



CHECK POINT RESEARCH



2020

CYBER SECURITY REPORT



Check Point®
SOFTWARE TECHNOLOGIES LTD

1 EXECUTIVE SUMMARY: NAVIGATING THE EVER-CHANGING CONTOURS OF CYBER SECURITY	4
2 TIMELINE OF 2019'S MAJOR CYBER EVENTS.....	7
3 2020 VISION: CHECK POINT'S CYBER SECURITY PREDICTIONS	12
Targeted ransomware	14
The Tokyo 2020 Olympics as prime target	15
Phishing attacks go beyond email	15
Mobile malware attacks step up	16
More IoT devices, more risks.....	17
Data volumes skyrocket with 5G	18
AI will accelerate security responses	18
Security at DevOps speed.....	19
Rethinking cloud approaches.....	19
4 2019 CYBER SECURITY TRENDS	21
Introduction	22
Shifting attacks to supply chain targets	24
Magecart becomes an epidemic.....	25
Attacks against cloud environments	27
Evolving mobile landscape	28
Targeted ransomware	30
Reemergence of exploit kits	31

5 	GLOBAL MALWARE STATISTICS	33
	Cyber attack categories by region	35
	Global threat index map	36
	Top malicious file types: web vs. email	37
	Top malware families	38
	Global analysis of top malware	39
6 	HIGH-PROFILE GLOBAL VULNERABILITIES	49
	Microsoft RDP Vulnerabilities:	
	BlueKeep and DejaBlue (CVE-2019-0708, CVE-2019-1182)	50
	Oracle WebLogic Server Vulnerabilities	
	(CVE-2017-10271, CVE-2019-2725)	51
	Exim Mail Server Remote Code Execution	
	Vulnerability (CVE-2019-10149)	51
7 	REVIEW OF 2019 CYBER THREAT PREDICTIONS.....	53
8 	RECOMMENDATIONS TO PREVENT THE NEXT CYBER ATTACK	59
	Choose prevention over detection	60
	Leveraging a complete unified architecture	61
	Keep your threat intelligence up to date	61
9 	ZERO TRUST NETWORKS: BEST PRACTICES	62
	APPENDIX: MALWARE FAMILY DESCRIPTIONS	67



NAVIGATING THE EVER-CHANGING CONTOURS OF CYBER SECURITY

EXECUTIVE SUMMARY

Each year, Check Point Research (CPR) reviews previous year cyber incidents to gather key insights about the global cyber threat landscape. In this 2020 Cyber Security Annual Report, we offer a review of 2019's major cyber incidents, suggest predictions for 2020, and recommend best practices to help keep your organization safe from cyber attacks.

With the popularity of cloud computing and network-connected smartphones, it's no secret that there are more ways to invade an organization. A once hardened network perimeter is now blurred and porous to cyber attacks, and the bad actors are well aware.

If there's one clear takeaway from 2019, it's that no organization, big or small, is immune from a devastating cyber attack. Cyber exploits are more sophisticated, illusive, and targeted than ever before. With cybercrime rates estimated to have generated US\$1.5 trillion in 2018,¹ navigating today's complex cyber threat landscape requires comprehensive cyber security.



ENTIRE LOCAL GOVERNMENTS WERE FORCED
TO DECLARE A STATE OF EMERGENCY DUE TO
MASSIVE LEAKS OF SENSITIVE DATA AND THE
LOSS OF SERVICES.

In 2019, becoming an under protected, “sweet spot” for hacking was dangerous for entire industries. A large number of state and local public sector agencies were ravaged by ransomware attacks. In some cases, entire local governments were forced to declare a state of emergency due to the massive leaks of sensitive data and loss of services.

In this 2020 Cyber Security Annual Report, we provide you with a timeline of 2019’s significant cyber events, including their relevant facts and insights. By analyzing our telemetric, product and vulnerability research, and our own ThreatCloud threat intelligence, we offer a detailed analysis of the cyber trends you need to consider. We then offer our 2020 vision which includes cyber security predictions.

Finally, we offer recommendations on cyber protection strategies, using security “hygiene” best practices, advanced technology, and the focus on prevention, not detection or remediation. In order to adopt a winning strategy against zero-day, unknown cyber attacks, prevention should be considered.

1 “33 Alarming Cybercrime Statistics You Should Know in 2019,” by Casey Cane, Security Boulevard, November 15, 2019

CHAPTER 2

TIMELINE OF 2019'S MAJOR CYBER EVENTS





Over 770 million email addresses and 21 million unique passwords were exposed in a popular hacking forum after hosted in the cloud service MEGA. It became the single largest collection of breached personal credentials in history, named "Collection #1".² Later in the year, Collection #1 was discovered as a minor slice of a bigger 1TB data leak, split into seven parts and distributed through a data-trading scheme.

Airbus, the world's second-largest manufacturer of commercial airplanes suffered a data breach, exposing personal data of some of its employees.³ Unauthorized attackers breached Airbus' "Commercial Aircraft business" information systems.



620 million account details were stolen from 16 hacked websites, and offered for sale on the popular dark web marketplace, Dream Market.⁴ Later on, the same threat actor using the alias "Gnosticplayers," published for sale another trove of 127 million accounts from 8 more hacked websites.



The world's largest email validation company, Verifications.io., fell victim to a major data breach due to an unprotected MongoDB database. Data from over 800 emails was exposed, containing sensitive information that included personally identifiable information (PII).⁵

JAN

01

FEB

02

MAR

03

² "The 773 Million Record "Collection #1" Data Breach," by Troy Hunt, Troyhunt.com, January 17, 2019

³ "Airbus Suffers Data Breach, Some Employees' Data Exposed," by Mohit Kumar, The Hacker News, January 31, 2019

⁴ "Hacker Breaches Dozens of Sites, Puts 127 New Million Records Up for Sale," by Swati Khandelwal, The Hacker News, February 15, 2019

⁵ "800+ Million Emails Leaked Online by Email Verification Service," by Bob Diachenko, Security Discovery, March 7, 2019



More than half a billion Facebook users' records were found exposed on unprotected Amazon cloud servers.⁶ The exposed data sets were collected and insecurely stored online by third-party Facebook app developers.

Personal data of over 100 million users of the Indian search service JustDial was exposed after an unprotected database was found online.⁷ The leaked data contained was collected in real-time from every customer who accessed the service via its website, mobile app, or even by calling, and includes usernames, email addresses, mobile numbers, addresses, occupation and even photos.



A Russian hacking group offered for sale access to networks of Anti-Virus companies and the source code of their software.⁸ The group, called Fxmsp, claimed to have breached the networks of McAfee, Symantec, and Trend Micro Anti-Virus firms, obtaining long-term remote access and stealing 30 terabytes of data which were offered for sale.



American Medical Collection Agency (AMCA) suffered a major data breach, exposing personal and payment information of almost 20 million patients after attackers infiltrated their web payment portal.⁹ The information included names, date of birth, address, phone, date of service, provider, balance information, and credit card or bank account. AMCA filed for bankruptcy as the breach led to both financial and legal consequences.

APR

04

MAY

05

JUN

06

⁶ "Facebook Caught Asking Some Users Passwords for Their Email Accounts," by Swati Khendelwal, The Hacker News, April 3, 2019

⁷ "Over 100 Million JustDial Users' Personal Data Found Exposed On the Internet," by Mohit Kumar, The Hacker News, April 17, 2019

⁸ "Fxmsp Chat Logs Reveal the Hacked Antivirus Vendors, AVs Respond," by Ionut Ilascu, Bleeping Computer, May 13, 2019

⁹ "Data Breach Forces Medical Debt Collector AMCA to File for Bankruptcy Protection," by Charlie Osborne, ZDNet, June 19, 2019



A second Florida city, Lake City, agreed to pay a \$500,000 after a ransomware attack crippled the city's computer systems for two weeks.¹⁰ The attack, dubbed "Triple Threat," combined three different methods of attack to target network systems and locked phone and email systems.

City Power, the electricity provider in the city of Johannesburg, South Africa, suffered serious disruptions after a ransomware attack. The attack prevented prepaid customers from buying electricity units and accessing City Power's official website, eventually leaving them without electricity power.



Capital One, one of the largest banking institutions in the United States, suffered a massive data breach, exposing personal information of over 106 million credit card applicants between 2005 and 2019. The hacker allegedly exploited a misconfigured firewall on one of Capital One's cloud servers and stole over 700 folders of data.

Over 20 Texas government organizations have been hit with ransomware in what appears to be a pre-coordinated attack against the entities. The cybercriminals behind the attack demanded \$2.5 million in ransom to decrypt the data.



A broad campaign of iPhone hacking was revealed. For at least two years, attackers used compromised websites to exploit 14 separate vulnerabilities in Apple's iOS, installing spyware on thousands of Apple devices that visited the malware-tainted websites. Attackers gained access to location data, photos, contacts, Keychain passwords, WhatsApp and other communication and social media content.

JUL

07

AUG

08

SEP

09

10 "Second US Town Pays up to Ransomware Hackers," BBC, June 26, 2019



Personal medical data of nearly one million people in New Zealand was exposed in an intrusion to the systems of Tu Ora Compass Health organization. A hacker under the name of “Vanda The God” threatened to sell the information. Investigations revealed the systems were hacked on four different occasions.



UniCredit, an Italian banking company, suffered a data breach that resulted in the leak of personal information belonging to 3 million customers, after an unknown attacker compromised an old file from 2015 containing records of Italian customers, including names, phone numbers and email addresses.



New Orleans mayor declares a state of emergency in wake of a cyber attack disrupting city’s services.

OCT

10

NOV

11

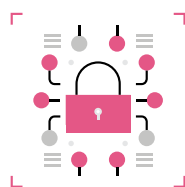
DEC

12



2020 VISION: CHECK POINT'S CYBER SECURITY PREDICTIONS

Per the saying, "hindsight is 20/20 vision," it's easier to know the right course of action after something has happened, while it's much harder to predict the future. However, we've analyzed security incidents over the past couple of years to forecast what's likely to happen in the cyber landscape over the next 12 months. Here are the key security and related trends that we expect to see during 2020. We start with our high-level geopolitical predictions and then to the technology-related trends.



IT'S CLEARLY EVIDENT THAT
ORGANIZATIONS MUST ADOPT A STRATEGY
OF PREVENTION AND NOT MERELY RELY
ON DETECTION OR REMEDIATION.

TARGETED RANSOMWARE

In 2019, we saw an escalation of sophisticated and targeted ransomware exploits. Specific industries were heavily victimized, including state and local government and healthcare organizations. The new, stark reality is that attackers are spending more time to gather intelligence on their victims, achieving maximum disruption and scaled-up ransoms. Attacks have become so damaging that the FBI has softened its previous stance on paying ransoms. They now acknowledge that in some cases, businesses may need to evaluate their options in order to protect their shareholders, employees, and customers.



**CYBERCRIMINALS ARE
USING VARIOUS ATTACK
VECTORS TO TRICK THEIR
INTENDED VICTIMS.**



Ransomware attacks were launched this year as a lethal mass weapon that can easily shut down large-scale organizations, cities, local governments and healthcare organizations. New Orleans mayor declared a state of emergency in the wake of massive cyber attack. This reflects a gradual escalation in what we expect will get even worse in upcoming years. In light of such events, it's clearly evident that organizations must adopt a strategy of prevention and not merely rely on detection or remediation.

Lotem Finkelstein,
Head of Threat Intelligence

THE TOKYO 2020 OLYMPICS AS PRIME TARGET

High-profile global exposure events are always within a hacker's line of sight. Previous Olympiad organizers faced extensive cyber incidents, with 500 million attacks estimated during the 2016 Rio Games and 250 million during the 2012 London Games.¹¹ We expect that attackers won't "discriminate" with the 2020 Olympiad and they'll invest as much effort, if not more, to disrupt this highly anticipated (and lucrative) event.

PHISHING ATTACKS GO BEYOND EMAIL

While email is the top attack vector, bad actors are using a variety of tricks to give up sensitive information. Increasingly, phishing involves SMS texting attacks against mobiles or the use of messaging on social media and gaming platforms.



While email remains the #1 attack vector, cybercriminals are also using a variety of other attack vectors to trick their intended victims into giving up personal information, login credentials, or even sending money. We have seen attackers obtain credentials to email accounts, study the victim for weeks and when the time is right, craft a targeting attack against partners and customers to steal money. Over the last two years, this attack has spiked with the increased use of SaaS-based email solutions."

Dan Wiley,
Head of Incident Response

¹¹ "State-Backed Cyber Attacks Expected at Tokyo 2020 Games," by Scott Ikeda, CPO Magazine, January 7, 2020

MOBILE MALWARE ATTACKS STEP UP

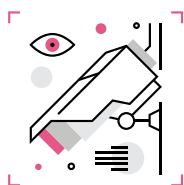
The first half of 2019 saw a 50% increase in attacks by mobile banking malware¹² compared to 2018. This malware can steal payment data, credentials, and funds from victims' bank accounts, and latest versions are made available for widespread distribution to anyone that's willing to pay the malware's developers. Like many cyber attacks, phishing will become more sophisticated and effective, luring mobile users to click on malicious web links.



Surprisingly, mobile banking malware requires little technical knowledge to develop, and even less to operate. The malware searches for a banking app on the infected device and creates a fake overlay page once the user opens it. The user will then enter the user's credentials, sending it directly to the attacker's server.

Maya Horowitz

Director, Threat Intelligence
& Research



FROM IP CAMERAS AND SMART ELEVATORS
TO MEDICAL DEVICES AND INDUSTRIAL
CONTROLLERS, IOT DEVICES ARE INHERENTLY
VULNERABLE AND EASY TO HACK. THE NEW
GENERATION OF SECURITY WILL BE BASED
ON NANO SECURITY AGENTS.

¹² "Check Point Research: From Supply Chain to Email, Mobile and the Cloud, No Environment is Immune to Cyber Attacks," Check Point, July 25, 2019

MORE IOT DEVICES, MORE RISKS

As 5G networks roll out, the use of connected IoT devices will accelerate dramatically. They will increase networks' vulnerability to large-scale, multi-vector Gen V cyber attacks. IoT devices and their connections to networks and clouds, are a weak link in security. It's hard to get visibility of these devices that can have complex security requirements. What's needed is a more holistic approach to IoT security, combining traditional and new controls to protect these ever-growing networks across all industry and business sectors. The new generation of security will be based on nano security agents. These micro-plugins can work with any device or operating system in any environment, controlling all data that flows to and from the device, and giving always-on security.



From IP cameras and smart elevators to medical devices and industrial controllers, IoT devices are inherently vulnerable and easy to hack. Moreover, most of these connected devices are not at all protected, as they're connected to corporate networks without anyone's knowledge. This security gap increases the risk of a successful cyber attack where critical devices can be shut down, damaged, manipulated, or used to infect other systems on the network. Now is the time to take action and secure IoT the same way we secure IT.

Itai Greenberg

VP Product Management

DATA VOLUMES SKYROCKET WITH 5G

The bandwidths that 5G enables will drive an explosion in numbers of connected devices and sensors. eHealth applications will collect data about users' well-being. Connected car services will monitor users' movements. Smart city applications will collect information about how users live their lives. This ever-growing volume of personal data will need to be protected against breaches and theft.

AI WILL ACCELERATE SECURITY RESPONSES

Most security solutions are based on detection engines built on human-made logic, but keeping this current against the latest threats and across new technologies and devices is impossible to do manually. AI dramatically accelerates the identification of new threats and responses to them, helping to block attacks before they can spread widely. However, cybercriminals are also starting to take advantage of the same techniques to help them probe networks, find vulnerabilities, and develop more ever more evasive malware.



AI is only as sophisticated as it's learning curve. Expose the machine to skewed data and suddenly the atypical can become the algorithms' "normal." When considering the dynamic world of cybercrime, AI detection can be manipulated by criminals who are savvy enough to understand this. Which is why a robust, future-proof fraud detection approach needs to include more than just AI.

Neatsun Ziv – VP
Threat Prevention



SECURITY SOLUTIONS NEED TO EVOLVE TO A NEW PARADIGM OF FLEXIBLE, CLOUD-BASED, RESILIENT ARCHITECTURES THAT DELIVER SCALABLE SECURITY SERVICES AT THE SPEED OF DEVOPS.

SECURITY AT DEVOPS SPEED

Many organizations have shifted workloads to the cloud.¹³ However, the level of understanding as to securing them remains dangerously low. Security is often an afterthought as traditional security can be perceived as inhibiting business agility. This is why security solutions need to evolve to a new paradigm of flexible, cloud-based, resilient architectures that deliver scalable security services at the speed of DevOps.

RETHINKING CLOUD APPROACHES

Increasing reliance on public cloud infrastructure increases enterprises' exposure to the risk of outages, such as the Google Cloud outage in March 2019.¹⁴ This will drive organizations to look at their existing data center and cloud deployments, and consider hybrid environments comprising both private and public clouds.



Cloud computing is fast-moving and dynamic. As organizations adopt new and more efficient cloud-based services and technologies to meet their business needs, cloud attack vectors become more complex and diversified. An additional concern is that cloud has enabled the increase in the speed and agility of development teams to use new technologies, but security controls for these new technologies often lag behind new technology adoption. So developers are either frustrated while waiting for the security controls, or press forward without the required security, and this is precisely what threat actors in the cloud are waiting for.

Zohar Alon

Head of Cloud Product Line

¹³ "Cloud Computing Trends: 2019 State of the Cloud Survey," Flexera Blog, February 27, 2019

¹⁴ "Google Cloud Outage Is Over, The Second One In Four Months," by Antony Savvas, Data | Economy, March 13, 2019

CONCLUSION

We don't yet have the benefit of hindsight to show exactly what security threats we will face in 2020. Today's hyper-connected world creates more opportunities for cybercriminals, and every IT environment is a potential target: on-premise networks, cloud, mobile, and IoT devices. But forewarned is forearmed. By using advanced threat intelligence to power unified security architectures, businesses of all sizes can automatically protect themselves from future attacks.

CHAPTER 4



2019 CYBER SECURITY TRENDS

INTRODUCTION

2019 presented a complex threat landscape where nation states, cybercrime organizations, and private contractors accelerated the cyber arms race, elevating each other's capabilities at an alarming pace. According to our Incident Response team, 1 out of every 5 calls to our hotline ends up with a targeted ransomware attack that shuts down operations. The catalyst to this global trend can be found in the fact that 28% of all organizations worldwide were subject to botnet infection during 2019. Successful infection of such a botnet opens the door to much more destructive attacks, like ransomware.

Attacks on mobile and cloud platforms also evolved this year, with more vulnerabilities exposed and potent exploits released in the wild. These advanced attacks on public cloud services enabled the massive data breaches we witnessed this year. And our data indicates that 27% of all organizations globally were impacted by cyber attacks that involved mobile device.¹⁵

SOME OF THIS YEAR'S CYBER ATTACK TRENDS:

- **One stop before the target** – In their ongoing search for potential entry points, threat actors are now reaching victims through their trusted service providers and business partners.
- **The year Magecart became an epidemic** – During Black Friday 2019 alone, Americans spent \$7.4 billion in online shopping. Following the money, threat actors are seeking ways to exploit this e-commerce ecosystem, to steal credit card details, and customers' private data.
- **Attacks against the cloud environment** – The magnitude of cloud attacks and breaches has continued to grow in 2019. Misconfiguration of cloud resources is still the number one cause for cloud attacks, but now we also witness an increasing number of attacks aimed directly at the cloud services providers.
- **Evolution in mobile landscape** – 2019 proved the mobile threat landscape is now fully matured. More malware types being migrated to the mobile arena and more vulnerabilities in mobile devices, apps and operating systems are being exploited in the wild.
- **Targeted ransomware** – 2019 has been the year of targeted ransomware attacks, with software services, health care and public sectors at the top of the victims list.



27% OF ALL ORGANIZATIONS
GLOBALLY WERE IMPACTED
BY CYBER ATTACKS
THAT INVOLVED MOBILE DEVICE.

¹⁵ Check Point Research

SHIFTING ATTACKS TO SUPPLY CHAIN TARGETS

In search of potential attack entry points, threat actors have shifted their strategies to locate vulnerable organizations that are single step away from their main target. Now, service providers and business partners of primary targets are also victimized.

The classic method is a supply chain attack. In October, Avast reported a security breach in which CCleaner was believed to be a target of such an attack.¹⁶ If successful, this attack would have exposed all the CCleaner clients to the attackers. The ShadowHammer attack used Asus's update mechanism with millions of clients to target a group of only a few hundred users.¹⁷ In the mobile arena, Check Point Research investigated and exposed a large-scale operation called Operation Sheep.¹⁸ In this attack, non-suspecting application developers used a data analytics SDK which later turned out to be malicious and harvested the contact information of more than 110 million end users.

Other attacks use trusted service providers and their system privileges to compromise targets. In one such attack, threat actors used exposed RDP to hack into three MSPs (Managed Service Providers) and used their Webroot SecureAnywhere

console to deploy the Sodinokibi (REvil) Ransomware on their clients' systems.¹⁹ MSPs became a popular target in 2019.²⁰

In the Sea Turtle attack, the threat actor's ultimate objectives were security organizations and ministries in the Middle East.²¹ However, they targeted secondary victims such as DNS registries, telecommunication companies and ISPs to get to their primary victims.

Some campaigns manage to fully achieve their objectives without even tackling the final targets. In Operation Softcell, the Chinese group APT10 hacked into large telecommunication providers and used them to monitor the geolocations and communication records of their final targets.²² In the Messagetap campaign, attributed to APT41, attackers monitored SMS traffic of specific individuals and also used keyword monitoring to surveil general clients' communication content.²³

Awareness to these threats resulted in the US Department of Homeland Security establishing the Information and Communications Technology Supply Chain Risk Management Task Force. The task force published its interim report in September, amongst other recommendations,

16 "Avast Fights Off Cyber-Espionage Attempt, Abiss," by Jaya Baloo, Avast Blog, October 21, 2019

17 "Operation ShadowHammer: a High Profile Supply Chain Attack," Kaspersky, April 23, 2019

18 "Operation Sheep: Pilfer-Analytics SDK in Action," by Fexiang He and Andrey Polkovnichenko, Check Point Research, March 13, 2019

19 "Customers of 3 MSPs Hit in Ransomware Attacks," by Jai Vijayan, Dark Reading, June 20, 2019

20 "At Least 13 Managed Service Providers were Used to Push Ransomware This Year," by Catalin Cimpanu, October 13, 2019

21 "DNS Hijacking Abuses Trust in Core Internet Service," by Danny Adamitis, David Maynor, Warren Mercer, Matthew Olney, and Paul Rascagneres, Talos Intelligence, April 17, 2019

22 "Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers," Cybereason Nocturnus, Cybereason, June 25, 2019

23 "MESAGETAP: Who's Reading Your Text Messages?" by Raymond Leong, Dan Perez, and Tyler Dean, Fireeye, October 31, 2019

assessing the feasibility of Qualified Bidder & Qualified Manufacturer Lists as a means of prevention.²⁴ In May 2019, President Trump signed an Executive Order authorizing the Commerce Secretary to regulate the acquisition and use of information and communications technology as well as services from foreign adversaries, which later led to a ban of the technology giant Huawei.^{25,26}

Extending the circle of targets to include victims outside of the organization makes it far harder to protect assets. Maintaining a healthy suspicion of previously trusted partners and their security mechanisms has become an imperative in 2019.

MAGECART BECOMES AN EPIDEMIC

This past Black Friday alone, Americans spent \$7.4 billion in online shopping. Following the money, threat actors are seeking ways to exploit this ever-growing e-commerce ecosystem.²⁷ Magecart style attacks do just that, injecting malicious JavaScript code into e-commerce websites to steal customers' payment methods information.

While JavaScript skimmers have been used for years to steal credit card information from online-shopping platforms, this phenomenon has been ramped up greatly in 2019 as multiple threat groups conduct massive attacks on major e-commerce websites.

The term Magecart first entered public awareness following the 2018 attacks on British Airways and Ticketmaster, referring to the name of the threat group behind these attacks. The original Magecart attacks targeted businesses utilizing the Magento open source PHP e-commerce platform, but today numerous unrelated groups and attacks on a variety of platforms, all involving credit card skimming, are jointly referred to as Magecart.^{28,29}

24 "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report," Cybersecurity and Infrastructure Security Agency (CISA), September 2019

25 "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," Whitehouse.gov, May 15, 2019

26 "US Bans Huawei from Selling Telecom Gear and Threatens its Supply Chain," by Brian Fung, CNN Business, May 16, 2019

27 "Black Friday Shoppers Spend Record \$7.4 Billion in Second Largest Online Sales Day Ever," by Alex Sherman, CNBC, November 30, 2019

28 "Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims," by Yonathan Klijsma, RISKIQ, September 11, 2018

29 "Inside and Beyond Ticketmaster: The Many Breaches of Magecart," by Yonathan Klijsma and Jordan Herman, RISKIQ, July 9, 2019

A Magecart attack begins with gaining access to the backend server of an online retailer by exploiting known vulnerabilities, brute forcing operators' passwords or in some cases by installing skimmers in third party's code or services in a Supply-Chain attack. One such attack targeted PrismWeb, an e-commerce platform.³⁰ The attackers injected a skimming script into the shared JavaScript libraries used by online stores, thus affecting more than 200 online university campus stores in North America. After gaining access to compromised websites, attackers injected malicious JavaScript skimmers into the targeted services. The skimmers exfiltrate payment details to designated drop servers. For online stores that manage their own payments, such as Forbes, skimmer code is injected directly into the subscribers' payment section.³¹ For stores which use external payment services, fake payment forms are injected into the redirection page to convince customers to enter payment details before being redirected to the payment service.³²

During this past year, Magecart attacks hit hundreds of regular shopping sites, hotel chains and other organizations, from commerce giants like Procter & Gamble to small and medium businesses.^{33, 34, 35} Desktop and mobile platforms alike were affected. Unsecured cloud services provide an ideal entry point, as seen in a campaign involving misconfigured AWS S3 buckets.³⁶

One of the reasons for the surge in Magecart attacks is that each element of this criminal process can be separately purchased in underground forums. The available services include lists of websites using specific content management systems, brute forcing services, web shells, and a variety of JavaScript skimmers to money mule chains leased to convert the information into cash and goods. All of these give access to Magecart operations without requiring advanced offensive cyber skills.

-
- 30 "Mirrorthief Group Uses Magecart Skimming Attacks to Hit Hundreds of Campus Online Stores in US and Canada," by Joseph C. Chen, Trend Micro, May 3, 2019
 - 31 "Magecart Hackers Inject Card Skimmer in Forbes Subscription Site," by Pierluigi Paganini, Security Affairs, May 16, 2019
 - 32 "Skimmer Acts as Payment Service Provider via Rogue iframe," by Jerome Segura, Malware Bytes Labs, May 21, 2019

-
- 33 "Ongoing Attack Stealing Credit Cards from Over a Hundred Shopping Sites," Swati Khandelwal, The Hacker News, May 8, 2019
 - 34 "Magecart Skimming Attack Targets Mobile Users of Hotel Chain Booking Websites," by Joseph C. Chen, Trend Micro, September 18, 2019
 - 35 "P&G Online Beauty Store First Aid Beauty Hit by Magecart Attack," by Pierluigi Paganini, Security Affairs, October 26, 2019
 - 36 "Spray and Pray: Magecart Campaign Breaches Websites En Masse Via Misconfigured Amazon S3 Buckets," by Yonathan Klijnsma, RISKIQ, July 10, 2019

ATTACKS AGAINST CLOUD ENVIRONMENTS

As we noted in our 2019 midyear report, misconfiguration and mismanagement of cloud resources are still the number one cause for cloud attacks, but now we also witnessed an increasing number of attacks aimed directly at cloud services providers.³⁷ With a growing public cloud industry, the frequency and magnitude of cloud attacks and breaches continued to grow in 2019.



**MORE THAN 90%
OF ENTERPRISES
USE SOME TYPE
OF CLOUD SERVICE.**

27

The cloud industry is growing exponentially and is expected to rise from the current revenue of \$227 Billion in 2019 to \$354 Billion by 2022.³⁸ Currently, more than 90% of enterprises use some type of cloud service.³⁹ According to Check Point's 2019 Cloud Security Report most of them use Software as a Service (SaaS) products with Microsoft Office 365 being the most popular service used by 66% of surveyed organizations.⁴⁰ And still, 67% of security teams complained about lack of visibility into their

cloud infrastructure, security, and compliance.

This year, we witnessed a record number of data breaches with employees and clients information stolen in enormous quantities. A misconfigured cloud environment was the main cause for the vast number of data theft incidents. In April, unprotected Amazon servers resulted in the exposure of more than half a billion records of Facebook users, through third-party apps.⁴¹ Misconfigured Box accounts leaked terabytes of sensitive data, and in another case, sensitive income information of roughly 80 million Americans, hosted on a Microsoft cloud server, had been exposed online.^{42,43} Tens of millions of passenger records owned by two airline companies stored on unsecured Amazon buckets have been exfiltrated and later exchanged in online forums.⁴⁴

Misconfigured cloud accounts lead not only to data exfiltration but also to active exploitation of clients. By scanning for misconfigured Amazon S3 buckets, a Magecart group located and injected JavaScript skimmers to the code of thousands of websites through exposed buckets, using them to collect credit card information from the websites' customers.⁴⁵

- 37 "The Evolution of Cyber Attacks in 2019," Check Point Software Technologies LTD, July 2019
- 38 "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020," Gartner, November 13, 2019
- 39 "2019 State of the Cloud Report from Flexera," Flexera, 2019
- 40 "Check Point's 2019 Cloud Security Report Identifies Range of Enterprise Security Challenges in Public Clouds," Check Point Press Releases, July 16, 2019

- 41 "Hundreds of Millions of Facebook User Records Were Exposed on Amazon Cloud Server," by Jason Silverstein, CBS News, April 4, 2019
- 42 "Box Data Leak- Terabytes of Data Exposed from Companies Using Cloud Based Box Accounts," by Balaji N., GB Hackers on Security, March, 12 2019
- 43 "Exposed Database Leaks Addresses, Income Info of Millions of Americans," by Sergiu Gatalan, Bleeping Computer, April 29, 2019
- 44 "Millions of Lion Air Passenger Records Exposed and Exchanged on Forums," by Ionut Ilascu, Bleeping Computer, September 17, 2019
- 45 "Spray and Pray: Magecart Campaign Breaches Websites En Masse Via Misconfigured Amazon S3 Buckets," by Yonathan Klijsma, RISKIQ, July 10, 2019

One source cites that although cryptocurrencies have declined in value, cloud infrastructures are a huge target for cryptomining campaigns. Container management platforms, cloud APIs, and control panels were among the cloud structures targeted by threat actors.⁴⁶ In May, Microsoft Azure cloud services were used to store malware or implement command and control servers.⁴⁷

Not only misconfiguration leads to attacks on a cloud infrastructure. The infrastructure itself is prone to vulnerabilities. Vulnerability in SoftNAS cloud platform discovered this March could allow unauthorized attackers to bypass authentication, gaining access to a company's web-based admin interface and to run arbitrary commands as root.⁴⁸ Other vulnerabilities, exploiting hardware re-provisioning procedures could allow attackers to gain a foothold and take control of future provisioned IaaS servers.⁴⁹

Threat actors follow close behind their intended victims. As organizations increase their security awareness, the threat actors adopt more advanced ways to exploit cloud-based assets.

46 "Enterprise Cloud Infrastructure a Big Target for Cryptomining Attacks," by Jai Vijayan, Dark Reading, March 13, 2019

47 "Threat Actors Abuse Microsoft Azure to Host Malware and C2 Servers," by Pierluigi Paganini, Security Affairs, June 2, 2019

48 Untitled, by Digital Defense Inc., SoftNAS Cloud Zero-day Blog, March 20, 2019

49 "'Cloudborne' IaaS Attack Allows Persistent Backdoors in the Cloud," Threatpost, Tara Seals, February 26, 2019

EVOLVING MOBILE LANDSCAPE

2019 proved that the mobile threat landscape is now fully matured. From nation-state cyber operations, through private espionage and intelligence companies to cybercrime organizations, everyone adjusts their cyber weapons to evolving mobile device technology.

Although threat actors did not exploit the mobile ecosystem initially, this year we saw a continual increase in mobile-related cyber attacks. Hackers became more proficient as they gained operational experience. More and more malware types have been adjusted to mobile devices, and instead of relying solely on phishing campaigns to reach victims, we're now seeing an increasing number of vulnerabilities exploited in the wild.

Current types of mobile malware now include Remote Access Trojans (RAT), banking Trojans, cryptominers, adware, and even ransomware.^{50,51,52} Adware is still the most common type of mobile malware, and can be found on popular application markets like Google Play and App Store.

One example is Agent Smith, which replaced legitimate applications with a backdoor replica on millions of devices, hijacking their ad revenues. Banking Trojans and RATs like Gustuff and Cerberus target users of large number of

50 "iPhone Users Warned As Malware and the U.S. Supreme Court, Targets Apple," by Davey Winder, Forbes, July 30, 2019

51 "Banking Trojans Are Top Financial Services Threat," by Phil Muncaster, Infosecurity Magazine, December 6, 2019

52 "Android Ransomware is Back," by Lukas Stefanko, WeLiveSecurity, July 29, 2019

financial mobile apps, and even exploit vulnerabilities in mobile network protocols to bypass 2FA schemes.^{53,54,55,56} Numerous examples of spyware were also reported this year, including the Egyptian government monitoring dissidents activity, the Chinese spying on Tibetans, Middle East campaigns, attacks involving European residents, and more.^{57,58, 59} Mobile cryptominers and ransomware activity also continued in 2019.⁶⁰

With a maturing mobile malware arena, more threat actors relied on vulnerabilities for their initial infection or secondary stage escalation, as opposed to bad user practices. Such vulnerabilities in Android OS were reported on multiple occasions for exposing users to RATs and other threats.^{61,62} iPhone vulnerabilities were exposed and exploited as well.

The details of a two-year long operation published in August, revealed a large-scale campaign using 14 iOS vulnerabilities. Some of them zero-day attacks to hack into thousands of iPhones.⁶³

According to reports, vulnerabilities in WhatsApp were exploited by the NSO Group and allowed attackers to take over users' phones.⁶⁴ However, NSO is not the only private company exploiting such weaknesses and offering commercial exploitation services. DarkMatter and Gamma Group offer similar utilities, mostly used by nation-states for surveillance operations.^{65,66} Not just new and expensive vulnerabilities threaten mobile platforms. Check Point Research revealed that even popular mobile applications, available on the Google Play, remain susceptible to long-known vulnerabilities in their dependencies.⁶⁷

Nation-states and professional corporations are not the only ones to take part in this venture. Smaller actors offer Malware as a Service (MaaS) and their frequency in the malware landscape is increasing.

-
- 53 "Gustuff: Weapon of Mass Infection," by Ivan Pisarev, Group IB, April 4, 2019
 - 54 "Cerberus: A New Android 'Banking Malware for Rent' Emerges, by Swati Khandelwal, The Hacker News, August 13, 2019
 - 55 "New SIM Card Flaw Lets Hackers Hijack Any Phone Just by Sending SMS," Mohit Kumar, The Hacker News, September 12, 2019
 - 56 "Criminals are Tapping into the Phone Network Backbone to Empty Bank Accounts," by Joseph Cox, Vice, January 31, 2019
 - 57 "Tibetan Groups Targeted with 1-Click Mobile Exploits," by Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Robert Diebert, Munk School, September 24, 2019
 - 58 "Mobile Cyberespionage Campaign 'Bouncing Golf' Affects Middle East, by Ecular Xu and Grey Guo, Trend Micro, June 18, 2019
 - 59 "Exodus: New Android Spyware Made in Italy," Security Without Borders, March 20, 2019
 - 60 "Android Ransomware is Back," by Lukas Stefanko, WeLiveSecurity, July 29, 2019
 - 61 "Attackers Exploit 0-day Vulnerability that Gives Full Control of Android Phones," by Dan Goodin, Ars Technica, October 3, 2019
 - 62 "Android: New StrandHogg Vulnerability is Being Exploited in the Wild," by Catlin Cimpanu, ZDNet, December 2, 2019

-
- 63 "Mysterious iOS Attack Changes Everything We Know About iPhone Hacking," by Andy Greenberg and Lily Hay Newman, Wired, August 30, 2019
 - 64 "The NSO WhatsApp Vulnerability – This is How It Happened," by Check Point Research, May 14, 2019
 - 65 "Inside the UAE's Secret Hacking Team of American Mercenaries," by Christopher Bing and Joel Schectman, Reuters, January 30, 2019
 - 66 "Powerful FinSpy Spyware Found Targeting iOS and Android Users in Myanmar," Swati Khandelwal, The Hacker News, July 10, 2019
 - 67 "Long-known Vulnerabilities in High-Profile Android Applications," by Slava Makkaveev, Check Point Research, November 21, 2019

This year, we witnessed the discontinuation of the Anubis banking Trojan and the rise of Cerberus with its integrated evasion techniques, which are offered to paying-customers in underground forums.^{68, 69}

As we stated in our midyear report, the mobile arena is gearing up with more vulnerabilities exposed and exploited.⁷⁰ New malware strains are being migrated to the mobile arena, and actors of all sizes are hacking into valuable assets available through our mobile devices.

TARGETED RANSOMWARE

Ransomware attacks have remained active, but with one main difference in 2019: They're more targeted. Ransomware distribution has shifted from a numbers game to a more targeted approach of "big game hunting," where advanced threat actors find or buy their way into specific target organizations. This has enabled them to encrypt vital infrastructure and demand high ransom payments.

The targeted approach almost entirely replaced the mass distribution method for ransomware, which peaked in 2017 through 2018. At its highest, over 30 percent of all businesses, as well as many home users, were impacted.

The majority of successful targeted attacks were fueled by the growing cooperation between threat actors. One example is the massive spam distribution of Emotet, which found a foothold in many corporations worldwide, opening the door to other threat actors willing to pay for access. As a result, what started as a "simple" Emotet infection often expanded into a full-blown infection of the Ryuk or Bitpaymer ransomwares, operated by the Trickbot and Dridex gangs respectively.

Different threat actors have different methods so the initial infection vector of such ransomware attacks can vary. This can range from spear-phishing to hacking into unsecured and misconfigured RDP servers and to outsourcing it to botnet operators. And in some cases, they even used torrent uploaders and Managed Service Providers to gain the initial foothold inside big companies.^{71, 72}

Rather than immediately deploy a ransomware, offenders often spend weeks exploring the compromised network to locate high-value assets as well as backups, thus maximizing their damage. Ironically, companies that try to protect their data by using cloud services occasionally find that their service provider itself has been targeted.^{73,74}

68 "Anubis Android Banking Malware Returns with Extensive Financial App Hit List," by Charlie Osborne, ZDNet, July 9, 2019

69 "Cerberus- A New Banking Trojan from the Underworld," Threat Fabric, August, 2019

70 "The Evolution of Cyber Attacks in 2019," Check Point Software Technologies LTD, July 2019

71 "Torrent Sites Ban Popular Uploader 'CracksNow' for Sharing Ransomware," by Ernesto, Torrent Freak, February 17, 2019

72 "Ransomware Gangs Hack MSPs to Deploy Ransomware on Customer Systems," by Catalin Cimpanu, ZDNet, June 20, 2019

73 "Ransomware Bites Dental Data Backup Firm," Krebs on Security, August 29, 2019

74 "Cloud Hosting Provider DataResolution.net hit by the Ryuk Ransomware," Security Affairs, Pierluigi Paganini, January 2, 2019

At the top of the victims list, software services, health care, and government are the most targeted sectors. US municipalities were a popular choice in the public sector in 2019, including Orange County CA (\$400K ransom), Cleveland Hopkins International Airport, City of Baltimore (\$18M recovery cost), Riviera Beach City (\$600K ransom), Lake City, Florida (\$500K ransom), La Porte County IN (\$130K ransom), New Bedford MA (\$5.3M ransom) and more.^{75,76,77,78,79, 80,81}

Once their files are encrypted, victims face the choice of paying ransomware or suffering high recovery costs or permanent loss of data. Many, like Norsk Hydro Aluminum, opt to not pay ransom demands and find the recovery costs extremely high (\$50M).^{82,83} Others ignored public resolutions against paying but found their data was still inaccessible afterward, likely due to the

threat actor's unreliability or incompetence.^{84,85} The tendency to pay demands, sometimes encouraged by insurers, might be one of the major reasons behind this year's explosion of targeted ransomware attacks.

REEMERGENCE OF EXPLOIT KITS

Exploit Kits belong to a small yet not very exclusive club – Drive-By attacks. They allow threat actors to infect unaware users just by browsing to a compromised website from a vulnerable browser, without any additional action on the user's part. This technique is effective. It relies heavily on unpatched browsers and plugins like Internet Explorer and Adobe Flash for successful exploitation. As a direct result, the popularity and effectiveness of such Exploit Kits fluctuates according to the disclosure of new browser vulnerabilities. When a new vulnerability is disclosed, the attackers are presented with a small window of opportunity, where they can potentially exploit a large base of end-users, until a patch is widely deployed. In 2019 however, after a steady decline in their popularity, we have witnessed a resurgence of new exploit kits that are unrelated to the release of new vulnerabilities. Overall, at least six new exploit kits were observed in the wild, which contradicted expected behavior, as no new easy-to-implement high-risk vulnerabilities were disclosed during 2019.

75 "Orange County Computer Network Hit by Ransomware Attack," by Zachary Eanes, The News & Observer, March 18, 2019

76 "Cleveland Acknowledges for First Time Hopkins Airport Hack Involved Ransomware," Cleveland.com, April 29, 2019

77 "Baltimore Estimates Cost of Ransomware Attack at \$18.2 Million as Government Begins to Restore Email Accounts," The Baltimore Sun, by Ian Duncan, May 29, 2019

78 "The Riviera Beach City Pays \$600,000 in Ransom," by Pierluigi Paganini, Security Affairs, June 20, 2019

79 "Two Florida Cities Paid \$1.1 Million to Ransomware Hackers This Month," by Mohit Kumar, The Hacker News, June 26, 2019

80 "La Porte County Pays \$130,000 Ransom to Ryuk Ransomware," by Ionut Ilascu, Bleeping Computer, July 14, 2019

81 "Ransomware Gang Wanted \$5.3 Million from US City, but They Only Offered \$400,000," by Catalin Cimpanu, ZDNet, September 4, 2019

82 "Norsk Hydro Will Not Pay Ransom Demand and Will Restore From Backups," by Catalin Cimpanu, ZDNet, March 22, 2019

83 "Norsk Hydro Estimates March Cyber Attack Cost at \$50 Million," by Pierluigi Paganini, Security Affairs, April 30, 2019

84 "Mayors Pass Resolution Against Paying Ransomware Ransoms," by Colin Wood, Statescoop, July 10, 2019

85 "Payroll Provider Gives Extortionists a Payday," Krebs on Security, February 23, 2019

We also witnessed the arrival of the SpelevoEK, which exploits a flash vulnerability with Virtual-Machine evasion functionality.⁸⁶ In July, RadioEK was observed using well-known vulnerabilities to deliver AZORult stealer and Nemty ransomware, mostly in Japan.⁸⁷ This was followed by LordEK delivering njRAT and Eris ransomware.⁸⁸ In September, we “welcomed” Purple Fox, which was previously delivered by RigEK, but matured into an independent fileless exploit kit, as well as BottleEK which targeted the Japanese market.^{89, 90} In October, CapesandEK reshaped publicly shared source code into a new stealthy product.⁹¹

Though these new exploit kits do not introduce any new complexity or previously unseen features to the ecosystem, and they’re often just copy-pasted from known vulnerabilities, POC code, and other exploit kits, they’re still effective. A previous report by Check Point Research shows the potential of exploit kits as an infection source, as well as the market they’re sold in.⁹² Overall, the sharp rise in the popularity of exploit kits means that more unprotected users are exposed to this threat.

86 “2019-03-16 – Spelevo Ek Examples,” Malware Traffic Analysis.Net

87 “Weak Drive-by Download attack with “Radio Exploit Kit,” nao_sec, July 15, 2019

88 “Virus Bulletin Researcher Discovers New Lord Exploit Kit,” by Martjin Grooten, Virus Bulletin, August 5, 2019

89 “Say hello to Bottle Exploit Kit targeting Japan,” nao_sec, December 12, 2019

90 “‘Purple Fox’ Fileless Malware with Rookit Component Delivered by Rig Exploit Kit Now Abuses PowerShell,” by Trend Micro, Trend Micro, September 9, 2019

91 “New Exploit Kit Capes and Reuses Old and New Public Exploits and Tools, Blockchain Ruse,” by Trend Micro, Trend Micro, November 5, 2019

92 “Inside the Hacking Community Market – Reselling RIG EK Services,” Check Point Research, October 24, 2019

CHAPTER 5



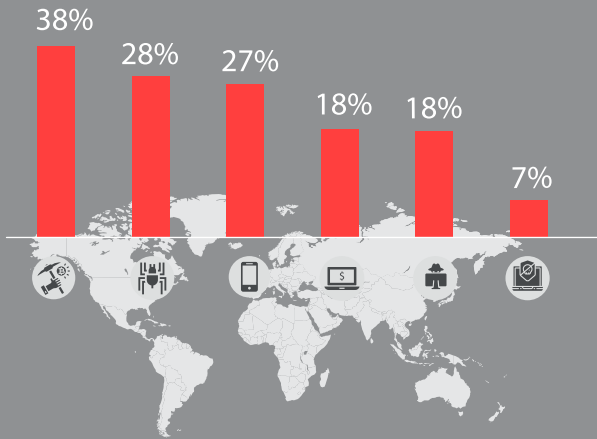
GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections of this report are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between January and December 2019⁹³

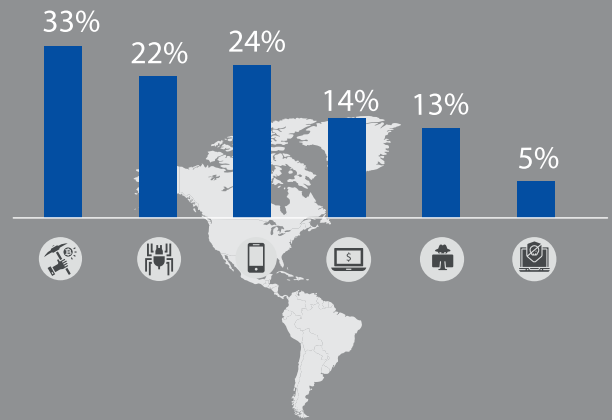
⁹³ "Live Cyber Threat Map," Check Point Software LTD

CYBER ATTACK CATEGORIES BY REGION

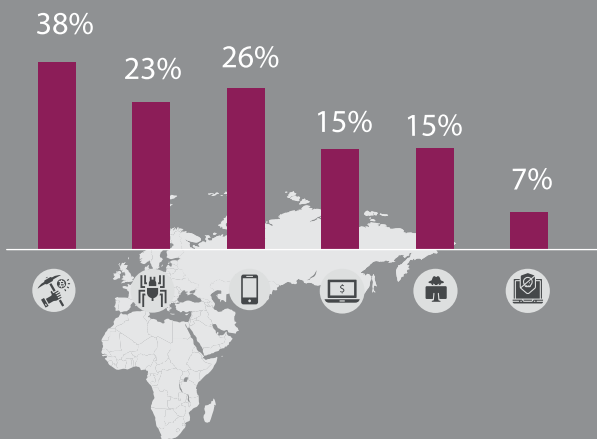
GLOBAL



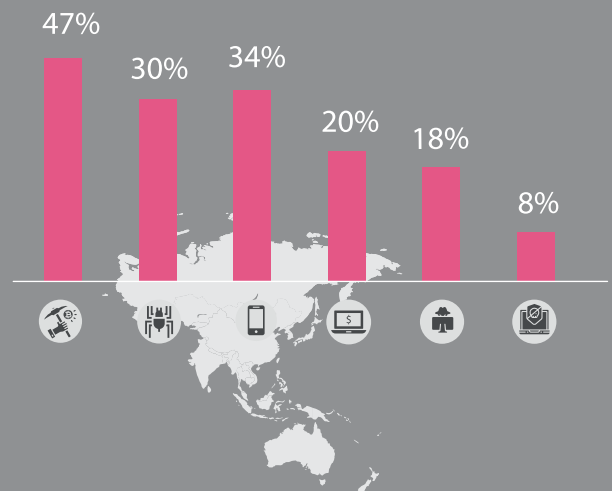
AMERICAS



EUROPE, MIDDLE EAST, AND AFRICA (EMEA)



APAC



Crypto miners



Botnet



Mobile



Banking



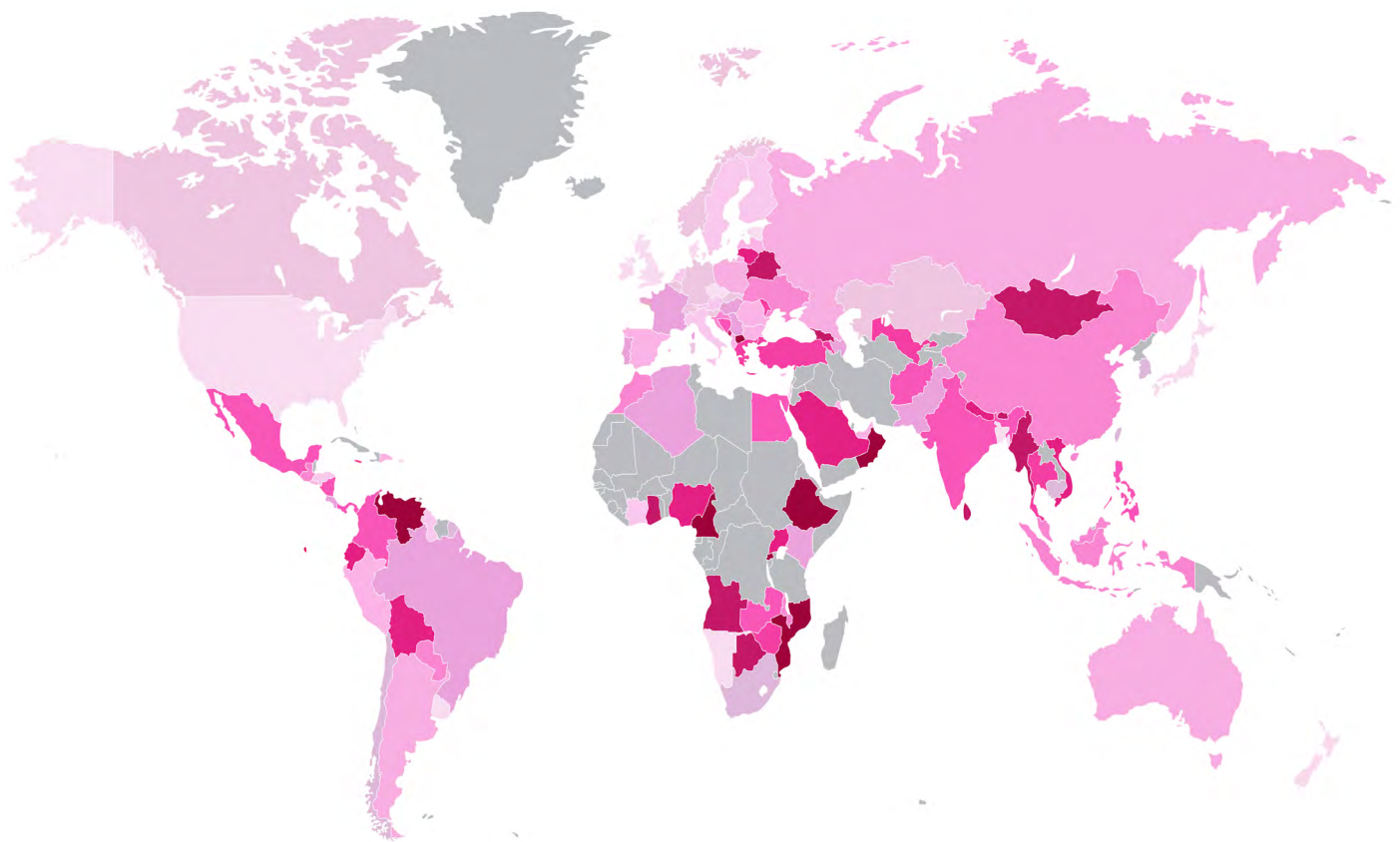
Infostealer



Ransomware

GLOBAL THREAT INDEX MAP

Check Point's Threat Index is based on the probability that a machine in a certain country will be attacked by malware. This is derived from the ThreatCloud World Cyber Threat Map, which tracks how and where cyberattacks are taking place worldwide in real time.



TOP MALICIOUS FILE TYPES: WEB VS EMAIL

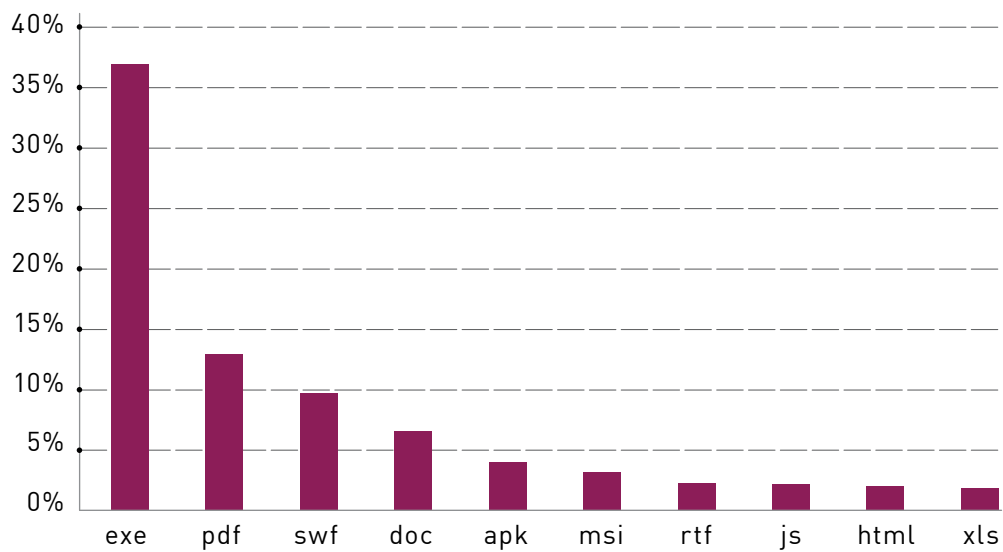


Figure 1: Web – Top malicious file types

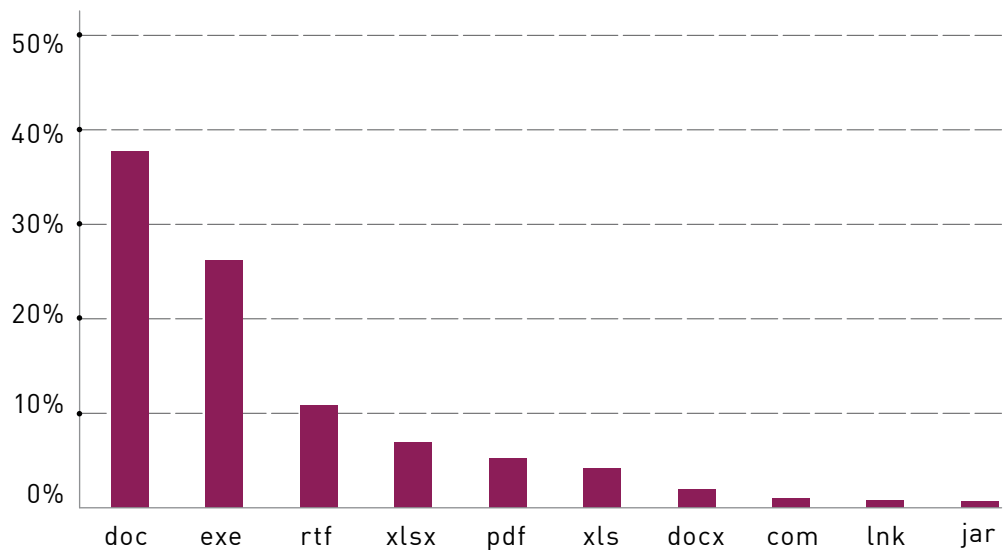


Figure 2: Email – Top malicious file types

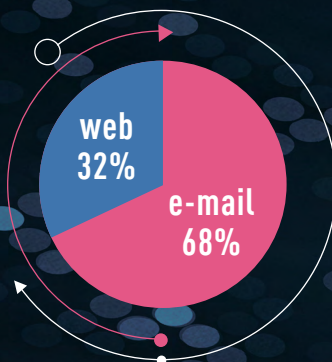


Figure 3: Distribution protocols – Email vs web attack vectors

TOP MALWARE FAMILIES

GLOBAL

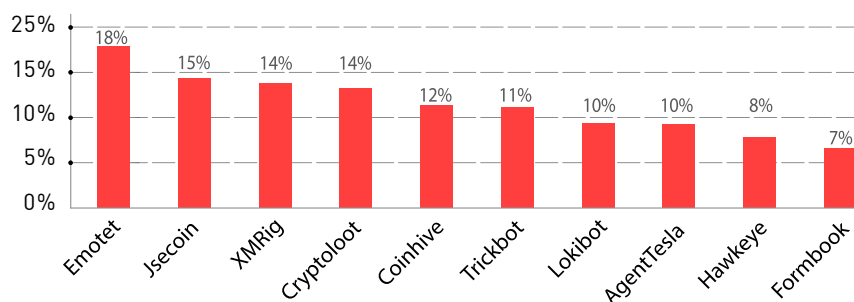


Figure 4: Most Prevalent Malware Globally
Percentage of corporate networks impacted by each malware family

AMERICAS

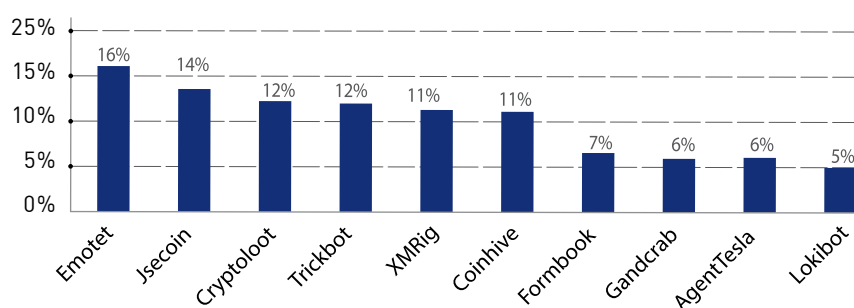


Figure 5: Most Prevalent Malware in the Americas

EUROPE, MIDDLE EAST, AND AFRICA (EMEA)

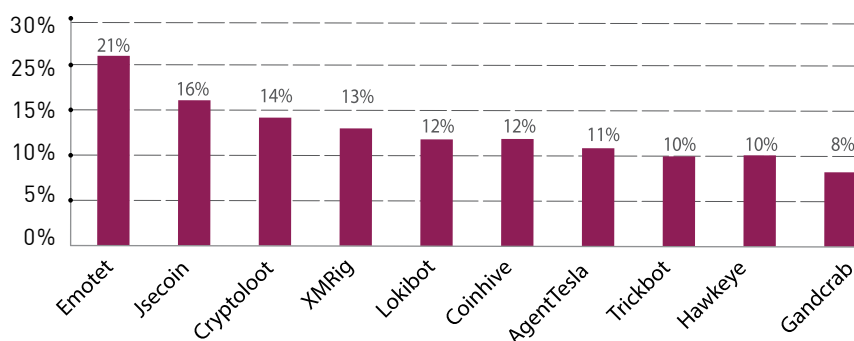


Figure 6: Most Prevalent Malware in EMEA

ASIA PACIFIC (APAC)



Figure 7: Most Prevalent Malware in APAC

GLOBAL ANALYSIS OF TOP MALWARE

Cryptominers remain the most prevalent malware type with a small decrease in most regions. On the other hand, ransomware presented a slight increase compared to 2018, though still remaining at the bottom of the malware type list. While the number of impacted companies is relatively low, the severity of the attack on each company is much higher. This is the result of the year-old business model of targeted ransomware attacks. We measured a surge in botnet activity, likely fueled by the increasing revenue they generate, through malware distribution services, malspam, sextortion email activity, and DDoS attacks.

EMOTET

First identified in 2014 and classified as a Banking Trojan, Emotet was designed to steal personal financial information. But like many other malware families, it has since evolved to use its existing assets for additional income sources and upgraded its evasion and propagation mechanisms. In 2019, Emotet had evolved into a botnet, mostly distributed via large-scale spam campaigns. Emotet has established itself as a king amongst malware distributors, capable of delivering infections to a large number of infected hosts. It is also able to act as a launching platform for precise and coordinated attacks against well-financed organization. Most notable is the cooperation of Emotet with Trickbot and Dridex, which resulted in a number of devastating ransomware attacks.⁹⁴

94 "Triple Threat: Emotet Deploys Trickbot to Steal Data & Spread Ryuk," by Noa Pinkas, Lior Rochberger and Matan Zatz, Cybereason, April 2, 2019

TOP CRYPTOMINING MALWARE

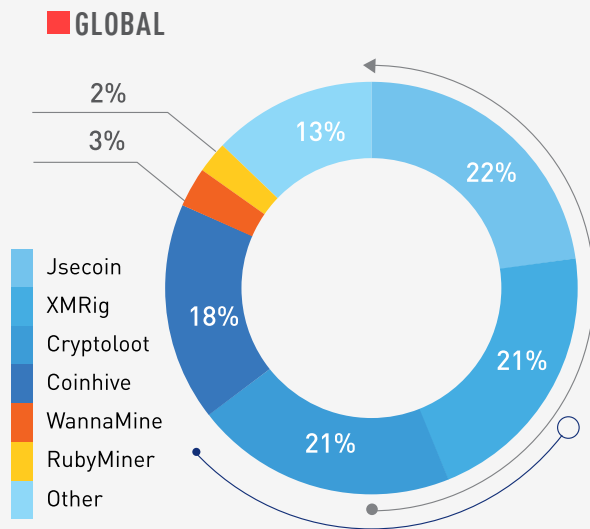


Figure 8: Top Cryptomining Malware Globally

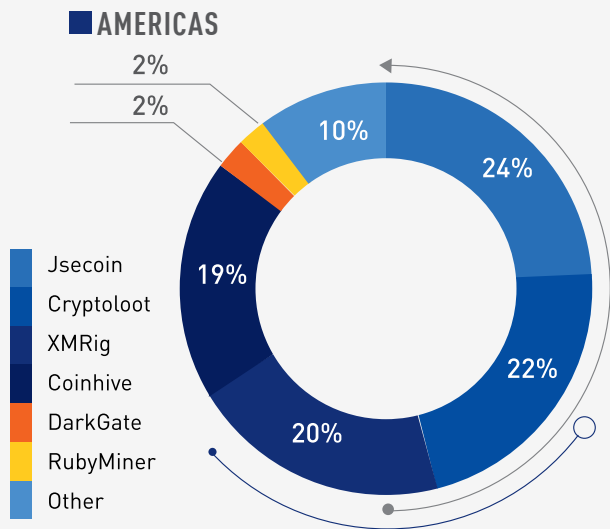


Figure 9: Top Cryptomining Malware in the Americas

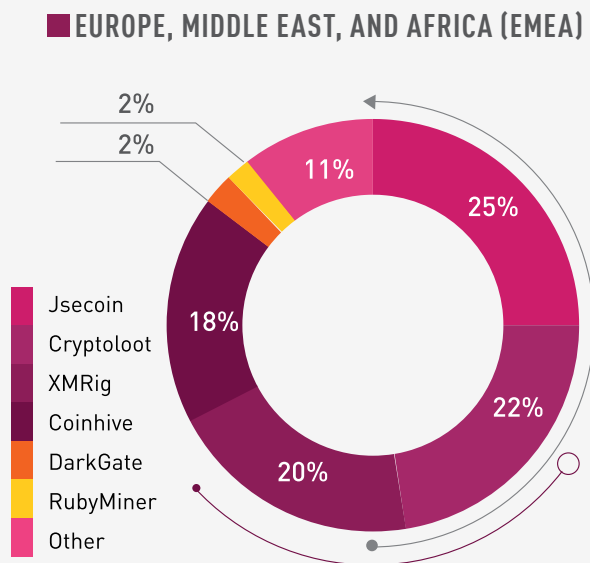


Figure 10: Top Cryptomining Malware in EMEA

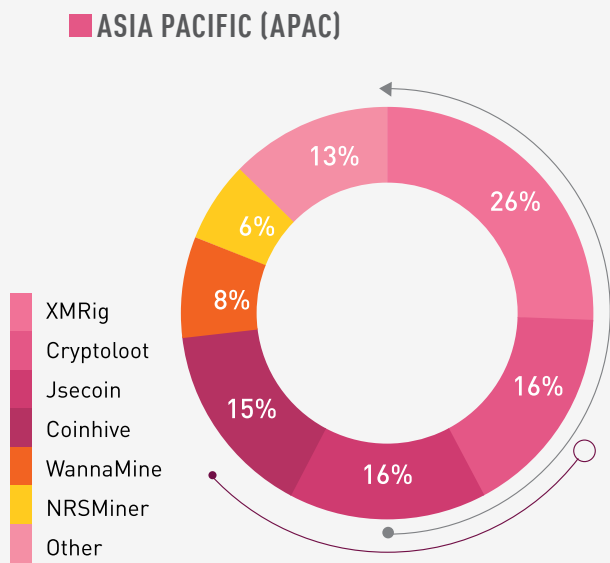


Figure 11: Top Cryptomining Malware in APAC

CRYPTOMINERS GLOBAL ANALYSIS

Coinhive, the drive-by cryptominer, shut down its operations in March, ceasing to exploit websites and online games for mining Monero.⁹⁵ Thus, Coinhive vacated its high place in the cryptominers arena to JSEcoin and Cryptoloot. XMRig, an open source Monero mining software often abused by various malware (like NRSMiner) for local exploitation of victim's resources, especially dominates the Asia pacific [APAC] area.

BANKING TROJANS GLOBAL ANALYSIS

Trickbot and Ramnit populate the top places of the banking Trojans table. Their popularity is due to fact that they not only serve as banking Trojans but also offer additional services. This is definitely a trend as pure banking Trojans have become rare once threat actors realized that a foothold on a victim's machine could be used for a lot more than just stealing sensitive banking information.

⁹⁵ "Coinhive Dead but Browser-Based Cryptomining Still a Threat," by Ionut Ilascu, Bleeping Computer, May 2, 2019

RAMNIT

Ramnit, the prolific banking Trojan, has kept its place at the top of the 2019 banking Trojan list. Over the years, Ramnit has expanded its targets to include online advertising, web services, social networking, and e-commerce sites. In 2019, Ramnit returned to its roots and was spotted largely targeting financial services websites to coincide with tax return activity, primarily in Italy.⁹⁶

⁹⁵ "Coinhive Dead but Browser-Based Cryptomining Still a Threat," by Ionut Ilascu, Bleeping Computer, May 2, 2019

⁹⁶ "Ramnit Returns to its Banking Roots, Just in Time for Italian Tax Season," by Remi Cohen and Roy Moshailov, F5 Application Threat Intelligence, April 23, 2019

TOP BANKING TROJANS

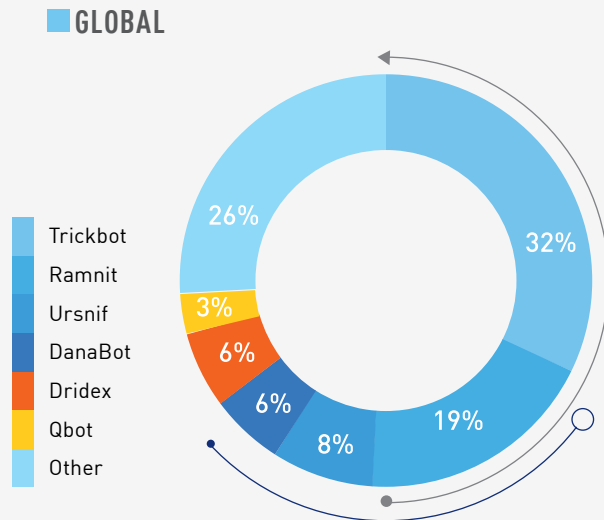


Figure 12: Most Prevalent Banking Trojans Globally

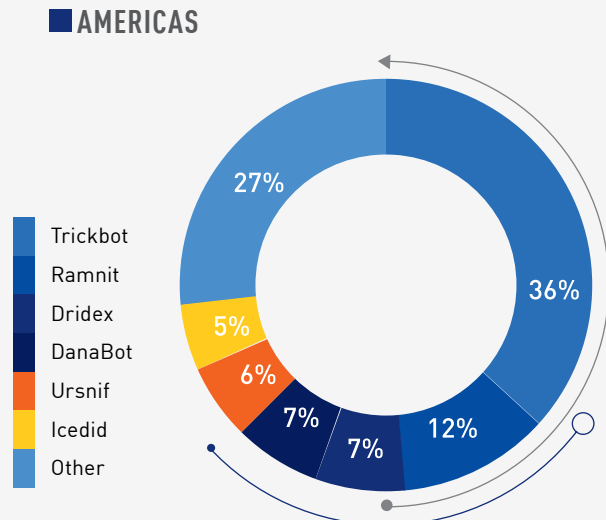


Figure 13: Most Prevalent Banking Trojans in the Americas

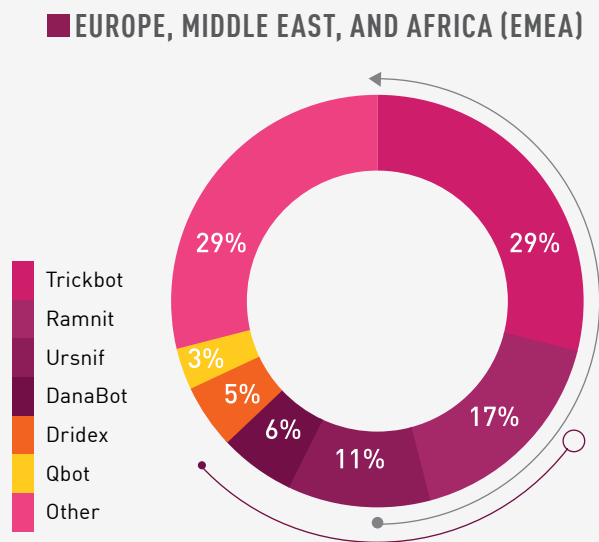


Figure 14: Most Prevalent Banking Trojans in EMEA

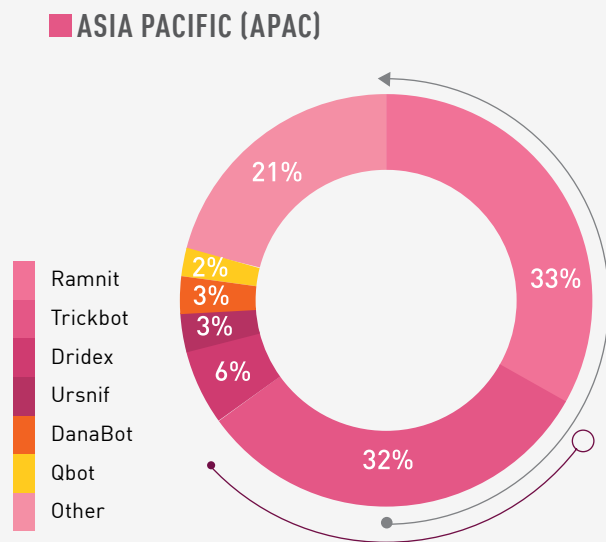


Figure 15: Most Prevalent Banking Trojans in APAC

BOTNET GLOBAL ANALYSIS

Many of today's popular botnets were initially specialized to a single task. Banking Trojans like Emotet and Trickbot make use of their resources and infrastructure to spread other malware and have long become full featured botnets. Cryptominers like KingMiner⁹⁷ have upgraded their operation to fully mature botnets. Other botnets like Phorpiex⁹⁸ diversify their operations to generate income from Sextortion operations in addition to regular malspam campaigns and DDoS services.

TRICKBOT

Trickbot is a notorious Banking Trojan known since 2016. Besides its impressive capabilities in stealing banking information, Trickbot acts as a botnet, with a modular architecture enabling agile functionality for the gang behind it. Whether they're selling installations for other threat actors, stealing banking credentials, mining Cryptocurrency, or launching a full-scale APT operation, the operators behind Trickbot have the platform to do it all.⁹⁹

97 "KingMiner: The New and Improved CryptoJacker," by Ido Solomon and Adi Ikan, Check Point Research, November 29, 2018

98 "In the Footsteps of a Sextortion Campaign," by Gil Mansharov and Alexey Bukhteyev, Check Point Research, October 16, 2019

99 "Anchor Project, The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT," by Vitali Kremez, December 10, 2019

TOP BOTNETS

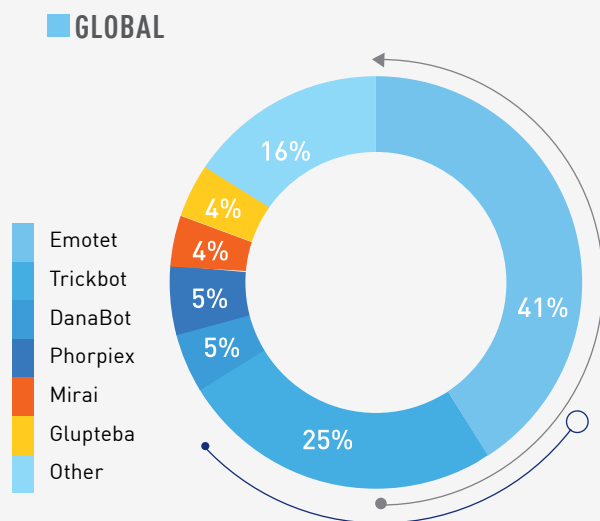


Figure 16: Most Prevalent Botnets Globally

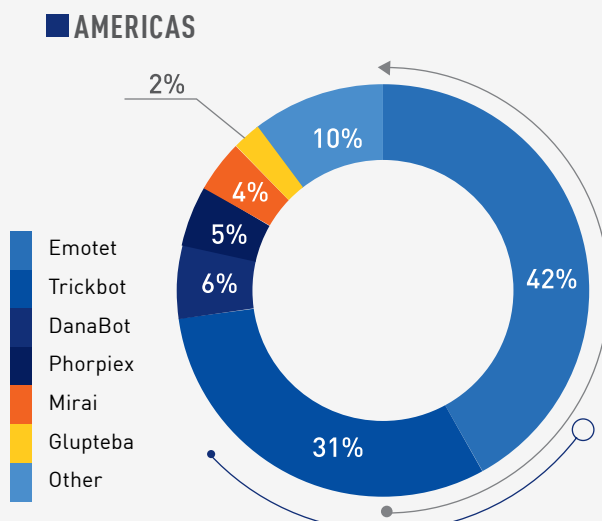


Figure 17: Most Prevalent Botnets in the Americas

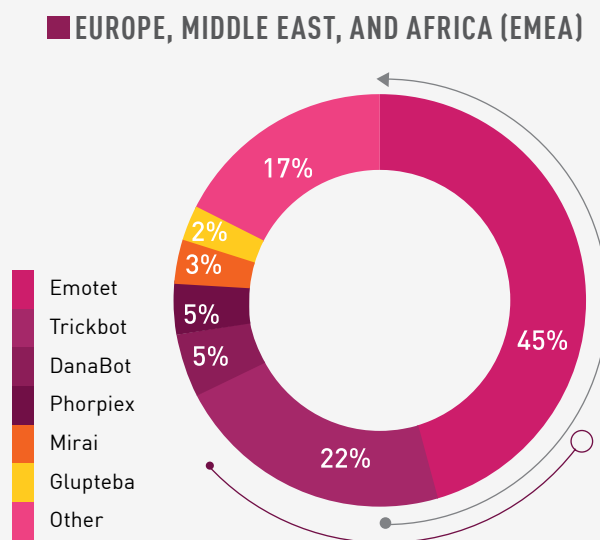


Figure 18: Most Prevalent Botnets in EMEA

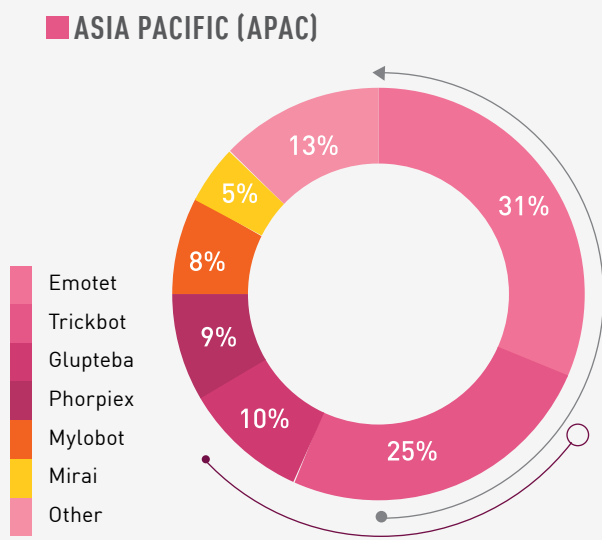


Figure 19: Most Prevalent Botnets in APAC

MOBILE MALWARE GLOBAL ANALYSIS

NECRO

Necro, the Android Trojan, was an unexpected addition to our top charts. Responsible for this quick rise to the top, is the CamScanner app - available on the Google Play store. With more than 100 million installations, CamScanner is one of the most popular document-to-pdf applications on the app store. This entire user base was instantly exposed to a malicious backdoor once the developers of the application unknowingly switched their ads library to a back-doored one infected with Necro.¹⁰⁰

Adware continues to be one of the most lucrative business models for mobile malware authors. This is substantiated by our top mobile malware, including Guerrilla, AndroidBauts, and the newly discovered xHelper, being ads and click-fraud related.¹⁰¹

100 "Malicious Android app had More Than 100 Million Downloads in Google Play," by Kaspersky Team, Kaspersky Daily, August 27, 2019

101 "Xhelper: Persistent Android Dropper App Infects 45K Devices in Past 6 Months," by May Ying Tee and Tommy Dong, Symantec, October 29, 2019

TOP MOBILE MALWARE

GLOBAL

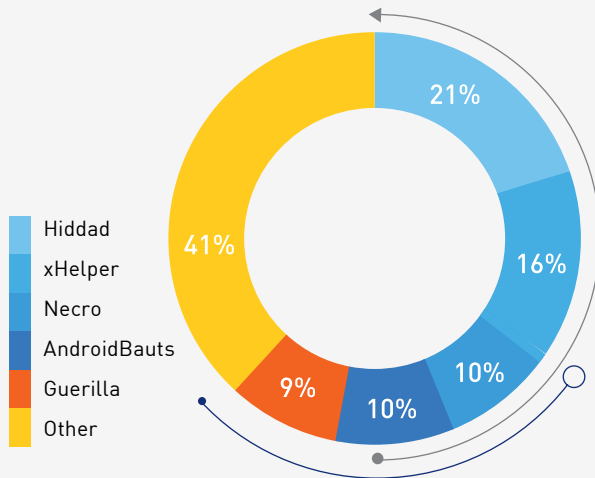


Figure 20: Top Mobile Malware Globally

AMERICAS

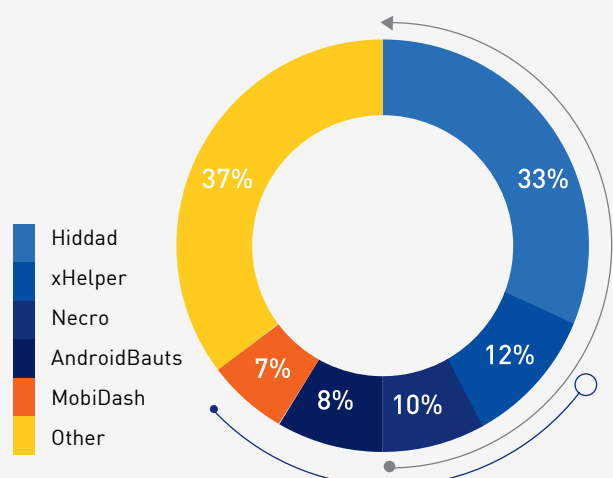


Figure 21: Top Mobile Malware in the Americas

EUROPE, MIDDLE EAST, AND AFRICA (EMEA)

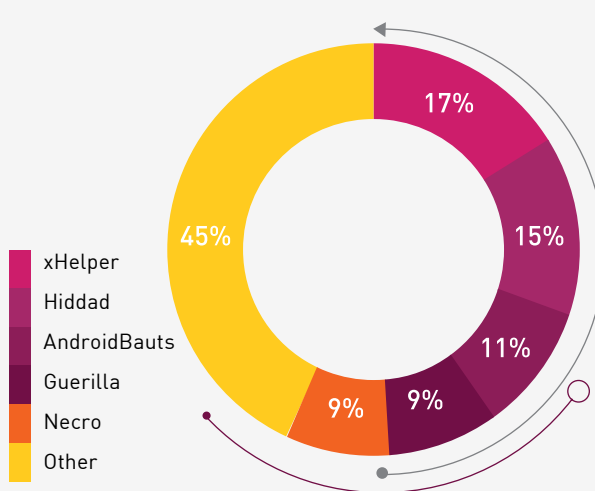


Figure 22: Top Mobile Malware in EMEA

ASIA PACIFIC (APAC)

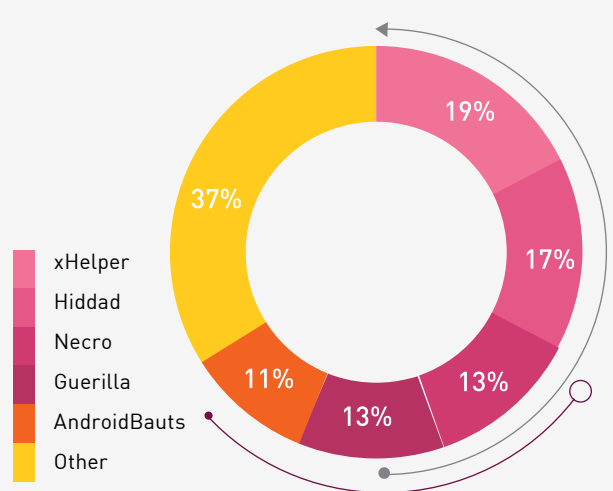


Figure 23: Top Mobile Malware in APAC

INFOSTEALER GLOBAL ANALYSIS

Not surprisingly, commodity malware dominates the infostealer arena. New and non-proficient threat actors would download or buy off-the-shelf malware from hacking forums and dark markets. These ready-to-launch kits often come in an easy-to-install package, including a payload generator where you can configure multiple functionality options and a C&C web panel to where all the stolen information would be collected and displayed.

FORMBOOK

Introduced in 2016, Formbook has immediately gained popularity among the community of beginning threat actors. It's a classic example of malware as a service. For around \$50, the authors provide a hosted instance of Formbook, minimizing the infrastructure building overhead for the attackers who want to launch a campaign. This simplicity brought it to the top of the malware list, with new Formbook spam campaigns launched on a weekly basis.¹⁰²

Formbook itself is relatively advanced for commodity malware. It's coded in Assembly with a number of built-in anti-analysis and anti-sandbox techniques to evade detection. It possesses everything the attacker needs to successfully spy on a target, including browser form grabbing, screenshots taking, password theft, and additional payload execution.

102 "More Malspam Pushing Formbook," SANS ISC InfoSec Forums, 2019

TOP INFOTEALER MALWARE

GLOBAL

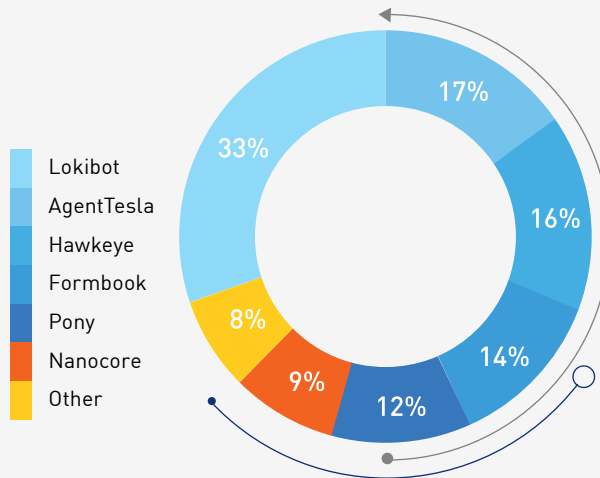


Figure 24: Top Infostealer Malware Globally

AMERICAS

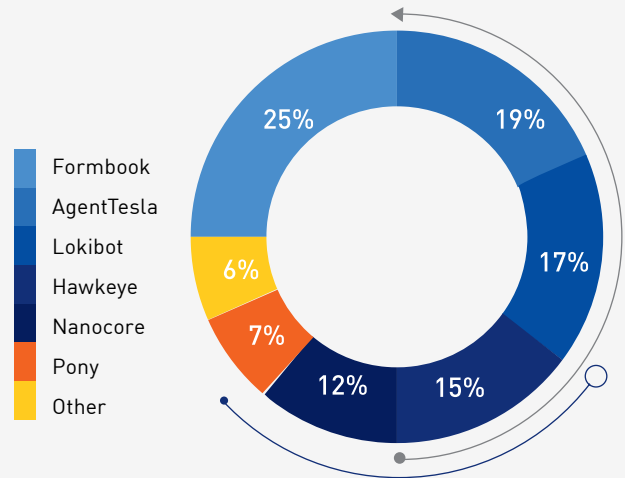


Figure 25: Top Infostealer Malware in the Americas

EUROPE, MIDDLE EAST, AND AFRICA (EMEA)

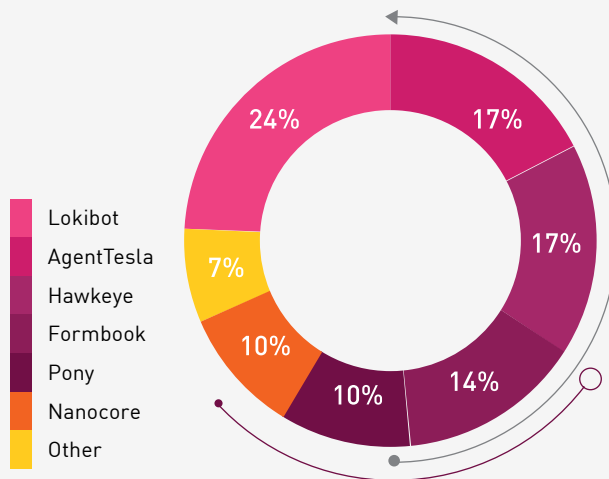


Figure 26: Top Infostealer Malware in EMEA

ASIA PACIFIC (APAC)

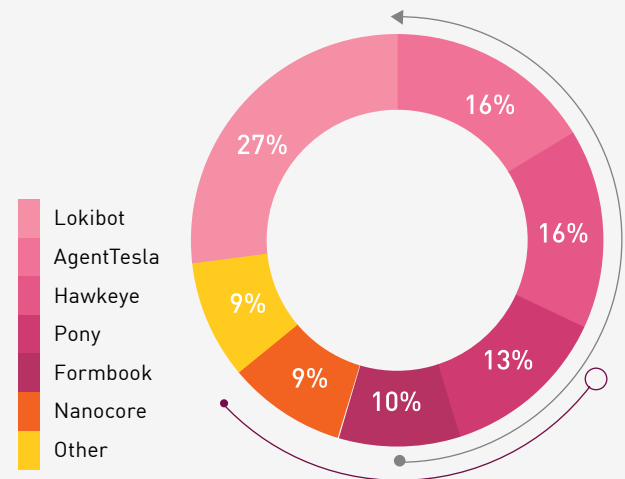


Figure 27: Top Infostealer Malware in APAC

CHAPTER 6



HIGH-PROFILE GLOBAL VULNERABILITIES

The following list of top attacks is based on data collected by the Check Point Intrusion Prevention System (IPS) sensor-net and details some of the most popular and interesting attack techniques and exploits observed by Check Point researchers in 2019.

MICROSOFT RDP VULNERABILITIES: BLUEKEEP AND DEJABLUE (CVE-2019-0708, CVE-2019-1182)

First reported in May 2019, BlueKeep was highlighted as critical security vulnerability by Microsoft, followed by additional related vulnerabilities months later, dubbed DejaBlue. The vulnerabilities exist in the Remote Desktop Protocol (RDP), allowing Remote Code Execution (RCE), which is especially dangerous due to its wormable nature that could lead to quick worldwide epidemic. Soon after its publication, actors started scanning the internet for vulnerable devices. By September, Metasploit released a BlueKeep exploit and in November, the first campaign exploiting BlueKeep has been reported, leveraging it to install cryptominers.^{103,104,105} To this point, no wormable variant of malware using these RDP exploits has been detected in the wild, with a WannaCry scale disaster still waiting to happen.

103 "Internet Scans Found Nearly One Million Systems Vulnerable to BlueKeep," by Pierluigi Paganini, Security Affairs, May 28, 2019

104 "Exploit for Wormable BlueKeep Windows Bug Released Into the Wild," by Dan Goodin, Ars Technica, September 6, 2019

105 "First Cyber Attack 'Mass Exploiting' BlueKeep RDP Flaw Spotted in the Wild," by Pierluigi Paganini, Security Affairs, November 3, 2019

ORACLE WEBLOGIC SERVER VULNERABILITIES

[CVE-2017-10271, CVE-2019-2725]

The various critical remote code execution vulnerabilities that reside in Oracle WebLogic Servers allow unauthorized attacker to remotely execute arbitrary code, and affect numerous applications and web enterprise portals using the servers. This year alone cyber criminals have exploited the Oracle WebLogic Server vulnerabilities including the newly discovered one, which has been patched this April, to deliver the Sodinokibi ransomware as well as the Satan ransomware, and to install Monero Cryptomining malware.^{106,107,108}

EXIM MAIL SERVER REMOTE CODE EXECUTION VULNERABILITY

[CVE-2019-10149]

A significant vulnerability disclosed this year targets the popular MTA software Exim. An attacker can easily exploit this vulnerability by sending a crafted packet to the victim's server, leveraging insufficient validation in the recipient's email address. Successful exploitation can result in the execution of arbitrary commands. This year we have witnessed a significant amount of exploitation attempts in the wild, as new malware strains have abused this newly discovered vulnerability in order to install cryptomining software on targeted servers.¹⁰⁹

Interestingly, according to Check Point global attack sensors, throughout 2019, 85% of the attacks observed leveraged vulnerabilities registered in 2017 and earlier.

106 "Crooks Exploit Oracle WebLogic Flaw to Deliver Sodinokibi Ransomware," by Pierluigi Paganini, Security Affairs, May 1 2019

107 "The Satan Ransomware Adds New Exploits to its Arsenal," by Pierluigi Paganini, Security Affairs, May 22 2019

108 "CVE-2019-2725 Exploited and Certificate Files Used for Obfuscation to Deliver Monero Miner," by Mark Vicente, Johnlery Triunfante, and Byron Gelera, Trend Micro, June 10 2019

109 "New Pervasive Worm Exploiting Linux Exim Server Vulnerability," by Amit Serper and Mary Zhao, Cyber Reason, June 13, 2019

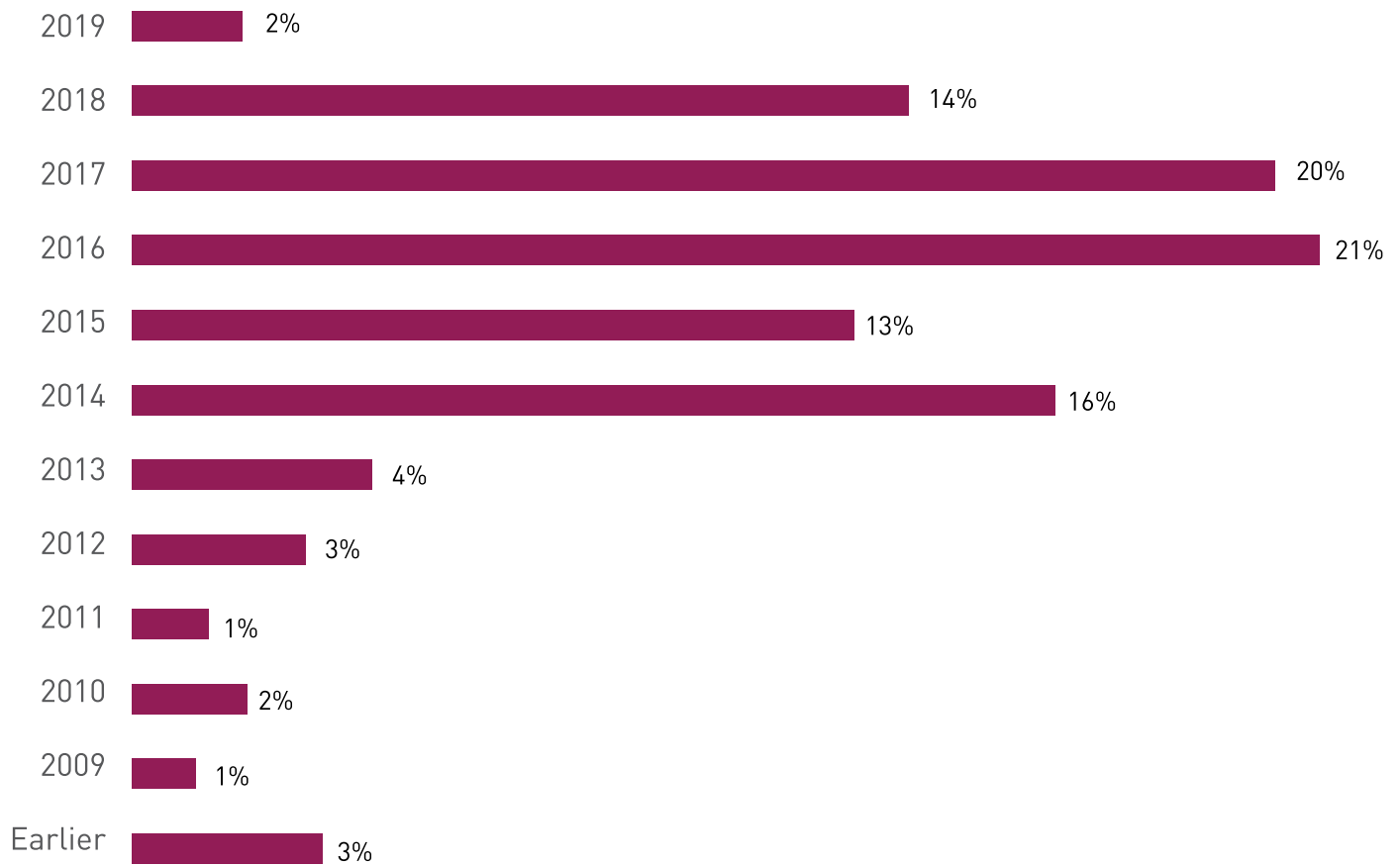
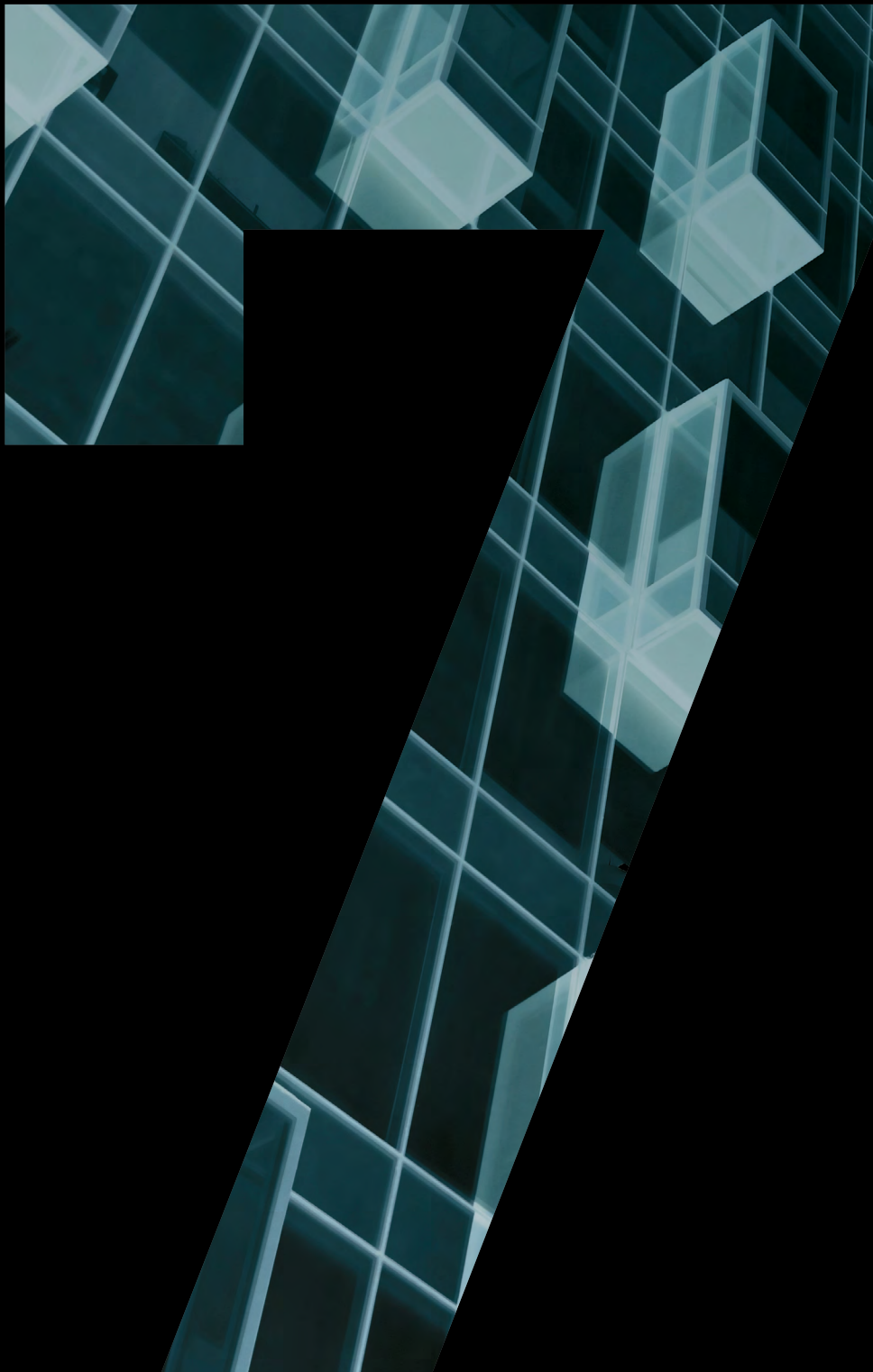


Figure 28: Exploited CVEs by Year

CHAPTER 7




REVIEW OF 2019 CYBER THREAT PREDICTIONS

CLOUD

We expected to see threat actors targeting specific company departments and employees, also known as spear phishing, in order to reap more lucrative rewards. The growing popularity of public cloud environments has led to an increase of cyber attacks targeting resources and sensitive data residing within these platforms. While more organizations move to the cloud, awareness that they are still responsible for the security of data held there is still lagging.

Following the 2018 trend, practices such as misconfiguration and poor management of cloud resources remained the most prominent threat to the cloud ecosystem in 2019 and, as a result, subjected cloud assets to a wide array of attacks. This year, misconfiguring cloud environments was one of the main causes for a vast number of data theft incidents experienced by organizations worldwide.



In April, more than half a billion records of Facebook's users were exposed by a third party on unprotected Amazon cloud servers. Misconfigured Box.com accounts leaked terabytes of extremely sensitive data from many companies, and in another case sensitive financial information of 80 million Americans hosted on a Microsoft cloud server was exposed online. Besides information theft, threat actors intentionally abused the different cloud technologies for their computing power.

So far this year, cloud cryptomining campaigns stepped up, upgraded their technique set and were capable of evading basic cloud security products, abusing hundreds of vulnerable exposed Docker hosts and even shutting down competitors' cryptomining campaigns operating in the cloud.

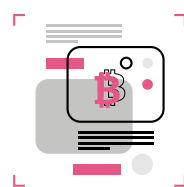
In addition, in 2019 Check Point researchers witnessed an increasing number of exploitations against public cloud infrastructures. A vulnerability in SoftNAS Cloud platform discovered in March may have allowed attackers to bypass authentication and gain access to a company's web-based admin interface and then run arbitrary commands.¹¹⁰ Furthermore, a new type of attack vector, dubbed Cloudborne, demonstrated that hardware re-provisioned to new customers could retain backdoors that can be used to attack future users of the compromised system.

¹¹⁰ Untitled, by Digital Defense Inc., SoftNAS Cloud Zero-Day Blog



KEY FINDINGS OF THE 2019 CLOUD SECURITY REPORT¹¹¹

- **The top four public cloud vulnerabilities:** the leading vulnerabilities cited by respondents were unauthorized cloud access (42%), insecure interfaces (42%), misconfiguration of the cloud platform (40%), and account hijacking (39%).
- **The leading operational cloud security headaches:** security teams struggle with a lack of visibility into cloud infrastructure security and compliance (67% in total). Setting consistent security policies across cloud and on premise environments and a lack of qualified security staff tie for third place (31% each).
- **Legacy security tools are not designed for public clouds:** 66% of respondents said their traditional security solutions either don't work at all, or only provide limited functionality in cloud environments.
- **Security challenges inhibit cloud adoption:** the biggest barriers to wider public cloud adoption cited by respondents are data security (29%), risk of compromise (28%), compliance challenges (26%) and a lack of experience and qualified security staff (26%).



THREAT ACTORS HAVE BEEN ADOPTING A NEW APPROACH REGARDING CRYPTOMINERS, AIMING AT MORE REWARDING TARGETS THAN CONSUMER PC'S AND DESIGNING MORE ROBUST OPERATIONS. AMONG THE NEW VICTIMS ONE CAN FIND CORPORATIONS, FACTORIES, POWERFUL SERVERS AND EVEN CLOUD RESOURCES.

NETWORK

The infamous cryptominers remained a prevalent malware type in 2019's threat landscape. This is despite the shutdown of the notorious drive-by mining service 'CoinHive' this March, which led to a decrease in the popularity of cryptominers among threat actors. As a result, and in order to remain prevalent in 2019, threat actors have been adopting a new approach regarding cryptominers, aiming at more rewarding targets than consumer PC's and designing more robust operations. Among the new victims one

111 "Cloud Security Challenges, Solutions, and Trends,"
Check Point Software Technologies LTD, 2019

can find corporations, factories, powerful servers and even cloud resources. And if that was not enough, we have even seen them integrating cryptominers as part of a DDoS botnet for side-profits.

DNS Attacks target one of the most important mechanisms that govern the internet – the Domain Name System (DNS). The DNS is in charge of resolving domain names into their corresponding IP addresses and it is a crucial part of the internet's trust chain. Such attacks target DNS providers, name registrars, and local DNS servers belonging to the targeted organization and are based on the manipulation of DNS records. DNS takeovers can compromise the whole network and enable multiple attack vectors: control of email communications, redirection of victims to a phishing site, and more. One of the biggest advantages DNS attacks provide is the option to issue legitimate looking certificates by Certificate Authorities which rely on DNS to verify that you are the legitimate holder of the domain in question.

The growing popularity of DNS attacks pushed the Department of Homeland Security and the Internet Corporation for Assigned Names and Numbers (ICANN) to issue official warnings of a significant risk to this key component of the Internet infrastructure. Large incidents involving DNS attacks include attacks on government and internet and telecommunications infrastructure, as depicted in the recent DNSspionage and SeaTurtle campaigns.

IOT

For enterprises 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 being targets in and of themselves. This is due to them being harder to secure while being adopted into the corporate infrastructure at an increasing rate, thus enlarging the attack surface. A recent industry study reveals: 67% of enterprises have experienced an IoT security incident.¹¹² From smart TV's, IP cameras, and smart elevators, to hospital infusion pumps and industrial PLC controllers, IoT and OT (Operational Technology) devices are inherently vulnerable and easy to hack. Many of these devices come with out-of-the-box security flaws such as weak or hardcoded passwords, misconfigurations in the operating system, and known vulnerabilities (CVEs). Their inherent security weaknesses and the fact that they are poorly protected made IoT devices an attractive target for bad actors.



**67% OF ENTERPRISES
HAVE EXPERIENCED
AN IOT SECURITY
INCIDENT**

¹¹² "State of Enterprise IT Security in North America: Unmanaged and Secured," Armis, 2019

Hackers are continually looking for ways to exploit device vulnerabilities so they can attack the devices themselves or better use them as an entry point to the corporate network. IP cameras can be used to spy on users, medical devices can be shut down, and critical infrastructure (such as power grid controllers) can be taken over to generate colossal damage. The risk is high and enterprises across different industries are exposed.

NATION-STATE

In the last few years governments have become highly concerned about cyber threats targeting critical infrastructures, such as power grids. As a result, many countries have formed entities such as CERTs. 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.

As seen in the recent cyber operations against Iran,¹¹³ following attacks on Saudi Arabia's oil facilities, this prediction found reality and will continue to do so moving forward. Another angle can be seen back in March 2019, when Amnesty International published a report that uncovered a targeted attack against journalists and human rights activists in Egypt.¹¹⁴ The victims even received an e-mail from Google warning them that government-backed attackers attempted to steal their passwords. According to the report, the attackers did not rely on traditional phishing methods or credential-stealing payloads, but rather utilized a stealthier and more efficient way of accessing the victims' inboxes: a technique known as "OAuth Phishing". By abusing third-party applications for popular mailing services such as Gmail or Outlook, the attackers manipulated victims into granting them full access to their e-mails. Check Point research traced these cyberattacks on Egyptian activists to government.

113 "Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials," by Idrees Ali, Reuters, October 15, 2019

114 "Phishing attacks using third-party applications against Egyptian civil society organizations," by Amnesty International, March 6, 2019



RECOMMENDATIONS TO PREVENT THE NEXT CYBER ATTACK

CHOOSE PREVENTION OVER DETECTION

Organizations that stress the prevention of unknown, zero-day threats can win the cyber security battle. Attacks from unknown threats pose critical risks to businesses, and unfortunately, they're also the hardest to prevent. That's why many businesses resort to detection-only protection. Some rely on event monitoring and threat hunting by Security Operations Center (SOC) teams to detect them after breaching their systems. But this is a far less effective strategy. The strategic imperative for organizations is to prevent cyber attacks before they breach enterprise systems.

Traditional cyber security vendors often claim that attacks will happen, and that there's no way to avoid them. They claim the only thing left to do is to invest in technologies that detect the attack once it has already breached the network, and mitigate the damages as soon as possible. This is untrue. Not only can attacks be blocked, but they can be prevented, including zero-day attacks and unknown malware. With the right technologies in place, the majority of attacks, even the most advanced ones can be prevented without disrupting the normal business flow.

LEVERAGING A COMPLETE UNIFIED ARCHITECTURE

Without a consolidated solution, companies need a long list of security tools to address all possible attack vectors. This approach can be needlessly complex, expensive, and ineffective. Building security using a patchwork of single-purpose products from multiple vendors usually fails. It results in disjointed technologies that don't collaborate and create security gaps. It can also introduce a huge overhead of working with multiple systems and vendors. As a result, many attacks are not prevented, forcing organizations to invest more on post-infection and breach mitigation.

In order to achieve comprehensive security, companies should adopt a unified multi-layer approach that protects all IT elements – networks, endpoint, cloud, and mobile. Sharing the same prevention architecture, threat intelligence, and management can more effectively protect your organization.

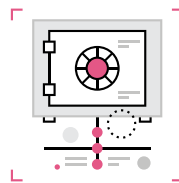


ONE OF THE MOST EFFECTIVE
PROACTIVE SECURITY
SOLUTIONS AVAILABLE TODAY
IS THREAT INTELLIGENCE.

KEEP YOUR THREAT INTELLIGENCE UP TO DATE

To prevent zero-day attacks, organizations first need incisive, real-time threat intelligence that provides up-to-minute information on the newest attack vectors and hacking techniques. Threat intelligence must cover all attack surfaces including cloud, mobile, network, endpoint, and IoT, because these vectors are commonplace in an enterprise. Attack vectors continually evolve to exploit vulnerabilities on these platforms.

In the constant fight against malware, threat intelligence and rapid response are vital capabilities. To maintain business operations, you need comprehensive intelligence proactively stop threats, management of security services to monitor your network, and incident response to quickly respond to and resolve attacks. Malware is constantly evolving, making threat intelligence an essential tool for almost every company to consider. When an organization has financial, personal, intellectual, or national assets, a more comprehensive approach to security can protect you against today's sophisticated attacks. And one of the most effective proactive security solutions available today is threat intelligence.



34% OF CYBER-ATTACKS
ARE PERPETRATED BY
INSIDERS, MAKING IT CLEAR
THAT LEGACY SECURITY
INFRASTRUCTURES,
CHARACTERIZED WITH
FLAT NETWORKS, ARE
DANGEROUSLY INEFFECTIVE.

CHAPTER 9



ZERO TRUST NETWORKS: BEST PRACTICES

TO “DIVIDE AND RULE” YOUR NETWORK

Zero Trust security is no longer just a concept. It has become an essential security strategy that helps organizations protect their valuable data in a “perimeter-everywhere” world. Implementing Zero Trust Networks, the key principle of the Zero Trust security model, is crucial in preventing malicious lateral movement within the network.

Today, 34% of cyber-attacks are perpetrated by insiders¹¹⁵ making it clear that legacy security infrastructures, characterized with flat networks, are dangerously ineffective. Using stolen credentials and compromised devices, hackers have managed to gain privileged access, move laterally within enterprise networks, and steal valuable data for months, without being detected. As evidence of this, 1.76 billion records were leaked in January 2019 alone.¹¹⁶

¹¹⁵ “Zero Trust Networks to the Rescue,” by Dana Katz, Check Point Blog

¹¹⁶ “Zero Trust Networks: Best Practices to ‘Divide and Rule’ Your Network,” by Dana Katz, Check Point Blog, 2019

Zero Trust Networks is about having the ability to “Divide and Rule” your network in order to reduce the risk of lateral movement. The key idea is to create a network segmentation by placing multiple inspection points within the network to block malicious or unauthorized lateral movement; so in the event of a breach, the threat is easily contained and isolated.

The best practice is to create a very granular segmentation by defining “least privileged” access control strategy; where user/system can gain access only to the resources that they are meant to use. For example, an access to source code should be granted only to R&D team members. This way only the absolute minimum, legitimate traffic between segments is allowed, while everything else is automatically denied.

BEST PRACTICES FOR ZERO TRUST NETWORKS

- **Identify** the data and assets that are valuable to the organization, e.g. the customer database, source code, smart building management systems, etc.
- **Classify** the level of sensitivity of each asset – such as ‘highly restricted,’ e.g. the customer database, ‘restricted,’ e.g. the HR portal, which is open to all employees, including the level of sensitivity of public assets, such as the corporate website.
- **Map** data flows among all entities across your network, including:
 - 1. North-bound traffic**, such as sales teams accessing Salesforce.com via managed devices on the corporate network only.
 - 2. East-West traffic**, such as from a frontend web portal to backend servers.

3. South-bound traffic, such as from the website backend server to Google Analytics via the internet.

- **Group** assets with similar functionalities and sensitivity levels into the same micro-segment. For example, all R&D internal assets, such as source code and ticket management system.
- **Deploy** a segmentation gateway, whether virtual or physical, to achieve control over each segment.
- **Define** a “least privilege” access policy to each of these assets, for example, allowing each R&D group to access only their own team’s source code.

Tip: Find the right balance between the granularity of the segmentation and the number of perimeters or micro-segments that can effectively and efficiently be managed.

MAINTAIN SECURITY HYGIENE PATCHING

All too often, attacks penetrate by leveraging known vulnerabilities for which a patch exists but has not been applied. Organizations should strive to make sure up-to-date security patches are maintained across all systems and software.

SEGMENTATION

Networks should be segmented, applying strong firewall and IPS safeguards between the network segments in order to contain infections from propagating across the entire network.

REVIEW

Security products’ policies must be carefully reviewed, and incident logs and alerts should be continuously monitored.

AUDIT

Routine audits and penetration testing should be conducted across all systems.

PRINCIPLE OF LEAST PRIVILEGE

User and software privileges should be kept to a minimum – is there really a need for all users to have local admin rights on their PCs?

COVER ALL ATTACK VECTORS

Mail or message

Send a mail or text message with a malicious attachment or a malicious link.

Web browsing

Compromise the user's browser (typically through exploit kits) or trick a user to download and open a malicious file.

Server and systems exploitation

Infect by exploiting unpatched vulnerabilities in any online host.

Mobile apps

One of the most common sources for compromising mobile devices is through mobile apps.

External storage

Physically mounted drives allow malicious files to enter without even traversing the network.

PHISHING

A fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy person. To achieve effective coverage, organizations should seek a single solution that can cover all attack surfaces and vectors. One solution that provides broad prevention across all attack surfaces, including mail, web browsing, systems exploitation, external storage, mobile apps and more.

YOUR CYBER SECURITY BATTLE IS WON

Or lost, depending on how well you can prevent unknown, zero-day threats. Organizations need to adopt a proactive battle plan to stay ahead of cyber-criminals and prevent attacks, not merely detect and remediate them. Relying on remediation can have devastating consequences to any organization, as once the malware was able to penetrate an IT surrounding – in many occasions this means infection that will spread in seconds and will be merely impossible to get rid of. Organizations today should assume that they will eventually be compromised at some point. Even if an organization is equipped with the most comprehensive, state-of-the-art security products, the risk of being breached cannot be completely eliminated. Detecting and automatically blocking the attack at an early stage can prevent damage.

To win the cyber security battle, companies need strong threat intelligence, threat prevention technology, and a consolidated security architecture that protects all attack vectors.

APPENDIX MALWARE FAMILY DESCRIPTIONS

AgentTesla	AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input, system clipboard, and can record screenshots and exfiltrate credentials belonging to a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). AgentTesla is openly sold as a legitimate RAT with customers paying between \$15 - \$69 for user licenses.
AndroidBauts	AndroidBauts is an Adware targeting Android users that exfiltrates IMEI, IMSI, GPS Location and other device information and allows the installation of third party apps and shortcuts on mobile devices.
Anubis	Anubis is a banking Trojan malware designed for Android mobile phones. Since its initial detection, it has gained additional functions including Remote Access Trojan (RAT) functionality, keylogger, audio recording capabilities and various ransomware features. It has been detected on hundreds of different applications on the Google Store.
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, allows anyone to host an Azorult C&C server with moderately low effort.
Bitpaymer	Bitpaymer is a ransomware that was involved in high profile targeted attacks. Usually delivered as the final stage after a successful intrusion and reconnaissance by the Dridex gang. Targets mostly mid-large businesses, demands high ransoms, and even after paying, it had a low data recovery success rate due to errors in the decryption tool.

BottleEK	Named after the playful image presented to potential victims, the Bottle Exploit Kit is specifically targeted at Japan. Using extensive browser and environment enumeration, BottleEK makes sure the target is Japanese before proceeding with an actual exploit attempt. Using CVE-2018-8174 and CVE-2018-15982, it delivers custom malware, also specifically targeted at Japan.
Capesand EK	Capesand EK - Capesand exploit kit was first reported in October 2019. It exploits vulnerabilities in Adobe Flash and Microsoft Internet Explorer but is currently under development and new exploits are expected to be added gradually.
Cerberus	Cerberus - Remote Access Trojan with specific banking screen overlay functions for Android devices, first seen in the wild in June 2019. Cerberus is operated in a Malware as a Service model, filling the void created following the discontinuation of banking Trojans like Anubis and Exobot. Cerberus has features like SMS control, key-logging, audio recording, location tracking and more.
Coinhive	Crypto Miner designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JS uses great computational resources of the end users machines to mine coins, thus impacting its performance.
Cryptoloot	A JavaScript cryptominer, designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JS uses great computational resources of the end users machines to mine coins, thus impacting its performance.
Danabot	Danabot is a banking Trojan written in Delphi that targets the Windows platform. While originally targeting Australian users via spam, the targeting has shifted to additional targets globally. Besides displaying fake banking websites, it also capable of stealing browser passwords and cryptocurrency wallets, as well as execution of additional malware like ransomware.

DarkGate	Darkgate is a multifunction malware active since December 2017 combining ransomware, credential stealing, RAT and cryptomining abilities. Targeting mostly windows OS, DarkGate employs a variety of evasion techniques.
Dridex	Dridex is a Trojan that targets the Windows platform. This malware is reportedly downloaded by an attachment found in spam emails. This malware identifies itself with a remote server by sending out information about the infected system. Furthermore, it can download and execute arbitrary modules received from the remote server.
Emotet	Emotet is an advanced, self-propagate and modular Trojan. Emotet once used to employ as a banking Trojan, and recently is used as a distributor to other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, it can also be spread through phishing spam emails containing malicious attachments or links.
Eris Ransomware	Eris ransomware was first spotted in May 2019, being delivered by the Rig exploit kit. It appends the .ERIS suffix to encrypted files on the system, and victims are instructed to contact the ransomware's operators via email with their unique Victim ID in order to receive payment instructions.
Fallout EK	Fallout Exploit Kit was first reported in February 2019 delivering GandCrab ransomware and AZORult infostealer. Uncommon with exploit kits, Fallout has been using PowerShell to run its payloads.
FormBook	FormBook is an Infostealer targeting Windows OS, first detected in 2016. It is marketed in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.

GandCrab	GandCrab is a RaaS malware (Ransomware as a Service). First discovered in January 2018 it operated an “affiliates” program, with those joining paying 30%-40% of the ransom revenue to GandCrab and in return get full-featured web panel and technical support. Estimations are that it affected over 1.5 million windows users before retiring and halting its activities in mid-2019. Decryption tools exist to all GandCrab versions.
Glupteba	Glupteba is a backdoor known since 2011 which gradually matured into a botnet. By 2019 it included a C&C address update mechanism through public bitcoin lists, an integral browser stealer capability and a router exploiter.
Guerrilla	Guerrilla is an Android Trojan found embedded in multiple legitimate apps and is capable of downloading additional malicious payloads. Guerrilla generates fraudulent ad revenue for the app developers.
Gustuff	Gustuff is an Android banking Trojan introduced in 2019, and capable of targeting customers of over 100 leading international banks, users of cryptocurrency services, and popular ecommerce websites and market-places. In addition, Gustuff can also phish credentials for various other Android payment and messaging apps, such as PayPal, Western Union, eBay, Walmart, Skype and others. Gustuff employs various evasion techniques including using the Android Accessibility Service mechanism to bypass security measures used by banks to protect against older generation of mobile Trojans.
Hawkeye	Hawkeye is an infostealer malware, designed primarily to steal users’ credentials from infected Windows platforms and deliver them to a C&C server. In the past years, Hawkeye has gained the ability to take screenshots, spread via USB and more in addition to its original functions of email and web browser password stealing and keylogging. Hawkeye is often sold as a MaaS (Malware as a Service).

Hiddad	Android malware which repackages legitimate apps, and then release them to a third-party store. Its main function is displaying ads, however it is also able to gain access to key security details built into the OS.
IcedID	IcedID is a banking Trojan which first emerged in September 2017, and usually uses other well-known banking Trojans to empower its spread potential, including Emotet, Ursnif and Trickbot. IcedID steals user financial data via both redirection attacks (installs local proxy to redirect users to fake-clone sites) and web injection attacks (injects browser process to present fake content overlaid on top of the original page).
Hummer	Hummer, also known as Hummingbad, is an Android adware generating revenue through advertisement display and application downloading on to infected mobile platforms. First identified in early 2016 it reached its peak by the end of the year. The threat group behind the malware is the Yingmob Chinese advertising analytics company.
JSecoin	Web-based Crypto miner designed to perform online mining of Monero cryptocurrency when a user visits a web page without the user's approval. The implanted JavaScript uses great computational resources of the end users' machines to mine coins, thus impacting the performance of the system.
KingMiner	KingMiner is a Monero cryptomining malware which targets Windows servers to exploit their resources. It was first reported in June 2018 and employs a verity of evasion techniques to bypass emulators and detection methods.

LockerGoga	<p>LockerGoga ransomware was first seen in the wild towards the end of January 2018, while targeting heavy industry companies. It appears that the threat actors behind the attack invest time and efforts in choosing the victims and are working to launch the attack in perfect timing and against critical assets. The attack usually involves encryption of Active Directory server and endpoints, in order to leave no alternative other than paying the ransom. Using a combination of AES-256 and RSA makes the encryption very solid, however, a poor code design, makes the encryption process very slow.</p>
Lokibot	<p>LokiBot is an infostealer with versions for both Windows and Android OS. It harvests credentials from a variety of applications, web browsers, email clients, IT administration tools such as PuTTY and more. LokiBot has been sold on hacking forums and believed to have had its source code leaked thus allowing for a range of variants to appear. It has been first identified in February 2016. Since late 2017 some Android versions of LokiBot include ransomware functionality in addition to their infostealing capabilities.</p>
Lord EK	<p>LordEK is an Exploit Kit that was first discovered in August 2019. Only utilizing one vulnerability, CVE-2018-15982, it's not the most advanced Exploit Kit on the market, but it still manages to take a bite of the bigger players' market</p>
MageCart	<p>Magecart is a type of attack in which malicious JavaScript code is injected into e-commerce websites and third-party suppliers of such systems in order to steal payment details.</p>

Mirai	<p>Mirai is a famous Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. The botnet is used by its operators to conduct massive Distribute Denial of Service (DDoS). Mirai botnet first surfaced on September 2016 as quickly made headlines due to some large-scale attacks among which are 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 backbone.</p>
MobiDash	<p>MobiDash is a stealthy Android Adware. Displays pop-up advertisements, and is very hard find and uninstall from the device. Surfaced around 2015, and continues to spread to date.</p> <p>Usually waits three days before starting to show ads, and can be avoided by not allowing apps from unknown sources.</p>
NanoCore	<p>NanoCore RAT, is a modular Remote Access Trojan targeting Windows users, with features like keystrokes collection, password stealing and even cryptocurrency mining. It is being sold on underground forums and observed in large scale malspam campaigns.</p>
Necro	<p>Necro is an Android Trojan Dropper. It was found inside the CamScanner app from Google Play and was installed more than 100 million times. Capable of downloading other malware, showing intrusive ads and stealing money by charging paid subscriptions. It is assumed that the Necro Dropper was added by advertisers and not by the actual app developers, and was cleaned from Google Play and from the following versions of CamScanner.</p>

njRAT	<p>One of the oldest Remote Access Trojans on the market, njRat has been used by many different threat actors. From state-sponsored Chinese hacking groups to script-kiddies spying on their friends, the ease of access and ease of use of this tool means we'll most likely be seeing it for years to come.</p> <p>Among its abilities you will find keylogging, remote code execution, password stealing, and even spying via the infected machine's webcam and microphone.</p>
NRSMiner	<p>NSRMiner is a cryptominer that surfaced around November 2018, and was mainly spreading in Asia, specifically Vietnam, China, Japan and Ecuador.</p> <p>After the initial infection, it uses the famous EternalBlue SMB exploit to propagate to other vulnerable computers in internal networks and eventually starts mining the Monero (XMR) Cryptocurrency.</p>
Phorpiex	<p>The Phorpiex (aka Trik) botnet has been active for almost a decade and is currently comprised of more than 500,000 infected hosts. Known for distributing other malware families via spam campaigns as well as fueling large scale Sextortion campaigns.</p>
PurpleFox	<p>PurpleFox started its way as a file-less rootkit, being spread to thousands of victims by Rig Exploit Kit. However, it seems the malware authors were not keen on paying the middleman to infect new hosts. PurpleFox has evolved and is now being spread using its own drive-by download platform.</p>
Radio EK	<p>Radio Exploit Kit is very simplistic. Using the tried-and-proven Proof-of-Concept code for CVE-2016-0189, it is mostly observed in Japan, delivering AZORult.</p>
Ramnit	<p>Ramnit is a banking Trojan which incorporates lateral movement capabilities. Ramnit steals web session information, giving the worm operators the ability to steal account credentials for all services used by the victim, including bank accounts, corporate and social networks accounts.</p>

RigEK	The most veteran of currently operating exploit kits, RigEK has been around since mid-2014. Its services being offered on hacking forums and the TOR Network. Some “entrepreneurs” are even re-selling low-volume infections for those malware developers not yet big enough to afford the full-fledged service. Currently using CVE-2018-8174, but has gone through many changes over the years to deliver anything from AZORult and Dridex to little-known ransomwares and cryptominers.
RubyMiner	RubyMiner is a Cryptocurrency miner that targets Linux and Windows servers. It was found exploiting old Ruby on Rails and PHP vulnerabilities in unpatched websites to mine Monero (XMR), using the legitimate XMRig crypto mining tool.
Ryuk	A ransomware used in targeted and well-planned attacks against several organizations worldwide. The ransomware’s technical capabilities are relatively low, and include a basic dropper and a straight-forward encryption scheme. Nevertheless, the ransomware was able to cause a severe damage the attacked organizations, and led them to pay extremely high ransom payments of up to 320,000 USD in Bitcoin. Unlike the common ransomware, systematically distributed via massive spam campaigns and exploit kits, Ryuk is used exclusively for tailored attacks. Its encryption scheme is intentionally built for small-scale operations, such that only crucial assets and resources are infected in each targeted network with its infection and distribution carried out manually by the attackers. Indeed, the malware encrypts files store on PCs, storage servers and data centers.
Sodinokibi	Sodinokibi is a ransomware-as-a-service which operate an “affiliates” program and first spotted in the wild in 2019. Sodinokibi encrypts data in the user’s directory and delete shadow copy backups in order to make data recovery more difficult. Moreover, Sodinokibi affiliates use various tactics to spread it - through spam and server exploits, as well as hacking into managed service providers (MSP) back ends, and through malvertising campaigns redirect to the RIG exploit kit.

Spelevo EK	The Spelevo Exploit Kit started its operations in March 2019. Initially leveraging CVE-2018-15982, it has evolved into using social engineering as an additional vector of infection. Spelevo is being used to spread malware such as IcedID, Dridex, and Ursnif. Also of note is Spelevo's use of domain shadowing as an additional layer of misdirection.
Trickbot	Trickbot is a Dyre variant that emerged in October 2016. Since its first appearance, it has been targeting banks mostly in Australia and the U.K, and lately it has started appearing also in India, Singapore and Malaysia.
Ursnif	Ursnif is banking Trojan that targets the Windows platform. It is usually spread through exploit kits - Angler and Rig, each at its time. It has the capability to steal information related to Verifone Point-of-Sale (POS) payment software. It contacts a remote server to upload collected information and receive instructions. Moreover, it downloads files on the infected system and executes them.
Wannamine	WannaMine is a sophisticated Monero crypto-mining worm that spreads exploiting the EternalBlue exploit. WannaMine implements a spreading mechanism and persistence techniques by leveraging Windows Management Instrumentation (WMI) permanent event subscriptions.
xHelper	xHelper is an Android malware, which mainly shows intrusive popup ads and notification spam. Very hard to remove once installed due to its reinstallation capabilities. First observed in March 2019, xHelper has now Infected more than 45,000 devices. The attackers used web-redirects to pages hosting android apps containing xHelper, and explanations on how to install unofficial Android apps.
XMRig	XMRig is open-source CPU mining software used for the mining process of the Monero cryptocurrency, and first seen in-the-wild on May 2017.
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.

CONTACT US

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

CHECK POINT RESEARCH PODCAST

Tune in to cp<radio> to get CPR's latest research,
plus behind the scenes and other exclusive content.
Visit us at <https://research.checkpoint.com/category/cpradio/>

WWW.CHECKPOINT.COM

©2020 Check Point Software Technologies Ltd. All rights reserved 2020.

