cp<r>

CHECK POINT RESEARCH

2019

SECURITY REPORT

Welcome to the Future of Cyber Security

Check Point®
SOFTWARE TECHNOLOGIES LTD

INTRODUCTION

2018 introduced a challenging threat landscape. Threat actors consistently improved their cyber weapons, adopted new methods and adapted their attacks to emerging technologies. And although it may have seemed the past year was quieter, this is far from the case.

In the 2019 Security Report we review the latest threats facing organizations in the fifth generation of the cyber landscape and provide you with our observations and insights from the past year.

These attacks can be characterized as more targeted and stealthy, with the aim of sowing greater destruction. Whether carried out by cyber criminals or nation-states, the targeted attacks of 2018 revealed that financial and espionage motivations are not the only driving factors. With more attacks that shut down entire organizations or disrupted international events, 'boutique' ransomware attacks became very popular during 2018.

We also review the predictions made in our 2018 Security Report and assess to what extent these proved accurate. Along the way we provide cutting edge analysis from our in-house experts to arrive at a better understanding of today's threat landscape.

We then take a look under the hood of today's cyber crime world and show how this ecosystem remains a core part of the cyber threat landscape. Whether it is ransomware, banking trojans, keyloggers or cryptojackers, we look at what these malware types are and how they are now more accessible to potential cyber criminals due to Malware-as-a-Service (MaaS) services. This is the age of the democratization of cyber crime.

We then hone in on how threat actors are able to keep one step ahead by targeting the weakest points in an organization's IT infrastructure – the cloud, mobile and IoT. Indeed, these platforms offer a threat actor a much higher chance of success and fewer obstacles to overcome due to them being far less protected.
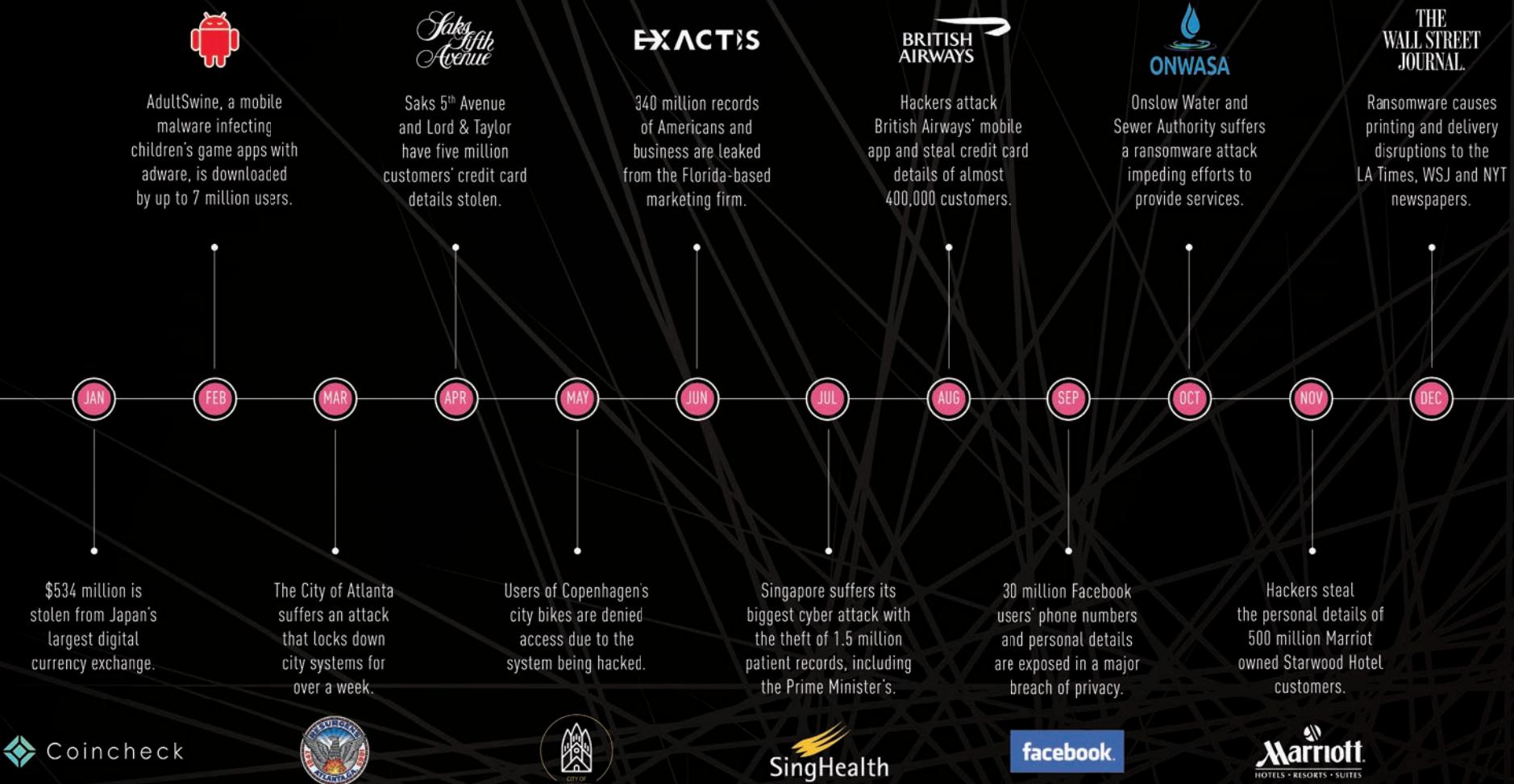
As a result, their profits can often be higher due to more private data stored on mobile devices and larger databases and resources held in the cloud. So with account takeovers becoming increasingly common, and the introduction of GDPR in 2018, potential data breaches and other attacks are simply too costly to ignore.

Finally, we provide some predictions of how we think the cyber threat landscape will evolve in the year ahead, looking specifically at the categories of Cloud, Mobile, Network, AI, IoT and Nation-State attacks. And finally, to stay ahead of these trends and predictions, we conclude with some expert recommendations and requirements that organizations should adopt in order to prevent fifth generation cyber attacks.

2019 SECURITY REPORT

TIMELINE OF 2018 ATTACKS

AdultSwine, a mobile malware infecting children's game apps with adware, is downloaded by up to 7 million users.

Saks 5th Avenue and Lord & Taylor have five million customers' credit card details stolen.

340 million records of Americans and business are leaked from the Florida-based marketing firm.

Hackers attack British Airways' mobile app and steal credit card details of almost 400,000 customers.

Onslow Water and Sewer Authority suffers a ransomware attack impeding efforts to provide services.

Ransomware causes printing and delivery disruptions to the LA Times, WSJ and NYT newspapers.

JAN · FEB · MAR · APR · MAY · JUN · JUL · AUG · SEP · OCT · NOV · DEC

$534 million is stolen from Japan's largest digital currency exchange.

The City of Atlanta suffers an attack that locks down city systems for over a week.

Users of Copenhagen's city bikes are denied access due to the system being hacked.

Singapore suffers its biggest cyber attack with the theft of 1.5 million patient records, including the Prime Minister's.

30 million Facebook users' phone numbers and personal details are exposed in a major breach of privacy.

Hackers steal the personal details of 500 million Marriot owned Starwood Hotel customers.

MAJOR CYBER ATTACKS OF 2018

RANSOMWARE ☠

Atlanta Ransomware Attack

In March, the SamSam ransomware struck the City of Atlanta in a big way by infecting and halting the operation of multiple city services for over a week. Services affected were the city's law courts that prevented court cases from proceeding, warrants being issued, and residents being able to access the city fine online payment services. The malware entered through one of the many public-facing entry points, such as FTP servers and various VPNs, and demanded a ransom of almost $7,000 be paid in Bitcoin to unlock each affected computer.

Ukraine Energy Ministry

In April, threat actors used ransomware to take the website of Ukraine's energy ministry offline and encrypt its files. It's believed that threat actors took advantage of vulnerabilities in Drupal 7, the off-the-shelf content management system software, to carry out the attack. Check Point Research carried out a detailed analysis of the vulnerabilities in versions 6-8 of Drupal to reveal how it works.

> *$2.7 million spent by the City of Atlanta to repair damage from ransomware attack.*
>
> Source: Atlanta Journal-Constitution newspaper – www.ajc.com

Boeing Ransomware Attack

WannaCry ransomware attacks were still active in 2018, as seen in the attack on a Boeing production plant in Charleston, South Carolina. The attack was spread rapidly throughout the company's manufacturing IT systems and there was concern that the virus would hit equipment used in functional tests of planes and potentially spread to airplane software.

Ransomware took center stage in 2017, though last year saw a dramatic fall in this type of attack. Regardless of the decline, however, ransomware attacks have not disappeared, and instead continue to be a major cause of concern for organizations across all industries worldwide.

According to our research into the GandCrab ransomware, threat actors are merely adapting their techniques, sometimes in real time, offering an affiliate system to allow technically low-level criminals to get in on the lucrative form of attack.

Itai Greenberg
VP of Product Management

DATA BREACHES

Facebook Data Breach

In March, reports emerged of how Cambridge Analytica, a political data firm, collected the personal data of over 50 million Facebook users via a 'personality test' app that scraped details about people's personalities, social networks, and their engagement on the social platform. The scandal had a major impact on the internet giant and arguably led to a dramatic drop in their share price.

> *76% of organizations experienced a phishing attack in the past year.*
>
> Source: 2018 IT Professionals Security Report Survey

Exactis Data Breach

In June, Exactis, a marketing and data aggregation firm based in Florida, left a database exposed on a publicly accessible server. The database contained two terabytes of information that included the personal details, including email addresses, physical addresses, phone numbers, and a host of other personal information, of almost 340 million American citizens and businesses.

Marriott Hotels Data Breach

A massive data breach exposed the records of over 500 million customers of the Marriott-owned Starwood Hotels, taking the title of being the world's second largest data breach. Most of those affected had their name, postal address, phone number, email address, passport number and arrival and departure information exposed. Under the GDPR rules, Starwood may face significant financial penalties of up to four percent of its global annual revenue if found to be in breach.

Although data breaches have been occurring continuously, 2018 was a turning point in respect to how data is perceived and how important it is to protect it. With the introduction of GDPR in May, organizations worldwide need to make data protection a priority and be compliant with on a legal and regulatory level.

With cloud becoming an increasingly popular way to store data, either through SaaS services or cloud storage containers, it's become apparent that relying on cloud providers is not enough. Instead, organizations must adopt the Mutual Responsibility model to protect both their data and any means used to access it.

Zohar Alon
Head of Cloud Products

MOBILE MALWARE

'AdultSwine' Malicious Apps

Check Point researchers revealed a new and nasty malicious code on Google Play Store that hides itself inside approximately 60 game apps, several of which are intended for use by children. According to Google Play's data, the apps were downloaded between three million and seven million times. Dubbed 'AdultSwine,' the malicious apps wreaked havoc by displaying ads from the web that are often highly inappropriate and pornographic, attempting to trick users into installing fake 'security apps' and inducing users to register to premium services at the user's expense.

Man in the Disk

A shortcoming in the way Android apps use storage resources was discovered that could open the door to an attack resulting in any number of undesirable outcomes, such as silent installation of unrequested, potentially malicious, apps to the user's phone. The hugely popular game, Fortnite, was found to be susceptible to such an attack and quickly patched a release for its users to install.

> *The 'AdultSwine' malware was installed up to **7 million times** across 60 Children's Games Apps.*
>
> Source: Check Point Research

LG Vulnerabilities

Check Point Research discovered two vulnerabilities that reside in the default keyboard on all mainstream LG smartphone models. These vulnerabilities are unique to LG devices, which account for over 20% of the Android OEM market in the US, according to a 2017 survey. Both vulnerabilities could have been used to remotely execute code with elevated privileges on LG mobile devices by manipulating the keyboard updating process, acting as a keylogger and thereby compromising the users' privacy and authentication details. Both vulnerabilities were reported to LG, who then released a patch.

With the mobile threat landscape always evolving, even the most trusted mobile app stores continue to prove themselves insufficient for defending against attacks. Although these stores are improving their own threat prevention technologies, there is still a continuous high infection rate among the world's five billion mobile phone users. This proves why consumers and employees who use their own devices for business activities require their own on-device threat prevention technology as well. The attacks seen over the past year confirms just how vulnerable the data stored on our mobile devices really is.

Brian Gleeson
Head of Threat Prevention
Product Marketing

NEVER DOES A DAY GO
BY THAT WE DO NOT SEE
ORGANIZATIONS UNDER
CONSTANT ATTACK FROM
THE EVER GROWING NUMBER
OF MALWARE SPREADING
AT HIGHER RATES THAN EVER.

CRYPTOCURRENCY ATTACKS

Jenkins Miner

Check Point Research discovered one of the biggest malicious mining operations ever seen. Dubbed 'Jenkins Miner', the operation targeted powerful Jenkins servers using a hybridization of a Remote Access Trojan (RAT) and XMRig miner. Distributed over several months, the cryptomining malware targeted victims around the globe to mine valuable cryptocurrency, negatively impacting organizations' servers by causing slower load times and raising the potential for a Denial of Service.

> **Over 20%** *of organizations are impacted by Cryptojacking Malware every week.*
>
> Source: Check Point ThreatCloud

RubyMiner

By using old vulnerabilities published and patched in 2012 and 2013, a threat actor attempted to exploit 30% of all networks worldwide and plant the RubyMiner crytomining malware on their servers to mine the Monero cryptocurrency. Among the top countries targeted were the United States, Germany, United Kingdom, Norway and Sweden, though no country went unscathed.

Coinrail Hacked

The South Korean cryptocurrency exchange, Coinrail, was hacked in June causing the price of Bitcoin to drop sharply by 10%. The hack caused the loss of around 30% of the coins traded (around $35 million worth) on the exchange and highlighted the lack of security and weak regulation of the global cryptocurrency markets. This was the latest in a spate of attacks on virtual coin exchanges; others included Japan's CoinCheck where over $500 million in coin value was stolen.

> **40%** *of organizations were impacted by cryptominers last year.*
>
> Source: Check Point ThreatCloud

The end of 2017 marked the rise of cryptominers, continuing in full force throughout 2018. Unlike ransomware, cryptomining offers cyber criminals a much stealthier style of attack that can remain on an organization's servers for months without being detected. During this time, and as long as it is undetected, its authors earn a steady stream of passive income.

Also in contrast to ransomware, cyber criminals are at much less risk while illicitly making money. Whether it is using a user's private computer, infecting a website with a crypto-mining advertisement or harnessing the immense CPU power of an organization's server, it does not take long for criminals to earn large amounts of their preferred digital currency.

Maya Horowitz
Director of Threat Intelligence & Research

BOTNETS

IoTroop's First Attack

In late January 2018, the 'IoTroop' botnet, discovered by Check Point researchers in October 2017, launched its first attack against the financial sector. IoTroop is a powerful internet of things (IoT) botnet comprised primarily of compromised home routers, TVs, DVRs, and IP cameras. The first attack used 13,000 IoT devices across 139 countries to target a financial organization with a DDoS attack, followed by two more attacks against similar targets within 48 hours.

> *The Ramnit Botnet infected* **100,000** *in just two months.*
>
> Source: Check Point Research, Ramnit's Network of Proxy Servers

Pyeongchang Winter Olympics

According to the International Olympic Committee (IOC), a DDoS attack on the Pyeongchang Winter Olympic Games took the official Olympic website offline for 12 hours and disrupted WiFi and televisions at the Olympic stadium. Although critical operations were not affected by the incident, event organizers had to shut down servers and the official games website to prevent further damage.

> **49%** *of organizations experienced a DDoS attack in the past year.*
>
> Source: 2018 IT Professionals Security Report Survey

Attack on US Democratic Candidates

In July 2018, hackers targeted the campaigns of at least two US Democrat candidates during the 2018 primary's season. Using DDoS attacks to disrupt campaign websites for over 21 hours, potential voters were denied access to key information or resources during periods of active fundraising and positive news publicity.

Anti-virus software makes recruiting an army of bots to launch a DDoS attack from unprotected computers a tricky task for threat actors. However, with organizations increasingly turning to popular, yet unprotected and vulnerable IoT devices to keep tabs on their operations, the number of opportunities for a large botnet recruitment drive also increases.

It should come as no surprise that, as a result of such large botnet recruitment, we are seeing larger DDoS attacks.

Richard Clayton
Head of Botnet Research

APT ATTACKS

Big Bang APT

The Check Point Threat Intelligence Team discovered the comeback of an APT surveillance attack against institutions across the Middle East, specifically the Palestinian Authority. The attack began with the targets receiving an attachment, sent in a phishing email, which included a malicious executable. The malware's functions included taking a screenshot of the infected machine, logging details about the victim's system and stealing a list of documents with certain file extensions.

> *The US and UK formally blamed Russia for the 2017 NotPetya ransomware attack that caused **billions of dollars** in damages worldwide.*
>
> Source: Check Point ThreatCloud

SiliVaccine

In exclusive research, Check Point Researchers revealed some alarming details about North Korea's home-grown anti-virus software, SiliVaccine. One of several interesting factors was that a key component of SiliVaccine's code is a direct copy of Trend Micro's anti-virus scanning engine. Known to be sent to foreign journalists that report on North Korean activities, the researchers discovered that SiliVaccine includes highly suspicious behavior that would allow the monitoring of these journalists' activities.

Russia UK Relations

As tensions in UK and Russia relations intensified over UK accusations that Russia poisoned two UK citizens on home soil, the UK's National Cyber Security Centre warned that Russian state actors were targeting UK critical infrastructure by infiltrating supply chains. Although attribution is notoriously difficult, the attacker's techniques seemed to bear the hallmarks of 'Energetic Bear,' a Russian hacking group that has been tied to attacks on the energy sector since 2012.

> *614 GB of data related to weapons, sensor and communication systems stolen from US Navy contractor, allegedly by Chinese government hackers.*
>
> Source: Check Point ThreatCloud

Over the past year, a rare glimpse into APT attacks has shown that nation-state and non-state organizations will go to great lengths in order to gain intelligence on their adversaries.

Government agencies must be on high alert for the clear and present threat of cyber warfare. It's an act of aggression that remains and will continue to be an attractive weapon of choice due to its high impact, low risk of attribution and cost effectiveness.

Dan Wiley
Head of Incident Response

2018 THREAT TRENDS

Cryptomining Is Here to Stay

At the beginning of 2018, cryptomining malware made a magnificent rise utilizing a wide scope of targets including personal computers,[1] powerful servers,[2] mobile devices,[3] and even the cloud environment.[4] When it comes to mining there is no doubt that they are here to stay. Indeed, cryptomining attacks soared in 2018, affecting over 40% of organizations worldwide at its peak, compared to 20.5% at the end of 2017, and dominated the top cyber attacks[5] and malware families seen in the wild for 12 months straight.

In January 2018, total cryptocurrency values dropped rapidly, shrinking[6] by about 86% from their peak. Despite this, cryptominers detached themselves from cryptocurrencies' market cap and kept their place as the most prominent malware infection used by threat actors in 2018.

As we will see in the next installment of this Security Report, from an attackers' perspective, cryptojackers can be highly lucrative, are simple to launch and easy to conceal. Furthermore, cryptojacking attacks allow threat actors to carefully walk the thin line of legitimacy, knowing that cryptojacking is not considered as offensive as other attack techniques such as ransom extortion or data theft.

In the second half of 2018, due to the attention they gained from security vendors, cryptojackers went through a rapid evolution, becoming more sophisticated and capable of overcoming security solutions. As a result, we witnessed cryptojackers that presented various evasion techniques[7], quick adoption of exploits, and even those embedded in multi-staged attacks to serve additional malware[8] to the infected machine.

When it comes to mining it seems threat actors have become more creative and continue to invent increasingly deceptive techniques to serve miners. These include drive-by attack kits and implanting miners inside legitimate applications' installers such as Flash update and Windows Installer.

A year after they took the world by storm, cryptominers show no intention of slowing down soon. New, sophisticated malware families keep integrating mining capabilities to their code and tens of thousands of websites are constantly compromised to exploit their users' resources.

[1] https://www.bleepingcomputer.com/news/security/winstarnssmminer-coinminer-campaign-makes-500-000-victims-in-three-days/

[2] https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/

[3] https://securityaffairs.co/wordpress/70968/malware/hiddenminer-android-miner.html

[4] https://motherboard.vice.com/en_us/article/8x5wy5/cryptocurrency-tesla-bitcoin-mine-ethereum

[5] http://blog.checkpoint.com/2018/12/11/november-2018s-most-wanted-malware-the-rise-of-the-thanksgiving-day-botnet/

[6] https://coinmarketcap.com/charts/

[7] https://www.kaspersky.com/about/press-releases/2018_new-fileless-crypto-miner

[8] https://securityaffairs.co/wordpress/75070/malware/zombieboy-monero-miner.html

Ransomware Attacks Go Boutique

Ransomware is today a household term even among non-technical-oriented individuals. In the last four years it has spread massively, in large-scale campaigns, targeting all industries and successfully sowing panic in their victims, prompting them to pay any sum in ransom to retrieve their data safely.

In 2018, however, we witnessed ransomware adapting to become more targeted to ensure more lucrative profits. This evolution is a direct result of a noted decrease in the actual ransom payments, probably derived from the growing security awareness and mitigation techniques adopted by many companies, including routine back-up policies and the free availability of decryption tools.

This new strategy allows threat actors to maximize their revenue, as a tailored attack against organizations' critical assets is a great tactic to ensure the ransom payments. Furthermore, it allows cyber crime to enter safely under the radar of security vendors, by not engaging with a mass distribution campaign which is likely to lead to more exposure.

This year the SamSam ransomware reaped millions in cryptocurrencies after shutting down Atlanta[9] and Colorado[10] city councils' departments, hospitals,[11] and the medical testing giant LabCorp.[12] In other cases the port of Barcelona and the port of San Diego suffered major ransomware attacks that significantly disrupted critical operations. Another strain of ransomware also hit Bristol Airport[13] in the UK, and shut down flight display screens for two days.

As victims of targeted ransomware attacks don't usually disclose the full damage and attack details, these cases are probably only a drop in the ocean of the actual total attacks launched using this strategy. The equation is simple though; the greater the potential damage, the higher the chance the ransom will be paid.

In addition, the infection stage, previously dominated by vast spam or drive-by methods, was replaced by an extensive reconnaissance effort aimed to locate the most lucrative targets. This involves searching unsecured Remote Desktop Protocol (RDP) connections, manual network mapping and credential purchasing in hacking forums. The Ryuk ransomware,[14] for example, exposed by Check Point security researchers in August 2018, had conducted highly-planned and sophisticated attacks against well-chosen organizations and netted $640,000 for its operators. While working on this report, Ryuk hit the newspaper print and online media publishing company, Tribune Publishing,[15] and prevented the distribution of many leading U.S. newspapers, including the Wall Street Journal, New York Times and Los Angeles Times.

[9] https://www.bleepingcomputer.com/news/security/city-of-atlanta-it-systems-hit-by-samsam-ransomware/

[10] http://securityaffairs.co/wordpress/69492/malware/samsam-ransomware-colorado-dot.html

[11] http://securityaffairs.co/wordpress/68052/malware/samsam-ransomware-campaign.html

[12] https://www.csoonline.com/article/3291617/security/samsam-infected-thousands-of-labcorp-systems-via-brute-force-rdp.html

[13] https://securityaffairs.co/wordpress/76248/breaking-news/bristol-airport-cyber-attack.html

[14] https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/

[15] https://www.forbes.com/sites/daveywinder/2018/12/30/north-korea-implicated-in-attack-that-stops-wall-street-journal-and-new-york-times-presses/#63ca369220a2

Malware Synergy

The shift of prominent malware families, such as the Emotet[16] Banking Trojan, from banking credential theft to the distribution business, marks a significant phenomenon observed in 2018. Malware families previously known for their single, well-functioning utility are now expanding their operations and offering additional capabilities. Furthermore, new malware families are often released to the wild with more than one significant goal or attack vector.

Hybrid malware, which demonstrate a few and often entirely different functions, are a great way for an attacker to guarantee that their operation yields profits. One example is a ransom demand that is deployed together with collecting user credentials, or harvesting sensitive information for future phishing attack. Another example is a botnet that can perform cryptocurrency mining using the bot network's CPU resources, and in parallel, utilize the same bots to distribute email spam.

These functions, though, do not have to be carried out by the same malware. Often, two malware developers could join forces in a single campaign involving different malware strains, either to ensure revenues and success or to achieve multiple goals.

In October 2018, computers and servers of North Carolina's Onslow Water and Sewer authority were attacked by the Ryuk ransomware, a highly-targeted, manually operated family. Interestingly, the investigation found that a primary stage of the well-planned attack involved[17] 'TrickBot', 'AdvisorsBot' and the 'Emotet' multi-functional malware. The notorious 'TrickBot' had partnered with 'IcedID', both banking malware, and machines infected by 'IcedID' had downloaded 'TrickBot' too. In another prominent case, the successful Ramnit 'Black' campaign[18] was observed spreading the AZORult info-stealing malware.

The increase in threat actor collaboration and capabilities expansion marks a great step for cyber criminals, pose a great danger to organizations, and should serve as a reminder that high-profile attacks may be just the first step in a more prolonged operation.

Cloud Risk Trends

2018 introduced a new fertile playground for threat actors – public cloud environments. Containing vast amounts of sensitive data, as well as great computational resources, the cloud has everything a threat actor could dream of. Furthermore, correlating to the increased movement of companies to public cloud services as the main platform for storing and managing their workloads, we witnessed multiple new techniques, tools and exploitations emerging against the cloud this year.

[16] https://research.checkpoint.com/emotet-tricky-trojan-git-clones/

[17] http://blog.checkpoint.com/2018/10/23/ransomware-stopped-working-harder-started-working-smarter-botnets-phishing/

[18] https://research.checkpoint.com/new-ramnit-campaign-spreads-azorult-malware/

Nonetheless, the majority of the attacks observed targeting the cloud are mainly derived from poor security measures including misconfigurations and the use of weak credentials which usually involve data compromise and information leakage. This reality essentially leaves so many exposed assets that attackers no longer need exploit a specific vulnerability to gain unauthorized access to sensitive resources. One example is the fitness software company 'Fitmetrix', unfortunately exposed[19] millions of customer records stored in a database hosted on AWS. In another case, personal details of nearly 700,000 American Express[20] India customers were exposed online via an unsecured MongoDB server.

In addition, in 2018 we observed cyber criminals utilizing misconfiguration in the cloud, abusing services hosted there for a wide range of attacks. Among them was performing cryptocurrency mining[21] by leveraging the vast computing power stored in the cloud, enslaving exposed cloud servers to trigger DDoS attacks[22], and even launching man-in-the-middle attacks by exploiting publicly open S3 buckets.

It is therefore safe to say that the bigger the cloud gets, the bigger the target and attention it attracts for cyber criminals. Setting up small environments on public cloud is relatively easy, but when it comes to moving a whole network infrastructure to public cloud, additional security measures must be adopted in order to ensure no asset is left exposed.

Mobile Trends: A Target on Apple's Back

As one of the most prominent actors in the mobile device industry, Apple is considered to have the most secure operating system. Together with keeping this system closed source, Apple has multiple built-in security measures aiming to protect their users from a variety of cyber threats. However, some may say that it is not enough.

As Apple's user-base has grown, it has become a more attractive target to threat actors wishing to get their hands on Apple devices' sensitive data and exploit their tools against them.

[19] https://securityaffairs.co/wordpress/77073/data-breach/fitmetrix-data-breach.html

[20] https://securityaffairs.co/wordpress/77815/data-breach/amex-india-data-leak.html

[21] https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/

[22] https://threatpost.com/demonbot-fans-ddos-flames-with-hadoop-enslavement/138597/

During 2018 we witnessed an increase in the number of vulnerabilities exposed for iOS. In one month alone three passcode bypass vulnerabilities[23] were discovered affecting all current iPhone models, including the recently released iOS version 12.0.1, and allowed a potential threat actor to gain access to a user's photos and contacts.

The severe 'Text Bomb'[24] flaw was also found in Apple devices running on iOS and macOS, and was capable of freezing apps and crashing iPhones. Another flaw revealed in 2018 was found in the process of pairing iPhone devices with Mac workstations or laptops, allowing attackers to take over the paired iPhone device without the owners' knowledge.

In addition, traditional malware has now upgraded their capabilities to target iOS devices. The Pegasus Spyware,[25] a cryptocurrency wallet and credential theft malware, and 'Roaming Mantis', a Banking Trojan and cyptocurrency miner[26] disguised as a calendar app, are just few of the threats which managed to breach Apple's Garden Wall and penetrate the App Store last year.

However, these threats are dwarfed by the specially crafted attacks that emerged towards Apple's devices. These include the FallChill malware that utilized a unique Mac function to secretly take screenshots of a victim's phone. This was the first time to see an APT activity,[27] allegedly carried out by the Lazarus Group, targeting OSX devices.

Together with the several high-profile attacks that occurred against Apple itself,[28] it appears then that in 2018 threat actors are now willing to prove that no environment, brand or operation system can be immune against cyber attacks.

Nation-States: No Longer an Officer and a Gentleman

Cyberspace often provides a veil of secrecy for nation-states to achieve operational gains. Over the past years, however, a trend has emerged to indicate that several have given up this veil and now operate quite openly, almost provocatively. Indeed, national interests are continuously exposed, with unrestrained demonstration of offensive capabilities. Of course, while no country takes responsibility for cyber-attacks, attribution is sometimes not too difficult to assign.

The precedents for such openness can be found in the aggressive Russian attacks against the Ukraine. Black Energy, which took down the power grid[29] in Ukraine in 2015 and NotPetya[30] which shut down the entire country in 2017, marked the way for several more countries to operate more freely; sometimes without the use of evasion techniques or fully covering their tracks.

[23] https://thehackernews.com/2018/10/iphone-lock-passcode-bypass.html

[24] https://threatpost.com/apple-rushes-fix-for-latest-text-bomb-bug-as-abuse-spreads/129987/

[25] https://thehackernews.com/2018/09/android-ios-hacking-tool.html

[26] https://arstechnica.com/information-technology/2018/03/theres-a-currency-miner-in-the-mac-app-store-and-apple-seems-ok-with-it/

[27] https://securelist.com/operation-applejeus/87553/

[28] https://www.welivesecurity.com/2018/08/17/australian-schoolboy-apples-network/

[29] https://www.bankinfosecurity.com/ukrainian-power-grid-hacked-a-8779

[30] https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

The infamous North Korean hacking group, Lazarus, was considered responsible for numerous violent attacks over the last year and before too. Indeed, with the devastating WannaCry attack, the Sony hack,[31] SWIFT banking theft[32] and the hacking of Cryptocurrency Exchanges,[33] North Korea abandoned elegance in 2018 and marched to a far more aggressive approach.

Iran was also demonstrating evolving cyber capabilities in the cyber espionage arena in 2018. As illustrated by Check Point Research, Iran's Domestic Kitten[34] campaign was aimed towards international elements as well as against its own citizens to serve its national interests, utilizing both mobile and desktop attack vectors to achieve its goals. With Domestic Kitten, Iran managed to carry an extensive surveillance campaign through mobile apps for years, and with Charming Kitten, an additional Iranian group, it joined a long list of espionage campaigns against Western and academic targets, using spear phishing emails.[35] Again, it put minor efforts in hiding their operations.

Alongside intelligence goals like espionage or surveillance campaigns, nation-state cyber attacks exposed some new missions such as sabotage, financial gains and revenge. Such was arguably the case with 'Olympic Destroyer' which threatened to ruin the Winter Olympic Games[36] in South Korea this year. While no attribution has yet been confirmed, considering the above trend it may not be too difficult to hazard a guess as to who the perpetrator might be. While the West retains a degree of statehood in cyberspace, there are nation-states, mainly eastern ones, who appear to be acting unbridled in their own interests.

[31] https://securityaffairs.co/wordpress/75994/cyber-warfare-2/north-korea-agent-indictment.html

[32] https://securityaffairs.co/wordpress/78382/apt/lazarus-latin-american-banks.html

[33] https://securityaffairs.co/wordpress/77213/hacking/cyber-attacks-crypto-exchanges.html

[34] https://research.checkpoint.com/domestic-kitten-an-iranian-surveillance-operation/

[35] https://threatpost.com/charming-kitten-iranian-2fa/139979/

[36] https://www.theguardian.com/sport/2018/feb/11/winter-olympics-was-hit-by-cyber-attack-officials-confirm,%20 http:/blog.talosintelligence.com/2018/02/olympic-destroyer.html

REVIEW OF 2018 PREDICTIONS

In last year's Security Report we predicted where each information systems platform was headed in 2018. To compare, we have revisited those predictions to see how they fared over the past twelve months.

Mobile

We expected that flaws in mobile operating systems and technology would continue to be discovered and this was very much the case. As seen by our discovery of vulnerabilities that reside in the default keyboard on all mainstream LG smartphone models, which account for over 20% of the Android OEM market[37] in the US, flaws such as these leave the door open to attackers carrying out Remote Code Injection attacks to spread malware.

In addition, flaws were found by Check Point Research in the Android operating system itself, leaving the External Storage component on devices worldwide exposed to a Man-in-the-Disk attack. Despite app developers being provided with guidelines on how they can avoid leaving their applications vulnerable, it is well known that developers do not have security front of mind when creating such apps. Operating system providers also do not do enough to ensure their devices are protected. As a result, the need remains for organizations to deploy advanced protection against mobile malware and interception of communications.

Mobile malware continued to proliferate too, as seen by up to seven million users who downloaded the AdultSwine[38] malware that infected over 60 children's game apps and exposed them to inappropriate ad content. RottenSys[39], a mobile adware, infected over five million devices with adware since 2016. Also, cryptominers entered the threat landscape not only on PCs and web servers, but across five billion mobile devices in use around the globe.

Cloud

Not surprisingly, and as expected, the theft of data stored on the cloud continued to plague organizations of all sizes as they transitioned their infrastructures to this cost-effective and agile platform. From fitness apps like Under Armour and PumpUp to retailers and ticket box office companies like TicketFly, not to mention Facebook, data breaches occurred on a daily basis and will continue to do so across all industries due to the value they hold for cyber criminals.

[37] https://phandroid.com/2017/05/08/lg-market-share-q1-2017/

[38] https://research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

[39] https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/

In addition, the introduction of GDPR last year added extra stress and pressure to those who hold customer data not only in the cloud but on their organization's servers in general. It's understood that these new regulations carry hefty fines for those who do not comply.

For this reason, we encourage all our customers to take the Shared Responsibility model seriously and not rely solely on their cloud provider's basic protections to keep them safe from known and unknown threats.

Network

Last year we predicted that ransomware 'refer a friend' schemes would surface. While those programs have yet to be seen, what *is* prevalent, as predicted in last year's report, is the Ransomware-as-a-Services now being offered through affiliate programs on the Dark Web. These programs advertise themselves to technically low-level threat actors wanting to get in on the action at a low cost.

In addition, while cryptominers entered network servers to harness the large CPU power they offer, ransomware attacks have not disappeared. WannaCry, the mega attack of 2017 with suspected North Korean origins, was responsible for attacks on Boeing's IT systems last year and it could be adapted to function as a cryptominer in the future.

After all, worms like ransomware that infect networks never really die out. Indeed, we are still seeing worms like Conficker from 2009 and traces of SQLSlammer from 2003 still in circulation.

IoT

Following our report into the ways threat actors could invade the privacy of consumers' homes via IoT devices such as vacuum cleaners, our prediction came true that these same types of exploits could well be applied to enterprise organizations' use of IoT devices

Through the discovery of vulnerabilities in DJI drones, the manufacturer of choice for 70% of the worldwide drone market, we revealed how gaps in the security of these devices can expose enterprises to great damage. Threat actors are presented with an opportunity to view and steal sensitive information of critical infrastructure, for example, collected by the drone and could be used in a future attack.

It's still the case that users are generally not aware of the security element of their IoT devices, and tend to leave the default settings in their original state. This continues to leave the door wide open for attackers to gain access to a consumer or organization's IT network.

Cryptocurrencies

Despite our expectation, digital currencies are still not heavily regulated. For this reason, we continue to see cryptocurrencies as the payment method of choice for cyber criminals behind ransomware attacks, and as an incentive for crypto-mining malware.

What began as a relatively new malware at the end of 2017 became the new norm in 2018. Our prediction, as detailed in this report, was right on.

In addition, our forecast that the value of these currencies would drop also came to pass although we thought it would be due to intervention of international government and law enforcement agencies. Instead, it was the increase of attacks on cryptocurrency exchanges themselves, such as those seen on Bithumb, Coinrail and CoinCheck. As we predicted, this sent shockwaves through the lucrative digital industry. In turn, this made investors nervous and dramatically lowered the value of Bitcoin, among others.

UNDER THE HOOD OF CYBER CRIME

Daybreak

Prior to the year 2000, hackers were primarily one-man operations exploiting weaknesses in computer operating systems or networks. In most cases, these computer enthusiasts experimented and explored this new online network and challenged themselves to 'beat the system.' In fact, despite being early cyber criminals, rarely was their behavior financially motivated. Indeed, while there was the potential for financial damage and security risks, the 'one-man-hacker' lacked the same motive and intent of the criminal gangs that were soon to follow.

After the Dawn

Not long after, once there were more people, websites and services available online, cyber criminals began to organize themselves and perfect their hacking techniques. Hardened criminal gangs soon realized that internet users saw it as safe, despite the technology being riddled with exploitable gaps and holes. Furthermore, the anonymity of the Internet served as a shield and far less risk of detection. Next, as shops and financial services moved online, vast amounts of financial data were transferred to cyber space. And where money flows, criminals are never far behind, always on the prowl to steal anything of value.

In short, gangs introduced a professional element to the world of cyber crime. Nowadays we are no longer looking at curious amateurs exploiting weaknesses in computer operation operating systems, but rather organized criminal gangs infiltrating computer networks for financial gain.

THE DEMOCRATIZATION OF CYBER CRIME

Crucial to understanding the new age of cyber crime is the awareness that today's cyber crime ecosystem is one that reflects and matches the legitimate world of business, albeit completely illegal.

The main roles in this underground economy break down into the following categories:

Programmers – develop malware to extort or steal data from potential victims.

Merchants – trade and sell the victim's stolen data.

IT Technicians – build and maintain the IT infrastructure (servers, databases, etc.) for criminals.

Hackers – search and find vulnerabilities in systems, applications and networks.

Fraudsters – create and carry out new ways to scam and manipulate potential victims.

Hosting Services – provide hosting services for the criminal's fraudulent content and sites.

Management – hire and form their cyber crime teams and manage the operation.

A Programmer's Tool Box

At their disposal, programmers have a variety of malware types they can create. Named by the brilliant, late Israeli computer researcher, Yisrael Radai, malware are software programs with the purposefully malicious intent to act against the requirements of the computer user. The types of malware most commonly seen in the wild fall mainly into the following categories:

SPYWARE

Often referred to as 'keyloggers', spyware tracks and steals digital information while keeping the victim fully unaware of the situation. It is particularly interested in financial data such as credit card details and online banking login credentials.

TROJANS

Disguised as safe programs, Trojans are designed to fool users, so that they unwittingly install it on their own system, and are then later sabotaged by it. Trojans are generally used to steal both financial and personal identifiable information (PII).

Over **10,000** different malicious files are detected per day.

Source: Check Point ThreatCloud Intelligence

VIRUSES

Dating back to the 1970s, a computer virus is a contagious piece of code that infects software and then spreads from file to file within a system. When infected software or files are shared between computers, or on the Internet, the virus spreads to new hosts.

RANSOMWARE

By locking down data on a victim's computer, typically by encryption, ransomware demands payment sent to an attacker in order for the encrypted files to be released and computer access restored to the victim.

Over **700** Malware Families are being used on a daily basis.

Source: Check Point ThreatCloud Intelligence

BOTWARE

The purpose of Botware is to turn the victim's computer into a "zombie" and become part of a larger network of devices that await instructions from its controller to launch an attack. A distributed denial-of-service (DDoS) is a key example.

CRYPTOJACKERS

Cryptojacking is the unauthorized use of the victim's computer to mine cryptocurrency and send it back to the attacker. It feeds off the victim's CPU power and results in the victim's computer slowing or even crashing.

In today's cyber crime landscape, cyber criminals are no longer the ones with the direct technical capabilities of creating the malware that's used in attacks. Nor are they necessarily the ones who need any know-how in distributing the attack. In fact, very little knowledge is required.

Instead, all a cyber criminal needs is access to the underground communication channels that act as the main marketplace for this ecosystem. There they will manage to "order" a malware or even a direct attack against a chosen target. This is the democratization of cyber crime.

The Dark Web

Making up a large chunk of the internet, the Dark Web is a hive of illicit activity. From illegal guns and drug dealing to Malware-as-a-Service (MaaS) programs, buyers and sellers use this medium to trade and exchange knowledge and products.

Hacking forums on the Dark Web have long been a popular platform and an important means of communication among cyber criminals. It allows them to publish job offers, market their products and consult with one another.

After all, large operations and campaigns cannot be carried out by one person and necessitate the recruitment of a team to share the workload. In other cases, these forums serve as places where malware and tools crafted for malignant reasons can be traded or sold to affiliates and generate revenue without the developer being directly involved in an attack.

The services offered online include malware kits, stolen data or even a package that contains a malware ready for distribution and a comprehensive management panel which allows unskilled hackers to easily track and control their infection rates and revenues. The different Malware-as-a-Services available include the infamous AZORult, FileLocker and Kraken ransomware that made headlines over the past year. The authors of GandCrab ransomware even offer technical support and tutorial videos for their product.

However, the takedown of Dark Web marketplaces such as the Hansa Market and Alpha Bay in 2017, spawned the next stage in the cyber game of cat and mouse. Threat actors soon shifted to new channels to evade authorities. In fact, they quickly transitioned to the increasingly popular and highly secure mobile messaging app, Telegram, to pursue their trade.

57% of onion sites have illegal content.

Source: Europol "Internet Organized Crime Threat Assessment, 2017"

Communication Channels

Telegram's hosted chat groups, known as 'channels', are used to broadcast messages to an unlimited number of subscribers, and, while their entire messaging history can be viewed, any response to the public messages is held privately. The discretion these channels provide goes a long way to help conceal a cyber criminal's identity and conversations.

Any threat actor with a shady skill, service, or product to offer or buy can enjoy private, end-to-end, encrypted chats instead of exposed threads in online forums. If in the past several steps were required to ensure an anonymous connection to Tor, the Dark Web browser, today any Telegram user can easily join channels with a single tap on their phone and start to receive notifications of clandestine conversations or offers while keeping their identity completely hidden.

This has allowed for much easier completion of the first stage in organizing an attack – connecting with those who can help put it all together.

One region in which these shady channels are flourishing is Russia and some have already attracted thousands of subscribers. Such examples are 'Dark Jobs', 'Dark Work' and 'Black Markets', to name a few. In addition, some channels, such as an Iranian channel which goes by the name of 'AmirHack', can contain up to 100,000 members.

These channels are not restricted to just recruiters and job-hunters. They also run advertisements for the sale of stolen documents or hacking tools. This is especially worrying, considering the accessibility of the channels and the promises of high salaries made to those who might otherwise refrain from carrying out such activities.

As a result, this poses a risk of growth in cyber crime rates as these positions are not only openly marketed but they are also available to inexperienced users, making dangerous tools available to anyone.

Hacking Tools and Services

"Wanted for a dark project: Cryptor running on all systems from Windows XP to 10. Bypassing the top AV especially Avast and Defender".

Example:
A cyber criminal's advertisement as posted in a Telegram channel.

The message (top right image) found in a Telegram group is a good example of how someone with no prior experience in malware development can run an entire operation by leveraging Telegram channels. In this case, whoever is behind the advertisement is outsourcing an entire project and is responsible for payment only.

DARK JOB
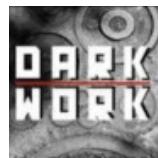
NAME: Виктор Тимур 18+
MEMBERS: 6,873

Description: Info (submit an advert, advert guarantees, guarantor) @dark_job_info_bot)
Main posts: Job hunting, company employees.

DARK WORK

NAME: Трофим Степан
MEMBERS: 762

Description: The Best Dark Net Message Board to Submit an Advertisement.
Main posts: Selling and creating hacking tools.

YP

NAME: Дмитрий Ефим
MEMBERS: 4,425

Description: submit an ad - @banMarket_bot Advertising / Guarantor-@deluxe_R @Rhodesk Chat - @banMarket_chat)
Main posts: Selling schemes and documents.

Examples of illicit communication groups on Telegram

Other illegitimate services in some of Telegram's more crooked channels include forging legal documents such as IDs, passports, banking documents and more. As you can imagine, Photoshop experts and freelance designers are in high demand in these markets.

Next Generation Phishing Kits

One of the most advanced phishing kits, the '[A]pache Next Generation Advanced Phishing Kit', is another example of how easily accessible, and yet highly damaging, tools are promoted and sold on the Dark Web.

Allowing any aspiring cyber-criminal with very little knowledge to run a professional phishing campaign, the notorious [A]pache Phishing Kit instructs those looking to steal credit card details by luring potential victims to fake shopping sites.

At $100-$300, the cost of buying this advanced Phishing Kit was higher than more standard phishing kits. Standard kits usually retail at $20-$50, though some are even free. However, those provide login pages and prompts for personal and financial information. [A]pache's next generation phishing kit, however, provided threat actors with a full suite of tools to carry out their attack. These included an entire back-office interface with which they could create convincing fake retail product pages and manage their campaign.

In order to convincingly persuade their victims that they're shopping at a genuine site, cyber criminals also need a domain that's similar to the targeted brand, for example, www.walmart-shopping.com. Those can be provided as well by illegitimate hosting services on the Dark Web. Once registered, a threat actor is ready to deploy the kit to a PHP and MySQL supported web host, log in to the kit's admin panel and begin configuring their campaign. It's really as simple as that.

To simplify this set up process further, [A]pache made a simple user interface within the admin panel where the threat actor could paste the product URL of the legitimate retailer and the product information would automatically be imported to the phishing page. Cyber criminals could then view their 'products' and change the original prices.

Example:
A fake retail site offered by next generation Phishing Kits for sale on the Dark Web.

*Botnet hire costs **$60** a day and can cause $720,000 in damages.*

Source: "A day attack with DDoS booter cost $60", Security Affairs, March 2016

Bots for Rent

In 2018, the Malware-as-a-Service industry offered additional services.

Some of the year's most prominent malware distributors, giant multi-purposed botnets, now offer their most valuable resources, their bots, for rent. This allows any actor to take part in high-scale global campaigns. For example, Emotet, originally a massive banking malware targeting European banking customers, has shifted its focus and now offers global packing and distribution services, leveraging its self-propagation capabilities. Ramnit, another prominent banking malware, demonstrated similar behavior with a single affiliate campaign, 'Black', which caused approximately 100,000 infections.

Ransomware Goes Agile

Due to the lack of knowledge required, as well as the ease of access and low cost of underground services, cyber criminals are more commonplace. Promoted on Dark Web hacking forums, the GandCrab Ransomware-as-a-Service affiliate program serves as a good example of how amateurs can now profit from the ransomware extortion business as well.

This model is very profitable for the malware authors and allows them to focus on malware development, while delegating the delivery stage to multiple distributors who buy or rent the product as part of an affiliation program.

As a partnership program, GandCrab lets its users keep up to 60% of the ransom revenues collected from victims, while its developers keep up to 40%. In exchange for these fees, the buyers receive the tools to initiate an attack and GandCrab's creators offer support and updates to the ransomware itself. This essentially adds another incentive for affiliates to choose their Ransomware-as-a-Service over competing suppliers. According to our research, GandCrab has dozens of active affiliates (80+), the largest of which distributes over 700 different malware during any given month. As a result, within just two months GandCrab had infected over 50,000 victims and claimed an estimated $300-600K in ransom payments.

The Accessibility of Cyber Crime

As illustrated in our journey into today's world of cyber crime, hiring services, accessing malware, and anonymously selling stolen data has never been easier. It has led to the proliferation of amateurs wanting to get in on the action. From a disgruntled employee to a bored teenager, anyone with a little capital and motivation can become a threat actor.

The convenience of encrypted channels like Telegram allows threat actors and those who wish to take part in cyber crime to communicate in a more secure manner. Sadly, although popular messaging applications have improved the security of user information over the years, they are also being abused by those fleeing from prying eyes, and the law.

In addition, Malware-as-a-Service provides everything a cyber criminal needs to get started and threatens modern organizations in two ways. It creates a demand for better, easier-to-use malicious programs, as malware developers seek to distinguish themselves from any competition. This leads to significant strides in the accessibility and sophistication of malware threats.

Furthermore, Malware-as-a-Service vastly increases the number of individual threats, as it empowers those who would not otherwise have the technical skills to create their own malicious programs. This effectively allows just about anyone to launch a cyber attack.

As a result, and together with the range of services and products now available in today's cyber crime ecosystem, there is a myriad of opportunities to carry out cyber attacks. Indeed, while the number of cyber criminals seems to be rising due to the low technical barrier to entry, the number of cyber attacks on both organizations and individuals is growing accordingly.
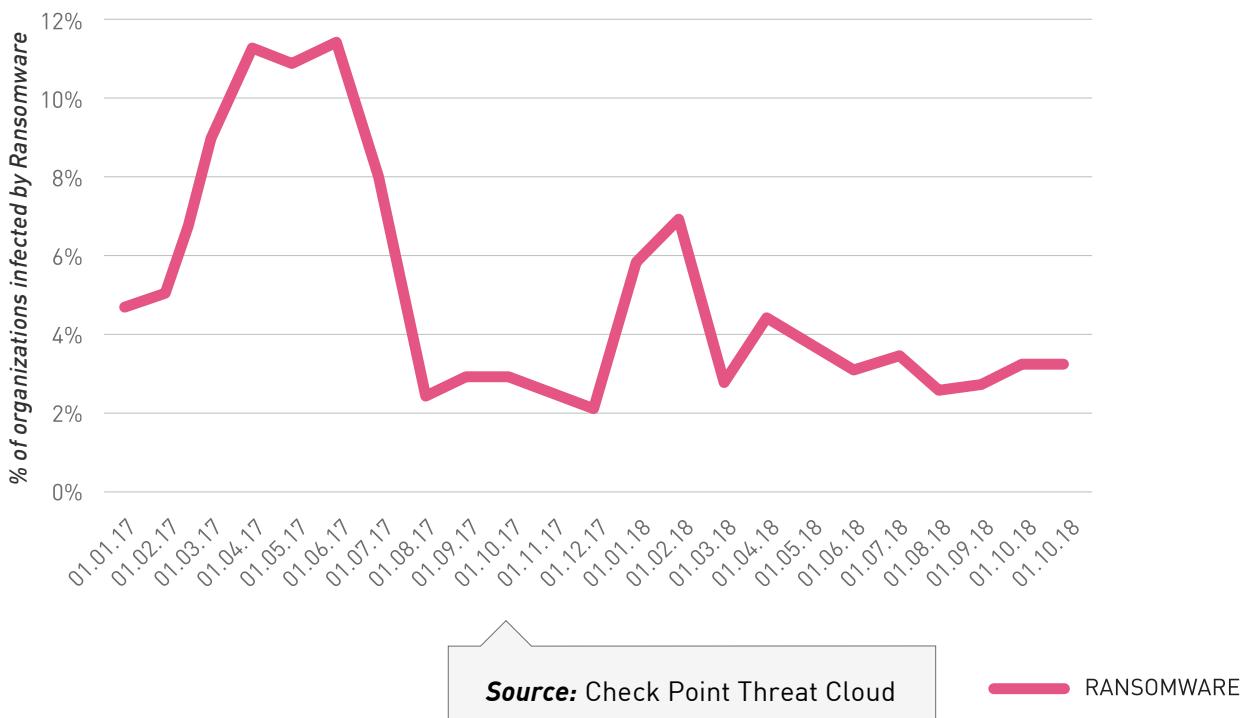
STEALTH-LIKE MALWARE

Ransomware Gets More Targeted

Whereas 2017 was filled with large scale, headline grabbing attacks that served as a wakeup call to both private individuals and businesses alike, threat actors kept a lower profile in 2018. Don't be fooled. When it comes to cyber attacks, out of sight does not mean out of mind. Organizations are under constant attack from the ever-growing number of malware, spreading at higher rates than ever.

In 2017, cyber criminals continued to profit from ransomware attacks. It tapered off, though, towards the end of 2017 and the beginning of 2018. In fact, this trend was so sharp that compared to its heyday just a few months before, it seemed to barely register on the radar at all.

DECLINE OF RANSOMWARE ATTACKS 2017-2018

Source: Check Point Threat Cloud — RANSOMWARE

Despite its decline, ransomware has not disappeared from the cyber threat landscape. Instead, cyber criminals found more lucrative payoffs with targeted ransomware attacks versus the wide-cast style of attacks seen in previous years. Distributing millions of emails with no specific victim in mind gave way to planned and researched attacks on highly targeted victims. The extra effort apparently paid off as targeted ransomware attacks have allowed criminals to earn payoffs in the millions of dollars.

Attacks carried out against the City of Atlanta in March 2018 serve as a good example. Targeted by the SamSam ransomware, cyber criminals were able to extort much larger amounts due to the nature of the victim, the pressure it felt from its citizens, as well as the City's ability to pay the larger ransom amount. Compare this to the non-targeted GandCrab ransomware attacks, for example, where the demands maxed out at about $1,000 per victim, while the SamSam ransomware typically demands as much as $50,000 from its victims.

46% of organizations were hit by ransomware attacks in 2018.

Source: Security Report Threat Prevention Research among IT and Security Professionals, November 2018

The prime goal is detecting the target network's crown jewel, an asset that when shut down can cripple the company's activities within minutes, leaving the victims no option but to pay the demanded ransom to avoid colossal damages which may even result in higher costs. Ransomware operators such as Ryuk even aim at neutralizing victims' backups servers and encrypting them as well.

So far, the targeted approach has proven effective throughout 2018, generating larger revenues for the attackers, and definitely worth the greater efforts. Together with the fact that the premeditated, manual strategy assists the attackers in evading detection, it is a guarantee that this trend is going to stay with us for a while.
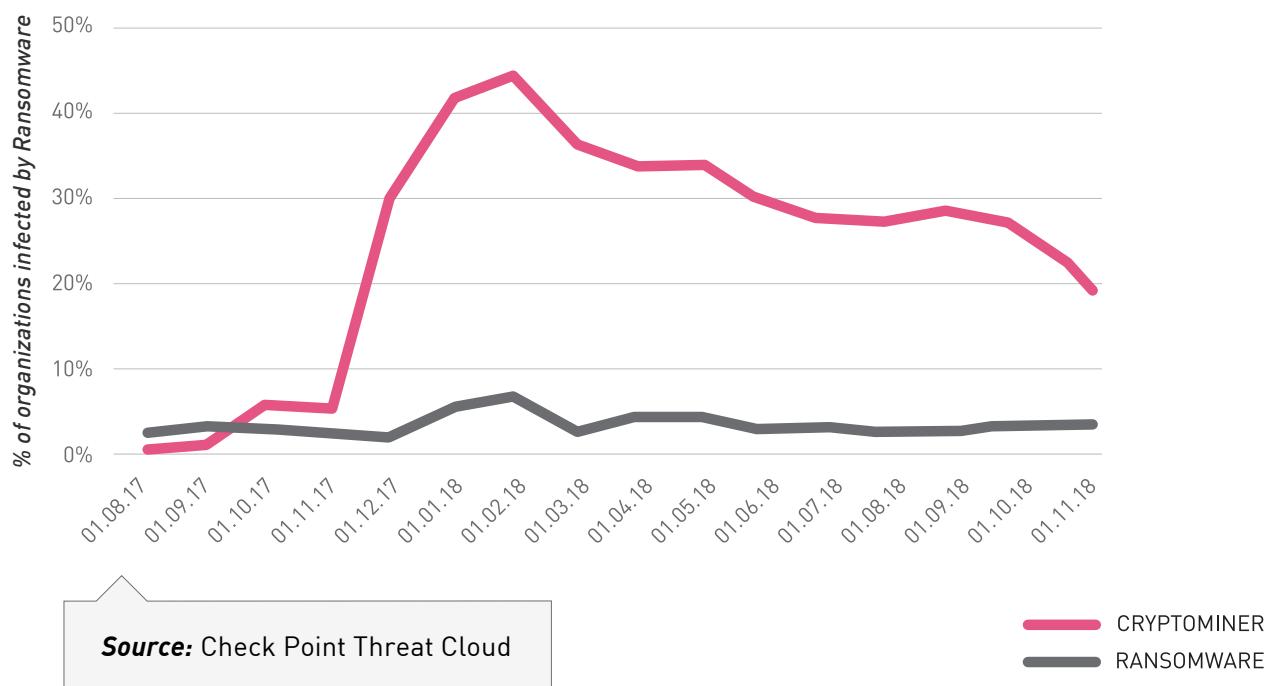
The Rise of the Cryptominers

Meanwhile, as ransomware became more targeted, a new mass-delivered malware took root. Unlike ransomware, though, it was far more stealth-like and did not alert its victims at all. In fact, in contrast to ransomware attacks, its victims were unaware of the attack until they realized the cyber criminals had already harvested their profits.

Enter the cryptominers, a far quieter and more stealth-like malware, yet no less dangerous.

As seen in the graph below, the rise in cryptomining was dramatic. Why was this?

THE RISE OF CRYPTOMINING ATTACKS 2017-2018

Source: Check Point Threat Cloud

CRYPTOMINER
RANSOMWARE

*RubyMiner attempted to exploit **30%** of all corporate networks worldwide.*

Source: Check Point Research blog, "RubyMiner affects 30% of WW Networks," January 2018
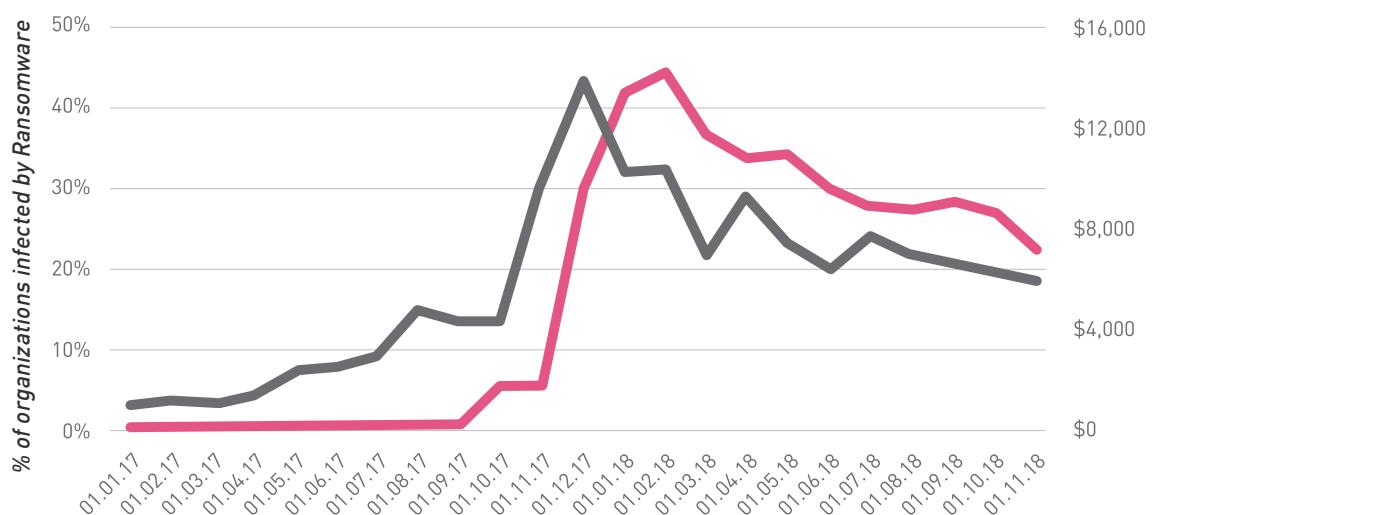
There are several reasons for the increase in cryptomining and the decline in ransomware attacks.

1. Few victims pay the ransom. Despite the high infection rate of large scale ransomware attacks such as WannaCry, for example, only $140,000 was earned in the attack. While this may seem like a lot, it is actually a small payment rate considering that over 400,000 computers were infected.

2. The volatility of cryptocurrency rates. When ransom payments are demanded in Bitcoin, it is crucial for the digital currency to have a favorable exchange rate to the dollar. This means the rate has to be optimal; not too high that the victim will be unlikely to pay, and not too low that it's unprofitable for the attacker. In addition, while it is still very much a valuable currency, it has dropped hugely since mid-2017, making ransom payments much less attractive when they're paid.

3. Cryptojacking malware is more effective. Ransomware is highly visible and triggers alerts inside an organization. They may well be infected once, pay or not pay, but then they will take measures to keep it from happening again. Cryptojackers are stealthy, flying under the radar. They do not set off alerts or alarms and often their presence is unknown, which allows the attacker to hijack their target to generate income for as long as they wish, unbeknownst to their victims.
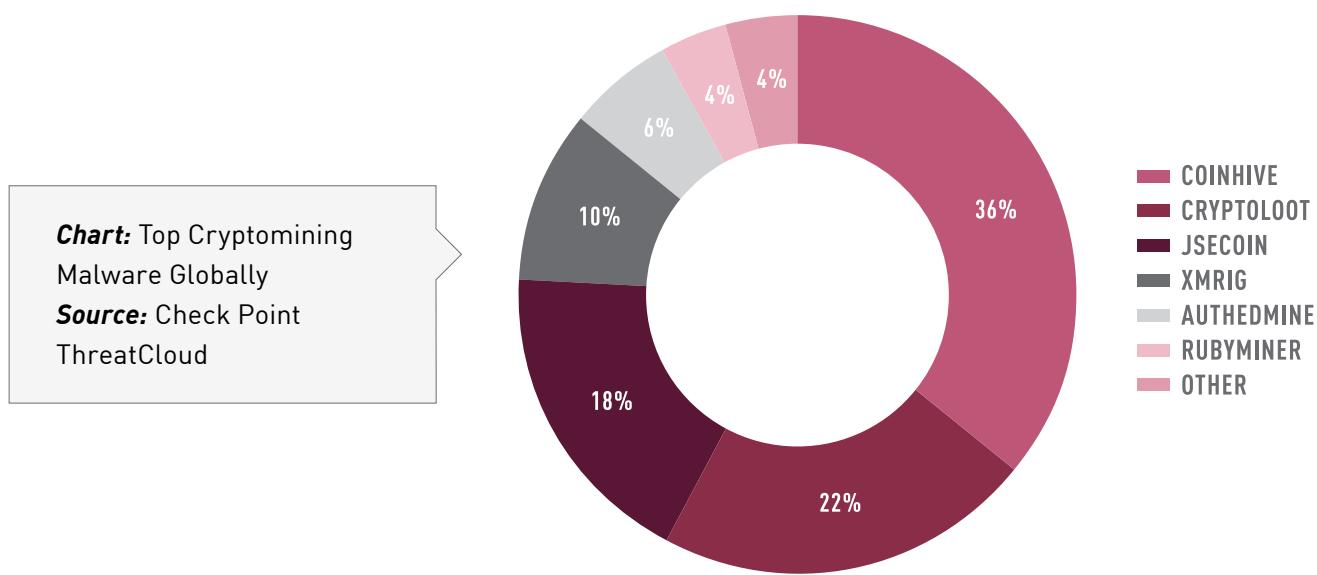
In addition to the above, the rapid rise in cryptocurrency value was a major factor in the use of cryptojackers to harvest this lucrative currency for malicious actors. Furthermore, the correlation between the rise, and subsequent drop, in cryptocurrency values and the rise of cryptomining attacks is reflected clearly in the below chart.

Source: Check Point Threat Cloud and CoinMarketCap.com

CRYPTOMINER
PRICE OF BITCOIN

CRYPTOMINERS' IMPACT ON ORGANIZATIONS VS. PRICE OF BITCOIN

Cryptojacking has thus allowed criminals to switch from a smash-and-grab approach, which usually turns out to be a one-hit-wonder strategy, to a prolonged clandestine operation. No longer do threat actors need to deal with uncooperative victims who do not pay up, or those who have a data back-up, rendering the attack ineffective. Instead, the change in strategy is highly effective to enable them to slip through the cracks of an organization's security posture, open a door for future attacks, and fundamentally change the nature of attacks and how organizations need to defend against them.

Chart: Top Cryptomining Malware Globally
Source: Check Point ThreatCloud

- COINHIVE
- CRYPTOLOOT
- JSECOIN
- XMRIG
- AUTHEDMINE
- RUBYMINER
- OTHER

As seen in the following chart, the most prominent cryptomining malware dominating the Global Top Cryptominers Malware list are Coinhive, CryptoLoot and JSEcoin. These malware have also kept their place at the top of the list since 2017.

These popular web-based cryptominers are easily integrated into websites, willingly by website owners as well as unknowingly by threat actors who utilize those websites' high traffic to generate cryptocurrency. Taking a different approach, the RubyMiner campaign targeted unpatched Windows and Linux servers, and maintained its high rank during the first half of 2018. As revealed by Check Point researchers last January, RubyMiner attempted to exploit 30% of all corporate networks worldwide to mobilize powerful servers into its operators' mining pool.

The Evolution of Cryptominers

Since their creation, cryptominers have come a long way. Evolving from simple website compromise, cryptominers have been observed this year spreading through Facebook Messenger, YouTube ads and Google Play, while infecting tens of thousands of websites, personal computers and powerful severs such as Jenkins. In 2018, though, cryptominers upgraded and vastly improved their capabilities, becoming more sophisticated and even more destructive.

Motivated by a clear interest in increasing the percentage of computational resources leveraged, and crafted to be even more profitable, cryptominers today target anything that could be perceived as standing in their way. As a result, we have witnessed cryptominers targeting SQL databases, industrial systems, nuclear power plants, and, most worryingly, cloud infrastructure. Cryptominers have also evolved recently to where they can exploit high-profile vulnerabilities while evading sandboxes and security products in order to increase their infection rates.

The mobile arena was not deprived of cryptomining attacks either. Last April, the Android Cryptominer, dubbed HiddenMiner, targeted numerous devices, continuously mining Monero until the devices' resources were drained. Mobile miners have even managed to penetrate Apple's App Store, with a malware that steals victims' login credentials to cryptocurrency wallets.

Adding more fuel to the fire, since the beginning of 2018 a variety of new attack methods have surfaced. One such new attack leverages the potential with cryptocurrency trading systems. Among others, these methods include virtual wallet and credential theft, cryptocurrency transaction maneuvering, as well as ICO (Initial Coin Offering) scams that lure victims to invest in a fake premature cryptocurrency.

> *Cryptominers infected **10x** more organizations than ransomware but only **1 in 5** IT Security Professionals are aware they were affected.*
>
> Source: Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Moreover, other malware families have begun integrating mining capabilities into their arsenal. Ransomware, as well as prominent Banking Trojans, including Panda and TrickBot, are now targeting not only bank accounts but also cryptocurrency wallets and trading system accounts, adding features of cryptocurrency credential theft to their arsenal.
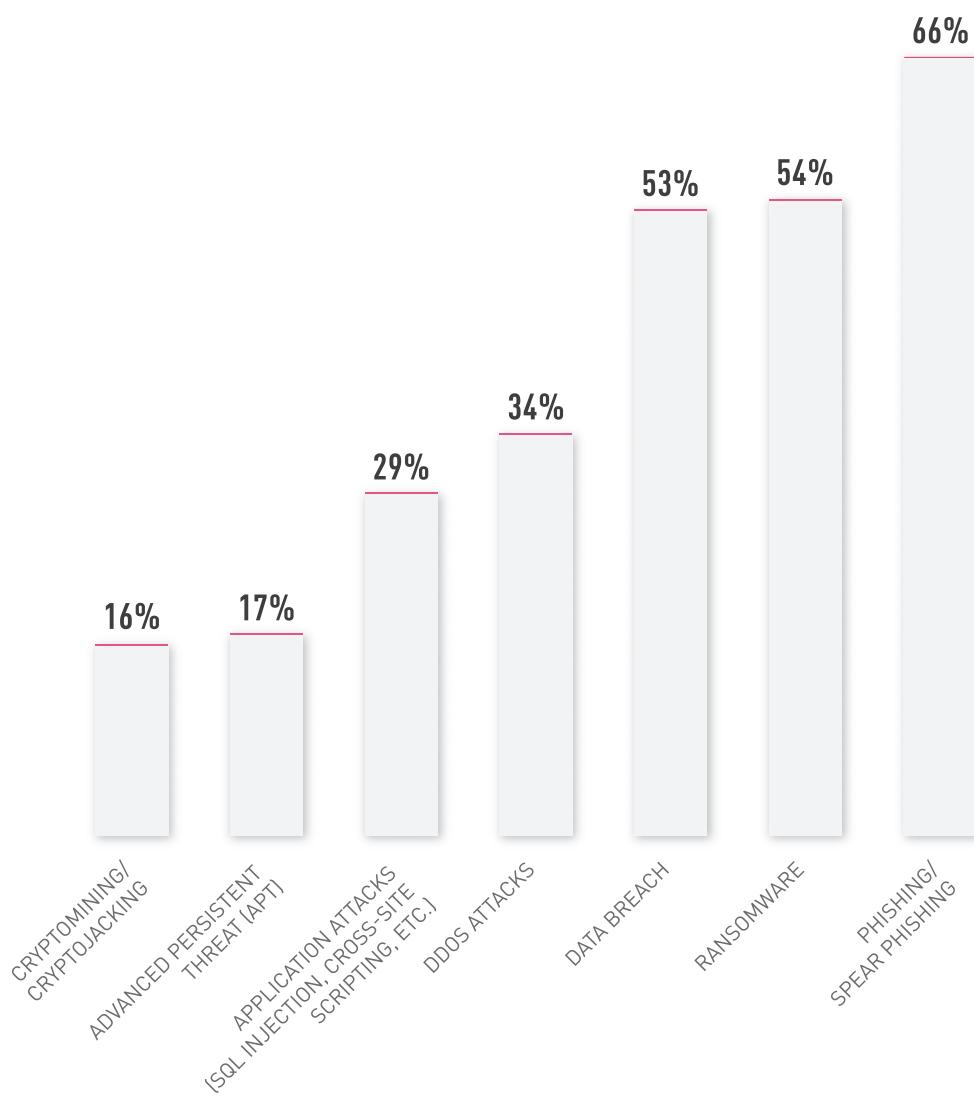
*Only **16%** of organizations are concerned about cryptomining attacks.*

Meanwhile, the world sleeps.

Despite exposing this conspicuous threat, organizations have been less responsive in defending against covert attacks. This is concerning as cryptojackers can easily act as back doors to launch other malware types. Banking Trojans can lie undetected for months, if not years, before being detected.
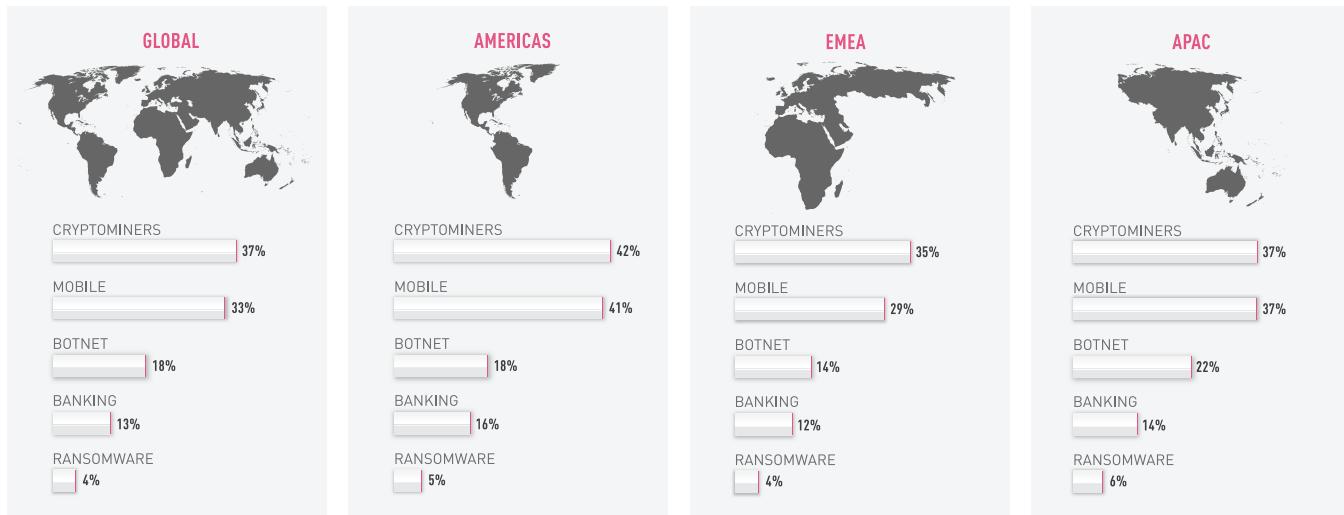
WHICH OF THE FOLLOWING TYPES OF CYBER-ATTACKS DO YOU CURRENTLY SEE AS THE GREATEST THREATS TO YOUR ORGANIZATION?

| Attack Type	Percentage
CRYPTOMINING/CRYPTOJACKING	16%
ADVANCED PERSISTENT THREAT (APT)	17%
APPLICATION ATTACKS (SQL INJECTION, CROSS-SITE SCRIPTING, ETC.)	29%
DDOS ATTACKS	34%
DATA BREACH	53%
RANSOMWARE	54%
PHISHING/SPEAR PHISHING	66%
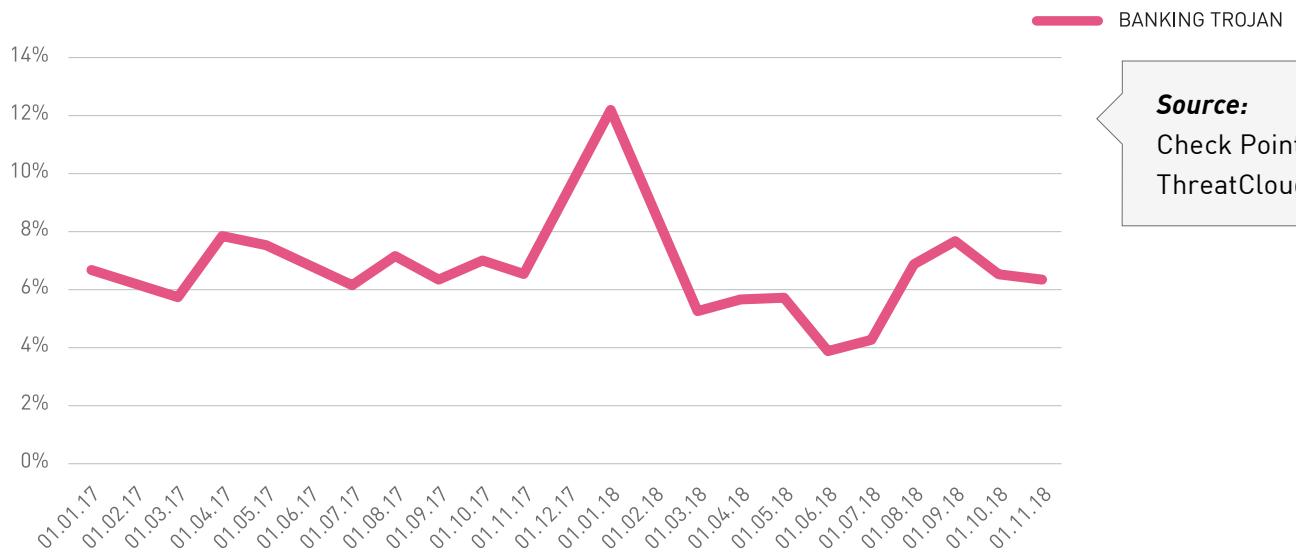
The Rise of Banking Trojans

Banking Trojans are helping cyber criminals to commit the perfect crime, stealing money from the accounts of unsuspecting victims, virtually untraceably and with minimal risk. As such it's no surprise that Banking Trojans are another prevalent type of malware. As seen in the map on the next page, in Asia-Pacific countries they far outstripped ransomware in the number of attacks.

Map: The Most Prevalent Malware Type Across World Regions

GLOBAL

CRYPTOMINERS	37%
MOBILE	33%
BOTNET	18%
BANKING	13%
RANSOMWARE	4%

AMERICAS

CRYPTOMINERS	42%
MOBILE	41%
BOTNET	18%
BANKING	16%
RANSOMWARE	5%

EMEA

CRYPTOMINERS	35%
MOBILE	29%
BOTNET	14%
BANKING	12%
RANSOMWARE	4%

APAC

CRYPTOMINERS	37%
MOBILE	37%
BOTNET	22%
BANKING	14%
RANSOMWARE	6%

PERCENTAGE OF ORGANIZATIONS IMPACTED BY BANKING TROJANS IN THE LAST TWO YEARS
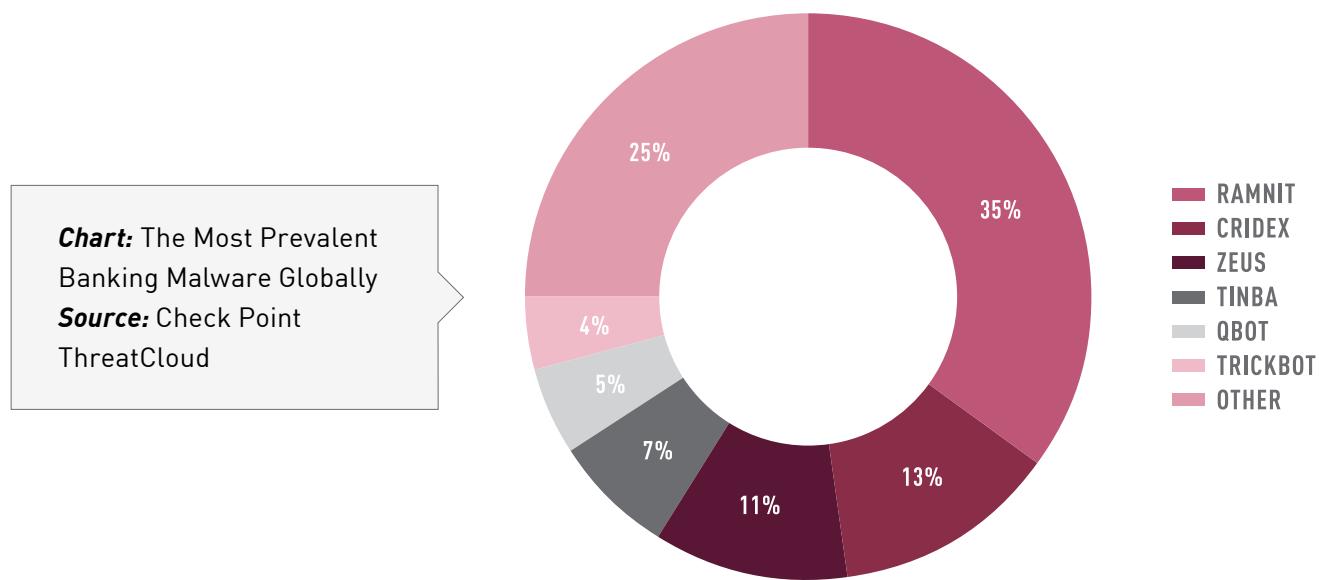
— BANKING TROJAN

Source: Check Point ThreatCloud

Banking Trojans are also among the stealthiest of all malware types. After a Trojan infects a user's PC or web browser, it will lie dormant and wait for the user to visit their online banking website. When the user does this, the Trojan is activated and uses keylogging to steal the victim's username and password and send it secretly to the criminals behind the attack. These criminals can then log into the user's bank account and transfer funds, usually through a complex network of transactions to cover their tracks.

Many Trojans can perform sophisticated Man-in-the-Browser (MiB) techniques such as web injections or redirection mechanisms. With this attack type, the Trojan's actions in real time are disguised, subtly changing what the user's browser displays so that it appears as if transactions are proceeding normally while the theft is happening. Other tactics include displaying fake warning pages that ask a user to re-enter their login information, or showing users a fake logout page while keeping them signed into their accounts. The aim is to conceal the Trojans' actions from users for as long as possible, to enable the criminals to continue stealing from their accounts.

In addition, Banking Trojans are transitioning to mobile. These typically involve malware which displays fake overlays on the mobile device's screen when a user tries to use an application. The overlays look the same as the login pages of banking apps, and can steal login credentials, or intercept SMS messages from the user's bank, enabling the criminal to harvest mobile transaction authentication credentials.

Chart: The Most Prevalent Banking Malware Globally
Source: Check Point ThreatCloud

- RAMNIT
- CRIDEX
- ZEUS
- TINBA
- QBOT
- TRICKBOT
- OTHER

Ramnit is the most prominent banking Trojan of the past year. It first appeared in 2010 and has remained active ever since. Ramnit's popularity is in line with the exposure by Check Point researchers of a massive new 'Black' campaign based on the banker. The campaign turned the victim machines into malicious proxy servers and resulted in over 100,000 infections. Shortly after the 'Black' campaign was shut down, a new Ramnit campaign emerged, distributing the AZORult info-stealer and downloader, via the RIG and GrandSoft Exploit Kits.

TrickBot is another dominant banking Trojan widely observed in 2018 that reached the top of the global, Americas and EMEA rankings. As an advanced malware based on plugins, TrickBot is constantly being updated with new capabilities, features and distribution vectors. This enables TrickBot to be a flexible and customizable malware that can be distributed as part of multi-purpose campaigns. In 2018 we witnessed TrickBot being delivered via multiple global spam campaigns, as well as creatively cooperating and sharing profits with the IcedID banking malware.

CLOUD IS YOUR WEAKEST LINK

Few are surprised by the popularity of the cloud. It offers flexible computing options at a fraction of the cost and time. Organizations can conveniently improve data storage and server processing or use Software-as-a-Service (SaaS) products.

Cloud computing has become an integral piece of today's IT infrastructure. Its 'try before you buy' and 'pay as you go' models provide organizations with the ability to test the technology, and integration with the cloud is fast and usually requires virtually no organizational downtime.

However, much like other emerging technologies, the cloud can be abused. So it's imperative to know its vulnerabilities, especially the holes in security.

91% of organizations are concerned about cloud security.
Source: 2018 Cloud Security Report, Dome9

Cloud's Weakest Points

In brief, the main security challenges with the cloud and the services it provides include:

External Exposure – Cloud services are typically accessed from any location and any device. All that's needed is an internet connection. While ease of access can boost company agility, services running in the cloud versus those on premise are more likely to be breached.

Only Default Security – Typically, cloud services are provided with only basic security which allows unrestricted open internet file sharing. This vulnerability can open the door to any number of malware attacks.

Cloud services are vulnerable across three main attack vectors:

1. Account Hijacks – Gaining unauthorized access to an individual or organization's email or computer account for malicious purposes. In a Check Point survey, Account Hijacks were the biggest concern amongst customers and partners.

2. Malware Delivery – Propagation, especially through in-app file sharing services, such as Box or OneDrive cloud apps, in order to commit a variety of cyber crimes.

3. Data Leaks – Whether intentionally or unintentionally, data leakage occurs with the seamlessness of sharing information with cloud services.

Due to the cloud's security challenges, the Check Point Incident Response team is seeing an increase in security breaches with cloud services, both with SaaS and Infrastructure-as-a-Service (IaaS) models.

18% of organizations experienced a cloud security incident in the past year.

Source: 2018 Cloud Security Report, Dome9

Despite the upward trend in security breaches with the cloud, however, 65% of IT professionals still underestimate the damage they can cause. The obvious concern is that organizations are not taking cloud security seriously enough. The breach of sensitive data held in the cloud is a huge risk for an organization, and threat actors know it. The rate of cyber attacks against cloud-based targets is growing, and with little sign it will slow down.

When asked why they may not be securing their cloud assets, a full 30% of survey respondents believe security is the responsibility of the cloud service provider. This negates recommendations that cloud security follow the Mutual Responsibility model shared by the cloud provider and the customer.

65% of IT professionals underestimate the damage caused by attacks on the cloud.

Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Whether an organization suffers a financial, informational or reputational loss, the overall effect of a cloud attack can be devastating to a business. To understand the potential damage of a cloud attack, let's take a closer look at Account Hijacks.

1 in 3 IT Professionals still consider security to be the responsibility of the cloud service provider.

Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

49% of organizations are increasing their cloud security budget in the next year.

Source: 2018 Cloud Security Report, Dome9

How Do Account Hijacks Occur?

To take over an account, the attacker must first gain the victim's trust. The most common method to achieve trust is to use social engineering. Phishing attacks are the most common method for stealing log-in credentials from unsuspecting users.

Here's how it typically works. The cyber criminal sends an "urgent" email from Microsoft support or another service provider requesting a response from the victim. A click on a link in the email will allow the attackers to hijack the victim's account. We've all seen these phony emails, yet people still fall prey to the scheme.
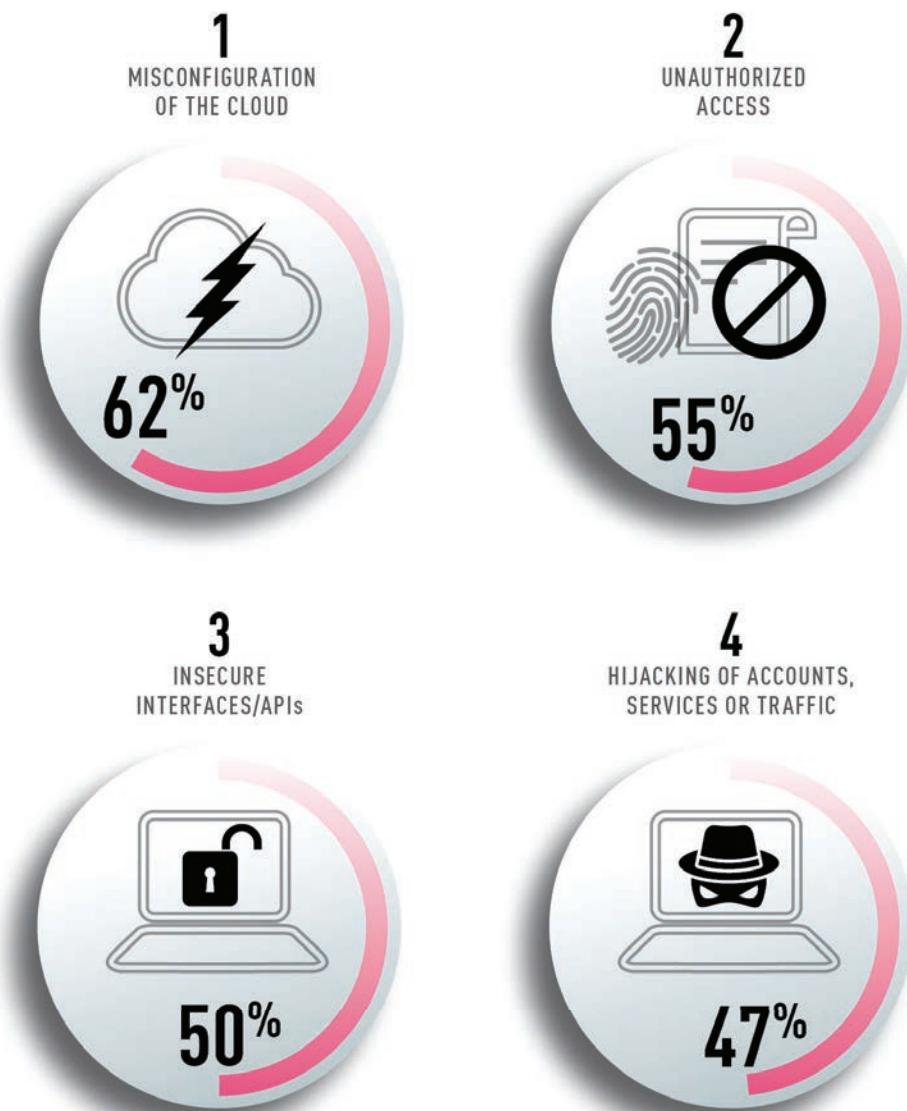
After proceeding to click on the link and enter their log-in credentials when prompted, the unsuspecting victim may also receive a push notification by SMS to his mobile device. This is mainly used to add an extra element of authenticity to the phishing scam, which the victim, having already trusted the initial source of the attack, will also likely approve and continue as instructed. Of course, as the victim unknowingly provides these sensitive log-in details to the attacker, the attacker uses them to gain access to the victim's SaaS account, for example, helping themselves to the private and confidential information stored there.

47% OF ORGANIZATIONS THINK ACCOUNT HIJACKS ARE THE BIGGEST THREAT TO THEIR CLOUD SECURITY.

Source: 2018 Cloud Security Report, Dome9

Figure 1: The Top 4 Security Threats Facing
Public Cloud as Perceived by IT Professionals
Source: 2018 Cloud Security Report, Dome9

1
MISCONFIGURATION
OF THE CLOUD

62%

2
UNAUTHORIZED
ACCESS

55%

3
INSECURE
INTERFACES/APIs

50%

4
HIJACKING OF ACCOUNTS,
SERVICES OR TRAFFIC

47%

62% of IT Professionals are most concerned about Data Loss or Leakage.

Source: 2018 Cloud Security Report, Dome9

***67%** of those who experienced a cyber attack rated its impact as medium or high.*

New Threats Transition to the Cloud

Along with a wide range of benefits, the cloud infrastructure introduces a new, fertile and attractive environment for attackers who crave the enormous amount of available computing resources and sensitive data it holds. Indeed, 2018 has brought us various sophisticated techniques and tools exploited against cloud storage services.

Several cloud-based attacks, mainly those involving data exfiltration and information disclosure, derived from poor security practices. Credentials left available on public source code repositories or the use of weak passwords are just some examples of how threat actors gained access and control over unprotected resources hosted in the cloud.

Another rising threat taking the cloud environment by storm are cryptominers, targeting the cloud infrastructure in order to exploit the vast computational power it presents and generate huge profits for cyber criminals.

Application Programming Interfaces (APIs) that are used to manage, interact and extract information from services have also been a target for threat actors. The fact that cloud APIs are accessible via the Internet has opened a window for threat actors to take advantage and gain considerable access to cloud applications.

As time passes, threats to the cloud will continue to evolve. Attackers will continue to develop more and more tools for their cloud playground, pushing the limits of the public cloud services. Indeed, as new cloud exploitations emerge, there is no doubt that the next attack is already taking place.

This introduces a whole new environment in which victims are exposed to more attack vectors that could be exploited by threat actors trying to find the weakest link that leads to a person or organization's data.

Required Prevention Solutions

In order to prevent such phishing attacks, an in-depth security solution is needed to detect such phishing attempts. A trusted prevention solution can scan the content of emails, evaluate the trustworthiness of the sender, and maintain specially researched keywords and a list of other such variables.

Whereas many solutions perform such scanning detections on traffic received from outside of an organization's network, what they fail to detect, however, is traffic already received from within the network. In fact, it's vital for a solution to scan internal emails from within an organization as phishing scams can be easily spread from an already compromised account.

A solution that performs internal scans must also work in harmony with the existing security of the cloud provider and perform security checks from within the email cloud service. This is something that is not currently done by most of the current solutions available in the cyber security product solutions market. Such security features that come with the cloud service itself are often shut down.

Before a prevention solution is adopted, it's vital to ensure your IT environment is clean. This can be accomplished by your cloud security solution's anomaly monitoring that monitors and detects anomalies such as forwarding rules, i.e., a compromised account sending malicious emails to external users.

In order to prevent account takeovers, any device granted access to the SaaS platform must be clean and compliant with the security policy of the company to prevent devices with malware or OS exploits from logging in.

Of course, detection by itself is never sufficient. Prevention is preferred so your cloud security solution protects the last line of defense in your network security architecture. By applying identity protections, your solution can prevent unauthorized access to accounts. Such identity protections must be able to deflect phishing attempts and yet still be easy to deploy with zero friction to users.

THE MOBILE AND IoT WEAK SPOTS

MOBILE'S WEAK SPOT

Mobile security is a major security concern these days – and for good reason. Nearly all employees now routinely access corporate data from smartphones, and the challenge is to keep sensitive information out of the wrong hands.

The main security challenge with mobile devices is that they are easy to overlook. Today's smartphones are mobile computers that have been pressed into action by businesses throughout the world. This has made network security a bigger and more diverse challenge. The use of mobile devices and apps has also added a new range of attack vectors and additional security challenges for IT.

The proliferation of personal smartphones and tablets in the workplace exposes your company to increased risks. While a breach of personally identifiable information or payment card data is certainly a top concern for many businesses, there are other risks that organizations need to consider. Chief among these are the cost of breaches and responding to incidents, the potential damage to brand reputation, and a loss of competitive advantage if valuable trade secrets or intellectual property become public knowledge.

Mobile systems, the networks they connect to, and the applications they run can all be exploited to steal sensitive information such as documents, calendar appointments, email messages, texts, and attachments. As Check Point Research illustrated via announcements of threat actors taking advantage of the World Cup last year to spy on government agencies through malicious mobile applications, cyber criminals can use the smartphone in other ways. A device's microphone and camera can be used to spy on their targets, and then send recordings to a secret remote server. They can also capture user names and passwords as users log in to corporate systems containing sensitive data.

With this in mind, let us take a closer look at the four major threats to mobile security in today's corporate environment.

***59%** of IT Professionals do not use Mobile Threat Defense.*

Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Trojans and Malware

Social engineering scams remain astonishingly effective. In fact, trickery is just as troubling on the mobile front as it is on desktops.

Many mobile users are unaware of the dangers and they are far too trusting when clicking on links they receive via SMS or social media apps such as WhatsApp. This can often lead to the device getting infected by a wide array of mobile malware.

Trojans, for example, carried within an app or installed through an unsecured network connection, infect a device with malicious code that may conduct surveillance by eavesdropping and recording conversations, extracting call logs, tracking locations, logging keyboard activity, and collecting passwords.

*Only **9%** of IT Professionals consider threats on mobile a significant risk.*

Source: Check Point Security Report Threat Prevention Research among IT and Security Professionals, November 2018

Fake Apps

Malicious apps can take control of mobile devices and although the app may not appear to be malicious, users may not notice or understand the permissions they grant during installation. What's more, even popular apps can be reverse-engineered and injected with malicious code, and then uploaded to an app store under a different name.

Criminals can also create seemingly authentic copies of apps that include similar icons, descriptions, screenshots, and even user reviews. But, of course, they don't work as intended. Instead, victims receive a malicious payload, such as a

subscription to an expensive texting service or a stealthy surveillance tool. Indeed, malicious apps can enable a host of activities, such as remotely seizing control of the device's camera and microphone to spy on users and their surroundings. Such were the apps the Check Point Research team came across on multiple occasions throughout 2018, proving just how prevalent these highly invasive apps are.

Man-in-the-Middle Attacks

Man-in-the-Middle attacks can eavesdrop, intercept and alter traffic between two devices. You believe you're interacting with a known and trusted entity, but in fact an attacker is copying credentials, snooping on instant messages, or stealing sensitive information. The familiar alert and warning signs on PCs and laptops are far more subtle and easily overlooked on mobile devices. Small screen sizes can also hide web addresses, making it harder to validate the address the browser is pointing to.

Public WiFi hotspots, which are convenient for internet access, are easy to fake. An attacker can create a spoofed WiFi network, or eavesdrop and alter a legitimate network's encrypted communications by using spoofed certificates or downgrading the communication link so that it is no longer encrypted. The attacker can then intercept communications, alter data in transit or install a Trojan.

System Vulnerabilities

Each version of an operating system for a mobile device offers vulnerabilities that cyber criminals can use to launch attacks. Unfortunately, as new versions are notoriously late to market, critical security updates might not make it through testing for weeks or even months, leaving users exposed.

Android is particularly vulnerable. The thousands of different types of Android smartphones and tablets are not updated consistently and at the same time. Most devices are still using older Android versions in which vulnerabilities have not been patched.

Apple's iOS, on the other hand, is less vulnerable because Apple makes only a handful of different devices and consistently prompts users to update them. However, the number of attacks carried out on Apple's iOS is increasing due to the more sophisticated types of attacks that are carried out on this operating system.

IoT's WEAK SPOT

There is no doubt that today's world is becoming ever more interconnected, so much so that we should perhaps no longer talk so much about the Internet of Things (IoT) but rather the Internet of Everything. Whether it is agriculture, manufacturing or healthcare, almost every industry is embracing the proliferation of smart devices available to them to get deeper insights and more data to aid them in their work.

IoT devices make our lives easier. Smart home technology, for example, can help users improve energy efficiency by enabling them to turn on (and off) lights and appliances with the tap of a touchscreen. Some connected devices, such as smart medical equipment and alarm systems, can even help save lives.

Take medical devices, for example. This subset of IoT belonging specifically to healthcare and its supporting technologies, the Internet of Medical Things, is made up of smart, connected devices that automatically collect, process, and digitally relay information from the physical world through a shared network infrastructure.

Networked medical devices give healthcare professionals the ability to be much more accurate with their treatment regimens, far more efficient in administering care, and way quicker collecting and responding to biomedical information.

> *There will be an estimated **125 million** Healthcare IoT devices in 2019.*
>
> Source:Statistica.com, Estimated Healthcare IoT Device Installations

As a result, IoMT technologies are currently exploding, both in terms of their popularity and capabilities. Put simply, IoMT is redefining the practice of medicine. And while this new frontier of medicine is very exciting and hugely promising, it is not without its problems.

There are also serious security risks associated with IoT technology. As the IoT ecosystem expands, so does the attack surface for cyber criminals. In other words, the more we rely on connected technology in our day-to-day lives, the more vulnerable we are to the cyber threats that are increasingly tailored to exploit vulnerabilities and security design flaws in IoT devices.

This presents a daunting challenge for cybersecurity professionals. They must not only protect their own devices, but they must also defend against threats targeting external machines that might connect to their IT networks as a whole.

The current IoT landscape then can be compared to the early days of the internet, when viruses, worms, and email spam plagued users. Many companies raced to join the internet 'gold rush' without necessarily considering the importance of internet security.

The Security Issues

While the concerns regarding medical IoT devices may be more particular, the major malfunction with IoT device security as a whole lies in the fact that they are usually poorly coded. This is mainly due to the device manufacturers' pursuit of profitability over user security. So when insecure devices are connected to the open internet, they become the route for a disaster waiting to happen.

For example, cyber criminals can hack insecure security cameras or other smart devices and use them to access the rest of an organization's corporate or individual's home network. Alternatively, thousands of these insecure IoT devices can be combined to form a zombie botnet army to launch devastating DDoS attacks.

In addition, IoT devices themselves can be exploited to give threat actors unauthorized entry, as illustrated by Check Point's research into LG automatic vacuum cleaners that showed how a hacker could take over the device's camera to spy on users. However, it is often forgotten that the data collected by these devices is usually stored in the cloud. In this respect, as shown by recent research into drones, an attack on the IoT-Cloud infrastructure could leave photos and film footage taken by the drone devices exposed to theft. This is just one example of how sensitive data stored in the cloud could be breached, though with so much data collected by IoT devices as a whole, organizations should be extremely cautious about how that data is stored.

Another hurdle IT professionals face with regard to network compliance is the sheer lack of regulation surrounding the entire IoT ecosystem. Though there may soon be IoT regulations in the state of California, which is leading the way in the area of IoT regulations, it is currently the responsibility of IT professionals to audit devices for compliance. Regardless of these regulations, there will continue to be millions of devices still in use from before these new requirements come into force, which will still have a large potential for exploiting the weaknesses in these outdated devices.

2019 CYBER THREAT PREDICTIONS

Cyber Crime

Whereas in the past we saw attacks causing mass damage across hundreds of thousands of targets simultaneously, it would be fair to say that the threat actor's mind is turning more towards far more specific closely chosen and more lucrative targets. As a result, we predict the biggest threats to organizations in 2019 will continue to be motivated by the ability to make a profit.

As the cyber crime industry matures, we expect to see similar types of attacks continue, yet bring in a higher return for their creators. In the case of ransomware this would mean attacking assets where threat actors can demand a higher ransom and with a higher likelihood of the victim making payment; cryptomining targets assets that offer greater CPU capacity and therefore faster mining with a smaller footprint. This would mean cloud infrastructure is under threat due to the scalable and agile features they offer.

Targeted phishing attacks, often in the form of whaling, that often rely on natural human error will likely become more prevalent and a more popular attack strategy. In addition, we expect to see more attacks using cloud infrastructure and IoT devices not only as direct targets themselves but also as the main point of entry due to these devices often being less secure than networks, endpoint and on premise data centers, and offering attackers an easier way in.

Mobile

An organization's fleet of company-issued and BYOD mobile devices continues to be overlooked as far as security is concerned. As a result, we believe that not only will mobile malware become more prolific in the year ahead but also that an all-in-one mobile malware that combines capabilities for multiple purposes will become more prevalent. This includes the combination of banking Trojans, key-loggers and ransomware that will give attackers multiple options from which they can profit from an infected device.

Rates of banking malware that steal two-factor authentication or create a fake bank credentials window were steadily increasing in 2018, and will continue to grow, replacing malicious cryptomining apps as the main mechanism for malicious profit.

Cloud

The scalability of the cloud allows organizations to do things they could only imagine with their own data centers. However, as the level of understanding about securing the cloud remains low, we can expect to see an increasing number of attacks aimed there to specifically achieve account takeovers.

We expect to see threat actors targeting specific company departments and employees, also known as spear phishing, in order to reap more lucrative rewards. For example, account payables/receivables mailboxes are tempting to hack as they offer an opportunity to manipulate invoices, transfer funds or send intellectual property to the attacker. All this can be achieved from a trusted and genuine hijacked email account.

While more organizations move to the cloud, awareness that they are still responsible for the security of data held there is still lagging. While it is true that there is less control over the cloud, this doesn't mean there is less to do from a security perspective. For while the cloud may be somewhat more secure against attack methods that were used in the past, this means we are likely to see attacks more focused on the business logic of the cloud.

49% of organizations will increase their cloud security budget in the next year.

Source: 2018 IT Professionals Security Report Survey

Network

The introduction of GDPR in May last year helps address this issue of data theft by protecting the rights of EU customers. As a result of this step, we may well see other global authorities following suit and introducing further regulations to protect data privacy.

Cryptojacking also proved to be a profitable form of attack in 2018. With so many organizations still unaware of its potentially crippling effect, it's likely we will continue to see cryptojackers prevalent across IT networks. What's more, we may well see cryptojackers being used against more lucrative targets and more low profile methods to allow for longer infection times.

Artificial Intelligence

When more and more decisions are being made by artificial intelligence and machine learning algorithms, it is only a matter of time before threat actors turn their attention to the potential for havoc these mechanisms hold. After all, we have already seen how voting patterns can be manipulated by big data and the algorithms used by social networks.

AI is gradually being incorporated into many industries, often disrupting them to make them more automated. The Finance sector, for one, is increasingly using it to facilitate insurance policies and claims. Were a threat actor, either independent or nation-state backed, to target these mechanisms and manipulate the results they produce, the fallout could be catastrophic. As the 2008 economic crash reminded us, the financial system is fragile. When sensitive decisions are being made by mere algorithms, it is these decision making systems themselves that could well become a target of attack. Indeed they serve as an attractive target for threat actors potentially manipulate the manner in which highly impactful decisions are made.

IoT

The main issues associated with insecure IoT devices as far as consumer privacy and safety is concerned, is that standard IoT devices, from wireless routers to smart fridges and toasters, may be undermined by vulnerabilities within them.

For enterprises though, IoT devices will remain the weakest link in security and we predict that more attacks will make use of them as their point of entry as well as them being the targets in and of themselves. This is due to them being harder to secure and yet are being adopted into the corporate infrastructure at an ever increasing rate, thus enlarging the attack surface.

As a result, we expect more authorities will follow the example set by California which recently introduced a new state law to improve cyber security. By 2020, in order to sell products in California, manufacturers will need to ensure that devices, such as home routers, have a unique pre-programed password or an enforced user authentication process as part of the set up. Default passwords such as 'password' or 'default' will be deemed weak and in breach of new state law. This positive step should encourage manufacturers to produce products with greater built-in security that can then be rolled out to the wider global market.

Nation-State

In the last few years governments have become highly concerned by cyber threats that target critical infrastructures, such as the power grid. As a result, many countries have formed entities such as CERTs to oversee their national cyber security (committees, agencies, authorities, etc.).

However, CERTs are more of an advisory nature as well as serving to support regulations and investigations. This can leave governments and their citizens exposed. And if citizens do not think the digitally connected world is safe, this could weaken many world economies.

While we have yet to see non-state actors use cyber attacks to inflict mass damage and even loss of life, nation-states will most certainly continue and increase their use of cyber warfare. Critical infrastructure will continue to be a target of choice though international cyber espionage will offer greater rewards for those who manage to successfully carry it out, and greater losses for those who fail to protect against it.

Citizen data privacy will become an even hotter topic of contention, especially due to such data being well proven to impact so greatly on voting patterns and election outcomes. With the analysis of big data now a mainstream discipline, the protection of that data will continue to be paramount in order to avoid fraudulent activity and the abuse of it.

PROTECTION RECOMMENDATIONS

A Unified Security Architecture

Today's cyber-attacks are more deceptive than ever. They can shift seamlessly between vectors, while targeting organizations of all sizes. Countering aggressive threats requires an advanced security strategy.

A holistic approach to your security architecture is what's required to tackle known and unknown threats across your organization's entire IT network. You need to take a prevention-first view to block attacks before they happen, not just detect them. By doing so, your organization can remain one step ahead of today and tomorrow's cyber threats.

A unified security architecture is the recommended solution. By implementing a solid, unified and interconnected architecture, your business can eliminate single points of failure by providing the necessary strength and resiliency to maintain operations and security under any circumstances. Anything less exposes your organization to infiltration due to communication gaps with disparate systems that fail to integrate and communicate with each other.

When being able to monitor mobile, cloud and network, and leverage real-time threat intelligence from a shared intelligence platform, you can dynamically and seamlessly apply a security policy that prevents attacks and keeps your business operations running smoothly.

A unified and advanced multi-layered threat prevention environment offers essential capabilities. These include CPU-level sandbox prevention, threat extraction, anti-phishing and anti-ransomware solutions to defend against known and unknown 'zero-day' attacks.

Mobile

When it comes to protecting businesses from cyber-attacks, we know threat actors will always exploit weak links. One of the softest targets and universally overlooked are your mobile devices. While granting your staff access to company information via mobile has many benefits, it also exposes your business to great risks.

New threats on mobile platforms are being discovered all the time. Take the Man-in-the-Disk vulnerabilities, for example, which were shortly noticed in the Android

version of the massively popular Fortnite game shortly after their discovery by Check Point Research. In addition, traditional attacks like man-in-the-middle attacks over Wi-Fi and smishing attempts over SMS can all be used to steal sensitive information such as emails, texts, photos, calendar appointments and attachments.

As a result, Android and iOS mobile devices must include a threat defense solution to prevent advanced cyber attacks. This technology protects the operating system, apps and network, without impacting performance or user experience.

What's needed is a technology that offers on-device network threat prevention, improved usability and data privacy features to:

1. Prevent phishing attacks on all applications: email, messaging and social media.

2. Prevent browsing to malicious sites where devices may become infected.

3. Block infected devices from sending sensitive data to botnets.

4, Keep infected devices from accessing corporate applications and data.

5. Mitigate threats without relying on user action or mobile management platforms.

To protect against OS vulnerability exploits, this requires the use of both static and dynamic techniques to monitor all configuration changes at a device's root level and the use of a behavioral analysis engine to detect unexpected system behaviors.

Prevention of malware delivered through fake apps should include a solution that captures apps as they are downloaded, and runs each app in a virtual 'sandbox' environment to analyze its behavior. In addition, amongst other variables, it should aggregate and correlate intelligence about the app's source and reputation of the app's servers as well as reverse-engineer the app for code-flow analysis.

In sum, mobile malware is no longer rare. Organizations should protect their mobile devices just as they do with endpoints and network, and not leave themselves exposed to potentially painful attacks.

Cloud

Businesses come in all shapes and sizes: big and small, public and private, local and global. But most have one thing in common: the cloud. The cloud is ushering in a new era of business. From software and platforms to infrastructure as a service, the cloud is revolutionizing modern IT networks, enhancing agility and efficiency.

But not all clouds have a silver lining. Naturally, clouds are always connected, so they're an attractive target for cyber attackers. In fact, anything placed in the cloud

is potentially at risk. As a result, cloud security must be a shared responsibility between cloud service providers, who cover the infrastructure, and cloud customers who must protect their assets hosted in the cloud.

Once a threat is introduced, be it ransomware, account takeovers or cryptominers, there is nothing in the cloud to natively protect your applications, platforms, data or infrastructure. Nor is there anything to prevent such malware from propagating among cloud applications, attack virtual segments, or even ride unimpeded back to corporate networks.

And yet the cloud is here to stay and it is constantly evolving. Dynamic clouds therefore require dynamic security that's elastic, empowers agility and stays ahead of the most sophisticated attacks. This security must deliver proactive protection for cloud infrastructures and SaaS applications while supporting auto-scaling and one-click deployments.

To avoid account takeovers, a growing menace in cloud security that has led to many data breaches, solutions should include identity protection technologies. This will prevent unauthorized users and compromised devices from accessing your SaaS applications hosted in the cloud. By intercepting any unauthorized access and limiting data exposure through user behavior engines and shared intelligence of malware, OS exploits and network attacks and APIs across all other network devices, organizations can protect their sensitive cloud-hosted information.

The ongoing move toward private clouds and a Software-Defined Data Centre (SDDC), where all the infrastructure elements (networking, storage, CPU and security) are virtualized and delivered as a service, also raises new security challenges. Such challenges include ensuring security is not compromised when new applications are instantly deployed and move around the data center as well as keeping internal traffic growth visible and network security policies enforceable.

Therefore, organizations should adopt a private cloud security solution that protects dynamic virtual environments from external and internal threats, including those propagating via inter-VM traffic. Comprehensive security protections should also include firewall, IPS, anti-bot, anti-malware, and be designed to protect communications between applications in the private cloud through tight integration with leading private cloud platforms such as VMware NSX and Cisco ACI.

Advanced features such as auto-provisioning and auto-scaling along with automatic policy updates will also ensure security protections keep pace with all changes to your cloud. Additionally, a single unified console that offers consistent visibility, policy management, logging, reporting and control across all cloud environments will allow IT professionals to manage these systems with greater confidence and ease.

CONCLUSION

While threat actors try hard to keep a lower profile for their menacing activities, they do not escape our watchful eye. Indeed, never does a day go by that we do not see organizations under constant attack from the ever growing number of malware spreading at higher rates than ever.

As we have seen through the latest threat trends, malware has evolved to be more stealth-like than ever and open to almost anyone to carry out an attack. Indeed, the democratization of the cyber crime ecosystem paves the way for new, unskilled attackers to enter the malware distribution arena. Anyone willing to pay can easily obtain the suitable tools and services needed to launch any kind of cyber attack.

In the fifth generation of the cyber threat landscape, as technology has evolved, so too do threat actors' adapt and abuse such technologies for their own malicious ends. The cloud environment has changed the way companies manage, store and share their data, applications, and workloads. Along with a wide range of benefits, though, the cloud infrastructure also introduces a new, fertile and attractive environment for attackers who crave the enormous amount of available computing resources and sensitive data it holds.

While we consider the cloud to be an organization's weakest link, should they be using such services, threats posed to them via their employees' mobile and IoT devices are also ones to seriously take into account as one of many attack vectors from which sensitive data can be stolen or leveraged to launch an attack.

Despite the ever growing number of malware, however, infiltrating IT networks from an increasing number of entry points, there are advanced threat prevention solutions available. Indeed, the specific advantages these technologies hold over more traditional solutions must be implemented if organizations are to stay ahead of cyber criminals in today's threat landscape.

APPENDIX: MALWARE FAMILY DESCRIPTION

MALWARE	DESCRIPTION
Andromeda	Andromeda is a modular bot for malicious activity, and was first spotted in 2011. It is used mainly as a backdoor to deliver additional malware on infected hosts, but can be modified to create different types of botnets.
AdvisorsBot	AdvisorsBot is a sophisticated downloader first spotted in the wild in May 2018. AdvisorsBot has significant anti-analysis features including using "junk code" to slow down reverse engineering, and Windows API function hashing to make it harder to identify the malware's functionality.
Authedmine	Authedmine is a version of the infamous JavaScript miner Coinhive. Like Coinhive, Authedmine is a web-based cryptominer used to perform online mining of Monero cryptocurrency when a user visits a particular web page. Unlike CoinHive, Authedmine requires the website user's explicit consent before running the mining script.
AZORult	AZORult is a Trojan that gathers and exfiltrates data from the infected system. Once the malware is installed on a system (typically delivered by an Exploit Kit such as RIG), it can send saved passwords, local files, crypto-wallets, and computer profile information to a remote C&C server. The Gazorp builder, available on the Dark Web, enables anyone to host an AZORult C&C server with minimal effort.
BadRabbit	BadRabbit is a ransomware that targets the Windows platform. The malware has a list of usernames and passwords to access and spread to SMB shares on other systems in the network. It can also spread via the EternalRomance exploit.
Bancos	Bancos 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.
BlackEnergy	BlackEnergy is a Trojan-type program that targets the Windows platform. 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.
Bunitu	Bunitu is a Trojan that targets the Windows platform and sets up a proxy on the infected system to allow malicious activities. Bunitu also adds itself to the list of Windows firewall authorized applications.

MALWARE	DESCRIPTION
Cerber	Cerber, also known as Zerber, was first introduced in February 2016. It is an offline ransomware, meaning that it does not need to communicate with its C2 server before encrypting files on an infected machine.
Chapak	Chapak is a malware dropper and installs malware on the victim's machine after being installed itself. Unlike a downloader, which contacts a remote server to receive access to files, the dropper already contains the malware when installed on the machine. Chapak dropper does not damage the infected computer directly but delivers a malware payload or a number of types of malware with various features.
CNRig	CNRig is a Cryptonight CPU miner for Linux and is based on the open source Monero miner XMRig. CNRig has an automatic update mechanism.
Coinhive	Cryptominer designed to perform online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources, thus impacting their performance.
Cridex	Cridex is a Banking Trojan for the Windows platform. It attempts to steal victim's credentials, such as credit card information. It can download and execute other malicious files on the infected system and is spread via removable drives and network shares.
Cryptoloot	Cryptoloot is a JavaScript cryptominer designed to perform online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources, thus impacting its performance. Cryptoloot is a competitor of Coinhive.
Cryptor	Cryptor is a ransomware which was first discovered in August 2018 and masquerades as the legitimate SuperAntiSpyware Anti-Malware program. Cryptor uses the domain superantispyware.com to distribute the ransomware. Upon encryption, Cryptor creates a ransom note in every folder, which includes a unique victim key and a demand of 0.125 Bitcoin as payment. If the infected machine language and location settings point to Brazil or a Russian-language country, the ransomware does not encrypt the files.
Dorkbot	IRC-based worm that enables remote code execution and downloads additional malware to the infected system. Dorkbot's primary purpose is to steal sensitive information and launch Denial-of-Service attacks.
Dorvku	Dorvku is a Trojan that targets the Windows platform. The malware collects system information and sends it to a remote server. It also collects sensitive information from targeted web browsers.

MALWARE	DESCRIPTION
Emotet	Emotet is an advanced, self-propagating and modular Trojan. Emotet functioned as a banking Trojan, and is currently used to distribute other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. Emotet can also be spread through phishing spam emails.
FileLocker	FileLocker is a ransomware that was first discovered in late 2017, and is a variant of Hidden Tear, the first open-source ransomware for prospectve attackers on GitHub. FileLocker attacks the machines of Korean users. Upon successful infection and encryption, FileLocker demands payment of 50,000 Won (approximately $50) to retrieve the files. Due to a flaw in the malware, a decryptor can be created to retrieve the decryption key from the malware executable.
Fireball	Fireball is an adware distributed by the Chinese digital marketing company Rafotech. It acts as a browser-hijacker which changes the default search engine and installs tracking pixels, and can be turned into a fully functioning malware downloader.
Gafgyt	Gafgyt is a backdoor that targets Linux platforms. This malware spreads as a result of exploiting the vulnerability CVE-2014-6271. Gafgyt contacts a remote server to receive and execute commands on the infected system. These commands include the capability to open a backdoor on the infected system and to perform various DoS attacks.
GandCrab	GandCrab is a ransomware which targets mainly Scandinavia and English-speaking countries. GandCrab is distributed via the RIG and GrandSoft Exploit Kits, as well as email spam. The ransomware is operated in an affiliates program, with those joining the program paying 30%-40% of the ransom revenues to the GandCrab author. In return, affiliates get a full-featured web panel and technical support.
Guerrilla	Guerrilla is an Android Trojan which is embedded in multiple legitimate apps. It downloads additional malicious payloads to generate ad revenue for the app developers.
Hiddad	Hiddad is an Android malware which repackages legitimate apps, and then releases them to a third-party store. Its main function is to display ads. It can also gain access to key security details built into the OS.
HiddenMiner	HiddenMiner is a strain of Android cryptominer that was first seen in April 2018. The HiddenMiner is delivered through a fake Google Play update app, and uses the host device resources to mine Monero.
IcedID	IcedID is a banking Trojan which first appeared in September 2017. It uses other banking Trojans to enable it to spread, including Emotet, Ursnif and TrickBot. IcedID steals user financial data via both redirection attacks (installs local proxy to redirect users to fake web sites) and web injection attacks (injects browser process to present fake content overlaid on top of the original page).

MALWARE	DESCRIPTION
JSEcoin	Web-based cryptominer that performs online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources to mine coins, thus impacting the machine's performance.
Kraken	Kraken is a ransomware Trojan that targets the Windows platform. The malware collects system information and sends it to a remote attacker via the Discord chat service. Kraken downloads and executes the decryptor on the infected system to demand payment for decrypting the files. It can also kill processes on the infected machine.
Lotoor	Lotoor is a hack tool that exploits vulnerabilities on the Android operating system to gain root privileges on compromised mobile devices.
Mirai	Mirai is an Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. Mirai botnet first appeared in September 2016 and quickly made headlines for large-scale attacks, including a massive DDoS attack used to knock the entire country of Liberia offline, and a DDoS attack against the Internet infrastructure firm Dyn, which provides a significant portion of the United States internet's infrastructure.
Necurs	Necurs is one of the largest spam botnets currently active in the wild. In 2016, it was estimated to consist of approximately 6 million bots. The botnet is used to distribute many malware variants, primarily banking Trojans and ransomware.
NetSupportRAT	NetSupportRAT is a commercial Remote Access Tool (RAT) that was developed for system administrators to enable remote access to client machines. However, NetSupport is widely abused by malicious actors to gain unauthorized access to victim machines without their knowledge or consent. The RAT is distributed via fake software updates for Adobe Flash, Google Chrome and Mozilla Firefox. When accessing the compromised website, a malicious JavaScript is downloaded, collects system information and downloads the RAT.
Nivdort	Nivdort is a Trojan family which targets the Windows platform. It gathers passwords and system information or settings such as the Windows version, IP address, software configuration and approximate location.
NotPetya	NotPetya is a ransomware which was spread in a worldwide attack with a high concentration of hits in Ukraine, including the Ukrainian central bank, government offices and private companies. The ransomware has worm capabilities and abuses active sessions and steals credentials. Additionally, NotPetya was used in the "EternalBlue" SMB exploit. After the malware infiltrates into a network, it makes lateral movements to infect the entire network.

MALWARE	DESCRIPTION
OilRig APT	Also known as APT34, OilRig is an Iranian APT group active since 2016, and is believed to be a state-sponsored group under the guidance of the Iranian Intelligence Agency and the Iran Revolution Guard Corps (IRGC). The group attacks various targets and organizations across the Middle East, and its primary goal is espionage and sensitive data theft. The victims include mostly financial, aviation, infrastructure, government and university organizations. The group uses spear phishing to deliver its changing payload to its victims.
Olympic Destroyer	Olympic Destroyer is a data wiper malware attributed to the North Korean APT group Lazarus and is spread using the EternalRomance exploit. Olympic Destroyer was utilized in a campaign aimed at the PyeongChang 2018 Winter Olympics, and caused downtime to internal WiFi and television systems, and disrupted some operations during the games' opening ceremony. Olympic Destroyer can hack a computer's data recovery procedures and delete crucial Windows services, causing computers running Windows to be unable to boot.
Panda	Panda is a Zeus variant that was first observed in the wild at the beginning of 2016, and is distributed via Exploit Kits. Since its initial appearance, Panda has targeted financial services in Europe and North America. Before the Olympic Games of 2016, it also ran a special campaign against Brazilian banks.
Parite	Parite is a polymorphic virus which infects executable files on the infected host and on network drive. It drops a malicious DLL file into the Windows temporary directory which is injected into the explorer.exe process.
Pegasus	Pegasus is a highly sophisticated zero-day spyware which targets Android and iOS mobile devices, and is commonly attributed to the Israeli cyber intelligence firm NSO group. Pegasus infects its targets via spear phishing SMS messages which contain a malicious link, and utilizes three zero-day vulnerabilities which allow it to silently jailbreak the device and install the malware. Pegasus features multiple spying modules such as taking screenshots, recording calls, accessing messenger applications, keylogging and exfiltrating browser history. Pegasus is offered for sale, mostly to government-related organizations and corporations.
Qbot	Qbot is a backdoor that drops and downloads other malware. It also establishes a connection with a remote HTTP server without user consent and steals sensitive information.
Ramnit	Ramnit is a banking Trojan which incorporates lateral movement capabilities. Ramnit steals web session information, enabling the worm operators to steal account credentials for all services used by the victim, including bank accounts, corporate and social networks accounts.

MALWARE	DESCRIPTION
RIG Exploit Kit	RIG EK was first introduced in April 2014. It has since received several large updates and continues to be active to this day. RIG is used by many threat actors to distribute malware.
Roaming Mantis	Roaming Mantis is an Android banking Trojan that was first seen in March 2018. It steals users' sensitive information, login credentials and the secret code for two-factor authentication. Roaming Mantis is distributed using DNS hijacking attacks, disguised as Chrome browser or Facebook apps. An evolved version of Roaming Mantis also targets iOS devices with phishing attacks, and desktops and laptops with the Coinhive cryptomining script.
RubyMiner	RubyMiner is a Monero miner that targets both Windows and Linux servers. It seeks out vulnerable versions (such as PHP, Microsoft IIS, and Ruby on Rails) to mobilize them to its mining pool, and to install the open source Monero miner XMRig.
Ryuk	Ryuk is a ransomware used in targeted attacks against several organizations worldwide. The ransomware's technical capabilities are relatively low, and include a basic dropper and a straightforward encryption scheme. Nevertheless, the ransomware caused severe damage and forced victims to pay extremely high ransom payments of up to $320,000 in Bitcoin. Unlike most ransomware, which is distributed via massive spam campaigns and Exploit Kits, Ryuk is used exclusively for targeted attacks. Its encryption scheme is intentionally built for small-scale operations; only crucial assets and resources are infected in each targeted network, and infection and distribution are carried out manually by the attackers.
Sality	Sality is a virus which is spread by infecting .exe and .scr files as well as via removable drives and network shares. Systems infected with Sality can communicate over a peer-to-peer (P2P) network for spamming purposes.
SamSam	SamSam is an independently acting ransomware. After it is installed on a system, it encrypts the files without any need to communicate with a C&C server. SamSam scans for vulnerable servers with unpatched software. Unlike other ransomware campaigns, there is no need for any user action such as clicking a certain link or opening a malicious attachment for the infection to take place. The attackers can trigger the ransomware remotely once it has found vulnerability in the server and penetrated the network. Once a network has been breached, the ransomware spreads through the local network to infect additional computers.
Satan	Satan is a Ransomware-as-a-service (RaaS) that was first seen in January 2017. Its developers offer a user-friendly web portal with customization options, allowing anyone who buys it to create custom versions of Satan ransomware and distribute it to victims. New versions of Satan were observed using the EternalBlue exploit to spread across compromised environments, as well as performing lateral movement using other exploits.

MALWARE	DESCRIPTION
Satori	Satori is a variant of the Mirai IoT botnet. The payload delivered by an IoT (Internet of Things) botnet targets vulnerable HG532 Huawei home routers, and is based on a zero-day vulnerability in the device. After infection, the botnet utilizes the infected machines for various purposes including cryptocurrency mining and credentials theft. The attack was first identified by Check Point researchers in November 2017.
Scarsi	Scarsi is a malware used to infect as many victims as possible to form a botnet, a network of computers, usually controlled by the owner via C&C servers, for illicit purposes such as DDoS attacks, mining cryptocurrency, mail spam, etc.
Stone Panda APT	Also known by the nickname APT10, Stone Panda is an elite APT group active since 2009, and is believed to be of Chinese origin and state sponsorship. The group's primary goal is intellectual property theft and it often targets government documents of national security importance. Stone Panda's most notable attack included a well-planned operation which targeted MSSP providers worldwide which were leveraged by the group to gain access to the networks of several of their customers. Its targets are spread worldwide, but APT10 heavily attacks US-based and Japanese companies belonging to both the business and government sectors.
TheMoon	TheMoon is a botnet which appeared in 2014 and infected Linux servers. In 2017, it switched to IoT devices. In 2018, the botnet integrated a new zero-day exploit for the Dasan GPON router into its code, allowing its operators to recruit them to the botnet.
TheTruthSpy	TheTruthSpy is an Android spyware first seen in May 2017. It monitors WhatsApp messages, Facebook chats, and internet browsing history.
Tinba	Tinba is a banking Trojan which targets mainly European banking customers and uses the Blackhole Exploit Kit. Tinba steals the victim's credentials using web-injects, which are activated as the user tries to connect his account.
Triada	Triada is a modular backdoor for Android which grants super-user privileges to download second stage malware. Triada has also been seen spoofing URLs loaded in the browser.
TrickBot	TrickBot is a Dyre variant that appeared in October 2016. Since its first appearance, it has targeted primarily banks in Australia and the UK, and lately also in India, Singapore and Malesia.
Virut	Virut is a major botnet and malware distributor in the Internet, and is used in DDoS attacks, spam distribution, data theft and fraud. The malware is spread through executables originating from infected devices such as USB sticks as well as compromised websites, and attempts to infect any executable file. Virut alters the local host files and opens a backdoor by joining an IRC channel controlled by a remote attacker.

MALWARE	DESCRIPTION
VPNFilter	VPNFilter is a Trojan that targets Linux operating systems running on MIPS and x86 architectures. The malware downloads a binary from a control server and executes it. The downloaded binary retrieves and executes commands from the control server which allows it to execute shell commands, disable the device, upload files, and more. It has been reported that this malware is capable of modifying NVRAM values. Furthermore, this malware may achieve persistence by adding itself to the Chrome tab.
WannaCry	WannaCry is a ransomware which was spread in a large scale attack in May 2017, and utilizes a Windows SMB exploit called EternalBlue to propagate within and between networks.
WannaMine	WannaMine is a sophisticated Monero cryptomining worm that spreads utilizing the EternalBlue exploit. WannaMine implements a spreading mechanism and persistence techniques by leveraging Windows Management Instrumentation (WMI) permanent event subscriptions.
XMRig	XMRig is open-source CPU mining software used for mining Monero cryptocurrency. It was first seen in the wild in May 2017.
Zacinlo	Zacinlo is a highly sophisticated and persistent malware that targets the Window platform and has been active since 2012. Zacinlo takes screenshots, spams the system with advertisements, opens multiple browser sessions and replaces legitimate ads on a website with its own ads, and designs specially crafted ads to manipulate users into clicking them. Zacinlo can also carry out man-in-the-middle (MitM) attacks to intercept traffic, detect and remove competing adware and also any local services it deems dangerous such as security software.
Zapchast	Zapchast is an IRC-controlled backdoor that allows an attacker to access and control an affected machine. When the backdoor is run, it establishes a connection to an IRC (Internet Relay Chat) server. It then creates a bot in a specific IRC channel or server, and uses the channel to control its multiple bots and launch distributed denial of service (DDoS) attacks.
Zeus	Zeus is a widely distributed Windows Trojan which is mostly used to steal banking information. When a machine is compromised, the malware sends information such as the account credentials to the attackers using a chain of C&C servers.

Check Point®
SOFTWARE TECHNOLOGIES LTD

WORLDWIDE HEADQUARTERS

5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. HEADQUARTERS

959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391 | 650-628-2000 | Fax: 650-654-4233

UNDER ATTACK?

Contact our Incident Response Team:
emergency-response@checkpoint.com

checkpoint.com