2018 SECURITY REPORT

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT RESEARCH

Check Point SOFTWARE TECHNOLOGIES LTD

CONTENTS

INTRODUCTION

2017 was a pivotal year that surprised many in the IT security industry. From the resurgence of destructive ransomware, IoT botnets, data breaches and mobile malware to sophisticated multi-vector technologies, it is clear we are witnessing an inflection point and a transition to the fifth generation of cyber attacks.

As the cyber landscape evolves, the World Economic Forum recently placed cyber attacks as one of the top three global risks for 2018. Indeed, we are now seeing threat actors effectively weaponizing ransomware as a way to cripple large institutions, affecting the health and lives of nation-states' populations, as well as causing pain to many businesses' bottom lines.

Data breaches took center stage in the past year, with some shocking revelations about major customer data compromises. Furthermore, the size and frequency of such attacks, from Uber to Equifax, shows no sign of slowing.

Security gaps in mobile features such as Bluetooth, as well as mobile app stores, have also meant that many malware variants continue to roam freely. In fact, millions of mobile devices worldwide have been infected by malicious apps generating high revenues for those who manage to infiltrate such app stores.

In addition, the increasing popularity and meteoric rise in value of crypto-currencies took the world by storm and led to a significant increase in the distribution of cryptominers, which quickly became a favorite monetizing attack vector.

And finally, the leak of alleged CIA cyber tools by hacktivist groups was seen to cast a long shadow over the global information security ecosystem as a whole. From alleged election hacking to critical infrastructure sabotage, more evidence came to light of nation-state-backed technologies being behind some of the largest global cyber attacks.

In this report, we will take a look back over the past year and try to make sense of it. In turn we will realize how the threat landscape, by entering the fifth generation of cyber security, now spans across countries and industries along multiple vectors of network, cloud and mobile and uses state-sponsored technologies to do so. By reviewing recent attacks we can understand, however, how 97% of organizations are not prepared for the fifth generation of cyber attacks. We will then be able to take a closer look at what 2018 may have in store and, most importantly, how best to prepare for it.

2017 TIMELINE OF MAJOR CYBER ATTACKS

Jan

PRINCETON UNIVERSITY

Princeton University is among 27,000 victims to have their data wiped by the MongoDB vulnerability.

Feb

PlayStation

2.5 million Xbox and PlayStation user profiles, including names, emails and personal IDs, are leaked.

Mar

Verifone

Verifone, the giant in credit and debit card payments, has its point-of-sales solution attacked.

Apr

NEW YORK POST

The New York Post mobile app is hacked and sends out a flurry of fake news alerts.

May

Emmanuel Macron, a presidential candidate, has 9GB of sensitive documents leaked in an attempt to sabotage France's presidential elections.

Jun

MAERSK

Following WannaCry in May, Petya causes mass disruption worldwide to FedEx, Maersk, WPP and many others.

Jul

CopyCat, a mobile malware, infects over 14 million Android devices worldwide and earns the attackers $1.5 million in fake ad revenues in just two months.

Aug

УКРПОШТА
ГОЛОВНА ПОШТА КРАЇНИ

The Ukraine's national Post Office is targeted in a DDoS attack to disrupt national operations.

Sep

EQUIFAX

Equifax, a large credit agency, has 143 million customers' data stolen including social security numbers, credit card details and more.

Oct

TRAFIKVERKET

A spate of DDoS attacks brings down Sweden's Transport administration services causing huge disruption.

Nov

UBER

57 million Uber driver and customer details are stolen in an AWS account hijack. Uber pays $100,000 to cover up the breach.

Dec

bitcoin

Crypto-currencies mining platform NiceHash is compromised and loses 4,700 bitcoin ($70 million) to hackers.

MAJOR CYBER **INCIDENTS OF 2017**

SHOCKING DATA BREACHES

EQUIFAX DATA BREACH

In September, Equifax, one of the top three credit agencies in the US, suffered a breach that affected over 145 million customers. By exploiting a security flaw in the software package, "Apache Struts," hackers were able to steal highly sensitive data including names, addresses, dates of birth, credit card numbers, Social Security numbers and driver license numbers.

DELOITTE DATA BREACH

Deloitte, one of the world's largest accountancy firms, was the victim of a cyber attack that went unnoticed for months and affected six of their clients. It is strongly believed that the hackers breached an administrator account of Deloitte's email system, which was stored in the Azure cloud.

UBER DATA BREACH

Due to hackers gaining login credentials to access data stored on Uber's AWS account, the personal information of 57 million customers and drivers were stolen. To make matters worse, Uber chose to cover up the breach by paying the attackers $100,000 to delete the confidential documents rather than report it.

UNC HEALTH CARE

Over 1,300 pre-natal patients of the University of North Carolina Health Care System were affected by a serious data breach. Breached information included full names, addresses, races, ethnicities, Social Security numbers and a variety of health-related information.

The rise of cloud computing has been due to its promise of greater agility, ease of integration and lower costs.

The main security challenges of cloud services, however, lie in them being externally exposed. This means they can be accessed from any location and from any device. What's more, they come with inefficient default security built in.

We work hard to encourage our customers to not rely solely on their service provider but rather to join them in the Mutual Responsibility model to protect both their data and any means used to assess it.

Yoav Daniely, Head of Product Management, Cloud Security

78%

OF COMPANIES CONSIDER IAAS AND SAAS CLOUD SECURITY TO BE THEIR MAIN CONCERN [1]

64%

OF ORGANIZATIONS HAVE EXPERIENCED A PHISHING ATTACK IN THE PAST YEAR [2]

STATE-LEVEL MALWARE

"VAULT 7" LEAK

In April, the WikiLeaks hacktivist group leaked a suite of hacking tools believed to belong to the Central Intelligence Agency (CIA). The leak illustrated to what extent nation-state level technologies are thought to be used in the fifth generation of cyber attacks. The extraordinary collection of hacking tools gave its possessor the entire hacking capacity of the CIA. Its malware arsenal and dozens of zero-day weaponized exploits were thought to be targeted against a wide range of US and European company products, including Apple's iPhone, Google's Android, Samsung TVs and Microsoft Windows.

US CRITICAL INFRASTRUCTURE

The US government warned that 'Dragonfly,' an allegedly state-backed advanced persistent threat (APT) group, has been using a combination of tactics and techniques to try and gain access to vital industrial control systems (ICS) at US energy companies and other critical infrastructure organizations via the networks of their suppliers and trusted third parties.

ATTACK RATES IN EMEA

Check Point Research revealed how ransomware attacks in EMEA have doubled from 28% in 2016 to 48% in 2017 due to highly sophisticated malware now being unleashed by low-level hackers. Almost 20% of organizations were impacted by the Fireball malware, infecting over 250 million computers worldwide. In addition, threat actors were able to create havoc caused by WannaCry through the use of high-end attack tools and techniques developed by state-sponsored developers.

Hacktivists and cyber criminals alike are now using state-level malware with devastating effect.

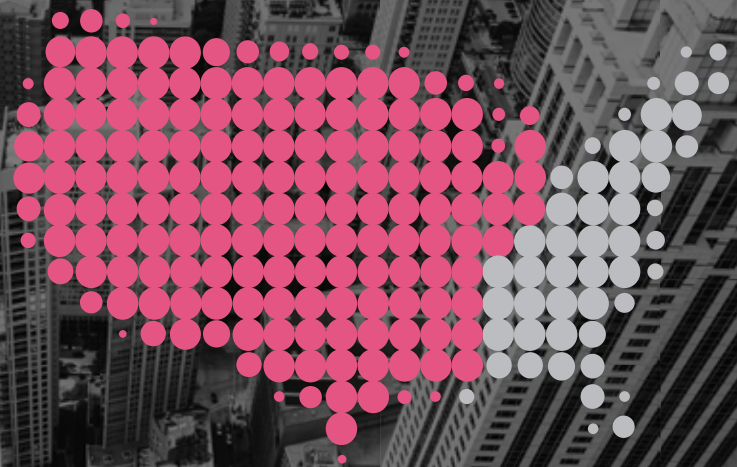
In many cases the common element is exploiting the human element within a public sector organization.

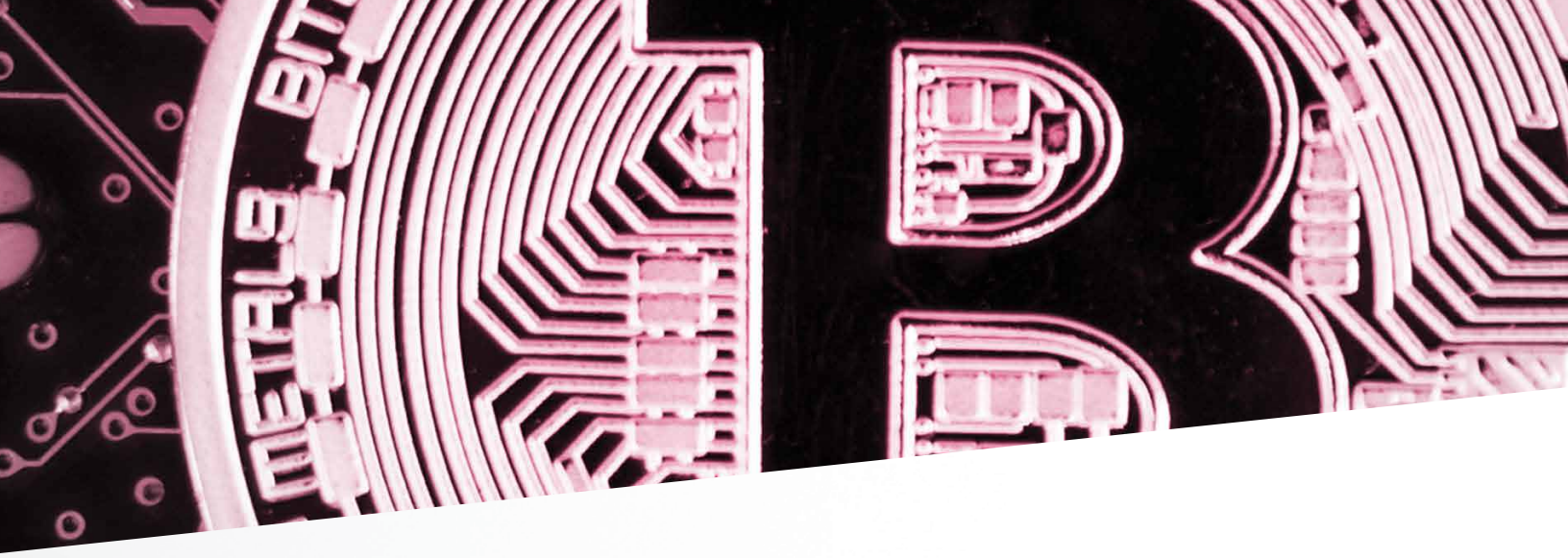
With so much at stake as far as geopolitics is concerned, not to mention people's lives, it is an area of cyber security that needs to be taken very seriously by all government agencies worldwide.

Richard Clayton, Head of APT Research

39 OUT OF 50 STATES

WERE ALLEGEDLY HACKED IN THE LAST US PRESIDENTIAL ELECTION [3]





CRAFTY CRYPTO-CURRENCY HEISTS

YOUBIT HACKED

With the theft of $120 million worth of Bitcoin from Youbit, a relatively unknown South Korean crypto-currency exchange, cyber criminals were seen tapping in to the crypto-currency craze in a big way. Rather than doing the hard work of mining the valued digital asset itself, cyber criminals instead often choose to steal it from others who have done so. Due to the meteoric rise in crypto-currency prices last year, billions of dollars have already been stolen from individuals and exchanges alike.

CONFIDO SCAM

A startup on the Ethereum platform, Confido, scammed thousands and then vanished from the internet after raising $374,000 from investors in an Initial Coin Offering (ICO) fundraiser. While many crypto-currencies are still trying to find a useful application in the real world, Ethereum has become a darling among financial types because ICOs allow startups to raise huge investments in lightning fast funding rounds.

ETHEREUM HEIST

A hacker pulled off the second biggest heist in the history of digital currencies by exploiting a critical flaw in the Parity multi-signature wallet on the Ethereum network, draining three massive wallets of over $31,000,000 worth of Ethereum in a matter of minutes. The attacker could have stolen much more if it wasn't for the quick action of benevolent white-hat hackers who rapidly organized to block him.

Due to its anonymity, cyber criminals were amongst the earliest adopters of crypto-currencies. But with Bitcoin's market cap growing from $1 billion to $500 billion in just a year (as per the time of publication), it is hard for others not to have noticed the digital currency boom.

No longer do criminals need to attempt large bank heists. Instead, they have focused their efforts on devising new and creative ways in which to steal from unique digital wallets. This not only benefits them but also takes away resources from those who legitimately mine these increasingly valuable digital assets.

Steve Johnson, Head of Advanced Threat Prevention

59%

OF COMPANIES CONSIDER RANSOMWARE TO BE THEIR BIGGEST THREAT [4]

SCARY RANSOMWARE STRIKES

WANNACRY

Thousands of operations and patient appointments were cancelled at the UK's National Health Service (NHS), as well as mass disruption across thousands of companies and public utility organizations worldwide, including Telefónica and German State Railways, as a result of the infamous WannaCry ransomware attack. The attack sent organizations back to pen and paper methods as the ransomware locked down their computer systems and demanded payment in Bitcoin to decrypt their files and return access.

NOTPETYA

Costing Nurofen and Durex manufacturer Reckitt Benckiser over $100 million alone in disrupted production and deliveries, the NotPetya ransomware caused large-scale havoc around the world. Although it was primarily aimed at the Ukraine, it affected companies globally, from Danish logistics firm Maersk to the US delivery service FedEx and the UK's advertising firm, WPP. After taking grip of an infected computer, the malware demanded $300 worth of Bitcoin to be paid to the perpetrators.

BAD RABBIT

In October, another new large-scale ransomware attack was unleashed against critical infrastructure companies as well as organizations in the healthcare, finance, distribution and software industries. The attack mainly focused on the Ukraine where Kiev Metro, Odessa International Airport and the Ministries of Finance and Infrastructure were brought down. This time the perpetrators locked down their victims' computers and demanded $280 worth of Bitcoin to decrypt it.

Ransomware has played a role in cyber security since the late 1980s. Thirty years later however, we are seeing it placed on center stage.

Back in the 1980s, healthcare was the primary target. But ransomware is now relevant to every business and individual.

As long as it continues to be an extremely effective method for financial gain, and organizations remain uneducated about the necessity of maintaining their cyber security hygiene, we should not be surprised to see these evolving attacks continue in the years ahead.

Tal Eisner, Head of Product Marketing, Threat Prevention

19,494

HOSPITAL APPOINTMENTS WERE CANCELLED DUE TO THE WANNACRY RANSOMWARE ATTACK[5]

DAMAGING DDOS ATTACKS

KOREAN BANK EXTORTION

In exchange for not disrupting the online services of seven South Korean banks, a group calling itself "Armada Collective" demanded about $315,000 to be paid in Bitcoin by threat of a Distributed Denial of Service (DDoS) attack. South Korean financial institutions are accustomed to being targets of cyber attacks, having faced similar threats since 2011.

UK NATIONAL LOTTERY

Millions of customers were disappointed to not be able to buy their weekly lottery tickets as the UK National Lottery's website was knocked offline by a large-scale DDoS attack. To make matters worse, the organization had been warned earlier in the month of such an attack if a Bitcoin ransom was not paid.

SWEDEN ATTACKED

In October, a flurry of DDoS attacks against the ISPs that power the Sweden Transport Administration's (Trafikverket) transportation services were carried out, causing huge train delays and disrupting travel for many busy commuters. The attack took down the agency's email system, website, and traffic maps, resulting in train traffic and other services needing to be managed manually.

24%

OF COMPANIES HAVE EXPERIENCED A DDOS ATTACK IN THE PAST YEAR.

Over the past year, DDoS attacks have hit targets ranging from major media websites to critical infrastructure. As the perpetrators of these attacks are often shadowy figures, it makes understanding their exact reasons for launching them even harder. Primarily, though, the reasons range from competitor abuse to political hacktivism.

Our research shows that in recent years the attempted recruitment of IoT devices, from which many DDoS attacks are now launched, has become widespread. This is mainly due to these online devices being made with weak authentication and therefore vulnerable to intrusion and manipulation by threat actors.

Yariv Fishman, Head of Product Management, Security Vertical Solutions

INVASIVE MOBILE MALWARE

COPYCAT & EXPENSIVEWALL

CopyCat, the mobile malware that infected more than 14 million devices around the world, made millions of dollars by taking advantage of outdated devices with fake apps. It earned the hackers behind the campaign approximately $1.5 million in fake ad revenues in just two months. In addition, a new variant of Android Malware, dubbed ExpensiveWall, that registered mobile-device users for paid services without their permission was discovered in the Google Play Store. The malware had infiltrated the Google Play app store and infected at least 50 apps. The infected apps were downloaded between 1 million and 4.2 million times before Google removed them.

LAZARUS GROUP GOES MOBILE

A new cluster of malware samples which targets Samsung devices and Korean language speakers was discovered, including some found in Korean Bible apps. The Lazarus Group, allegedly backed by North Korea, is popularly believed to be behind the attack with the intention of specifically targeting the population of South Korea.

PRE-INSTALLED MOBILE MALWARE

Our Mobile Threat Research Team found that every organization had suffered a mobile malware attack in the past year, with 89% experiencing at least one man-in-the-middle attack over a Wi-Fi network. In addition, 36 Android devices within just two companies of our survey sample contained malware which was pre-installed somewhere in the delivery chain. Some of the malware even had access to system privileges, meaning they could not be removed by the user and the device had to be re-flashed.

As noted in our Mobile Impact Report, every large company in the past year has experienced a mobile malware attack.

Our findings have also shown that even the most highly trusted app stores have weaknesses that are exploited on a regular basis and constantly offer malicious apps.

The fifth generation of the cyber landscape gives criminals a wider attack surface and thus more opportunities to take advantage of it. In addition, new vulnerabilities, whether through Bluetooth or Wi-Fi, mean both organizations and consumers alike need to be aware of the risks mobile devices pose.

Jeremy Kaye, Head of Mobile Security

OVER **300**

APPS IN THE GOOGLE PLAY STORE CONTAINED MALWARE AND WERE DOWNLOADED BY OVER 106 MILLION USERS[7]

100%

OF ALL BUSINESSES HAVE HAD A MOBILE MALWARE ATTACK[8]

BOTNET ARMY RECRUITMENT

HAJIME BOTNET

Like the infamous Mirai botnet, Hajime spread through unsecured devices that have open Telnet ports and use default passwords. Hajime has reached an astounding spread of over 300,000 devices, but its purpose remains unknown. While some speculate it is an operation to clean the IoT internet from the Mirai botnet, it could easily be abused for malicious purposes.

BLUEBORNE

A new attack vector, dubbed 'BlueBorne,' was discovered, operating via a combination of eight different vulnerabilities affecting Android, iOS, IoT devices, Windows, and Linux. The BlueBorne vulnerabilities are 'wormable,' meaning they can spread from one device to the next without further commands from the attacker, thus creating large botnets. This attack vector requires no action from the user, nor any preconditions or configurations aside from the Bluetooth being active.

IOTROOP BOTNET

A brand new Botnet, dubbed 'IoTroop,' evolved and recruited IoT devices at a far greater pace and with more potential damage than the Mirai botnet of 2016. IoTroop spread via security holes in IoT software and hardware, and indications show that over one million organizations were affected. The botnet has still yet to launch its attack, but when it does the results could be potentially devastating.

> IT TOOK **1 in 5** ORGANIZATIONS BETWEEN TWO WEEKS AND A YEAR TO FULLY RECOVER FROM THREATS[9]

LATEST TRENDS
ACROSS THE CYBER SECURITY LANDSCAPE

MALWARE MEETS CRYPTO-CURRENCIES

Malware developers are fast adapters and tend to follow rising trends to reach a widespread and effective operation. Due to such a dazzling rise in value in 2017, the current trend that threat actors are following is crypto-currencies.

There have been several aims of cyber criminals in the crypto-currency arena. Some aim to mine crypto-currencies by stealing users' computing power through malware known as cryptominers. We have seen these to be delivered through web browsers that use ad-blockers, as well as Torrent download sites.

Another method cyber criminals use is to claim to share any mined crypto-currencies with the user. In fact, their real intention is to display illegitimate ads or conduct a different malicious activity.

Rather than spending time and effort mining crypto-currencies, the more sophisticated attacks go for a more 'traditional' bank robbery method and head straight for the money, stealing directly from the crypto-exchanges themselves. And of course, if the crypto-exchanges are too hard to break into, there is always the option of illegitimately obtaining the credentials of a user's crypto-currency wallet.

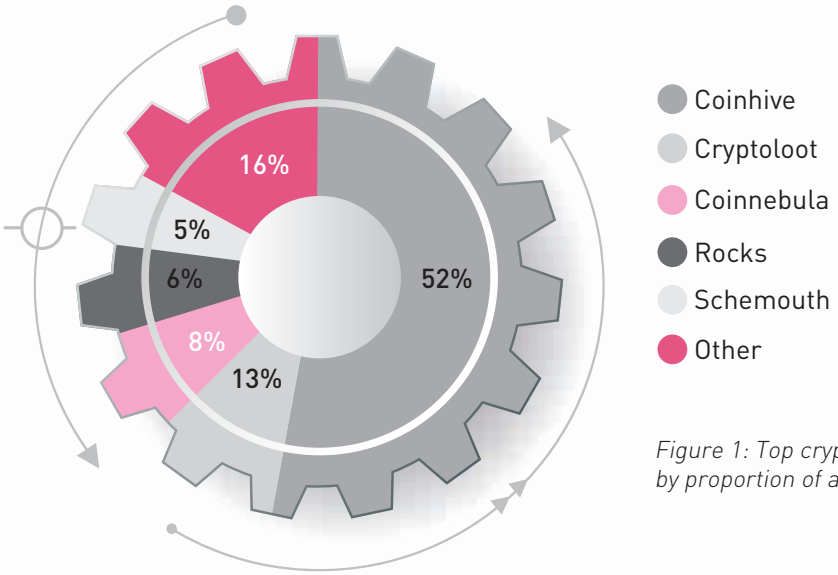


Figure 1: Top crypto-mining malware by proportion of attacks. [10]

MALWARE TARGETING MAC OS

Over the past year, we witnessed an increasing amount of attacks targeting Apple's MacOS. Indeed, what was once a rare occurrence has now turned into a real menace. Unfortunately, malware developers have managed to find new and creative ways to bypass Apple's protective fences and target Mac and iOS users with advanced malware.

However, the growing number of malware developed to target this reputable operating system has different purposes. The most notable is the OSX/Dok malware, which aims to intercept the user's passwords and any other sensitive information by controlling all of their network communications.

Ironically, the confidence that MacOS users show in the security of their operating system is often their downfall when they come under attack. Unlike other operating systems, only limited security solutions exist for MacOS, and even fewer users implement them. As a result, once an attacker has succeeded in bypassing the built-in protections, no additional obstacles remain.

Since the large amount of Mac users is a great incentive for hackers looking to broaden their attack surface, we are likely to continue seeing the same trend we have seen against Windows also affecting MacOS in coming years. In turn, this will require Mac users to upgrade their security and use dedicated technologies capable of preventing zero-day attacks.

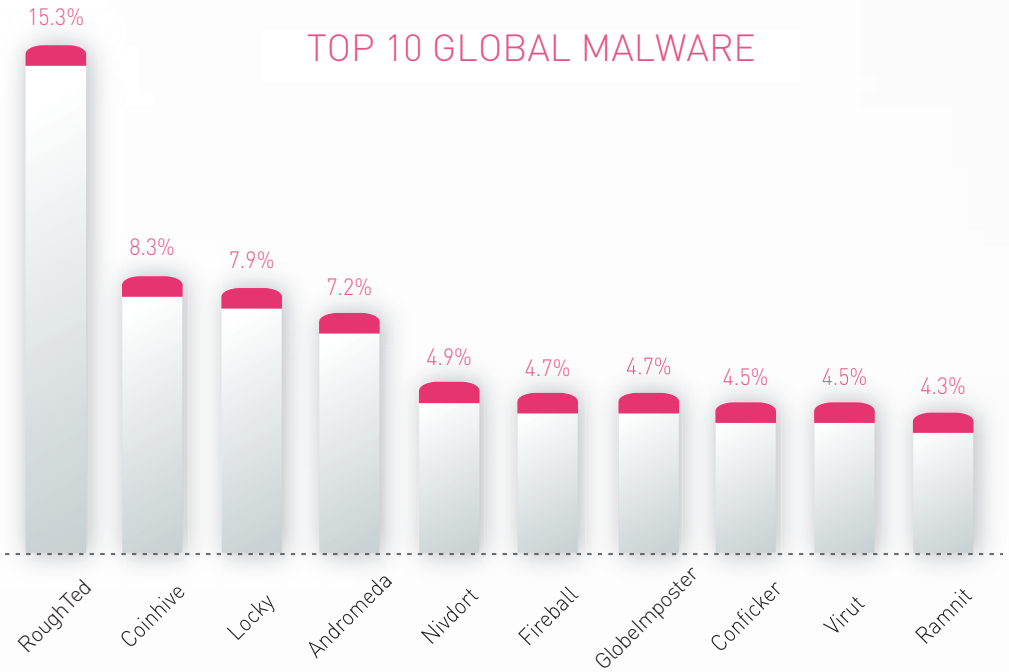


Figure 2: Most Prevalent Malware Globally: Percentage of corporate networks experiencing each malware type. [11]

MASS MALWARE: THE RISE OF INDUSTRIAL BOTNETS

Mirai, the infamous botnet of 2016 that caused havoc around the world, means 'Future' in Japanese. In 2017, as botnets spread in malicious numbers, reach and purpose, that 'future' had clearly arrived.

Furthermore, in both the PC and mobile worlds, botnets became more capable and vicious, launching bigger campaigns than ever before.

Most notably, the past year saw our discovery of the 'Judy' malware, an auto-clicking adware which, at up to 18.5 million downloads, may well be the largest ever mobile malware infection on Google Play.

The main trait common to botnets is that they all rely on gaining a critical mass to achieve their goal. Whether it be DDoS, cryptomining or mass advertising, the key is to infect as many devices as possible, making it almost impossible to eradicate the attack by regular means. Instead, more preventative measures through a higher level of malware detection and prevention are required.

MALWARE DEVELOPERS LEARN FROM THE BEST

With cyber security often being a 'cat and mouse' game, the next generation of malware creators are beginning to use the most advanced tactics of the day to bypass security measures and stay ahead of the chase. They are increasingly doing this by learning from the 'cat' (security agencies) themselves.

The WannaCry ransomware attack of May 2017 that used the 'EternalBlue' vulnerability serves as a good example. In this case however, as in many others, success was achieved by taking advantage of late security patches or the lack of implementation of such patches. Originally discovered by the NSA, the attack exploited the vulnerability to penetrate networks and spread within them. Organizations that failed to update their security ended up paying a heavy price.

A similar discovery was made via the Vault 7 leak, which revealed that some of the code used by the CIA to hack into mobile devices had been borrowed from ordinary malware. The key takeaway for enterprises and users is that all cyber threats relate to each other, no matter where they originate, and should be taken into consideration when protecting computer networks.

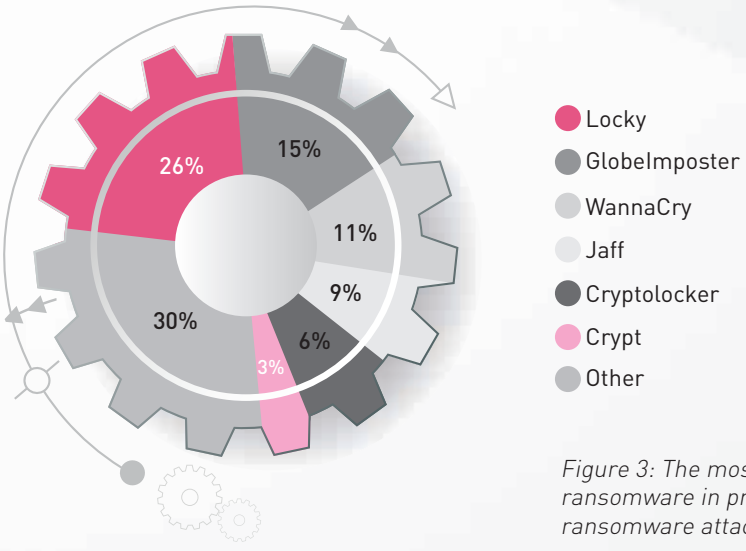


Figure 3: The most prevalent global ransomware in proportion to all ransomware attacks globally. [12]

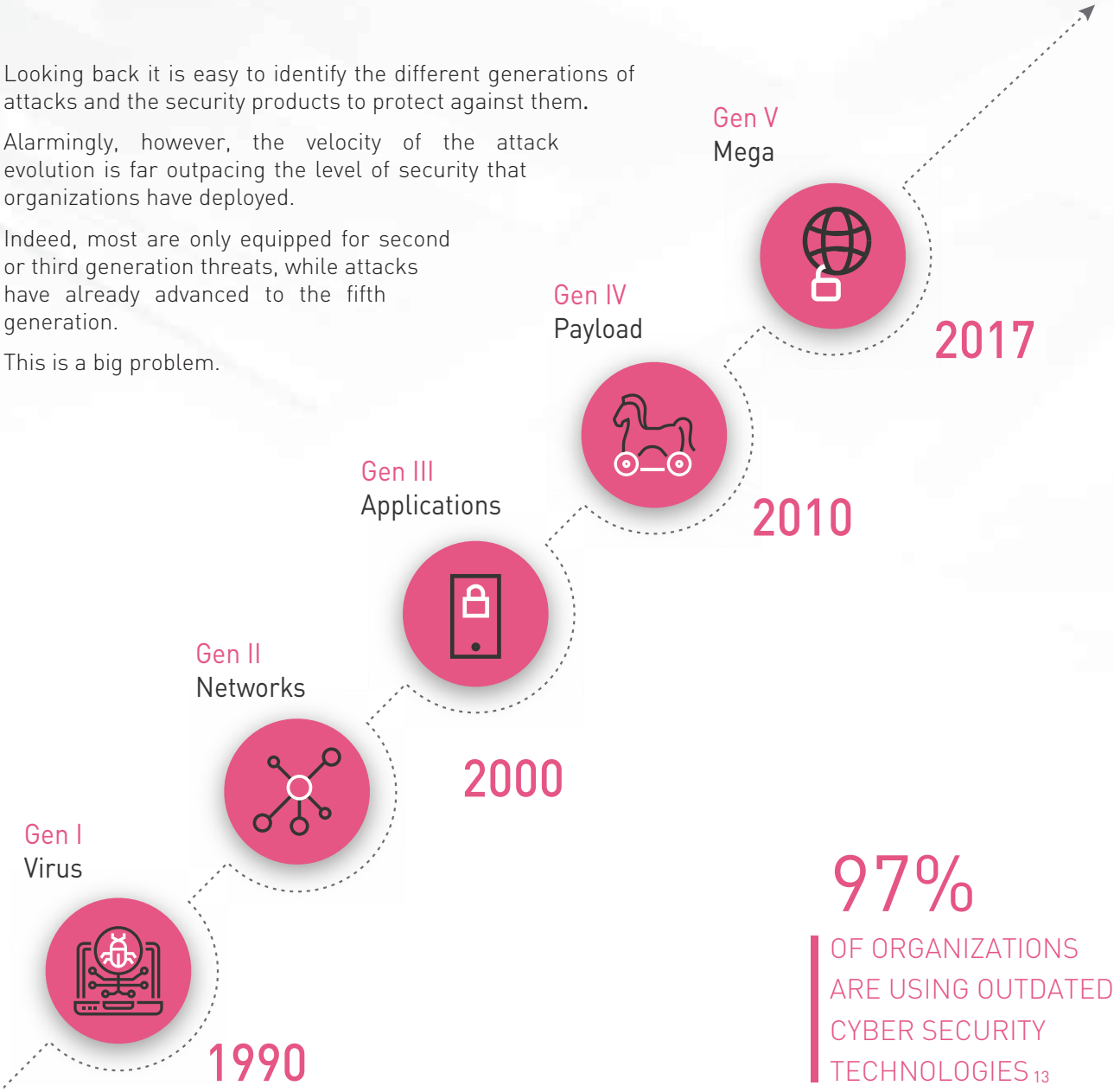
THE FIFTH GENERATION OF MEGA CYBER ATTACKS HAS ARRIVED.

Looking back it is easy to identify the different generations of attacks and the security products to protect against them.

Alarmingly, however, the velocity of the attack evolution is far outpacing the level of security that organizations have deployed.

Indeed, most are only equipped for second or third generation threats, while attacks have already advanced to the fifth generation.

This is a big problem.



97%

OF ORGANIZATIONS ARE USING OUTDATED CYBER SECURITY TECHNOLOGIES [13]

REPORT
BY INDUSTRY

FINANCE: MAKING THE WORLD GO ROUND

INTRODUCTION

The years of stock brokers and bank tellers shouting orders over the noise of ringing phones and typewriters are long gone. Today, the backbone of the financial world is computers and, with hundreds of billions of dollars on the line every day, attacks are inevitable.

The primary motive for finance sector cyber attacks is obvious, the money. However, money is not all that is at stake.

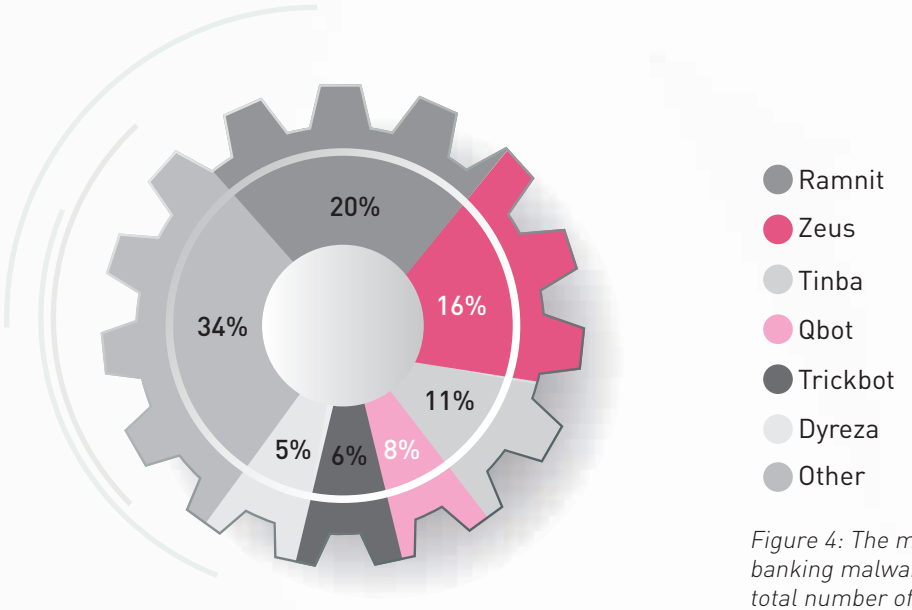


Figure 4: The most prevalent global banking malware in proportion to the total number of cyber attacks on banks. [14]

THE PROBLEM

The financial sector faces cyber threats from three main areas; the SWIFT network, consumer banking malware and information theft.

As the theft of $60 million from the Far Eastern International Bank in Taiwan proved not long ago, propriety banking systems are still vulnerable to attack. In this case, the custom built malware was inserted not only into PCs and web servers, but into a SWIFT terminal used by the bank. Once there, the thieves were able to obtain credentials needed for payment transfers and then doctor transfers made by the SWIFT network.

As a result of the many measures banks have now implemented to detect and prevent attacks on their customers' accounts though, the number of banking malware has declined.

This has, however, lead to malware developers turning their attention to easier targets and avoiding the strict defenses of banks. As thieves no longer need to break into a bank account itself in order to acquire the victim's money, this has resulted in a direct increase in ransomware attacks. In this way it is enough to simply hold a victim's computer for ransom and extort their money from them.

While in the PC world malware shifted from banking to ransomware though, mobile banking cyber criminals continue to flourish. Indeed, the rise in mobile banking has introduced new risks for convenience seeking users who perhaps are not aware of the threats to their mobile devices.

Another arena is that of the information that banks and credit agencies hold. This year we received an unfortunate reminder of this via the Equifax breach, which compromised sensitive information of almost half the citizens of the United States.

Finally, with the blockchain starting to look like being the future of finance, hackers have also been targeting the latest trend in the financial sector, crypto-currencies. Last December Bitfinex, the world's largest digital currency exchange was shut down after a massive Denial of Service attack. This was only the latest in a long list of attacks which have hit this market, with damages stretching far into the millions of dollars.

ADVICE & RECOMMENDATIONS

To stay protected against the exploitation of SWIFT networks, financial institutions must implement not only standard security measures, but also cutting-edge protections which will deter even the most sophisticated attacker.

The theft from the Taiwanese bank could have been avoided by using advanced forensic capabilities to provide full visibility by monitoring and recording all endpoint events, including files affected, processes launched, system registry changes and network activity. A solution should be in place that traces and reports the steps taken by malware and that blocks a perpetrator's attempt to hide their tracks.

To keep ransomware delivery via malicious files at bay, financial organizations must have sophisticated measures in place to block known and unknown threats. A threat extraction and emulation system that also consolidates monitoring, logging, reporting, and event analysis to correlate data and give actionable attack information will also save valuable time for an IT security team.

Financial institutions should understand that protecting their customers' data in the cloud is a shared responsibility between themselves and their cloud service provider. As part of that responsibility, financial organizations should ensure they patch all known vulnerabilities immediately as well as have comprehensive cloud threat prevention solutions implemented that offer zero-day protection and agile and automated delivery management that is scalable to their needs.

Although users should have their own anti-malware solution implemented on their mobile devices, financial institutions would do well to embed advanced mobile cyber security solutions directly into the banking apps their customers use. In this way they can protect not only against malware threats, SMS Phishing (SMiShing) attempts and issues of authentication, but also against any vulnerabilities in the mobile operating system itself.

The good news is that as security monitoring and controls tighten, attackers are becoming more discouraged, as seen with the demise of PC bankers.

As new technologies like the Blockchain sprout, banks need to look closely at their security infrastructure and move into the next generation of cyber security technologies. In this way they can strive to leave no vault door unlocked and block all cyber criminals' attempts to help themselves to the bullion.

SHOPPING FOR **RETAIL**

INTRODUCTION

With thousands or even millions of credit cards and consumer identities housed deep within their networks, criminals have good reason to expend their efforts in targeting the retail vector.

Over the years, cyber criminals have devised more sophisticated ways of abusing Point-of-Sale (PoS) terminals and hacking networks of retailers to steal customers' identity and credit card details. Indeed, the breadth and severity of these attacks is only increasing.

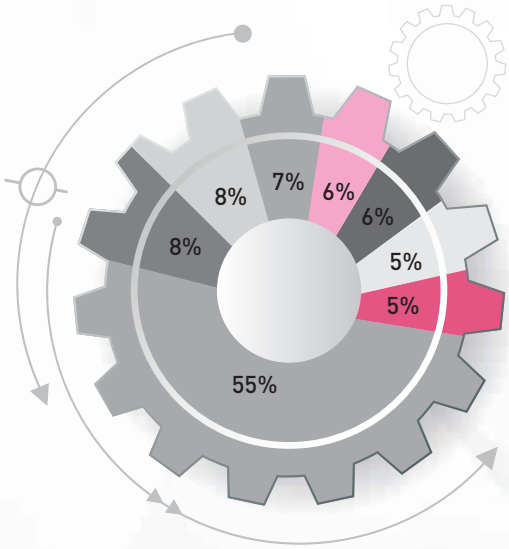


Figure 5: Top Global Mobile Malware. As more consumers shop from their mobile devices, mobile malware developers have greater incentives to achieve a wider spread. [15]

THE PROBLEM

With cyber-criminals aiming to steal personal and financial customer data, submitted via online shopping, digital marketing and loyalty schemes, it is easy to understand why over a third of retailers have already been the victim of a cyber attack.

Stolen data sold on the black market can now reach up to $20 per record, so it is not surprising that credit card information, along with personal contact details, dates of birth and information on purchasing habits is the most common target for cyber theft.

An example of this was the GameStop data breach early last year. After stealing thousands of customers' name, address and credit card details, including CVV2 numbers, the hackers went on to sell them on the dark web.

In addition, Forever 21 joined other retailers, such as Chipotle, Kmart, Brooks Brothers, Target and T.J.Maxx, by experiencing a point-of-sale attack. In this case, hackers gained access to customers' payment information by disabling the tokenization and encryption measures the retailer had installed just two years earlier.

As our research into the AliExpress shopping website illustrated, another method used to gain access to retailers' customer information is via phishing attacks. In this case it was phishing combined with an XSS attack, used to make the victim feel even more convinced nothing suspicious was occurring. Indeed, throughout the past year, large retailers such as Amazon, Best Buy, Walmart and Nike were all used to bait customers into falling for online shopping scams.

The harm done to a business's reputation, as well as the financial costs, can be huge. Some estimates put the average cost to a company at $172 per stolen record. This includes remediation costs, cost of lost business due to downtime, regulatory fines and legal costs. In addition, our surveys found that up to 20% of shoppers would not return to shop at a retailer that fell victim to a cyber attack. This is a hefty price to pay for what is essentially preventable.

20%

OF SHOPPERS SAY THEY WOULD NOT RETURN TO A RETAILER THAT WAS A VICTIM OF A CYBER ATTACK [16]

1 in 3

RETAILERS HAVE ALREADY BEEN HIT BY A CYBER ATTACK [17]

ADVICE & RECOMMENDATIONS

May 2018 sees the introduction of the EU's General Data Protection Regulations (GDPR), which will have far reaching ramifications on retailers, among others, worldwide. To avoid the consequences of a breach, companies must adopt a security mindset with dynamic architectures that updates with real-time protections.

First, PCI DSS should be implemented into business-as-usual activities as part of an overall security strategy. This can occur by actively monitoring the security controls, ensuring effective and proper operation. In addition, audit security policies need to work in real time as well as guarantee the correct configuration and operation of security controls such as Firewall, Antivirus, IPS (Intrusion Prevention Systems) and DLP (Data Loss Prevention).

Retailers that use PoS devices must also provide end-to-end encryption for all credit card transactions in order to protect customer data. It is also critical to see network defense as a range of multiple access points rather than a single perimeter.

A multi-layered approach that includes enforcement, control and management is also vital. We recommend creating a gateway and endpoint-based protection plan that identifies and blocks malware designed to infect machines, and collects and extracts customer information. Administrator determined security policies and automated protections also need to be established with rules that specifically define access control and data security policies with enforcement points.

Finally, in case of an attack, businesses need a response plan in place to ensure damage control of business integrity, their reputation and operations. This plan needs to be well rehearsed with all involved knowing their role and how it interacts with others on the response team.

THE SECURITY CURE **FOR HEALTHCARE**

INTRODUCTION

From a cyber security perspective, perhaps the most vulnerable industry is the healthcare industry, which not only treats vulnerable people but is itself extremely vulnerable.

As part of an industry that the public relies upon to literally save their lives, healthcare providers are easy targets for extortion. Having sensitive information leaked or operations shut down is not an option.

THE PROBLEM

The healthcare industry is often denied hardware updates due to manufacturer regulations, and in any case has a great need for maximum medical device uptime.

Sadly, this means it was one of the hardest hit by the WannaCry attack that took down a large part of the UK's National Health System (NHS) in May last year. In this case, computers essential for various functions, including MRI scanners, laboratory testing facilities and pharmacy needs were taken off-line leading to the cancellation of thousands of appointments and operations.

The healthcare industry is also targeted by hackers looking to steal large amounts of sensitive information, whether for identity theft, fraud schemes or selling them on the Dark Net. Such was the case with the Henry Ford Health System in Detroit last year, which saw more than 18,000 records of unique patient data stolen.

And finally, another threat vector that has become increasingly prominent over the past year is vulnerabilities in medical devices themselves.

Indeed, while the WannaCry ransomware attack affected over 200,000 Windows systems in the UK, it also infected Bayer Medrad radiology equipment both locally and in the US as well. The damage done via these devices can often go unseen but nevertheless medical device outages of these kind increase resource needs, delay care and trigger more clinical mistakes.

This is just as scary as it sounds. Allowing hackers to potentially endanger patients' health remotely by exploiting existing vulnerabilities is certainly a threat which must be addressed and remediated before such attacks are released in the wild.

ADVICE & RECOMMENDATIONS

To ensure patients receive the emergency services they need, organizations need a solution that will not just detect advanced threats to its network, but ultimately prevent them from entering at all. This means having a solution that includes Firewall IPS, app control, anti-bot, and anti-spam capabilities, as well as threat emulation and threat extraction technologies.

Healthcare providers should certainly ensure they have CPU-level exploit detection capabilities too. This will enable them to deliver a cleansed document while the file gets checked in the background, at no cost to the organization's smooth operations. In this way, they can block malware designed to bypass regular sandboxing technologies, and maintain their security against advanced threats such as WannaCry.

In addition, healthcare providers should try to minimize the complexity of their networks, and attempt to keep the distinct software versions used to a minimum, and monitored from a single user interface. This would make it easier to keep their systems up to date and monitor the threat landscape as well as implement security patches in a timely manner.

Finally, to protect IoT devices, thorough discovery and awareness of what is connected within the healthcare environment needs to be known. Only then can proper segmentation of these devices, and proper access policies, be carried out. This will enable prevention of potential attacks by deep-packet inspection and URL filtering, for example, to maintain the integrity of the data that these devices hold and the operations that they perform.

THE EVOLUTION OF **MANUFACTURING**

INTRODUCTION

Starting with the Industrial Revolution in 18th-Century Manchester, the manufacturing industry has typically undergone a revolution every hundred years. In an age of ever increasing technological advancement, though, times are changing at a faster pace, as we see the era of controller-based automation gradually replaced by the 'Smart Factory', otherwise known as Industry 4.0.

While it aims to streamline manufacturing output and enhance digital capabilities throughout supply chain processes, however, Industry 4.0 also brings with it new cyber risks and threats.

THE PROBLEM

In the belief that their factories are not a target for cyber criminals, many manufacturing businesses came to an abrupt awakening in May 2017. In this month, the WannaCry ransomware attack caused the shutdown of Renault-Nissan automobile plants in Europe and the Honda automobile plant in Japan and created mass disruption of enterprise production cycles globally. Over the summer of the same year, about half of the victims of the Petya ransomware attack were manufacturers.

It is not just manufacturing plants that are at risk from cyber attacks though. Every manufacturer has vital information that would be detrimental should it be lost or stolen, from research and development data to design plans, not to mention customer information. The risks to the manufacturing sector are wide-ranging and exponentially growing.

As global industry enters the next industrial revolution, developing a fully integrated strategic approach to those risks will be fundamental to manufacturing value chains as they combine operational technology (OT) and information technology (IT).

With more access points available to penetrate in the vast network that covers not only the industrial supply chain but also the connected devices used in the administration of the business and factory itself, organizations need to consider ways to secure those points to prevent unauthorized access.

82%

OF MANUFACTURERS HAVE EXPERIENCED A PHISHING ATTACK IN THE PAST YEAR [18]

ADVICE & RECOMMENDATIONS

Like any other industry, manufacturers should implement employee cyber security education programs, so that the workforce understands the most basic IT security practices.

Furthermore, risk assessments should be carried out across the manufacturing environment to identify the most valuable assets, where they are placed, who has access to them and how they can be protected. This should include a thorough review of the enterprise, the DSN, industrial control systems, and all connected devices. Good hygiene techniques such as segmentation between OT and IT can also not be stressed enough.

There is also a need to deploy specialized ICS/SCADA technologies. Deep packet inspection of the SCADA protocols such as MQTT/BACnet/Modbus communication between the machines and the management systems that control them, is needed in order to prevent manipulation of the manufacturing environment. Furthermore, solutions must include high visibility parameters including granular control of ICS/SCADA traffic, virtual patching through the use of ICS signatures and rugged appliances for harsh environments.

Through the use of both security appliances and cloud-based threat emulation services to protect against zero-day and unknown malware, manufacturers can secure their networks against ransomware at a more granular level too, including CPU-level inspection.

Moreover, manufacturers can prevent unauthorized access to corporate information through the use of program control, anti-phishing, anti-spyware, data security, and remote access, offering comprehensive protection through a unified security architecture.

Protecting Industry 4.0 is a complex and wide-ranging task, though there are many elementary and standard ways organizations can take action and protect themselves.

By combining this approach with robust access controls, mission-critical operation technology can be secured at application points and endpoints to protect both data and processes.

A MATTER OF **NATIONAL SECURITY**

INTRODUCTION

Due to its very nature, the government sector holds valuable information both on the national and the private level. With sensitive data concerning each and every citizen, as well as information on government policy, from energy to diplomacy, this makes it a popular target for hackers.

Through implementing new technologies and making more services available online, government agencies also face an ever increasing attack surface. These steps are unquestionably necessary, but entail certain risks which must be assessed and protected against.

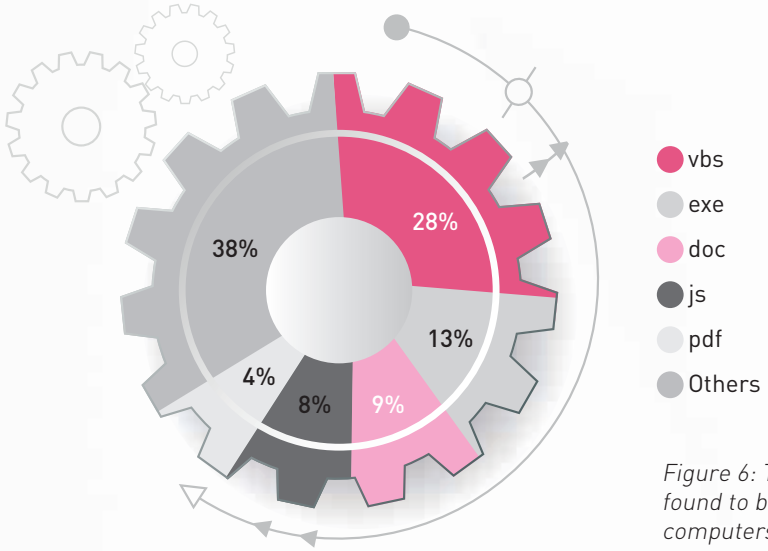


Figure 6: The top malicious file types found to be used to infect users' computers. [19]

THE PROBLEM

With state-sponsored technologies often being used in attacks against national agencies and institutions, the government sector is often targeted by the most advanced, sophisticated and adamant perpetrators, usually referred to as Advanced Persistent Threat (APT) groups.

Rather than searching for the easiest target, APT groups usually choose targets carefully and stick with them for as long as it takes to gain access. If necessary, they will develop tailor-made weapons to penetrate a specific gap in the network's security, against which it is extremely hard to defend.

One of the most common attack methods used against government institutions is 'phishing.' In June 2017, thieves hacked the Denver District Public School system's payroll to steal $40,000 from employees via a phishing scam. This kind of attack took advantage of arguably the most vulnerable part of any network's security, the human element. In cases like this, phishing emails appear to be sent from an address that the victim is accustomed to working with and trusts.

Account hijacks of cloud applications are also very common. This was seen in the breach of many UK politicians' email accounts earlier last year, which saw access gained to even the Prime Minister's account through a brute-force attack.

In addition, as demonstrated by the takedown of The Ukraine's national bank, power grid and airport in June 2017, government infrastructures were among global targets affected by the Petya ransomware attack. This attack sabotaged not just national infrastructure but also caused economic damage to nation-states through the forced downtime of manufacturing plants.

These threats cannot be treated lightly. The consequences can range from weakened negotiating positions and economic damage, all the way to the impairment of a state's national sovereignty. Simply put, they turn the new era of technology into a government official's nightmare.

ADVICE & RECOMMENDATIONS

To protect against the myriad of next generation phishing attacks, a new and multi-dimensional approach is required. These defenses need to protect email infrastructure, provide highly accurate anti-spam coverage and defend governments from a wide variety of virus and malware threats delivered within email.

For government agencies to be able to prevent account hijacks, such as those experienced by the UK Parliament, they need to implement security solutions that combine both network and on-device intelligence. This technology needs to have the ability to deeply inspect the network and endpoint security posture.

Current technologies often fail because not only are they not always sufficiently secure, but are also cumbersome to implement.

New technology is needed that is both transparent to the user and simple to use without the end user even being aware that it is running. In addition, it must make real deterministic time decisions that will prevent an imposter's access.

In the past, using a zero-day exploit meant game over, but not anymore. In recent years we have developed technologies capable of detecting and blocking zero-day exploits which we didn't even know existed. These are used to counter the efforts of APT groups capable of creating these exploits to target a single government agency with ransomware.

Attacks against a government's critical infrastructure, which was often built without any concern for cyber security and is thus riddled with vulnerabilities, are increasing.

However, today dedicated solutions for these systems do exist, tailored to allow a seamless operation of the infrastructure while keeping it safe against such threats.

32%

OF GOVERNMENT OFFICES WERE VICTIM TO A DATA BREACH IN THE PAST YEAR [20]

THE ROAD **AHEAD**

INTRODUCTION

As Abraham Lincoln once said, "You cannot escape the responsibility of tomorrow by evading it today." This can not be overstated enough in the world of cyber security.

In this section we will take a look at what may be the expected threats to our networks and data in the future, and in the next section we will see how organizations can prepare themselves for their responsibility to avoid them.

77% 

OF IT PROFESSIONALS FEEL THEIR SECURITY TEAMS ARE UNPREPARED FOR TODAY'S CYBER SECURITY CHALLENGES [21]

THE FUTURE IS CLOUD AND MOBILE

Mobile devices are part of the IT ecosystem and businesses around the world. However, in most organizations, these devices are not secured at anywhere near the level they should be in relation to the value of the assets they store. Flaws in mobile operating systems and technology will continue to be discovered, highlighting the need for organizations to deploy advanced protection against mobile malware and interception of communications.

Mobile malware will also continue to proliferate, especially mobile banking malware, as the Malware-as-a-Service (MaaS) trend, which lowers the demand for technical ability on the part of the threat actor and thus makes it easier to carry out attacks, continues to evolve and grow.

In addition, we can expect to see mobile cryptominers being used to harvest crypto-currencies for criminals in the near future. So far cryptominers have affected web servers and PCs but with mobile security being less developed this is likely to be the next attack channel.

MOVING TO THE CLOUD

Enterprises will continue to move their data to the cloud at a greater pace as companies look to make their operations ever more profitable in an economically challenging world.

Although cloud usage is now widespread among businesses due to the agility and cost reductions it offers, it is still relatively new technology and continues to evolve. This provides hackers more backdoors to access deeper into enterprise systems.

As a result, misconceptions about the levels of security needed, along with a lack of understanding regarding the responsibility for that security, are common. This leaves the door wide open to breaches.

During 2017 over 50% of security incidents handled by Check Point's incident response team were cloud-related, and more than 50% of those were account takeovers of SaaS apps or hosted servers. Data leaks will continue to be a major concern for organizations moving to the cloud, especially due to an increased use of cloud-based file sharing services.

The growing adoption of SaaS-based email such as Office 365 and Google's G Suite, as well as IaaS, makes it an attractive target for cyber criminals, and we expect that these will be increasingly targeted during 2018.

Furthermore, these potential threats will be compounded by the heavy penalties that regional regulations such as GDPR could inflict upon companies who do not comply with these new regulatory obligations.

50%

OF SECURITY INCIDENTS HANDLED BY CHECK POINT'S INCIDENT RESPONSE TEAM WERE CLOUD RELATED [22]

SECURING YOUR NETWORK

Ransomware has proven to be a highly effective money-maker for criminals, as well as a disguise for more destructive purposes. Because of its effectiveness against all types of users, from consumers to corporations, ransomware will continue to grow, and we can expect to see more large, orchestrated worldwide outbreaks along the lines of WannaCry, Petya and Bad Rabbit.

Furthermore, we can expect additional creative extortion tactics from criminals, such as 'refer-a-friend' concepts to encourage victims to spread the malware in return for lower ransom payments to have their computers unlocked.

As operating systems become more secure, we can expect to see a decline in the use of exploits to target vulnerabilities in them. In turn, this will bring an increase in the use of basic hacking techniques that rely on human error and social engineering to help propagate the spread of ransomware.

In addition, the ability of ransomware to raise funds for cyber-criminals has already initiated the Ransomware-as-a-Service and other cottage industries within the Dark Web. We can expect these to grow with the services offered targeting not only regular computer networks but mobile and IoT devices too.

75%

OF ORGANIZATIONS HAVE SECURITY STAFF & RESOURCE ISSUES [23]

INTRODUCING GDPR

The European Union's new General Data Protection Regulations (GDPR) will have far reaching consequences for many organizations worldwide. Core elements of the GDPR detail a number of 'Rights of EU Citizens' with respect to how their personal data is used. The list is extensive and will require significant changes to applications, policies and procedures to attain compliance. As a result, GDPR, with the timeframe and penalties it involves, will place a significant stress on any organization that handles EU citizen data.

However, as the regulation is new, there is no experience from previous audits that an organization can draw upon. In addition, many aspects of GDPR are still a work in progress. For example, GDPR establishes a European Data Protection Board (EDPB) to "take an active role in enforcing EU data protection law." However, at the time of printing, the formalization of the EDPB is still in progress and the specifics are yet to be determined.

Nevertheless, the limited lead time until the regulation goes into effect means organizations should already be allocating focus and resources for implementing their GDPR strategy. This includes their plans for staffing, data audit and classification, risk analysis, logging of activity and breach identification and fundamental controls.

IOT GETS SMARTER

The proliferation of IoT devices will continue and expand the potential attack surface. Hence we will see more variations of the Mirai and BlueBorne attacks on IoT and connected devices coming our way in 2018 and beyond.

As more smart devices are built into the fabric of enterprise networks, and wider networks too, organizations will need to start using better security practices for both the devices and the networks they connect to. This will be critical to preventing potential large-scale attacks and may even be enforced by international regulations.

Beyond the large-scale DDoS attacks we saw in 2017, home IoT devices will be exploited by cyber criminals to gain access not only to a victim's home network but also directly to snoop around their physical home too. This was highlighted by our report into LG's Smart Home Devices last year. As home users are generally not aware of the security element of their home IoT devices, they tend to leave the default settings in their original state. This leaves the door open for attackers to constantly have access to a user's home network.

Smart City IoT initiatives will continue their momentum, helping cities to provide better customer service while substantially reducing costs. At the same time fifth generation cyber security solutions will need to be seriously considered every step of the way in order to prevent potential attacks.

Due to how severely health organizations were hit by the WannaCry attack, the healthcare vertical will also start to put an emphasis on protecting internet connected medical devices within hospitals so as to prevent potential life threatening attacks.

DIGITAL CURRENCIES

With crypto-currencies increasingly being the payment method of choice for the criminals behind ransomware outbreaks and the funding of other illegal activities, will we perhaps see more stringent regulations starting to be applied to them?

The significant resources needed to create crypto-currencies have also driven the emergence of cryptominers. These are the new quasi-malware tools which are being used to generate revenue by hijacking the CPU power of unsuspecting computer users to generate currency, often without the user's knowledge or consent. We have already seen several examples of this and, with the value of crypto-currencies being so high, we can expect to see cyber criminals finding new ways of exploiting victims' computer power to mine these currencies for their own financial gain.

In addition, due to the high value of Bitcoin and other crypto-currencies, the systems surrounding them, such as crypto-currency exchanges, are also likely to be targeted by criminals looking to exploit vulnerabilities.

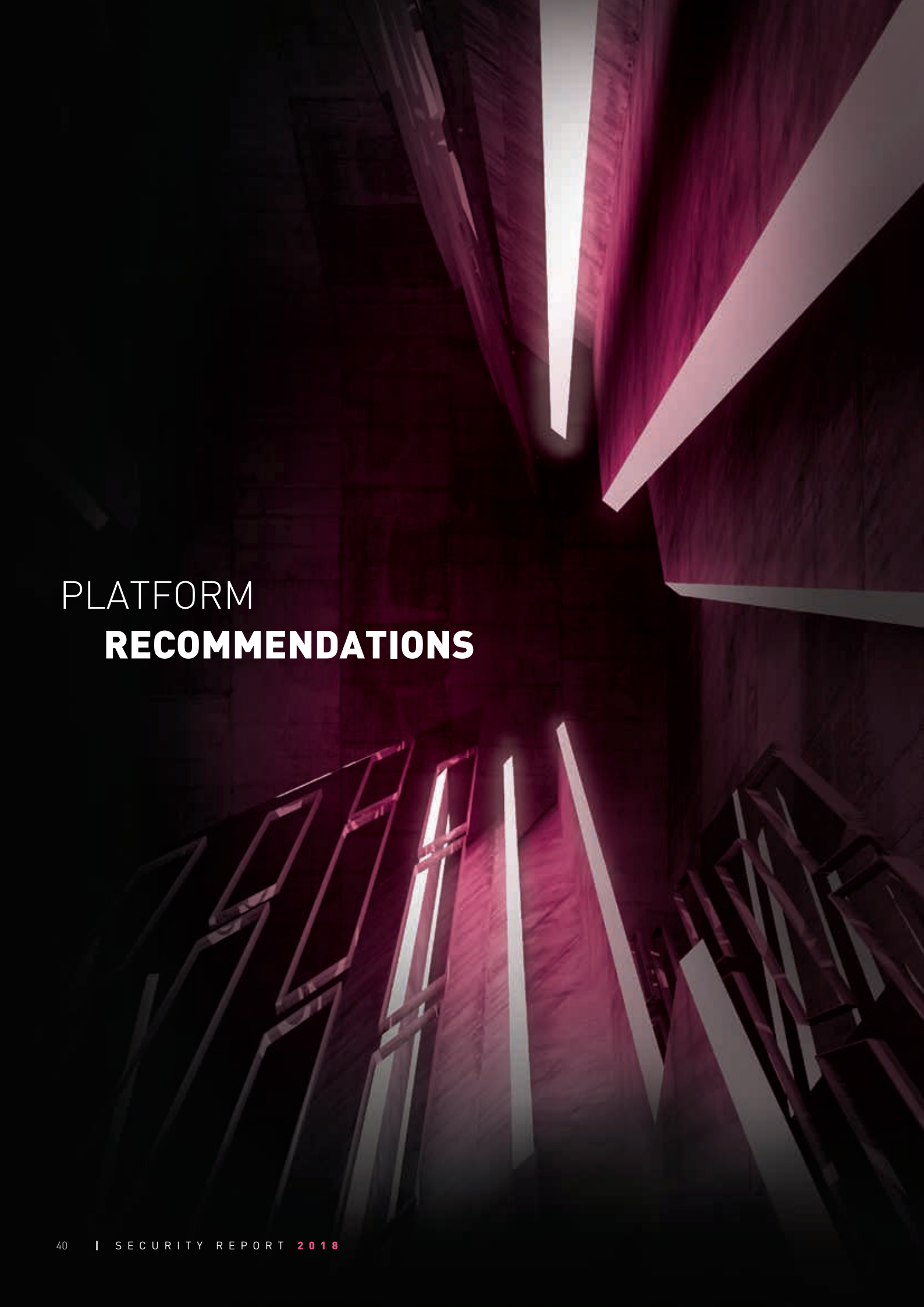
A combination of these factors could well cause international government and law enforcement agencies to take action over the abuse of crypto-currencies, which will in turn adversely affect the value of the currency itself.

DEFENDING THE NATION-STATE

In 2018 and beyond, cyber defense will gain traction and prominence among government agencies as they become more sensitive and attuned to the connected world in which they and their citizens live.

Furthermore, state-sponsored agencies will continue to develop cyber attack technologies for defense and offense, and financially driven criminal groups will continue to seek ways to monetize cyber attacks. In addition, hacktivists will continue to use cyber attacks to convey their messages and non-state terrorist groups may well also shift to cyber space as weapons that used to be confined to government defense departments are made more public.

As a result, we may well start to see governments deploying more protection over their own critical infrastructure such as power and water utilities, health services, local government administration offices and the IT infrastructure that supports them.



PLATFORM **RECOMMENDATIONS**

MOVING TO 5TH GENERATION IT SECURITY ARCHITECTURE

From converging applications and data onto IP-based networks to rolling out 'cloud native' applications, to BYOD policies and the use of IoT devices, the rapid digital transformation of business places ever-increasing demands on security.

Current security architectures to manage all this are outdated and are the most common cause for unavailability and security issues, lead to catastrophic failure.

By implementing 'Gen V' architecture, though, businesses can eliminate single points of failure by providing the necessary strength and resiliency to maintain operations and security under any circumstances.

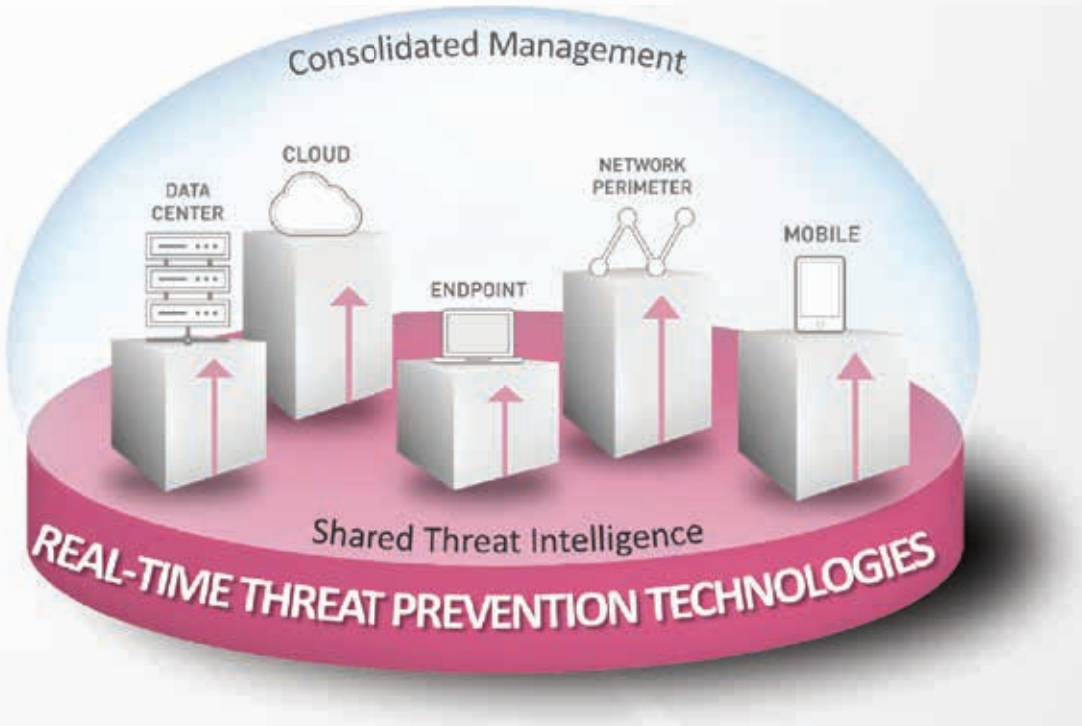
> THOSE USING PREVENTION TECHNOLOGIES ARE **30%** FASTER IN IDENTIFYING AND REMEDIATING THREATS [24]

'Gen V' security architecture builds a consolidated, unified security architecture that manages and integrates with mobile, cloud and networks to protect against and prevent fifth generation cyber attacks. Integrated threat prevention also needs to work with a dynamic security policy across all platforms that expresses business needs, supports cloud demands with auto scaling and is able to flexibly integrate with third-party APIs.

Furthermore, a unified and advanced multi-layered threat prevention environment must include CPU-Level sandbox prevention, threat extraction, anti-phishing and anti-ransomware solutions to defend against known and unknown 'zero-day' attacks.

In this way, having the right architecture upon which the entire security infrastructure operates is the only way to ensure a single, cohesive wall of protection to prevent fifth generation cyber attacks.

A CONSOLIDATED MANAGEMENT
USING BEST SECURITY TECHNOLOGIES



BUILDING YOUR CLOUD INFRASTRUCTURE

As organizations have evolved, business data is increasingly accessed through cloud platforms anytime and anywhere. This means that network traffic is travelling outside traditional IT security protections, and the risks associated with that present a huge challenge. What's more, malware introduced into the cloud can easily propagate among cloud applications, attack virtual segments or even ride unimpeded back to corporate networks.

To overcome these challenges, businesses need to achieve synergy between security best practices and cloud security technologies. These should primarily include advanced blocking and prevention techniques. In addition they should include strong and familiar management tools and techniques with comprehensive visibility, monitoring and reporting. This will enable them to quickly identify malicious network activity or known indicators of compromise (IOCs) and respond accordingly.

In order to secure cloud-based data centers, it is vital to keep the cloud's agility and velocity at an optimum so that the solution has seamless automation and orchestration with a wide array of cloud infrastructures such as AWS, Cisco ACI, Microsoft Azure, OpenStack, VMWare and others. Moreover, the solution must include advanced security controls designed for cloud infrastructure that builds upon network security with support for micro-segmentation. This can help decrease the attack surface and be an important first step in avoiding cyber attacks within the virtual network.

The protection of SaaS applications by blocking account takeovers, phishing attempts and the prevention of zero-day malware from propagating into corporate networks requires advanced solutions. In addition, these solutions should aim to identify legitimate user access by analyzing real-time data, across both PC and mobile devices.

Finally, to fully embrace the cloud, organizations need to have both the correct policies and technologies in place to ensure their protection. This means adopting the balanced 'Shared Responsibility' model between themselves and the cloud provider to protect both the cloud infrastructure and the data that resides there.

BEYOND THE CORPORATION

As organizations move closer, on both Mobile and SaaS platforms, to the 'BeyondCorp' model, access controls are shifted from the perimeter to individual devices and users. This provides for an unprecedented level of access being provided to critical business information. Granting employees access to that information on the mobile devices they choose has many benefits, but it also exposes your business to risks.

Zero-day malware, man-in-the-middle attacks over Wi-Fi, smishing attempts over SMS and exploits of OS vulnerabilities can all be used to steal sensitive information such as emails, texts, photos, calendar appointments and attachments.

As a result, organizations must ensure all their mobile devices are installed with the next generation of advanced

94%

OF COMPANIES EXPECT ATTACKS ON MOBILE DEVICES TO INCREASE [25]

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

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

Only solutions that include behavioral analysis to detect rogue hotspots and malicious network behavior will be able to automatically disable suspicious networks. On-device remediation technologies will also be able to dynamically trigger a secure VPN that protects the privacy and integrity of your communications.

Comprehensive mobile and SaaS security should be a system of components that work together cohesively. Only solutions that can analyze behavior across all vectors for indicators of attack can protect mobile devices effectively to keep them safe.

NO WEAKEST LINKS

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats requires a different approach than traditional firewalling to keep enterprise networks and data secure.

The fifth generation of network security needs to include a unified approach with security features such as Firewall, IPS, Anti-Bot, Antivirus, Application Control, and URL Filtering to combat known, and unknown, cyber attacks and threats.

Together with advanced threat emulation and extraction techniques at the higher OSI levels, 'Gen V' technologies go further and deeper into malware inspection at the CPU-level, as well as OS-level, to identify exploits. Innovative sandboxing techniques need to include the fast and accurate detection and blocking technologies, evasion resistance and deep inspections of the widest array of files, including non-executables.

By combining multiple threat extraction technologies tightly within a single appliance, the network sandbox solution should also be capable of running preventions at different points in time, based on signatures and dynamic analysis while working speedily to control network access, without hindering business operations.

CONCLUSION

In the past 25 years, attacks, as well as security protections, have advanced rapidly. Cyber attacks have progressively evolved using the newest innovations for committing cyber crimes. However most organizations have not evolved and are still using second or third generation cyber security. This creates a huge disadvantage as we have now entered the fifth generation of cyber attacks.

Fifth generation cyber attacks, such as the mega attacks of 2017, are defined as large-scale and fast-moving attacks. These sophisticated attacks easily bypass the conventional, static detection-based defenses being used by most organizations today.

To combat these latest attacks, companies must deploy fifth-generation cyber security that uses advanced real-time threat prevention that protects all networks, virtual, cloud, remote office and mobile operations of a business.

97%

OF ORGANIZATIONS ARE USING OUTDATED CYBER SECURITY TECHNOLOGIES [26]

Unfortunately, today's attacks are the most advanced and impactful we have ever seen and yet the security deployed by most businesses is generationally behind and incapable of protecting against these attacks. Our research shows that the vast amount of companies today are using only second or third generation protections, with only 3% actually using fifth generation tools and techniques.

In order to ensure better protection against the advanced attacks outlined in this report, organizations must step up to 'Gen V' security solutions to protect against the fifth generation of cyber attacks.

For more information on how to achieve fifth generation cyber security, please read our Gen V Report

REFERENCES

1. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
2. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
3. Source: Bloomberg, June '17, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections
4. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
5. Source: UK National Audit Office, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
6. Source: Check Point C-Level Perspective Survey, April '17, sample size: 59 C-Level Executives.
7. Source: Check Point Mobile Threat Research Publications, https://research.checkpoint.com/check-point-mobile-research-team-looks-back-2017/
8. Source: Check Point Mobile Threat Research Report, November '17, sample size: 850 organizations.
9. Source: The State of Security Efficiency Survey, February '18, sample size: 452 participants.
10. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
11. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
12. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
13. Source: Check Point Research Survey of IT Security Professionals, March '18, sample size: 443 participants.
14. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
15. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
16. Source: KPMG Consumer Loss Barometer Survey, August '17, https://home.kpmg.com/cn/en/home/insights/2016/08/consumer-loss-barometer.html
17. Source: KPMG Consumer Loss Barometer Survey, August 17, https://home.kpmg.com/cn/en/home/insights/2016/08/consumer-loss-barometer.html
18. Source: Check Point Meta-Analysis by Industry Survey, February '18, sample size: 450 participants.
19. Source: Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/h2-2017-global-threat-intelligence-trends-report/
20. Source: Check Point Meta-Analysis by Industry Survey, February '18, sample size: 450 participants.
21. Source: Check Point Survey of IT Security Professionals, December '17, sample size: 452 participants.
22. Source: Check Point Incident Response Team.
23. Source: Check Point Survey of IT Security Professionals, December '17, sample size: 452 participants.
24. Source: Check Point Survey of IT Security Professionals, December '17, sample size: 452 participants.
25. Source: Check Point Dimensional Research Survey into Mobile Device Security, sample size: 410 participants.
26. Source: Check Point Research Survey of IT Security Professionals, March '18, sample size: 443 participants.

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

WWW.CHECKPOINT.COM