CHECK POINT
RESEARCH

MID-YEAR REPORT

CYBER ATTACK TRENDS

2017

Check Point
SOFTWARE TECHNOLOGIES LTD

TABLE OF CONTENTS

INTRODUCTION

When it comes to the global cyber landscape, this year seems to have picked up where the previous year left off. In 2016, we witnessed sophisticated new malware emerging on a monthly basis, revealing new capabilities, distribution methods, and attack services offered for sale via multiple platforms, such as the infamous Cerber ransomware as-a-service, and the Angler Exploit Kit, which has since ceased operation.

2017 is shedding light on a new trend – simple, yet highly effective malware families are causing rapid destruction globally. The samples are distributed by unknown threat actors, yet wield high-end attack tools and techniques developed by elite nation-state actors. In addition, massive theft operations, such as the infamous Shadow Brokers leak of tools allegedly developed by the U.S. National Security Agency (NSA), have led to some of the world's most sophisticated malware ending up in the hands of unskilled attackers. For the first time ever, we have witnessed a phenomenon such as the 'WannaCry' ransomware affecting public infrastructure as well as medical facilities around the world.

Even with WannaCry and NotPetya making global headlines, most organizations continue to rely on a strategy of detection and response after an attack has occurred as their primary means of defense. Many of these prominent attacks use known malware variants that could have been blocked had the proper security measures been deployed in the first place. Unfortunately, 99% of organizations still have not put in place the fundamental cyber security technologies available to prevent these types of attacks. The bottom line: these threats could have been prevented had the proper security mechanisms been in place.

To provide organizations with the best level of protection, security experts must be attuned to the ever-changing landscape and the latest threats and attack methods to keep their security posture at the highest standard. The Check Point Cyber Attack Trends report provides a comprehensive overview of the malware landscape in the top categories of ransomware, banking and mobile threats, based on threat intelligence data drawn from the ThreatCloud World Cyber Threat Map between January and June 2017.

GLOBAL TRENDS

TREND 1: NATION-STATE CYBER WEAPONS ARE NOW IN THE HANDS OF CRIMINALS

Data leakage incidents have significantly evolved in sophistication, frequency and volume of data being accessed. As seen in several incidents throughout the first half of 2017, the theft and consequent availability of key nation-state hacking tools, combined with wide scale zero-day vulnerabilities, now enable unskilled hackers to carry out highly sophisticated attack campaigns.

KEY INCIDENTS

- **MARCH:** Thousands of documents detailing the CIA's efforts and methodologies for hacking into iPhones, Android devices and Smart TVs, were released.
- **APRIL:** The Shadow Brokers threat group released a dump containing NSA exploits and hacking tools, considered to be the most damaging release yet, due to the number of exploits made available, plus the sophistication and variety of the exploits. The leaked cache, which contains almost 300 megabytes of material, contains tools that target most versions of the Windows operating system, as well as code for hacking into EastNets, the largest SWIFT service provider in the Middle East.
- **MAY:** The WannaCry ransomware was poorly written, was not packed, was not obfuscated, and contained the peculiar 'Kill Switch.' And yet, this malware exhibited extraordinary lateral movement capabilities, based largely on the Shadow Brokers leak and more specifically the EternalBlue exploit for Windows SMB. The leaked code served to upgrade a simple ransomware into one of the most influential global attacks observed in recent years, impacting a large proportion of public and civil facilities.
- **JUNE:** The same NSA capabilities that had been evident in the WannaCry attack were reused in NotPetya – a wide attack focused on Ukrainian organizations that took down entire networks. This incident demonstrated that while threat actors learn from each successful wave of attack, often reuse effective weapons; organizations and individuals continue to ignore these lessons and refuse to implement readily available and effective security measures.

Interestingly, a reversed trend was observed as well – as revealed in the Vault 7 leak. Some of the code used by the CIA to hack into mobile devices was borrowed from ordinary malware. The key takeaway for users is that all cyber threats are related, regardless of where they originate.

TREND 2: THE LINE BETWEEN ADWARE AND MALWARE IS FADING, AND MOBILE ADWARE BOTNETS ARE ON THE RISE

Adware, which automatically displays or downloads advertising material on an infected machine, was until recently not among our greatest concerns, as while sometimes annoying, its sole purpose is to generate revenue and not to cause actual damage. However, what if in recent months, the status quo for operating below the radar of the security community has changed? The Fireball malware, a browser-hijacker that is primarily meant to push advertisements, is also capable of executing any arbitrary code on its victim's machine. This has led to a major change in our approach to adware, especially those owned by massive, seemingly-legitimate organizations. As our research continues, we can point to more and more sophisticated adware families which operate in a similar way.

In parallel, mobile adware botnets continue to expand and dominate the mobile malware arena. In the first half of 2017, we witnessed a persistent rise in the spread and technical capabilities of mobile adware botnets. We began the year by reporting about HummingWhale, the new variant of the infamous HummingBad malware which was prominent in 3rd party app stores last year. The new version managed to not only develop a brand new tactic to steal ad revenues, but also penetrate Google's security and upload dozens of apps to Google Play. Later on, we unraveled Judy, an auto-clicking adware which might be the largest malware infection ever on Google Play. As hundreds of millions of machines worldwide are infected by adware, turning those payloads into potential malware downloaders can generate an even greater income for the companies or actors behind them.

This trend continued to evolve with CopyCat, a mobile malware that infected 14 million Android devices, rooting approximately 8 million of them, and earning the hackers behind the campaign approximately $1.5 million in fake ad revenues in two months. CopyCat uses a novel technique to generate and steal ad revenues. CopyCat is a fully developed malware with vast capabilities, including rooting devices, establishing persistency, and injecting code into Zygote – a daemon responsible for launching apps in the Android operating system – that allows the malware to control any activity on the device.

TREND 3: MACRO-BASED DOWNLOADERS CONTINUE TO EVOLVE

As malware continues to evolve, the same is true for its delivery methods. During the past six months, we have seen some new methods for exploiting Microsoft Office files, which no longer require victims to open the door for the attackers by enabling macros.

KEY INCIDENTS

- **CVE-2017-0199:** In April, we saw a wave of weaponized RTF files delivering many types of malware from ransomware to Remote-Access-Trojans (RATs), using an undisclosed method. The vulnerability consisted of the RTF file downloading an HTA file disguised as another RTF and then executing it via Windows HTA handler. Initially, this vector was reported as a zero-day, which was used only by one malware family. However, the ease with which this vulnerability could be exploited meant that others caught on very quickly and began to use this method in other attacks.
- **HOVER MOUSE:** Most malicious documents rely on executing macros or embedded objects. In June, we encountered a brand new method of exploitation - abusing PowerPoint's Element Definitions. By modifying a slide's XML data, a threat actor can set and alter the actions performed by the different elements in the slide. In this particular scenario, a victim is sent a PowerPoint presentation which displays only a hyperlink. When the user passes the mouse over the hyperlink, a PowerShell script is called, which then downloads and executes the malicious payload.

TREND 4: A NEW WAVE OF MOBILE BANKERS ON GOOGLE PLAY

On top of the large adware campaigns which we have grown accustomed to finding on Google Play, a new wave of mobile bankers, most of which belong to the BankBot family managed to enter the play store undetected and infect users. This is an alarming development as the bankers malware harm users directly, and supposed to be easier to detect. However, the perpetrators combined open-sourced banking malware code with complex obfuscation techniques to successfully and repeatedly bypass Google's protections.

MAJOR CYBER BREACHES

It's an unfortunate reality that cyber attacks are more than a rare occurrence. Recent headlines have demonstrated the agility, scale and persistence of cyber criminals. Moreover, hackers are targeting all geographies. All regions suffered numerous attacks so far in 2017. Here is a recap of the most major and well known attacks in each region.

Americas

- **February 23, 2017:** Researchers found a critical security flaw in the edge servers of the web security company Cloudflare. A buffer overflow bug caused a major leak of sensitive user information from 3,400 websites, including Uber, 1Password, and the online dating site OKCupid.
- **March 7, 2017:** In a leak dubbed "Vault7", WikiLeaks released over 8,000 files and documents, presumably belonging to the Central Intelligence Agency (CIA). These documents contain information about dozens of exploits and vulnerabilities for various platforms, including web browsers, Windows, Android, Apple products, and security products. The leak also contains information about practices and methods allegedly used by the CIA, including an entire division which specializes in masking hacks so that they are blamed on other actors.

- **April 7, 2017:** Unknown hackers breached the emergency siren system of Dallas, Texas, repeatedly activating all of the city's 156 sirens for approximately an hour late Friday night. As the siren system only uses radio communications with no internet connection available, it is assumed that the attack was carried out by radio transmissions
- **April 14, 2017:** The Shadow Brokers group, which had released hacking tools allegedly belonging to the NSA late last year, leaked additional tools, also believed to belong to the NSA, exploiting 0-day vulnerabilities for both Windows and the SWIFT banking system. Following the leak, it was revealed that Microsoft had already patched the vulnerabilities in a little-publicized security update. One month later, on **May 12**, a global attack infected tens of thousands of machines with the WannaCry ransomware using a vulnerability in the Windows OS SMB EternalBlue communication protocol, developed by the NSA and leaked by the group. The victims included hospitals, telecommunication companies, car manufacturers and others.
- **May 11, 2017:** Edmodo, a popular educational technology company based in California, was the victim of a breach. Personal data was stolen from approximately 77 million user accounts belonging to students, parents and teachers. The leaked information includes email addresses, usernames and hashed passwords. It was reported that the hacker offered the data for sale on a dark web forum for $1,000.

Europe, the Middle East and Africa (EMEA)

- **January 7, 2017:** E-Sports Entertainment Association League, a popular video gaming community owned by the Germany-based eSports company Turtle Entertainment GmbH, suffered a breach, revealing gaming servers data and users' personal details. According to researchers, the number of users affected by the breach may have reached 1.5 million.
- **January 12, 2017:** Cellebrite, an Israeli company known for developing mobile forensics and hacking tools, was breached, leading to the theft of 900 GB of customer data. According to its announcement, the breached web server contained basic information of customers registered for alerts and notifications for Cellebrite products, as well as hashed passwords of customers that had not yet migrated to Cellebrite's new end-user license management system.
- **April 9, 2017:** Wonga, a UK-based loan firm, suffered a breach affecting up to 270,000 customers, most of them in the UK. According to Wonga, the leaked data may include e-mail addresses, home addresses, phone numbers, partial credit card numbers and bank account numbers.

Asia-Pacific (APAC)

- **February 13, 2017:** The McDonald's India app, McDelivery, leaked the personal data of over 2.2 million customers, including name, email address, phone number, home address and social profiles. The leak is the result of an unsecured public API. Although McDelivery acknowledged the issue on February 13, as of March 17, the fix had not yet been completed and the app was still leaking customer data.
- **March 14, 2017:** GMO Payment Gateway, the Japanese provider of payment processing services, confirmed that a security flaw in the company's systems running Apache Struts 2 led to the leak of personal and financial data from the websites of two of its clients: the Tokyo metropolitan government and the Japan Housing Finance Agency. The leaked information includes over 100,000 credit card numbers and expiration dates, as well email addresses, phone numbers and dates of birth.
- **April 13, 2017:** Some 500,000 Australian websites were rendered inaccessible for an hour and a half, after the DNS servers of Melbourne IT, an Australian Internet company, and its subsidiaries fell victim to a massive DDoS attack. The attack affected the company's web hosting, email platforms and customer administration portal access.
- **April 24, 2017:** An unknown hacker broke into HipChat, a group chat platform owned by the Australia-based enterprise Atlassian. A significant amount of user account information, which includes names, email addresses and hashed passwords, may have been stolen, as well as chat room metadata. For a fraction of users, messages and chat room content may have been stolen as well.

GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections of this report are based on data drawn from the Check Point ThreatCloud World Cyber Threat Map between January and June 2017. For each malware family, the percentage shown represents its share of recognized malware attacks on organizations worldwide.

TOP MALWARE FAMILIES

In the following graph we present the percentage of organizations globally that were affected by each malware family.

Global

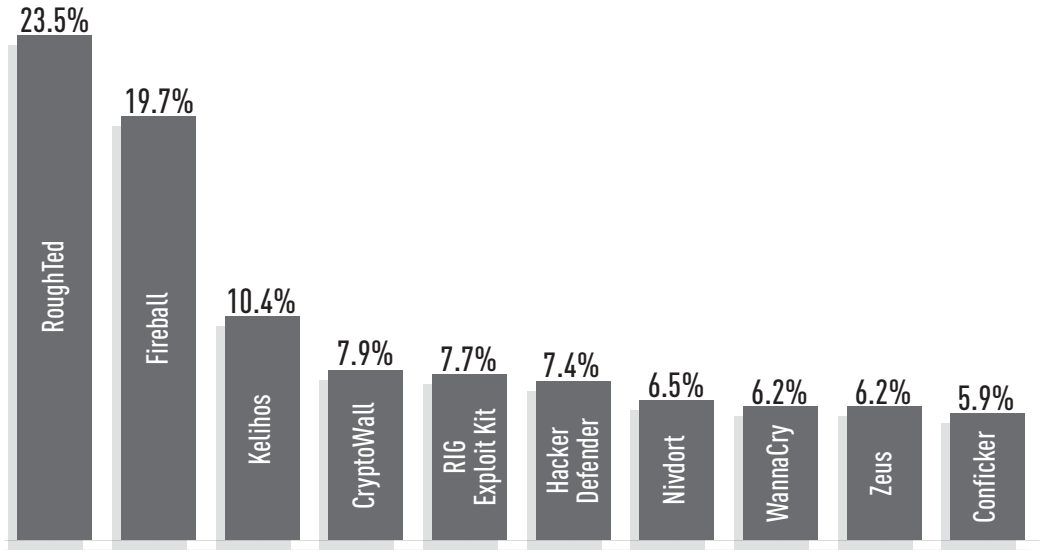

Figure 1: Most Prevalent Malware Globally

For each of the regions below we present two graphs: the first details the most prevalent malware in that region, followed by a second graph that details the malware families with the highest presence in that region compared to the others. For example, RoughTed is prevalent in all regions; however, Winnti is mostly concentrated in the Americas and not throughout the EMEA or APAC. Together, the charts give a holistic view – the targeted malware chart doesn't simply present the malware that are only on the top of the list for one country, it presents malware families that clearly target a specific region – the list is based on a significant difference in the infection rate of the malware in each region.

Americas

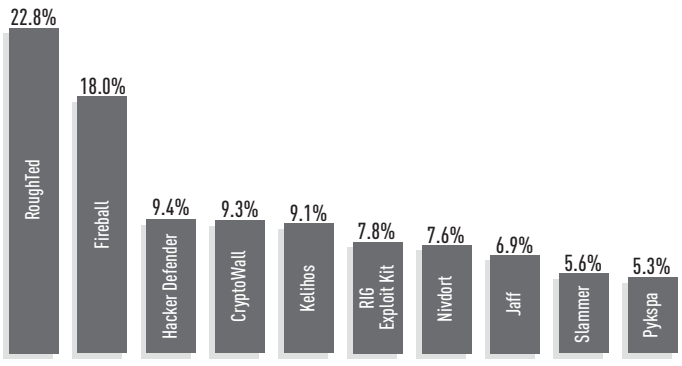

Figure 2: Most Prevalent Malware in the Americas

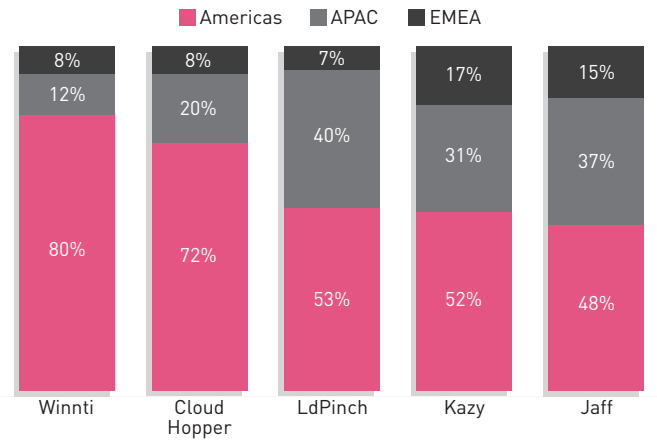

Figure 3: Top Targeted Malware in the Americas

Europe, Middle East and Africa (EMEA)

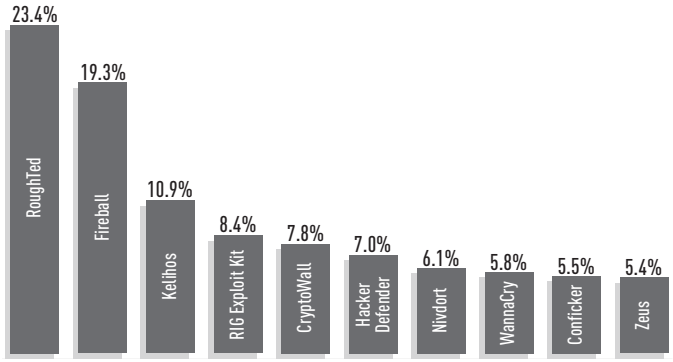

Figure 4: Most Prevalent Malware in EMEA

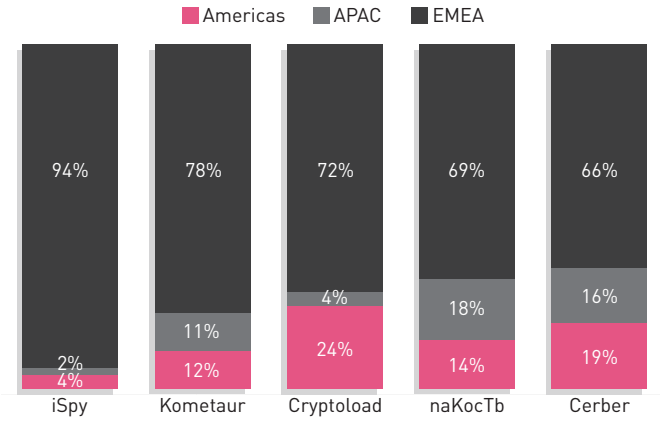

Figure 5: Top Targeted Malware in EMEA

Asia-Pacific

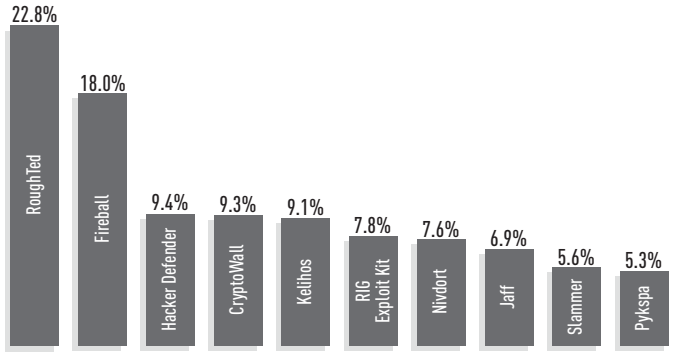

Figure 6: Most Prevalent Malware in APAC

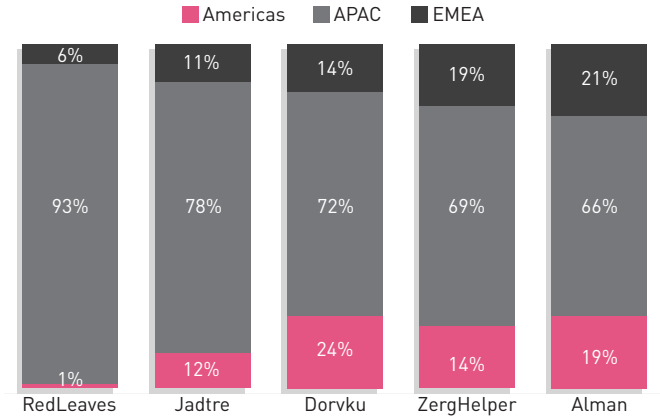

Figure 7: Top Targeted Malware in APAC

Global Analysis of the Top Malware

- Even though the WannaCry attack had a massive Impact all around the globe, the malware did not land on the Americas Top Malware Families rank. The malware's absence from this rank is in line with the fact that most of the major organizations attacked by WannaCry, such as Telefonica, Britain's National Health Service, Nissan Motor Manufacturing UK and PetroChina, are all based in Europe or APAC.
- RoughTed and Fireball start at the top of the rank in all three regions, and accordingly in the global rank as well. As of late May, RoughTed, a massive malvertising campaign, has been used to deliver links to malicious websites and payloads such as adware, exploit kits and ransomware. According to our data, 28% of all organizations globally were affected by the RoughTed campaign during June.
- Conficker, one of the largest and oldest active botnets, made it to the first place of our Global Top Malware Families rank in the first half of 2016 – but a year later, we can see a sharp decline to #10 on our list due to new wide-spread malware, including RoughTed and Fireball, that revealed itself during this period.

TOP RANSOMWARE

Graphs in this section of the report represent the percentage of organizations that were affected by each ransomware. The graphs present a global view and also regional insights into the top ransomware.

Global

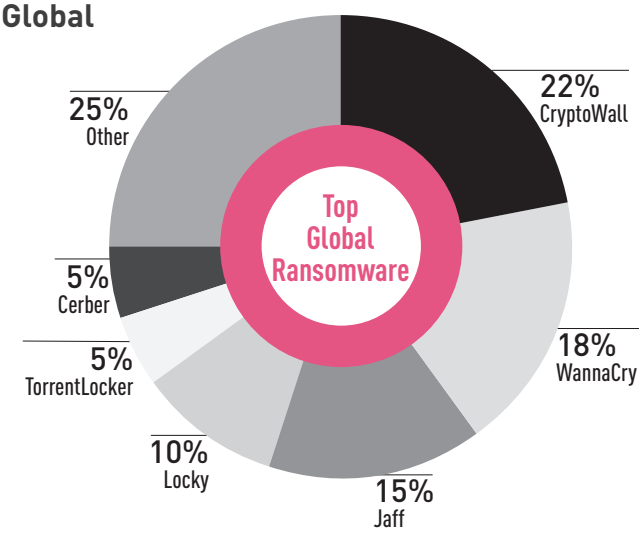

Figure 8: Most Prevalent Ransomware Globally

Americas

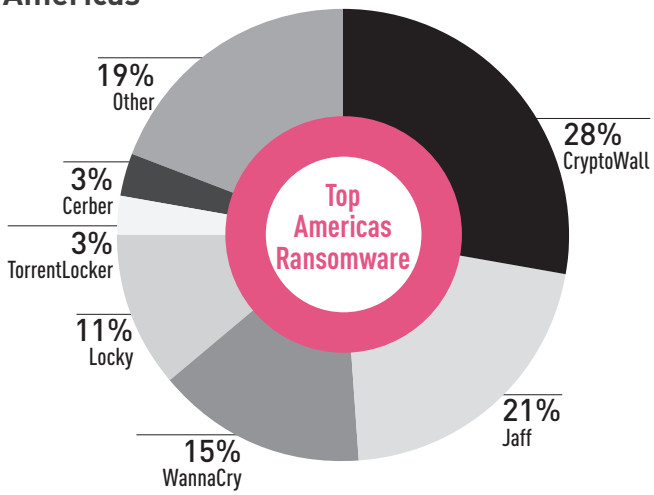

Figure 9: Most Prevalent Ransomware in the Americas

EMEA

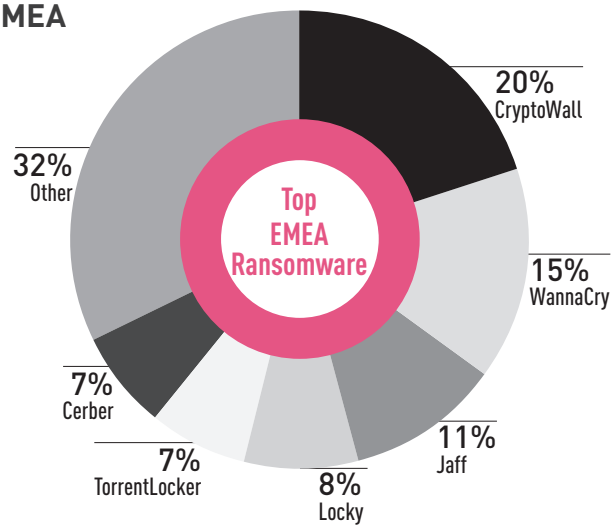

Figure 10: Most Prevalent Ransomware in EMEA

APAC

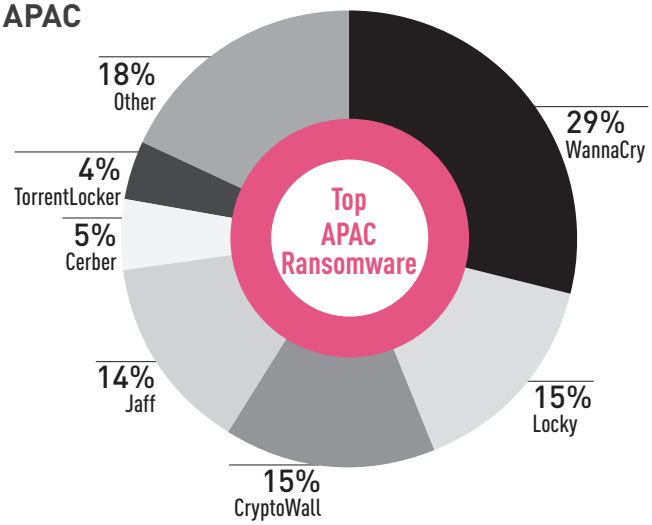

Figure 11: Most Prevalent Ransomware in APAC

Ransomware Global Analysis

- Comparing the first half of 2016 to the first half of 2017, the percentage of attacks out of the top three ransomware in all three regions almost doubled, increasing from an average of 26% to an average of 48%.
- Jaff ransomware stands out in our global and regional top ransomware charts, as among senior ransomware families such as Cryptowall, Locky and Cerber, which have dominated the ransomware landscape for over a year, Jaff only emerged in May 2017. A key reason for this ransomware's vast distribution is the fact that it has been spread by one of the largest spam botnets ever observed – the notorious Necurs botnet.

TOP BANKING MALWARE

In this section of the report the graphs illustrate the percentage of organizations that were affected by each banking malware. The graphs provide global views and also regional insight into the top banking malware.

Global

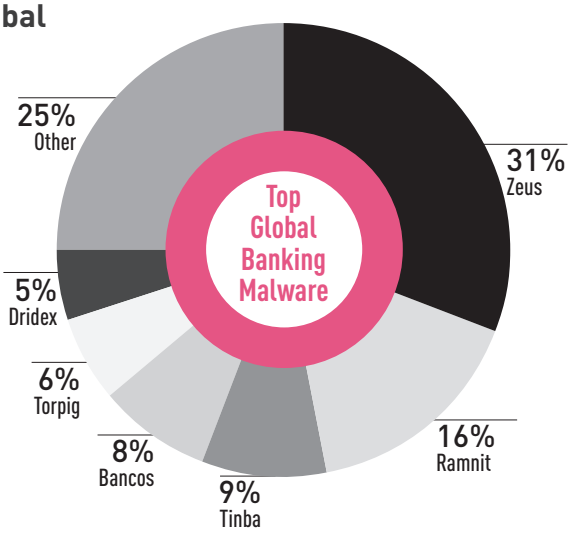

Figure 12: Most Prevalent Banking Malware Globally

Americas

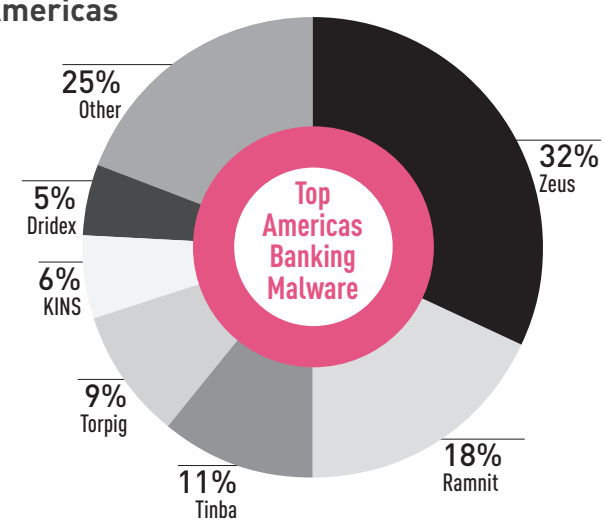

Figure 13: Most Prevalent Banking Malware in the Americas

EMEA

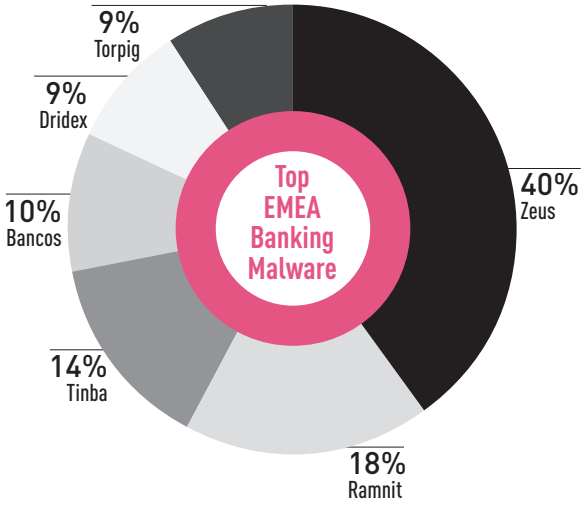

Figure 14: Most Prevalent Banking Malware in EMEA

APAC

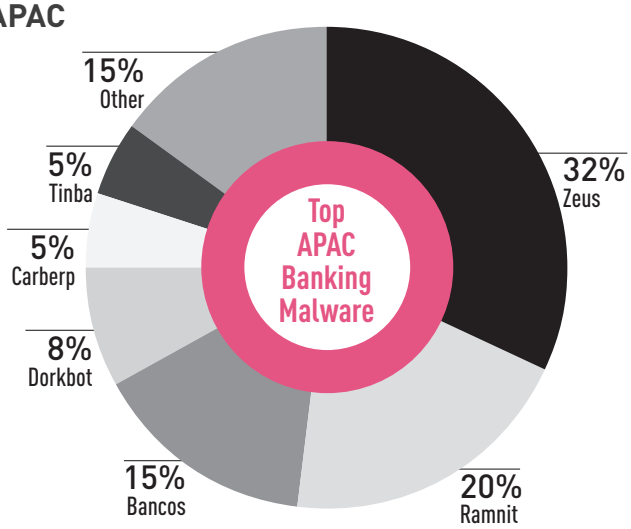

Figure 15: Most Prevalent Banking Malware in APAC

Banking Malware Global Analysis

- The most prominent banking Trojans, dominating the Global Top Banking Malware list, Zeus, Ramnit and Tinba, have kept their place at the top of the list since the second half of 2016. Furthermore, the malware listed in the global rank is not new. It was present in 2016. A review of the most prominent Banking Trojans observed over time can be found in the report Banking Trojans; From Stone Age to Space Era, a joint report by Check Point and Europol.
- Zeus took command of the top spot in banking malware for all regions – a similar status for Zeus was also observed in the second half of 2016.
- Carberp, a sophisticated banking malware whose source code was leaked in 2013, only made it to the top banking malware rank of the APAC region. Interestingly, the recent CIA leak, mentioned in Trend 1, revealed that the agency borrowed a few elements from the malware code when its source code was leaked and made available to the public, in 2013.

TOP MOBILE MALWARE

New variants of the infamous HummingBad malware emerged at the start of 2017, keeping HummingBad at the top of the global mobile malware list.

Global

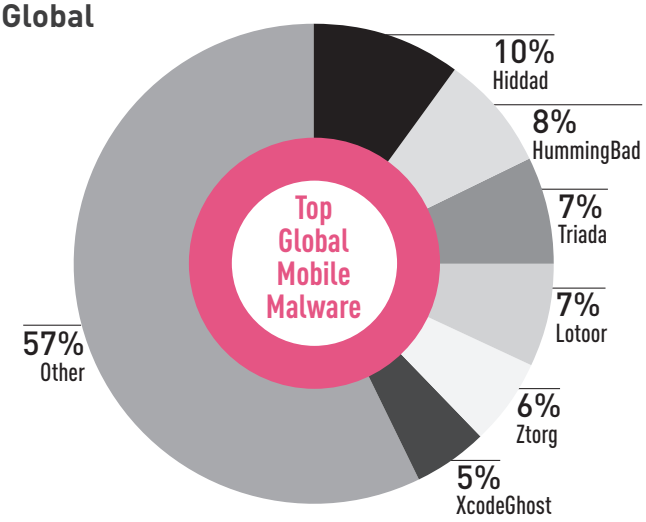

Figure 16: Top Mobile Malware Globally

Americas

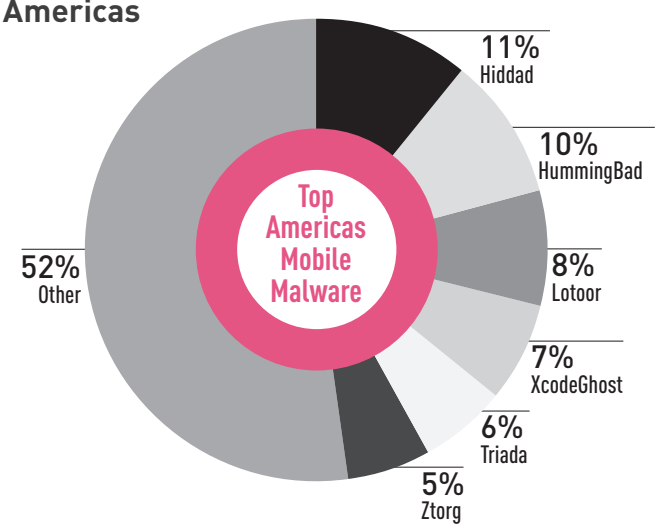

Figure 17: Top Mobile Malware in the Americas

EMEA

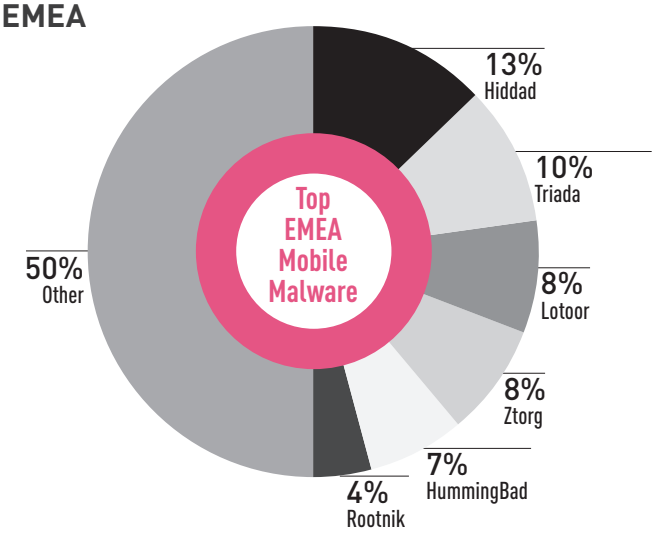

Figure 18: Top Mobile Malware in EMEA

APAC

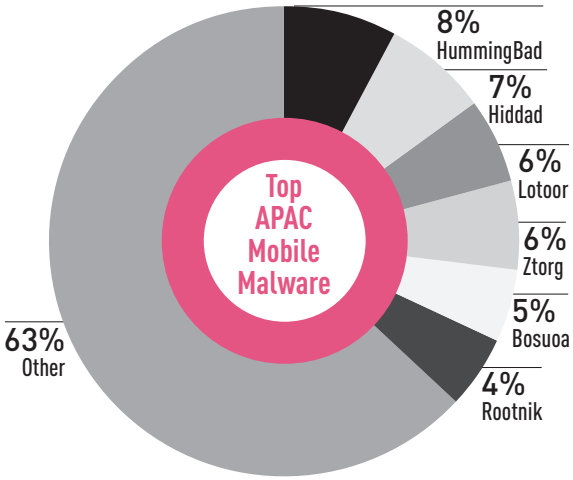

Figure 19: Top Mobile Malware in APAC

Mobile Malware Global Analysis

- New variants of the HummingBad malware, dubbed HummingWhale, emerged in the start of 2017 keeping HummingBad in the top mobile malware globally throughout the entire first half of the year. HummingWhale, also operated as a dropper, is used to download and execute additional apps, but it can also upload fraudulent apps on a virtual machine, and for the first time, it made its way onto Google Play.
- Xcodeghost, a compromised version of the iOS developer platform Xcode, that was altered so that it injects malicious code into any app using the platform, only appears in the Americas top mobile malware rank. According to our data, the top countries attacked by the malware are the US and Canada. Similar to 2016, Xcodeghost is also among the Top Mobile Malware globally.
- This is the first time Hiddad, Android malware used mainly to display ads which emerged in late 2016, appears in the top mobile malware ranks – furthermore, the relatively new malware is making an appearance on the global list, as well as the top mobile malware ranks in the Americas and EMEA regions.

CYBER ATTACK CATEGORIES BY REGION

The infographic below shows the spread by region of three of the main malware categories: banking, mobile and ransomware.

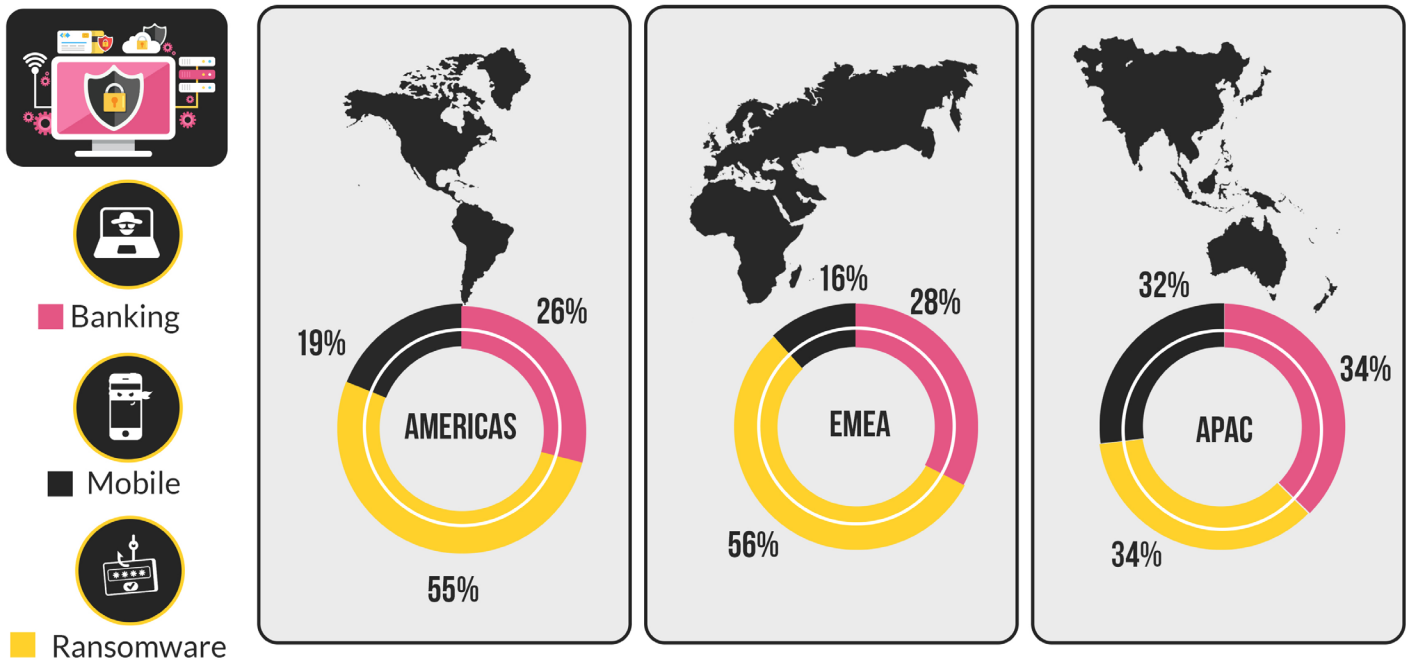

Figure 20: Attack Categories by Region

Note: We did not include an 'other malware' category as the focus is on comparing the three most common types of malware to one another and to compare to the three most common types of malware in the H2 2016 Threat Intelligence Trends Report.

GLOBAL THREAT INDEX MAP

The Check Point Threat Index is based on the probability that a machine in a certain country will be attacked by malware. This is derived from the ThreatCloud World Cyber Threat Map, which tracks how and where cyberattacks take place worldwide in real time. The map below displays the risk index globally and highlights the main risk areas around the world - lighter pink indicates low risk, dark pink indicates high risk, grey indicates insufficient data.

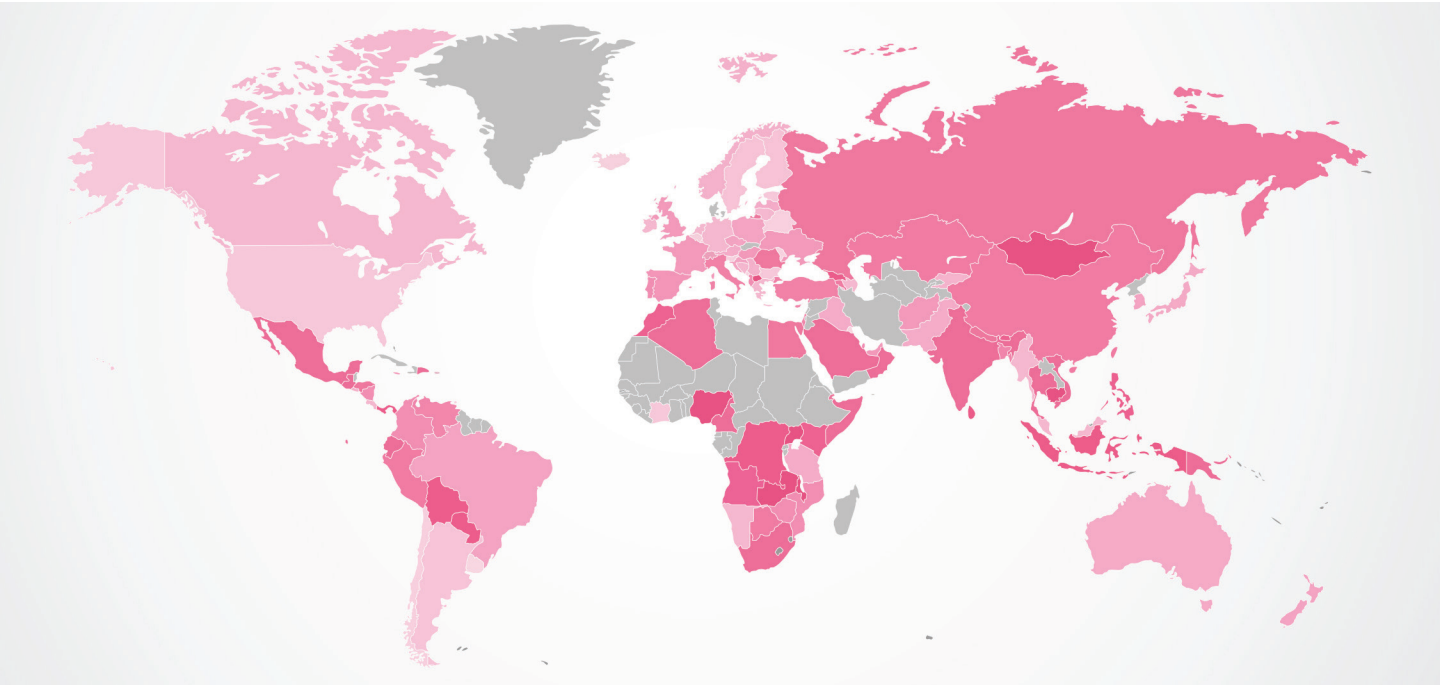

Figure 21: The 2017 H1 World Cyber Threat Index Map

SUMMARY OBSERVATIONS

The first half of 2017 showcases the nature of today's threat landscape. Globally spread malware, such as Fireball, which operated under the radar until several months ago, are now at the top of our global malware rank. Massive attack campaigns, including the WannaCry and NotPetya ransomware, have definitely left their mark and entered the global ranks as well. In parallel, as seen in 2016 as well, a few older malware families such as the Cryptowall ransomware, Conficker botnet and Kelihos Botnet managed to maintain their standing in terms of global distribution. We can assume that their vast distribution, maintained via massive botnets spread throughout the globe, is a key reason for their constant market dominance. These prominent botnets don't always stand on their own and push smaller malware families aside – in many cases, they are the key distributors of newer malware, mostly ransomware and banking malware. This is yet another reason for their continuous appearance in the top malware charts.

Among the top ransomware lists, one new family, which emerged in May 2017, stands out. This is the Jaff ransomware, massively spread via the notorious Necurs botnet. As previously observed, some prominent ransomware families such as Locky and Cerber, that stood out as dominators of the ransomware market in our H2 2016 Threat Intelligence Trends report, demonstrate a long tail distribution, meaning that a small number of these families are responsible for a disproportionately large percentage of the attacks, while thousands of other ransomware families are rarely seen. We observed a similar 'long tail' effect in the mobile landscape.

The Check Point ThreatCloud is the largest collaborative network dedicated to exposing and fighting cybercrime. It uses a global network of threat sensors to deliver the most up-to-date threat data and cyber-attack trends. The ThreatCloud database identifies millions of malware types daily, and contains more than 250 million addresses analyzed for bot discovery, as well as over 11 million malware signatures and 5.5 million infected websites.

RECOMMENDATIONS

It's evident cybercriminals aren't slowing down. In fact, based on the 2017 data to date, and analysis of WannaCry and NotPetya, the latest trends show malware being reconfigured to be far more effective at spreading laterally throughout organizations to rapidly cause large scale damage. Yes, even these types of sophisticated attacks could have been prevented had enterprises utilized solutions and techniques available to them today, such as proper network segmentation, threat emulation, threat extraction and endpoint security. With the all the news highlighting cyber risks these days, it's shocking only 1% of organizations have implemented the necessary solutions to proactively prevent these types of attacks.

While some organizations are taking a preventative approach, many organizations still implement point solutions, each only able to address individual problems. This approach creates 'device sprawl', with all the associated system complexity and maintenance challenges. With almost 1,600 cybersecurity companies worldwide, point solutions lead to gaps and fragmentation which allow threats to bypass security solutions undetected. This fragmented approach remains focused on remediation, after the damage has already been done, rather than preventing the problem in the first place. It's time to change the course of action and apply a new architecture focused on prevention rather than detection. Organizations need to replace their current mindset of using point solutions and mitigating the damage after the attack with a new approach of focusing on security prevention and using a unified architecture for managing security threats in the network, cloud and mobile devices.

By understanding emerging threats and implementing the latest prevention technologies, organizations can create a solid cybersecurity defensive posture. This approach turns security into an enabler, unlocks innovation and fosters an environment for high performance and productivity without compromise.

APPENDIX – MALWARE FAMILY DESCRIPTIONS

- **Alman –** The McDonald's India app, McDelivery, leaked the personal data of over 2.2 million customers, including name, email address, phone number, home address and social profiles. The leak is the result of an unsecured public API. Although McDelivery acknowledged the issue on February 13, as of March 17, the fix had not yet been completed and the app was still leaking customer data.
- **Bancos –** Banker which steals financial information, using keylogging to record the victim's credentials as they are entered on a targeted bank webpage. Bancos can also supplement or replace a legitimate bank login page with a fake webpage. The Trojan is active primarily in Latin America, particularly in Brazil, and is spread mostly via phishing.
- **Bosuoa –** Android malware, which disguise itself as a legitimate mobile application, but instead sends multiple premium SMS messages to certain predefined numbers, which lead to significant costs.
- **Carberp –** Sophisticated Banking Trojan botnet which targets remote banking and payment systems. Carberp is designed to steal user credentials and monitor user browsing activities, and is based on modules, which can be downloaded separately to the victim machine. It is estimated that the botnet was coded by a group of highly skilled Russian actors. In 2013, the Carberp source code was leaked and made available for download on various forums.
- **Cerber –** An offline ransomware, meaning that it does not need to communicate with its C&C server before encrypting files on an infected machine. It is spread mostly via malvertising campaigns which leverage exploit kits, but also through spam campaigns. It is operated by its author as a ransomware as-a-service; the author recruits affiliates to spread the malware for a share of the ransom payment.
- **Cloud Hopper –** Malware campaign associated to a known Chinese APT group dubbed APT10 and aimed to gain network access and persistence for sensitive information gathering by targeting managed security service providers (MSSP), as an entry point to their customers networks. The malware is deployed based on remote access to the organization network, and the obtained access is leveraged by the attackers to collect sensitive data.
- **Conficker –** Worm that allows remote operations and malware download. The infected machine is controlled by a botnet, which contacts its Command & Control server to receive instructions.
- **Cryptoload –** Downloader, used mainly to download ransomware to the victim machine. Cryptoload is usually sent within archive files as attachments in spam campaigns, and has been previously used to download Cryptowall ransomware, TeslaCrypt ransomware and Locky ransomware, as well as Fareit Info-stealer
- **CryptoWall –** Ransomware that started as a Cryptolocker doppelgänger, but eventually surpassed it. After the takedown of Cryptolocker, CryptoWall became one of the most prominent ransomwares to date. CryptoWall is known for its use of AES encryption and for conducting its Command & Control communications over the Tor anonymous network. It is widely distributed via exploit kits, malvertising and phishing campaigns.
- **Dorkbot –** IRC-based Worm designed to allow remote code execution by its operator, as well as download additional malware to the infected system, with the primary motivation being to steal sensitive information and launch denial-of-service attacks. It install a user-mode rootkit to prevent viewing or tampering with its files and modifies the registry to ensure that it executes each time the system starts. It will send messages to all of the infected user's contacts, or hijack an existing thread, to contain a link to the worm's copy.
- **Dorvku –** Malware which targets Windows operating system users. Dorvku collects system information and sends it to a remote server. It also collects sensitive information from targeted web browsers, and accepts commands to perform malicious activities on the infected system.
- **Dridex –** Banking malware that leverages macros in Microsoft Office to infect systems. Once a computer is infected, Dridex attackers steal banking credentials and other personal information to gain access to the user's financial records. It is spread through malicious spam e-mail with a Microsoft Word document attachment. Dridex first steals banking credentials and then attempts to generate fraudulent financial transactions.
- **Fireball –** Browser-hijacker that can be turned into a full-functioning malware downloader. It is capable of executing any code on the victim machines, resulting in a wide range of actions from stealing credentials to dropping additional malware.

- **Gamarue –** Used to download and install new versions of malicious programs, including Trojans and Adware, on victim computers.
- **Hacker Defender –** User-mode Rootkit for Windows, can be used to hide files, processes and registry keys, and also implements a backdoor and port redirector that operates through TCP ports opened by existing services. This means it is not possible to find the hidden backdoor through traditional means.
- **Hiddad –** Android malware which repackages legitimate apps and then released them to a third-party store. Its main function is displaying ads, however it is also able to gain access to key security details built into the OS, allowing an attacker to obtain sensitive user data.
- **HummingBad –** Android malware that establishes a persistent rootkit on the device, installs fraudulent applications, and with slight modifications could enable additional malicious activity such as installing a key-logger, stealing credentials and bypassing encrypted email containers used by enterprises.
- **iSpy –** Keylogger which is sold on various underground forums. iSpy captures passwords, collects passwords stored in web browsers and records webcams and Skype sessions. The malware is spread mainly via spam campaigns carrying malicious attachments.
- **Jadtre –** Virus which targets the Windows platform. It modifies system files, collects private information from the infected host and redirects to compromised sites to spread additional malware. In addition, Jadtre provides backdoor access to infected hosts. Jadtre is usually spread by freeware or spam email campaigns and can propagate itself by infecting executable files accessible through network drives.
- **Jaff –** Ransomware which began being distributed by the Necrus botnet in May 2017, via spam emails containing a PDF attachment which contains an embedded DOCM file. As the malware first emerged, it was massively spread at an infection rate of approximately 10,000 emails sent per hour.
- **Kazy –** Dropper designed to install malware onto infected computer systems. Kazy can be used by criminals to install practically any kind of malware onto their victims' machines including banking malware, info-stealers and spyware.
- **Kelihos –** Botnet mainly involved in bitcoin theft and spamming. It utilizes peer-to-peer communications, enabling each individual node to act as a Command & Control server.
- **KINS –** Also dubbed ZeusVM, KINS is a variant of the infamous Zeus Trojan. It is a banking Trojan that was offered for sale as a service on a closed Russian underground forums. The malware consists of a dropper and a variety of modules such as Remote Desktop Protocol module that allows bot managers to remotely access compromised machines. On 2015, the KINS builder and the source code of its management panel were leaked online.
- **Kometaur –** Trojan that targets Windows users. It contacts a remote server and sends information about the targeted system. It can also attempt to update itself.
- **LdPinch –** Trojan that targets Windows users. The malware is designed to delete, block, modify, or copy data and disrupt computer or network performance. The malware masquerades as a legitimate file or software.
- **Locky –** Ransomware which started its distribution in February 2016, and spreads mainly via spam emails containing a downloader disguised as an Word or Zip attachment, which then downloads and installs the malware that encrypts the user files.
- **Lotoor –** Hack tool that exploits vulnerabilities on Android operating system in order to gain root privileges on compromised mobile devices.
- **naKocTb –** Downloader, programmed to allow its operators to download and upload files to a victim's computer in a way that is transparent to the victim. The malware can be delivered to users via spam campaigns or bundled with free program installers that are published on suspicious websites.
- **Necurs –** Botnet used to spread malware by spam emails containing a malicious attachment, mainly Ransomware and Banking Trojans such as the Locky ransomware, Jaff ransomware and Dridex banking malware.
- **Nivdort –** Multipurpose bot, also known as Bayrob, that is used to collect passwords, modify system settings and download additional malware. It is usually spread via spam emails with the recipient address encoded in the binary, thus making each file unique.
- **Pykspa –** Worm that spreads itself by sending instant messages to contacts on Skype. It extracts personal user information from the machine and communicates with remote servers by using a Domain Generation Algorithms (DGA).
- **Ramnit –** A banking Trojan designed to steal banking credentials, FTP passwords, session cookies and personal data. Upon infection, Ramnit also allows remote control when the machine is connected to the internet.

- **RedLeaves –** Malware used in a campaigns which targeted users in the Healthcare, Energy, Critical Manufacturing and Information Security sectors worldwide. The malware consists of an executable, a loader and a Remote Access Tool (RAT) which collects various types of information from the victim system, such as system architecture and privileges, and sends it to its Command & Control server.
- **RIG Exploit Kit –** Exploit Kit first introduced in 2014. RIG delivers Exploits for Flash, Java, Silverlight and Internet Explorer. The infection chain starts with a redirection to a landing page that contains JavaScript that checks for vulnerable plug-ins and delivers the exploit.
- **Rootnik –** Android malware which uses a customized open-source root tool called "Root Assistant" to gain root access to Android devices, and maintains persistence by installing several APK files. The malware can than download executable files from remote servers and execute them on the infected device for various purposes, and steal sensitive user information.
- **RoughTed –** Large-scale malvertising used to deliver various malicious websites and payloads such as scams, adware, exploit kits and ransomware. It can be used to attack any type of platform and operating system, and utilizes ad-blocker bypassing and fingerprinting in order to make sure it delivers the most relevant attack.
- **Sality –** Virus that allows remote operations and downloads of additional malware to infected systems by its operator. Its main goal is to persist in a system and provide means for remote control and installing further malware.
- **Slammer –** Memory resident worm targeted to attack Microsoft SQL 2000. By propagating rapidly, the worm can cause a denial of service condition on affected targets.
- **Tinba –** A Trojan that steals the victim's credentials using web-injects, activated as the users try to login to their bank website.
- **Torpig –** Information stealing Trojan which collects sensitive information and banking credentials from the infected host and sends this information to a remote server without user permission. Machines infected by Torpig also form a massive botnet
- **TorrentLocker –** Ransomware that encrypts user documents, pictures and other type of files. Victims are requested to pay up to 4.1 Bitcoins (approximately US $1800) to the attackers to decrypt their files.
- **Triada –** Modular Backdoor for Android which grants superuser privileges to downloaded malware, as helps it to get embedded into system processes. Triada has also been seen spoofing URLs loaded in the browser.
- **WannaCry –** Ransomware which was spread in a large scale attack in May 2017 utilizing a Windows SMB exploit called EternalBlue in order to propagate within and between networks.
- **Winnti –** Backdoor that installs a rootkit on victim's system, and hooks critical functions and system driver of the infected Windows system. It collects system information and sends the data to a remote server, from which it also receives further instruction. Winnti might inject malicious payload into various processes, and it has been reported that some variants of this Backdoor might be signed with a legitimate certificate.
- **XcodeGhost –** A compromised version of the iOS developer platform, Xcode. This unofficial version of Xcode was altered so that it injects malicious code into any app that was developed and compiled using it. The injected code sends app information to a Command & Control server, allowing the infected app to read the device clipboard.
- **Zerghelper –** iOS malware which targets Chinese users, and therefore displays different behaviors according to the device's location in the world. The malware was able to bypass Apple's security. Once installed on a device in China, the app uses social engineering to install two configuration profiles, based on which applications that did not go through Apple's review, and may contain malicious code, can be downloaded to the infected device.
- **Zeus –** A sophisticated family of Banking Trojan that uses man-in-the-browser keystroke logging and form grabbing in order to steal banking information and victim accounts. Zeus targets popular operating systems such as Windows and Android and is usually distributed to end-users through social engineering tactics such drive-by downloads and phishing emails.
- **Ztorg –** Trojan that uses root privileges to download and install applications on the mobile phone without the user's knowledge.

ABOUT CHECK POINT RESEARCH

Check Point Research provides leading cyber threat intelligence to Check Point Software customers and the greater intelligence community. The research team collects and analyzes global cyber attack data stored on ThreatCloud to keep hackers at bay, while ensuring all Check Point products are updated with the latest protections. From the moment a breach is initiated, ThreatCloud begins sharing data across the entire network, providing researchers with the intelligence they need to deeply analyze and report on attacks. Check Point Research publications and intelligence sharing fuel the discovery of new cyber threats and the development of the international threat intelligence community to keep you secure.

LEADING THE THREAT INTELLIGENCE COMMUNITY

The research team consists of over 100 analysts and researchers currently cooperating with other security vendors, law enforcement, and different CERTs. Their data sources also include open sources, the ThreatCloud customer sharing network, and dark web intelligence. Internally, the team has developed their own machine learning modules, anomaly detection, reverse engineering, and campaign hunting techniques that all assist in staying ahead of hackers and the latest cyber threats.