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

Monthly Security Bulletin

September 2018

Table of Contents:

1. Which Mobile Threats Do You Need to Prepare For?

Mobile devices are more ubiquitous than ever, with immeasurable amounts of data now being shared and manipulated on mobile platforms. Organizations rely heavily on their mobile environment to make business more efficient, increase productivity and enable employees to work while away from the office. However, this productivity is threatened by constantly evolving and proliferating mobile threats.

Mobile devices are today's target of choice for attackers. Illegally exploiting their capabilities allows cybercriminals to locate users, eavesdrop on their conversations, and access their files, microphones, cameras and more. Still, many organizations underestimate the dangers posed by mobile threats.

Mobile Malware Is Rising

Threat actors primarily use three sensitive vectors to access mobile data: applications, networks and the devices themselves.

Mobile applications are widespread among employees, partners and clients and handle more information than any other media. According to Pradeo's biannual "Mobile Security Report," 77 percent of mobile threats occur at the application level. Mobile applications can frequently be the source of data leakage, and insecure applications can introduce unnoticed malware or spyware onto a device, exposing organizations to attacks and data breaches.

Malware can be divided into two categories: those that have known viral signatures and are labeled in virus databases, and those that are zero-day threats, or threats that have yet to be identified. Because they cannot be as easily detected, zero-day threats are much more dangerous.

Unfortunately, Pradeo reported a 92 percent rise in zero-day malware in the last six months, suggesting that modern threat actors are increasingly abandoning recognizable attacks and innovating to evade traditional security protections. Only mobile security solutions performing real-time behavioral analysis can detect this latter type of malware and ensure effective protection.

Out-of-Date Operating Systems Are Open Doors

Another mobile threat vector lies in the mobile device itself — particularly its operating system (OS). According to the report, the volume of mobile threats operating at the device level has increased by 100 percent. Many of these involve compromising a device's OS, which gives attackers the privileged access they need to easily steal data from organizations.

Most mobile OS flaws are quickly discovered and patches are made available by the manufacturer. However, many mobile users wait days or weeks before installing new updates, giving cybercriminals a chance to take advantage of these vulnerabilities.

Public Wi-Fi Remains a Threat

People often connect their phones to public networks without realizing the potential risks. This leads to an increase in threats such as man-in-the-middle (MitM) attacks. In fact, attacks occurring over public Wi-Fi are the most common network threats facing mobile devices.

Employees that travel frequently are the most sensitive to such exploits and are at risk of exposing corporate data while connected to airport or restaurant Wi-Fi. Organizations need to make sure their traveling employees are aware of the risks and consider equipping them with security solutions that keep them protected against public Wi-Fi threats.

How Can Organizations Protect Their Mobile Environment?

Organizations often rely on unified endpoint management (UEM) solutions to manage and enforce compliance within their mobile fleet. These solutions can also enhance security, especially when integrated with other mobile threat defense solutions that provide on-device threat detection and remediation.

Combining UEM and integrated mobile defense solutions can help your organization embrace a proactive, automated strategy for combating mobile threats instead of relying on a reactive one.

Source: https://securityintelligence.com/which-mobile-threats-do-you-need-to-prepare-for/

2. Public IP Addresses of Tor Sites Exposed via SSL Certificates

A security researcher has found a method that can be used to easily identify the public IP addresses of misconfigured dark web servers. While some feel that this researcher is attacking Tor or other similar networks, in reality he is exposing the pitfalls of not knowing how to properly configure a hidden service.

One of the main purposes of setting up a dark web web site on Tor is to make it difficult to identify the owner of the site. In order to properly anonymize a dark web site, though, the administrator must configure the web server properly so that it is only listens on localhost (127.0.0.1) and not on an IP address that is publicly exposed to the Internet.

Yonathan Klijnsma, a threat researcher lead for RiskIQ, has discovered that there are many Tor sites that utilize SSL certificates and also misconfigure a hidden service so that it is accessible via the Internet. As RiskIQ crawls the web and associates any SSL certificate it discovers to it's hosted IP address, it was easy for Klijnsma to map a misconfigured hidden Tor service with its corresponding public IP address.

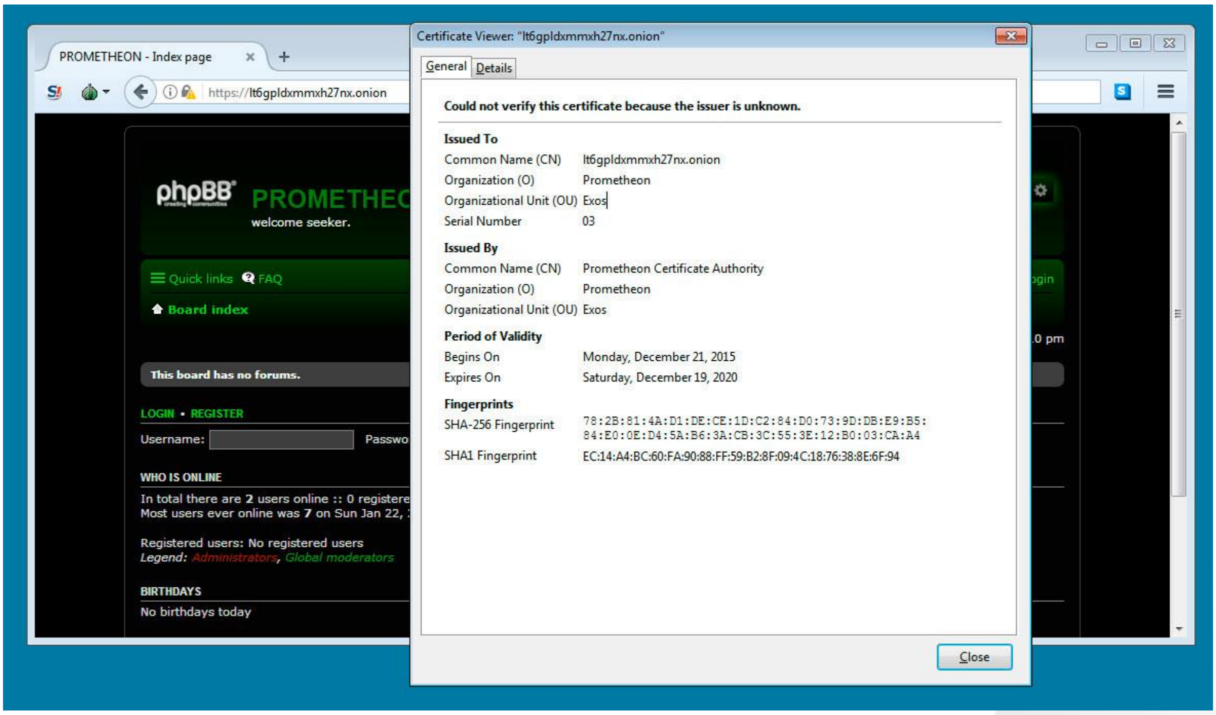
"The way these guys are messing up is that they have their local Apache or Nginx server listening on any (* or 0.0.0.0) IP address, which means Tor connections will work obviously, but also external connections will as well," Klijnsma told BleepingComputer. "This is especially true if they don't use a firewall. These servers should be configured to only listen on 127.0.0.1."

When asked how often he sees misconfigured servers that expose their public IP address, he told us that it is quite common.

"Continuously. I'm not even kidding. Some don't listen on http/https, so I don't know what they are, but they have onion addresses and live on both clear and dark web." Klijnsma told BleepingComputer.

SSL certs help ID public IP address of dark web sites

When operators of Tor hidden services add an SSL certificate to their site, they associate the .onion domain with the certificate as shown below.



This board has no forums.

WHO IS ONLINE

In total there are 2 users online :: 0 registere
Most users ever online was 7 on Sun Jan 22,

Registered users: No registered users
Legend: Administrators, Global moderators

BIRTHDAYS

No birthdays today

Certificate Viewer: "lt6gpldxmmxh27nx.onion"

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	lt6gpldxmmxh27nx.onion
Organization (O)	Prometheon
Organizational Unit (OU)	Exos
Serial Number	03

Issued By

Common Name (CN)	Prometheon Certificate Authority
Organization (O)	Prometheon
Organizational Unit (OU)	Exos

Period of Validity

Begins On	Monday, December 21, 2015
Expires On	Saturday, December 19, 2020

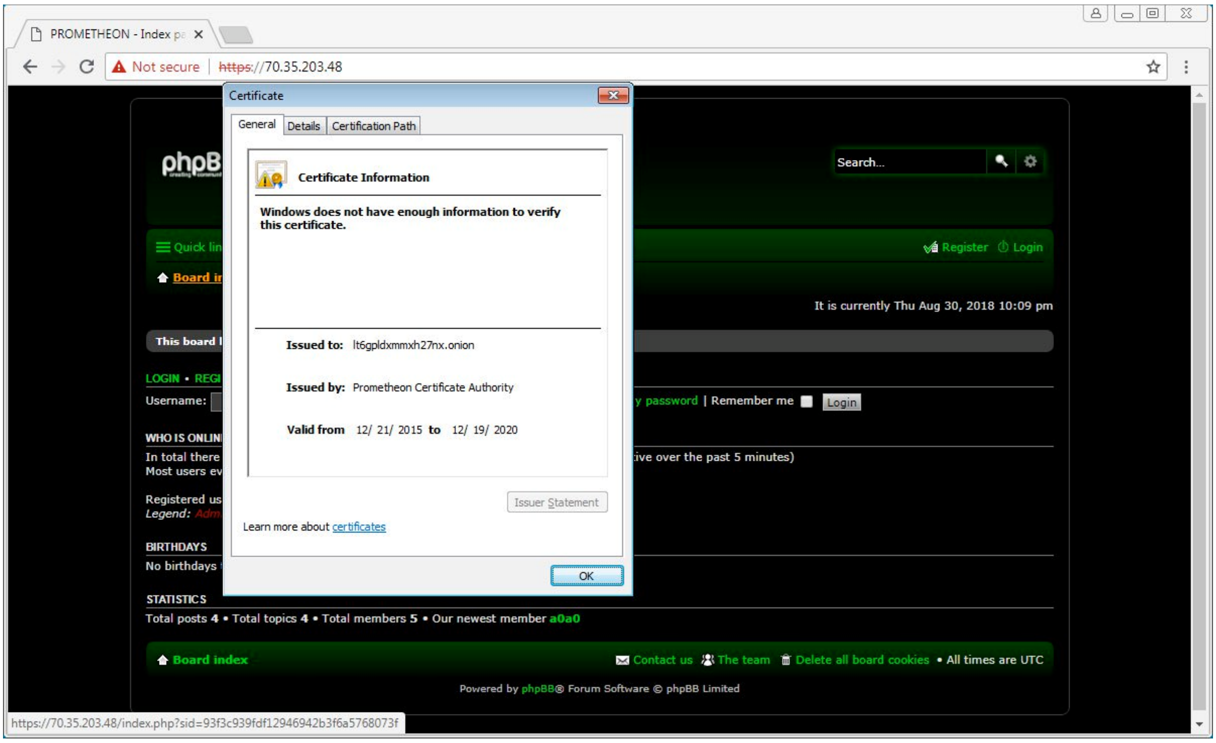
Fingerprints

SHA-256 Fingerprint	78:2B:81:4A:D1:DE:CE:1D:C2:84:D0:73:9D:DB:E9:B5: 84:E0:0E:D4:5A:B6:3A:CB:3C:55:3E:12:B0:03:CA:A4
SHA1 Fingerprint	EC:14:A4:BC:60:FA:90:88:FF:59:B2:8F:09:4C:18:76:38:8E:6F:94

Figure 2.1. Tor Site with SSL Certificate

If the Tor site is misconfigured so that it listens on a public IP address, this same certificate containing the .onion domain will be used for that IP address as well. As RiskIQ crawls the Internet and catalogs all SSL certificates it finds being used by a site, it will associate this .onion certificate with the public IP address it finds it on.

This allows Klijnsma to use the RiskIQ database to easily search for .onion certificates and see what public IP address they are mapped to as shown below.



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: lt6gpldxmmxh27nx.onion

Issued by: Prometheon Certificate Authority

Valid from 12/ 21/ 2015 to 12/ 19/ 2020

Learn more about certificates

It is currently Thu Aug 30, 2018 10:09 pm

Username:

WHO IS ONLINI

In total there … ive over the past 5 minutes)
Most users ev

Registered us
Legend: Adm

BIRTHDAYS
No birthdays

STATISTICS
Total posts 4 • Total topics 4 • Total members 5 • Our newest member a0a0

Figure 2.1. Tor certificate exposed on the public IP address

Tor users think Klijnsma is attacking Tor

Some users feel that Klijnsma's research is an attack on Tor, while the researcher says it's actually the opposite. Instead of attacking Tor, Klijnsma is trying to bring to light the inherent problems associated with not properly configuring a Tor hidden service.

In order to protect a site from being exposed in this manner, it's quite simple according to the researcher. "They should only listen on 127.0.0.1."

Source: https://www.bleepingcomputer.com/news/security/public-ip-addresses-of-tor-sites-exposed-via-ssl-certificates/

3. Mikrotik routers pwned en masse, send network data to mysterious box

Researchers uncover botnet malware pouncing on security holes

More than 7,500 Mikrotik routers have been compromised with malware that logs and transmits network traffic data to an unknown control server. This is according to researchers from 360 Netlab, who found the routers had all been taken over via an exploit for CVE-2018-14847, a vulnerability first disclosed in the Vault7 data dump of supposed CIA hacking tools.

Since mid-July, Netlab said, attackers have looked to exploit the flaw and enlist routers to do things like force connected machines to mine cryptocurrency, and, in this case, forward their details on traffic packets to a remote server.

“At present, a total of 7,500 MikroTik RouterOS device IPs have been compromised by the attacker and their TZSP traffic is being forwarded to some collecting IP addresses,” the researchers explained.

The infection does not appear to be targeting any specific region, as the hacked devices reside across five different continents with Russia, Brazil, and Indonesia being the most commonly impacted.

The researchers noted that the malware is also resilient to reboots, leaving a firmware update as the only permanent solution to the problem.

“In order for the attacker to gain control even after device reboot(ip change), the device is configured to run a scheduled task to periodically report its latest IP address by accessing a specific attacker's URL,” Netlab wrote.

“The attacker also continues to scan more MikroTik RouterOS devices by using these compromised Socks4 proxy."

360 Netlab said it does not know what the ultimate aim of the attacker will be. They note, however, that the controller oddly seems to be interested in collecting traffic from the relatively obscure SNMP ports 161 and 162.

“This deserves some questions, why the attacker is paying attention to the network management protocol regular users barely use? Are they trying to monitor and capture some special users’ network snmp community strings?” 360 Netlab asked.

“We don’t have an answer at this point, but we would be very interested to know what the answer might be.”

Source: https://www.theregister.co.uk/2018/09/04/mikrotik_routers_pwned/

4. White-Hats Go Rogue, Attack Financial Institutions

Hackers rooted in the white-hat part of the business moonlight as bank robbers, pouring their knowledge and skills into creating and modifying malware that allows them to infiltrate financial institutions.

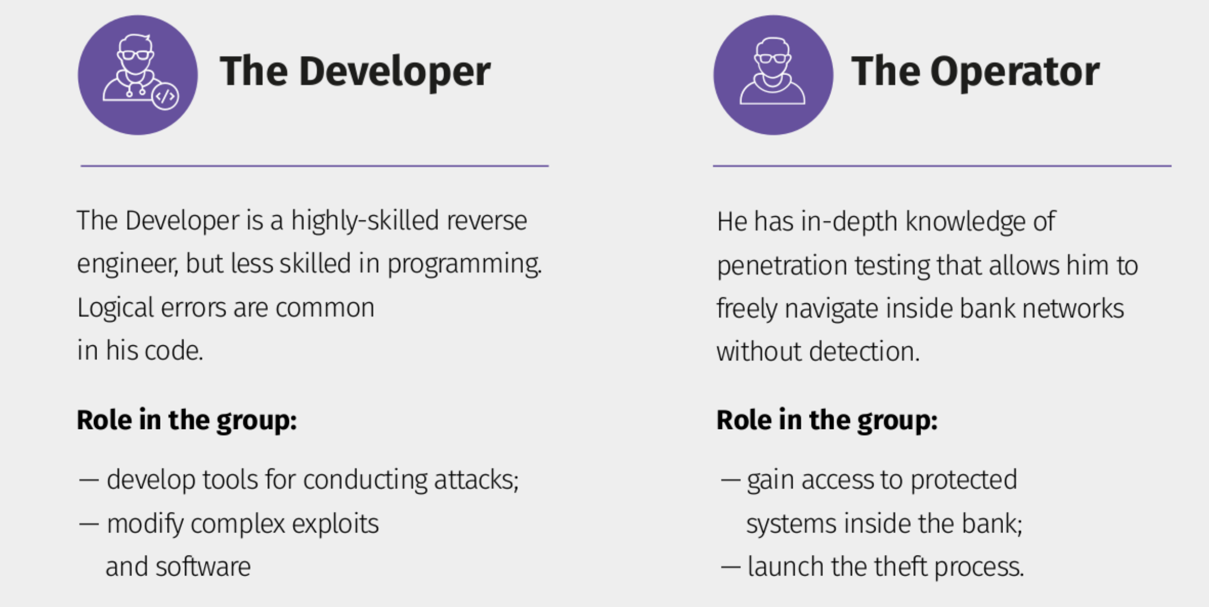
The group is believed to have only two members and shows perseverance as well as the ability to learn from its own failures.

The Developer and the Operator

According to a report shared with BleepingComputer by international cybersecurity company Group-IB, the newest financially-motivated group on the market has a Developer and an Operator, each playing well-defined roles. The name they received from the researchers is Silence.

The Developer is in charge of building attack tools and customizing utilities employed by other money-driven cybercriminals. This betrays a highly qualified reverse engineer and access to malware samples typically available in private caches of security companies.

The other member of the group is the Operator, who appears to be a seasoned penetration tester. His role is to compromise banks and initiate the thefts.



The Developer

The Developer is a highly-skilled reverse engineer, but less skilled in programming. Logical errors are common in his code.

Role in the group:

— develop tools for conducting attacks;
— modify complex exploits and software

The Operator

He has in-depth knowledge of penetration testing that allows him to freely navigate inside bank networks without detection.

Role in the group:

— gain access to protected systems inside the bank;
— launch the theft process.

Figure 4.1. Description of the two members in the group

Group-IB says that based on their analysis the two are Russian speakers, presenting as evidence a list of commands in Russian, typed on an English keyboard. The analysis also states that based on the groups access to certain resources and their tactics, it is believed that they both have a background in legitimate whitehat security activities.

"From circumstantial analysis over two years of attacks, it appears that Silence group members have worked or are currently working in legitimate information security activities," Group-IB's report stated. "The group has access to non-public malware samples, patched Trojans available only to security experts and also TTP changes suggest that they modify their activity to mimic new attacks and red teaming activity."

Source: https://www.bleepingcomputer.com/news/security/white-hats-go-rogue-attack-financial-institutions/

5. Threat Actors Peddling Weaponized IQY Files Via Necurs Botnet

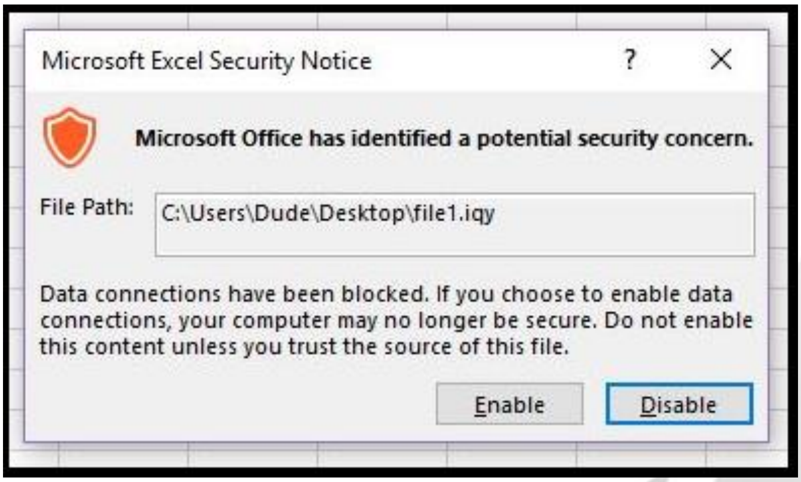
Have you ever walked through a store and spotted an item that looked strange to you, but you put it in your cart anyway? Maybe it was appealing because it was something new you wanted to check out. Maybe it was shiny — you had to have it. If so, threat actors are looking for shoppers just like you. They constantly distribute new "products," typically in the shape of crafty email spam, to lure the unsuspecting user. A recent wave of malicious "products" has hit the virtual high streets in the form of unsolicited email with internet or web query file (IQY) attachments.

IQ What? Why?

What is an IQY file attachment, and why is it the flavor of the month for threat actors? Microsoft Excel uses this type of file to pull data from the internet into a spreadsheet. To do that, a URL is embedded into an IQY file, and the file facilitates pulling the data from the specified webpage.

While IQY file extensions may sound foreign to many users, if you look at enterprise-level networks that use SharePoint, a web-based collaborative platform that integrates with Microsoft Office, for example, you would be sure to find many instances where IQY files are used.

These files help network users share and edit Excel spreadsheets, among other uses. As you can imagine, a common productivity file with an embedded URL could easily be used for nefarious purposes. This is why these types of files are not made to run code without interacting with the user. To prevent their content from loading automatically, a security prompt is built into the file asking the user if he or she would like to "enable" a data connection when opening an IQY file.



Microsoft Excel Security Notice

Microsoft Office has identified a potential security concern.

File Path: C:\Users\Dude\Desktop\file1.iqy

Data connections have been blocked. If you choose to enable data connections, your computer may no longer be secure. Do not enable this content unless you trust the source of this file.

Figure 5.1. Warning box asking user to "enable" or "disable" a data connection in an IQY file (Source: IBM X-Force)

Small and Handy — In the Wrong Hands

IQY files are attractive to threat actors for a couple of reasons. For one, they are easy to create. An IQY file can be created by using a text editing program. Threat actors can insert their malicious instructions into the text editor along with an actionable URL and save it with an ".iqy" extension. They can then use the file to deliver malicious code directly from their malware infection zones. IQYs are also small and inconspicuous, making them easier to plant in an unsolicited email.

This type of file attachment is relatively unusual and not commonly seen attached to emails, and that is why it can be interesting to an attacker. Attackers constantly shuffle file types in their spam campaigns in an attempt to create an element of surprise for unsuspecting users. They are also trying to catch security solutions off guard, especially those that filter common file types and extensions used in phishing and malware infection campaigns.

IQY Attacks!

Some recent statistics from IBM X-Force research revealed that the use of IQY files in spam campaigns has been on the rise in recent months. One major malspam distributor, the Necurs Botnet, was observed using weaponized IQY file attachments for the first time starting on May 25, 2018.

Between late May and mid-July 2018, IBM X-Force researchers captured over 780,000 spam emails that came from Necurs resources in their spam traps. All of those messages contained IQY attachments.

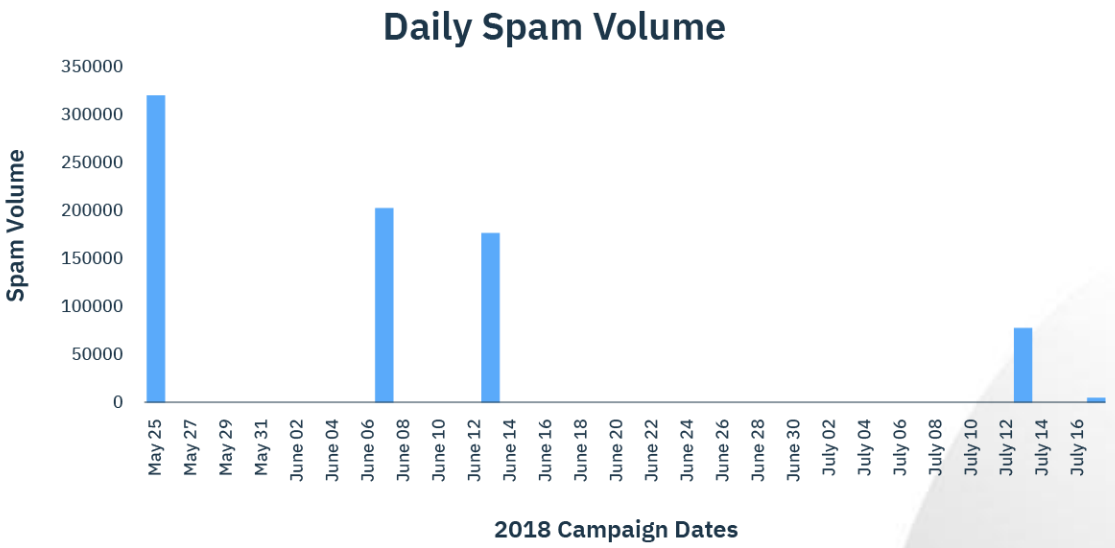
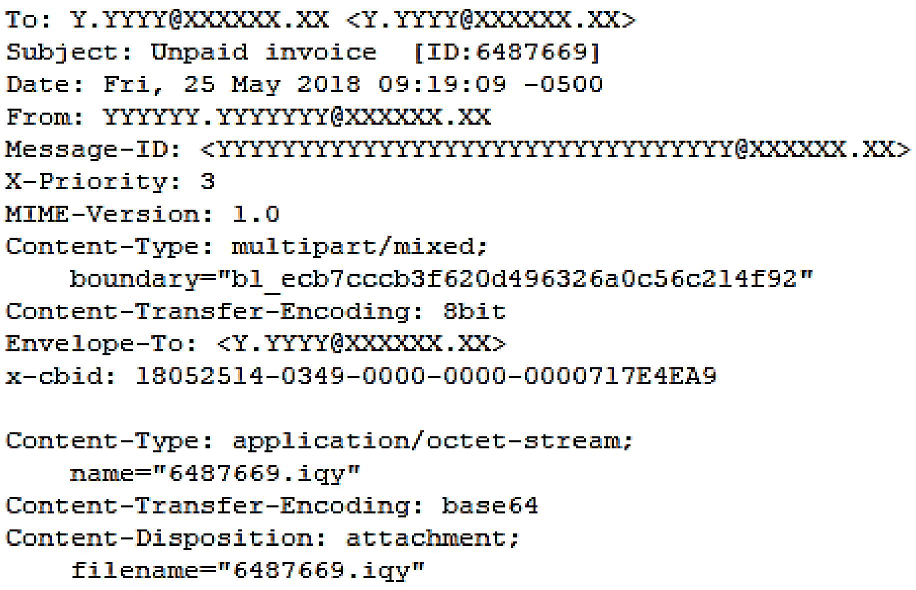


Figure 5.2. IQY attachment spam campaigns spewed by the Necurs Botnet (Source: IBM X-Force)



```
To: Y.YYYY@XXXXXX.XX <Y.YYYY@XXXXXX.XX>
Subject: Unpaid invoice  [ID:6487669]
Date: Fri, 25 May 2018 09:19:09 -0500
From: YYYYYY.YYYYYYY@XXXXXX.XX
Message-ID: <YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY@XXXXXX.XX>
X-Priority: 3
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="bl_ecb7cccb3f620d496326a0c56c214f92"
Content-Transfer-Encoding: 8bit
Envelope-To: <Y.YYYY@XXXXXX.XX>
x-cbid: 18052514-0349-0000-0000-000071 7E4EA9

Content-Type: application/octet-stream;
    name="6487669.iqy"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="6487669.iqy"
```

Figure 5.3. Example of email message with IQY attachment (Source: IBM X-Force)

Upon further analysis of the emails captured in our spam traps, the IQY attachments were confirmed to contain malicious URLs. Once users were lured into executing the connection to the embedded URL, the chain of infection on the device was set in motion. This led to the eventual download of the FlawedAmmy RAT, a malicious remote access tool of which source code was leaked in March 2018, giving rise to numerous campaigns that spread this malware to hundreds of thousands of users.

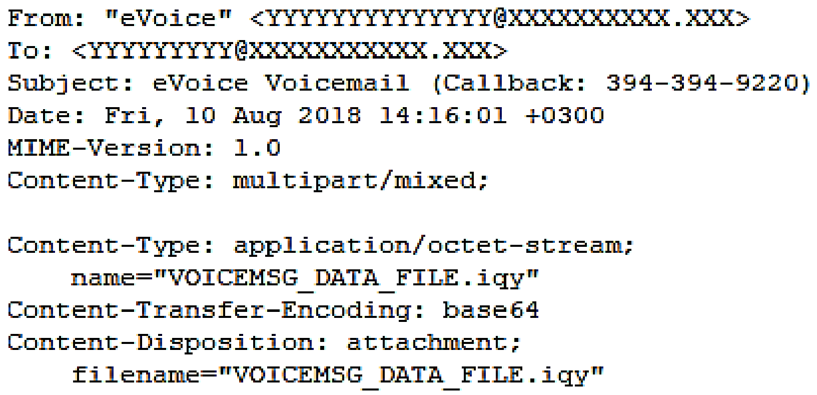
Below are some examples of malicious URLs contained inside Necurs IQY attachments in campaigns X-Force followed:

- http://clodflarechk[.]com/2.dat;
- http://brembotembo[.]com/2.dat;
- http://thespecsupportservice[.]com/duo.dat;
- http://brtt7[.]com/preload.gif;
- http://169.239.129[.]17/404;
- http://t69c[.]com/A.

Enough IQY Files to Go Around

In mid-July 2018, a threat actor group known as DarkHydrus also began using malicious IQY attachments. DarkHydrus' spear phishing emails contained Roshal Archive Compressed (RAR) files that concealed a weaponized IQY file. According to SecurityWeek, the URL inside the IQY file led to running a PowerShell script on the victim's device to set up a backdoor. The campaign is believed to have been nation-state motivated.

Another instance yet: The most recently observed use of malicious IQY attachments came from the Marap downloader malware. The Marap phishing email campaign started in August 2018. IBM X-Force researchers were able to capture emails from this campaign starting on August 10, 2018, confirming they included malicious IQY file attachments.



```
From: "eVoice" <YYYYYYYYYYYYYY@XXXXXXXXXX.XXX>
To: <YYYYYYYYY@XXXXXXXXXXX.XXX>
Subject: eVoice Voicemail (Callback: 394-394-9220)
Date: Fri, 10 Aug 2018 14:16:01 +0300
MIME-Version: 1.0
Content-Type: multipart/mixed;

Content-Type: application/octet-stream;
    name="VOICEMSG_DATA_FILE.iqy"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="VOICEMSG_DATA_FILE.iqy"
```

Figure 5.4. Necurs-borne email hauling IQY attachment that fetches the Marap malware (Source: IBM X-Force)

IQY — You Know Why…

Using various and often little-known file types and extensions in spam email is a growing trend among major botnet and spam distributors. To ensure that their malicious emails reach recipients and do not end up blocked by email filters, cybercrime groups shuffle their tactics all the time, delivering booby-trapped files in many shapes throughout the year.

Since IQY files are inherently useful and prevalent on many enterprise networks, some security practices can help mitigate the risk associated with them without having to block the use of those files altogether.

Useful Tips for Defenders

- One of the best defense strategies is to spread the word about popular spammer tactics. Ensure that everyone within your organization is aware of the dangers that IQY files pose. As their popularity in spam campaigns rises, incorporate IQY files into organizational antispam and phishing training.
- If IQY files are not used within your environment, they can be blocked with group policies. System administrators can modify Trust Center settings to disable data connections initiated from within Excel spreadsheets.
- If IQY files are required on your organization’s networks, get creative with advanced email filtering rules. Some email security solutions give the option to inspect the contents of an email attachment. Keep in mind that blocking specific malicious content found in an attachment could still allow legitimate IQY files through.

- Use IP whitelisting in email filtering rules for allowed senders of IQY files. Be cautious of using domain whitelisting rules because threat actors commonly spoof email domains during spear phishing attempts.
- Keep up to date on emerging threats and indicators of compromise (IoCs) gleaned from them. Block access to known malicious URL IoCs that current threat actors are using in IQY files.
- Ensure your security information and even management (SIEM) systems can identify threats, especially unknown ones. IBM's QRadar SIEM uses analytics and intelligence to identify indicators of advanced threats that might otherwise go unnoticed.

Source: https://securityintelligence.com/threat-actors-peddling-weaponized-iqy-files-via-necurs-botnet/

6. US still takes top spot for hosting malicious domains and exploit kits, researchers find

The US was also found to be the number one hoster for exploit kits, accounting for more EKs globally than all other countries combined. Security researchers also found cybercriminals consistently exploit older vulnerabilities as well.

The United States still takes the crown for hosting malicious domains and exploit kits in Q2 2018, according to a new study. According to statistics from Palo Alto Network's Unit 41, the US was the number one hoster of malicious domains that potentially served web-based threats at a global level.

Researchers found the US hosted 248 malicious URLs between April and June 2018 (Q2), a drop from 257 recorded in Q1. Other top countries hosting malicious domains include Russia, China, Hong Kong and the Netherlands. Besides the Netherlands and the US, the number of malicious domains dropped across most of the top countries, particularly in Russia and China.

In China, the number of malicious domains hosted dropped from 106 in Q1 to just two in Q2. In Russia, the number shrunk from 20 in Q2 to two malicious domains.

EK top spot claimed by the US

The US was also found to be the number one hoster for exploit kits as well, accounting for more EKs globally than all other countries combined. In fact, the US accounted for more than twice the number of EKs as the number two hoster - Russia.

The US was the number one source for Grandsoft, Sundown and Rig and the number two source for KaiXin. Meanwhile, Russia was number two globally for Grandsoft, Sundown and Rig. Researchers found KaiXin - which targets the 4-year-old vulnerability - CVE-2014-6332 - seemed to be more popular in Asia and primarily popped up in China, Hong Kong and Korea.

Old is gold

In terms of vulnerabilities, Unit 42 found threat actors still rely on much older flaws to exploit in new attack campaigns. Two nine-and-a-half-year-old Microsoft IE vulnerabilities - CVE-2009-0075 and CVE-2008-4844 - made it to the top five list. Other frequently exploited vulnerabilities in this quarter included an OLE automation flaw (CVE-2014-6332), one in Adobe Reader (CVE-2015-5122) and a Microsoft VBScript flaw (CVE-2016-0189).

Meanwhile, the latest security vulnerability aggressively leveraged in exploit kits is CVE-2018-8174, a Microsoft VBScript vulnerability that was heavily used in zero-day attacks. The vulnerability was patched by Microsoft in May 2018. However, DarkHotel APT exploited this flaw, also known as DoubleKill, in zero-day attacks.

"This vulnerability wasn't publicly known until the second quarter and we can see was quickly used by attackers taking advantage of it, making it number two on our list in the second quarter, exploited by 291 malicious URLs," researchers noted. "The net lessons from this quarter's statistics are the very old and very new vulnerabilities show themselves to be useful. There's also a steadiness to the vulnerabilities attackers are favoring since four of the top five vulnerabilities this quarter were in use last quarter.

"In the realm of vulnerabilities, we see remarkable consistency, with a nearly identical roster of vulnerabilities under attack in this quarter as last quarter. The only notable addition to this roster is a vulnerability known to be used in zero-day attacks."

Source: *https://cyware.com/news/us-still-takes-top-spot-for-hosting-malicious-domains-and-exploit-kits-researchers-find-e2301db2*

7. 4 New Smart Office Security Risks and How to Mitigate Them

Internet of Things (IoT) devices will bring a bevy of benefits to businesses, including productivity, energy savings, efficiency, safety and so much more. So it's no wonder the smart office market is forecast to nearly double by 2023, according to a study by Mordor Intelligence.

But smart devices also present a new and growing security threat. Any smart device connected to the company Wi-Fi, officially sanctioned or otherwise, can present a risk to the network. Or, in other words, your company's next major security risk may come from a device as seemingly innocent as the coffee machine.

In fact, the security risk from IoT devices has become one of the hottest and most vexing topics of discussion within the cybersecurity community.

Why We Need New Categories for IoT Devices in the Enterprise

Technology buyers are presented with smart devices in predictable categories, such as "device management," "security," "safety automation," "heating, ventilation and air conditioning automation," "smart ergonomics" — the list goes on and on.

From a security standpoint, however, we need new ways of thinking about workplace IoT devices — by which I mean new categories. Let's take a closer look at four categories for smart office devices from a security point of view.

1) USB-Powered Gadgets

The bring-your-own-device (BYOD) challenge persists. In the past, we understood and could predict what endpoints employees would bring into the enterprise network. But when those devices are IoT smart office gadgets, it's almost impossible to guess what will show up, how it will work and what the implications are for security.

The most innocuous-seeming general category of devices might be anything that gets power from a USB port. These devices include cup warmers, reading lights, fans, desktop humidifiers, Wi-Fi extenders — you name it. They don't seem to make an office particularly "smart."

What's troubling about this category is that while these devices ostensibly use USB ports for power only, they are in fact plugging into a data port. Any of these devices could contain storage, processing and a malicious payload. Most are bought cheaply and manufactured overseas by no-name companies.

To an IT security professional, the practice of blindly purchasing connected devices is functionally equivalent to finding a USB thumb drive in the parking lot and plugging it in to a system inside the firewall.

2) Spy Tech

Anything with a camera or microphone could expose company secrets. We're entering an age of smart speakers and displays, which were initially aimed at consumers but are now headed for the enterprise. These devices work normally by capturing audio with microphones and storing it in a remote server.

Of somewhat less concern are the cameras, which could be used to spy on a room in the same way that some attackers have been able to hijack the cameras in laptops. It's very early days for these devices, and the security implications won't be hammered out for years. In the meantime, the harvesting and off-site storage of audio, video and photographs continues.

3) DDoS Robots

Office IoT devices can be hijacked and dragooned into service as part of a distributed denial-of-service (DDoS) attack.

Last year, the IoT Reaper botnet shut down major internet providers by taking over millions of IoT devices. It focused mostly on exploiting known security flaws and targeted mainly security cameras, DVRs, and other camera-based devices and major-brand routers.

4) Orphan Devices

The introduction of smart office devices may involve a handoff in responsibility from facilities to IT. Any office equipment that plugs into the building's electrical outlets but not the network probably falls under the purview of facilities. Anything that plugs into the network — or plugs into a device that plugs into a network — is likely IT's problem.

A whole range of orphan-making is taking place with a transition to a smart workplaces. Devices normally managed by facilities are increasingly connecting to the network as part of a larger push for the smart office. Yet, in many cases, these devices are still managed by facilities — or they're left in a kind of orphan state where nobody's really paying attention to what the devices are up to.

Let's say conventional thermostats are replaced with "smart" thermostats, for example. Is IT involved in the purchase? Are these devices getting updates from the manufacturer? Are they getting "updates" from individuals or organizations that are not the manufacturer? Chances are, these devices are falling through the cracks with nobody managing the security end of things.

The purpose of these categories is to clarify responsibility and the actions that need to be taken to protect against the specific risks associated with each type of device.

How to Manage the Smart Office Smartly

Industry groups are working to figure out the larger issues around IoT security inside enterprises, but you can't afford to wait. Here's what you and your organization can do right now to protect yourselves from new threats posed by smart devices:

- **Develop an IoT strategy**. This should include, among other things, a ban on devices that cannot or will not get security patches and updates from the manufacturer. It should also include a policy of disabling all unused features for smart office equipment.
- **Maintain an inventory of every smart device.** Make sure the database includes details about the manufacturer, how updates are handled and security specifics. A centralized inventory helps facilitate communication between departments and among new hires.

- **Train employees about the special risks associated with IoT devices**. Everyone needs to be as leery about USB-powered cup warmers as they are about thumb drives.
- **Actively share information.** across departments and vendors about security-related events that take place with smart office devices.
- **Invest in a unified endpoint management (UEM) system.** Make sure you select a solution that covers IoT devices just like it does other computing categories.
- **Use strong password management tools**. Institute the same stringent password requirements for IoT devices as you would networked computers. Above all, change and manage the default passwords for IoT devices that have them. Attackers know the default passwords and will search for them.

The smart office is ushering in a better work environment, but it's important to address security gaps sooner rather than later. After all, expanding your workplace network without managing security just isn't very smart.

Source: https://securityintelligence.com/4-new-smart-office-security-risks-and-how-to-mitigate-them/

8. Active Spy Campaign Exploits Unpatched Windows Zero-Day

The PowerPool gang launched its attack just two days after the zero-day in the Windows Task Scheduler was disclosed.

The recently discovered Windows zero-day – which still doesn't have a patch – has been used in the wild for the last week, with an active info-stealing campaign emerging just two days after its disclosure on Twitter.

The flaw is a local privilege escalation vulnerability in the Windows Task Scheduler's Advanced Local Procedure Call (ALPC) interface — it allows a local unprivileged user to change the permissions of any file on the system and modify it, including system files that are executed by privileged processes.

Security researcher "SandboxEscaper" spilled the beans on the flaw on August 27 with some amount of frustration in the vulnerability reporting process: "I don't [redacted] care about life anymore. Neither do I ever again want to submit to MSFT anyway," the researcher said in a since-deleted tweet, while linking to a proof-of-concept (PoC) exploit code on GitHub.

The PoC was straightforward: "SandboxEscaper's PoC specifically overwrites a printing-related DLL to make it launch notepad.exe, then triggers the Print Spooler service (spoolsv.exe) to load the DLL," explained researchers at Barkly, in a blog about the newly-discovered exploit posted Wednesday. "As a result, notepad.exe is spawned as SYSTEM."

The PoC feature full source code, thus lowering the malware development bar considerably; most PoCs offer only compiled code, which would require reverse-engineering on the part of bad actors.

"It was easy for PowerPool developers to integrate the exploit into their code," Matthieu Faou, malware researcher at ESET, told Threatpost. "The reverse-engineering of an exploit is generally highly time-consuming."

So perhaps it's no surprise that within two days, the PowerPool gang, a known threat group, had modified the PoC to gain write access to the GoogleUpdate.exe function, which is the legitimate updater for Google applications. As such, it runs with admin privileges. According to researchers at ESET, PowerPool has replaced the updater with a malicious executable that is thus launched with elevated privileges whenever the updater is called.

The Campaign

According to ESET researchers, the PowerPool group initially compromises victims via spear-phishing emails with a malicious attachment. The emails use a typical "you have not settled this invoice" lure.

That attachment – no word on the format, but PowerPool has used tricky Symbolic Link (.slk) file attachments in the past – is a first-stage malware with two Windows executables, used for reconnaissance on the machine.

The main executable is a backdoor that establishes persistence and collects basic machine and proxy information; it then exfiltrates the data to the command-and-control (C2) server. ESET said that it can also execute commands. The other executable only does one thing: It takes a screenshot of the victim's display and sends it to the C2.

If the attackers decide that the victim machine looks like a good prize, the first-stage backdoor fetches a second-stage malware, which is more rudimentary than the usual APT backdoor, ESET researchers noted. However, it uses the zero-day exploit to elevate its privileges to system admin, which gives the attackers an unfettered view to other parts of the network.

The team found that the second-stage code thus downloads an array of open-source lateral-movement tools, mostly written in PowerShell. Among other things, these can retrieve usernames and hashes from the Security Account Manager (SAM); perform pass-the-hash SMB connections; retrieve Windows credentials; and lift stored passwords from Outlook, web browsers and so on.

More to Come

The campaign is limited for now, according to ESET telemetry, which may indicate that the recipients are carefully chosen rather than on the receiving end of a mass-mailing spam effort. However, it's unlikely to be the only use of the zero-day by threat groups.

“The disclosure of vulnerabilities outside of a coordinated disclosure process generally puts many users at risk,” ESET researchers noted in their analysis posted on Wednesday. “This specific campaign targets a limited number of users, but don’t be fooled by that: it shows that cybercriminals also follow the news and work on employing exploits as soon as they are publicly available.”

Users should be on high alert: CERT-CC has confirmed that all supported Windows versions are vulnerable.

“Windows has a customer commitment to investigate reported security issues, and proactively update impacted devices as soon as possible,” a Microsoft spokesperson told Threatpost last week. “Our standard policy is to provide solutions via our current Update Tuesday schedule.”

While Microsoft has yet to roll out a patch (one could be upcoming in September’s Patch Tuesday), a third-party “micropatch” is available from 0Patch for 64-bit versions of Windows 7, Windows 10, Windows Server 2008 and Windows Server 2016. There are also mitigations (not yet acknowledged by Microsoft) listed on the CERT-CC site.

Source: https://threatpost.com/active-spy-campaign-exploits-unpatched-windows-zero-day/137237/

9. Bug bounty alert: Elon Musk invites hackers to torpedo Tesla firmware

Carmaker won't void warranties for those seeking security vulnerability rewards

Tesla says it will allow security researchers to hunt for vulnerabilities in its cars' firmware – as long as it is done as part of a new bug bounty program.

The luxury electric automaker said this week it will reflash the firmware on cars that have been bricked by infosec bods probing for exploitable bugs in its code, provided they have suitably enrolled in the Elon Musk-run biz's updated bounty program. And any sanctioned searching can be carried out with worrying about being sued by Tesla's legal eagles.

“If, through your good-faith security research, you (a pre-approved, good-faith security researcher) cause a software issue that requires your research-registered vehicle to be updated or ‘reflashed,’ as an act of goodwill, Tesla shall make reasonable efforts to update or ‘reflash’ Tesla software on the research-registered vehicle by over-the-air update, offering assistance at a service center to restore the vehicle's software using our standard service tools, or other actions we deem appropriate,” Tesla’s updated security policy now reads.

“Tesla has complete discretion as to the software or other assistance that will be provided and it may be only for a limited number of times. Tesla's support does not extend to any out-of-pocket expenses (e.g. towing) incurred by you.“

Tesla also said that research done through its bug bounty program will not be subject to any legal reprisal, either through criminal complaints (via the US Computer Fraud and Abuse Act) or copyright assertions (the US Digital Millennium Copyright Act). Warranties will also remain valid for those who enroll as security researchers.

“Tesla will not consider software changes, as a result of good-faith security research performed by a good-faith security researcher, to a security-registered vehicle to void the vehicle warranty of the security-registered vehicle, notwithstanding that any damage to the car resulting from any software modifications will not be covered by Tesla under the vehicle warranty,” the policy reads.

The announcement will put to rest fears from security bods that Tesla would wield the DMCA and the CFAA laws as weapons against anyone who hacked its products for research. Without the fear of legal reprisal, infosec types will now be free to pop open Tesla firmware to hunt for bugs and claim rewards.

Among those applauding the carmaker was Bugcrowd founder Casey Ellis, whose startup oversees payouts made through Tesla's bug bounty program.

Ellis told The Register that while Tesla had previously had a good relationship with researchers, putting everything down into a concrete policy will help to bring more researchers into the fold.

"The problem they're addressing with safe-harbor is the overall reservation in the hacker community to engage to help because of the anti-hacking laws which exist," Ellis explained. "They're also signaling the importance of bilateral safe-harbor to other companies which are running similar programs."

This doesn’t however, mean that just anyone can screw up their Tesla and get a free reflash from the company. To be protected by the security policy, owners will need to register both themselves and their cars as part of the bug research program. Researchers will also be subject to guidelines for responsible disclosure, including not accessing other people’s data, giving Tesla a reasonable time frame to patch the discovered flaw, and not exposing their hacked cars to any unsafe conditions.

Those who want to be enrolled in the research program will need to contact Tesla directly to be vetted.

Source: https://www.theregister.co.uk/2018/09/06/tesla_bug_bounty_policy_update/

10.Generally Disclosing Pretty Rapidly: GDPR strapped a jet engine on hacked British Airways

Analysis

If Equifax's mother-of-all-security-disasters last year underlined one thing, it was that big companies think they can weather just about anything cybercriminals – and regulators – can throw at them.

One unpatched web server, 147 million mostly US customer records swiped, and a political beating that should pulverise a company's reputation for good ("one of the most egregious examples of corporate malfeasance since Enron," said US Senate Democratic leader Chuck Schumer), and yet Equifax is not only still standing but perhaps even thriving.

While it's true the full financial consequences yet to unfold, it's hard not to notice that its shares last week rode back to within spitting distance of where they were before the breach was made public.

It all stands in fascinating contrast to what is happening in the UK and Europe, where the mood over database security breaches is darkening. It's not that there are necessarily more of them so much as the speed with which they are being revealed.

Last week's British Airways hack makes an interesting case study, not simply because of the technically embarrassing fact cybercriminals were able to skim up to 380,000 transactions in real time but the speed with which the company owned up to the calamity.

Confessions

According to BA, the attack began at 22.58 BST on August 21, and was stopped at 21:45 BTS on September 5. This meant BA had taken 15 days to notice hackers were grabbing its customers' card numbers, but under 24 hours to tell the world via Twitter and email – a contender for a world record for computer security breach confessions.

Security analysts RiskIQ have speculated that the same gang was behind June's Ticketmaster web breach, which took a still fairly rapid five days to surface after being discovered on June 23. Perhaps the best example of how the security breach atmosphere is changing is T-Mobile US, which uncovered miscreants slurping account records of 2.2 million customers on August 20 and revealed that fact only four days later.

Compare this haste to Equifax, which detected its breach on July 29 last year, but only told the world months later on September 7.

Why the sudden hurry? In the case of BA, officially, the answer is Article 33 of Europe's GDPR, under which cyber-break-ins involving personal data must be reported within 72 hours. Security breaches are now understood as having their own lifecycle. At the user end, a recent report from EMW Law LLP found that complaints to the UK's Information Commissioner after May’s GDPR launch reached 6,281, a doubling compared to the same period in 2017.

“This is definitely due to the awareness and the run up to the GDPR,” agreed Falanx Group senior data protection and privacy consultant Lillian Tsang. But there’s more to it than that. “Reporting a breach shows awareness, the notion of “doing” something – even if the breach cannot be mitigated quick enough. It does show pragmatism, rather than a reactive stance of yesteryears.”

Breaches will never become just another battle scar to be marked up to experience – they are too serious and expensive for that no matter what the shareholders think when share prices recover. What is becoming stressful is the speed of disclosure.

“Crisis management is a relatively new yet vitally important area to focus on. As more chief staff realise that it’s a case of when rather than if a breach occurs, it is highly possible that more businesses have a ready-made crisis procedure waiting for a potential strike,” said ESET security specialist, Jake Moore.

As the breaches keep coming however, he believes an example will eventually be made of someone. “The ICO are likely to want to stick the GDPR message to a high-profile company to show its magnitude and therefore companies are ready to show that they are more compliant than ever before.”

It could be that BA’s rapid breach disclosure has set the benchmark at the sort of uncomfortable standard many, including its competitors, will struggle to match. ®

Source: https://www.theregister.co.uk/2018/09/12/ba_equifax_breach_notification_speed/

11. Five Weakest Links in Cybersecurity That Target the Supply Chain

Third-party breaches have become an epidemic as cybercriminals target the weakest link. Organizations such as BestBuy, Sears, Delta and even NYU Medical Center are just a few that have felt the impact of cyberattacks through third-party vendors.

The fallout from these breaches can be costly, as the average enterprise pays $1.23 million per incident, up 24 percent from $992,000 in 2017 according to Kaspersky Lab. The same report also notes that SMBs spend $120,000; an increase of 36 percent from last year.

With a spike in cyberattacks directly targeting supply chains across the globe, the problem stems from several issues: all of them involve some type of necessary sharing, from shared credentials to shared infrastructure.

Weakest Link No. 1: Shared Credentials

Look no further than the Target breach to see how terribly things can go wrong when businesses share their credentials with third-party vendors, especially with companies that seem benign: Target's breach was reportedly through an air conditioning vendor. When a company shares sensitive credentials with a supplier, the door is left wide open to potential attacks. It should also be noted that most companies–even smaller ones–work with anywhere from several to thousands of vendors, increasing the risk exponentially. This situation dictates that companies must ensure that a rigorous vetting process is put in place before sharing credentials.

Weakest Link No. 2: Shared Data

Shared data can be another key weakness. Companies share highly sensitive and private content with vendors, including customer data, which is unavoidable. These vendors may also share data with many more whose cyber security posture is not known. Case in point: The Experian breach ended up exposing millions of Americans' personal data, but it also exposed 15 million customers' data who applied for the T-Mobile service. While Experian was the primary target, T-Mobile suffered a huge loss as well.

Weakest Link No. 3: Shared Code or Applications

Ticketmaster made this mistake with Inbenta Technologies, a third-party supplier hosting a Ticketmaster customer support product. As part of this process, Ticketmaster received customized JavaScript code, which a hacker gained access to through Inbenta and then modified the code to be malicious. Every single piece of code or application that a company shares with a supplier means exposure to another potential attack.

Weak Link No. 4: Shared Network

Connecting with other companies can be a boon for business, but this particular type of collaboration is also rife with risk. Imagine a scenario in which WannaCry ransomware is able to run rampant from company to company all around the world. For those IT teams that have no choice but to use these types of connections, it is absolutely essential to downsize the number of vendors that share a connection, create tighter permissions and monitor them on an ongoing basis.

Weakest Link No. 5: Shared Infrastructure

Problems with shared infrastructure can quickly cause a direct blow to businesses by halting continuity. For example, if the vendor supplying retail infrastructure suddenly drops or the service goes down, the company is instantly left without a way to handle transactions. And just like that, customers are forced to head to a competitor. Medical processing services are another example; the service goes down and, without warning, the doctors have a difficult time doing their jobs because their patient information is temporarily inaccessible, as we saw in a recent incident at MEDAntex.

Mitigating Risks with Suppliers

The first step in reducing security risks associated with third-party vendors is to hammer out a digital vendor risk management plan that includes rules, procedures and a rigorous vetting process. The vetting process has to go far beyond a mere questionnaire; it must also include the context and level of risk of business relationships. Automation is key for these processes so that companies are able to scale to manage hundreds and thousands of vendors on a daily basis.

An outside reporting company should be employed to continuously monitor the cyber posture of any third-party vendor and ensure it's on par with the security risk level that the evaluating organization accepts. There should also be a way to alert the evaluating organization of infractions, so that they can easily work with vendors to correct and improve their security posture. With these processes in place, the whole digital ecosystem could be improved significantly.

Source: https://threatpost.com/five-weakest-links-in-cybersecurity-that-target-the-supply-chain/137453/

12. Zero-Day Bug Allows Hackers to Access CCTV Surveillance Cameras

Between 180,000 and 800,000 IP-based closed-circuit television cameras are vulnerable to a zero-day vulnerability that allows hackers to access surveillance cameras, spy on and manipulate video feeds or plant malware. According to a Tenable Research Advisory issued Monday, the bugs are rated critical and tied to firmware possibly used in one of 100 different cameras that run the affected software. NUUO, the Taipei, Taiwan-base company that makes the firmware, is expected to issue a patch for the bug Tuesday. The company lists over a 100 different partners including Sony, Cisco Systems, D-Link and Panasonic. It's unclear how many OEM partners may use the vulnerable firmware. The vulnerabilities (CVE-2018-1149, CVE-2018-1150), dubbed Peekaboo by Tenable, are tied to the software's NUUO NVRMini2 webserver software.

"Once exploited, Peekaboo would give cybercriminals access to the control management system, exposing the credentials for all connected video surveillance cameras. Using root access on the NVRMini2 device, cybercriminals could disconnect the live feeds and tamper with security footage," researchers said.

Last year, the Reaper Botnet, a variant of the Mirai botnet, also targeted NUUO NVR devices, according to Tenable. These most recent vulnerabilities similarly open cameras up to similar botnet attacks. The first vulnerability (CVE-2018-1149) is the zero-day. Attacker can sniff out affected gear using a tool such as Shodan. Next, the attacker can trigger a buffer-overflow attack that allows them to access the camera's web server Common Gateway Interface (CGI), which acts as the gateway between a remote user and the web server. According to researchers, the attack involves delivering a cookie file too large for the CGI handle. The CGI then doesn't validate user's input properly, allowing them to access the web server portion of the camera. "[A] malicious attackers can trigger stack overflow in session management routines in order to execute arbitrary code," Tenable wrote.

The second bug (CVE-2018-1150) takes advantage of a backdoor functionality in the NUUO NVRMini2 web server. "[The] back door PHP code (when enabled) allows unauthenticated attacker to change a password for any registered user except administrator of the system," researchers said. NUUO's fix includes version 3.9.1 (03.09.0001.0000) or later. According to Tenable, NUUO was notified in June of the vulnerability. Under Tenable's notification and disclosure policies it gave NUUO 105 days to issue a patch before publicly disclosing the bugs.

"It's unfortunate, but each camera will need to be updated manually by users," said Renaud Deraison, co-founder and CTO of Tenable in an interview with Threatpost.

"We believe vulnerable IoT devices such as these raise serious questions about how we as an industry can manage large numbers of devices. Even in a corporate environment, if the number of connected devices grows at the forecasted rate, we are going to need to rethink our patching cadence and methodology," Deraison said.

Source: https://threatpost.com/zero-day-bug-allows-hackers-to-access-cctv-surveillance-cameras/137499/

13. New trends in the world of IoT threats

Cybercriminals' interest in IoT devices continues to grow: in H1 2018 we picked up three times as many malware samples attacking smart devices as in the whole of 2017. And in 2017 there were ten times more than in 2016. That doesn't bode well for the years ahead.

We decided to study what attack vectors are deployed by cybercriminals to infect smart devices, what malware is loaded into the system, and what it means for device owners and victims of freshly armed botnets.

One of the most popular attack and infection vectors against devices remains cracking Telnet passwords. In Q2 2018, there were three times as many such attacks against our honeypots than all other types combined.

service	% of attacks
Telnet	75.40%
SSH	11.59%
other	13.01%

When it came to downloading malware onto IoT devices, cybercriminals' preferred option was one of the Mirai family (20.9%).

#	downloaded malware	% of attacks
1	Backdoor.Linux.Mirai.c	15.97%
2	Trojan-Downloader.Linux.Hajime.a	5.89%
3	Trojan-Downloader.Linux.NyaDrop.b	3.34%
4	Backdoor.Linux.Mirai.b	2.72%
5	Backdoor.Linux.Mirai.ba	1.94%
6	Trojan-Downloader.Shell.Agent.p	0.38%
7	Trojan-Downloader.Shell.Agent.as	0.27%
8	Backdoor.Linux.Mirai.n	0.27%
9	Backdoor.Linux.Gafgyt.ba	0.24%
10	Backdoor.Linux.Gafgyt.af	0.20%

Top 10 malware downloaded onto infected IoT device following a successful Telnet password crack

In Q2 2018 the leader by number of unique IP addresses from which Telnet password attacks originated was Brazil (23%). Second place went to China (17%). Russia in our list took 4th place (7%). Overall for the period January 1 – July 2018, our Telnet honeypot registered more than 12 million attacks from 86,560 unique IP addresses, and malware was downloaded from 27,693 unique IP addresses.

Since some smart device owners change the default Telnet password to one that is more complex, and many gadgets don't support this protocol at all, cybercriminals are constantly on the lookout for new ways of infection. This is stimulated by the high competition between virus writers, which has led to password bruteforce attacks becoming less effective: in the event of a successful crack, the device password is changed and access to Telnet is blocked.

An example of the use of "alternative technology" is the Reaper botnet, whose assets at end-2017 numbered about 2 million IoT devices. Instead of bruteforcing Telnet passwords, this botnet exploited known software vulnerabilities:

- Vulnerabilities in D-Link 850L router firmware;
- Vulnerabilities in GoAhead IP cameras;
- Vulnerabilities in MVPower CCTV cameras;
- Vulnerability in Netgear ReadyNAS Surveillance;
- Vulnerability in Vacron NVR;
- Vulnerability in Netgear DGN devices;
- Vulnerabilities in Linksys E1500/E2500 routers;
- Vulnerabilities in D-Link DIR-600 and DIR 300 – HW rev B1 routers;
- Vulnerabilities in AVTech devices;

Advantages of this distribution method over password cracking:

- Infection occurs much faster;
- It is much harder to patch a software vulnerability than change a password or disable/block the service.

Although this method is more difficult to implement, it found favor with many virus writers, and it wasn't long before new Trojans exploiting known vulnerabilities in smart device software started appearing.

New attacks, old malware

To see which vulnerabilities are targeted by malware, we analyzed data on attempts to connect to various ports on our traps. This is the picture that emerged for Q2 2018:

Service	Port	% of attacks	Attack vector	Malware families
Telnet	23, 2323	82.26%	Bruteforce	Mirai, Gafgyt
SSH	22	11.51%	Bruteforce	Mirai, Gafgyt
Samba	445	2.78%	EternalBlue, EternalRed, CVE-2018-7445	–
tr-069	7547	0.77%	RCE in TR-069 implementation	Mirai, Hajime
HTTP	80	0.76%	Attempts to exploit vulnerabilities in a web server or crack an admin console password	–

winbox (RouterOS)	8291	0.71%	Used for RouterOS (MikroTik) authentication and WinBox-based attacks	Hajime
Mikrotik http	8080	0.23%	RCE in MikroTik RouterOS < 6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–
GoAhead httpd	81	0.16%	RCE in GoAhead IP cameras	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Authorization bypass (CVE-2017-12113)	–
RDP	3389	0.12%	Bruteforce	–
XionMai uc-httpd	8000	0.09%	Buffer overflow (CVE-2018-10088) in XionMai uc-httpd 1.0.0 (some Chinese-made devices)	Satori
MySQL	3306	0.08%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–

The vast majority of attacks still come from Telnet and SSH password bruteforcing. The third most common are attacks against the SMB service, which provides remote access to files. We haven't seen IoT malware attacking this service yet. However, some versions of it contain serious known vulnerabilities such as EternalBlue (Windows) and EternalRed (Linux), which were used, for instance, to distribute the infamous Trojan ransomware WannaCry and the Monero cryptocurrency miner EternalMiner.

Here's the breakdown of infected IoT devices that attacked our honeypots in Q2 2018:

Device	% of infected devices
MikroTik	37.23%
TP-Link	9.07%
SonicWall	3.74%
AV tech	3.17%
Vigor	3.15%
Ubiquiti	2.80%
D-Link	2.49%
Cisco	1.40%
AirTies	1.25%
Cyberoam	1.13%

HikVision	1.11%
ZTE	0.88%
Miele	0.68%
Unknown DVR	31.91%

As can be seen, MikroTik devices running under RouterOS are way out in front. The reason appears to be the Chimay-Red vulnerability. What's interesting is that our honeypot attackers included 33 Miele dishwashers (0.68% of the total number of attacks). Most likely they were infected through the known (since March 2017) CVE-2017-7240 vulnerability in PST10 WebServer, which is used in their firmware.

Port 7547

Attacks against remote device management (TR-069 specification) on port 7547 are highly common. According to Shodan, there are more than 40 million devices in the world with this port open. And that's despite the vulnerability recently causing the infection of a million Deutsche Telekom routers, not to mention helping to spread the Mirai and Hajime malware families.

Another type of attack exploits the Chimay-Red vulnerability in MikroTik routers running under RouterOS versions below 6.38.4. In March 2018, it played an active part in distributing Hajime.

IP cameras

IP cameras are also on the cybercriminal radar. In March 2017, several major vulnerabilities were detected in the software of GoAhead devices, and a month after information about it was published, there appeared new versions of the Gafgyt and Persirai Trojans exploiting these vulnerabilities. Just one week after these malicious programs were actively distributed, the number of infected devices climbed to 57,000.

On June 8, 2018, a proof-of-concept was published for the CVE-2018-10088 vulnerability in the XionMai uc-httpd web server, used in some Chinese-made smart devices (for example, KKMoon DVRs). The next day, the number of logged attempts to locate devices using this web server more than tripled. The culprit for this spike in activity was the Satori Trojan, known for previously attacking GPON routers.

New malware and threats to end users

DDoS attacks

As before, the primary purpose of IoT malware deployment is to perpetrate DDoS attacks. Infected smart devices become part of a botnet that attacks a specific address on command, depriving the host of the ability to correctly handle requests from real users. Such attacks are still deployed by Trojans from the Mirai family and its clones, in particular, Hajime.

This is perhaps the least harmful scenario for the end user. The worst (and very unlikely) thing that can happen to the owner of the infected device is being blocked by their ISP. And the device can often by “cured” with a simple reboot.

Cryptocurrency mining

Another type of payload is linked to cryptocurrencies. For instance, IoT malware can install a miner on an infected device. But given the low processing power of smart devices, the feasibility of such attacks remains in doubt, even despite their potentially large number.

A more devious and doable method of getting a couple of cryptocoins was invented by the creators of the Satori Trojan. Here, the victim IoT device acts as a kind of key that opens access to a high-performance PC:

- At the first stage, the attackers try to infect as many routers as possible using known vulnerabilities, in particular:
  - CVE-2014-8361 – RCE in the miniigd SOAP service in Realtek SDK;
  - CVE 2017-17215 – RCE in the firmware of Huawei HG532 routers;
  - CVE-2018-10561, CVE-2018-10562 – authorization bypass and execution of arbitrary commands on Dasan GPON routers;
  - CVE-2018-10088 – buffer overflow in XiongMai uc-httpd 1.0.0 used in the firmware of some routers and other smart devices made by some Chinese manufacturers.
- Using compromised routers and the CVE-2018-1000049 vulnerability in the Claymore Etherium miner remote management tool, they substitute the wallet address for their own.

Data theft

The VPNFilter Trojan, detected in May 2018, pursues other goals, above all intercepting infected device traffic, extracting important data from it (user names, passwords, etc.), and sending it to the cybercriminals’ server. Here are the main features of VPNFilter:

- Modular architecture. The malware creators can fit it out with new functions on the fly. For instance, in early June 2018 a new module was detected able to inject javascript code into intercepted web pages.

- Reboot resistant. The Trojan writes itself to the standard Linux crontab job scheduler and can also modify the configuration settings in the non-volatile memory (NVRAM) of the device.
- Uses TOR for communication with C&C.
- Able to self-destruct and disable the device. On receiving the command, the Trojan deletes itself, overwrites the critical part of the firmware with garbage data, and then reboots the device.

The Trojan's distribution method is still unknown: its code contains no self-propagation mechanisms. However, we are inclined to believe that it exploits known vulnerabilities in device software for infection purposes.

The very first VPNFilter report spoke of around 500,000 infected devices. Since then, even more have appeared, and the list of manufacturers of vulnerable gadgets has expanded considerably. As of mid-June, it included the following brands:

- ASUS;
- D-Link;
- Huawei;
- Linksys;
- MikroTik;
- Netgear;
- QNAP;
- TP-Link;
- Ubiquiti;
- Upvel;
- ZTE.

The situation is made worse by the fact that these manufacturers' devices are used not only in corporate networks, but often as home routers.

Conclusion

Smart devices are on the rise, with some forecasts suggesting that by 2020 their number will exceed the world's population several times over. Yet manufacturers still don't prioritize security: there are no reminders to change the default password during initial setup or notifications about the release of new firmware versions, and the updating process itself can be complex for the average user. This makes IoT devices a prime target for cybercriminals.

Easier to infect than PCs, they often play an important role in the home infrastructure: some manage Internet traffic, others shoot video footage, still others control domestic devices (for example, air conditioning).

Malware for smart devices is increasing not only in quantity, but also quality. More and more exploits are being weaponized by cybercriminals, and infected devices are used to steal personal data and mine cryptocurrencies, on top of traditional DDoS attacks.

Here are some simple tips to help minimize the risk of smart device infection:

- Don't give access to the device from an external network unless absolutely necessary
- Periodic rebooting will help get rid of malware already installed (although in most cases the risk of reinfection will remain)
- Regularly check for new firmware versions and update the device
- Use complex passwords at least 8 characters long, including upper and lower-case letters, numerals, and special characters
- Change the factory passwords at initial setup (even if the device does not prompt you to do so)
- Close/block unused ports, if there is such an option. For example, if you don't connect to the router via Telnet (port TCP:23), it's a good idea to disable it so as to close off a potential loophole to intruders.

Source: https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

14.XBash Malware Packs Double Punch: Destroys Data and Mines for Crypto Coins

Researchers have discovered a new sophisticated malware family in the wild, which wrecks havoc on Windows and Linux systems with a combination of data destructive ransomware and malicious cryptomining. The malware, dubbed by Palo Alto Networks' Unit 42 researchers who discovered it as Xbash, has been targeting weak passwords and unpatched vulnerabilities to infect systems. Xbash also shares striking similarities to worms like WannaCry and Petya/NotPetya, such as self-propagation capabilities and its ability to rapidly spread.

"Xbash aimed on discovering unprotected services, deleting victim's MySQL, PostgreSQL and MongoDB databases, and ransom for Bitcoins," the researchers said in a post. "Xbash uses three known vulnerabilities in Hadoop, Redis and ActiveMQ for self-propagation or infecting Windows system."

Xbash has an array of features that make it stand out. It specifically targets Windows and Linux, it's developed in Python, it fetches IP addresses and domain names from its C2 servers for exploiting, and it has intranet scanning functionality. Researchers discovered four different versions of Xbash so far. All have an array of sophisticated capabilities, including quick development (using Python), easy installation, anti-detection features and cross-platform capabilities. Despite this high level of sophistication, researchers said that code and timestamp differences among the four versions show that the malware is still under active development.

The botnet began to operate since as early as May 2018, and so far, researchers said they observed 48 incoming transactions to the Bitcoin wallet addresses (totaling $6,000 total) used by the malware – possibly indicating 48 victims of its ransom behavior.

Attack Vector

The malware focuses on three known vulnerabilities: A Hadoop YARN ResourceManager unauthenticated command execution flaw (discovered in 2016 with no CVE), a Redis arbitrary file write and remote command execution glitch (found in 2015 with no CVE), and ActiveMQ arbitrary file write vulnerability (CVE-2016-3088).

Xbash offers two separate functions for Windows and Linux targets – the malware is capable of understanding the operating system of a targeted system and delivering a payload designed for that OS.

It appears that on Windows, Xbash will focus on malicious cryptomining functions and self-propagation techniques, while on Linux systems, the malware will flaunt its data destructive tendencies; as the malware triggers a downloader to execute a coinminer on Windows, while on Linux it flaunts ransomware functions.

On Linux, Xbash first attempts to log in to a service – generally MySQL, MongoDB, and PostgreSQL. Once successfully logged in, it will delete almost all existing databases in the server and create a new database named "PLEASE_READ_ME_XYZ." It will then insert a ransom message into a table labeled "WARNING" in the new database

The ransomware message asks for .02 BTC, or around $125, as a payment to release the compromised databases. On Windows, the malware will execute a JavaSCript or VBScript downloader. The downloader in turn calls on a coinminer to be executed onto the system: "Depending on Xbash's version, this new startup item will download a malicious HTML or a Scriptlet file from Xbash's C2 server, and to execute the JavaScript or VBScript code in the file via "mshta" or via "regsvr32". These scripts will then invoke PowerShell to download a malicious PE executable or PE DLL file," researchers said. However, Unit 42 researchers said that they have no found evidence of code in Xbash that back up deleted databases at all – meaning that the malicious malware poses as ransomware, but still destructs databases after the ransom has been paid.

Analysis shows that the malware is likely linked to Iron Group, a group publicly linked to other ransomware campaigns including those that use the Remote Control System (RCS), whose source code was believed to be stolen from the HackingTeam in 2015. Researchers made the connection after discovering that Xbash hard-coded a bunch of domain names as its C2 servers – some of which were reused from previous Windows coinminers attributed to Iron cybercrime group.

“After further investigation we realized it’s a combination of botnet and ransomware that developed by an active cybercrime group Iron (aka Rocke) in this year,” the researchers said.

Source: https://threatpost.com/xbash-malware-packs-double-punch-destroys-data-and-mines-for-crypto-coins/137543/

15. Gamma, Bkp, & Monro Dharma Ransomware Variants Released in One Week

This week we have seen three new Dharma Ransomware variants released that append either the .Gamma, .Bkp, & .Monro extensions to encrypted files.

It is highly unusual for this ransomware family to release so many variants released in a short period of time. Typically, one variant used for a month, if not more, and then a new variant is released. Instead, we saw three new variants released in the same week.

All three variants were discovered by security researcher Jakub Kroustek, who posted the samples on Twitter.

When victims are infected with these variants their files will be encrypted and renamed. Depending on the particular variant they are infected with a file called test.jpg would be encrypted and renamed to test.jpg.id-%ID%.[bebenrowan@aol.com].gamma, test.jpg.id-%ID%.[icrypt@cock.li].monro, or test.jpg.id-%ID%.[bkp@cock.li].bkp. These ransomware infections will also drop a ransom note named FILES ENCRYPTED.txt that contains payment instructions.

Source: https://www.bleepingcomputer.com/news/security/gamma-bkp-and-monro-dharma-ransomware-variants-released-in-one-week/

How to protect yourself from the Dharma Ransomware

In order to protect yourself from Dharma, or from any ransomware, 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 the Dharma Ransomware is typically installed via hacked Remote Desktop services, it is very important to make sure it’s 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.

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 you them,
- 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 accessible only via a VPN.

16.Mozilla Launches Firefox Monitor Data Breach Notification Service

On the 25th of September, Mozilla announced the release of Firefox Monitor, a free service to help users find out whether or not their accounts have been part of a breach. This new service was created in partnership with Troy Hunt's Have I been Pwned, whose data is being supplied to Mozilla to power the Firefox Monitor service.

Users can use the Firefox Monitor service to check whether their passwords or emails have been part of a data breach and can also be configured to notify users when their information has been detected.

"It can be hard to keep track of when your information has been stolen, so we're going to help by launching Firefox Monitor, a free service that notifies people when they've been part of a data breach," writes Nick Nguyen of Mozilla. "After testing this summer, the results and positive attention gave us the confidence we needed to know this was a feature we wanted to give to all of our users."

Mozilla explains that their service basically scans the Have I Been Pwned's database and alerts users if it finds a match.

To use the service, simply visit the https://monitor.firefox.com/ and enter your email address. The service will then check if your email address has been part of any breaches and list any that are detected. You can also sign up to receive notifications if your email address is ever detected in future breaches.

What to do if your email address has been pwned?

If you've been pwned, it is recommended that audit any account that were part of the breach, change your password at any sites you use the same credentials, enable two-factor authentication whenever possible, and use strong and unique passwords for every site that you create an account.

If you're interested, you can sign up for the free service here and Mozilla will send you a notification to inform if any of your accounts or email addresses have been exposed in data breaches

Source: https://www.bleepingcomputer.com/news/software/mozilla-launches-firefox-monitor-data-breach-notification-service/

17. Your Web Applications Are More Vulnerable Than You Think

A recent study shined a light on an attack vector that is often overlooked: the insecurity of web applications.

According to the report, issued by Positive Technologies, 44 percent of web applications are vulnerable to data leakage and security problems. In other words, threat actors have easy access to the personal customer data those applications handle across a variety of verticals such as banking, e-commerce and communications.

In addition, 48 percent of the applications were found to be vulnerable to unauthorized access, with 17 percent having exploits that could result in a full takeover by a threat actor. But perhaps the most eye-opening finding is that 100 percent of the web applications tested had some sort of vulnerability in general.

Security as an Afterthought

The web app as an attack vector isn’t a new problem, although we may not have realized how severe the vulnerabilities were. And worse, we’ve allowed the problem to linger: Many developers and IT decision-makers don’t take web app security seriously. Mozilla gave 93 percent of websites it observed a failing grade for security against cross-site scripting (XSS), for example. Application security tends to be treated as an afterthought, pushed behind other, more pressing security issues.

The biggest problem, no matter the programming language used, is XSS, according to the report. The authors also pointed to data leakage, fingerprinting and brute-force attacks as common issues across the board.

App Security Lags Despite Increasing Awareness

"Web application security is still poor and, despite increasing awareness of the risks, is still not being prioritized enough in the development process," said Leigh-Anne Galloway, Positive Technologies cybersecurity resilience lead, as quoted in Infosecurity Magazine. "Most of these issues could have been prevented entirely by implementing secure development practices, including code audits from the start and throughout."

Why is web app security falling behind? In a blog post for Secure Code Warrior, Pieter Danhieux blamed human behavior, stating that not only do humans behave in ways that introduce vulnerabilities and security threats, but developers aren't always brought into the security loop.

"How are developers supposed to write secure code if nobody ever teaches them about why it's important, the consequences of insecure code, and most importantly, how to prevent writing these vulnerabilities in their respective programming frameworks in the first place?" he wrote.

How Cybercriminals Exploit Web Applications to Spread Malware

The Postitive Technologies report cited two primary areas of motivation for cybercriminals to take advantage of web application vulnerabilities. The first is to use apps to infect and spread malware throughout enterprise networks.

"This method was used to spread the Bad Rabbit ransomware: attackers compromised web applications belonging to media outlets and masked malware as an Adobe Flash Player update installer," the report explained.

In another case, an attacker exploited a vulnerability to disseminate phishing emails targeting bank employees.

Some threats don't even involve direct attacks against web apps; cybercriminals can use applications in various ways to launch malware attacks. The moment your website or web application is compromised — no matter the method — your organization's reputation takes a hit, which can lead to financial loss.

Data Theft in a Regulated World

The report also cited data theft as a key motivation for targeting web applications. Data leakage is a problem in any situation, be it customer data or corporate intellectual property.

However, the stakes of stolen data have been raised in a post-General Data Protection Regulation (GDPR) and a pre-California Consumer Privacy Act (CCPA) world.

As more states decide to step up measures to protect customer data, any type of data loss can create extraordinary headaches for company leaders. Loss of data can cost an organization hundreds of thousands to millions of dollars in fines, according to data compiled by TermsFeed. At the same time, as more effort is put into data protection, stolen data will become more valuable on the dark web, encouraging threat actors to improve their targeting and attack styles.

How Can Companies Protect Web Applications?

Data privacy regulations require most companies to improve their web application security capabilities. IT leaders can start by building security measures directly into the app's design as a way to put consumer security and privacy front and center.

"For application security, this means that security and privacy need to be thought about in the planning stages of the Software Development Life Cycle (SDLC)," cybersecurity expert Amit Ashbel wrote for ITProPortal. "Unfortunately, this is not currently the case with many organizations so this will be a large task for the industry."

Built-in security and privacy measures are crucial. Web app developers should also implement a web application firewall, bolster password management, deploy mobile application management features and install security plugins where available.

As the Positive Technologies report pointed out, it is clear that security issues in web applications aren't getting the attention they require, because their annual studies are finding the same mistakes and concerns repeating themselves. Lax security may have been overlooked in the past, but as privacy regulations and their consequences gain traction, application vulnerabilities and data leakage can cost your organization more than just a light fine and a slap on the wrist.

Source: https://securityintelligence.com/your-web-applications-are-more-vulnerable-than-you-think/

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.