2020

Threat Report

BlackBerry | CYLANCE

Contents

Introduction

The BlackBerry® Cylance® 2020 Threat Report contains a broad range of topics vital to the interests of businesses, governments, and end-users. It delivers the combined security insights of BlackBerry, a trailblazer in the Internet of things (IoT) and mobile security, and Cylance, an early pioneer of AI-driven cybersecurity and endpoint security market disruptor, which was purchased by BlackBerry in February 2019.

As always, this report represents our piece of the overall security puzzle. Our goal is to make security information, predictions, and lessons learned accessible to everyone, regardless of role or title. The 2020 Threat Report examines 2019's major security breaches and considers recent advancements that may prevent past mistakes from repeating. We provide a deep dive into current cybersecurity issues with an eye toward not merely chronicling what happened, but also analyzing the conditions that allowed for those events.

That said, this report is not intended to be merely a retrospective examination of the major threats of 2019. It is a high-level look at the security issues affecting the hyper-connected world of 2020, including elements of IoT, mobile devices, user identity, embedded systems, adversarial AI, and other contemporary issues.

We sincerely hope the information contained in this report will enable readers to be more proactive and well informed in their efforts to combat the onslaught of threats that will surely be unveiled in the new year — and over the course of the next decade.

Executive Summary

- Advanced persistent threat groups and other adversaries released updated malware and displayed innovative attack techniques throughout 2019. Their focus on improving encryption routines and concealing malicious payloads through steganography raised the bar for security researchers and threat detection solutions. Threat actors were also able to widely distribute attacks by compromising managed security service providers (MSSPs) and infiltrating their customers' environments.
- IoT is growing rapidly as vehicles, appliances, and other devices become increasingly capable of connecting to various networks. This connectivity growth creates a similar expansion of the attack surface, providing multiple opportunities and venues for threat actors to compromise systems. Keeping business technology secure as it interacts with IoT devices is difficult, but advancements in continuous user authentication may provide a solution.
- Modern vehicles have advanced to the point where they closely resemble edge computing devices. Unfortunately, vulnerabilities in the supply chain, design process, and updating procedures have made vehicles an easy target for attackers. Vehicle vulnerabilities may lead to disastrous outcomes if the industry and third-party vendors don't take steps to improve automobile cybersecurity.
- Deep fake technology is becoming more widely accessible. This has led to deep fake personas appearing on social media sites and fake voice authorizations being used to commit fraud. Organizations should consider training employees on identifying and responding to the indicators of deep fake technology use.
- Mobile security is facing several challenges ranging from vulnerable mobile device management (MDM) servers, to enterprise clients and their interaction with IoT devices. Automating various security controls, improving the obfuscation of mobile app code, and encouraging users not to root/jailbreak their phones helps mitigate mobile risks.

Deep fake technology is becoming more widely accessible. This has led to deep fake personas appearing on social media sites and fake voice authorizations being used to commit fraud.

APT Trends in 2019

An advanced persistent threat (APT) refers to a sophisticated threat actor that gains access and carries out sustained attacks against an enterprise network. APTs generally try to remain undetected for extended periods of time while carrying out surveillance, data exfiltration, lateral movement, and other malicious operations.

Originally, APT groups were most often state-sponsored, and their motivation was aligned with the corresponding state's ideology and interest. In recent times, the term is now also used to refer to highly skilled and sophisticated threat actors who may not be affiliated with any particular nation state, but whose motivation is primarily economic gain.

APTs may target specific individuals within a compromised organization. Social engineering, spear phishing, and even insider information obtained from disgruntled employees may be used against carefully targeted victims.

By reviewing threat intelligence on APT groups, companies can understand who is attacking their enterprise, the actor's modus-operandi, and motives. This information can prove useful for protecting vulnerable systems against advanced threats.

The analysis that follows provides summaries of some of the tools, techniques, and specific actors uncovered by our threat research conducted in 2019.

Social engineering, spear phishing, and even insider information obtained from disgruntled employees may be used against carefully targeted victims.

TECHNIQUE

Host-Dependent Encryption

In 2019, BlackBerry Cylance noted an increase in APT-related malware samples using host-dependent encryption to protect their payloads. In the past, this technique was used to protect the most sensitive, highly tailored backdoors, and usually implemented via Windows® Data Protection APIs.

Recently, these encryption mechanisms have become more diverse and widespread. Some threat actors have built host-dependent encryption into their generic loaders that are distributed with a range of various tools and malware.

For example, the OceanLotus group has started to wrap nearly all their implants in a multi-stage loader. The loader can be configured to derive the decryption key for the payload using username, computer name, IP address, or MAC address information. This technique prevents analysts and malware hunters from decrypting the payload without having a deep knowledge of the victim's environment.

In another example, an initial dropper copies itself and encrypts some of its malicious code using a one-time randomly generated key. It then deletes the original binary and re-runs the encrypted version specifying the generated key as parameter. Decrypting the code containing malicious functionality now requires researchers to know the command line parameter used to execute the second malware copy. Discovering what the randomly generated key was is a very difficult, if not impossible task.

TOOL

Ransomware as a Cyber Weapon

Another trend we are seeing is the use of ransomware in targeted attacks. This trend first gained widespread public attention with the outbreak of WannaCry (2017)[1]. After a brief period of decline, ransomware has come back with a vengeance. Traditionally, ransomware attacks were financially motivated cyber crimes directed at individual users and small or midsize businesses. More recently, however, we have observed a substantial increase in cases of big companies, public institutions, and governments being hit by ransomware.

In some of the most sophisticated scenarios, attackers will choose their victims carefully and do a thorough reconnaissance to find the best way in. Once they gain access to the victim's environment, the attackers first deploy information-stealing malware and exfiltrate sensitive data before encrypting all files.[2] In case the affected company refuses to pay for the decryption tool, the attackers will try to blackmail them with a threat of publishing the stolen information. This information often contains personal data of the company's customers and therefore would constitute a data privacy breach.

The threat actors behind targeted ransomware attacks tend to reuse known malware families. Many of these malware families are sold on underground forums or bought from ransomware-as-a-service (RaaS) vendors. The aim of most of these attacks is often simple extortion. However, some ransomware attacks may aim to disrupt processes and services by destroying vital data. In some cases, the payment infrastructure and/or the encryption routines are flawed, making file decryption or ransom payment impossible. In these cases, the attacks resemble simple wipers that pose as ransomware but ultimately only destroy data. Ransomware families used in the highly targeted attacks of 2019 include Sodinokibi, Ryuk, and Zeppelin.

TECHNIQUE

MSSPs Being Targeted To Deploy Ransomware

During mid-2019, a new ransomware called Sodinokibi/Sodin/REvil appeared in the wild. It targeted businesses and caused mass disruption in some U.S. government agencies. Similar to GandCrab, the technical details of Sodinokibi are fairly mundane, but its deployment methods are noteworthy.

In most cases, the initial compromise occurred via targeted phishing attacks aimed at managed service providers (MSPs) and MSSPs[3] managing IT and security within the target organization. The threat actors would leverage a foothold in the target organization by using remote management tools like Go2Assist or NinjaRMM.

Once inside, attackers deployed common tools like Passcape's password recovery tool to steal credentials. Threat actors also accessed servers hosting security software and disabled them. Next, the attackers connected to domain controllers and used existing software deployment tools to push ransomware to every machine in the environment.

MSPs and MSSPs are proving to be high-value targets for threat actors. Once attackers establish a foothold, they can easily pivot to the hundreds of other diverse and vulnerable targets in the environment. Making sure MSPs and MSSPs use effective cybersecurity tools will be critical for organizations in 2020.

TECHNIQUE

Living Off the Land

Threat actors continue to rely heavily on living-off-the-land (LotL) techniques that use trusted system resources for cyber attacks without triggering security alerts. Attack vectors vary, but include:

- Using reconnaissance and lateral movement tools like WMI and built-in scripting languages (PowerShell, VBScript, etc.)
- Using administrative and development tools for:
  - Evasion
  - Deploying fileless malware
  - Proxying execution

LotL attacks remain a perennial threat and a powerful technique adversaries leverage in the latter stages of the attack lifecycle.

THREAT ACTOR

Update on OceanLotus

During early 2019, the Vietnamese APT group known as OceanLotus (APT32/CobaltKitty) began a campaign aggressively targeting multi-national automotive manufacturers.[4] These attacks may have been intended to bolster the country's domestic automotive industry, though the attacker's motives remain unknown. OceanLotus infiltrated automotive companies by using spear phishing emails containing macro-enabled documents and sending them to public-facing departments like recruiters and customer service teams.

Once opened, the documents typically download and execute either CobaltStrike beacons or additional downloaders (KerrDown) responsible for deploying advanced backdoors. The attackers often used LotL techniques, relying on PowerShell and WMI for reconnaissance and RDP for lateral movement.

During these automotive attacks, BlackBerry Cylance researchers observed new backdoors being deployed by OceanLotus. These updated backdoors are capable of modular command-and-control (C&C) communications and are typically loaded into memory by highly bespoke, fileless loaders. The new OceanLotus backdoors employ advanced obfuscation, encryption, and steganography[5] techniques to remain hidden.

BlackBerry Cylance researchers also uncovered a suite of novel remote access trojans (RAT) employing advanced network attack capabilities. These RATs, called Ratsnif, were developed by OceanLotus. The malware, which appears to have been under active development since 2016, offers a veritable swiss-army knife of network attack techniques. They combine features such as packet sniffing, gateway/device ARP poisoning, DNS poisoning, HTTP injection, and MAC spoofing[6].

TOOL

Open Source and Commercial-Off-the-Shelf Tooling

The malicious use of open source and commercial-off-the-shelf tools is another trend that has continued to grow this year. Toolkits like Cobalt Strike, PowerSploit, and Empire have been used by threat actors for actions ranging from state-sponsored activity to financially-motivated attacks.[7]

These tools, originally created for penetration testing, are easily adapted for malicious use by threat actors. One of the advantages of using widely available tools is that it makes attack attribution more difficult and may allow attackers to avoid detection. Companies may dismiss or downplay alerts for these tools believing them to be related to past penetration testing.

TECHNIQUE

Steganography

Attackers continue to use steganography to conceal payloads and communications. Steganography involves concealing a file or message within another file, ideally without raising any suspicions. Attackers have hidden code and data within graphic file formats for years, an excellent example being the OceanLotus exploitation of PNG files[8].

In the second half of 2019, we discovered attackers concealing payloads within WAV audio files[9]. In general, the use of steganography helps adversaries evade detection because the key malicious content is only present in memory. Detecting and blocking steganography attacks requires effective memory monitoring and threat defenses.

THREAT ACTOR

APT-28 Activity

The APT-28 group continued to perform attacks aligned with Russian foreign and economic interests in 2019.[10] The World Anti-Doping Agency (WADA) was again the target of an attack suspected to be the work of APT-28. This would be the second time WADA was the victim of state-sponsored cyber attacks. These attacks come at a time when Russian attendance at the 2020 Tokyo Summer Olympics is under review.

Analysis performed by BlackBerry Cylance Threat Intelligence during 2019 provided insight into a previously unknown APT-28 backdoor. All indications from the analysis points towards a new and undocumented implant with a relatively immature set of features. The unique domain generation algorithm (DGA) implementation provided a strong indicator that the code is related to other published APT-28 tools[11]. The new backdoor uses multiple embedded static libraries: a trade-off between achieving low detectability and deploying larger executables.

Our analysis of this APT-28 backdoor[12] suggests the group is engaged in per-target tooling or efforts to rebuild feature sets into new tools.

TOOL

Ryuk

Ryuk is the most active ransomware we saw in 2019. In most engagements, it was deployed by the threat actor along with Trickbot and Emotet. Its primary infection vector is a phishing document containing a malicious Microsoft® Office macro that downloads the Emotet malware. Trickbot is then dropped and used to accomplish a few specific goals.

First, Trickbot can compromise banking credentials and has traditionally been known as a banking trojan. In some attacks, Trickbot is used to first compromise banking information before Ryuk is brought in for encryption operations. This attack technique provides a one-two punch for the threat actor.

Second, Trickbot is excellent at spreading malware. It first dumps passwords from memory, then uses Windows SMB default shares to laterally move and propagate.

Third, Trickbot is controlled by a C&C channel that also deploys Ryuk. The attacker usually spends a couple of weeks inside the environment mapping and conducting reconnaissance to find important servers and backups to encrypt. More sophisticated threat actors typically avoid encrypting workstations and only target the servers.

THREAT ACTOR

Fin9

The group commonly known as Fin9 targeted MSSPs in the United States and abroad in 2019. Their motivation appears to be financial since they primarily commit gift card fraud after obtaining access to a network. The group uses phishing emails to gain an initial foothold then compromises credentials and laterally moves through the environment using various methods.

Fin9 uses LotL techniques, leveraging the preferred remote access technology supported within the victim environment. This threat group has been seen using Keseya VSA, ScreenConnect, TeamViewer, and native RDP. Fin9 has also been observed using a modified version of the ScreenConnect client configured to connect with their own infrastructure.

Fin9 is known to target defensive infrastructure as well as uninstall or disable endpoint agents to evade detection. Once the group has identified clients of the MSSP, they spread into those networks by leveraging trusted access.

TECHNIQUE

Adversarial Machine Learning

Since the advent of the antivirus industry, malicious actors have sought to bypass and evade detection by content-scanning engines. Attackers increase the likelihood of a successful attack by ensuring their threats remain undetected. Over time, cybersecurity specialists have witnessed many novel (and not so novel) evasion techniques to bypass the eminent detection technology of the day. Some examples include:

- Polymorphism to evade signature scanning
- Anti-virtualization to bypass emulation and sandboxing
- Text manipulation to bypass spam filters
- Other mutation techniques based on obfuscation and encryption

As expected, we are now witnessing a rise in targeted attacks against machine learning and AI, the latest technology employed against cyber threats.

The idea of adversarial attacks being performed against machine learning models is not new. Researchers and adversaries both explore ways to manipulate data in order to subvert the machine learning decision making process.[13] Popular methods include evading detection from spam engines, fooling image recognition to overlook objects, and poisoning data sets used to train AI models.

Over the past year, several attacks have surfaced that aim to influence machine-learning classifiers and subvert a model's determination from malicious to benign. One example is stuffing attacks that mutate existing threats by including excessive amounts of benign features. Another is tampering attacks that alter file headers and modify code or data to mimic benign samples.

Thankfully, what might seem like a perennial problem for the industry is also a blessing in disguise for machine learning. The increase in attacks against machine-learning classifiers encourages security researchers to extend training sets and refine feature spaces used for training models. These steps should ultimately result in machine-learning classifiers with greater resilience to anomalies and stronger efficacy against future attacks.

2019 Overall Threat Trends

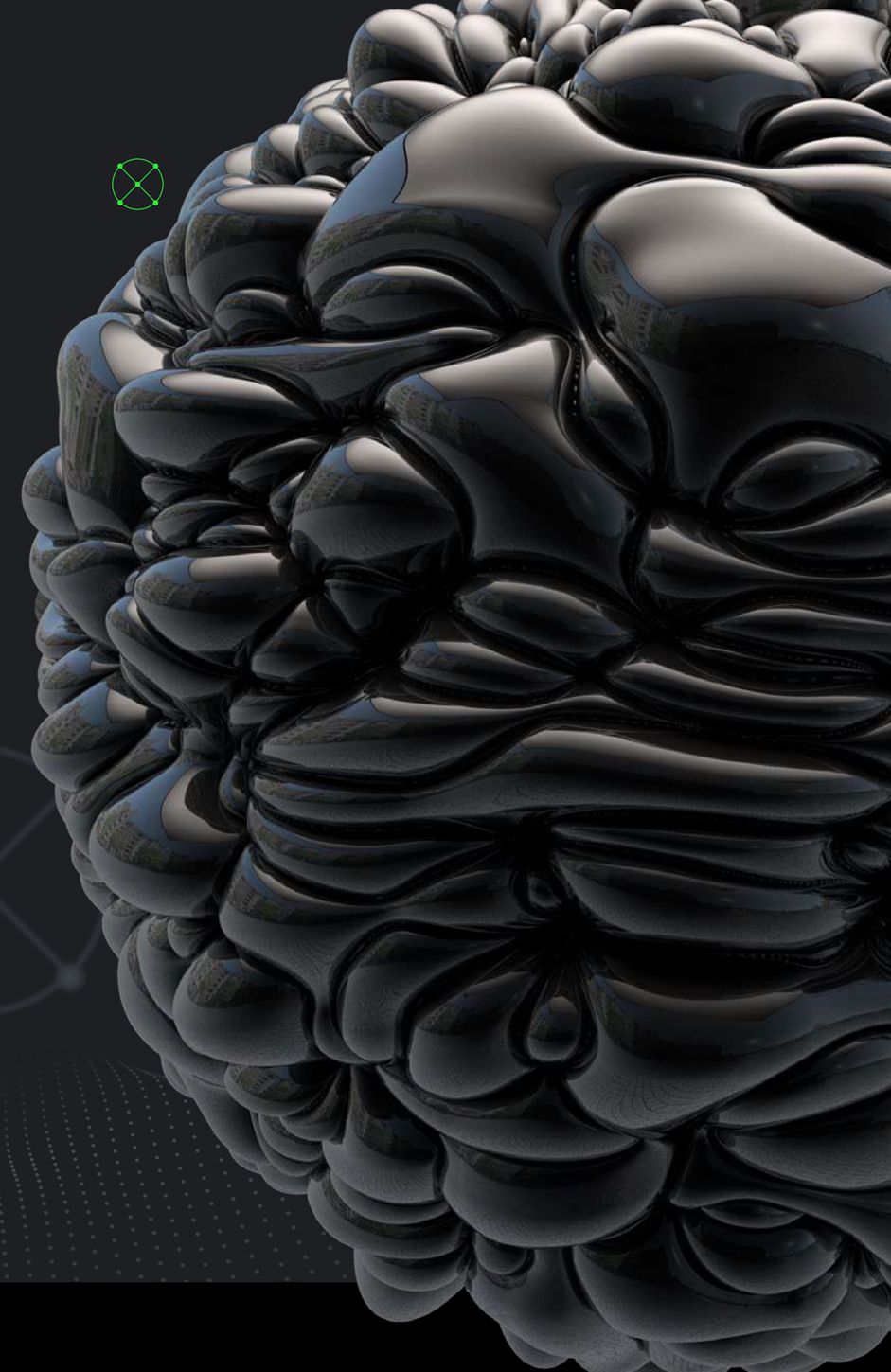
Phishing

Phishing is a technique that relies on social engineering to lure victims into divulging confidential information such as passwords and banking details. The most common way users encounter phishing is through emails containing malicious attachments or links.

Phishing campaigns may be incredibly broad and indiscriminate, targeting millions of individuals with the same lure to maximize potential victims. This method is typically used by financially motivated attackers who are not focused on a specific person or organization. Alternatively, phishing can be fine-tuned to target a single victim using specific details relevant to them. This technique is called spear phishing and is more likely to be used by attackers looking for access to a specific system.

Phishing remains a threat today due to the potential of human error. The attacks are constructed to trick victims into opening attachments or following malicious links. However, technology is improving in this area due to a recent surge in the popularity of phishing attacks. The 2019 Verizon DBIR report cited that phishing was the top threat action: involved in 32% of confirmed breaches, as well as 78% of cyber-espionage incidents[14].

As with many aspects of cybersecurity, the best defense is training and awareness. However, user education is especially critical for combating phishing as it specifically targets the human element. Training should focus on awareness around opening attachments and links from unknown sources. Scanning attachments that seem suspicious or checking the full URLs of links are also good anti-phishing practices.



Ransomware

Ransomware is a category of malware that encrypts files on machines and network storage devices. Threat actors then extort payment from victims who want their files decrypted and their access to them restored. Attackers often exfiltrate sensitive data from an environment before deploying ransomware and may use it as leverage to coerce the victim to pay. The contents of the stolen data may influence the final ransom price demanded by the threat actors, depending on its sensitivity.

Victims of these attacks are often told to pay using cryptocurrencies. However, there is no guarantee that paying the ransom will result in the data being decrypted. Organizations affected by ransomware may see a financial impact beyond the initial decryption cost due to loss of revenue while systems are down. Costs may also arise from the permanent loss of data if decryption never happens.

There are several variations of ransomware. Its production and use are often easier than other forms of malicious payloads. In some cases, ransomware uses functionality already built into the operating system. Ransomware is also adaptable, with alterations in campaigns sometimes being as simple as changing the address for payments.

Ransomware is often deployed to endpoints through popular social engineering techniques like phishing. The responsibility of keeping an organization secure no longer lies with a single team, but through ensuring best practices are observed by all end-users. Each person plays a vital role in maintaining security. That said, there are many effective methods for reducing the likelihood of ransomware infections, including:

- Ensuring that AV products are up to date and that the latest version is running on all devices
- Where possible, ensuring files and attachments are scanned before being opened
- Performing regular data backups and keeping copies off-site

Coinminers

With the rise of cryptocurrencies, criminals have recognized a unique opportunity to generate an additional revenue stream on compromised machines. By using a computer's hardware, malicious software can generate crypto coins that are automatically deposited in the attacker's wallet.

Coinmining requires minimal work (and technical skill) from the attacker's perspective. Additionally, coinmining malware can passively generate revenue from all infected machines unlike ransomware, which might only see returns from one in 1,000 victims.[15]

Slow system performance may be an indicator of a coinminer infection. This malware operates by taxing CPU and GPU resources to mine cryptocurrency. Users can protect themselves from coinminers by not clicking on suspicious links or opening malicious email attachments.

- Technology — Software: 26%
- Service Provider: 11%
- Manufacturing: 10%
- Healthcare: 9%
- Government — Local/Education: 7%
- Other: 37%

- Retail and Wholesale: 47%
- Finance — Banking / Investments: 12%
- Healthcare: 7%
- Service Provider: 7%
- Technology — Software: 5%
- Other: 22%

What Makes a Target Appealing To Attackers?

Retail and Wholesale

The retail and wholesale industries appeal to threat actors due to their contact with sensitive customer information. Mobile point-of-sale (POS) devices regularly access credit cards, debit cards, and e-commerce platforms. Many retailers and wholesalers are set up to accept online payments as well, giving threat actors another avenue to harvest information.

While disrupting these organizations is often not a primary goal of these attacks, it can be an inevitable consequence. The theft of confidential and personal information often leads to reputational and financial damages and customers being subjected to future fraudulent actions.

Technology/Software

Malicious attacks on technology and software companies are usually intended to steal intellectual property or to establish a distribution platform for malware. Malware distribution platforms are useful for performing supply-chain attacks. A supply-chain attack infects known-good files at the source. This allows threat actors to initiate an infection downstream without needing to organize sophisticated distribution campaigns.

Supply-chain attacks require a significant amount of time and a core understanding of the targeted technology since remaining hidden is critical for success. Otherwise, threat actors could push their own software instead of infected copies of trusted software. These attacks are difficult to pull off, but are also hard to detect as seen in the 2017 CCleaner attack[16].

Threat actors may steal intellectual property to get source code that allows them to craft exploits. They may also steal it to circumvent the costs associated with researching the desired intellectual property from scratch. Attackers often perform lateral movement and other information-gathering tactics when searching for specific data within an organization.

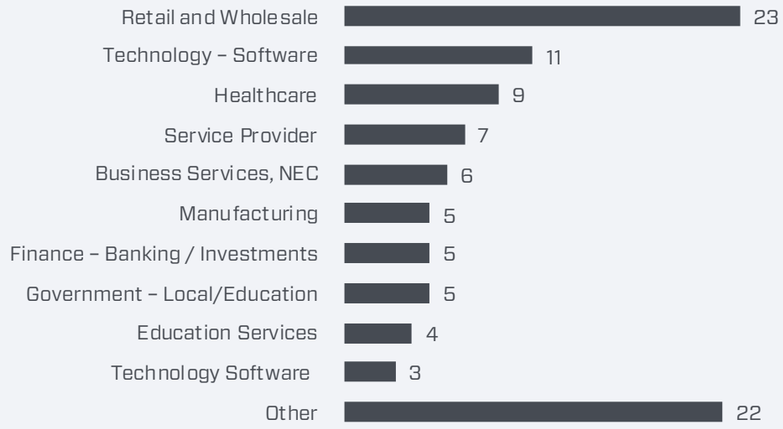
Service Providers

Like technology and software companies, threat actors will use a service provider's customer base to increase their distributions. Threat actors infiltrate service providers to establish a one-stop shop for the distribution of malicious tools. Each customer accessing the compromised central service provider gives attackers an opportunity to expand the reach of their malicious infrastructure.

Healthcare

Over the last few years, several healthcare organizations have been compromised by cyber attacks. The healthcare industry appeals to threat actors for many reasons, including:

- Their possession of confidential medical information
- IoT devices operating and collecting information in sensitive locations



Threat actors may steal intellectual property to get source code that allows them to craft exploits.

- The continued use of legacy systems that offer a considerable attack surface
- IT departments that lack the resources to provide adequate security coverage

Healthcare organizations are more likely to pay ransoms than an average user due to the importance and time-sensitive nature of their work.[17] Furthermore, health insurance companies store financial information along with personally identifiable information, which can command a hefty price on underground markets. This information can later be used for stealing identities and committing bank fraud. Information stealers and ransomware are the most common types of malware used against the healthcare industry.

Finance/Banking

The financial services industry is a popular target for attackers due to the sensitive data they possess and their access to financial accounts. Threat actor interest in these institutions has grown as more financial services move away from physical money and into the digital space. Attackers have responded to changes in the industry by showcasing increased capabilities, like the recent rise in ATM malware.[18] This malware is used to steal credit and debit card information on a large scale.

In some cases, the size of these companies makes them appealing targets. For example, the Equifax data breach in 2017 led to over 143 million customer records being stolen, costing the company over $600 million. One trend, not limited to the financial industry, is finance departments being targeted by threat actors. Attackers seek to gain access to accounts or systems of particular staff members, with the goal of fraudulently authorizing large company payments. These payments are quickly laundered by being split up, sent overseas, and redirected through multiple accounts to prevent banks from reversing the transactions.

Government

Government organizations are a high-value target to threat actors for many reasons, including:

- Access to military intelligence
- Various political motivations
- Access to financial information
- Significant quantities of personally identifiable information
- Information about sensitive government contracts

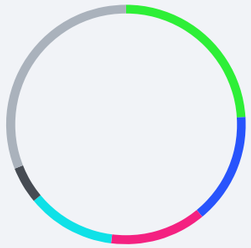
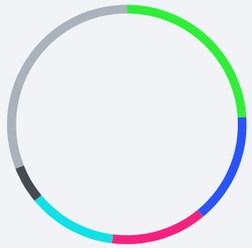
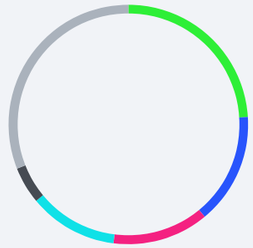
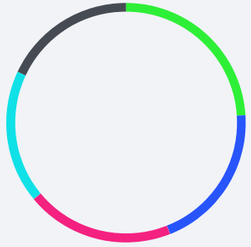
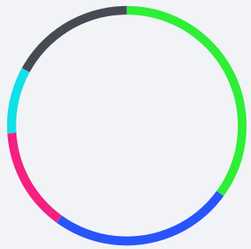
Attacks against government entities can have cascading effects that not only impact critical national infrastructure, but impact individuals as well. Some of the more serious forms of government-focused cyber attacks can threaten lives[19].

In 2019, police departments and local councils were attacked[20], resulting in significant financial impacts and costly follow-up investigations. Furthermore, government organizations may be exposed to legal actions, depending on data regulations, if information is stolen.

Attacks against government entities can have cascading effects that not only impact critical national infrastructure, but impact individuals as well. Some of the more serious forms of government-focused cyber attacks can threaten lives.

Industries Most Impacted by Three of the Most Prevalent Threats of 2019

	Emotet	Ramnit	Upatre
2019	Retail and Wholesale: 24% Transportation: 15% Education Services: 13% Government — Local/Edu.: 12% Manufacturing: 5% All Others: 31%	Retail and Wholesale: 27% Technology — Software: 10% Manufacturing: 8% Technology/Software: 7% Finance — Banking / Invest.: 7% All Others: 41%	Retail and Wholesale: 29% Technology/Software: 21% Defense and Aerospace: 10% Manufacturing: 9% Finance — Banking / Invest.: 5% All Others: 26%
2018	Government: 24% Healthcare: 20% Non-Profit: 20% Logistics: 18% All Others: 18%	Manufacturing: 35% Professional Services: 25% Media: 14% Products: 9% All Others: 17%	Technology: 50% Professional Services: 12% Manufacturing: 6% Finance: 4% All Others: 28%


Top Cyber Threats of 2019: Windows, Mac, and Linux

BlackBerry Cylance Research Operations uses an in-house tooling framework to monitor the threat landscape for attacks across different operating systems. Observing malicious files in the wild allows us to proactively leverage threat data to improve both current and future machine learning models.

This information also provides meaningful threat intelligence to our customers and the business community. Our top threats were harvested from 2019 threat data, identified, and associated with internally identified industry verticals.

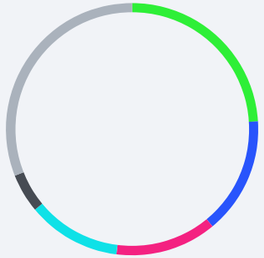
Here is a short summary of the top threats that most impacted widely used computer operating systems in 2019, as well as suggestions for mitigating the risks associated with these threats. The Windows section, due to their considerable customer base, includes tables showing the top five affected business verticals.

Windows Threats

Emotet

Top 5 Verticals Affected

- Retail and Wholesale: 24%
- Transportation: 15%
- Education Services: 13%
- Government — Local/Edu.: 12%
- Manufacturing: 5%
- Other: 31%



The malware family known as Emotet first appeared as a standalone banking trojan during the summer of 2014. It initially targeted the customers of a select list of German and Austrian banking institutions. Emotet uses carefully customized spam emails as an infection vector to compromise hosts.

Early Emotet was primarily designed to steal banking credentials along with other sensitive information. It propagated via social engineering techniques coupled with spam emails with malicious zip attachments to trick users into running the malware.

Once an infection occurs, Emotet uses advanced techniques to inject its malicious payload into a legitimate process. The malware also uses polymorphism to evade traditional, signature-based cybersecurity. These obfuscation techniques allow Emotet to operate while minimizing its chances of being detected.

Emotet achieves persistence across reboots by modifying the auto-start registry keys and service entries. As it evolved, Emotet became a modular malware, meaning it has the ability to download further modules and plugins to extend its functionality. Modules provide additional capabilities like Outlook scraping, mail spamming, password scraping, and the ability to connect to a botnet.

Three years after its discovery, Emotet began acting as a delivery mechanism for downloading other malware threats onto compromised systems. It delivered third-party malware like the Dridex banking trojan and Panda banker, and information stealing malware like AzoRult and Gootkit. Emotet's infection vector was also continuously changing. It initially leveraged spam emails with malicious zip files and embedded links. Emotet later used spam emails with weaponized Microsoft® Word docs containing heavily obfuscated malicious macros, PDFs, .xml files, and password-protected Word documents.

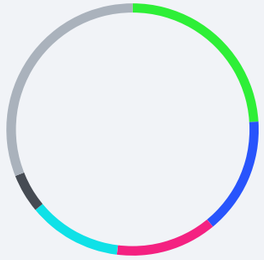
Threat actors behind Emotet continuously update its code to circumvent the latest AV detection and defensive measures. After a short hiatus over the summer of 2019, Emotet re-emerged in September with a new spam campaign using social engineering techniques. Once a system is infected, the malware enumerates a user's email inbox and inserts itself into existing legitimate email threads. It then creates new emails referencing current news events, attaches a malicious document to the thread, and mails itself to victims. This method makes it vastly more likely that an unwitting user will be tricked into opening the malicious email along with the infected attachment.

To mitigate Emotet risks:

- Keep all devices and software up to date
- Utilize a contemporary security solution
- Monitor host logs for suspicious service creation (Windows event ID 7045)
- Monitor host logs for suspicious scheduled task creation (Windows event ID 106)
- Deploy strong email security and anti-spam filtering to block malicious attachments and suspicious links
- Utilize spam blacklisting
- Ensure that Microsoft Office is configured by default to automatically deactivate all macros and to only execute macros that are verified as trustworthy
- Block all network connections to known Emotet/Heodo Botnet IPs and URLS

Kovter

Top 5 Verticals Affected



- Technology/Software: 23%
- Finance — Banking / Invest.: 21%
- Business Services: 15%
- Manufacturing: 9%
- Healthcare: 6%
- Other: 26%

Kovter is a sophisticated fileless trojan family. In order to maintain persistence on an infected system, it saves obfuscated script code in the registry, which runs during every boot. Technically, the payload exists in the registry, not as a file on disk. As a result, Kovter raises the bar for security analysts looking for the source of the infection.

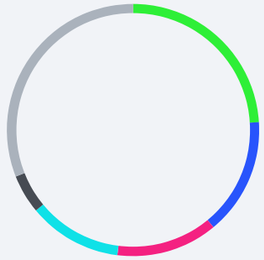
Kovter mainly spreads through malvertisements and exploit kits. The malware's main purpose is to perform click-fraud. Although the Kovter botnet was taken down at the end of 2018, we continued to see variants of Kovter in 2019.

To mitigate Kovter risks:

- Implement policies to protect against email threats
- Disable macro loading in Microsoft Office products
- Ensure browsers and plugins are up to date and monitored for suspicious behavior
- Consider disabling JavaScript®
- Disable command line shell scripting language wherever it's not required
- Ensure PowerShell is updated and configured to be security focused
- Monitor systems for unusual registry modifications
- Monitor logging and inbound/outbound network traffic

Poison Ivy

Top 5 Verticals Affected



- Retail and Wholesale: 44%
- Defense and Aerospace: 12%
- Technology/Software: 7%
- Manufacturing: 7%
- Finance — Banking /Invest.: 6%
- Other: 24%

Poison Ivy is a popular Windows RAT toolkit first identified in 2005. It is freely available online. Over the years, this commodity malware has been used by various groups and threat actors and deployed in several high-profile campaigns.

The toolkit is written in pure assembly (the Poison Ivy server or backdoor) and Delphi (the Poison Ivy client). It provides a graphical user interface where the builder generates customizable Poison Ivy servers as PE files or shellcode with no system dependencies.

Features include compressed encrypted communications, keylogging, capturing webcam/screen/audio/video, file transfers, system administration, password theft, and traffic relaying. The toolkit also accommodates third-party plugins.

Poison Ivy achieves persistence through ActiveX startup or registry key entries that execute on system startup. The Poison Ivy server can be copied to the System folder, Windows folder, or to alternate data streams in an effort to avoid detection. Poison Ivy contains options to configure a process mutex and perform process injection. Injection can be performed into the default browser process to bypass firewalls or into another specified running process.

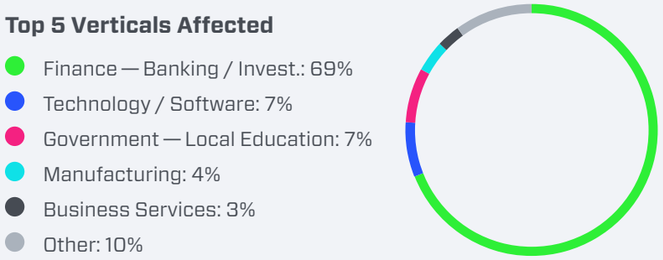
Poison Ivy is often spread by spear phishing campaigns with Poison Ivy servers dropped by weaponized Microsoft Word documents, PDFs, and Microsoft® Help Files. Once the Poison Ivy server executes on a target machine, it connects to the Poison Ivy client on the attacker's machine. The attacker can use this connection to take control of the target system.

To mitigate Poison Ivy risks:

- Phishing
  - Educate employees on phishing attempts
  - Implement policies to protect against email and phishing threats
  - Keep systems and applications up to date
- Poison Ivy Backdoor
  - Implement strong password policy within the organization
  - Monitor logging and network activity
  - Assign users appropriate account privileges
  - Monitor for applications or services that execute with system boot

Qakbot

Top 5 Verticals Affected



- Finance — Banking / Invest.: 69%
- Technology / Software: 7%
- Government — Local Education: 7%
- Manufacturing: 4%
- Business Services: 3%
- Other: 10%

Qakbot is a family of multi-pronged threats that first appeared in 2009. Most strains observed in the wild are highly robust and adaptable. Many contain various trojan family components as well as the capability to evolve, mutate, and self-propagate. Early variants were used primarily to steal data and establish a persistent foothold within the target environment.

Qakbot campaigns between 2009 and 2012 aimed to steal online banking credentials, which predictably increased this malware's popularity among cyber criminals. In 2017, several noticeable differences were found in new variants of Qakbot. Changes included the adaptation of Qakbot to target 64-bit systems and a complete malware rewrite in 2017. The updated Qakbot dedicated over 20% of its code functionality to evasion and persistence operations. While initially spread through phishing emails, Qakbot now contains modules for self-replication as well as the ability to laterally move across network shares.

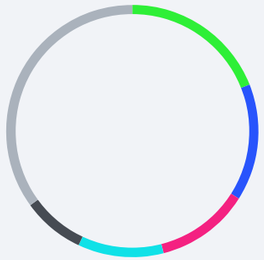
Qakbot can impact businesses by performing account and administrator lockouts. This makes containment and removal of the malware considerably difficult. Qakbot is a resilient threat that has resurfaced many times since 2009 despite the efforts of both law enforcement and AV vendors.

To mitigate Qakbot risks:

- Contain the spread of a Qakbot infection
- Cut off communication with the C&C server
- Implement proper privilege and access right distribution amongst end-users
- Monitor new service creation and newly formed scheduled tasks (can be achieved by tracking event ID 7045)
- Deploy up-to-date and effective antivirus technology on the endpoint
- Take note of IP/domains associated with the previous attack and monitor for reinfection
- Determine the original attack vector and mitigate this to avoid future attacks

Ramnit

Top 5 Verticals Affected



- Technology/Software: 19%
- Education Services: 15%
- Finance — Banking / Invest.: 12%
- Retail and Wholesale: 11%
- Manufacturing: 8%
- Other: 35%

Ramnit is a parasitic virus that infects Windows PE executable files. It also has worming capabilities that allow it to spread to removable media and create shortcuts pointing to copies of the malware. Ramnit can infect HTML files by injecting them with VBS code. Users who later access the HTML files are infected with the virus.

Ramnit is designed to function as a banking trojan as well as a remote access trojan. Over time, the original version of Ramnit was modified to include new capabilities. Upgrades included an ability to create a backdoor, a C&C server, and communications to coordinate infected machines in botnet campaigns. In February 2015, European authorities took down a Ramnit botnet that infected 3.2 million machines. However, Ramnit resurfaced again in December 2015.

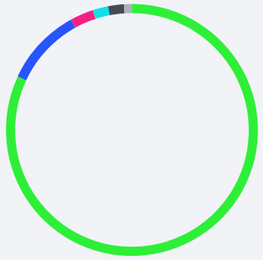
By 2016, new variants of Ramnit targeted major banks in the U.K. Some Ramnit campaigns and attacks now operate in a truly fileless manner, without relying on directly running PowerShell or JavaScript code pieces. Ramnit is known to store XOR-encrypted payload data in the registry. Ramnit's loader thread then parses and decrypts the binary large object (BLOB) from the registry to perform process injections.

To mitigate Ramnit risks:

- Monitor outbound connection requests to suspicious addresses/IPs
- Educate employees on typical phising and spear phishing techniques
- Ensure account privileges are mediated to the appropriate employees
- Keep detection and mitigation software on the endpoint up to date
- Stop execution of non-verified email attachments sent to end-users

Sakurel

Top 5 Verticals Affected



- Finance — Banking / Invest.: 82%
- Manufacturing: 10%
- Technology / Software: 3%
- Service Provider: 2%
- Retail and Wholesale: 2%
- Other: 1%

Sakurel, also known as Sakula and VIPER, is a RAT which connects to a server and opens a remote shell. The compile timestamps on Sakurel samples show that the malware first surfaced in November 2012. This malware is typically used in targeted attacks. Sakurel is downloaded from malicious URLs that deliver exploits the Microsoft® Internet Explorer Use-After-Free Remote Code Execution Vulnerability (CVE-2014-0322)[21]. This was a zero-day vulnerability in Internet Explorer at the time of discovery.

When the trojan is executed, it copies itself to %Temp%\MicroMedia\MediaCenter.exe. It then drops and registers the %Temp%\MicroMedia\MicroSoftSecurityLogin.ocx file as an ActiveX component.

The trojan creates the following registry entry to run every time Windows starts: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"MicroMedia" = "%Temp%\MicroMedia\MediaCenter.exe".

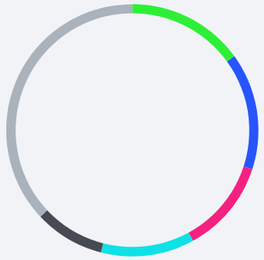
Sakurel then modifies the hosts file to redirect the browser to a compromised URL or IP address. It connects to the oa[.]ametekesen[.]com remote server and opens a remote shell. Additionally, Sakurel may monitor the victim's browser activity and download additional files.

To mitigate Sakurel risks:

- Ensure that all software and hardware is up to date
- Educate employees on the dangers of clicking unknown links to prevent the unintentional compromises of devices and networks
- Implement a strategy that involves regular backups of critical data and store this data in multiple locations for redundancy
- Ensure users are limited to appropriate account privileges
- Disable unused and/or unnecessary ports as they can be used as an attack vector by the malware
- Setup secure remote access controls (e.g. only allow remote access through VPNs or hardened security gateways)
- Perform monitoring and logging of all network activity

Upatre

Top 5 Verticals Affected



- Technology/Software: 15%
- Manufacturing: 15%
- Defense and Aerospace: 12%
- Service Provider: 12%
- Pharmaceutical: 9%
- Other: 37%

Upatre, first discovered August 2013, reached its zenith in 2015. While it has declined in popularity since then, it remains a viable threat, particularly for technology organizations and other professional services providers.

Upatre usually spreads through spam emails that contain infected file attachments. These emails often pose as invoices or voicemail message notices. This malware can also be encountered through attached password-protected archives or installed drive-by through infected website links.

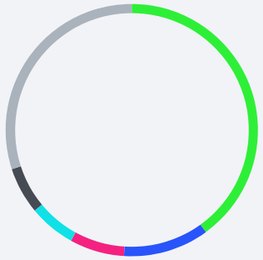
When executed, Upatre can download other malware on infected systems like the Zeus/Zbot banking trojan and variants of Rovnix rootkit, Crilock ransomware, and others.

To mitigate Upatre risks:

- Ensure your system and applications are up to date
- Educate your employees on phishing attack scenarios (as human error is the main infection vector)
- Do not click or download attachments received in email by unknown senders
- Do not be fooled by familiar-looking icons in the attachment (e.g. PDF icons)
- Have a modern AV solution in place
- Disable macros in Microsoft Office

Ursnif

Top 5 Verticals Affected



- Service Provider: 40%
- Energy and Mining: 11%
- Apparel and Fashion: 7%
- Manufacturing: 6%
- Technology / Software: 6%
- Other: 30%

The Ursnif banking trojan, now over a decade old, has a particularly colorful history. Numerous source code leaks and variations have led to this threat also being known as Gozi, ISFB, Rovnix, and Dreambot. Ursnif uses a technique known as web injection or man-in-the-browser (MiTB) to steal banking information and victims' funds.

Ursnif is able to modify web page content before it appears to users by hooking core functions inside well-known browser DLLs. This technique allows the malware to steal credentials even if the website is using Transport Layer Security (TLS). Attackers can then use stolen credentials to withdraw money from victims' banks without alerting them. This attack mimics a legitimate transaction, making it particularly hard for banks to detect.

While still predominantly a banking trojan, the most recent version of Ursnif has a range of capabilities, including:

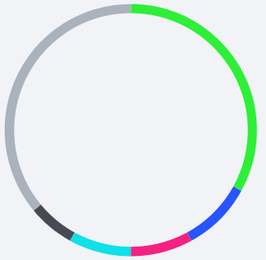
- Downloading and launching other software or malware families
- Running a SOCKS proxy server
- Screenshot capturing
- Keylogging
- Stealing credentials from browsers, Microsoft Internet Explorer, Microsoft® Outlook®, and Mozilla® Thunderbird®
- Stealing cryptocurrency wallets

To mitigate Ursnif risks:

- Avoid establishing connections to unsecured networks (public Wi-Fi, etc.)
- Don't keep sensitive information stored in browser history (credit card information, etc.)
- Update browsers to the latest versions and consistently monitor for patch information
- Determine the original attack vector and mitigate this to avoid future attacks
- Ensure browser plugins are up to date and monitored for suspicious behavior
- Take note of IPs and domains associated with the previous attack and monitor for reinfection
- Utilize a firewall to filter and block all inbound and outbound connections to unverified and untrusted locations
- Enable cloud-delivered protection and automatic sample submission on Windows® Defender

Vercuse

Top 5 Verticals Affected



- Retail and Wholesale: 33%
- Defense and Aerospace: 9%
- Technology/Software: 8%
- Manufacturing: 8%
- Technology — Software: 6%
- Other: 36%

Vercuse is a threat typically distributed via drive-by download or through compromised removable USB drives. Copies of Vercuse are dropped in multiple hidden folders. To achieve persistence, the malware also adds registry keys that run on startup. Specifically, Vercuse modifies the following subkey: "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce" with data: "'SecurityUpdate<5 random numbers>'" and sets value: "%APPDATA%\Microsoft\Windows\~temp~<5 random numbers>iN.exe".

Payloads dropped by Vercuse can vary, though many appear as Backdoor:Win32/Poison. Vercuse will masquerade as legitimate software, such as the Microsoft Malware Removal tool. The malware uses several methods of AV evasion, including anti-sandbox techniques and tool-specific detection (based on the text displayed in the window name). If a specific tool is used, Vercuse will terminate its running processes. The biggest threat posed by Vercuse is its ability to drop additional malware samples.

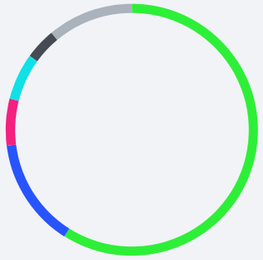
To mitigate Vercuse risks:

- Ensure all endpoint applications and systems are up to date with the latest software
- Avoid sites outside of necessary business due to the nature of the primary attack vector
- Watch out for non-native antivirus applications appearing on the endpoint
- Be aware of non-scheduled security updates taking place

Zegost

Top 5 Verticals Affected

- Service Provider: 59%
- Govt. — State/Provincial: 14%
- Technology/Software: 6%
- Manufacturing: 6%
- Business Services: 4%
- Other: 11%



Zegost is an infostealer typically spread by phishing emails containing malicious attachments or by unsuspecting users visiting infected websites. The malware's primary purpose is to steal and exfiltrate user information and report back to its C&C architecture. First discovered in 2012, Zegost gained notoriety when it targeted Nepalese Government sites by using a Java® exploit described in CVE-2012-0507[22]. The malware has many active variants and is still being used today.

Once Zegost infects a system, it steals user information, performs keystroke logging, and monitors mouse events. The malware has also been observed using compromised devices to participate in distributed denial of service (DDOS) attacks. All information gathered by the malware is sent back to the C&C server. Zegost can also use its C&C server to update and/or delete itself. This malware adds a registry key that runs during startup to achieve persistence. Zegost can also install further malware at the request of its C&C server(s).

To mitigate Zegost risks:

- Educate employees on phishing threats and dangers
- Implement policies to protect against email and phishing attack vectors
- Keep systems and applications up to date
- Install the latest version of Java
- Monitor network activities for illicit connectivity
- Look for the presence of registry key 'Kris' and executable 'BJ.exe', which are affiliated with this malware family

Mac Threats

CallMe

CallMe is a malware backdoor specifically targeting the macOS® operating system and its users. First seen in the wild in 2013, the malware tends to focus on Asia-specific targets. The malware is dropped onto users' devices using maliciously crafted Microsoft Word documents that rely on exploiting CVE-2009-0563[23], a vulnerability which has since been patched since 2009.

Once on a system, it attempts to reach out to its C&C server and copy itself onto the device as well as create a launch point. In order for the backdoor to maintain root permission access after reboot, it copies files to the 'LaunchDaemons' folder.

The malware also creates temporary file(s) '/tmp/tmpAddressbook.vcf' that contain the users contact data and 'tmp/__system', which is the running backdoor. The backdoor is not developed for use on newer editions of the macOS and Microsoft Word. If a user is running macOS Mountain Lion or later, they will be notified when the backdoor tries to access their user contacts. The notification also informs users that Microsoft has patched the Word vulnerability used by the malware.

To mitigate CallMe risks:

- Make sure Microsoft products (like Microsoft Word) are up to date
- Ensure macOS is updated
- Educate end-users on the dangers of allowing unknown programs to run and execute on devices
- Monitor networks for suspicious activity

KeRanger is one of the first ransomware threats to target the macOS operating system.

KeRanger

KeRanger is one of the first ransomware threats to target the macOS operating system. This malware was distributed by threat actors compromising the installer for the Transmission BitTorrent client application. KeRanger was signed with a valid Mac Developer ID in 2016, meaning it could bypass the built-in macOS Gatekeeper feature that blocks untrusted applications. Once discovered, the fraudulent signature was quickly revoked.

When executed, KeRanger encrypts many different file types found in the /Volumes directory and its subdirectories. When it encrypts the user's files, it appends a '.encrypted' file extension to them. KeRanger then drops the 'README_FOR_DECRYPT.txt' file that instructs the user to download the TOR browser and also provides payment instructions.

To mitigate KeRanger risks:

- Ensure macOS is updated
- Educate users to not download applications from unknown sites
- Backup system information as frequently as possible
- Have a business strategy for dealing with ransomware incidents

LaoShu

First discovered in early 2014, LaoShu is a RAT that employs spam emails as its primary infection vector. This signed malware attempts to trick an unwitting user into executing it by masquerading as a PDF file. It is actually a .app Mach-O application file. Once executed, it opens a backdoor that gives an attacker the ability to control, steal, or exfiltrate sensitive information.

Some LaoShu variants can scan a host for commonly used document files like .doc/docx, .xls/xlsx, and .ppt/pptx. If found, these document files are compressed into a .zip format for subsequent exfiltration to C&C servers controlled by the attacker. LaoShu variants can also download additional files/ malware to a victim machine, take screenshots, and run shell commands.

To mitigate LaoShu risks:

- Keep all devices and software up to date
- Utilize a contemporary security solution
- Implement and enforce a strong and complex password policy
- Utilize a firewall to filter and block any or all inbound and outbound connections to unverified and unknown locations
- Deploy a strong email security and anti-spam filtering solution to block malicious attachments, suspicious links, and links to download files
- Use spam blacklisting
- Implement an internal employee education program emphasizing the importance of handling suspicious emails
- Utilize access control lists (ACLS) and password protection to limit user access to shared files
- Disable file-sharing where it is not needed

NetWiredRC

NetWiredRC is a multi-platform RAT that can be used in Windows, macOS, and Linux® systems. It is a form of malicious software that is installed without the user's knowledge. NetWiredRC is used to harvest sensitive information, perform keylogging, capture screens, give attackers remote access to the compromised machine, and more.

NetWiredRC, also known as OSX.Wirenet/OSX.Netwire, was first discovered in 2012. It was one of the first infostealing malware families to steal passwords from Linux and macOS systems. To achieve persistence, NetWiredRC acts as launch agent and as a login item. This malware is particularly popular with APT33 group.

To mitigate NetWiredRC risks:

- Block 212[.]7[.]208[.]65 (NetWire's C&C) in your router/ firewall
- Monitor for presence of "%home%/WIFIADAPT.app" in your home directory, and if found, delete it

XcodeGhost

XcodeGhost, first identified in 2015, is a malware that affects both iOS® and macOS. It is also the first compiler malware in macOS. XcodeGhost's malicious code was repackaged into some versions of the Xcode installers, Apple's official tool for developing apps for iOS and macOS.

The malicious installers were uploaded to Baidu's cloud file sharing service used by Chinese iOS and macOS developers. It successfully infected multiple iOS apps, at least two of which were submitted and accepted into the App Store. XcodeGhost's main objective is to gather information on infected devices and upload it to C&C servers.

XcodeGhost is often considered the first large-scale attack on Apple's App Store®. XcodeGhost infections give attackers remote access abilities, the option to steal device information, power to read and write to the clipboard, and browser hijacking capabilities.

To mitigate XcodeGhost risks:

- Ensure that all software and hardware is up to date
- Implement a strategy that involves regular backups of critical data and store it in multiple locations for redundancy
- Ensure that apps being downloaded from the iOS App Store are 100% trustworthy
- Setup secure remote access controls (e.g. only allow remote access through VPNs or hardened security gateways)

Linux Threats

Gafgyt

Gafgyt is a variant of a competing botnet, JenX. First discovered in 2014, Gafgyt has been updated as recently as September 2019. The malware uses remote code execution exploits to gain access and recruit routers into its IoT botnet. Gafgyt specifically targets gaming servers with DDOS attacks. The malware also targets small organizations and home-based wireless routers, including models from Zyxel, Huawei, and Realtek.

Gafgyt typically has hardcoded functions related to specific vulnerabilities, with its multiple variants targeting different exploits. Once a system is infected, the malware will pull additional binaries down from hardcoded URLs. The malware also sends the compromised device's information to its C&C server to add it into the botnet.

The Gafgyt botnet uses HTTP flooding to perform its attacks. It contains specific commands to attack Cloudflare services and Valve Source Engine services. The malware also has the ability to kill other botnets that currently reside on infected devices.

Unusual networking activity may indicate a Gafgyt infection. Gafgyt targets unpatched vulnerabilities in networking devices from a range of different manufactures.

To mitigate Gafgyt risks:

- Make sure all wireless routers have the latest firmware updates

Mirai

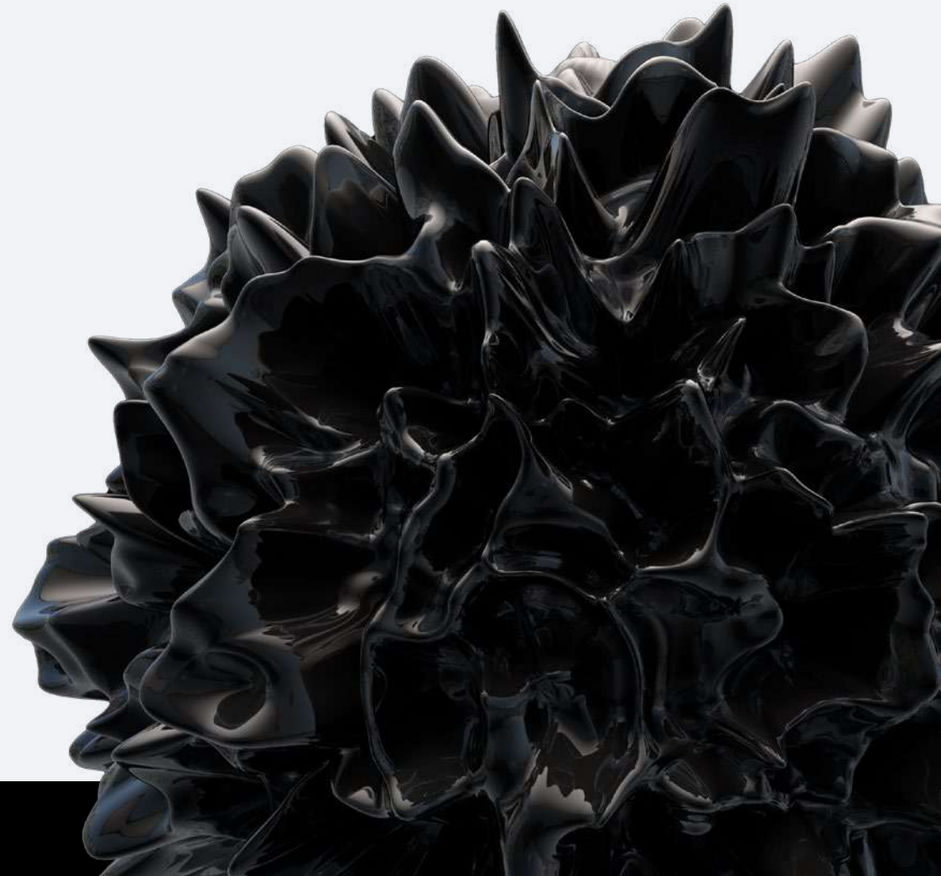
Mirai is a malware botnet based on the Linux platform. It compromises IoT devices in order to conduct large-scale distributed DDOS attacks. First identified in August 2016, Mirai has been leveraged in some of the most prolific DDOS attacks in the world[24]. Two notable examples include the assault on Brian Krebs' website and the Dyn attack on DNS servers, affecting millions of endpoints.

Mirai contains a hard-coded list of do-not-infect IP addresses, including the U.S. Postal Service and U.S. Department of Defense. When a vulnerable IoT device is located, Mirai launches a dictionary attack consisting of over 60 default factory login credentials. If a system is successfully infected, Mirai will run a system scan to identify and remove any competing malware.

Multiple variants of Mirai have surfaced since the original 2016 detection, each tailored to a specific vulnerability identified in an IoT device. The source code of Mirai is readily available on GitHub®, making it easy for threat actors to create variants. The arrest of the original authors has done little to slow the persistence of the botnet. Mirai continues to pose a serious risk due to the popularity of IoT devices and user's tendency keep default passwords.

To mitigate Mirai risks:

- Consistently monitor network activity of IoT devices
- Isolate compromised devices
- Implement effective network monitoring tools
- Keep antivirus software up to date



Setag

Setag is a Linux-based malware variant first spotted in the wild in 2016. It installs a backdoor, usually after being downloaded by unwitting users visiting a malicious site. It may also be dropped on systems by other malware variants.

Once installed on a host, Setag drops various configuration files, including a list of IP addresses used to facilitate DDOS attacks. This malware also gives an attacker the ability to control, scrape, and exfiltrate sensitive information.

As Setag evolved, it gained the ability to achieve persistence across reboots by adding scripts to the /etc/rc(integer 1-5).d/ and /etc/init.d/ locations. Setag also started being delivered to hosts via the exploitation of - Apache Struts2 Remote Code Execution Vulnerability (CVE-2017-5638)[25].

Setag variants have been seen as recently as July of 2019, including in an attack chain targeting Elasticsearch Databases.

To mitigate Setag risks:

- Keep all devices and software up to date
- Use a contemporary security solution
- Ensure system patches are up to date (Setag is known to exploit Apache Struts2 Remote Code Execution Vulnerability (CVE-2017-5638))
- Implement an internal employee education program regarding the importance of safe Internet browsing (not opening suspicious attachments, not executing unknown software, etc.)
- Monitor systems for the creation of the "/usr/bin/dpkgd/" folder, a Setag indicator of compromise
- Implement a reputable network security solution to block all connections to known Setag C&C infrastructure

XOR.DDoS was first seen in 2014 and used in a large-scale DDOS attack in 2015. XOR.DDoS utilizes infected Linux-based systems.

XOR.DDoS

XOR.DDoS was first seen in 2014 and used in a large-scale DDOS attack in 2015. XOR.DDoS utilizes infected Linux-based systems. The malware infects systems by relying on brute force attacks to discover the password to vulnerable device Secure Shell (SSH) services. Once SSH credentials are acquired, this threat uses root privileges to run a script that downloads and installs further XOR.DDoS malware.

XOR.DDoS gathers basic system information before encrypting it and sending it to its C&C server. The malware creates a cron job that runs hourly to ensure XOR.DDoS is active. This malware can download and execute other files, update itself, kill running processes, remove files, and execute DDOS attacks. XOR.DDoS can also use TCP-SYN flooding, TCP-ACK flooding, and DNS amplification.

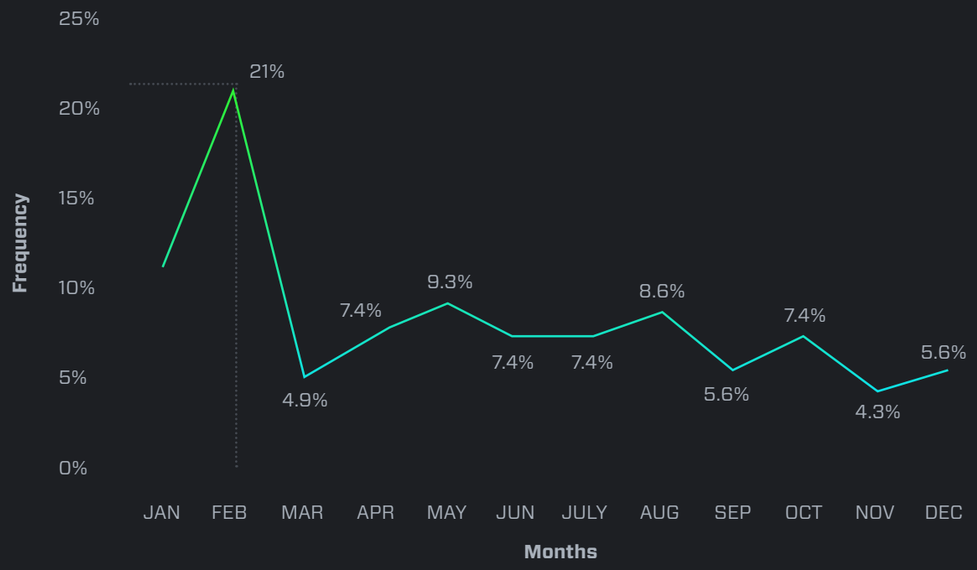
To mitigate XOR.DDoS risks:

- Make sure systems are patched and up to date with the latest versions of Linux
- Ensure password hardening is implement on all devices as the main attack vector for XOR. DDoS is poor security and weak passwords
- Prevent unauthorized access of root privileges
- Monitor systems for suspicious network activity
- Monitor systems for unexpected script execution

Notable Data Breaches in 2019

Unfortunately, the majority of notable data breaches in 2019 still resulted from unsecured databases, rather than from sophisticated and novel techniques deployed by modern attackers. This was once again the worst year on record for data breaches, and there clearly remains much work to be done in education and firming up security for organizations in the modern era.

Frequency of notable data breaches in 2019



American Medical Collection Agency, AMCA

American Medical Collection Agency, a billing collections service provider, had its payment portal attacked, leading to an exposure affecting over 200,000 victims. The data leak originated around September 2018 and persisted for at least seven months. The breach was discovered when its Card Not Present (CNP) database was found for sale on the dark web.[26]

The data was traced back to AMCA's online portal after evidence of social security numbers and dates of birth were discovered.[27] AMCA's affected customers included medical testing giants LabCorp and Quest Diagnostics. The breach eventually led to AMCA filing for bankruptcy, citing costs incurred from sending customer notifications and losing its largest clients.[28]

September 2018

- 140,000 social security numbers and dates of birth
- 200,000 victims

Threat Actor Goes on a Spree

In February 2019, 617 million records were stolen from compromised websites. These were released by an attacker who previously expressed a desire to put one billion records up for sale on the dark web . Most of the data released came from intrusions occurring in 2018 but were undisclosed at that time. Some of the affected targets included:

- Dubsmash, a video messaging application
- 500px, a photography social networking site
- Mindjolt, a gaming platform
- Wanelo, a digital mall
- Yanolja. a South Korean travel company

It was reported that the attacker exploited web application vulnerabilities to access and exfiltrate user account data[29].

February 2019

- 617 million records
- Web application vulnerabilities

Gearbest

In March 2019, a security researcher discovered an exposed Elasticsearch server belonging to the online shopping giant, Gearbest. The server contained over 1.5 million customer data records related to payment records, orders, etc. It was reported that this data was stored unencrypted[30]. Gearbest mentioned in their disclosure that the breach may have affected newly registered customers whose data was temporarily stored within the exposed database.[31,32]

March 2019

- Online retailer
- 1.5 million customer records
- Unencrypted database

Sept 2018

American Medical Collection Agency, AMCA

200,000 Victims

Feb 2019

Threat Actor Spree

617 Million Records

March 2019

Gearbest

1.5 Million Customer Records

July 2019

National Revenue Agency (NRA) of Bulgaria

5 Million Citizens Impacted

National Revenue Agency (NRA) of Bulgaria

In July 2019, an anonymous threat actor reached out to the Bulgarian media to report details of a an attack against the "servers of the Ministry of Finance". This attack affected approximately 57 folders with files containing national identification numbers, tax and social security payments, debts, etc. Up to 5 million Bulgarian citizens were potentially affected by this breach. The NRA confirmed the attack the following day and stated that "its servers were accessed through a rarely used VAT refund service for deals abroad" with the breach affecting 3% of their database.[33, 34]

July 2019

- 5 million citizens impacted
- 3% of the database
- National ID numbers, tax and social security payments

What Can Be Done

Data breaches are caused by several factors. Practicing good security hygiene and enforcing back-to-basics measures can effectively reduce the likelihood of a breach. Steps that can improve your security posture include:

To mitigate phishing attacks:

- Regular security awareness training of users on social engineering tactics
- Enforcement of multi-factor authentication across enterprise-deployed apps
- Configuration of DMARC for combatting domain impersonations

To mitigate compromised credentials:

- Enforce password managers for storing enterprise secrets
- Use AI-driven user behavior analytics for monitoring user activity
- Enforce strong passwords that are regularly rotated
- Assign permissions based on the principle of least privilege

To mitigate security misconfigurations:

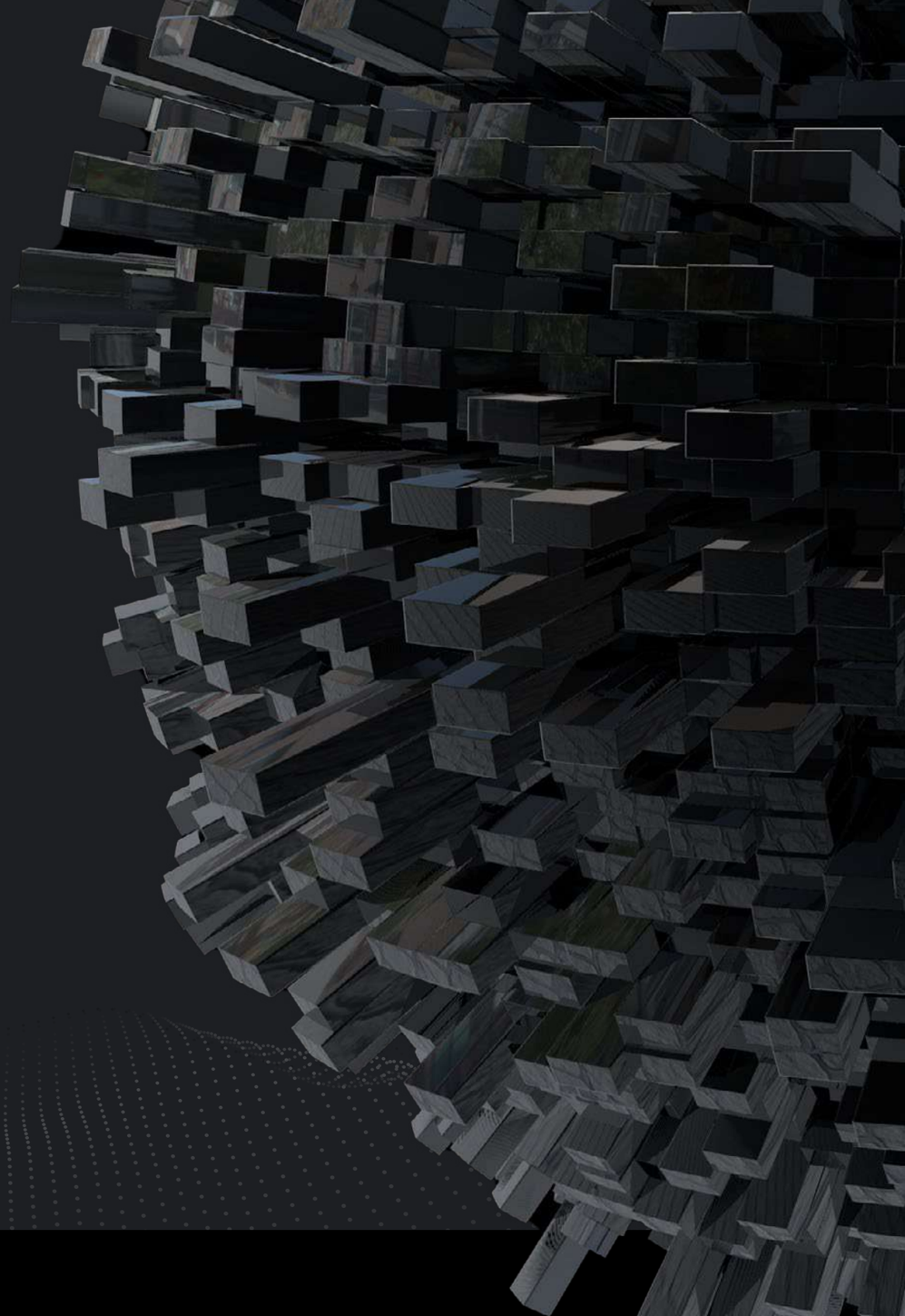
- Regularly patch software vulnerabilities
- Have automated, continuous integration processes that enforce organization-defined policies for deploying cloud resources

Identity Access Management: Securing the Enterprise of Everything

Today's professionals enjoy unprecedented access to data. Cloud infrastructure and global connectivity have made information widely available across locations while technology companies have provided countless devices for accessing it. However, it is important to remember that attack surfaces expand along with the reach of wireless information and the growth of connected devices. As a result, many endpoint protection strategies run into issues when work resources interact with IoT devices.[35]

Consider an employee who uses their smart phone to access work emails. When travelling, the worker pairs their phone with their car. How secure is the phone? How secure are the various third-party apps that have access to the phone? How secure is the embedded system in the automobile? The very nature of IoT devices all but guarantees a weak link will exist somewhere in each chain of interconnectivity.

The attack surface also grows when organizations migrate from only allowing corporate-issued devices to embracing bring-your-own-device policies. As more employees access organizational data from personal devices, the task of verifying user identity becomes increasingly critical to businesses. Multi-factor authentication (MFA) is one widely adopted technique used to address the identity verification problem. This method requires users to confirm their identity through a second source when they log in to their accounts. By verifying the legitimacy of a user, organizations lower the risk of their data being maliciously breached.



While MFA is a critical component of effective cybersecurity strategies, it cannot solve all user identity problems. For example, MFA is often a one-time action that does not consider normal behaviors and habits of the user. Often times, a user will authenticate in the morning and be considered a trusted user for the rest of the day. What happens if the user leaves their workstation? How can an organization know if an authenticated session started in the morning is used by the same person that afternoon?

On a related note, Amnesty International reports threat actors are using phishing sites to intercept and steal two-factor authentication (2FA) codes[36]. Other attackers prefer to find ways to bypass 2FA or MFA by focusing on vulnerabilities in specific elements of the authentication process. One well known bypass involves exploiting flaws in SMS communications to redirect authentication codes to the attacker instead of the intended recipient[37]. While 2FA and MFA are a strong step in the right direction, there is clearly room for improvement.

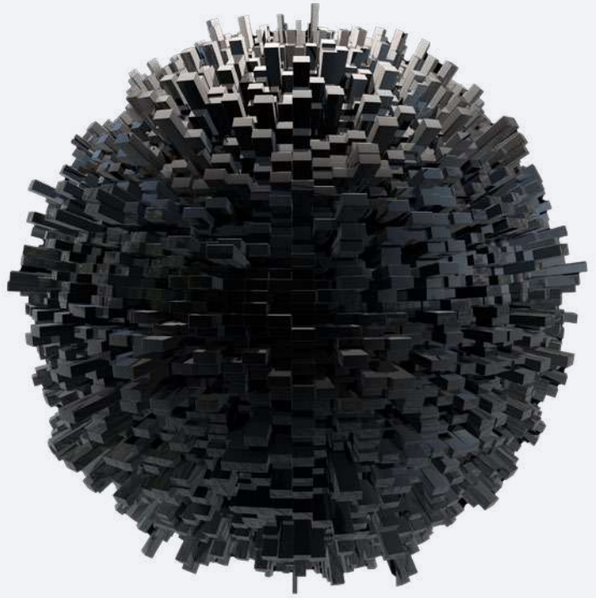
Since 2016, incidents involving compromised accounts and credentials have increased by 280%.[38] This increase is largely due to stuffing attacks, where threat actors use stolen usernames and passwords to gain access to multiple online sites. While relatively unsophisticated, stuffing attacks are successful and highlight the urgent need for better identity access management.

One security concept that needs to be revisited is the idea of a single, static, binary yes/no identity authentication process. This approach works for granting initial access to a system but offers no means of verifying identity over significant periods of time. A wiser alternative is to allow authentication systems to establish a continuous trust level.

For example, perhaps during the initial logon, our system is 100% certain a user is correctly identified. Later in the day, perhaps due to anomalous access request or new online behaviors, our system's confidence in the user drops to 70%. This loss of trust should indicate that it is time for the user's identity to be re-authenticated.

Continuous user authentication may sound like a resource-intensive effort that could hinder user productivity. However, highly trained, adaptive AI is capable of detecting and analyzing user behavior without becoming overly intrusive to employees. It can also consider information ranging from user's geographic location to their normal activity schedules when determining trust levels. With AI-driven user identification, an employer could vary a user's access for work done from the office, at home, in public spaces, etc.

These are a few of the concepts and considerations that directed the development of BlackBerry Cylance's new AI-driven, continuous user authentication technology. In the near future, our advanced user identity technology will be integrated with existing IoT, mobile, and enterprise security platforms.



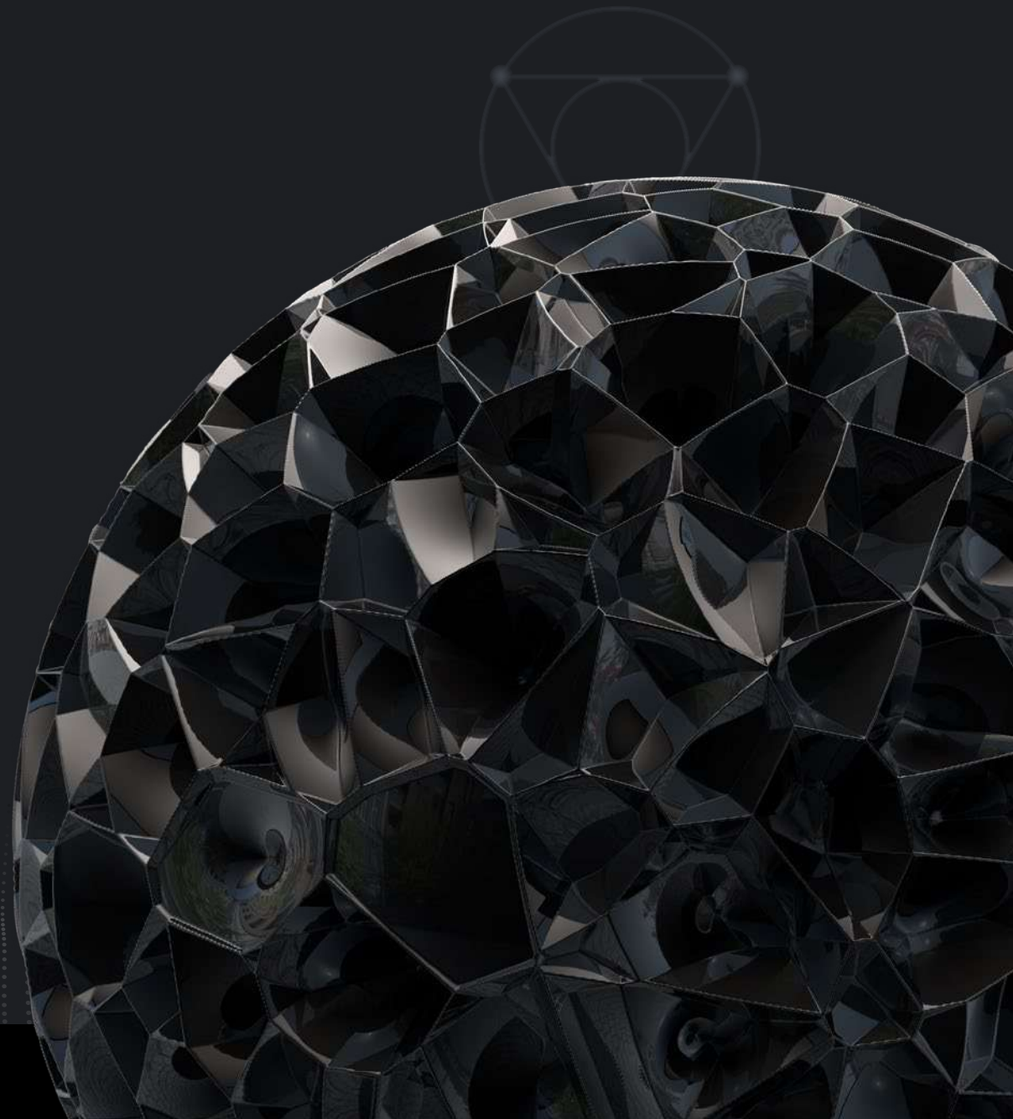
With AI-driven user identification, an employer could vary a user's access for work done from the office, at home, in public spaces, etc.

Mobile Security Issues

Learning from Other's Mistakes

It is often difficult to spot the flaws in one's security posture before a breach occurs. For example, in 2017, Equifax failed to implement adequate and multi-layered security to protect sensitive customer data[39]. This breach affected 148 million consumers. The subsequent investigation led to the Mandiant report that contained 11 remedial recommendations for Equifax:

- Enhance vulnerability scanning and patch management
- Reduce retention of sensitive data in databases
- Increase restrictions and controls for accessing data in critical systems
- Enhance network segmentation, restricting access from the Internet
- Deploy added web application firewalls and tuning signatures to block attacks
- Deploy file integrity monitoring technologies on application and web servers
- Enforce additional network, application, database, and system-level logging
- Deploy privileged account management solutions
- Increase encrypted traffic by deploying additional inline network traffic decryption capabilities
- Increase endpoint detection and response agent technologies
- Increase additional email protection and monitoring technologies



We conducted research to assess whether mobility solutions faced the same vulnerabilities as those that impacted Equifax. Where potential mobility threats were found, we considered the threat and identified potential mitigations. We then worked to ensure that enterprise departments could account for and implement the various mitigations we provided. Ownership of these strategies was established by providing them to specific teams within the business. For example, mitigations sent to a group responsible for specific elements of mobile security would also become their future responsibility to implement.

When considering the future delivery of secure MDM services, mobility and IoT vendors will focus on concepts like security resilience and improvement programs. By evaluating attacker objectives (derived from other breaches in the industry), they can cover many different technical control areas more effectively, including:

- Endpoint security
- Logging enhancements through software inventories
- Data protection
- New product introduction processes

Mobility and IoT specialists should give special consideration to the ownership of applied components used to enable mobility solutions. Functional components should be managed as distinct and separate functions. Separation should exist between the enterprise server, enterprise client, connected IoT devices, and other hardware-backed solutions. This approach allows businesses to assess risk more effectively between business processes and the technologies that enable them.

As a result of our research, we believe mobility and IoT providers can easily assess top priorities and identify primary threats to a product. The consumer can likewise develop their own top priority list to focus their security response and threat mitigation activities.

Mobility and IoT providers take a systematic approach to identify potential exposures. This threat-mapping process allows them to maximize protective, detective controls, and integrate response and recovery processes throughout the environment.

We have identified several threats in functional components that mobility and IoT providers should address, including:

As a result of our research, we believe mobility and IoT providers can easily assess top priorities and identify primary threats to a product.

Enterprise MDM Server Dangers

- Lateral movement within the product environment
- Weaknesses in the MDM endpoints and APIs
- Exposure of MDM from external components and routing mechanisms
- Integration with other MDM systems that have pre-existing security issues
- Cross-tenant cloud issues (for cloud users)
- Security issues introduced in new features
- Vulnerabilities in open source software or third-party libraries
- Web vulnerabilities
- Weak cryptography
- Insufficient logging and monitoring

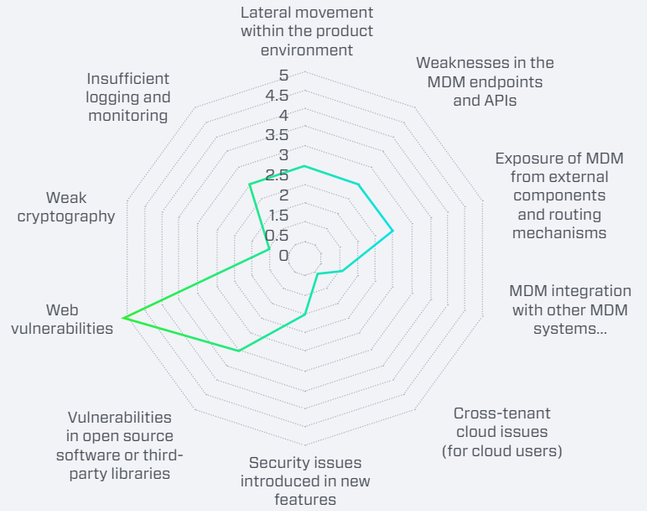


Figure 1. High-level synopsis of the predicted escalation and criticality/pervasiveness of threats.

Enterprise Client Dangers

- Client application data leakage
- Inadequate DLP strategies coupled with changes in OS
- Plain text transport and storage
- Reverse engineering to identify unknown application development vulnerabilities
- Bypassing of Android root and iOS jailbreak protection with rooting tools and hooking frameworks
- Bypassing or breaking application integrity protection
- Jailbreak and root detection hiding or masking
- Unknown application development vulnerabilities
- Client testing

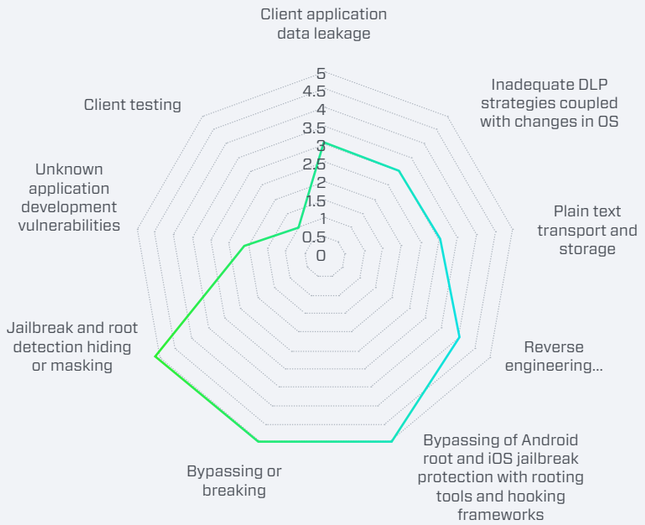


Figure 2. High-level synopsis of the predicted escalation and criticality/pervasiveness of threats.

IoT Dangers

- Challenges of migrating from self-hosted to cloud, including data handling, authentication, and authorization
- Secret handling in the cloud when scaling workloads where infrastructure platforms manage resources
- Changes in architecture or new implementation driving changes in the threat model that were not anticipated
- Database injection attack due to database migration or changes
- Business logic flaws, privilege escalation, and authentication
- Generic web application vulnerabilities (OWASP Top 10)

Figure 3. High-level synopsis of the predicted escalation and criticality/pervasiveness of threats.

End-users, MDM, and IoT vendors should consider these pervasive threats holistically and systematically develop a plan to manage them. Security plans should use industry best practices while also considering the examples of other's failures. By working together to maintain and manage security, customers and vendors can greatly minimize the impact of an attack.

The Iceberg Effect

The Iceberg Effect refers to a paradigm concept created by the previous diagrams, where 20% of dangers appear above centerline and 80% below. As the client analysis in Figure 2 shows, if the MDM provider and consumer focus on the large percentage of threats below the centerline, they can significantly minimize the external attack surface.

Over the past year, we have seen an increase of customer-commissioned testing that focuses on several attacks, including:

- Reverse engineering to identify unknown application development vulnerabilities
- Bypassing or breaking application integrity protection
- Jailbreak and root detection hiding or masking

An attacker with the right skills and adequate time can usually discover creative ways to bypass security controls. There are several well-known tools and explicitly documented standards available to help attackers. Many of these resources are free to the public. Examples of tools include Frida, a dynamic instrumentation toolkit that enables attackers to execute their own scripts in locked-down software. Frida allows attackers to hook into live processes and add functionality to applications. Magisk, another tool, allows attackers to assume root access and perform other system modifications. Magisk modifies a system without physically changing the system files, commonly called a system-less root. This technique can bypass device

tampering checks. It could also allow the attacker to install malicious applications or software granting them access to other systems.

Responding To Mobile Threats

How can MDM vendors manage mobility problems more effectively? One approach is automating various security controls that protect, detect, and respond to threats. There are also several manual controls that contribute to a holistic security strategy for consumers. Fundamental improvements to application code obfuscation, integrity checks, and root and jailbreak detection can reduce the attack surface. Greatly increasing the time needed to perform analysis of compiled code can also discourage attackers from undertaking such efforts. Any security measure that allows the enterprise more time to detect, respond, and recover from a breach is a net gain for organizations.

MDM vendor applications and code should focus on code flow, and string and symbol obfuscation. Mobile application code should challenge attackers trying to perform static analysis to identify key attributes or functions for malicious use. Fundamental improvements in coding can play a big role in the cybersecurity strategies of 2020. We recognize that fundamental improvements in obfuscation are also playing a foundational role in cybersecurity strategies today. There is an increased emphasis and demand for providers who play a key role in offering obfuscation-as-a-service.

We have observed several vendors implementing jailbreak and root detection strategies. Interest in these strategies will continue to grow as more people become aware of their significance. In some cases, root and jailbreak actions allow the unchallenged attack of the device and related resources. Security specialists should consider using improved root detection strategies at critical infrastructure points. Self-detection strategies should also be improved to ensure detection is not bypassed all together.

Organizations should consider both the strength and application of integrity controls, which can prevent malicious applications from being used as an attack platform.

We have also seen a significant focus and improvement to critical tamper-evident solutions. This indicates that MDM providers and consumers should consider adequate on-device tamper-evident detection mechanisms. Solutions should include a multi-faceted approach to detection. Avoid solutions that focus on one method and do not distribute and obfuscate anti-tamper code. Recommended anti-tampering solutions should include triggers when sensitive operations occur (such as application startup).

Application integrity has been a cornerstone to the success of enterprises today. We have seen application integrity validation make several significant advances. For example, Google SafetyNet provides a set of services to protect applications from security threats, including:

- Device tampering
- Bad URLs
- Potentially harmful apps
- Fake users

MDM vendors are now building on these types of frameworks to enable stringent integrity controls, thereby building trust in the mobility ecosystem. Organizations should consider both the strength and application of integrity controls, which can prevent malicious applications from being used as an attack platform.

In conclusion, we see the application layer (within the client vertical) as a perimeter boundary worthy of vendor and consumer focus. To some extent, this area presents a cat-and-mouse problem, with faceless attacks continuing apace against the legitimate businesses and users. There are many types of attacks focused on engineering at the code level. Therefore, there are multiple strategic goals for advancing security parameters in line with both perceived and realized threats:

- Continual security observation
- Learning from the mistakes of others (as we did from Equifax)
- Learning from vendors who are recognized as experts in their field
- Observing the evolving dynamics between consumers and attackers
- Building a long-term business strategy that enables every layer (down to the core technology) to detect, prevent, and respond to changing security needs

Trends To Watch in 2020

Deep Fakes Supporting Threat Activity

Deep fakes, a blended term coined by Reddit® users, refers to manipulated digital representations created by machine learning techniques. Specifically, the manipulation process uses a generative adversarial network (GAN) to generate and refine altered outputs.

In 2019, a persona named Katie Jones was discovered using a profile picture of an identity that did not exist. While the intent of this profile remains unclear, Katie posed as a researcher working for the CSIS (Center for Strategic and International Studies) and had several high-profile connections on LinkedIn[40, 41].

Furthermore, security researchers found a significant increase in the number of deep fake videos released within the first seven months of 2019. This increase was almost double the numbers reported in 2018[42]. There were also three real-world cases in which AI-generated audio spoofed CEO voices to trick victims into transferring large sums of money[43].

This is a trend that may increase in 2020, driven by factors like:

- Disinformation campaigns supporting geopolitical activity
- An increase in the availability and sophistication of tools needed to produce realistic outputs
- Deep fakes effectiveness as a social engineering tool

Organizations can prepare for this trend by enacting policies that require multi-stage validations before financial transactions are approved. Employers should consider regularly educating employees on what deep fake technology is, and how it can be used for fraud.

...security researchers found a significant increase in the number of deep fake videos released within the first seven months of 2019.

Increased Data Loss from Misconfigured Cloud Resources

BlackBerry Cylance examined publicly disclosed data breaches in 2019 and observed some interesting trends regarding data leakages caused by cloud misconfigurations. On average, there were at least three disclosures of exposures caused by unsecured databases and servers every month. These data exposures led to a total of over seven billion records being publicly exposed.

This number comes as no surprise as organizations continue to struggle with balancing their needs for continuous integration with safe deployment practices. Security measures are often implemented as an afterthought and may be driven by the pressures of regulatory compliance. On another end of the scale, some entities struggle with understanding their role in the shared responsibility model[44] where:

- The cloud service provider (CSP) is expected to secure the infrastructure supporting the underlying hardware and software depending on the model adopted
- The customer secures configurations related to consumed resources

Furthermore, security operations centers (SOCs) tend to get fatigued by non-contextualized high-volume alerts, leading to the possibility of potentially malicious activity slipping off the radar of the SOC analyst who tries to prioritize the alerts that require a response.

As more organizations look to prioritizing cloud investments, Gartner forecasts an increase in infrastructure-as-a-service (IaaS) offerings provided by public clouds, with a projected increase in revenues of $38.9 billion in 2019 to $49.1 billion in 2020[45]. Considering the projection and the ongoing challenges with improving the security of the cloud, we likewise expect to see an increase in data breaches caused by misconfigured assets. These losses will likely occur as a result of the inadequate efforts applied towards balancing security measures and managing software-defined infrastructure required to support the ever-evolving business needs.

On average, there were at least three disclosures of exposures caused by unsecured databases and servers every month. These data exposures led to a total of over seven billion records being publicly exposed.

Organizations can better prepare themselves by embracing a multi-faceted approach to cloud security by (but not limited to):

- Having automated configuration policies that drive continuous integration and reduce human errors
- Adopting threat-intelligence-driven awareness training for developers (focusing on active cloud security threats and best practices)
- Increasing visibility of the environment by leveraging network and user behavioral analytics that can spot anomalies in system configuration and user activity

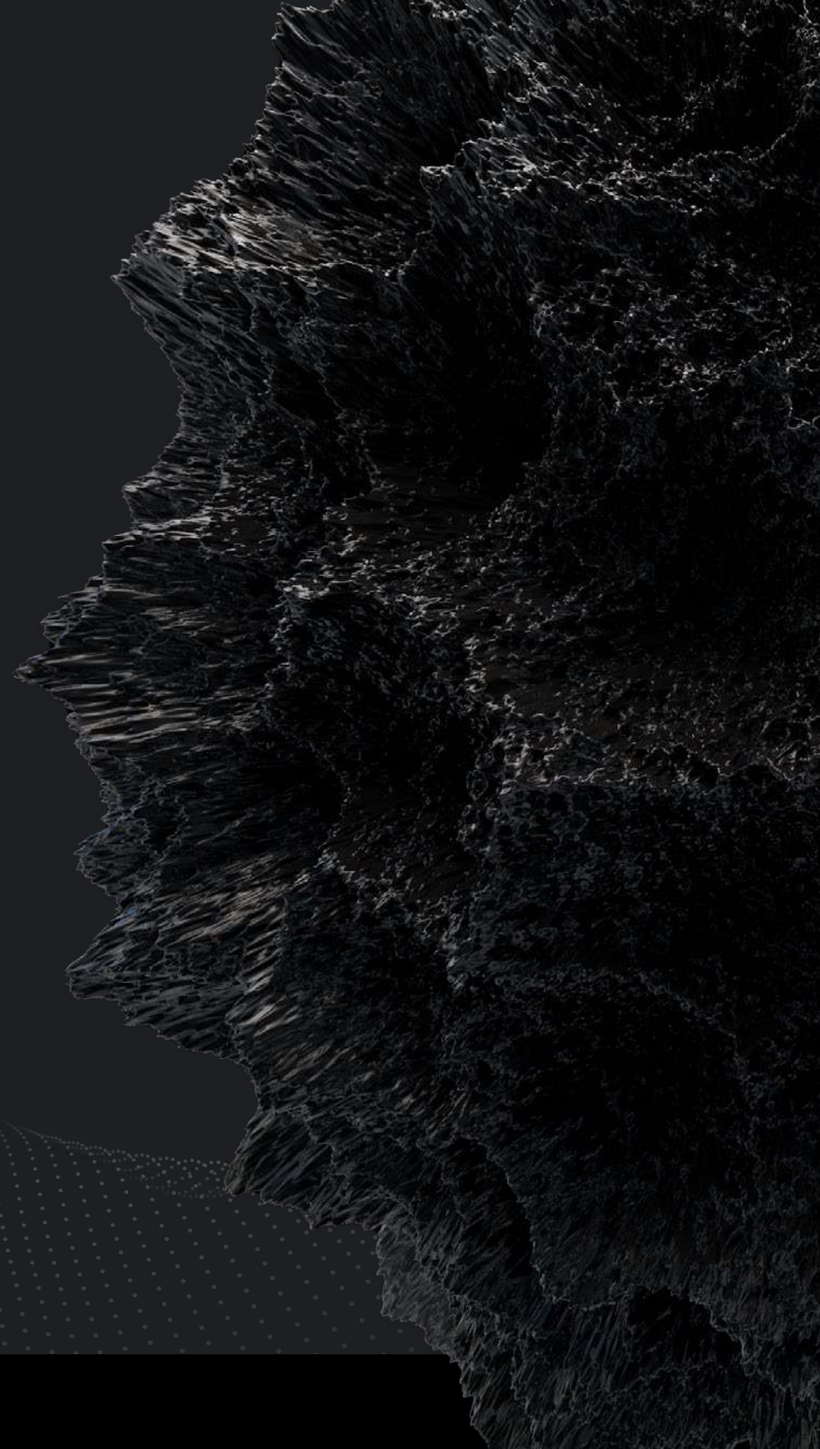
Vulnerable Vehicles in 2020

One reliable way to avoid cyber attacks is by holding nothing of value for threat actors. Automobiles have long been shielded from attackers simply by virtue of being low-value targets. As modern vehicles become more connected to various communication networks, this dynamic is changing. Unfortunately, vehicles are quickly becoming mobile-edge devices that utterly lack the security development enjoyed by other connected technology.

For example, many vehicle original equipment manufacturers (OEM) do not diligently protect their products. In fact, over 60% of OEMs test less than half of their hardware and software for vulnerabilities[46]. The long lifecycle of vehicles poses another challenge for security specialists. A private automobile may be used for seven to 15 years without receiving a single update to its various software or firmware components. This negligence gives threat actors ample time to figure out ways to compromise a vehicle.

The vendor supply chain required to create a vehicle also gives it an expansive attack surface. Each OEM manufacturer in the supply chain may introduce unknown vulnerabilities to the automobile. Things only get more complex when you consider the number of nations and companies that may be contributing to the end product.

...many vehicle original equipment manufacturers (OEM) do not diligently protect their products. In fact, over 60% of OEMs test less than half of their hardware and software for vulnerabilities.



Technology Raises Vehicle Profiles

Every time a technological system is added to a vehicle, it increases the attack surface by introducing more potential attack points. Consider the various on-board systems operating in vehicles today. There are network communication systems, sensor arrays (including LIDAR and RADAR), cameras, geolocation devices, and legacy systems that control engine and fuel performance. The amount of personal data being collected by vehicles is increasing as well. Modern automobiles may store or process personal information, performance metrics, geographic location information, and more.

Increasing the valuable data collected by vehicles without likewise improving their cybersecurity posture is bound to make automobiles tempting targets for threat actors. Vulnerabilities created by the supply chain, missing software and firmware updates, connected IoT devices, and after-market upgrades offer threat actors a generous attack surface. If steps to improve vehicle security are not taken soon, automobiles may well become the target of choice for attackers seeking easy victims.

Who Is Breaching Vehicles?

A recent report by Upstream[47] analyzed reported vehicle cyber attacks occurring between 2010 and 2018. Attacks were divided between White Hat actors who were performing legitimate research and malicious Black Hat actors. While attacks against vehicles generally increased over time, the most remarkable change came in 2018 when Black Hat attacks outnumbered White Hat attacks. When malicious attacks outnumber those performed by researchers, it can indicate threat actors have discovered a security-weak industry, and more will come.

Another class of breaches, outside of the White Hat/Black Hat paradigm, consist of unintentional information exposure by vehicle drivers. Consider rental cars used by several different drivers, each who sync their mobile devices with various vehicle systems. When the car passes to the next driver, these systems may still contain personal or private data from the last occupant.

The same situation can arise when someone sells their car. If an automobile provides a web portal or mobile app that tracks the vehicle's usage, the old owner may still have access. Used car buyers risk exposing data like geolocation information, garage door access codes, or various login credentials to the original vehicle owner. The car seller faces dangers as well, since old mobile Bluetooth® connections may have stored contact information, music, and frequently visited locations[48].

What Can Be Done?

Securing vehicles from cyber threats will be a monumental task. As noted, vulnerabilities arise from the vehicle supply chain, OEM process, IoT connections, and numerous other aspects of creating and operating an automobile. Modern vehicles are quickly becoming mobile computers with weak or no protection from cyber threats. There is no one-size-fits-all solution to address these multiple security vulnerabilities, but there are some important changes that can improve the situation, including:

- Designing with security in mind. Automobile manufacturers and OEM vendors should consider cybersecurity strategies starting at the first stage of design rather than adding it as an afterthought.
- Implementing data encryption on any vehicle system that stores vehicle or driver information.
- Developing comprehensive systems of trust to authenticate components as cyber secure.
- Actively searching for and responding to cyber events for the lifecycle of automobiles. They should leverage resources like the Automotive Information Sharing and Analysis Center (Auto-ISAC), which tracks, analyzes, and reports on vehicle cyber threats.
- Developing a system of updating vehicle software and firmware securely and remotely. Making security patches publicly available on a website is another option, but it opens the updates up to other risks. Attackers may reverse engineer publicly available updates. Customers may decide manually updating their vehicles is too troublesome and not make the updates.

The Road Ahead

Vehicles are becoming more technology-driven and interconnected as time progresses. To march toward an era of automated vehicles without first securing them against cyber attacks would be a tragic (and completely avoidable) mistake. It is vital that the automotive industry start implementing strong cybersecurity measures in their supply chains, manufacturing, and maintenance systems. Failing to properly secure vehicles may expose companies to penalties for breaching privacy laws, and more importantly, put drivers' lives at risk.

Predictions: Looking Ahead in 2020

While it is impossible to predict the future, we asked our experienced BlackBerry Cylance experts to share their thoughts on upcoming cybersecurity issues. Here are some of the issues our people will be keeping a close eye on as we enter the new year.

Crimeware-as-a-Service Increases Ransomware Attacks

Everything-as-a-service is a defining characteristic of our current corporate landscape. Perhaps it was inevitable that the concept eventually spread to the Internet's darkest corners as crimeware-as-a-service (CaaS). Today, skilled threat actors sell their cyber crime tools and services to networks of malicious actors. This enables the specialization and selling of criminal services in a manner mirroring that of the legitimate business world. The increasing sophistication of cyber criminals comes as no surprise given the growing profit potential of cyber attacks. Unfortunately, the trend of CaaS will likely accelerate in the coming year as connectivity and new technologies expand the attack surface. In particular, ransomware-as-a-service is likely to proliferate and continue to target organizations and government agencies. The legacy nature of some industry and government data systems means the RaaS wave is still cresting and unlikely to break in 2020.

AI-Based Technology Augments Employees and Simplifies Cybersecurity

Often, the publicity surrounding an AI product overstates its real-world value. However, recent AI innovations show hints of the transformational impact it can have. In 2020, AI will continue its ascent as companies grow tired of struggling with trying to manage an increasing number of security controls. Multiple security layers increase system complexity and often lead to well-intentioned, yet risky employee workarounds. To mitigate the risk of human error, AI will simplify security protocols and limit the impact of social engineering attacks. Over time, people will recognize AI-driven solutions are not an indictment of human capabilities, but a formidable addition to our distinctly human skillset.

Nuance Returns To The Facial Recognition Debate

Concerns about facial recognition are making headlines, with some cities instituting bans on its usage by police and other government agencies. These complete bans are symptomatic of broader privacy concerns but may represent an overreaction driven by the lack of nuance in conversations regarding the technology. As is typical, worst-and-best case scenarios are presented as facts, when the reality is likely found somewhere in the middle ground. While unfettered use of facial recognition can and is being used in some authoritarian countries, democratic nations are free to implement a more measured approach. As with previous innovative technologies like AI and autonomous vehicles, facial recognition's place in society should be decided through thoughtful and open dialogue.

Mobile Cybersecurity Becomes a Major Concern for Organizations

Recent research from BlackBerry Cylance found that state-sponsored APT groups are exploiting mobile devices with impunity to surveil:

- Specific people of interest
- Traditional foreign intelligence
- Economic espionage targets

The APT groups we observed operate from locations that include China, North Korea, and Iran. As public awareness of these attacks increases, expect to see significant investments from enterprises and governments in mobile threat detection and response.

Conclusion

Threat actors continued to innovate new strategies and tactics throughout 2019. Two of their notable achievements include using steganography techniques to obscure malicious payloads and improving their encryption schemes. Their work on updating legacy malware families paid off as well, as indicated by the top ranked cyber threats of 2019. Compromising MSPs and MSSPs allowed threat actors to easily distribute attacks against multiple organizations, a tactic likely to draw more attention in the future. Ransomware, which declined in 2018, also made a comeback.

The global attack surface is rapidly growing as embedded technology in vehicles, equipment, appliances, and other devices connect with business systems. Identity access management will play an increasingly vital role in cybersecurity strategies as more IoT devices connect with the Internet. Continuous user authentication, made possible through trained AI, offers organizations a way to protect themselves until manufacturers design their products with stronger security.

APTs and state-sponsored threat groups are exploiting vulnerabilities in mobile security. Combating these attacks will require a strong effort from MDM vendors, application engineers, and users who continue to jailbreak/root their phones. Mobile security vendors can proactively prevent some cybersecurity issues by learning from the mistakes made by other industries.

Deep fake technology may soon become a standard tool for threat actors committing fraud. As the technology becomes more accessible and easier to use, employees will need training on detecting and responding to deep fake threats. This type of threat may be imminent, as we can already observe deep fake identities being used to create social media profiles.

Businesses using cloud resources lost billions of records in 2019 due to misconfigured systems. This trend is likely to continue if organizations do not invest more into training and supporting their cloud security personnel. Reducing cloud-related breaches also requires CSPs and their customers to understand, implement, and enforce their part of the shared responsibility model.

There are many cybersecurity opportunities awaiting organizations and end-users in 2020. Vehicle manufacturers can dedicate themselves to improving supply chain security and delivering wireless updates. Mobile technology and IoT developers can improve their coding practices and threat detection capabilities. Users can exercise better security-awareness when connecting their IoT devices and by refraining from jailbreaking/rooting their phones.

BlackBerry Cylance remains dedicated to advancing the cause of cybersecurity for people and organizations worldwide. We will continue to train and deploy increasingly effective and advanced AI models, with the aim of securing technology, processes, and user identity. We will monitor the global threat landscape for emerging threats and seek to provide solutions where problems arise. To learn more about our plans for 2020 and beyond, visit us at www.cylance.com.

Acknowledgments

The BlackBerry Cylance 2020 Threat Report represents the collaborative efforts of our talented teams and individuals. In particular, we would like to recognize:

Adam Martin
Alan McCarthy
Andrew Crowley
Anuj Soni
Bob Slocum
Chris Greco
Claudiu Teodorescu
Dan Ballmer
David Rushmer
Dean Given
Douglas Kraus
Ebudo Osime
Eoin Healy
Eric Milam
Evelyn Ho
Garret Grajek
Geoff O'Rourke
Grant Courville
Ieva Rutkovska
Jessica Vose
John McGinnis
John Wood
Lydia McElligott
Lyndon Levett
Marisa Goodrich
Marta Janus
Masaki Kasuy
Patrick Huskey
Ryan Tracey
Shinsuke Honjo
Steve Barnes
T.J O'Leary
Tatsuya Hasegawa
Thom Ables
Tim Davies
Tom Bonner
William Savastano
Yi Zheng

Legal Disclaimer

The information contained in the BlackBerry Cylance 2020 Threat Report is intended for educational purposes only. BlackBerry Cylance does not guarantee or take responsibility for the accuracy, completeness, and reliability of any third-party statements or research referenced herein. The analysis expressed in this report reflects the current understanding of available information by our research analysts and may be subject to change as additional information is made known to us. Readers are responsible for exercising their own due diligence when applying this information to their private and professional lives. BlackBerry Cylance does not condone any malicious use or misuse of information presented in this report.

Endnotes

1 https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

2 https://www.zdnet.com/article/another-ransomware-strain-is-now-stealing-data-before-encrypting-it/

3 https://www.msspalert.com/cybersecurity-guests/sodinokibi-ransomware-still-very-relevant-for-mssps/

4 https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/

5 https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html

6 https://threatvector.cylance.com/en_us/home/threat-spotlight-ratsnif-new-network-vermin-from-oceanlotus.html

7 https://cyberarch.eu/red-teaming-adversary-simulation-toolkit/

8 https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html)

9 https://threatvector.cylance.com/en_us/home/malicious-payloads-hiding-beneath-the-wav.html

10 https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/#47d3e708617f

11 https://threatvector.cylance.com/en_us/home/flirting-with-ida-and-apt28.html

12 https://threatvector.cylance.com/en_us/home/inside-the-apt28-dll-backdoor-blitz.html

13 https://www.forbes.com/sites/forbestechcouncil/2018/02/20/how-ai-driven-systems-can-be-hacked/#2515d07179df

14 https://enterprise.verizon.com/resources/reports/dbir/

15 https://www.cyentia.com/ransomware-p1-payment-rate/

16 https://www.pcworld.com/article/3225407/ccleaner-downloads-infected-malware.html

17 https://securityboulevard.com/2019/09/taking-health-care-out-of-the-ransomware-hot-seat/

18 https://www.cpomagazine.com/cyber-security/atm-malware-and-jackpotting-attacks-could-be-making-a-return/

19 https://www.wired.com/story/russian-hackers-attack-ukraine/

20 https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/

21 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0322

22 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507

23 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0563

24 https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

25 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

26 https://www.helpnetsecurity.com/2019/06/04/quest-diagnostics-data-breach/

27 https://geminiadvisory.io/amca-largest-medical-breach/

28 https://krebsonsecurity.com/2019/06/collections-firm-behind-labcorp-quest-breaches-files-for-bankruptcy/

29 https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

30 https://www.verdict.co.uk/gearbest-data-breach/

31 https://en.wikipedia.org/wiki/2019_Bulgarian_revenue_agency_hack

32 https://en.gizchina.it/2019/03/gearbest-security-breach-official-statement/

33 https://en.wikipedia.org/wiki/2019_Bulgarian_revenue_agency_hack

34 https://thenextweb.com/security/2019/07/16/bulgaria-tax-agency-data-leak-hack/

35 https://www.zdnet.com/article/rogue-iot-devices-are-putting-your-network-at-risk-from-hackers/

36 https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/

37 https://hackernoon.com/why-do-most-people-ignore-two-factor-authentication-1bbc49671b8e

38 https://www.secureworldexpo.com/industry-news/2019-sotp-credentials-and-data-loss

39 https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

40 https://stratcomcoe.org/role-deepfakes-malign-influence-campaigns

41 https://www.welivesecurity.com/2019/10/31/deepfakes-seeing-isnt-believing/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+eset/blog+(ESET+Blog:+We+Live+Security)

42 https://www.bbc.com/news/technology-49961089

43 https://blog.malwarebytes.com/social-engineering/2019/11/deepfakes-and-linkedin-malign-interference-campaigns/

44 https://www.forbes.com/sites/forbestechcouncil/2019/07/05/how-to-prevent-security-breaches-resulting-from-cloud-misconfigurations/#34a085516c9e

45 https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g

46 https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf

47 https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/

48 https://www.wmcactionnews5.com/story/39022826/used-cars-increase-identity-theft-chances-bbb-finds/

BlackBerry | CYLANCE

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

MKTG 20-0049-20200211