 end of life deadline). There has been no such notice from WordPress or Joomla. Neither responded to a request for comment from Threatpost.

Source: https://threatpost.com/as-end-of-life-nears-more-than-half-of-websites-still-use-php-v5/138352/

14. Multiple D-Link Routers Open to Complete Takeover with Simple Attack

Eight D-Link routers in the company's small/home office "DWR" range are vulnerable to complete takeover – but the vendor said it is planning on only patching two, according to a researcher.

Błażej Adamczyk of the Silesian University of Technology in Poland discovered the vulnerabilities in May, uncovering that they affect the DWR-111, DWR-116, DWR-140, DWR-512, DWR-640, DWR-712, DWR-912 and DWR-921 models. However, he claims that D-Link told him that only the DWR-116 and 111 would be patched, because the rest have reached end-of-life and will no longer be supported.

However, D-Link hasn't issued the two promised patches, so after warning the vendor in September that he would publicly disclose the flaws if they weren't addressed within a month, Adamczyk has published his findings, along with a proof-of-concept video.

A full compromise including remote command-injection can be achieved by linking three cascading vulnerabilities together to attack the router's web-based settings panel. This can be done from a local network device or from the internet, depending on the configuration of the network. Most small/home office (SOHO) users have a fairly simple set-up, with the routers connecting directly to an internet connection to feed bandwidth to multiple WiFi devices inside the home or office. That presents a pretty straightforward attack surface for an attacker.

First, a directory-traversal bug (CVE-2018-10822) exists in the web interface for the D-Link routers, which allows remote attackers to read arbitrary files via a /.. or // after a "GET /uir" in

an HTTP request. This allows the bad guys to move laterally and read files in other directories, including password files.

That's where a second vulnerability (CVE-2018-10824) comes in: Passwords are stored in plaintext, including the administrative password, which can be found in a temporary file. In a proof-of-concept, a basic command returns a binary configuration file which contains administrative username and password in cleartext as well as many other router configuration settings. Thus, by using the directory traversal vulnerability, it is possible to read the file without authentication. "The attack is too simple," Adamczyk said in a recent posting. "An attacker having a directory traversal (or local file inclusion) can easily get full router access."

A third vulnerability (CVE-2018-10823) meanwhile is what opens the door for remote code-injection. This is a shell command-injection bug in the httpd server for several series of D-Link routers.

"An authenticated attacker may execute arbitrary code by injecting the shell command into the chkisg.htm page Sip parameter," Adamczyk explained. "This allows for full control over the device internals."

To exploit this, an adversary would log into the router using the credentials he or she lifted using the first two vulnerabilities, request a certain URL as laid out in the researcher's PoC, and then be able to see the passwd file contents in the response.

"Taking all the three together it is easy to gain full router control, including arbitrary code-execution," Adamczyk said.

Adding insult to injury, the researcher explained that the first vulnerability was actually introduced in a flawed patch for an older vulnerability, CVE-2017-6190. The older flaw also contained the plaintext password issue, CVE-2018-10824 – but it wasn't addressed for all releases, according to Adamczyk.

The vendor is no stranger to remote code-execution flaws; earlier in October it patched four vulnerabilities in the software controller tool used in its enterprise-class wireless network access points that would allow RCE. And, last year it was uncovered that its D-Link router model 850L wireless AC1200 dual-band gigabit cloud router was riddled with vulnerabilities that could allow a hacker to gain remote access and control of device.

Earlier this month a report came out showing that a staggering 83 percent of home and office routers have vulnerabilities that could be exploited by attackers. Of those vulnerable, over a quarter harbor high-risk and critical vulnerabilities, according to the American Consumer Institute on router safety.

The potential ramifications aren't just about putting SOHO users themselves at risk, given that in many cases remote users rely on these routers to connect to corporate networks.

Source: https://threatpost.com/multiple-d-link-routers-open-to-complete-takeover-with-simple-attack/138383/

15. New Windows Zero-Day Bug Helps Delete Any File, Exploit Available

Proof-of-concept code for a new zero-day vulnerability in Windows has been released by a security researcher before Microsoft was able to release a fix. The code exploits a vulnerability that allows deleting without permission any files on a machine, including system data, and it has the potential to lead to privilege escalation.

Fully patched Windows 10 is vulnerable

The vulnerability could be used to delete application DLLs, thus forcing the programs to look for the missing libraries in other places. If the search reaches a location that grants write permission to the local user, the attacker could take advantage by providing a malicious DLL. The problem is with Microsoft Data Sharing Service, present in Windows 10, Server 2016 and 2019 operating systems, which provides data brokering between applications.

Will Dormann, a vulnerability analyst at CERT/CC, tested the exploit code successfully on a Windows 10 operating system running the latest security updates. Behind the discovery is a researcher using the online alias SandboxEscaper, also responsible for publicly sharing in late August another security bug in Windows Task Scheduler component.

Bug is difficult to exploit

Malware developers were quick to incorporate in their software the exploit for the previous bug disclosed by SandboxEscaper. This is unlikely to happen with the issue in Data Sharing services. Although deleting operating system files and the prospect of privilege escalation are serious threats, the bug is "low quality" and a "pain to exploit," as SandboxEscaper herself describes it.

In a text file describing the bug, SandboxEscaper says that an attacker could trigger DLL hijacking in third-party software "or delete temp files used by a system service in c:/windows/temp and hijack them and hopefully do some evil stuff."

In a conversation with BleepingComputer, Acros Security CEO Mitja Kolsek said that he could not find a "generic way to exploit this for arbitrary code execution." He noted that the exploit can easily brick the machine, though, and that there is a potential risk of DLL hijacking.

"If non-admin local attacker can write to any folder in the PATH environment variable (which would almost surely already be a security issue by itself), they could delete a DLL and plant a malicious copy there to get it executed the next time some privileged process needs it. However, I expect better attack vectors will be found," Kolsek said.

Pro tem solution until official patch

Microsoft is yet to address the issue, but a temporary solution is already available through the 0Patch platform from Kolsek's company. A micropatch candidate was ready seven hours after the zero-day vulnerability announcement, and it blocked the exploit successfully. 0Patch now delivers the stable version of the micropatch for fully updated Windows 10 1803.

Source: https://www.bleepingcomputer.com/news/security/new-windows-zero-day-bug-helps-delete-any-file-exploit-available/

16. Debunking AI's Impact on the Cybersecurity Skills Gap

Artificial intelligence is the latest buzzword to take hold of the cybersecurity industry. It is being touted, among other things, as the ultimate solution to the cybersecurity skills gap. But just how accurate is this belief?

Will AI be the cure to all our cybersecurity ailments, as human security analysts are replaced by robots powered with artificial intelligence (AI) technology? Or will it make the skills gap even worse by changing the landscape? Only time will tell, but I feel the answer lies somewhere in the middle.

Will AI Solve All Our Cybersecurity Problems?

Enterprise IT security departments are facing a serious skills shortage. Not only are they struggling to find the right talent, but there is hardly any talent to choose from. This skills shortage comes at a time when security teams are struggling with the big data problem. There is just too much data for any enterprise IT team to manage, bare minimum. But to also be able to analyze all of that data, seeking out anomalies that could signal a looming threat, is another story entirely. Even if an enterprise IT team had enough manpower to manage the data at hand, there is just no way for us as humans to analyze that much data in real time.

AI is being lauded as the long-awaited fix for these cybersecurity woes, but is that a realistic proposition? When people talk about cybersecurity's future and the promise of AI, it conjures images of security operations centers running autonomously by robots instantaneously responding to alerts after quickly ingesting contextual insights in order to decide on the best response within microseconds. But before we get carried away with the idea of robots taking over the world, we need to look a little closer.

I argue the our greatest danger with AI is not – as Hollywood would like us to believe – robots eventually causing the downfall of humanity by taking over all available jobs, but rather not fully understanding both AI's benefits and limitations. AI will never fully replace humans. In fact, it may actually make the skills gap even worse for a time, as organizations struggle to find employees who are adept at managing these new technologies. In order for IT teams to successfully implement AI technologies, they will need a new category of experts to train the

AI technology, run it, watch over its outputs and analyze the results. This will require organizations to either hire humans already trained to do so or have existing team members learn even more cybersecurity-related skills.

In this scenario, AI is not actually replacing humans but rather giving them opportunities to expand their skill sets with new tools, while it does the heavy lifting of tedious, repetitive manual processes. Organizations that accept this opportunity to help employees grow their cybersecurity skills while tempering their expectations for a fully automated workforce will make giant strides in improving their cybersecurity operations with a combination of the two.

The Dawn of AI in Identity

From an identity governance standpoint, AI has great potential to alleviate the skills gap many organizations are currently feeling, rather than making it larger. Instead of replacing humans, AI can help identity teams do their jobs better, especially when it comes to the immense volume of identity data they must sort through to find anomalies and exposure points. Business applications and data usage are growing at an exponential rate, while the volume of identities is rapidly increasing both on the human side – from employees, contractors and business partners – and the non-human side – from bots and robotic process automation. This creates an enormous amount of activity from an ever-expanding list of users that generates a tremendous amount of data.

When it comes to identity governance, enterprises want to do two things: manage risk and drive efficiency. With an identity governance program that incorporates AI and machine learning, IT teams can rely on technology to more swiftly identify ways to reduce risk and improve efficiency. In this scenario, AI and machine learning will not replace expertise, but rather these algorithms will be used as a force-multiplier for security professionals who all need to efficiently and smartly sort through an increasing amount of information to do their jobs effectively. It's a powerful combination, and it's a win-win scenario for organizations and their employees.

AI + Cybersecurity: Time will Tell

AI is still in the early stages in cybersecurity and still needs to evolve. But now is the time to consider if and where artificial intelligence fits into cybersecurity strategy for businesses today. In order to use AI to its full potential, we must accept what AI is capable of and what its limitations are.

While AI may be great for processing large amounts of data or replacing autonomous manual tasks, it will never be able to replace a security analyst's insights into the organization based on these activities. While AI may one day help bridge the cybersecurity skills gap, employees can rest assured that it will not replace human expertise. I believe it will elevate what security analysts, identity management professionals and incident responders are capable

of, helping them work smarter, making their jobs less mundane and opening the door for an even more exciting career outlook.

Source: https://threatpost.com/debunking-ais-impact-on-the-cybersecurity-skills-gap/138570/

17. UK Slaps Facebook with $645K Fine Over Cambridge Analytica Scandal

The amount is the max allowed under pre-GDPR regulation but is barely a financial slap on the risk for the social-media giant.

The UK has fined Facebook $645,000 over Cambridge Analytica's data harvesting practices, which exploited the data of 87 million users of the social network.

That represents a gnat bite for the tech giant, which generated $5.1 billion in net profit in the second quarter of the year. However, the amount is the maximum penalty available to the UK's Information Commissioner's Office (ICO) under 1998's Data Protection Act.

"But for the statutory limitation on the amount of the monetary penalty, it would have been reasonable and proportionate to impose a higher penalty," noted the regulator.

The UK's updated Data Protection Act 2018, which implements the EU's GDPR rules, stipulates a maximum fine of 4 percent of annual global turnover ($1.6 billion in Facebook's case); but, it wasn't in place at the time of the Cambridge Analytica activities.

The ICO's 27-page penalty notice [PDF] found that Facebook failed to protect users by allowing a third-party application to hand over the data of millions of platform users to Cambridge Analytica – a consulting group that took that information to conduct elaborate social engineering efforts to sway votes for various high-profile political campaigns, including that of President Donald Trump.

The ICO noted that Facebook APIs gave developers access to user data without requiring clear and proper consent for several years, between 2007 and 2014; and, that once Facebook discovered that developers could use that loophole to harvest data in 2015 and subsequently eliminated it, the ICO said Facebook did not take sufficient action to ensure that any skimmed data was deleted.

While the investigation also concluded that it did not have any specific evidence that British users' social-media data was shared with Cambridge Analytica, the lack of data-handling controls alone warrants the penalty.

The ICO had said in July that it intended to level the maximum fine in payment for potential damage done to Facebook UK users; Information Commissioner Elizabeth Denham in a media statement on Tuesday reiterated that Facebook "should have known better and it should have done better."

She added, "We considered these contraventions to be so serious we imposed the maximum penalty under the previous legislation. The fine would inevitably have been significantly higher under the GDPR," she said.

"We are currently reviewing the ICO's decision," Facebook said in a media statement. "While we respectfully disagree with some of their findings, we have said before that we should have done more to investigate claims about Cambridge Analytica and taken action in 2015."

It added, "We are grateful that the ICO has acknowledged our full cooperation throughout their investigation and have also confirmed they have found no evidence to suggest UK Facebook users' data was in fact shared with Cambridge Analytica."

Source: https://threatpost.com/uk-slaps-facebook-with-645k-fine-over-cambridge-analytica-scandal/138579/

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

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