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

Monthly Security Bulletin

November 2018

Table of Contents

Executive summary

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

- 8 years after Stuxnet was uncovered in 2010, Israeli evening news bulletin Hadashot says that Iran has admitted they have been stricken again by a Stuxnet-like attack. Only this time it is "from a more violent, more advanced and more sophisticated virus than before, that has hit infrastructure and strategic networks." *Jump to article*
- "Two zero-day vulnerabilities in Bluetooth Low-Energy chips made by Texas Instruments (and used in millions of wireless access points) open corporate networks to crippling stealth attacks. "*Jump to article*
- "A proof-of-concept (PoC) attack details how an attacker can gain access a victim's Microsoft Live webmail session, without having the person's credentials. It relies upon the hijack of a Microsoft-owned Live.com website subdomain." *Jump to article*
- Although slowly being implemented, IoT has proven itself to be one of the trends that is here to stay and become a major part of how we conduct ourselves in our daily lives and business environments. However, with its all real and potential benefits, IoT has its brings also potential threats. The bigger connectivity for the sake of convenience could lead to breaches in power grids and cause widespread blackouts. *Jump to article*
- "A new ransomware has been discovered that installs DiskCryptor on the infected computer and reboots your computer. ". Despite being done in the past in a similar way, the new current ransomware is not affiliated with the previous attacks and we should take into consideration to the good practices now to avoid them. *Jump to article*
- 81K private Facebook messages put on the market for only 10 cents per account. The more worrisome part is that the hackers claim the "trove contains a fraction of the details they have from a larger cadre of 120 million accounts." *Jump to article*
- "The lowly password is much-maligned as being the weakest link in any company's security defenses." However, often they are the only hurdle in front of the malicious actors and despite new techniques coming out they remain the easiest application. Will this change in the future? *Jump to article*
- "A fresh botnet is spreading across the landscape, targeting router equipment. So far, hundreds of thousands of bots endpoints have already been identified, and they're apparently being marshaled to send out massive amounts of spam." *Jump to article*
- "Up to 4 million online merchants who use the popular WooCommerce WordPress plugin are vulnerable to a file deletion vulnerability that could allow a rogue "shop manager" to escalate privileges and eventually execute remote code on impacted websites." *Jump to article*
- "Tech advances are accelerating the use of facial recognition as a reliable and ubiquitous mass surveillance tool, privacy advocates warn. [..] Now facial recognition appears to be on the verge of blossoming commercially, with security use-cases paving the way." *Jump to article*

- "A large-scale spam campaign has launched, spreading the Emotet banking trojan. Worryingly, the offensive has launched about a week after a fresh module for mass email-harvesting was detected for the malware" *Jump to article*
- "There is a broadly held misunderstanding that self-signed certificates are inherently bad security." They do have several key limitations, such as the fact that they never expire, but there is case to be made that sometimes they may be more sufficient or even the better choice. *Jump to article*
- "Another day, another critical WordPress plugin vulnerability. The popular AMP for WP plugin, which helps WordPress sites load faster on mobile browsers, has a privilege-escalation flaw that allows WordPress site users of any level to make administrative changes to a website." *Jump to article*
- "A strange glitch in Gmail can be exploited to place emails into a person's "Sent" folder — even if that person never sent them." A potential phishing threat that opens the door for malicious actors to exploit. *Jump to article*
- Denial of Service(DoS) attacks do not need to be complicated. The "Kitten of Doom" attack is quite easy to carry out and stop Skype for Business or Lync to work while it lasts. *Jump to article*
- "The Internet of Things – connected devices that contain network sensors to allow for remote monitoring and control, are expected to hit 75-billion devices installed by 2025. It is this vast arrange of devices used globally that has now become the playground for cybercriminals as general cybersecurity trends in 2018 bare out. IoT threats are on the rise and are transforming to penetrate various IoT devices as they are introduced to the market." *Jump to article*
- "Ford Motor Company is known for making cars and trucks; but the future for the iconic automaker might look a little more like Facebook than an assembly line." Comments from the company's COE, regarding the amount of data the company has, had consumers worried about their privacy. *Jump to article*
- In a recent statement Marriott has revealed 500 million data breach. The even more worrisome part of the statement is that the discovered "unauthorized access dates back to 2014. *Jump to article*
- "The past few years have been very intense and eventful when it comes to incidents affecting the information security of industrial systems. That includes new vulnerabilities, new threat vectors, accidental infections of industrial systems and detected targeted attacks". That are the predictions for 2019? *Jump to article*

1. New Stuxnet Variant Allegedly Struck Iran

A malware similar in nature to Stuxnet but more aggressive and sophisticated allegedly hit the infrastructure and strategic networks in Iran.

Details about the supposed new attack are superficial at the moment, as there are no details about the supposed attack, the damage it caused or its targets.

A report on Wednesday from Israeli evening news bulletin Hadashot says that Iran "has admitted in the past few days that it is again facing a [Stuxnet-like] attack, from a more violent, more advanced and more sophisticated virus than before, that has hit infrastructure and strategic networks."

The Iranian Supreme Leader Ayatollah Ali Khamenei in a televised speech on Sunday said that the country's civil defenses should adapt to fight enemy infiltration via new threats.

On the same day, General Gholamreza Jalali, Iran's head of the Passive Defense Organization that is charged with combating sabotage activity, was quoted by ISNA news agency saying that the agency discovered and neutralized "a new generation of Stuxnet which consisted of several parts" that was trying to breach Iranian systems.

Stuxnet is believed to be the creation of the intelligence agencies in the US and Israel. It is an advanced toolset specifically tailored to target Siemens industrial control system equipment. More specifically, it reprogrammed the PLCs (programmable logic controller) for centrifuges in nuclear enrichment at various facilities in Iran.

Built for sabotage purposes, the malware was stealthy in its actions and made it look like the damage it caused to the centrifuges was, in fact, the result of an accidental malfunction of the equipment.

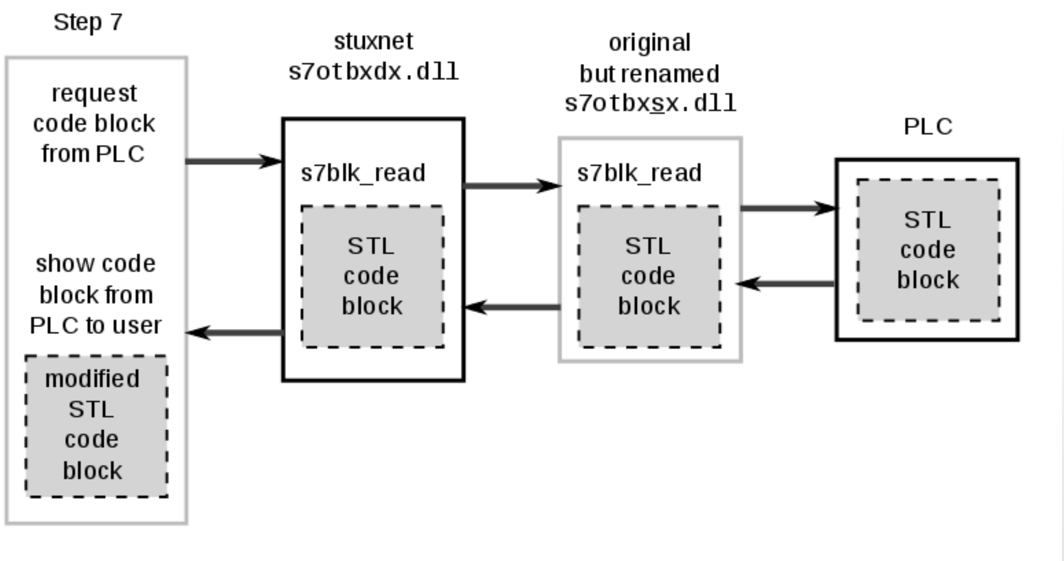


Fig. 1. Stuxnet modifying the PLC

Considering the news coverage and attention received from several cybersecurity companies that analyzed its modules, Stuxnet is unlikely to emerge in a recognizable version. General Jalil could have referred to malware with destructive modules that attempted to infiltrate and attack Iranian infrastructure.

Source: *https://www.bleepingcomputer.com/news/security/new-stuxnet-variant-allegedly-struck-iran/*

2. Two Zero-Day Bugs Open Millions of Wireless Access Points to Attack

Two zero-day vulnerabilities in Bluetooth Low-Energy chips made by Texas Instruments (and used in millions of wireless access points) open corporate networks to crippling stealth attacks.

Adversaries can exploit the bugs by simply being approximately 100 to 300 feet from the vulnerable devices. A compromised access point can then lead to an attacker taking control of the access point, capturing all traffic, and then using the compromised device as a springboard for further internal attacks.

The issue impacts Wi-Fi access points made by Cisco, Cisco Meraki and Hewlett-Packard Enterprise's Aruba, accounting for a large percentage of hardware used in corporations, according to researchers at Israeli security firm Armis. The firm discovered the two bugs earlier this year and publicly disclosed them on Thursday.

"Attacks can be devastating and carried out by unauthenticated users who can exploit these bugs and break into enterprise networks undetected while sitting in the company's lobby," said Ben Seri, head of research at Armis.

Texas Instruments released patches (BLE-STACK SDK version 2.2.2) for affected hardware on Thursday that will be available via OEMs. Cisco is expected to release patches for three Aironet Series wireless access points (1542 AP, 1815 AP, 4800 AP), along with patches for its Cisco Meraki series access points (MR33, MR30H, MR74, MR53E), on Thursday. And Aruba has released a patch for its Aruba 3xx and IAP-3xx series access points.

According to Aruba, "the vulnerability is applicable only if the BLE radio has been enabled in affected access points. The BLE radio is disabled by default."

Cisco representatives told Threatpost that the BLE feature is disabled by default on its Aironet devices.

Aruba is advising its affected customers to disable the BLE radio to mitigate the vulnerability.

"Fixed software was published for all of Cisco's affected products prior to Nov. 1. A PSIRT advisory was published at the time of the researcher's disclosure today via our established disclosure page. Meraki also published an advisory in the customer dashboard, and documentation is available to disable to involved settings," Cisco said in an email to Threatpost.

"The vulnerability can be exploited by an attacker in the vicinity of the affected device, provided its BLE is turned on, without any other prerequisites or knowledge about the device," according to researchers. The attacker does not need to be on the network, he or she just needs to be within range of access point and the BLE broadcasts/beacons.

Vulnerability Details

The first vulnerability (CVE-2018-16986) is tied to Texas Instrument chips cc2640/50 used in Cisco and Cisco Meraki access points. This vulnerability is a remote code-execution flaw in the BLE chip and can be exploited by a nearby unauthenticated hacker.

"First, the attacker sends multiple benign BLE broadcast messages, called 'advertising packets,' which will be stored on the memory of the vulnerable BLE chip in targeted device," researchers said. "Next, the attacker sends the overflow packet, which is a standard advertising packet with a subtle alteration – a specific bit in its header turned on instead of off. This bit causes the chip to allocate the information from the packet to a much larger space than it really needs, triggering an overflow of critical memory in the process."

Leaked memory is then leveraged by attackers to facilitate the running of malicious code on the chip. A backdoor is opened up on the chip, which an attacker can then use to command the chip wirelessly. From there, he or she can manipulate the main processor of the wireless access point and take full control over it locally and then remotely.

"The Texas Instrument chips are so common that an attacker could simply walk into a lobby of a company, scan for available Wi-Fi networks and begin the attack, on the assumption the BLE vulnerability is present," said Nadir Izrael, CTO and co-founder of Armis.

A second vulnerability (CVE-2018-7080) was discovered by Armis in Texas Instrument's over-the-air firmware download feature used in Aruba Wi-Fi access point Series 300 that also uses the BLE chip.

"This vulnerability is technically a backdoor in BLE chips that was designed as a development tool, but is active in these production access points," according to Armis. "It allows an attacker to access and install a completely new and different version of the firmware — effectively rewriting the operating system of the device."

Researchers said the second vulnerability exists because the over-the-air security mechanism can't differentiate between "trusted" or "malicious" firmware updates. By installing their own firmware update, an attacker can gain a foothold on the hardware and take over the access points, spread malware and move laterally across network segments, researchers said.

The vulnerabilities were collectively given the name BleedingBit from the way researchers were able to overflow packets at the bit level in the BLE memory module.

BLE is a relatively new Bluetooth protocol designed to for low-power consumption devices such as IoT hardware. It's significant for a number of reasons, such as its mesh capacities, but also for the fact it evolves the protocol from consumer uses (headphones and smartphone data transfers) to commercial IoT uses.

For this reason, Seri said there is concern that the BleedingBit vulnerabilities could impact a larger universe of BLE devices, such as smart locks used in hotel chains and point-of-sale hardware.

Last year, Armis discovered a nine zero-day Bluetooth-related vulnerabilities, dubbed BlueBorne, in Bluetooth chips used in smartphones, TVs, laptops and car audio systems. The scale of affected devices was massive, estimated to impact billions of Bluetooth devices.

Source: *https://threatpost.com/two-zero-day-bugs-open-millions-of-wireless-access-points-to-attack/138713/*

3. PoC Exploit Compromises Microsoft Live Accounts via Subdomain Hijacking

A proof-of-concept (PoC) attack details how an attacker can gain access a victim's Microsoft Live webmail session, without having the person's credentials. It relies upon the hijack of a Microsoft-owned Live.com website subdomain.

The PoC, developed by CyberInt, demonstrates what it characterizes as a "high-severity vulnerability" in a Microsoft Live subdomain (now fixed) that could have been leveraged for full Microsoft account takeover. From there, an adversary could have carried out broad attacks against multiple organizations and their customers.

While the PoC was specifically for a fixed issue, it demonstrates that session hijacking can open the door to advanced attacks, depending on the domain in question.

Subdomains are areas of a main website that can be used to host things like HR information, marketing materials, extranet sites, customer portals, promotional materials, microsites and so on; i.e., marketing.company[.]com, if it existed, would be a subdomain of company[.]com. Subdomain URL names are sometimes also aliases for content hosted on a cloud service, or they redirect traffic to a different domain – and this is where the trouble comes in.

These subdomains can become open to session-hijacking (i.e., takeover) when they're no longer used by their original owners, because many organizations simply don't remove or update dormant and expired pages and accounts.

"A threat actor can review the target organization's domain name server (DNS) information to determine if any subdomain records are configured to redirect or act as an alias for either an expired domain or a disused third-party [cloud] service," explained CyberInt, in a white paper shared with Threatpost. "In the case of expired domains, the threat actor can purchase the domain from any registrar or, in the case of third-party services, configure a new service using a previously configured or expired name to hijack the subdomain."

The PoC makes use of the latter tactic. Using a tool that CyberInt developed in-house to find subdomains that are vulnerable to session-hijacking, it found a subdomain of Live.com called "Windows Live," hosted on the Azure cloud platform. The subdomain lacked an updated DNS configuration, which opened the door to hijacking.

"Many cloud-based services allow you to do a manual configuration for your subdomain," Jason Hill, CyberInt lead researcher, told Threatpost in an interview. "But if the service hosted on that subdomain is shut down, and the DNS settings are not updated, suddenly the URL is pointing to an unconfigured cloud service. This allows another person to go in, configure that cloud service, and use the exact same subdomain name for their own purposes. They can log in and effectively take control of the old identity."

Once a subdomain has been hijacked, the threat actor can then take advantage of the reputation and legitimacy of the target organization to mount a range of attacks. This includes publishing content that appears to originate from the target's own website. Use cases include posting fake content meant to create reputational damage; getting past blacklist checks; hosting phishing or spear-phishing content to target the organization's employees or customers; create watering-hole attacks; and leveraging the subdomain for web-application attacks, such as cross-site request forgery (CSRF) and cross-site scripting (XSS), as well as authentication bypass and account takeover.

In the case of the Live subdomain, CyberInt researchers decided to see if more advanced attacks would be possible.

"We wanted to see what we could do," Hill explained to Threatpost. "We could see that Microsoft Live cookies can be configured to be accessible by all Live subdomains, so we developed a PoC code that could steal any cookies that a user has."

So an attacker could create a phishing email that says, log on and update your Live account. That could direct victims to the hijacked subdomain. It's convincing, given that the site is a legitimate Live.com domain. Adversaries could then write a script that steals and and then leverages the stolen cookies to gain access to various services.

As the firm explained in its white paper, "In this instance the PoC, having hijacked a Microsoft-owned live.com subdomain, weaponizes it by hosting a Flask (Python) application that would hijack the webmail session of any visiting victim."

For testing purposes, this PoC simply takes a screenshot of the victim's webmail inbox – although the firm said that it would be "trivial" to modify the attack to perform other unscrupulous tasks. Hill noted that it would be easy to use this same method to steal information from the mailbox or to send out emails; also, the gambit would work for gaining access to user sessions on other Live.com services.

While the Live.com subdomain was the subject of the PoC, Hill noted previous research showing that 96 percent of Fortune 500 companies have subdomains in place, and about a quarter of them are at risk for subdomain hijacking. It's not a new phenomenon, but one that remains an issue in cloud and web security.

"In practice, maintaining complex DNS configurations in ever-changing environments can result in legacy records being forgotten or inadvertent mistakes being made," according to Cyberint's report. "Without robust processes to sanity check new records and audit old records, many will fail to resolve mistakes and remove dormant or expired entries."

Source: https://threatpost.com/poc-exploit-compromises-microsoft-live-accounts-via-subdomain-hijacking/138719/

4. How an IoT Botnet Could Breach the Power Grid and Cause Widespread Blackouts

The Internet of Things (IoT) poses a major threat to our national infrastructure. An IoT botnet comprised of high-wattage devices such as air conditioners, heaters and washing machines could enable cybercriminals to launch a large-scale, coordinated attack on the power grid.

This finding, which was part of a study presented by Princeton researchers at the 2018 USENIX Security Symposium in August, demonstrates that the more interconnected our world becomes for the sake of convenience, the larger the implications for security.

Introducing MadIoT, the Latest IoT Security Threat

The presentation showcased a new class of potential attacks called "manipulation of demand via IoT (MadIoT)" that can use botnets to manipulate the power demand in the grid and cause widespread local power outages, and even large-scale blackouts. The attacks target the demand side of the national grid instead of the supply side, which includes heavily protected assets such as power lines and plants.

“Power grid security standards are all based on the assumption that the power demand can be predicted reliably on an hourly and daily basis,” the researchers wrote in their report. “Power grid operators typically assume that power consumers collectively behave similarly to how they did in the past and under similar conditions.”

This is particularly concerning now that some individuals, companies and government agencies are using IoT applications to control these power-sucking appliances, many of which have poor security measures in place.

How an IoT Botnet Could Roil the Energy Sector

The researchers examined three categories of attack by running simulations on real-world power grid models. The simulations found that MadIoT attacks can lead to local power outages and, in the worst cases, large-scale blackouts. These attacks could also be used to increase the cost of operating the grid, which would benefit a few utilities in the electricity market.

Let’s take a closer look at how these three scenarios played out.

In the first scenario, using simulators on the small-scale power grid model of the Western System Coordinating Council (WSCC), the researchers found it would take 90,000 air conditioners and 18,000 electric water heaters to disrupt the power demand in a targeted geographical area.

In another scenario, the researchers discovered that even a “small increase in power demands may result in line overloads and failures.” Using a model of the Polish power grid from summer in 2008, the researchers revealed that an increase of only 1 percent in demand would lead to a cascading grid failure with 263 line failures and outages for 86 percent of customers. In this scenario, criminals would need access to “about 210,000 air conditioners, which is 1.5 percent of the total number of households in Poland.”

In the third scenario, the researchers demonstrated that a 5 percent increase in the power demand during peak hours by an adversary can result in a 20 percent increase in the power generation cost. This kind of attack would likely be used for financial gain rather than to damage infrastructure, the researchers noted.

The third scenario mirrors an incident that occurred in early 2018 when cryptocurrency miners drove up the cost of power in Plattsburgh, New York. Because the town is so close to Niagara Falls, electricity prices in the area are extremely low, which attracted power-hungry miners, since mining requires a massive amount of energy. But all that crypto mining led to a surge in demand, and the town was forced to purchase energy on the open market to keep up. Eventually, the town imposed an 18-month moratorium on cryptocurrency mining companies while it worked to resolve the issue.

The IoT Botnet Threat Is Very Real

Taking over and enslaving interconnected, high-wattage appliances such as air conditioners and refrigerators might seem far-fetched, but as the Mirai botnet first taught us in 2016, the potential for IoT botnets to wreak havoc is very real. Just as Mirai took advantage of insecure routers and webcams, so too could an industrious attacker who gains access to the high-wattage appliances we use every day in our homes — which are increasingly connected to the outside world for the sake of convenience.

"This work sheds light upon the interdependency between the vulnerability of the IoT and that of the other networks such as the power grid whose security requires attention from both the systems security and power engineering communities," the researchers wrote.

The researchers also noted that they hope their work will help protect the grid against future threats associated with insecure IoT devices. Improved IoT security will become increasingly critical as more smart appliances hit the market.

It's Up to IoT Vendors to Prioritize Security

According to Graham Cluley, the threat of MadIoT serves as yet another reminder that IoT device manufacturers need to do more to prioritize security, such as test their appliances for vulnerabilities and work to prevent potential future compromise.

Security has been a concern around the IoT since the first connected devices came to market. With that in mind, the IoT Security Foundation published free security guidelines to help manufacturers adopt secure development.

"[IoT device vendors] sell a product at a certain cost. But having to maintain it for the next 10 years is not something that enters their thinking," said Paul Dorey, chairman of the IoT Security Foundation, in a recent Financial Times interview.

The bottom line is that both device makers and organizations deploying IoT technologies need to prioritize security as IoT devices proliferate. If they don't, they could be putting entire neighborhoods — even entire countries — at risk of a blackout.

Source: https://securityintelligence.com/how-an-iot-botnet-could-breach-the-power-grid-and-cause-widespread-blackouts

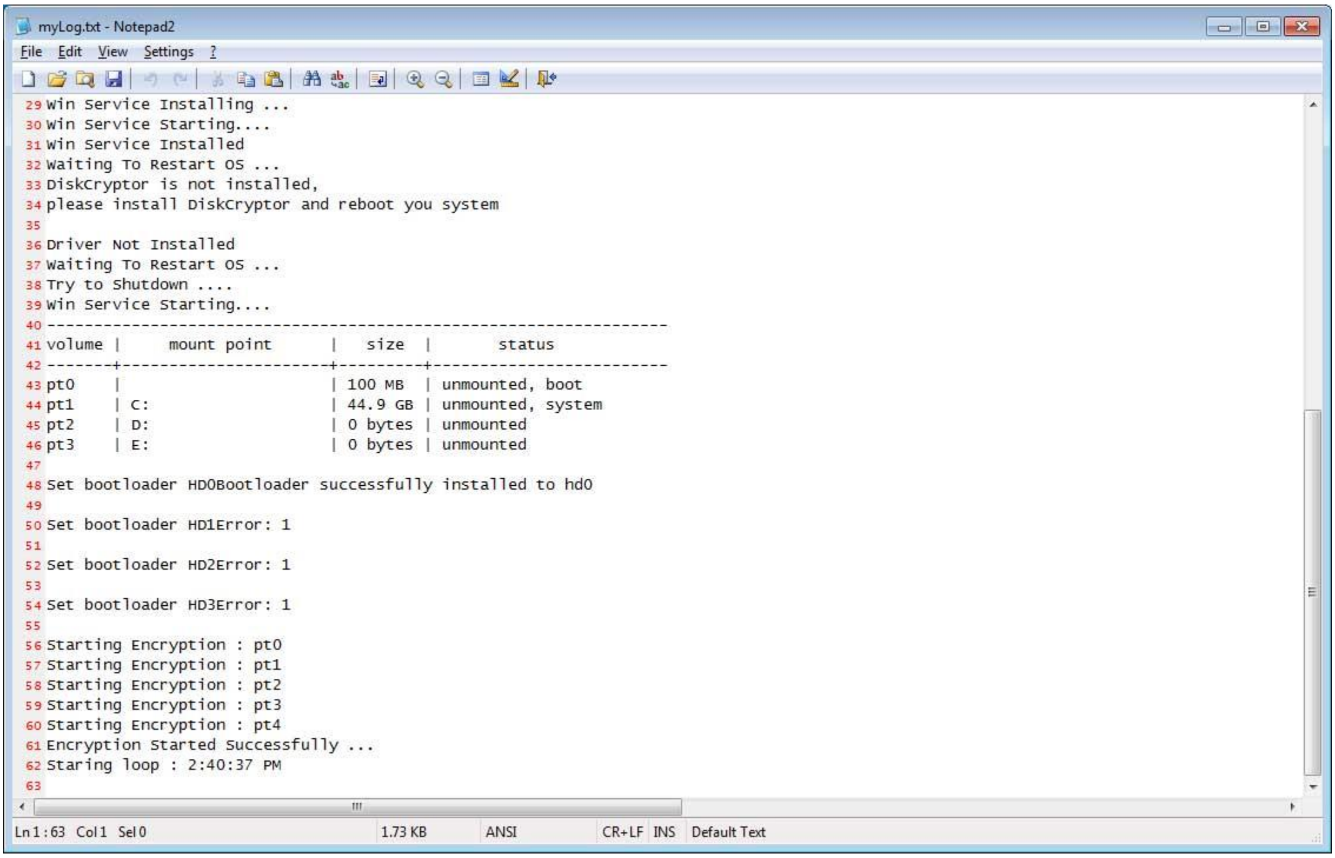
5. New Ransomware using DiskCryptor With Custom Ransom Message

A new ransomware has been discovered that installs DiskCryptor on the infected computer and reboots your computer. On reboot, victims will be greeted with a custom ransom note that explains that their disk has been encrypted and how to pay the ransom.

DiskCryptor is a encryption program that encrypts the whole disk and then prompts the user to enter a password on reboot. This password prompt occurs before Windows even starts and a user must enter the password to decrypt the drive and start the computer's normal boot process.

Discovered by MalwareHunterTeam, this ransomware is being run manually or called by another script as it requires an argument to be passed to the program, which is used as the password for DiskCryptor. It is also possible that the attackers are hacking into Remote Desktop Services and installing the ransomware manually.

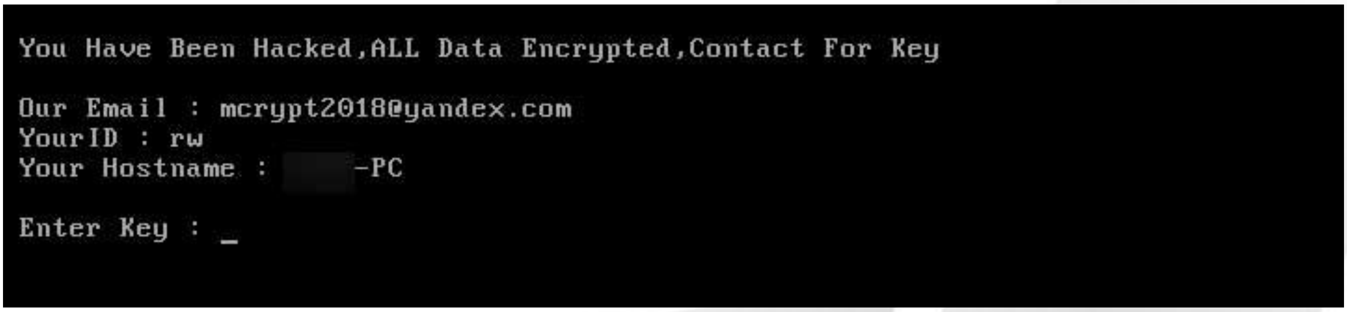
During the installation process, a log file will be created at C:\Users\Public\myLog.txt that shows the current stage of the encryption process.



```
Win Service Installing ...
Win Service Starting....
Win Service Installed
Waiting To Restart OS ...
DiskCryptor is not installed,
please install DiskCryptor and reboot you system

Driver Not Installed
Waiting To Restart OS ...
Try to Shutdown ....
Win Service Starting....
-----------------------------------------------------------------
volume |      mount point      |   size  |        status
-------+-----------------------+---------+------------------------
pt0    |                       | 100 MB  | unmounted, boot
pt1    | C:                    | 44.9 GB | unmounted, system
pt2    | D:                    | 0 bytes | unmounted
pt3    | E:                    | 0 bytes | unmounted

Set bootloader HD0Bootloader successfully installed to hd0

Set bootloader HD1Error: 1

Set bootloader HD2Error: 1

Set bootloader HD3Error: 1

Starting Encryption : pt0
Starting Encryption : pt1
Starting Encryption : pt2
Starting Encryption : pt3
Starting Encryption : pt4
Encryption Started Successfully ...
Staring loop : 2:40:37 PM

```

Fig. 2. C:\Users\Public\myLog.txt log file

Once the entire drive has been encrypted, it will reboot the computer and the victim will be shown a ransom note to contact mcrypt2018@yandex.com for payment instructions. It will then sit there waiting for the user to enter the decryption password.



```
You Have Been Hacked,ALL Data Encrypted,Contact For Key

Our Email : mcrypt2018@yandex.com
YourID : rw
Your Hostname : [redacted]-PC

Enter Key : _
```

Fig. 3. DiskCryptor Password Prompt

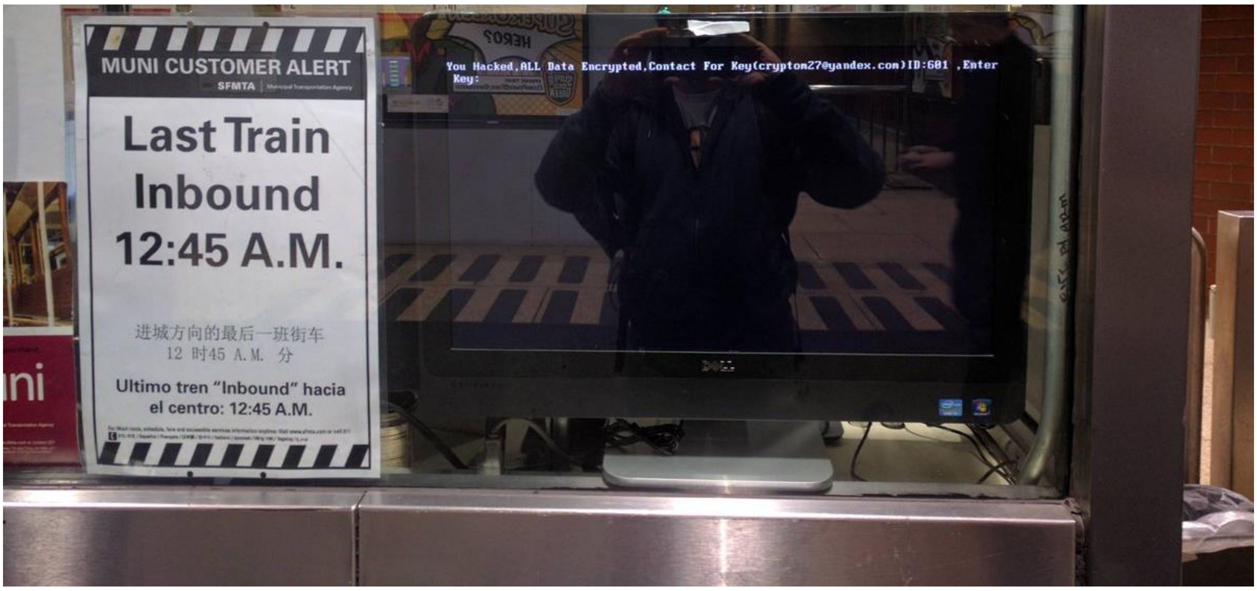
BleepingComputer has contacted the email listed by the ransom note, but had not heard back at the time of this publication.

DiskCryptor has been used by ransomware in the past

This is not the first time we have seen DiskCryptor used with ransomware.

In 2016, we saw the first use of DiskCryptor in a ransom infection called HDDCryptor, which has also been called Mamba. These ransomware infections also used custom ransom notes after encrypting the computer, but it does not appear that the current ransomware variant is affiliated with these older families.

The most publicized victim of a DiskCryptor infection was in November 2016 when 2,112 computers belonging to the San Francisco Municipal Railway system were infected with the Mamba ransomware. This effectively shut down their payment systems and caused the railway to allow passengers to use the trains for free over a weekend.



```
You Hacked,ALL Data Encrypted,Contact For Key(crypton27@yandex.com)ID:601 ,Enter
 Key:
```

Fig. 4. Twitter photo showing out of service ticket dispenser.

How to protect yourself from this Ransomware

In order to protect yourself from this ransomware, or from any variant, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

As this ransomware may be installed via hacked Remote Desktop services, it is very important to make sure RDP is locked down correctly. This includes making sure that no computers running remote desktop services are connected directly to the Internet. Instead place computers running remote desktop behind VPNs so that they are only accessible to those who have VPN accounts on your network.

It is also important to setup proper account lockout policies so that it makes it difficult for accounts to be brute forced over Remote Desktop Services.

For more detailed information, please see our guide on locking down Remote Desktop Services.

You should also have security software that incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following good online security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent them to you.
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore, it is important to keep them updated.
- Make sure you use have some sort of security software installed.
- Use hard passwords and never reuse the same password at multiple sites.
- If you are using Remote Desktop Services, do not connect it directly to the Internet. Instead make it accessibly only via a VPN.

Source: https://www.bleepingcomputer.com/news/security/new-ransomware-using-diskcryptor-with-custom-ransom-message/

6. Facebook Blames Malicious Extensions in Breach of 81K Private Messages

Investigators posed as buyers and were offered the messages at 10 cents per Facebook account.

Hackers have published what they claim are private messages from at least 81,000 Facebook accounts – and they say the trove contains a fraction of the details they have from a larger cadre of 120 million accounts.

In an English-language Dark Web advertisement (now taken down), the perpetrators offered the messages for 10 cents per account.

The BBC Russian Service investigated the supposed heist along with cybersecurity firm Digital Shadows. The team found that within the 81,000 Facebook users in the sample posting, those in the Ukraine and Russia are the main targets (although some others were also impacted, including in the U.K., U.S. and Brazil).

The BBC found evidence that the leaked portion of the archive is real. They contacted five Russian Facebook users included in the sample to ask them if the messages that were posted in the sample (covering things like vacation photos, a chat about a Depeche Mode concert and inter-family squabbling) were indeed their own; all five confirmed that they were.

The investigators also posed as a potential buyer and contacted the seller, who responded using the alias "John Smith". Upon questioning, Smith said that the data wasn't related to the Cambridge Analytica scandal nor the data breach revealed in September enabled via its "View As" feature.

Digital Shadows also traced the advertisement to an IP address in Saint Petersburg that the firm said has been used to spread the LokiBot password-stealing trojan in the past. However, Smith told the investigators that the data theft was not affiliated with Russian state actors.

Facebook for its part said that no hack or data breach has happened and that the messages were probably purloined via malicious browser extensions (it didn't specify which ones). However, it did announce that it's scrutinizing account security in the wake of the news, and, "we have contacted browser-makers to ensure that known malicious extensions are no longer available to download in their stores," according to Facebook executive Guy Rosen, speaking to the BBC.

He added, "We have also contacted law enforcement and have worked with local authorities to remove the website that displayed information from Facebook accounts."

Extensions are small programs that change the browser interface, add widgets, implement ad-blocking, provide background wallpaper and so on. The practice of cybercriminals abusing them goes back for years.

"The problem with these extensions is that they can — and most of them do, as part of their regular operation — see all the content that browser is showing you (and change it too, for that matter)," according to a Kaspersky Lab analysis. "This ability makes them highly adept at tracking the user's online movements and collecting various data. The case at hand is about data harvested from Facebook pages. But in principle, any information can be stolen this way. Banking data, for example, is also far from immune."

Even if the incident does not arise from any oversight by Facebook, the social-media giant is still feeling the fallout. On Twitter, users were quick to call this a par-for-the-course occurrence. Users made comments like, "WTF is up with Facebook?" and posted a variety of memes.

The #DeleteFacebook movement got a boost from the news, too. Lobo de Playa for instance tweeted under the hashtag, "You tell Facebook where you live, where you're from, where you work, how much $ you make, where you shop, where you vacation, how many kids you have, their ages, birthdays & schools, and everywhere you go every hour of every day. What could possibly go wrong?"

Source: https://threatpost.com/facebook-blames-malicious-extensions-in-breach-of-81k-private-messages/138770/

7. Passwords: Here to Stay, Despite Smart Alternatives?

The lowly password is much-maligned as being the weakest link in any company's security defenses. That's for good reason: It's a fact that password reuse, a lack of strong passwords, a failure to change them on a regular basis and other human errors plague the efficacy of this de facto standard for authentication. And that, in turn, has spurred start-ups, established security companies, industry coalitions and government agencies to work on concepts for moving beyond it. But the state of play for these efforts is still immature in terms of adoption.

The stakes are of course high: Nearly all data breaches start with compromised passwords. These are harvested via sophisticated phishing, brute force attacks, social engineering, malware exfiltration and more – and yet, the password remains the first, and sometimes only, line of defense against cyberattacks.

Alternatives to passwords include biometrics (like Apple's FaceID function), social media authentication (like "Log In with Facebook"), and more unusual ideas like two-tap authentication, where a browser-based button opens an email link to verify a person's identity. There's also the FIDO Alliance's FIDO 2.0 universal two-factor authentication standard, which is being adopted by financial institutions worldwide; and its offshoots, like the World Wide Web Consortium's WebAuthn approach, which eliminates the password requirement by implementing a cryptographic technique aimed at reducing friction for users.

"The login experience is continually changing based on user demand and the need to protect against today's sophisticated cybercriminal landscape," said Martin Gontovnikas, vice president of marketing and growth at Auth0, which is an identity-as-a-service vendor that implements WebAuthn. "Passwordless [approaches are] a signal of the kind of industry change we are all heading toward."

At least one security researcher, however, has declared that efforts to kill the password are set up to fail from the get-go, because alternate authentication systems have a fundamental usability problem: They require the user to learn how to do something different from what they're used to.

"The one thing that the humble password has going for it over technically superior alternatives is that everyone understands how to use it. Everyone," said Troy Hunt, creator of HaveIBeenPwned, in a blog published Monday. He added, "As soon as you ask people to start doing something they're not familiar with, the risk of them simply not going through with it amplifies and defeats the whole point of having the service in the first place."

Hunt acknowledged the promise of biometric approaches like Apple's FaceID and FIDO/WebAuthn, but noted, "they don't replace passwords, rather provide you with an alternate means of authenticating." He added that with WebAuthn, "the great hope is that it might redefine authentication to online services in an open, standardized way and ultimately achieve broad adoption. But that's many years out yet."

Statistics bear out this declaration: While alternatives to passwords are showing up more and more across services and application logins, in the grand scheme of things, these approaches have many inroads to make before they even come close to replacing passwords.

In a survey of its users released over the summer, Auth0 found that only 19.4 percent are using its WebAuthn-based "Passwordless" feature. Social-media verification fares better, with Google leading the pack (60.3 percent), followed by Facebook (24.1 percent). Trailing far behind though are LinkedIn (8.8 percent), GitHub (7.1 percent), and Windows Live (6.8 percent). And only 11.4 percent of Auth0 customers are using risk-based multifactor authentication, which uses factors such as geographic location, IP filtering, type of device and other tell-tale hints for identity verification.

"Adoption rates of MFA are on the low end due to the perception of added friction it supposedly creates for users, but it's a critical feature for stopping phishing attacks, as well as decreasing the probability of getting hacked," the report noted.

Those numbers represent a cross-section view of one customer set that already uses a password management platform (Auth0). Percentages across the general corporate population are likely much lower. Setting this against the backdrop of an ongoing explosion of password usage, and it becomes clear that killing the password is perhaps an unrealistic goal.

A report from Cybersecurity Ventures last year found that the number of passwords in use will likely surpass 300 billion by 2020. In just a few years, humans will be using over 100 billion passwords (while the number of people online is expected to grow to a little over 4 billion by 2020), with IoT devices and connected machines accounting for an additional 200 billion passwords.

While passwords are likely to be with us for some time, the prevalence of data breaches may spur corporations to explore alternatives, despite any added user friction that they may introduce: Gartner predicts that, through the end of 2020, enterprises that invest in new authentication methods and compensating controls will experience 50 percent fewer identity-related security breaches than peers that do not.

"Some of these controls can provide other significant security benefits, and implementation can likely be justified on those benefits alone," said the firm. "A secure email gateway (SEG), for example, can help combat phishing attacks. Other controls are specific to password risks, and the decision to implement should be made on a cost-benefit basis."

Hunt, for his part, said that companies should look for solutions that "improve the password situation rather than solve it… without fundamentally changing the way people authenticate."

For instance, Hunt noted in an earlier posting that taking into account anomalies to behavioral norms is a smarter way to beef up authentication security. He recommended not eliminating passwords, but rather implementing a staged access model.

"Once someone is successfully authenticated, should they have full access to all features?" he said. "For example, if it took a few goes to get the password right and they've come in from a previously unseen browser in a different country to usual, should they have unbridled access to everything? Or should they be limited to basic features and must verify they still control the registered email address before doing anything of significance?"

Self-proclaimed "password-killers," on the other hand, are unrealistic in their goals, he argued.

"Every single solution I've seen that claims to 'solve the password problem' just adds another challenge in its place thus introducing a new set of problems," he said. "This is why [new approaches are] not a password killer and why, for the foreseeable future, we're just going to have to continue getting better at the one authentication scheme that everyone knows how to use: passwords."

Source: https://threatpost.com/passwords-here-to-stay-despite-smart-alternatives/138784/

8. Rapidly Growing Router Botnet Takes Advantage of 5-Year-Old Flaw

A fresh botnet is spreading across the landscape, targeting router equipment. So far, hundreds of thousands of bot endpoints have already been identified, and they're apparently being marshaled to send out massive amounts of spam.

The botnet first emerged in September, according to 360Netlab telemetry, which dubbed it BCMUPnP_Hunter. It's so-named because of its penchant for infecting routers that have the BroadCom Universal Plug and Play (UPnP) feature enabled. The botnet takes advantage of a known vulnerability in that feature, which was discovered in 2013.

Multilayered Proxy Architecture

BCMUPnP_Hunter is essentially a self-built proxy network, according to researchers, which initially looks like it's being used to push out spam from web mail sources. The team said that the malware is well-written, and that it "seems that the author has profound skills and is not a typical script kid."

The firm's honeypot first detected multiple scan spikes on TCP port 5431; from there, it became clear that the chain of infection relies on multiple proxies.

"The interaction between the botnet and the potential target takes multiple steps, it starts with TCP port 5431 destination scan, then moving on to check target's UDP port 1900 and wait for the target to send the proper vulnerable URL," the team explained. "After getting the proper URL, it takes another four packet exchanges for the attacker to figure out where the shellcode's execution start address in memory is, so a right exploit payload can be crafted and fed to the target."

The sample of the botnet consists of two parts, the shellcode and a main payload. The latter includes a probe for the BroadCom UPnP vulnerability, and a proxy access network module.

On a more granular level, it executes a series of commands from the command-and-control server (C2). First, it scans ports for potential targets, and if found, the target IPs will be reported to a loader, which will then complete the subsequent infection process.

For the proxy service, the bot accesses the address provided and reports the access result to the C2.

"This can generate real economic benefits. Attackers can use this command to build a proxy network, and then profit from doing things such as sending spam, simulating clicks, and so on," researchers said. "The [TCP] proxy currently communicates with well-known mail servers such as Outlook, Hotmail, Yahoo! Mail, etc. … We highly suspect that the attacker's intention is to send spams."

The BroadCom UPnP Vulnerability

One notable aspect of the botnet is that it's leveraging a flaw that's existed for at least five years.

UPnP is a set of networking protocols that lets disparate devices on the same network – like personal computers, printers, internet gateways, Wi-Fi access points and mobile devices – automatically communicate and share information between each other.

In Broadcom's chip-level implementation of UPnP, used by hundreds of manufacturers, a remote preauth format string vulnerability exists that can be exploited to write arbitrary values to arbitrary memory addresses, and also to remotely read router memory. According to DefenseCode, which found the flaw, successful exploitation allows an unauthenticated attacker to execute arbitrary code with root privileges. Patches have been made available for most models, but millions of unpatched routers remain in the wild, according to DefenseCode.

Growing Threat

In terms of the size of the infection, the telemetry data released Wednesday showed that the botnet is growing rapidly. It performs scans for vulnerable routers every one to three days; and, 360Netlab found there to be 3.37 million unique IP addresses for infected devices in total. However, it’s likely that this number includes a lot of duplicates — addresses for devices whose IP addresses have just changed over time.

In a more realistic tally, the average number of bots doing the scans observed by the company is around 100,000 endpoints; but the number of potential infections may be as many as 400,000 according to a Shodan search, researchers said.

A closer look at the scans show that 116 different types of devices have been infected, including router models from ADB, Broadcom, D-Link, Digicom, Linksys/Cisco, NetComm, UTStarcom, ZyXEL and others.

To protect against botnet infection, users should update their routers to the latest firmware versions.

Source: https://threatpost.com/rapidly-growing-router-botnet-takes-advantage-of-5-year-old-flaw/138869/

9. WordPress Flaw Opens Millions of WooCommerce Shops to Takeover

A file delete vulnerability in WordPress can be elevated into a remote code execution vulnerability for plugins like WooCommerce.

Up to 4 million online merchants who use the popular WooCommerce WordPress plugin are vulnerable to a file deletion vulnerability that could allow a rogue “shop manager” to escalate privileges and eventually execute remote code on impacted websites.

Researchers at RIPS Technologies trace the bug to an unpatched design flaw in the privilege system of WordPress which can lead to an attack. While the flaw impacts many plugins on WordPress, one of the bigger impacted plugins is WooCommerce, an open source e-commerce plugin designed for small to large-sized online merchants using WordPress. WooCommerce powers 30 percent of all online stores — more than any other platform, according to WordPress.

“The vulnerability allows shop managers to delete certain files on the server and then to take over any administrator account,” Simon Scannell, security researcher with RIPS Technologies, said in a Tuesday post.

WooCommerce establishes “roles” for users ranging from customer, shop manager to admin. The shop manager role allows a user to manage all settings within WooCommerce platform, such as creating and editing products.

After a payload is injected that deletes the WooCommerce plugin, an attacker in the “shop manager” role can access the “admin” role.

A bad actor in the "shop manager" role could open the vulnerable log manager in WordPress and inject a payload to delete the WooCommerce plugin. By deleting this, it disables runtime restrictions on the plugin and the attacker can then edit and takeover the admin account.

"Arbitrary file deletion vulnerabilities aren't considered critical in most cases as the only thing an attacker can cause is a Denial of Service by deleting the index.php of the website," Scannell wrote. "[We] detail how deleting certain plugin files in WordPress can disable security checks and then leads to a full site takeover."

An admin account takeover by shop managers occurs because WordPress assigns filters to different roles – in this case WooCommerce roles. Roles are independent of one another and exist even if a plugin is inactive. The roles are stored in the database as a core setting of WordPress – however, it means that they only get executed when the plugin is active.

"The issue is that user roles get stored in the database and exist even if the plugin is disabled," according to Scannell. "This means that if WooCommerce was disabled for some reason, the meta privilege check which restricts shop managers from editing administrators would not execute and the default behavior of allowing users with edit_users to edit any user, even administrators, would occur."

That would allow shop managers to update the password of admin accounts and take over the entire site.

The exploit requires nothing more than an attacker being in control of an account with the user role "shop manager." However, the exploit is not perfect – one major drawback is that when executing the exploit, all data is lost on the target site, Scannell said.

A potential attacker could access the shop manager role via XSS vulnerabilities or phishing attacks, and then exploit the flaw to take over any administrator account and execute code on the server.

Scannell reported the arbitrary file deletion vulnerability in August, and a patch was released in October. Automattic, the company behind both WordPress and WooCommerce, did not respond to a request for further comment.

WordPress has faced other varying flaws over the past year. In August, researchers outlined a proof-of-concept exploit that would enable bad actors to target a severe vulnerability in the PHP programming language behind several major CMS companies, including WordPress. And in June, WordPress patched two bugs rated "medium" in its tooltips plugin, including one that can allow bad actors to do anything an administrative user would be able to do on a WordPress site.

Source: https://threatpost.com/wordpress-flaw-opens-millions-of-woocommerce-shops-to-takeover/138861/

10. New Boom in Facial Recognition Tech Prompts Privacy Alarms

Tech advances are accelerating the use of facial recognition as a reliable and ubiquitous mass surveillance tool, privacy advocates warn.

Somewhat quietly over the past couple of years there has been a flurry of breakthroughs in biometric technology, led by some leapfrog advances in facial recognition systems.

Now facial recognition appears to be on the verge of blossoming commercially, with security use-cases paving the way.

Last week, SureID, a fingerprint services vendor based in Portland, Ore., announced a partnership with Robbie.AI, a Boston-based developer of a facial recognition system designed to be widely deployed on low-end cameras.

The partners aim to combine fingerprint and facial data to more effectively authenticate employees in workplace settings. And their grander vision is to help establish a nationwide biometric database in which a hybrid facial ID/fingerprint can be used for things such as fraud-proofing retail transactions, or, say, taking a self-driving vehicle for a spin.

Some big questions about privacy, civil rights and civil liberties loom on the immediate horizon – and still must be fully addressed. But there is no denying that facial recognition has leapt to the front of the pack of alternative biometric authentication methods.

“Facial recognition’s benefits far outweigh alternative biometric methods in speed and ease in processing,” says Steve Surfaro, co-chair of the security applied sciences council at ASIS International. “Also, since artificial intelligence and deep learning neural networks have become mainstream, the reliability of facial recognition as taken a quantum leap.”

Natural Interface

Some of the most interesting advances are unfolding in the area of identifying individuals acting naturally in front of a surveillance camera. Robbie.AI, for instance, is honing a system tuned to recognized human emotion.

“Your face provides strong biometric cues, even if you dye your hair,” says Karen Marquez, Robie.AI’s chief executive officer. “Iris and retina are somewhat intrusive alternatives, as you need to place yourself close to the sensors, and that’s not a natural.”

SARF is capable of identifying people with heavy makeup, under poor lighting conditions and when portions of a face are obstructed by a cellphone.

Another example comes from Seattle-based tech company RealNetworks, where Mike Vance, senior director of product management, has received dozens of recent queries from K-12 schools across the nation seeking to participate in RealNetworks’ Secure, Accurate Facial Recognition (SAFR) program.

SAFR was rolled out with little fanfare at two Seattle pilot schools earlier this year. It combines commodity video surveillance cameras and PCs with facial recognition software supplied by RealNetworks. The system instantly recognizes teachers, administrators and parents. It open security doors for them and alerts security officers whenever a surveillance camera catches sight of an unauthorized adult on school property.

“The level of accuracy that we, and others, have been able to achieve far surpasses what was possible three years ago,” says Vance. “We can now tell you whether or not somebody who’s in front of a camera is who they’re asserting to be. We can find them out of millions of people in a database in a fraction of a second.”

Robie.AI and RealNetworks are by no means alone pushing facial ID systems into the commercial market. Google, Apple, Facebook and Microsoft have poured vast resources into theoretical research in the related fields of artificial intelligence, image recognition and face analysis. And the tech giants have openly shared key findings intending to accelerate the entire field.

Math at Work

At a basic level, facial recognition software revolves around applying algorithms to the 2D or 3D images of a human face in a way that correlates the contours of the eyes, nose, lips, ears, chin and numerous other variables. Thanks to advances in sensors, processing power, data analytics and neural networks, face detection and face matching processes have become very fast even as accuracy has continued to steadily improve.

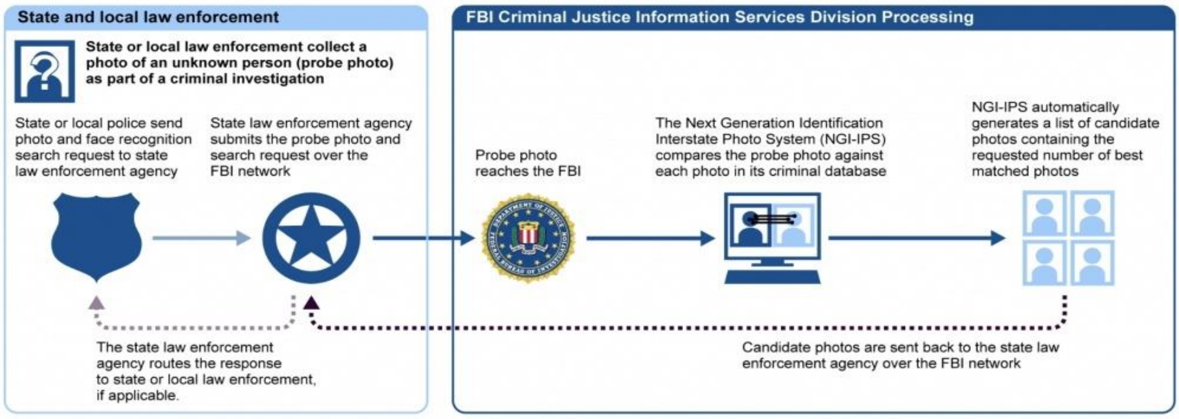

State and local law enforcement
State or local law enforcement collect a photo of an unknown person (probe photo) as part of a criminal investigation
State or local police send photo and face recognition search request to state law enforcement agency
State law enforcement agency submits the probe photo and search request over the FBI network
The state law enforcement agency routes the response to state or local law enforcement, if applicable.
FBI Criminal Justice Information Services Division Processing
Probe photo reaches the FBI
The Next Generation Identification Interstate Photo System (NGI-IPS) compares the probe photo against each photo in its criminal database
NGI-IPS automatically generates a list of candidate photos containing the requested number of best matched photos
Candidate photos are sent back to the state law enforcement agency over the FBI network

Fig.5 Face recognition searches in a criminal investigation

Illustration shows how law enforcement submits a “probe photo” of an unknown person from source such as an ATM camera to conduct face recognition searches in a criminal investigation.

The first generation of facial recognition systems actually have been in wide use for years at airports and border crossings, used primarily by border control officers and law enforcement agencies to catch criminals and deter terrorists. Their use for security access in other public settings, such as schools and workplaces, appear to be part of a natural progression.

RealNetwork's system, for instance, derives from the streaming technology it pioneered for media players in the 1990s, combined with images amassed via its RealTimes free app that let's users build photo slideshows. Customers photos and videos were used, with their permission, to train RealNetworks' facial recognition engine, which maps 1,600 data points for each face.

SAFR is tuned to identify people walking past a video cam who aren't looking squarely at the lens. It can delineate a variety of skin tones and distinguish nuances based on gender, age and geography.

"The algorithm that we've developed really relates back to our expertise from the 1990s of being able to scan video," Vance explains. "We were able to operate in extreme conditions back then, with not a lot of bandwidth to work with . . . we developed technologies to pick the right image out of a stream of video to compare against a database."

Growth Scenarios

It is become much clearer how facial ID systems hold the potential to be used much more routinely in secure access and law enforcement scenarios. And as public acceptance spreads, biometric innovations, pivoting off of facial IDs, are likely to utilized in retailing, public transportation and even healthcare, to do things like support a patient's pain management routine and even detect genetic diseases.

Buttressing this growth scenario, Allied Market Research earlier this month issued a report projecting that the "image recognition market" will rise from $17.91 billion in 2017 to $86 billion in annual revenue by 2025, a compounded annual growth rate of 22 percent. Allied's researchers noted that facial ID systems will be a big driver of that growth with both law enforcement and general commercial uses growing dramatically over that span.

The partnering of SureID and Robbie.AI embodies the path many experts believe lies ahead for commercial uses of the coming generation of facial recognition technologies. By integrating Robbie.AI's leading-edge facial ID technology with SureID's network of fingerprinting kiosks, now used to authenticate employees, the partners are taking aim at a sky-high goal, Marquez says.

They hope to supply the building blocks for a nationwide biometrics gathering system — one that can be widely shared to support broad consumer-focused initiatives, much as the tech giants shared results of their theoretical studies.

"This partnership can be a huge first step in developing holistic human biometric solutions that can protect us all against spoofing, impersonation, fraud and cybercrime," she says. "This includes everything from replacing logins, passwords and registration codes to responding to customer issues the moment they occur."

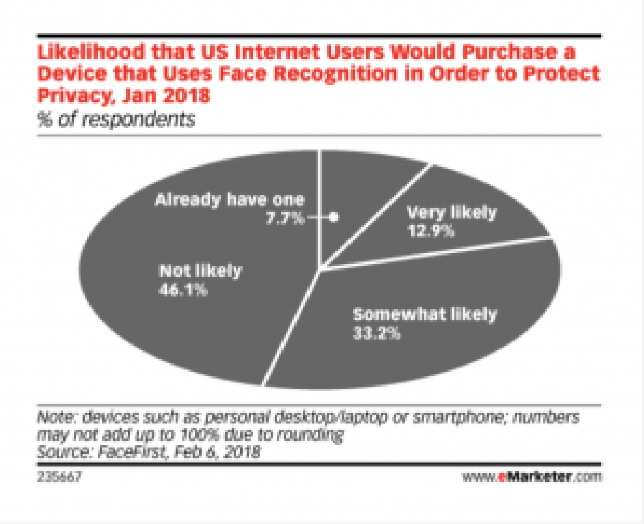
Marquez envisions a hybrid facial ID/fingerprinting system capable of alerting victims, in real time, as they are being targeted online by fraudsters. Other obvious use cases would be to provide real-time authentication to access autonomous vehicles or to control IoT devices in a smart home.

“Facial recognition and fingerprinting technologies have been around for years and if used correctly they are more secure than any written credential,” she says.

Privacy Matters

Before wider commercial uses of facial IDs can take root, one looming non-technical issue must be addressed: privacy. Jay Stanley, senior policy analyst for the American Civil Liberties Union, acknowledges that the average citizen has become much more accepting of always-on surveillance cams feeding a system that is continually assessing them.

“Right now everybody knows that when you walk down the street you’re recorded by a lot of video cameras, and that the video will just sit on some hard drive somewhere and nothing really happens to it unless something dramatic goes down,” observes Stanley. “The ultimate concern with this technology is that we’ll end up in a surveillance society where your I.D. is your face, and everybody is checking on you at every moment, monitoring you.”



Likelihood that US Internet Users Would Purchase a Device that Uses Face Recognition in Order to Protect Privacy, Jan 2018

% of respondents

Note: devices such as personal desktop/laptop or smartphone; numbers may not add up to 100% due to rounding

Source: FaceFirst, Feb 6, 2018

235667 www.eMarketer.com

With wider commercial use comes the potential for those in power to abuse the technology, Stanley says. “We’re talking about an enormously powerful surveillance capability that no government has ever had in the history of humanity.”

Privacy advocates need look no further than China to stoke their fears. China’s President Xi Jinping has been moving aggressively to possess moment-to-moment surveillance and assessment capability over Chinese citizens. China has rolled out a national surveillance network comprised of 200 million cameras, roughly four times the number in the U.S., and plans to have 300 million cameras in place by 2020, according to a report in the New York Times.

China says it is using this surveillance net to track down criminals and scofflaws, including jay walkers, whose punishment is to have their faces displayed on giant outdoor digital screens alongside lists of names of people who don’t pay their bills.

The developments in China have not been lost on the U.S. tech community, which is rightly concerned about how sort of authoritarian abuse might disrupt the fledgling facial ID market in the U.S. In July, Microsoft’s president and chief legal officer Brad Smith did something this corporate executives very rarely do: he actually called for federal oversight.

"We live in a nation of laws, and the government needs to play an important role in regulating facial recognition technology," Smith wrote in a blog post.

RealNetworks' Vance worries that more and more states might individually pass privacy regulations that would result in a patchwork of restrictions. Washington state, for instance, passed a 2017 law requiring companies to inform state residents before collecting biometric data and detailing what the data will be used for, much as required across the European Union.

"I think it's very important for people to come together and really understand how the technology is going to be used, but then also create ethical guidelines around that to ensure peoples' rights are being considered when these policies are put into place," Vance says.

Marquez, the Robbie.AI chief executive, agrees that well-defined limits are in order. "Companies must lead the process by being transparent," she says. "Facial recognition by itself can be a major advancement in data analysis and consumer protection in so many areas. Understanding the benefits and defining a framework for respecting civil rights is essential."

Source: https://threatpost.com/new-boom-in-facial-recognition-tech-prompts-privacy-alarms/138979/

11. Emotet Campaign Ramps Up with Mass Email Harvesting Module

The new variant can exfiltrate emails for a period going back 180 days, en masse.

A large-scale spam campaign has launched, spreading the Emotet banking trojan. Worryingly, the offensive has launched about a week after a fresh module for mass email-harvesting was detected for the malware.

Emotet is technically a banking trojan, but it's most often used as a dropper for a variety of secondary payloads (including TrickBot, Zeus Panda Banker, IcedID and other malwares), with credential-stealing, network propagation, sensitive information harvesting, port forwarding and other capabilities. It has a flexible, modular architecture, which, when combined with its persistence and worm-like method of rapid self-propagation throughout networks, makes it a considerable threat.

US-CERT in July issued a security notice for Emotet, noting that it's "among the most costly and destructive malware affecting state, local, tribal and territorial (SLTT) governments." It also said Emotet infections have cost SLTT governments up to $1 million per incident to remediate.

Recently, Emotet added a new module to up the ante on its ability to harvest victim email account credentials and contact lists: It can now exfiltrate entire email contents stretching back 180 days.

"Not only does that ratchet up the risk of losing sensitive information, it also means many victims will be required to initiate data breach notification protocol," Barkly researchers said in an email alert last week on the new module. "In addition to infecting new victims with the module, attackers are also installing it on previously infected machines they still have access to."

Just after that discovery, ESET noticed the latest campaign ramping up last week, following a bit of a lull for the malware's activity. The spam is well-crafted, and contains malicious links or Microsoft Word and PDF attachments disguised as invoices, bank account alerts or payroll reports. The messages purport to be from major banks, and use legitimate logos and other visuals to be more convincing.

The messages appear to be targeting English and German-speaking users in this latest Emotet campaign and appears to be most active in the Americas, the U.K., Turkey and South Africa.

"Following the instructions in the document, the victim enables macros in Word or clicks on the link in the PDF," explained ESET researchers, in a post on Friday. "The Emotet payload is subsequently installed and launched, establishes persistence on the computer and reports the successful compromise to its command-and-control server. In turn, it receives instructions on which attack modules and secondary payloads to download."

They also said that new builds of Emotet binaries are released approximately every two hours, in an effort to stay ahead of AV signatures.

The campaign is ongoing.

"This recent spike in Emotet activity just goes to show that Emotet continues to be an active threat – and an increasingly worrying one due to the recent module updates," the research team noted.

In terms of protection, since the Word documents distributed in this campaign require users to enable macros, admins should adjust Office settings to restrict or disable that option altogether.

Source: https://threatpost.com/emotet-campaign-ramps-up-with-mass-email-harvesting-module/139041/

12. Self-Signed Certificates Can Be Secure, So Why Ban Them?

In many organizations the use of self-signed certificates is forbidden by policy. Organizations may ban the use of self-signed certificates for several reasons: It is trivially easy to generate a certificate's key pair without reasonable entropy, to fail protect the private key of the key pair appropriately to its use, to poorly validate the certificate when used, and to misuse a self-signed certificate when a certificate authority should have been used instead. However, when properly and appropriately used, a self-signed certificate provides acceptable security in some situations.

There is a broadly held misunderstanding that self-signed certificates are inherently bad security. We offer this explanation to expand your understanding of certificate use. At the same time, we explain the circumstances under which McAfee's use of a self-signed certificate in one of our products provides adequate security for our customers.

For many uses of public key infrastructure (PKI), the correct method for signing a certificate is to use a well-known, trusted third party, a certificate authority (CA). "In a CA-based PKI system, the CA must be trusted by both parties. This is usually accomplished by placing the CA certificates in a whitelist of trusted certificates," says Wikipedia.

Indeed, self-signed certificates have several key limitations. Most important among these are:

- Self-signed certificates cannot be revoked.
- Self-signed certificates never expire.

However, there are cases for which a self-signed certificate may be sufficient, and perhaps a better choice than a certificate that has been signed by a CA.

In a public key infrastructure, in which parties to a communication are unknown to each other (and thus untrusted), the limitations of self-signed certificates presented above are important.

Consider browser-to-website connections. Users, via the browser, must ensure that the site to which they are connecting is indeed the intended site. In this case, having a trusted third party, the CA, is critical to validate that the web server in the connection is the one for which the certificate has been issued.

Establishing website-to-browser identity is the standard certificate use that transport layer security (TLS) pre-encryption authentication employs as well as the typical example for the use of certificates in general. This use case is also the driver for many organizational security policies in which the use of self-signed certificates is forbidden.

In the case where both sides of the communication know each other—often within the same entity—self-signing limitations become advantages. In this case, we can think of the certificate as a credential used to identify a particular entity to itself. This case is not entirely the same as attempting to establish trust between unknown parties.

In fact, when a certificate is used between two components in the same entity—that is, both sides are establishing that the other side is the one, intended component—the certificate is a form of shared secret, like a rather complex password.

In this case, there is no need for a third party to act as a root of trust. All that is required is that the key pair match—or, more precisely, that the public key can be used to verify that the certificate was signed with its private key mate (often called certificate pinning). Any public/private key pair will perform this function; an X.509 certificate happens to be a convenient and well understood “package” for the interaction.

The preceding self-signed use case presupposes that the private key of the certificate’s key pair has been and will continue to be protected with great care, similar to any important credential. One of the advantages of using an X.509 certificate for authentication is that the private key need not be installed (and thus is highly protected!) along with the certificate. The private key is used to generate the certificate. After generation, the private key is no longer needed to validate the certificate; only the public key is required.

Of course, a certificate when used as a credential requires sufficient protection, just as with any form of credential. Still, without the private key, the certificate becomes a one-of-a-kind credential; it can be reused if stolen, but it cannot be regenerated without access to the private key.

A self-signed certificate used for intercomponent authentication for TLS must be protected so that the likelihood of theft is very low. At McAfee, we provide layers of self-protection against the theft and reuse of products authentication certificates.

X.509 is nearly ubiquitous and has a great deal of programming and processing support. Hence, it is faster to deliver authentication based upon certificates than to build alternate software to validate key pairs. Besides, in the case of TLS, the protocol specifies X.509 certificates; certificates must be used to take advantage of TLS’ built-in authentication mechanism.

Because a self-signed certificate cannot be revoked and it does not expire, this reduces update and patching complexities in a connection between components built by the same entity and intended to be used solely within that closed context. However, to replace a certificate, for whatever reason, requires a software update because each self-signed certificate is the credential, rather than relying on trust of a certificate authority.

If the self-signed certificate’s private key were to become compromised in some manner, software could be updated with a new set of certificates and new keys. The compromised certificate would be tossed out, removed from service because it could not be used to establish trust between the parties. Because the old certificate is self-signed, it also will not work for other uses, such as the TLS server-side authentication we have described.

Essentially, once removed from its intended use, a self-signed certificate is useless to any party, malicious or otherwise.

Source: https://securingtomorrow.mcafee.com/mcafee-labs/self-signed-certificates-secure-so-why-ban/

13. Critical WordPress Plugin Flaw Grants Admin Access to Any Registered Site User

The privilege-escalation vulnerability would allow an attacker to inject malware, place ads and load custom code on an impacted website.

Another day, another critical WordPress plugin vulnerability. The popular AMP for WP plugin, which helps WordPress sites load faster on mobile browsers, has a privilege-escalation flaw that allows WordPress site users of any level to make administrative changes to a website.

The plugin, which has over 100,000 active installs according to its webpage, adds support for Google's mobile site acceleration tool, dubbed Google Accelerated Mobile Pages (AMP). Researchers at WebARX Security discovered that the plugin didn't include a check to verify the account permissions of the currently logged in user. In turn, that lack of permission verification opens up admin API access to anyone with a login for a site.

API calls are carried out using the Ajax development framework, they're essentially "hooks" used by site administrators to interact with the third-party and external functions they need to manage their site.

"In WordPress plugin development, you have the ability to register Ajax hooks which allows you to call functions directly," the WebARX team explained, in a posting on Thursday. "The main problem with this approach is that every registered user (regardless of account role) can call Ajax hooks. If the called hook doesn't check for account role, every user can make use of those functions."

The AMP plugin vulnerability is specifically located in the "ampforwp_save_steps_data" Ajax hook, which is called to save settings during the use of the installation wizard. Exploiting this would allow any user to update the plugin's settings.

Under those plugin settings, users can do a variety of things on a website, including placing ads, injecting custom HTML code, and manually uploading other WordPress plugins or malicious code like mining scripts or javascript malware.

The fix was to ensure that the plugin restricted this ability to those with admin privileges; the change was made in updated version 0.9.97.20 [download] of the plugin.

The critical issue with this particular vulnerability, according to WebARX, is that even registered users (i.e., site visitors who have signed up for loyalty accounts, accounts for forums or message boards, e-commerce accounts and so on) could make use of the flaw, making the barrier for exploitation very low for an attacker.

"Forrester estimates that 80 percent of breaches involve privilege misuse, and a good example is when applications don't bother enforcing role-based access controls," Andy Smith, vice president of product marketing at Centrify, told Threatpost. "That is what was uncovered in this week's WordPress plugin vulnerability, where administrative commands did not check to verify the user's role before execution, effectively allowing ANY user to perform administrative actions. In a world where developers are moving fast and DevOps pushes code quickly to production, it is critical that security checks get built into this automation flow and real DevSecOps processes get put in place to avoid such potentially costly mistakes."

This is just the latest privilege-escalation flaw in a string of recent WordPress plugin issues. Earlier in the month, a similar API call issue was discovered in the popular WP GDPR Compliance plugin, which has more than 100,000 active installs. That was actively exploited in the wild before being patched. Also this month, a file delete vulnerability that affected multiple plugins, including WooCommerce, was found impacting 4 million websites; it allowed full privilege escalation and administrative account takeover on e-commerce sites before a fix was issued.

"Bad actors are always on the lookout for vulnerable third parties that serve multiple websites," Alex Calic, strategic technology partnerships officer for the Media Trust, said via email. He added that while proper site protection includes updating and applying patches to any technologies provided by third parties. "unfortunately, most website operators remain unaware of who and how secure all their third parties are. This is their biggest source of risk because third-party code suppliers are popular targets among bad actors."

The good news is that in the case of AMP for WP, the new, fixed version is being pushed out via automatic updates.

Source: https://threatpost.com/critical-wordpress-flaw-grants-admin-access-to-any-registered-site-user/139162/

14. Gmail Glitch Offers Stealthy Trick for Phishing Attacks

The issue comes from how Gmail automatically files messages into the "Sent" folder.

A strange glitch in Gmail can be exploited to place emails into a person's "Sent" folder — even if that person never sent them.

Researchers who discovered the bug worry that it gives phishers and scammers another avenue to trick unsuspecting users into clicking on malicious links or opening rogue attachments.

The Gmail issue, discovered and outlined by software developer Tim Cotten this week, stems from the way that Gmail organizes its folders. It files an email into the Sent folder based on the address in the "from" field. So, if an attacker sends an email to a target, which has been specially crafted to also have that target's email address in the "from" field, the mail will automatically go to the person's inbox and Sent folder at the same time. This gives the false impression to the unwitting user that it was an email they themselves sent, said Cotten.

“So it appears that by structuring the from field to contain the recipient’s address along with other text, the GMail app reads the from field for filtering/inbox organization purposes and sorts the email as though it were sent from [the recipient], despite it clearly also having the originating mailbox as [another address],” he explained.

This is a potential boon for malicious actors. Spam emails to the inbox might be filtered out, but the mail that goes to the Sent folder will remain. An attacker could then, for example, send a follow-up email asking the victim to look back at previous correspondence to find something, and from there convince them to open something malicious.

“The confusion being injected into the average user experience is an open door for malicious actors… Imagine, for instance, the scenario where a custom email could be crafted that mimics previous emails the sender has legitimately sent out containing various links,” said Cotten. “A person might, when wanting to remember what the links were, go back into their sent folder to find an example: disaster!”

Making the issue trickier, after an email is filed in the Sent folder, it looks as though it’s been read/opened, like other sent messages, except for the fact that the subject is bolded.

This is apparently not the only Gmail-filtering bug out there; Cotten also posted a note from “tekstar” discussing another trick with auto-filtering.

“For example imagine Alice emails Bob and Chad, and in the ‘to:’ field for Bob she gives Bob a different name, like ‘Brad’ [but the address is still <bob@bob.com>],” tekstar said. “If Chad replies to this email, Bob will now be in his contact list as Brad. The email is still bob@bob.com but you can see how it could be malicious, or at least fodder for fun pranks.”

Source: https://threatpost.com/gmail-glitch-offers-stealthy-trick-for-phishing-attacks/139167/

15. Emoji Attack Can Kill Skype for Business Chat

The "Kitten of Doom" denial-of-service attack is easy to carry out.

A denial of service (DoS) vulnerability in the Skype for Business unified communications platform has been uncovered, which can be triggered by sending large numbers of emojis to the instant messaging client.

According to the SEC Consult Vulnerability Lab, which discovered the flaw (CVE-2018-8546), mounting an attack could not be easier. An attacker needs only to start blasting the target victim’s Skype for Business or Lync client with hundreds of emojis at once, in order to render it useless.

The researchers used the cute kitten emoji to demonstrate the attack (which also allowed the firm to name the attack “Kitten of Doom”). They found that starting at 100 emojis, the application will start to lag, and from there will become slower and slower as more emojis are sent. At 800 kittens though, an attacker hits pay dirt: "Your Skype for Business client will stop responding for a few seconds," the firm said, in a post this week. "If a sender continues sending emojis, your Skype for Business client will not be usable until the attack ends."

The attack vector is simple too: A malicious sender can just invite the target to join a meeting; or, he or she could contact someone directly via Skype.

Not all clients freeze upon the arrival of 800 kittens of doom: The flaw affects only Skype for Business 2016 MSO (16.0.93) 64-bit or before; and the Skype for Business precursor, Microsoft Lync 2013. The latter is vulnerable in the (15.0) 64-bit version, which is part of Microsoft Office Professional Plus 2013 or before.

The attack seems more made for pranks than anything else at first blush; the DoS state is after all not persistent, and only lasts as long as the kittens (or other emojis) keep coming. Also, this affects only the chat feature; the audio and video features in Skype for Business are handled by a separate, non-vulnerable thread.

However, as Sec-Consult pointed out, the availability of tools such as Lync and Skype for Business is a key part of how organizations function on a daily basis. Attack motivations could range from competitive dirty dealing (a competitor firm could troll executive clients, for example), to intra-office politicking (reducing the productivity of a rival department, for instance).

Microsoft issued a fix for CVE-2018-8546 in this week's Patch Tuesday update. For those that don't have the option to patch the system, workarounds include disabling emojis in the Skype for Business client (Tools -> Options -> IM -> Show emoticons in messages) and setting the privacy options so that only people from one's contact list can send messages.

A similar issue was also found back in 2015, where multiple animated emoticons would cause a client's CPU usage to skyrocket, the firm added.

Source: https://threatpost.com/emoji-attack-can-kill-skype-for-business-chat/139186/

16. Stopping the Infiltration of Things

The Internet of Things – connected devices that contain network sensors to allow for remote monitoring and control, are expected to hit 75-billion devices installed by 2025. These devices include everything from home routers, remote cameras to healthcare devices. This wide-ranging internet-of-things market sector includes industrial, consumer, banking, retail, manufacturing and healthcare – to name a few. It is this vast arrange of devices used globally that has now become the playground for cybercriminals as general cybersecurity trends in 2018 bare out. IoT threats are on the rise and are transforming to penetrate various IoT devices as they are introduced to the market.

The Throng of Threats

IoT devices come in many shapes and sizes from IP cameras to external, network-connected hard drives. These are known as "dumb" devices and are built with a single, or limited purpose. They are designed to be easy to deploy, with minimal configuration and setup required. The vulnerability, though, lies within the actual design. The ease of use is this very same feature that allows malicious actors to take over any IoT device. In a rush to market, IoT manufacturers have given little thought to security which has given rise to a myriad of malware including Mirai, Shishiga, Hajime, Okiru and Torii which have all kicked off an arms race of sorts within the Dark Web to see who can evolve these malwares into next generation attacks on corporate and government websites, ISP, Telecoms and more. This malicious malware is used to take over these devices to amass botnets used for such things as Denial-of- Service attacks (DDoS, spam and a variety of other crushing cyber plagues.

Just recently, there was a new IoT botnet discovered that infected 100,000 home routers designed to send Hotmail, Outlook, and Yahoo spam. In this case, "the vulnerability was discovered in 2013 by security researchers from DefenseCode and resides in the Broadcom UPnP SDK, a piece of software that was embedded in thousands of router models from multiple vendors."

Another threat has been pointed out by the US-China Economic and Security Review Commission which has warned that both government agencies and US companies face significant risk posed by the Chinese control of the IoT supply chain combined with what they term as "lax security protections and universal connectivity of IoT devices." The commission also predicts with the deployment of 5G, the cyberattacks leveraging IoT devices will only increase in size speed and impact.

The Growing Alarm

It is the number of devices in use and coming online combined with the severe threat to not only US citizens, but also whole industries like critical infrastructure and power utilities that could prove disastrous rather than just an inconvenience that is pushing Congress to take action to force IoT Manufacturers to embed security into devices.

Senator Mark Warner (D-Va.), who is the vice chairman of the Senate Select Intelligence Committee, is calling for U.S. agencies and Congress is one of the first representatives to introduce legislation to advance IoT security. California also passed legislation that would require manufacturers to have "reasonable security feature or features," and last month Europol, the European Union's law enforcement agency, and ENISA, the European Union Agency for Network and Information Security, held their IoT security conference to discuss the problem with industry—and how to go about securing IoT, before it's too late.

While many manufacturers will argue that requiring additional security for IoT devices will necessarily increase the cost of such devices, it is a price that must be accepted to prevent a calamity that could have an impact country-wide and even globally.

Stopping the IoT Incursion

While legislative action will ultimately result in the best long-term solution, it isn't an immediate fix. There are several ways to prevent IoT devices from becoming infected, but there are also other steps that must be taken to prevent these devices from causing further damage to other devices connected to the network.

It is a simple, easy first step that is often overlooked to start to secure IoT devices and it all starts with passwords. Passwords are often set to a default which can be conveniently discovered by looking in the online documentation. Because the devices are a snap to set up, users don't often change these passwords, and, when connected to the internet, provide the door for malicious actors to infect open devices to add to their arsenal of weapons.

Another opening for cybercriminals is known vulnerabilities. Once a vulnerability is discovered in IoT devices it spells open season for hackers who know that most IoT devices are not updated after they are deployed. What is even more troubling is that many devices can't even be updated after they are shipped. This means that once a device is deployed, the device is as-is because manufacturers haven't provided a way to make modifications to the firmware or patch vulnerabilities found post-production. This is exactly how malware writers like it because it means once they find the vulnerability and infect a device, the only way to stop the malware, is to replace the device.

As previously mentioned, IoT devices are single or limited-purpose devices. This means that they don't need full access to the network to perform their intended task. Deploying the device on the network with limited access to other devices, will prevent them from infecting other devices on the network. Ideally, IoT devices should only have access to what is essential to perform. Anything else should be blocked.

Finally, deploying IoT devices on a corporate network where they will have access to business-critical applications and devices, ensure there is a way to monitor the traffic they are generating. Alerts should be instated for any activities that are malicious or anomalous. For example, if network-connected smoke detectors start communicating with the mail server, you know you have a problem. Network traffic analytics is a clear path to knowing when this type of activity occurs.

With a force of will and some legislative push behind it, IoT manufacturers will be have to evolve the security of these devices or face possible long-term liability should a catastrophic event occur.

Source: https://threatpost.com/stopping-the-infiltration-of-things/139204/

17. Ford Eyes Use of Customers' Personal Data to Boost Profits

Ford's CEO sees the tech company model as key to the company's next chapter.

Ford Motor Company is known for making cars and trucks; but the future for the iconic automaker might look a little more like Facebook than an assembly line.

As it struggles with hemorrhaging earnings in markets outside of North America, industry-watchers are speculating that Ford is looking to a new source of income: The data it can collect from its 100 million customers.

Sure, connected cars are a reality; "infotainment" systems and mobile apps are deep repositories of lifestyle information for many car-makers – Ford included. But Ford's CEO recently suggested that the data collected by the company's financial services arm also represents a valuable, low-overhead asset.

"We have 100 million people in vehicles today that are sitting in Ford blue-oval vehicles," said Ford CEO Jim Hackett during a Freakonomics Radio podcast. "The issue in the vehicle, see, is: We already know and have data on our customers. By the way, we protect this securely; they trust us. We know what people make. How do we know that? It's because they borrow money from us. And when you ask somebody what they make, we know where they work, you know. We know if they're married. We know how long they've lived in their house because these are all on the credit applications. We've never ever been challenged on how we use that. And that's the leverage we got here with the data."

The comments, which were amplified by several auto-industry sources and the Detroit Free Press, sparked alarm in the Twitterverse. Against the backdrop of privacy disasters at Facebook and other stalwarts of the internet economy, the fear for many is that Ford sees selling access to consumers based on their lifestyle as a way forward.

"Every OEM has data like this, how do you feel about *your* data being used this way?" tweeted one marketing pro.

"I heard it yesterday, and was appalled," tweeted another. "No concern whatsoever for privacy and no reflection on whether or not this is a GOOD thing. Talked about linking with personal medical data while in the vehicle. No thought to ethical considerations. Another Zuckerberg. Disturbing."

Is Ford considering selling consumer data as a revenue stream? Hackett stopped short of saying that — and indeed, the data could instead simply be useful to the company internally, as a way to increase the value (and profit) of its other businesses.

With sales of vehicles flagging worldwide, the company is finding itself running out of financial freeway, so to speak. And even in the U.S., its strongest market, Ford is seeing little vehicular success of late beyond sales of its trucks and SUVs). Accordingly, the automaker is wisely taking steps to be more fully integrated into people's lives, by expanding into ancillary businesses that at first would seem to run counter to its mission.

For instance, it recently announced the acquisition of Spin, which is an electric scooter company. This continues an interest in "personal mobility" that has developed over the last two years; in 2016 for instance Ford decided to partner with Motivate, which is a bike-share company that runs the CitiBike program in New York City and other locations. It also invested in Chariot, which is a shuttle-bus service in San Francisco that works much like Lyft or Uber – routes are crowdsourced via a smartphone app.

The company said that it wants to tap into the growing pool of people that are "going green" and adopting healthier lifestyles by using alternate modes of travel for short distances. After all, almost 46 percent of Americans' vehicle trips are three miles or less, according to the National Household Travel Survey.

"Spin adds an exciting new offering to Ford's mobility portfolio as we try to help our customers get places more easily, more quickly and less expensively," Sunny Madra, the vice president of the company's Ford X division, said in a press statement. "As more people consider scooters to be a viable mobility option, now is the right time for Ford to work closely with Spin's highly experienced and dedicated team to help expand their service to more cities."

While the company talks up the altruistic aspects of these moves, the opportunity for collecting personal information may be where the real play is — perhaps not for sharing with third parties, but for better informing the rest of its business.

"[Spin] is a deal that makes sense because [Ford] will acquire data," Ivan Drury, an industry analyst at Edmunds.com, told NPR. "Acquiring and knowing how people are utilizing other modes of transportation in addition to the ones that they already have."

Hackett himself confirmed that assessment back in 2016, while discussing Motivate, which continues to expand to new markets.

"What we're doing differently in San Francisco that isn't done in New York is we put telemetry on that bike," he said at an investor conference. "Telemetry is a form of communication, so now the bike is pinging data to us. Listen, here's the deal. The opportunity is not bikes. That's not why Ford's in it. The opportunity is data, and the data is super valuable because it tells us these invisible paths that people are taking in this complex city in terms of how they want to get around. And there's something else cool about it because we can take that data and we can connect it in ways that our new shuttle is going to connect to the cloud as well."

It may make a lot of sense for Ford (and other automakers) to go in the data-broker direction to combat the financial headwinds stemming from the deeply cash-intensive vehicular design and production business, but a Ford spokesperson told Threatpost that this isn't part of the plan.

“In the podcast...Jim Hackett was painting a picture of the future possibilities of data use given the long-term relationship and trust we have with our customers,” she said. “Specifically, it is important to know we do not sell or monetize information from customer credit applications. We take seriously our obligations related to how we use this information. With regard to all data use, we are committed to protecting customer privacy and we do that by ensuring transparency and appropriate consent in the collection and use of all customer data.”

What is clear however is that many consumers are uncomfortable with Ford acting more like a tech company than an automaker. Kevin Bankston, director of privacy think-tank New America, on Monday tweeted about Ford’s interest in personal data, with a posting that quickly went viral.

“Ford’s CEO just said on NPR that the future of profitability for the company is all the data from its 100 million vehicles (and the people in them) they’ll be able to monetize,” he tweeted. “Capitalism & surveillance capitalism are becoming increasingly indistinguishable (and frightening).”

After that tweet was liked and retweeted thousands of times, he noted, “Hey @Ford, you should note just how viral my previous tweet has gone. I don’t have a huge following or anything. There’s just a whole lotta drivers uncomfortable with this direction. They already paid for their cars with $$$, they don’t also want to pay with their privacy.”

Source: https://threatpost.com/ford-eyes-use-of-customers-personal-data-to-boost-profits/139209/

18. [Heads-up] Bad Guys Love Marriott: 500 Million Data Breach Is Phishing Heaven

So I guess we have just reached the tipping point, it's "privacy game over" for business travelers.

For about 327 million of the 500, the breached data includes names, mailing addresses, phone numbers, email addresses, passport numbers (!), Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

The company said in a statement that it discovered "unauthorized access" to the database, which extended back until 2014.The hacker had copied and encrypted information and "took steps toward removing it," Marriott said.

In some cases, payment card numbers and expiration dates were also taken, but Marriott said it's unclear whether the hackers have information to decrypt the payment card numbers.

Marriott said it has set up a website for consumers impacted by the hack, at info.starwoodhotels.com, and a call center. "Call volume may be high, and we appreciate your patience," the company said. NPR mentioned that Starwood would send an email to all addresses affected.

Source: https://blog.knowbe4.com/heads-up-bad-guys-love-marriott-500-million-data-breach-is-phishing-heaven?

19. Threat predictions for industrial security in 2019

The past few years have been very intense and eventful when it comes to incidents affecting the information security of industrial systems. That includes new vulnerabilities, new threat vectors, accidental infections of industrial systems and detected targeted attacks. In response, last year we developed some Threat Predictions for Industrial Security in 2018, outlining the trends most likely to unfold in the year ahead.

The industrial cybersecurity threat landscape moves at a slower and more rigid pace than the information technology threat landscape in general. Attacks on ICS are still hard to monetize. Industrial organizations are still out of scope for the majority of cybercriminals. They are a relatively new target for adversaries who have already started attacking them. These are still applying existing tools and tactics to their attacks. That is why the majority of the industrial threat predictions from last year are still unfolding, although some of them have already come true.

Kaspersky Lab specialists have spent a few years investigating the cyberthreat landscape for industrial organizations and trying to bring their expertise and technology to OT environments. We are still on a long journey, with various to difficulties cope with and problems yet to solve. Constantly keeping in contact with many researchers in other security organizations and some ICS security pioneers from inside industrial companies; we have come to the conclusion that some of the difficulties we face are common to the industry. Solving some of those is mandatory to make the world more secure and safe.

So, although the fog of 2018’s predictions and threat landscape has yet to clear, we decided to focus on the major problems likely to affect the work of professionals involved in industrial systems in 2019.

Top four cybersecurity challenges facing industrial enterprises in 2019

1) The ever-increasing attack surface

The increasing amount of automation systems, the variety of automation tools, number of organizations and individuals with direct or remote access to automation systems, as well as the emergence of communication channels for monitoring and remote control between previously independent objects – all expand the opportunities for criminals to plan and execute their attacks.

2) Growing interest of cybercriminals and special services

A decrease in profitability and increase in risks from cyberattacks aimed at traditional victims is pushing criminals to search for new targets, including those within industrial organizations.

At the same time, special services in many countries, as well as other organized groups – motivated by internal and external political interests – and financially-motivated groups, are actively engaged in the research and development of techniques to implement espionage and terrorist attacks aimed at industrial enterprises.

Taking into account the current geopolitical context, the development of industrial enterprises' automation systems, and the transition to new management processes and models of production and economic activity, this situation will continue to develop in the coming years, negatively affecting industrial organizations.

3) The underestimation of general threat levels

A lack of public access to information about information security issues within industrial enterprises, coupled with the relative rarity of targeted attacks on automation systems, an excessive belief in emergency protection systems and the denial of objective reality is having a negative effect on the assessment of threat levels by owners and operators of industrial enterprises and their personnel.

4) The misunderstanding of threat specifics and the suboptimal choice of protection options

In the world of industrial cybersecurity, several high–profile incidents carried out with the help of targeted attacks against a very limited number of victims, created an information landscape that formed fully the idea of a potential threat – both among information security researchers and security developers, and among potential users of these tools.

However, the professional reporting of these incidents was often too difficult to understand by the majority of potential users, and was devoid of important OT details. The information field formed in these conditions, including the absence of a daily need to deflect the attacks aimed at automated control systems, gave developers a chance to create products that might protect better from the artificial scenarios thought up by researchers themselves, than from real world day-to-day threats. This could leave the automation systems of industrial enterprises vulnerable to real life attacks, including random ones and targeted attack campaigns organized by cyber criminals.

Source: https://securelist.com/ksb-threat-predictions-for-industrial-security-in-2019/88940/

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**

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 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'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 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.