telelink

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

Monthly Security Bulletin

July 2018

Contents

1. Microsoft July 2018 Patch Tuesday Fixes 53 Security Bugs Across 15 Products

The Microsoft July 2018 Patch Tuesday is out! This month, the OS maker fixed 53 security flaws in 15 different products.

The list of applications that received patches this month includes:

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Services and Web Apps
- ChakraCore
- Adobe Flash Player
- .NET Framework
- ASP.NET
- Microsoft Research JavaScript Cryptography Library
- Skype for Business and Microsoft Lync
- Visual Studio
- Microsoft Wireless Display Adapter V2 Software
- PowerShell Editor Services
- PowerShell Extension for Visual Studio Code
- Web Customizations for Active Directory Federation ServicesFlash fixes also included

On top of this, the Microsoft July 2018 Patch Tuesday also includes Flash Player security updates, which Adobe released just a few hours ago.

If you're not interested in all security updates and you'd like to filter updates per product, you can use Microsoft's official Security Update Guide, available here.

Tag	CVE ID	CVE Title
Adobe Flash Player	ADV180017	July 2018 Adobe Flash Security Update
.NET Framework	CVE-2018-8284	.NET Framework Remote Code Injection Vulnerability
.NET Framework	CVE-2018-8260	.NET Framework Remote Code Execution Vulnerability
.NET Framework	CVE-2018-8202	.NET Framework Elevation of Privilege Vulnerability
.NET Framework	CVE-2018-8356	.NET Framework Security Feature Bypass Vulnerability
Active Directory	CVE-2018-8326	Open Source Customization for Active Directory Federation Services XSS Vulnerability
ASP.NET	CVE-2018-8171	ASP.NET Security Feature Bypass Vulnerability
Device Guard	CVE-2018-8222	Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
Internet Explorer	CVE-2018-0949	Internet Explorer Security Feature Bypass Vulnerability
Microsoft Devices	CVE-2018-8306	Microsoft Wireless Display Adapter Command Injection Vulnerability
Microsoft Edge	CVE-2018-8289	Microsoft Edge Information Disclosure Vulnerability
Microsoft Edge	CVE-2018-8301	Microsoft Edge Memory Corruption Vulnerability
Microsoft Edge	CVE-2018-8325	Microsoft Edge Information Disclosure Vulnerability

Microsoft Edge	CVE-2018-8324	Microsoft Edge Information Disclosure Vulnerability
Microsoft Edge	CVE-2018-8297	Microsoft Edge Information Disclosure Vulnerability
Microsoft Edge	CVE-2018-8274	Microsoft Edge Memory Corruption Vulnerability
Microsoft Edge	CVE-2018-8278	Microsoft Edge Spoofing Vulnerability
Microsoft Edge	CVE-2018-8262	Microsoft Edge Memory Corruption Vulnerability
Microsoft Office	CVE-2018-8281	Microsoft Office Remote Code Execution Vulnerability
Microsoft Office	CVE-2018-8323	Microsoft SharePoint Elevation of Privilege Vulnerability
Microsoft Office	CVE-2018-8300	Microsoft SharePoint Remote Code Execution Vulnerability
Microsoft Office	CVE-2018-8312	Microsoft Access Remote Code Execution Vulnerability
Microsoft Office	CVE-2018-8299	Microsoft SharePoint Elevation of Privilege Vulnerability
Microsoft Office	CVE-2018-8310	Microsoft Office Tampering Vulnerability
Microsoft PowerShell	CVE-2018-8327	PowerShell Editor Services Remote Code Execution Vulnerability
Microsoft Scripting Engine	CVE-2018-8294	Chakra Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8280	Chakra Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8242	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8125	Microsoft Edge Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8298	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8287	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8288	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8290	Chakra Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8279	Microsoft Edge Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8283	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8286	Chakra Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8275	Microsoft Edge Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8296	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8291	Scripting Engine Memory Corruption Vulnerability
Microsoft Scripting Engine	CVE-2018-8276	Scripting Engine Security Feature Bypass Vulnerability
Microsoft Windows	CVE-2018-8308	Windows Kernel Elevation of Privilege Vulnerability
Microsoft Windows	CVE-2018-8309	Windows Denial of Service Vulnerability
Microsoft Windows	CVE-2018-8305	Windows Mail Client Information Disclosure Vulnerability
Microsoft Windows	CVE-2018-8206	Windows FTP Server Denial of Service Vulnerability
Microsoft Windows	CVE-2018-8319	MSR JavaScript Cryptography Library Security Feature Bypass Vulnerability

Microsoft Windows	CVE-2018-8313	Windows Elevation of Privilege Vulnerability
Microsoft Windows DNS	CVE-2018-8304	Windows DNSAPI Denial of Service Vulnerability
Microsoft WordPad	CVE-2018-8307	WordPad Security Feature Bypass Vulnerability
Skype for Business and Microsoft Lync	CVE-2018-8238	Skype for Business and Lync Security Feature Bypass Vulnerability
Skype for Business and Microsoft Lync	CVE-2018-8311	Remote Code Execution Vulnerability in Skype For Business and Lync
Visual Studio	CVE-2018-8172	Visual Studio Remote Code Execution Vulnerability
Visual Studio	CVE-2018-8232	Microsoft Macro Assembler Tampering Vulnerability
Windows Kernel	CVE-2018-8282	Win32k Elevation of Privilege Vulnerability
Windows Shell	CVE-2018-8314	Windows Elevation of Privilege Vulnerability

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2018-patch-tuesday-fixes-53-security-bugs-across-15-products/

2. Windows Malware Carries Valid Digital Signatures

Researchers from Masaryk University in the Czech Republic and Maryland Cybersecurity Center (MCC) monitored suspicious organizations and identified four that sold Microsoft Authenticode certificates to anonymous buyers. The same research team also collected a trove of Windows-targeted malware carrying valid digital signatures.

"Recent measurements of the Windows code signing certificate ecosystem have highlighted various forms of abuse that allow malware authors to produce malicious code carrying valid digital signatures," researchers wrote. In their work, the researchers also discovered several cases of potentially unwanted programs (PUPs), revealing that along with their ability to sign malicious code, bad actors are also able to control a range of Authenticode certificates.

Gaining this type of unauthorized access has traditionally been easy for attackers using drive-by downloads and phishing, according to Gabriel Gumbs, vice president of product strategy at STEALTHbits Technologies. "And while endpoint security achieved some increases in efficacy over the last five years with the evolution of end point protection platforms, we only ever treated the symptom – and the not cause – of permissive access," Gumbs said. "If an attacker can use a trusted signed certificate to install malware, then the malware will use the access rights granted to that user or the access rights left behind in the form of NTLM hashes to further penetrate the network," he continued. "While this development is a worrying one, applying a least access privilege model would reduce the threat greatly."

Because the value of stolen data will more than make up for the cost of a stolen certificate, malicious actors are inclined to pay for certificates in order to fly under the radar of most protection tools so that they can hide in plain sight as authorized software. "Malware purveyors seem focused on deep technical things until you see their real focus is actually a core business concept: ROI. Criminals are in it for the revenue, and they understand you have to spend money

to make money," added Jonathan Sander, chief technology officer at STEALTHbits Technologies.

The underground economy is growing because many organizations are rapidly expanding their use of code signing certificates. "They are foundational components in many applications and DevOps environments. Unfortunately, in many cases code signing certificates are secured by unsuspecting teams that are focused on delivering code quickly, which allows attackers to intercept them," said Kevin Bocek, vice president of security strategy and threat intelligence at Venafi.

"Organizations must have full control over every code signing certificate they use, especially during the software development pipeline and signing process," Bocek said.

Source: https://www.infosecurity-magazine.com/news/windows-malware-carries-valid/

3. Anubis Malware Re-Emerges Yet Again; Hackers Distributing It via Google Play Store

The Anubis banking malware arises once more with the threat actors allocating the malware on Google Play store applications keeping in mind the end goal to steal login credentials to banking apps, e-wallets, and payment cards. Hackers are constantly known for finding better approaches to sidestep the Google play store security as well as ways to distribute the malware through Android applications that will additionally go about as the initial phase in an "infection routine" schedule that gets the BankBot Anubis mobile banking Trojans by means of C&C server. Users as often as possible get tainted once they download and install the malevolent applications via the Google play store, even though the play store security investigates, all the applications that are transferred into Google Play, cybercriminals dependably execute the most complex and obscure strategies to evade the detection. Researchers as of late discovered anew downloader's in-app store that connected with Anubis banking malware. This campaign is known to contain no less than 10 malevolent downloaders masked as different applications. All the Downloader disseminated through Android applications is known to get more than 1,000 samples from the criminal's command-and-control (C&C) servers.

"In most Android banking Trojans, the malware launches a fake overlay screen when the user accesses a target app. The user then taps his or her account credentials into the fake overlay, which allows the malware to steal the data. BankBot Anubis streamlines this process."

Cyber criminals transferring applications into Google play store influence it to resemble a live authentic one; they compromise the clients by controlling them to trust that they are giving an "expertise" as a service. The researchers likewise found that these malignant play store applications that acted like the authentic ones, for the most part focus on the Turkish-speaking clients and the downloader applications in this specific crusade were intended to address Turkish clients just with a couple of various botnets and configurations. All these applications

are transferred to various categories, for example, online shopping to money related services and even an automotive app.

As indicated by an analysis by the X-Force, the adjustments in the downloader application propose that it is being kept up on a progressing premise, another sign that it is a ware offered to cybercriminals or a particular gathering that is centered on swindling particularly the Turkish mobile banking users.

Once the noxious downloader is effectively installed into the victim's Android then the app brings BankBot Anubis from one of its C&C servers. The BankBot Anubis malware forces clients to concede the consent by acting like an application called "Google Protect." This accessibility will go about as a keylogger getting the infected user's credentials from infected users mobile.

BankBot Anubis is known to target users in numerous nations also for example, Australia, Austria, Azerbaijan, Belarus, Brazil, Canada, China, Czech Republic, France, Georgia, Germany, Hong Kong, India, Ireland, Israel, Japan Kazakhstan, Spain, Taiwan, Turkey, U.K. as well as U.S.

Source: http://www.ehackingnews.com/2018/07/anubis-malware-re-emerges-yet-again.html

4. Using a DVR? Passwords of over 30,000 devices exposed in search engine

Tens of thousands of login passwords of DVRs from a Chinese maker have been reported compromised, after a security researcher found these credentials indexed in a search engine.

Ankit Anubhav, a principal researcher at Newsky Security, a cybersecurity firm for IoT devices, discovered these passwords being cached inside search results on ZoomEye, an IoT search engine. His further investigation into subject elements led him to Dahua DVRs that are running an outdated firmware, making them vulnerable to a flaw from five years ago.

The vulnerability he profiled was the CVE-2013-6117, a similar vulnerability that security researcher Jake Reynolds first unearthed from his own Dahua DVR back in 2013. It was fixed in the same year but apparently, it persists due to some devices that were not updated.

Source: https://www.ibtimes.co.in/using-dvr-passwords-over-30000-devices-exposed-search-engine-775029

5. Move Over, Ransomware: Why Cybercriminals Are Shifting Their Focus to Cryptojacking

According to the 2018 IBM X-Force Threat Intelligence Index, the frequency and sophistication of malicious cryptocurrency mining, also called "cryptojacking," has increased drastically in the past year. This mining is changing malicious actors' priorities: While they had previously targeted companies' data and financial assets, they are now seeking to extract value from organizations' computing resources. As a result, industries with powerful computers and

relatively weak defenses — such as scientific research institutions and media companies — are suddenly caught in the crosshairs.

5.1. A Brief History of Cryptocurrency Mining

Cryptocurrency mining emerged when bitcoin, the first decentralized cryptocurrency, hit the scene in 2009. The process of mining cryptocurrency requires computationally intensive calculations to verify transactions, and miners are rewarded with cryptocurrency for this labor-intensive work. Since mining is a competitive process, it requires extensive computing power. When bitcoin was first introduced, general-purpose central processing units (CPUs) could be used to mine it. But with each coin mined, the calculations required to mine the next coin become more complicated — demanding more computing power and more time to solve. The mining applications that followed were developed to harness the power of graphics processing units (GPUs) to work more efficiently than mining with CPUs. GPUs are commonly used in enterprise settings, but they are also used for PC gaming, rendering graphics, scientific modeling and a variety of other complex tasks. Today, bitcoin is mined with specialized application-specific integrated circuits (ASICs), which are optimized for the bitcoin algorithm, making general-purpose GPUs much less desirable for this purpose. However, bitcoin is no longer the only valuable cryptocurrency being mined. New cryptocurrencies, such as Ethereum and Monero, are ASIC-resistant and better suited for mining by general-purpose computers. The creators of these cryptocurrencies worried about the centralization of bitcoin mining because of ASICs. Therefore, they created mining algorithms that harness memory capacity and speed. As a result, these new coins can be mined with general-purpose computers — triggering the rapid growth of mining malware across the globe.

5.2. The Difference Between Web- and Host-Based Mining Malware

Current mining malware can be divided into two major groups: web- and host-based malware. Web-based mining malware is hosted on a website and activates when a user browses on an infected page. It is often written in JavaScript and executes as a web application on the local machine. This type of malware typically mines currencies like Monero, which is well-suited for mining via CPUs. Web-based miners are difficult to detect or stop because — while they don't install themselves on local machines — they exploit local machines for their own purposes, unbeknownst to the users. Potential consequences of this type of attack include significant performance degradation, crashes and even overheating for mobile devices, according to ZDNet. Host-based mining malware is a malicious application installed natively on the system, typically by a dropper-type Trojan. Often, the malware is just standard mining software running in a windowless mode in the background. Other times, however, it's more sophisticated. For example, the malware may use process-hollowing techniques to execute itself and then disguise the mining application's process inside a legitimate system process —

making it harder for users and antivirus solutions to identify and remove it. Host-based malware has better access to system resources, including the computer's GPU, making it potentially much more lucrative for cybercriminals. Additionally, the miner can schedule its activity for ideal times — so the user does not feel any performance impact — giving the cryptojacking better longevity on infected machines. One example of host-based cryptojacking was reported in February 2017 when malicious actors breached a popular software download site to infect Apple product updates with mining malware, according to Help Net Security. Apple OSX computers are known for their high-end hardware, making them appealing targets for mining malware.

5.3. New Strategies Mean New Targets

Mining malware represents a relatively new threat to businesses. Unlike ransomware, it exploits hardware resources rather than the value of data. Businesses typically have large internal networks, which translates to heavy processing power. As more companies move to cloud-based storage solutions, ransomware is becoming less effective at generating profit for criminals. Business owners with cloud storage can simply wipe their systems and restore their files from those backups. Attackers slinging mining malware aren't interested in collecting ransom payments. As soon as a miner starts working, its operator can start raking in profits in the form of cryptocurrency. Also, mining malware is much stealthier than ransomware because it doesn't need to alert the user in any way. While ransomware notifies the user of its presence as a way to elicit payment, mining malware can run in the background for months — or even years — before discovery, especially if security professionals aren't actively looking for it. Since mining performance is determined by hardware performance, infecting high-end workstations and desktops is a priority for threat actors. This tactic is bad news for creative and scientific industries that use powerful computers to develop films, animations and games or conduct complex research. These types of organizations are also less likely to have invested in security and more likely to have awareness gaps.

5.4. What Can Companies Do to Limit the Threat of Cryptojacking?

Mining malware poses a serious threat to businesses across all sectors. Computers infected with host-based malware can be further infected with ransomware, spyware and other malicious applications. Organizations should educate their users and security leaders about the threat and take a proactive approach to detect it on enterprise endpoints. Businesses should also invest in anti-malware programs to block known variants of mining malware and implement controls to identify mining activity. A security information and event management (SIEM) tool, for example, can alert security teams to high CPU and GPU usage during nonbusiness hours. Finally, behavioral analytics tools can help analysts identify abnormal

patterns in resource usage with automation. Interested in emerging security threats? Read the latest IBM X-Force Research.

The post Move Over, Ransomware: Why Cybercriminals Are Shifting Their Focus to Cryptojacking appeared first on Security Intelligence.

Source: https://securityintelligence.com/move-over-ransomware-why-cybercriminals-are-shifting-their-focus-to-cryptojacking/

6. Cisco Removes Undocumented Root Password From Bandwidth Monitoring Software

The Cisco Policy Suite is a complex piece of software available in three editions (for Mobile, Wi-Fi, and BNG [Broadband Network Gateways]) that Cisco sells to ISPs and large corporate clients and which lets network administrators set up bandwidth usage policies and subscription plans for customers/employees. The software is designed with network-intrusive features that allow it to keep track of individual users, tier traffic, and enforce access policies.

6.1. Secret password found during internal audits.

The undocumented root password lets an attacker gain access to this very powerful software and enables him to run malicious operations with root-level access. As such, the vulnerability received a rare severity score of 9.8 out of a maximum of 10 on the CVSSv3 scale. Cisco says there are no workarounds or mitigating factors and customers will have to install the patch it issued yesterday to remove the secret password. The fix is included with Cisco Policy Suite 18.2.0 and all prior versions are considered vulnerable. Cisco says it found the undocumented root password during internal security audits and all chances are that it may have been left behind during software debugging tests, as most of these incidents end up being.

6.2. Fifth backdoor feature found in as many months

This is the fifth undocumented password (aka backdoor) that Cisco has removed from its software in the past five months. Cisco removed similar backdoor accounts in software such as the Prime Collaboration Provisioning (PCP), the IOS XE operating system, the Digital Network Architecture (DNA) Center, and the Wide Area Application Services (WAAS) traffic optimizer. Besides CVE-2018-0375, Cisco patched 24 other security issues, including three others that received a classification of "critical" —CVE-2018-0374, CVE-2018-0376, and CVE-2018-0377— all also affecting the same Cisco Policy Suite software, and all providing "unauthenticated access" for remote attackers.

Source: https://csirt.cy/cisco-removes-undocumented-root-password-from-bandwidth-monitoring-software/

7. IoT Robot Vacuum Vulnerabilities Let Hackers Spy on Victims

Researchers have uncovered vulnerabilities in a connected vacuum cleaner lineup that could allow attackers to eavesdrop, perform video surveillance and steal private data from victims. Two vulnerabilities were discovered in Dongguan Diqee 360 vacuum cleaners, which tout Wi-Fi capabilities, a webcam with night vision, and smartphone-controlled navigation controls. These would allow control over the device as well as the ability to intercept data on a home Wi-Fi network.

"Like any other IoT device, these robot vacuum cleaners could be marshaled into a botnet for DDoS attacks, but that's not even the worst-case scenario, at least for owners," Leigh-Anne Galloway, cybersecurity resilience lead at Positive Technologies, said on Thursday.

The first bug (CVE-2018-10987) is a remote code execution issue that resides in the REQUEST_SET_WIFIPASSWD function (UDP command 153) of the vacuum.

"This vulnerability allows attackers to obtain superuser rights on the vacuum, meaning they can control it remotely, viewing video and images, and physically moving the vacuum," Galloway told Threatpost. "It can also be used in a botnet for DDoS attacks or for bitcoin mining."

An attacker can discover the vacuum on the network by obtaining its media access control (MAC) address – a unique identifier assigned for communications at the data link layer of a network. They can then send a specially-crafted user datagram communications protocol (UDP) request, which results in execution of a command with superuser rights on the vacuum. A crafted UDP packet runs "/mnt/skyeye/mode_switch.sh %s" with an attacker controlling the %s variable.

"To succeed, the attacker must authenticate on the device—which is made easier by the fact that many affected devices have the default username and password combination (admin:888888)," researchers said.

A second vulnerability (CVE-2018-10988) would also allow superuser rights, but additionally, could enable crooks to steal unencrypted data, including photos, video and emails, sent from other devices on the same Wi-Fi network. The bug exists in the vacuum's update mechanism – and it is less threatening as it requires attackers to have physical access to the vacuum. Attackers exploiting this bug could create a special script and place it on a microSD card, then insert it into the vacuum. After the card is inserted, the vacuum update system runs firmware files from the upgrade_360 folder with superuser rights, without any digital signature check. The script could run arbitrary code, such as a sniffer, to intercept private data sent over Wi-Fi by other devices.

Positive Technologies told Threatpost it followed responsible disclosure practices, alerting the company on March 15, 2018. Positive Technologies also submitted the vulnerabilities officially (CVE-2018-10987 and CVE-2018-10987).

"Positive Technologies does not have any information about whether or not the vulnerabilities have been fixed to date," the company told Threatpost.

A spokesperson with Chinese supplier Dongguan Diqee did not specify whether a patch was issued but said end users should change their default usernames and passwords.

"[It's a] default username and password problem, users can bind the device once they receive it and modify the password immediately after binding [is] completed and prevent others from listening with the default username and password," the spokesperson said. "After modification, the default username and password are not effective."

A similar incident occurred last year, when researchers discovered that LG's Hom-Bot IoT vacuum cleaner lineup was open to a hack that would let an attacker take control of the devices and their cameras –and give them the ability to live-stream video from inside a home. These vulnerabilities may also affect other IoT devices using the same video modules as Dongguan Diqee 360 vacuum cleaners. Such devices include outdoor surveillance cameras, DVRs, and smart doorbells, researchers said.

"New IoT devices are being created and deployed every day," Galloway told Threatpost. "If these issues continue to go addressed, IoT security will progressively get worse. To address security issues, the industry should create a comprehensive, agreed-upon set of guidelines in cooperation with all parties, from hardware manufacturers to service providers and security experts."

Source: https://threatpost.com/iot-robot-vacuum-vulnerabilities-let-hackers-spy-on-victims/134179/

8. Hackers Breach Russian Bank and Steal $1 Million Due to Outdated Router

A notorious hacker group known as MoneyTaker has stolen roughly $1 million from a Russian bank after breaching its network via an outdated router. The victim of the hack is PIR Bank, which lost at least $920,000 in money it had stored in a corresponding account at the Bank of Russia. Group-IB, a Russian cyber-security firm that was called in to investigate the incident, says that after studying infected workstations and servers at PIR Bank, they collected "irrefutable digital evidence implicating MoneyTaker in the theft." Group-IB are experts in MoneyTaker tactics because they unmasked the group's existence and operations last December when they published a report on their past attacks.

Experts tied the group to thefts at US, UK, and Russian banks and financial institutions going back as far as 2016. According to Group-IB, the MoneyTaker attacks that hit banks were focused on infiltrating inter-banking money transfer and card processing systems such as the First Data STAR Network and the Automated Work Station Client of the Russian Central Bank (AWS CBR) system.

9. How the hack unfolded

This is what happened this time as well, according to Group-IB. Hackers infiltrated PIR Bank's network at the end of May via an outdated router at one of the bank's regional branches.

"The router had tunnels that allowed the attackers to gain direct access to the bank's local network," Group-IB experts said. "This technique is a characteristic of MoneyTaker. This scheme has already been used by this group at least three times while attacking banks with regional branch networks."

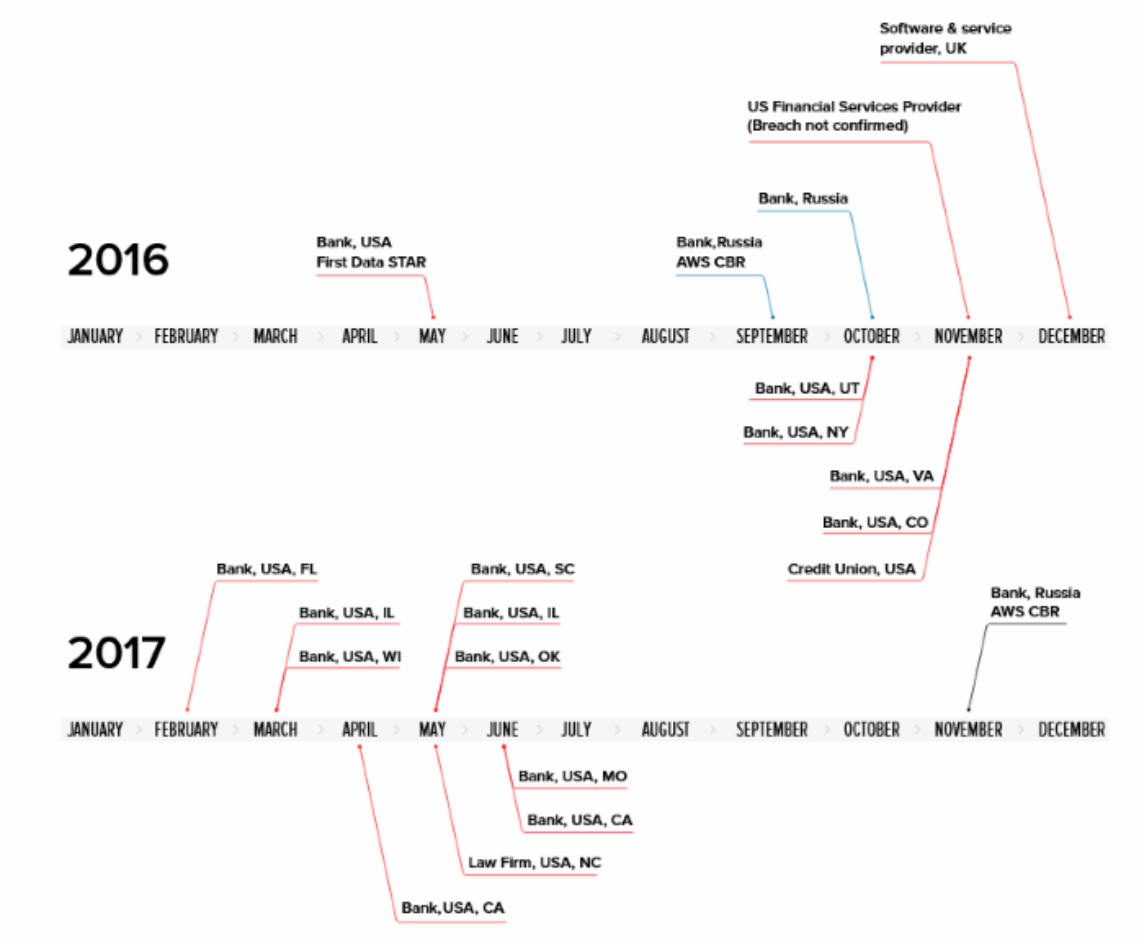
Hackers then used the router to infect the bank's local network with malware. They then used PowerShell scripts to gain persistence and carry out malicious operations without being detected. When, finally, the hackers breached PIR Bank's main network, they also gained access to its AWS CBR account, the system they needed to control financial transactions. On July 3, MoneyTaker used this system to transfer funds from PIR Bank's account at the Bank of Russia to 17 accounts they created in advance. Moments after the stolen funds landed in these accounts, money mules withdrew it from ATMs across Russia. PIR Bank employees discovered the hack a day later, on July 4, but by that moment it was already too late to reverse transactions. In typical MoneyTaker fashion, hackers tried clearing logs from infected computers in order to hide their tracks, but Group-IB said they found reverse shells the group used to access compromised computers.

9.1. Not the first MoneyTaker hack in Russia this year

"This is not the first successful attack on a Russian bank with money withdrawal since early 2018," says Valeriy Baulin, Head of Digital Forensics Lab Group-IB. "We know of at least three similar incidents, but we cannot disclose any details before our investigations are completed."

Group-IB says that at least two of these 2018 hacks of Russian banks have been carried out by the MoneyTaker group. The group's activities are very hard to track because they tend to use common OS utilities to perform malicious actions instead of relying on actual malware. They also clear logs and study each bank's network and system in advance, even stealing documentation to understand with what they're dealing with. During its three-year lifespan, it is believed the group stole tens of millions from banks since they started their hacking spree back in 2016. Group-IB says the average losses are of $500,000 per incident in the US and around $1.2 million per incident in Russia.

Past MoneyTaker hacks include 15 US banks, a US services provider, a UK banking software company, 5 Russian banks, and one Russian law firm. Below is a chart of past MoneyTaker hacks, last updated December 2017.



Source: *https://www.bleepingcomputer.com/news/security/hackers-breach-russian-bank-and-steal-1-million-due-to-outdated-router/*

10. Droppers Is How Android Malware Keeps Sneaking into the Play Store

For the past year, Android malware authors have been increasingly relying on a solid trick for bypassing Google's security scans and sneaking malicious apps into the official Play Store. The trick relies on the use of a technique that's quite common in desktop-based malware, but which in the last year is also becoming popular on the Android market. The technique involves the usage of "droppers," a term denoting a dual or multiple-stage infection process in which the first stage malware is often a simplistic threat with limited capabilities, and its main role is to gain a foothold on a device in order to download more potent threats.

10.1. Droppers are very effective on the mobile scene

But while on desktop environments droppers aren't particularly efficient, as the widespread use of antivirus software detects them and their second-stage payloads, the technique is quite

effective on the mobile scene. This is because most mobile phones don't use an antivirus, and there's no on-device threat scanner to catch the second-stage payloads. This means that the only security measures that are in place are the security scans that Google runs before approving an app to be listed on the Play Store.

Malware authors have realized in the past years that Google has a very hard time picking up "droppers" hidden in legitimate apps. For the past years, more and more malware operations have adopted this trick of splitting their code in two —a dropper and the actual malware. The reason is that droppers require a smaller number of permissions and exhibit limited behavior that could be classified as malicious. Furthermore, adding timers that delay the execution of any malicious code with a few hours also helps the malware remain undetected during Google's scans. These simple tricks allow tiny pieces of malicious code to slip inside the Play Store hidden in all sorts of apps, of many categories.

Once users run the apps, which in most cases do what they advertise, the malicious code executes, the droppers asks for various permissions, and if it gets them, then it downloads a far more potent malware.

10.2. Dropper use aided mobile banking trojans the most

The trick has been used predominantly by malware authors spreading versions of the Exobot, LokiBot, and BankBot mobile banking trojan but has also been adopted in the meantime by many others. Security researchers from ThreatFabric have blogged about the increased usage, popularity, and efficiency of dropper apps on the Play Store in May 2017, August 2017, September 2017, November 2017, and January 2018, describing attacks with Android banking malware strains such as BankBot (Anubis I), BankBot (Anubis II), Red Alert 2.0/2.1, LokiBot, and Exobot. Symantec and ESET have warned about this in the past as well.

This month, the technique was once more highlighted in an IBM X-Force report describing a recent distribution campaign for the Anubis II malware, one of the most recent BankBot variants.

"The campaign features at least 10 malicious downloaders disguised as various applications, all of which fetch mobile banking Trojans that run on Android-based devices," the IBM team said. "While the number of downloaders may seem modest, each of those apps can fetch more than 1,000 samples from the criminal’s command-and-control (C&C) servers."

10.3. DaaS — Downloader-as-a-Service

This recent trend of using similar-looking malware dropper apps (also referred to as malware downloaders) has led IBM experts to believe that some cybercrime gangs are now running a "downloader-as-a-service" (DaaS) operation, in which they are renting "install space" on their dropper apps to other multiple groups at the same time.

This explains why most droppers look the same and sometimes distribute a wide variety of payloads, and not just one malware alone. In fact, this is exactly what appears to be happening, according to Gaetan van Diemen, a security researcher with ThreatFabric, who shared his knowledge with Bleeping Computer earlier today and confirmed IBM's theory of DaaS services being available for Android malware operators.

"In the Android banking malware ecosystem, it is quite common for threat actors to buy so called 'loader' (dropper) services from other actors," van Diemen says.

"The reason for this MO to become more popular is because it allows a wider distribution of the malware from a 'trusted' source (the Google Play Store) and therefore attains a larger number of victims. This resulted in a new business model where installations in google play are sold to malware actors."

10.4. Mobile malware devs just mimicking the desktop market

In hindsight, this isn't that surprising because this is exactly what's happening on the desktop market where running a dropper operation for other criminal groups is a much more financially viable business than running an actual banking trojan. For example, this week Symantec released a report highlighting how the infamous and very dangerous Emotet banking trojan has slowly turned into a dropper and is now renting space and distributing other banking trojans with which it once used to compete.

10.5. Google's uphill battle

The growing popularity of malicious Android dropper apps is also one of the reasons Google has launched the Play Protect service, a security feature built into the official Play Store app that continuously scans locally installed apps for malicious behavior in the hopes of finding malicious modifications in local apps it did not pick up during the Play Store approval process. But van Diemen believes Google is at a disadvantage, at least, for now.

"It is quite difficult to detect dropper apps," the expert told us. "As you can imagine threat actors will put a lot of energy in keeping those apps undetected."

"For example, some dropper apps' malicious code only becomes active when it receives a command from the C&C server (meaning that without a certain delay or certain actions, the behavior of the app will seem benign). In some cases, the malicious banking malware is only dropped based on a certain delay or when the dropper app (for example a game) is intensively used on the device."

Such techniques seem simple enough but are somewhat hard to replicate and detect inside automated testing environments. It is hard to simulate an app's intensive use at the large-scale Google needs to check and re-check the millions of apps uploaded on the Play Store. But van

Diemen points out that Google could look and factor in additional indicators of malicious activity when performing its scans.

"What is surprising is that there is quite some intelligence and technical information about those droppers (publicly) available that could allow Google to detect these apps with ease," van Diemen told Bleeping Computer. "The Exobot campaign for example still uses a similar dropper app code than the first time it was found, in this case, we can even confirm that it is the same dropper panel still being used. Such information should have been used by Google's internal malware scanner (Bouncer) or Google Play Protect."

"Interestingly enough, we have also observed that most AV's also failed in detecting the dropper campaigns (sometimes for years), meaning that some awareness needs to be raised on the topic," the expert added.

Source: *https://www.bleepingcomputer.com/news/security/droppers-is-how-android-malware-keeps-sneaking-into-the-play-store/*

11. The evolution of email fraud: Risks and protection tips

Email fraud creates substantial risk for any organization – the FBI just reported, for instance, that Business Email Compromise has cost organizations more than $12 billion since October 2013. Despite all efforts, there's no way to be 100% secure against this threat.

The most overlooked aspect of this, however, is probably the relationship of account compromise and email fraud. While spoofing and other more explicit forms of fraud that take advantage of email's structure and inherent openness are a challenge, fraud that is executed through account compromise (either from phishing or a data breach) is maybe an overlooked "side business" within the email fraud landscape. In this situation, users are being impersonated from within their own accounts because a bad actor has gained access to it, allowing them to impersonate them and their level of authority in an organization with near-impunity.

What can organizations do today to make sure the risk of BEC scams is reduced?

There's a lot of things that make BEC attacks effective, but there are probably two aspects which most stand out: inattention and lack of awareness. See, most of the time, users are hurried, what to get through with their day, or are simply so overloaded that they don't stop and think about whether a payment request or other email is fraudulent or not. When you combine this with the fact that most users also don't know about email fraud threats or what they should be looking for to identify them, it's easy to see why when such a targeted attack makes it to a user's inbox it can be so effective.

In trying to prevent BEC scams, the main focus of any organization should be threefold: create awareness among your users, establish safe best practices, and deploy the proper protection. Education on what a BEC scam looks like and some of the tactics commonly

deployed (e.g. trying to get wire transfers in a hurry, using familiar phrases or fake invoices) can allow users to think twice when presented with a real scam. Explaining how the FROM field in email works, and how to identify a fraudulent sender address is another great piece of knowledge that can keep users from falling for BEC attacks.

Safe best practices are crucial, but sometimes organizations may not put enough emphasis on them. On the most basic level, no personal email should be used for business transactions (you'd be surprised how often this happens), and any transaction made through email should be verified by a trusty phone call – as long as you can make sure that the person you're talking to is who they say they are!

Finally, a solution that identifies and quarantines fraudulent email is essential to preventing most BEC attacks. Your users should be able to identify these emails, but it shouldn't consumer their time trying to figure out what email is authentic and what isn't. Deploying the proper protection, which programmatically filters the hallmarks of BEC attacks (like phony FROM addresses) and identifies tactics used in previous attacks significantly diminishes the risk to users while also saving them time, and further allowing your awareness and best practices programs to function as a "last line of defense", rather than something you need to rely on daily.

11.1. How can a newly appointed CISO effectively reduce the threat of email fraud?

Whether it's a Fortune 500 CISO or simply an IT Director at a 500-employee company, your own awareness of threats and the ability to prioritize your efforts around them is of the utmost importance. We already know that more than 90% of threats start with a phishing email, and hosted malware, ransomware, and fraud directed through email are all on a rapid rise because they're just so lucrative to cyber criminals. Understanding where most of your risks are – and that most of your threats are motivated by the search for easy profits – gives you the ability to anticipate what threats you'll face going forward. If that's email, then email protection and cloud security may be your first issues to address, if it's malicious files or network compromise, then that's what you'll need to protect against.

Then, as your effectiveness increases, and your priorities evolve, try to look at best practices from other businesses. Learn about their past stories so it will not become one of yours, and if you are ever faced with a crisis, don't be afraid to temporarily block some services (server ports, traffic, even USB ports) when something occurs to allow for proper investigation of a threat. Often, 30 minutes of downtime is better than a full week of recovering.

Finally, if you're in the position of addressing email fraud, take the same steps that we'd recommend against BEC. Create awareness, establish safe best practices, and get the right protection. The larger your organization is, the more threats you might face, so vendors and partners with a large breadth of experience and a detail-oriented understanding of threat

vectors should give you confidence in the solutions they provide. Your ability to take a collaborative, client-based approach to your security should better suit you all the more.

11.2. How do you expect email threats to evolve in the next five years? What should CISOs pay special attention to?

In the same way that account compromise is an overlooked risk with BEC, the compromise of email accounts could pose a subtle but systemic risk not just to organizations but users in both a professional and personal circumstance. The spread of virtual assistants, connected devices, the Internet of Things and more all mean that the amount of daily functions and data spread out over multiple devices is growing exponentially – and they're all often authenticated by the same combination of an email and password.

Vendors in these spaces may be taking steps to make this more secure, but while account compromise can represent access to these devices and services, these devices and services could also then represent points of access to networks, whether they're corporate, public or otherwise.

Source: *https://irishinfosecnews.wordpress.com/2018/07/24/the-evolution-of-email-fraud-risks-and-protection-tips/*

12. DDoS attacks in Q2 2018

Q2 2018 news includes: non-standard use of old vulnerabilities, new botnets, the cutthroat world of cryptocurrencies, a high-profile DDoS attack (or not) with a political subtext, the slashdot effect, some half-baked attempts at activism, and a handful arrests. But first things first.

Knowing what we know about the devastating consequences of DDoS attacks, we are not inclined to celebrate when our predictions come true. Alas, our forecast in the previous quarter's report was confirmed: cybercriminals continue to seek out new non-standard amplification methods. Even before the panic over the recent wave of Memcached-based attacks had subsided, experts discovered an amplification method using another vulnerability—in the Universal Plug and Play protocol, known since 2001. It allows garbage traffic to be sent from several ports instead of just one, switching them randomly, which hinders the blocking process. Experts reported two attacks (April 11 and 26) in which this method was likely used; in the first instance, the DNS attack was amplified through UPnP, and in the second the same was applied to an NTP attack. In addition, the Kaspersky DDoS Protection team observed an attack that exploited a vulnerability in the CHARGEN protocol. A slightly weaker attack using the same protocol to amplify the flood (among other methods) targeted the provider ProtonMail, the reason for which was an unflattering comment made by the company's executive director.

New botnets are causing more headaches for cybersecurity specialists. A noteworthy case is the creation of a botnet formed from 50,000 surveillance cameras in Japan. And a serious danger is posed by a new strain of the Hide-n-Seek malware, which was the first of all known bots to withstand, under certain circumstances, a reboot of the device on which it had set up shop. True, this botnet has not yet been used to carry out DDoS attacks, but experts do not rule out such functionality being added at a later stage, since the options for monetizing the botnet are not that many.

One of the most popular monetization methods remains attacking cryptocurrency sites and exchanges. What's more, DDoS attacks are used not only to prevent competitors from increasing their investors, but as a way of making a big scoop. The incident with the cryptocurrency Verge is a case in point: in late May, a hacker attacked Verge mining pools, and made off with XVG 35 million ($1.7 million). In the space of two months, the currency was hacked twice, although the preceding attack was not a DDoS. Not only that, June 5 saw cybercriminals bring down the Bitfinex cryptocurrency exchange, with the system crash followed by a wave of garbage traffic, pointing to a multistage attack that was likely intended to undermine credibility in the site. It was probably competitive rivalry that caused the renowned online poker site, Americas Cardroom, to suffer a DDoS attack that forced first the interruption and then cancellation of a tournament. That said, it was rumored that the attack could have been a political protest against the in-game availability of Donald Trump and Kim Jong Un avatars.

As always, the most media hype in the past quarter was generated by politically motivated DDoS attacks. In mid-April, British and US law enforcement bodies warned that a significant number of devices had been seized by Russian (supposedly Kremlin-sponsored) hackers in the US, the EU, and Australia with a view to carrying out future attacks. Then just a few days later, in late April, it was a Russian target that got hit: the site of the largest Russian political party, United Russia, was down for two whole days, yet there was precious little public speculation about the masterminds behind the DDoS campaign. An attack on the Danish railway company DSB, which struggled to serve passengers for several days as a result, was also alleged to be politically motivated. Some see it as a continuation of the attack on Swedish infrastructure last fall.

At the end of the quarter, attention was focused on the Mexican elections and an attack on an opposition party website hosting material about the illegal activities of a rival. According to the victim, the attack began during a pre-election debate when the party's candidate showed viewers a poster with the website address. However, it was immediately rumored that DDoS was not the culprit, but the Slashdot effect, which Reddit users also call "the hug of death." This phenomenon has been around since the dawn of the Internet, when bandwidth was a major issue. But it's still encountered to this day when a small resource suffers a major influx of legitimate web traffic on the back of media hype.

The Slashdot effect was also observed by the Kaspersky DDoS Protection team in early summer. After a press conference by the Russian president, a major news outlet covering the

event experienced a powerful wave of tens of thousands of HTTP GET requests all sent simultaneously. The size of the supposed botnet suggested a new round of attacks involving IoT devices, but further analysis by KDP experts showed that all suspicious queries in the User Agent HTTP header contained the substring "XiaoMi MiuiBrowser". In fact, owners of Xiaomi phones with the browser app installed received a push notification about the outcome of the conference, and it seems that many took an interest and followed the link, causing a glut of requests.

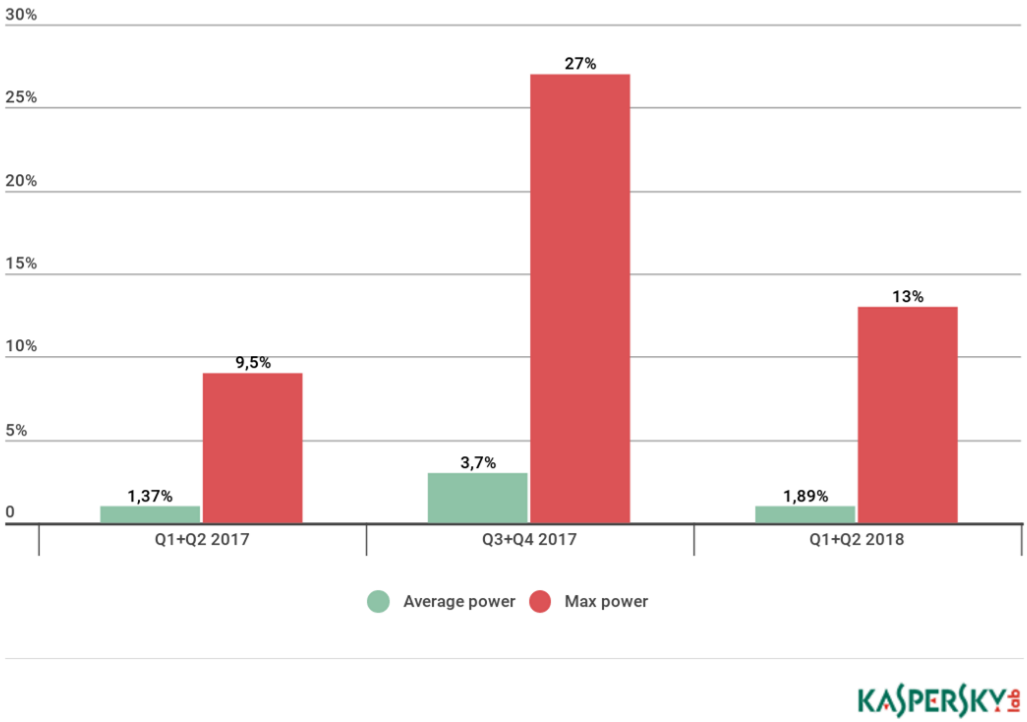
Meanwhile, law enforcement agencies have been making every effort to prevent organized attacks: in late April, Europol managed to shut down Webstresser.org, the world's largest DDoS-for-hire service. When it was finally blocked, the portal had more than 136,000 users and had served as the source of more than 4 million DDoS attacks in recent years. After the fall of Webstresser, conflicting trends were reported: some companies observed a significant decline in DDoS activity in Europe (although they warned that the drop was going to be relatively short-lived); others, however, pointed to a rise in the number of attacks across all regions, which may have been the result of attackers seeking to compensate by creating new botnets and expanding old ones.

On top of that, several DDoS attack masterminds were caught and convicted. German hacker ZZboot was sentenced for attacking major German and British firms with ransom demands. However, he avoided jail time, receiving 22 months of probation. At the other end of the Eurasian continent, in Taipei, a hacker named Chung was arrested for allegedly attacking the Taiwan Bureau of Investigation, the Presidential Administration, Chungwa Telecom, and the Central Bank. In the other direction, across the pond, a self-proclaimed hacktivist was arrested in the US for obstructing the work of police in Ohio.

Another, less significant, but more curious arrest took place in the US: an amateur hacker from Arizona was arrested, fined, and jailed after an online acquaintance posted a tweet with his name. Despite his rudimentary skills, the cybercriminal, calling himself the "Bitcoin Baron," had terrorized US towns for several years, crashing the websites of official institutions and demanding ransoms; in one incident, his actions seriously hindered emergency response services. He too tried to position himself as a cyberactivist, but his bad behavior ruined any reputation he might have had, especially his alleged (only by himself, it should be said) attempt to bring down the site of a children's hospital by flooding it with child pornography.

12.1. Quarter trends

In H1 2018, the average and maximum attack power fell significantly compared to H2 2017. This can be explained by the seasonal slowdown that is usually observed at the start of the year. However, a comparison of H1 indicators for 2017 and 2018 shows a measurable rise in attack power since last year.



Change in DDoS attack power, 2017-2018

One way to increase the attack power is third-party amplification. As mentioned in the news overview, hackers continue to look for ways to amplify DDoS attacks through new (or well-forgotten old) vulnerabilities in widely popular software, not without success, unfortunately. This time, the KDP team detected and repelled an attack with a capacity in the tens of Gbit/s that exploited a vulnerability in the CHARGEN protocol—an old and very simple protocol described in RFC 864 way back in 1983. CHARGEN was intended for testing and measurement purposes and can listen on both the TCP and UDP sockets. In UDP mode, the CHARGEN server responds to any request with a packet with a string length from 0 to 512 random ASCII characters. Attackers use this mechanism to send requests to the vulnerable CHARGEN server, where the outgoing address is substituted by the address of the victim. US-CERT estimates the amplification factor at 358.8x, but this figure is somewhat arbitrary since the responses are generated randomly.

Despite the protocol's age and limited scope, many open CHARGEN servers can be found on the Internet. They are mainly printers and copying devices in which the network service is enabled by default in the software. The use of CHARGEN in UDP attacks, as reported by KDP and other providers (Radware, Nexusguard), may indicate that attacks using more convenient protocols (for example, DNS or NTP) are becoming less effective, since there exist well-developed methods to combat this kind of UDP flooding. But the simplicity of such attacks makes cybercriminals unwilling to abandon them; instead they hope that modern security systems will not be able to resist antiquated methods. And although the search for non-standard holes will doubtless continue, CHARGEN-type amplification attacks are unlikely to

take the world by storm, since vulnerable servers lack a source of replenishment (how often are old copiers connected to the Internet?).

If cybercriminals are going retro in terms of methods, when it comes to targets they are breaking new ground. DDoS attacks against home users are simple, but not profitable, whereas attacks on corporations are profitable, but complex. Now DDoS planners have found a way to get the best of both worlds—in the shape of the online games industry and streamers. Let's take as an example the growing popularity of e-sports tournaments, in which the victors walk away with tens—sometimes hundreds—of thousands of dollars. The largest events are usually held at special venues with specially setup screens and stands for spectators, but the qualifying rounds to get there often involve playing from home. In this case, a well-planned DDoS attack against a team can easily knock it out of the tournament at an early stage. The tournament server might also be targeted, and the threat of disruption could persuade the competition organizers to pay the ransom. According to Kaspersky Lab client data, DDoS attacks on e-sports players and sites with the goal of denying access are becoming increasingly common.

Similarly, cybercriminals are trying to monetize the market of video game streaming channels. Streaming pros show live playthroughs of popular games, and viewers donate small sums to support them. Naturally, the larger the audience, the more money the streamer gets for each broadcast; top players can earn hundreds or thousands of dollars, which basically makes it their job. Competition in this segment is fierce and made worse by DDoS attacks with the capacity to interfere with livestreams, causing subscribers to look for alternatives. Like e-sports players, home streamers have virtually no means of protection against DDoS attacks. They are essentially reliant on their Internet provider. The only solution at present could be to set up specialized platforms offering greater protection.

12.2. Methodology

Kaspersky Lab has extensive experience of combating cyber threats, including DDoS attacks of all types and complexity. Company experts monitor the actions of botnets using the Kaspersky DDoS Intelligence system. The DDoS Intelligence system is part of the Kaspersky DDoS Protection solution and intercepts and analyzes commands sent to bots from C&C servers. What's more, the system is proactive, not reactive—there's no need to wait for a user device to get infected or a command to be executed. This report contains DDoS Intelligence statistics for Q2 2018.

In the context of this report, it is assumed that an incident is a separate (single) DDoS-attack if the interval between botnet activity periods does not exceed 24 hours. For example, if the same web resource was attacked by the same botnet with an interval of 24 hours or more, then this incident is considered as two attacks. Bot requests originating from different botnets but directed at one resource also count as separate attacks.

The geographical locations of DDoS-attack victims and C&C servers used to send commands are determined by their respective IP addresses. The number of unique targets of

DDoS attacks in this report is counted by the number of unique IP addresses in the quarterly statistics.

DDoS Intelligence statistics are limited to botnets detected and analyzed by Kaspersky Lab. Note that botnets are just one of the tools for performing DDoS attacks, and that the data presented in this report do not cover every single DDoS attack that occurred during the period under review.

12.3. Quarter results

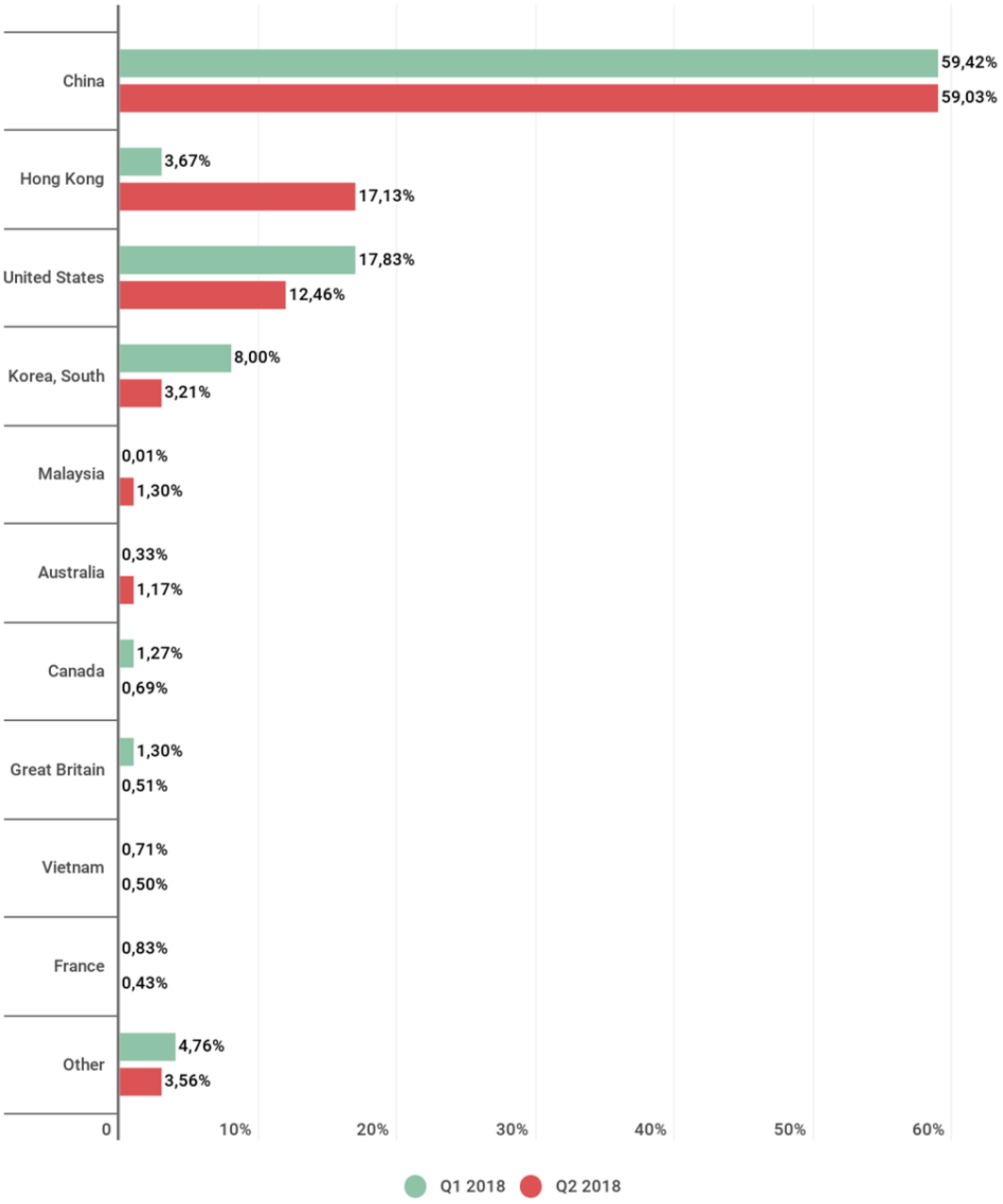
- The stormiest period for DDoS attacks was the start of the quarter, particularly mid-April. By contrast, late May and early June were fairly quiet.
- Top spot in terms of number of attacks was retained by China (59.03%), with Hong Kong (17.13%) in second. It also entered the Top 3 by number of unique targets with 12.88%, behind only China (52.36%) and the US (17.75%).
- The attacks were quite evenly distributed across the days of the week. The most and least popular were Tuesday and Thursday, respectively, but the difference is slight.
- The share of SYN attacks rose sharply to 80.2%; second place went to UDP attacks with 10.6%.
- The share of attacks from Linux botnets increased significantly to 94.47% of all single-family attacks.

12.4. Geography of attacks

The latest quarter threw up several surprises. The leader by number of attacks is still China, with its share practically unchanged (59.03% against 59.42% in Q1). However, for the first time since monitoring began, Hong Kong broke into the Top 3, rising from fourth to second: its share increased almost fivefold, from 3.67% to 17.13%, squeezing out the US (12.46%) and South Korea (3.21%), whose shares declined by roughly 5 p.p. each.

Another surprise package in the territorial ranking was Malaysia, which shot up to fifth place, now accounting for 1.30% of all DDoS attacks. It was joined in the Top 10 by Australia (1.17%) and Vietnam (0.50%), while the big-hitters Japan, Germany, and Russia all dropped out. Britain (0.50%) and Canada (0.69%) moved into eighth and seventh, respectively.

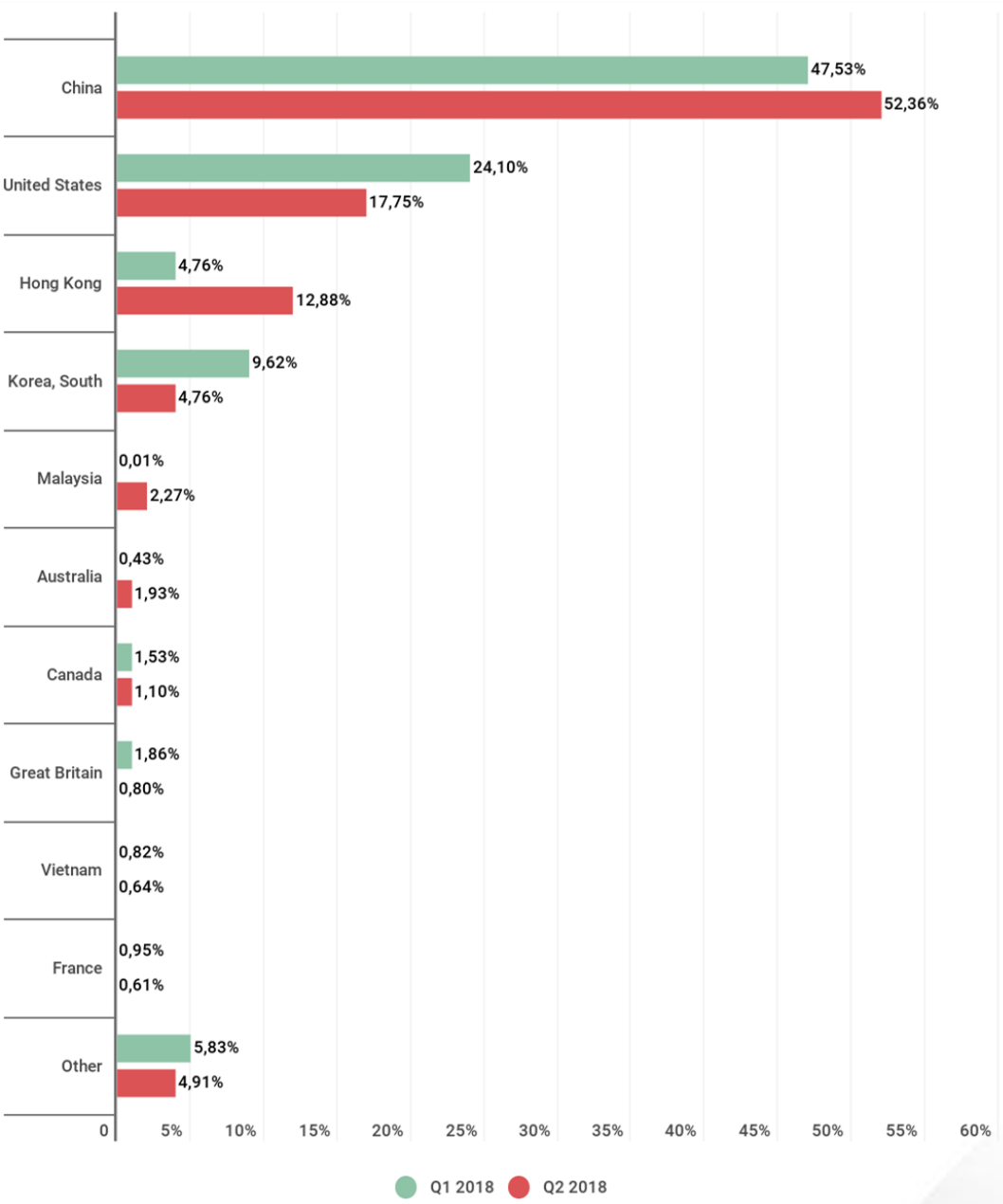
The Top 10 in Q2 also had a greater share of the total number of attacks than in Q1: 96.44% compared with 95.44%.



Distribution of DDoS attacks by country, Q1 and Q2 2018

The territorial distribution of unique targets roughly corresponds to the distribution of the number of attacks: China has the largest share (52.36%), a rise of 5 p.p. against the previous quarter. Second place belongs to the US (17.5%) and third to Hong Kong (12.88%), up from fourth, replacing South Korea (4.76%) (note that in Hong Kong the most popular targets are now Microsoft Azure servers). Britain fell from fourth to eighth, now accounting for 0.8% of unique targets. The Top 10 said goodbye to Japan and Germany but welcomed Malaysia (2.27%) in fourth place and Australia (1.93%) just behind in fifth. This quarter's Top 10

accounted for slightly more of the total number of unique attacks, reaching 95.09% against 94.17% in Q1.



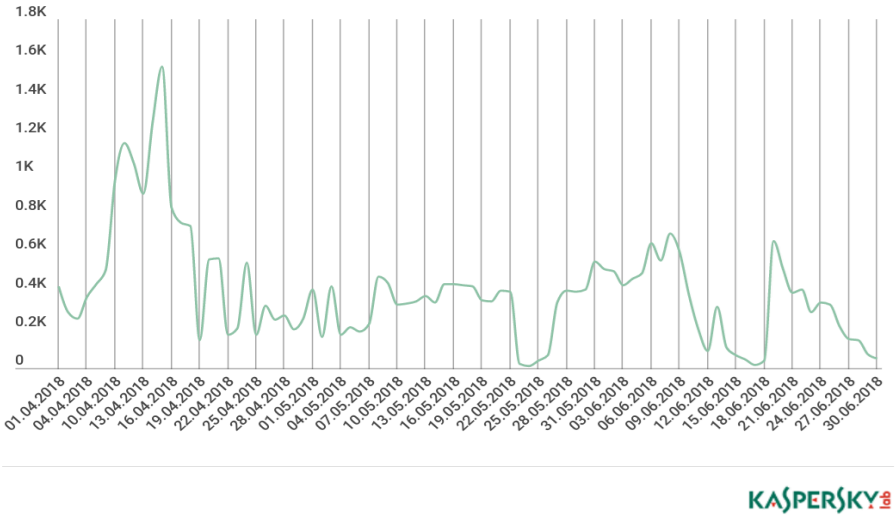
KASPERSKY

Distribution of unique DDoS-attack targets by country, Q1 and Q2 2018

12.5. Dynamics of the number of DDoS attacks

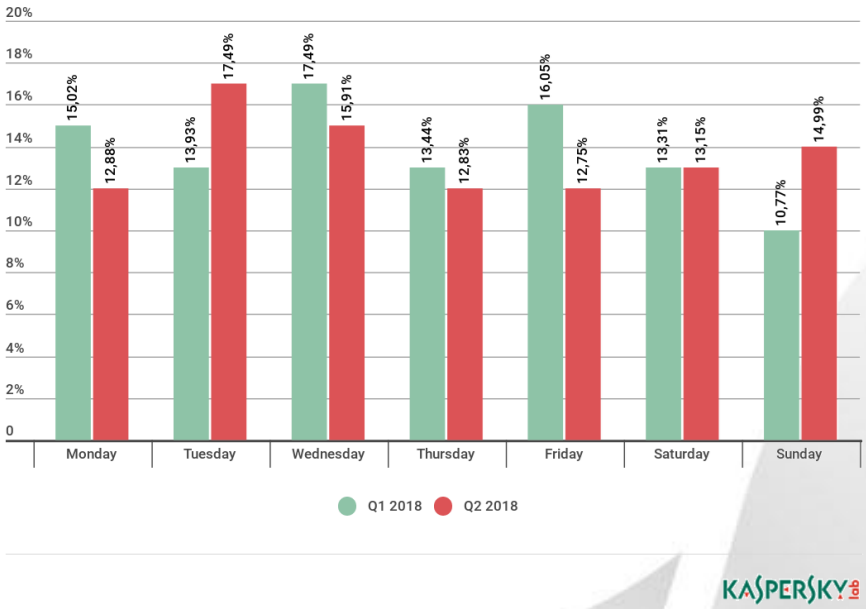
Peak activity in Q2 2018 was observed in mid-April: a significant increase in the number of attacks was registered in the middle third of this month, with two large spikes occurring just

days apart: April 11 (1163) and April 15 (1555). The quarter's deepest troughs came in the second half and at the end: the calmest days were May 24 (13) and June 17 (16).



Dynamics of the number of DDoS attacks, Q2 2018

In Q2 2018, Sunday went from being the quietest day for cybercriminals to the second most active: it accounted for 14.99% of attacks, up from 10.77% in the previous quarter. But gold in terms of number of attacks went to Tuesday, which braved 17.49% of them. Thursday, meanwhile, went in the opposite direction: only 12.75% of attacks were logged on this day. Overall, as can be seen from the graph, in the period April-June the attack distribution over the days of the week was more even than at the beginning of the year.

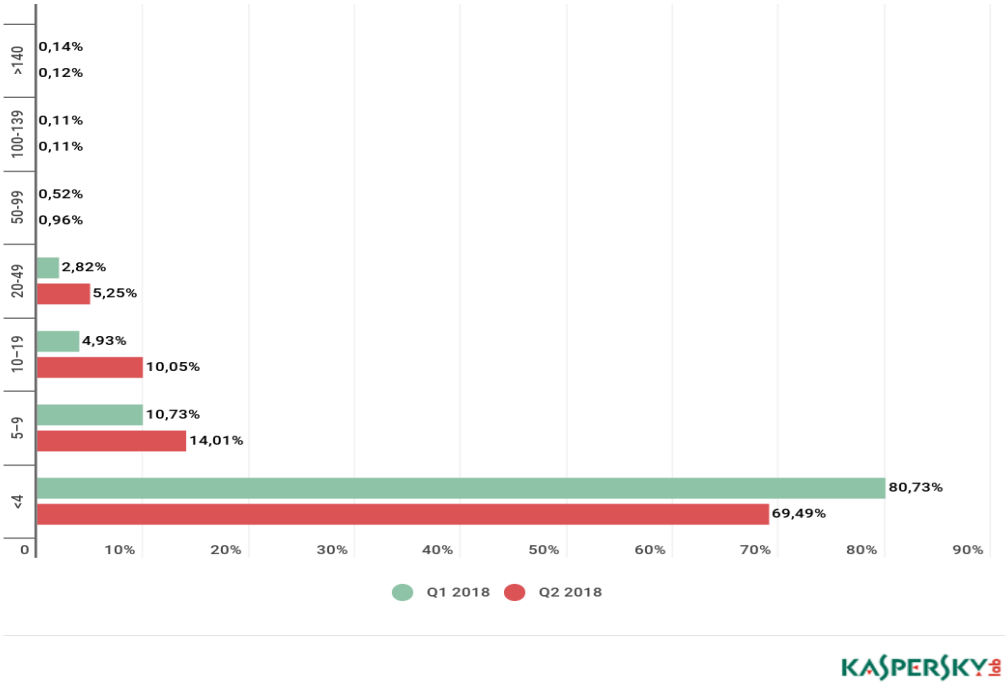


Distribution of DDoS attacks by day of the week, Q1 and Q2 2018

12.6. Duration and types of DDoS attacks

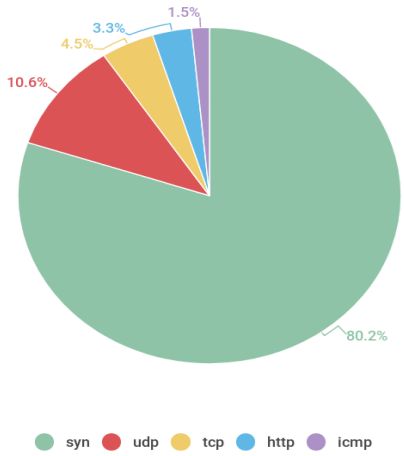
The longest attack in Q2 lasted 258 hours (almost 11 days), slightly short of the previous quarter's record of 297 hours (12.4 days). This time, the focus of persevering hackers was an IP address belonging to China Telecom.

Overall, the share of long-duration attacks fell by 0.02 p.p. to 0.12%. Whereas the share of attacks lasting from 100 to 139 hours remained the same, the share of attacks from 10 to 50 hours almost doubled (from 8.28% to 16.27%); meanwhile, the share of attacks lasting from five to nine hours increased nearly by half (from 10.73% to 14.01%). The share of short-duration attacks (up to four hours) fell sharply from 80.73% in January to 69.49% in March.



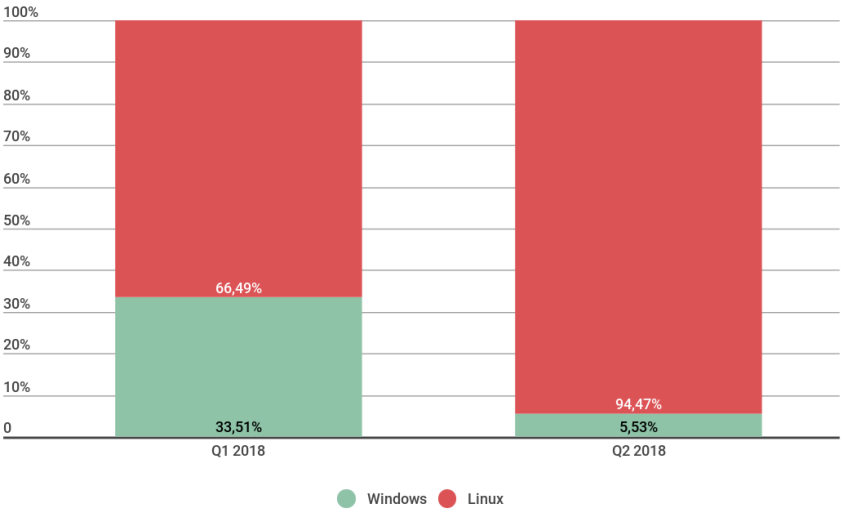
Distribution of DDoS attacks by duration (hours), Q1 and Q2 2018

All other types of attacks decreased in share; UDP attacks are in second place (10.6%), while TCP, HTTP, and ICMP constitute a relatively small proportion.



KASPERSKY

Distribution of DDoS attacks by type, Q2 2018



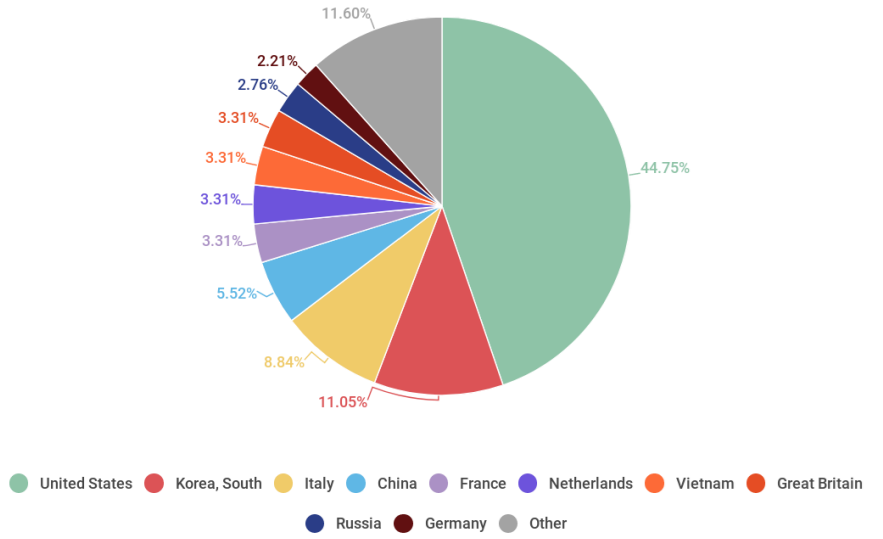
KASPERSKY

Correlation between Windows- and Linux-based botnet attacks, Q2 2018

12.7. Geographical distribution of botnets

The Top 10 regions by number of botnet C&C servers underwent some significant changes. Top spot went to the US with almost half of all C&C centers (44.75% against 29.32% in Q1). South Korea (11.05%) sank from first to second, losing nearly 20 p.p. China also dropped significantly (from 8.0% to 5.52%). Its place was taken by Italy, whose share climbed from 6.83% in the previous quarter to 8.84%. The Top 10 saw the departure of Hong Kong, but was joined—

for the first time since our records began—by Vietnam, whose 3.31% was good enough for seventh place.



Distribution of botnet C&C servers by country, Q2 2018

12.8. Conclusion

In Q2 2018, cybercriminals continued the above-outlined trend of searching for exotic holes in UDP transport protocols. It surely won't be long before we hear about other sophisticated methods of attack amplification.

Another technical discovery of note is the potential for creating botnets using the UPnP protocol; although evidence for them exists, they are still extremely rare in the wild, fortunately.

Windows botnet activity decreased: in particular, Yoyo activity experienced a multifold drop, and Nitol, Drive, and Skill also declined. Meanwhile, Xor for Linux significantly increased its number of attacks, while another infamous Linux botnet, Darkai, scaled back slightly. As a result, the most popular type of attack was SYN flooding.

The total attack duration changed little since the previous quarter, but the share of medium-duration attacks increased, while the share of shorter ones decreased. The intensity of attacks also continues to grow. The most lucrative targets for cybercriminals seem to be cryptocurrencies, but we can soon expect to see high-profile attacks against e-sports tournaments as well as relatively small ransoms targeting individual streamers and players. Accordingly, there will be market demand for affordable individual anti-DDoS protection.

Source: https://securelist.com/ddos-report-in-q2-2018/86537/

13. Quantum Leaps and Bounds: Why Quantum Computing Will Have a Positive Impact on Cybersecurity

Earlier this year, our chief technology officer (CTO) of data security, Walid Rjaibi, outlined his perspective on the risks that quantum computers might pose to cybersecurity, particularly concerning common algorithms used in encryption. He astutely observed, however, that the risks are only one part of the story. Quantum computing also has the potential to revolutionize our cybersecurity capabilities.

13.1. How Will Quantum Computing Enhance Cybersecurity?

According to a new IBM Institute for Business Value (IBV) paper, the two most notable areas of cybersecurity that quantum computing promises to enhance are machine learning and quantum number generation. Machine learning is already a widely used and understood term in the cybersecurity world. We use machine learning capabilities today in security information and event management (SIEM), data protection, incident response and other solutions to improve behavior anomaly detection, classification and prediction capabilities. Given their improved speed and power, quantum computers have the potential to enhance the efficacy of machine learning when used for cybersecurity pursuits.

Random number generation is a key component of cryptography (pun intended). Classical random number generation can be split into two categories: pseudo-random number generators (PRNGs) and true random number generators (TRNGs). TRNGs are more suitable for generating strong encryption keys (you can read more about why in the IBV paper). Quantum random number generators (QRNGs) would be a special subset of TRNGs, which exploit the inherent randomness of quantum physics to generate even more random sequences of numbers, thus stronger encryption keys. Download the complete IBM IBV paper: Preparing Cybersecurity Now for a Quantum World

13.2. Cybersecurity: Why the Sky Isn't Falling

As you may have learned at Think 2018, despite the risks quantum computing may pose to cybersecurity, the sky is not falling. There are many measures organizations can take to safeguard their critical data today and in the future.

For example, doubling the key size of existing symmetric encryption algorithms can help companies prepare for how the cybersecurity landscape may change when large-scale

quantum computers become available. Beyond that, the improvements quantum computing could potentially bring to cybersecurity will also contribute to stronger protection capabilities.

Source: https://securityintelligence.com/quantum-leaps-and-bounds-why-quantum-computing-will-have-a-positive-impact-on-cybersecurity

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