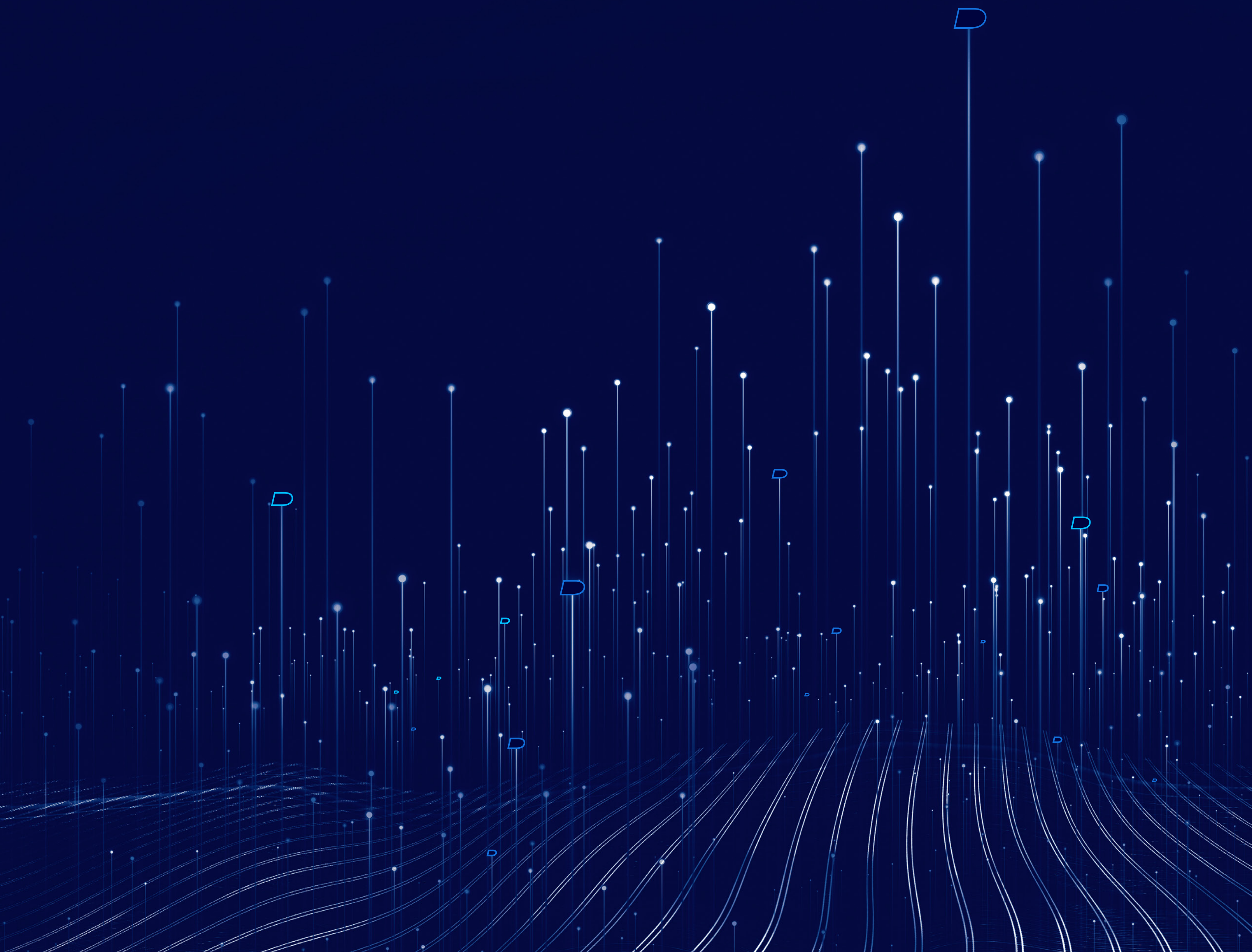
BlackBerry® Intelligent Security. Everywhere.

2022 THREAT REPORT



CONTENTS

INTRODUCTION

The BlackBerry 2022 Threat Report is not a simple retrospective of the cyberattacks of 2021. It is a high-level look at issues affecting cybersecurity across the globe, both directly and indirectly. It covers elements of critical infrastructure exploitation, adversarial artificial intelligence (AI), initial access brokers (IABs), critical event management (CEM), extended detection and response (XDR), and other issues shaping our current security environment.

This report examines 2021's major security events and how they may shape the cybersecurity landscape going forward.

This report covers topics confronting individuals and organizations around the world. As always, it represents our unique piece of the overall security puzzle. Our goal is to improve the global security posture by sharing our information, predictions, and experiences with everyone. To accomplish that, the report examines 2021's major security events and how they may shape the cybersecurity landscape going forward. It provides a deep dive into the cybersecurity issues we face today, and offers readers additional information and context to perform their own thoughtful analysis.

That said, readers expecting our annual breakdown of the top 10 malware attacks witnessed by BlackBerry over the past year will not be disappointed. Nor will those who look forward to our incident response (IR) year in review, annual cybersecurity legislative updates, and near-term predictions. Many of the sections our readers have come to enjoy from previous BlackBerry threat reports have returned. In addition, this year, we tackle supply chain attacks, dangerous new programming languages, security in the Metaverse, quantum computing, ransomware campaigns, and other relevant emerging topics.

The fluidity of modern cyberattacks can require organizations to frequently rethink their approach to cybersecurity and consider new options. They must constantly assess new technologies and approaches that can outperform legacy antivirus (AV) solutions, ranging from prevention-first AI to adopting Zero Trust architecture. Accordingly, the BlackBerry 2022 Threat Report offers suggestions on cybersecurity strategies and technologies that could have prevented the greatest security lapses of the past year.

We sincerely hope the information contained in this report will help protect users and keep organizations secure in 2022 and beyond.

EXECUTIVE SUMMARY

The most widely publicized cyber events of 2021 involved ransomware attacks on critical infrastructure and technology companies. The ransomware threat group REvil attacked Acer, JBS Foods, and others while DarkSide crippled Colonial Pipeline and Avaddon infiltrated AXA. In short, the scope and success of various threat groups last year–particularly against private sector companies considered part of national infrastructure–proved unsettling. Governments responded to the attacks, with G7 countries and NATO allies putting cybersecurity at the top of the public policy agenda. U.S. President Joe Biden issued an Executive Order on "Improving the Nation's Cybersecurity", while the Department of Justice established a Ransomware and Digital Extortion Task Force.

As the year wore on, a Microsoft® Exchange Server zero-day vulnerability spiraled into a crisis after the HAFNIUM group exploited the flaw. Other threat actors were quick to capitalize on the opportunity by reverse engineering the patch and targeting organizations worldwide. The swift proliferation of HAFNIUM-style attacks reinforced the importance of both organizations and individuals keeping software up to date. However, updating software as a reactive practice cannot save the initial victim of an attack–aka, the "sacrificial lamb". This has many organizations looking to alternative security approaches like the Zero Trust framework, XDR, and prevention-first AI.

At the end of 2020, a supply chain attack against SolarWinds made international headlines. The same style of attack reemerged in 2021, when Kaseya's VSA software was compromised, ultimately affecting over 1,000 businesses. Supply chain attacks often rely on the trust already established between providers and customers to propagate–offering another strong case for adopting a Zero Trust framework. While attacks on large organizations dominated the 2021 news cycle, small to medium-sized businesses (SMBs) also suffered countless attacks, both directly and through the supply chain. BlackBerry threat researchers discovered SMBs averaging 11 to 13 threats per device, a number much higher than enterprises.

Threat actors owe their success in 2021 to a variety of factors. Many have learned to adopt and mimic private sector capabilities by using service providers such as ransomware-as-a-service (RaaS), infrastructure-as-a-service (IaaS), and malware-as-a-service (Maas) to leverage malicious attacks. Others have created a layer of obfuscation between themselves and their targets by using IABs and impersonating other threat groups. New programming languages were exploited to some effect, with Go, D, Nim, and Rust making appearances across the threat landscape. Cobalt Strike remained active as a pivotal tool for command-and-control networks to proliferate malware and attacks.

300%

SMS phishing (smishing) attacks were up 300% in North America over the last year.

Progress was made on integrating security into connected vehicles with the International Organization for Standardization (ISO), the Society of Automotive Engineers (SAE), and the United Nations (UN) providing firm guidance to automakers. Mobile apps remained notoriously insecure. The vulnerable SHAREit app, which allowed remote code execution, was downloaded over one billion times. Recent studies found 63% of tested mobile apps use open-source code known to be vulnerable. Adding to smartphone users' woes, SMS phishing (smishing) attacks were up 300% in North America over the last year.

The cyberattacks of 2021 affected people at every level, from large organizations to individual cellphone owners. BlackBerry's internal reporting shows every industry is open to cyberattacks. The same cybersecurity issues that threaten non-profits are also risks for transportation companies, public organizations, utilities, healthcare organizations, financial institutions, etc. It reminded us that no one is safe. When it comes to cyberattacks, there is zero immunity. However, there are a number of cybersecurity innovations and approaches offering stronger protection to organizations. For example, organizations seeking effective new security measures should consider adopting a Zero Trust framework. They could also use prevention-first technology, migrate to an XDR platform, or engage a managed XDR team.

FEBRUARY

A water treatment plant in Oldsmar, Florida was compromised when an attacker attempted to poison the water supply.

CD Projekt Red was attacked by HelloKitty ransomware.

MARCH

Channel Nine in Australia had broadcasts disrupted by cyberattacks.

University of Highlands and Islands was attacked with Cobalt Strike.

CNA Insurance was attacked by Evil Corp.

Buffalo Public Schools in New York were attacked with ransomware.

Microsoft Exchange Servers were attacked by HAFNIUM.

APRIL

The Houston Rockets basketball team (NBA) was attacked by Babuk.

MAY

Colonial Pipeline was attacked by DarkSide.

AXA was attacked by Avaddon.

Brenntag (chemical distributor) was attacked by DarkSide.

Acer was attacked by REvil.

JBS Foods was attacked by REvil.

Ireland's Health Service Executive (HSE) was attacked by Conti.

JULY

Ransomware attacks were launched in Chile, Italy, Taiwan, and the U.K. by the LockBit threat group.

Kaseya suffered a supply chain attack from REvil.

NOVEMBER

The Robin Hood trading platform was breached and information on seven million user accounts was taken.

DECEMBER

Log4j vulnerability revealed and exploited by multiple threat actors.

These well-known attacks made national or international news due to their considerable scale, sophistication, ruthlessness, or ransom demands. However, their stories do not tell the true toll cyber crime took upon public and private organizations.

The cyberattacks of 2021 hit multiple industries, affected organizations of all sizes, and serve as stark reminders that no one is safe. There is zero immunity from dedicated threat actors, and anyone operating in the digital space may be targeted next. With malicious hacking attempts occurring every 39 seconds, an organization will exhaust itself relying on reactive security measures. Fortunately, prevention-first tools, predictive AI technologies, and Zero Trust frameworks can offer organizations an effective alternative to traditional cybersecurity solutions.

CYBER THREATS

COBALT STRIKE

No threat report would be complete without at least a passing mention of Cobalt Strike. This year, BlackBerry collated insights and trends from an internal dataset of over 7,000 Cobalt Strike Team Servers and 60,000 Beacons.

Tracking and monitoring Cobalt Strike Team Servers that are deployed in the wild can greatly assist the threat intelligence lifecycle. Doing so provides invaluable information for fine-tuning security solutions and aiding with incident investigations. A detailed breakdown of threat intelligence gained from analyzing Cobalt Strike can be found in The BlackBerry Threat Research and Intelligence Team's new eBook, *"Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence"*.

Our annual review of Cobalt Strike activity begins with some of the most interesting stats involving Team Server deployments.

For example, observe the top 10 autonomous system numbers (ASNs) and netblocks (ranges of consecutive IP addresses) responsible for hosting Cobalt Strike's immensely versatile Beacon payload. This reveals a fascinating trend: Threat actors are increasingly likely to use legitimate cloud providers for hosting. This allows the malware operators to conceal their traffic from monitoring systems, which makes the task of automated blocking trickier. Adding to detection difficulties, several large and reputable companies are found in the top 20 list of providers. Figure 1 shows the top 10 ASNs found hosting the Cobalt Strike Beacon:

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence

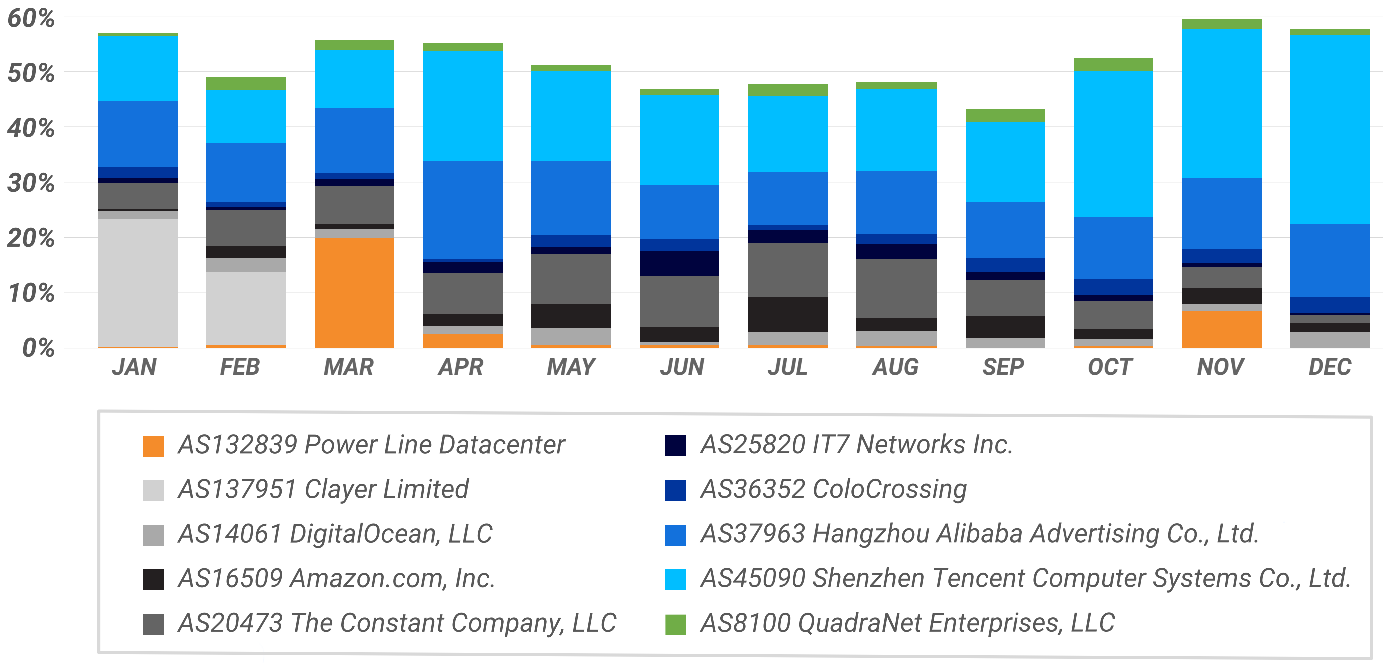


Figure 1 - Top 10 ASNs responsible for hosting the Cobalt Strike payload, Beacon

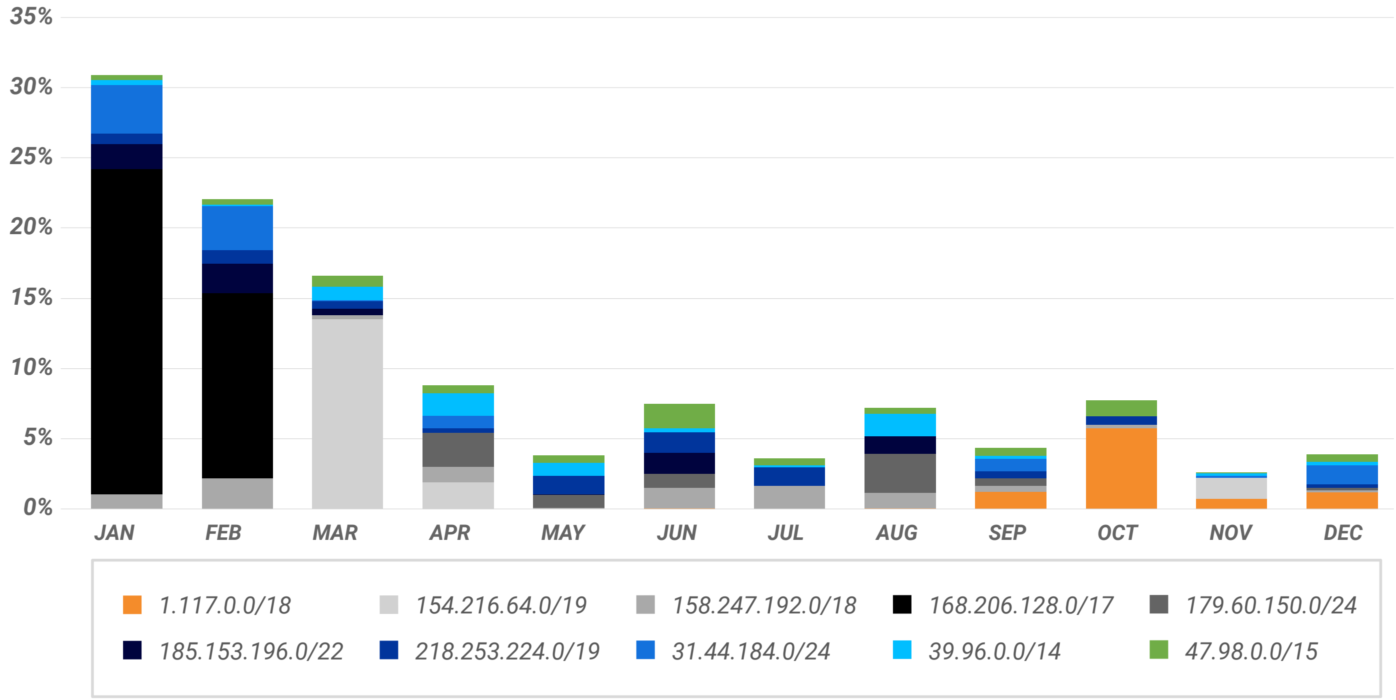


Figure 2 - Top 10 netblocks responsible for hosting Beacons

From a geographical perspective, the following countries are the top 10 used for hosting Beacon:

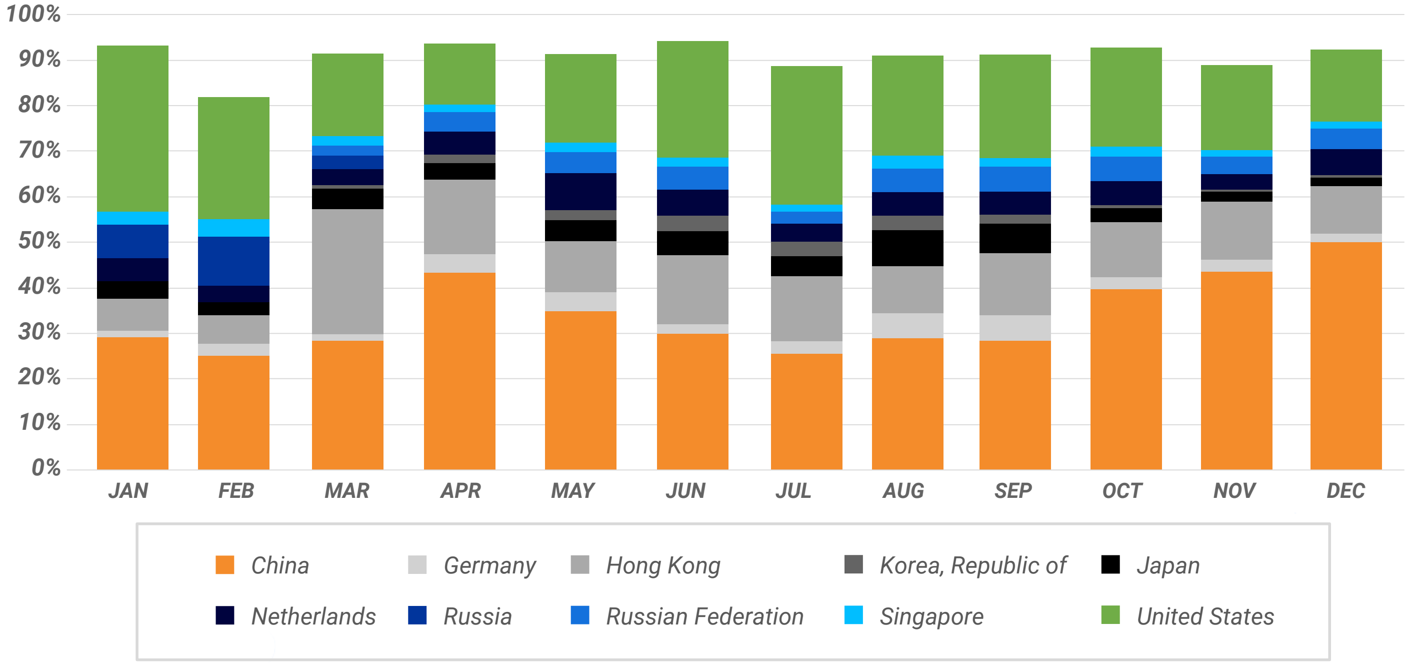


Figure 3 - Top 10 countries hosting Team Servers for Cobalt Strike

Ports 80, 443, and 8080 take top honors (seen in Figure 4) for serving up Beacon payloads from Team Servers. These ports are typically open in most environments, making them an obvious choice for routing command-and-control (C2) traffic.

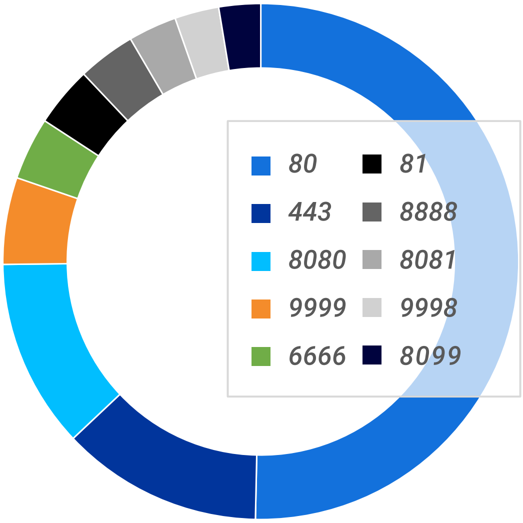


Figure 4 - Top 10 ports used for serving Beacon payloads

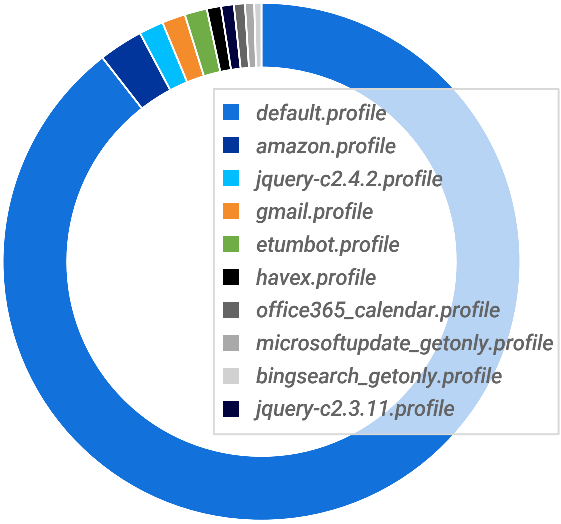


Figure 5 - Top 10 Malleable profiles used by Cobalt Strike Beacon

Cobalt Strike Beacons are highly configurable through their use of Malleable C2 profiles, which specify how a Beacon acts and looks in the target environment. These profiles also specify what parameters are used within their communication protocol and the method that Beacon uses to inject into other processes. The top 10 Malleable profiles observed throughout 2021 are shown in Figure 5.

Using Malleable C2 Profiles, Cobalt Strike Beacon can be configured to perform a technique called domain fronting. This is used to route HTTPS traffic via trusted third-party content delivery networks. The top 10 hosts used for domain fronting in 2021 were:

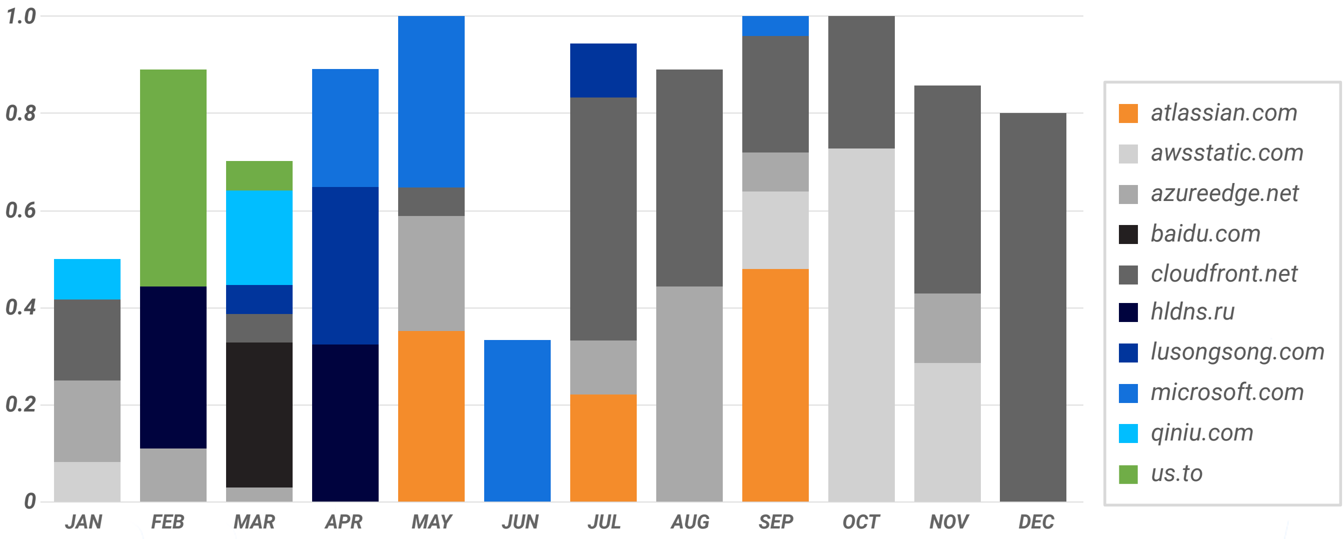


Figure 6 - Top 10 hosts used by Cobalt Strike Beacon for domain fronting and masquerading

Cobalt Strike Beacon can be configured to use DNS redirectors to forward C2 traffic to a Team Server. Figure 7 shows the top 10 DNS redirector Internet Protocols (IPs) from 2021.

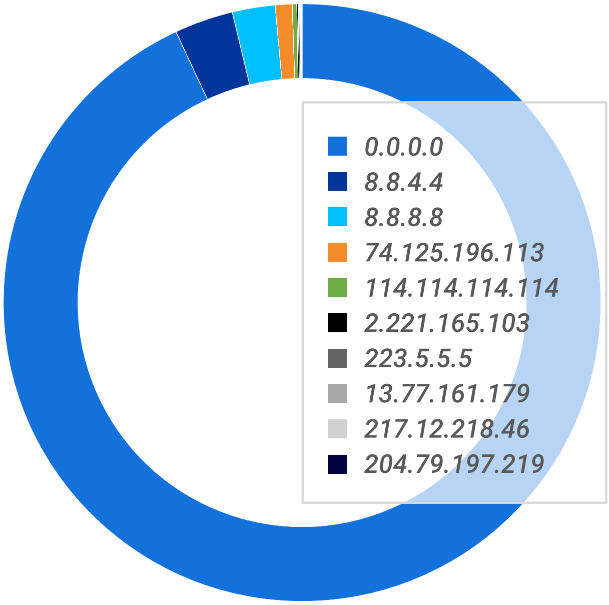


Figure 7 - Top 10 DNS redirector IPs used by Cobalt Strike

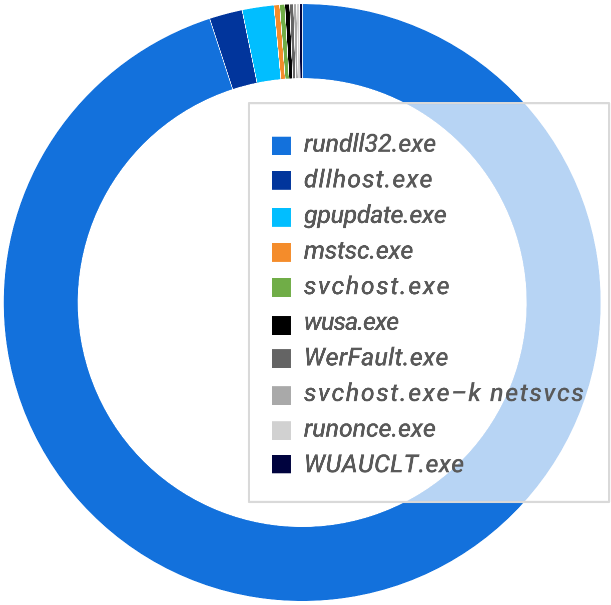


Figure 8 - Spawned processes created for Cobalt Strike injections

Cobalt Strike Beacon spawns processes and then injects dynamic-link library payloads into them. These processes can be configured to work on different architectures (x86/x64) through the SPAWNTO option. The default process, and most popular choice, is rundll32.exe. Refer to Figure 8.

In addition to the Secure Sockets Layer (SSL) certificates deployed on the Team Server, Beacons are also bundled with an additional SSL public key. This is part of a public/private key pair that is generated on the server whenever someone installs Cobalt Strike. The public key is subsequently embedded in all Beacons generated on the same server and used for C2 check-ins. It is important to note that this key pair is entirely different from the SSL key pair used for the HTTPS certificate on the Team Server.

Unlike watermarks, the SSL public key stored within a Beacon's configuration offers a fantastic means of clustering Beacons. It is virtually guaranteed that the keys are unique per Team Server installation, but are often reused, for example via virtual machine redeployments. In other instances, threat actors will use a single Team Server to configure payloads for deployment from other servers within their control. This makes spotting, tracking, and monitoring their infrastructure considerably easier.

The top 10 SSL public keys mostly belong to leaked builds of Cobalt Strike Team Server:

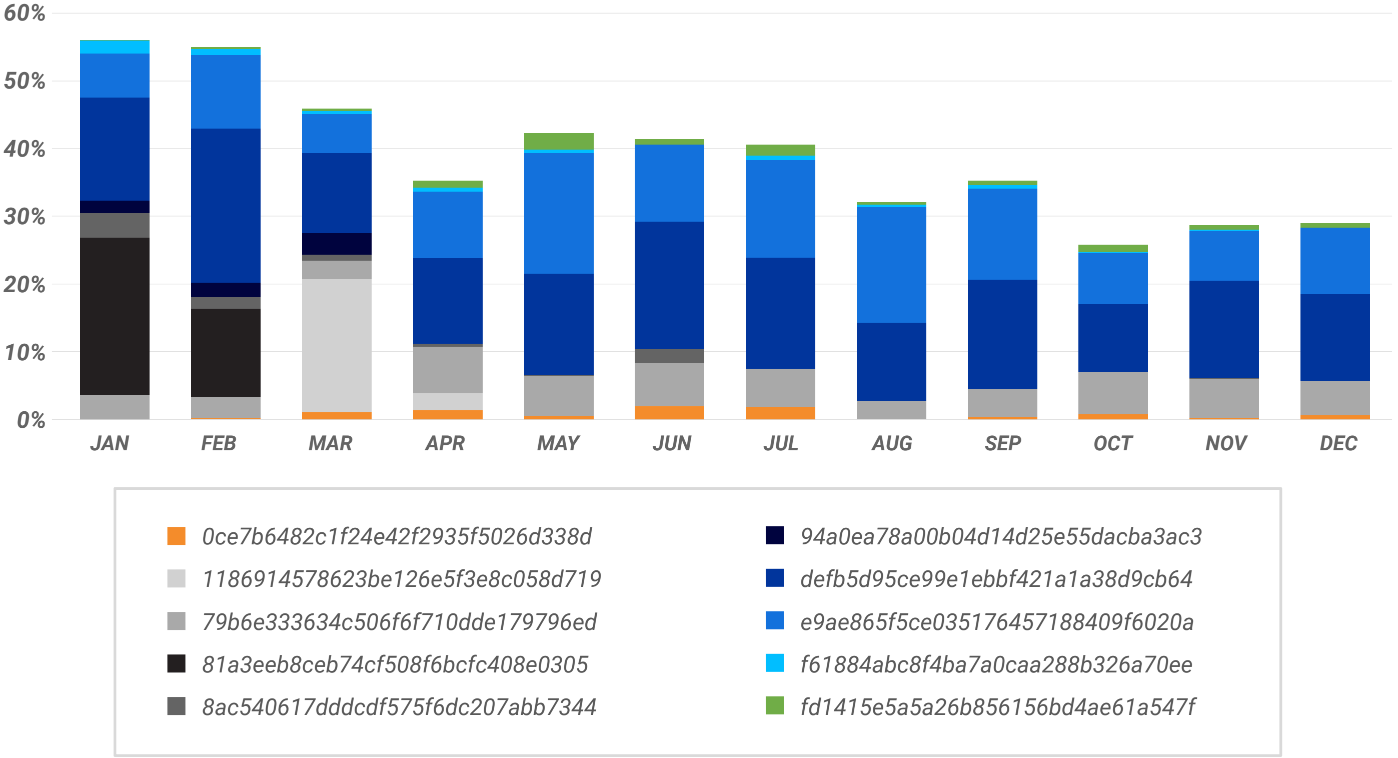


Figure 9 - The top 10 public keys of Cobalt Strike Team Servers

Finally, it is possible to track Team Server builds via a configuration setting called PROCINJ_STUB. It contains a message-digest algorithm (MD5) hash of the Cobalt Strike Java archive (cobaltstrike[.]jar). This archive contains the server-side component that provides the Team Server operators with a graphical user interface to generate, operate, deploy, and control Beacon payloads.

The MD5 hash of the cobaltstrike.jar package allows us to determine several things. By correlating it with its corresponding Java archive commonly found in online malware repositories such as VirusTotal, we discover:

- The exact version of the Team Server used
- Whether the Team Server in operation is a leaked, cracked, or a trial version
- If the Team Server is a private, licensed version

Even if the Java archive is unavailable to assist with version identification, it is still an extremely valuable clustering mechanism. This is especially true in the case of private and customized builds.

The top 10 Team Server builds in 2021 (based on the PROCINJ_STUB hash value) were as follows:

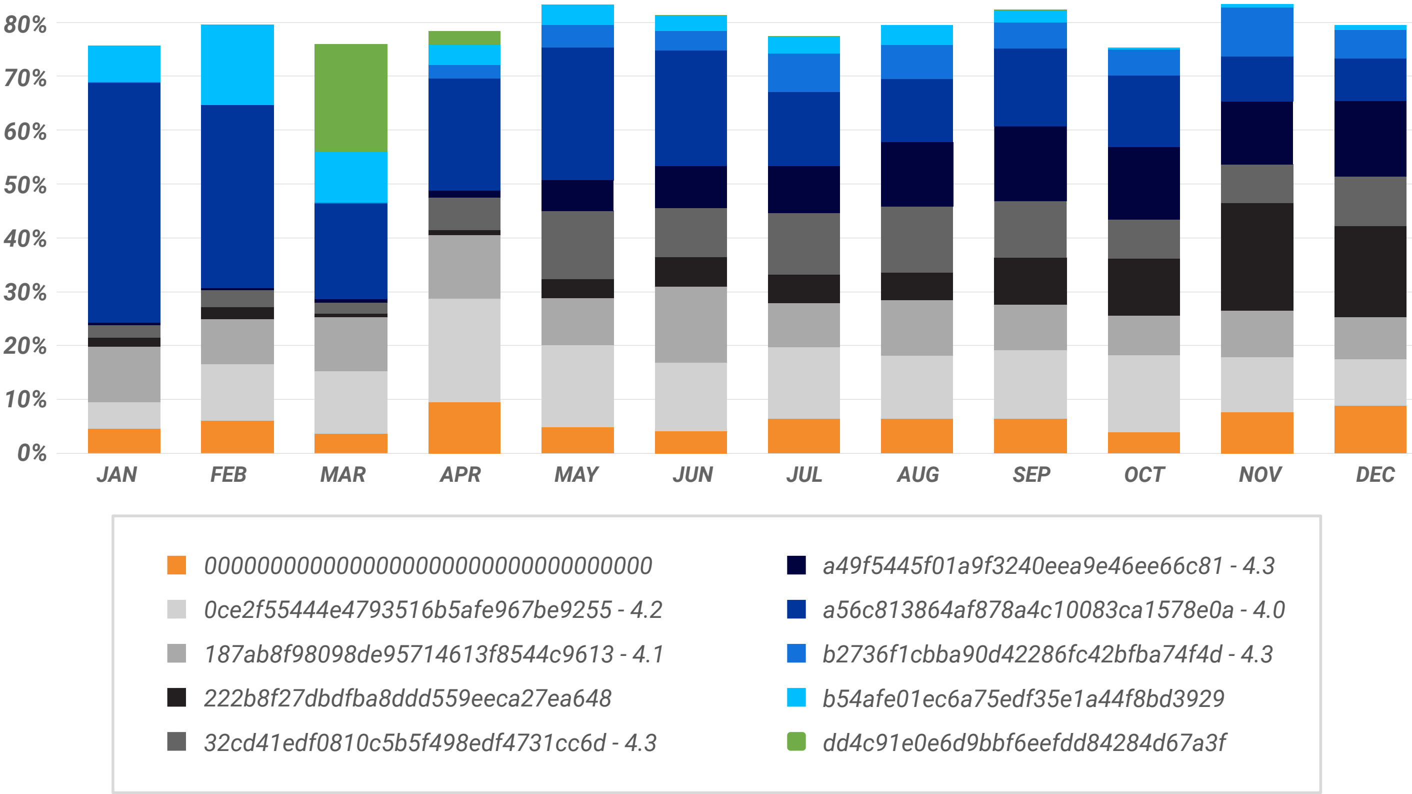


Figure 10 - The top 10 Team Server builds in 2021

In addition to our research, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) released a report on Cobalt Strike Beacon in May 2021. Their document includes a list of recommendations users and organizations can follow to minimize exposure to this threat.

SUPPLY CHAIN ATTACKS

Supply chain attacks are not a recent concept. However, the software supply chain has been increasingly used as an attack vector in recent years. Why is this the case? For one, the potential impact and spread of a supply chain attack can be far greater than that of targeting an individual victim. The potential for damage varies depending on the customer base of the product. The relation between producer and consumers is essentially one-to-many, with a single point of failure. This means that the larger the customer base, the larger the potential attack base, too.

Threat actors know exploiting the trust people place in the integrity and security of their supply chain is easier than compromising fortified targets. Adversaries typically look for the path of least resistance; the supply chain represents the latest evolution in their tradecraft.

WHAT IS A SUPPLY CHAIN ATTACK?

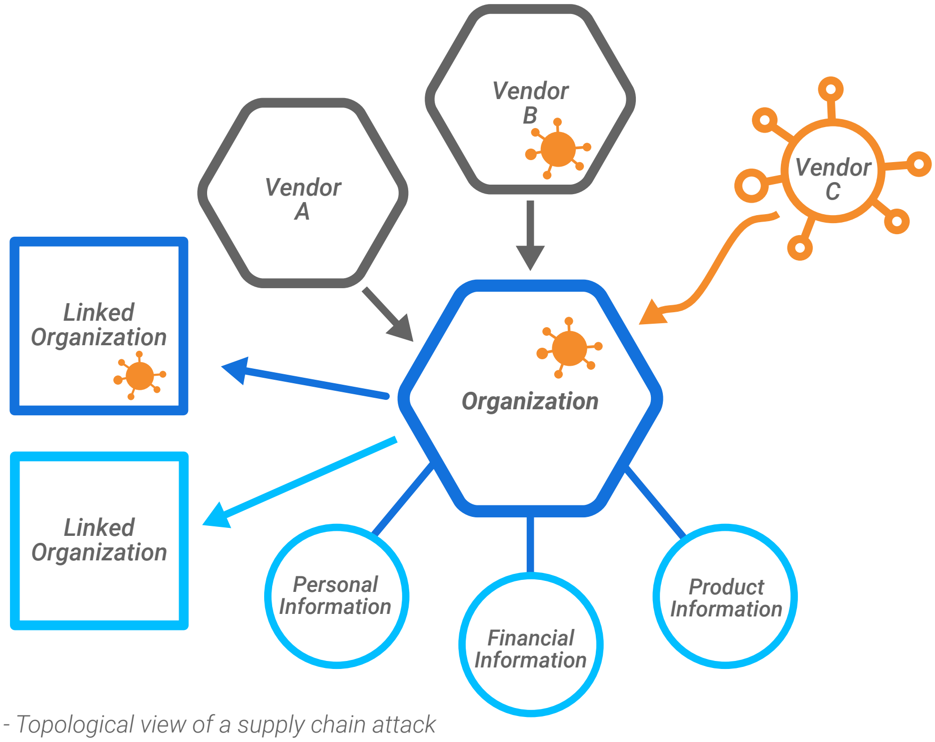


Figure 11 - Topological view of a supply chain attack

To better understand supply chain attacks, see the topological representation of company interactions in Figure 11. Supply chain attacks occur when an organization relies on a third party for part of their product development, hardware, software, or other services.

The U.S. Department of Defense defines a supply chain risk as one where the adversary may "sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such systems".

Take another look at Figure 11. The central organization depends on Vendors A through C for different requirements. All is well until Vendor C is breached and a foothold is established in their environment. Vendor C's product development lifecycle is compromised and a malicious component included in their product.

The product, in its compromised state, is distributed to the organization where it serves as a foothold for malicious adversaries to infiltrate and compromise.

Once attackers are inside, all information they can access may be exfiltrated, including product information, financial information, and personal information. If the compromised organization has a weak security posture, further propagation of this attack may spread to linked organizations and their customer base.

POTENTIAL IMPACT

Depending on the size of the compromised organization's customer base, the impact of a supply chain attack can be huge.

Determining which customers have been affected, and to what extent, can prove difficult. As a result, as soon as a breach has been identified, customers should be notified so they can begin their own remediation efforts. Organizations should plan for the worst in these scenarios: assume that their customers have been breached and the danger of further reputational damage is imminent. The longer it takes for threat disclosure and response, the greater the risk that attackers gain a persistent foothold in customer environments.

There is also the possibility of a knock-on effect, where if the breach is not contained, other linked organizations can be affected too.

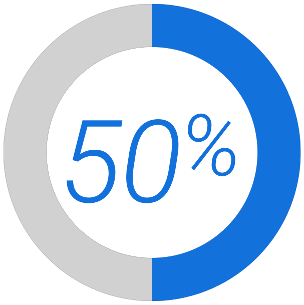
RECENT SUPPLY CHAIN ATTACKS

Supply chain attacks sound dangerous, and they are. The prospect of a trusted source being the initial point of compromise is one that many prefer to believe will not happen, but it does. Some examples of historical software supply chain attacks include:

- **The NotPetya ransomware attacks in 2017.** Attackers compromised the Ukrainian tax software MEDoc and caused billions in damages to pharmaceutical giants.
- **The SolarWinds breach in 2020.** The Orion IT Management and monitoring software was compromised and pushed out to a number of high-profile entities.
- **Kaseya in 2021.** A zero-day exploit allowed attackers to deploy an update to every customer running their Virtual System/Server Administration (VSA) software. The update was pure ransomware, and it encrypted a large portion of Kaseya's VSA customer base.

The European Union Agency for Cybersecurity recently published a report studying 24 supply chain attacks from January 2020 to July 2021. The report revealed some stark statistics:

- Suppliers either did not know or did not report how they were compromised in 66% of supply chain attacks.
- Advanced persistent threat (APT) groups were credited with carrying out 50% of supply chain attacks.
- Exploiting trust in the supplier accounted for nearly 62% of attacks on customers.



In 24 recent supply chain attacks, advanced persistent threat (APT) groups were credited with carrying out 50% of them.

HOW DO SUPPLY CHAIN ATTACKS EVADE DETECTION?

At its core, a supply chain attack is an abuse of trust. A trusted supplier or vendor is assumed to maintain rigorous security standards. For example, an analyst responding to alerts showing C2 network traffic may have a bias based on their level of trust in an application. They may see a particular domain of interest in the network traffic, or its SSL certificates. However, as it comes from a trusted application, the threat indicator is assumed to be legitimate.

This bias serves to highlight the benefits of a Zero Trust approach, and how implicit trust can be a major vulnerability. It also reinforces the need to investigate and more thoroughly vet third-party applications. A chain is only as strong as its weakest link: If one part breaks, the whole system can fail.

HOW CAN BETTER PROTECTION BE ACHIEVED?

Many security issues can be addressed through taking a holistic approach to security and adopting the principles of Zero Trust. All threat vectors need to be covered, including sources usually trusted as benign.

An organization’s product security incident response team (PSIRT) is likewise a key component of improving its security posture. For example, a PSIRT can work closely with other teams, communicating valuable security insights to them throughout the software development lifecycle (SDLC). As its inclusion in the SDLC continues, the PSIRT will reach new levels of maturity and become more proactive. This helps ensure that the products and build processes are as secure as possible. The risk of a supply chain attack is reduced when the lines of communication between teams are well-formed.

For security analysts, it is important to reduce one’s natural bias in favor of trusted applications and services. While certificate signing, provenance, build tooling, and other steps that can be taken have security value, it is imperative for security operations (SecOps) teams to always remain skeptical. Rapid disclosure and containment of a breach is likewise critical for protecting organizations and the customers that rely on their products or services.

Many security issues can be addressed through taking a holistic approach to security and adopting the principles of Zero Trust.

LOG4J/LOG4SHELL EXPLOITS

Log4j is an open-source logging package used by countless applications and major frameworks, including Apache Struts2. Toward the end of 2021, a vulnerability in this software component that attackers can exploit by sending specially crafted text was discovered. Attacks targeting this vulnerability, also called Log4Shell exploits, allow threat actors to fetch code from a remote server and perform remote code execution (RCE). Since Log4j is not malware, it is not susceptible to cybersecurity measures and tools exclusively focused on detecting malicious code.

The Log4j vulnerability, first reported by Chen Zhaojun on November 24, is further described in CVE-2021-44228. On December 10, the vulnerability was publicly disclosed in the National Vulnerability Database, maintained by the National Institute of Standards and Technology (NIST). Revelation of this vulnerability led to a swift increase in attacks that quickly numbered millions per hour.

The Log4j vulnerability is particularly troublesome, as it is difficult for organizations to know which applications and services are at risk. A standalone application using Log4j may be easy to identify, but what about cases where the package is six levels deep in the dependency chain? The widespread use of Log4j paired with the complex nature of software dependencies indicate this vulnerability will present a threat for years to come.

While anti-malware measures are not useful for detecting and remediating the Log4j vulnerability, other cybersecurity strategies can reduce an organization's exposure to this risk. For example, adopting a Zero Trust framework can limit an attacker's use of the vulnerability by restricting the access of exploited processes. Zero Trust environments can further reduce risks by enforcing least-privilege access polices throughout the environment. Also, as many cyberattacks rely on delivering a malicious payload, anti-malware tooling may ultimately prevent file-based attacks resulting from the exploit.

OLD DOGS NEW TRICKS–OBSCURE PROGRAMMING LANGUAGES

The BlackBerry Threat Research and Intelligence Team has been tracking and monitoring the threat landscape for the appearance of four obscure programming languages:

- **Go**
- **Nim**
- **D**
- **Rust**

These languages are currently being observed to track their use and adoption by threat actors. Selection of these languages was partially driven by an uptick in their misuse for malicious activities. Another factor is their increasing role in malware families authored and uncovered within the overall threat landscape.

Generally, new programming languages are often developed to improve on various aspects or shortfalls in current ones. This, consequently, also makes them an attractive option for abuse by threat actors. New languages can be used as a wrapper or loader for an existing malware family, to rewrite existing malware, or develop brand-new malware. This trend has been seen in the past with the use of VB6 and Delphi to develop wrappers for then-current malware.

Old Dogs, New Tricks: Attackers adopt exotic programming languages

More recently, in March 2021, the BazarLoader malware family was rewritten in the Nim programming language and dubbed Nimzaloader. Several months later, in May, RustyBeur appeared, which was a variant of the Buer-loader malware rewritten in Rust.

From a threat actor's perspective, the use of exotic programming languages provides many advantages. These include:

- Enhanced performance
- Lack of available analysis tooling
- Analysts' unfamiliarity with their composition
- Increased ability to thwart signature-based antivirus detection

It could be argued that these languages act as a layer of obfuscation. Their newness and the lack of available analysis tooling means they can look rather alien to inexperienced researchers.

BlackBerry observed these languages being used in the development of an increasing number of droppers and loaders. They were used as new, first-stage pieces of malware designed to drop/decode, load, and deploy commonly seen commodity malware families. Threats currently using these new languages include the Remcos and NanoCore remote access trojans and Cobalt Strike Beacons.

Many of these languages can also be cross compiled to target multiple operating systems. This powerful feature has been abused relentlessly by threat actors. Specifically, the Russian-based APT29 group and their Wellmess malware, which was written in Go and compiled to target both Windows® and Linux® operating systems. A further example of this was the appearance of ElectroRAT malware in January 2021. It was also developed in Go and then cross-compiled to target all major operating systems–Windows, macOS®, and Linux.

Nim and Go have been used in different parts of the same attack chain to enhance the attacker's detection evasion capability. For example, threat group APT28 leveraged a Nim-based downloader to retrieve a Go-based payload in its Zebrocy malware.

The benefits and popularity of these languages have resulted in an uptick in their adoption by the security community. Due to their offensive advantages, they are of particular use in the development of Red Team tooling. In late 2020, FireEye disclosed that a threat actor had gained unauthorized access to some of its Red Team tools. As a countermeasure, they released a statement along with a GitHub repository comprised of various detection signatures to help identify the stolen tools. Within this repository, FireEye revealed that its Red Team had been employing a combination of publicly available, modified tools and in-house custom tools. Some of these Red Team tools were written in DLang, Rust, and Go.

Malicious binaries authored in these languages currently constitute a small portion of those being utilized by threat actors. However, their use in cyberattacks is a trend that is likely to increase in the coming decade.

INITIAL ACCESS BROKERS

The BlackBerry Threat Research and Intelligence Team has been tracking a previously undocumented IAB that BlackBerry has dubbed Zebra2104. Our investigation uncovered a mass of interlinking malicious infrastructure that showed an unusual connection between several seemingly unrelated threat groups.

The first revelation came in April 2021, with the discovery of a Cobalt Strike Beacon-serving domain that also doubled as a C2 server. By following a trail of network breadcrumbs, we found numerous overlaps with previously documented malspam infrastructure. This infrastructure served various payloads, including Dridex, over the past year. It was also associated with a phishing campaign targeting Australian-based entities, both private and government.

Further research uncovered additional links to a MountLocker ransomware intrusion in March 2021, via some shared domain registrant information for the domain supercombinating[.]com. More digging revealed another related domain, mentiononecommon[.]com, that resolved to the same IP in an alternating fashion as supercombinating[.]com over several months. Open-source intelligence confirmed that this domain had previously been tagged as a StrongPity C2 server in June 2020.

Promethium (aka, StrongPity) is an APT group that has been active since 2012. The group typically uses watering hole attacks as a mechanism to deliver trojanized versions of commonly used utilities. WinRAR, CCleaner, and Internet Download Manager are a few of the utilities that have been maliciously repurposed to distribute the group's malware.

While seeking further evidence to prove these two disparate groups cooperated in some capacity, our researchers came across another interesting find. A tweet from The DFIR Report in August 2020 stated that additional ransomware was being distributed from supercombinating[.]com. This time, the malware belonged to Phobos family, not MountLocker.

This raised more questions regarding the connection between these threat groups. Were they related or just sharing the same infrastructure? Had we uncovered some sort of distribution system? Was an IAB the missing link binding these groups together?

An IAB is an entity whose aim is to gain unlawful access into an organization's network. They establish a foothold, usually by installing a backdoor, then sell their ill-gotten access on the dark web. Pricing for their services may range from as low as $25 USD up to thousands of dollars. After receiving access, buyers will often deploy malware within the victim environment.

Although different ransomware groups may share infrastructure, our research during this investigation indicates this was not the case. In numerous instances, a delay was seen between the initial compromise employing Cobalt Strike and the distribution of additional ransomware. These factors led us to infer that the overlapping infrastructure is not that of MountLocker, Phobos, or Promethium. Rather, it belongs to a fourth group that has acted as a middleman to facilitate the operations of the first three. This arrangement was achieved by either providing/selling initial access, or by the provision of IaaS.

Additionally, the domains found throughout this overlapping infrastructure used to resolve to IPs were provided by a singular Bulgarian ASN belonging to Neterra LTD.

The fact that all the IPs were clustered together on the same ASN adds credence to the theory that they are owned by one threat group. This group also likely laid the groundwork for the other threat actors to access networks breached by the IAB.

CHACHI

The BlackBerry Threat Research and Intelligence Team has been tracking a previously unnamed Golang remote access trojan (RAT) targeting Windows systems. We've dubbed this RAT ChaChi. This RAT has been used by operators of the PYSA (aka, Mespinoza) ransomware as part of their toolset to attack victims globally. Recently, the malware has been targeting education organizations.

ChaChi has been observed in the wild since the first half of 2020 without receiving much attention from the cybersecurity industry. The first known variant of ChaChi was used in attacks on the networks of local government authorities in France. It was listed as an indicator of compromise (IOC) in a publication by CERT France at the time of the attacks.

Since then, BlackBerry analysts have observed more refined versions of ChaChi being deployed by the PYSA ransomware operators. Their campaign focused on educational institutions across the U.S., which is evident by a recent increase in activity, as reported by the FBI.

PYSA Loves ChaChi: a New GoLang RAT

TYPES OF ATTACKS

RANSOMWARE

REVIL

REvil was first advertised on Russian language cyber crime forums and is associated with the threat actor Unknown (aka, UNKN).

The FBI named the Russia-affiliated RaaS group REvil (aka, Sodin or Sodinokibi) as the culprits behind attacks on the world's largest meat supplier, JBS. These attacks threatened the global food supply chain and serve as a reminder of the vulnerable state of critical infrastructure worldwide.

The malware acts as a RaaS, and became prolific after another RaaS group, GandCrab, shut down its operations. Security researchers have identified many similarities and code reuse between REvil and GandCrab. REvil was first advertised on Russian language cyber crime forums and is associated with the threat actor Unknown (aka, UNKN).

REvil is most famously associated with recent attacks on the travel insurance industry, Acer, and computer manufacturers. Acting as a RaaS, REvil relies on affiliates or partners to perform its attacks. The REvil developers receive a percentage of all proceeds from ransom payments. Because the ransomware is distributed by different entities, the initial infection vector can vary. Typically, infection is achieved via phishing campaigns, brute force attacks to compromise remote desktop protocol (RDP), or through software vulnerabilities. REvil is also known to be distributed by other malware, such as IcedID.

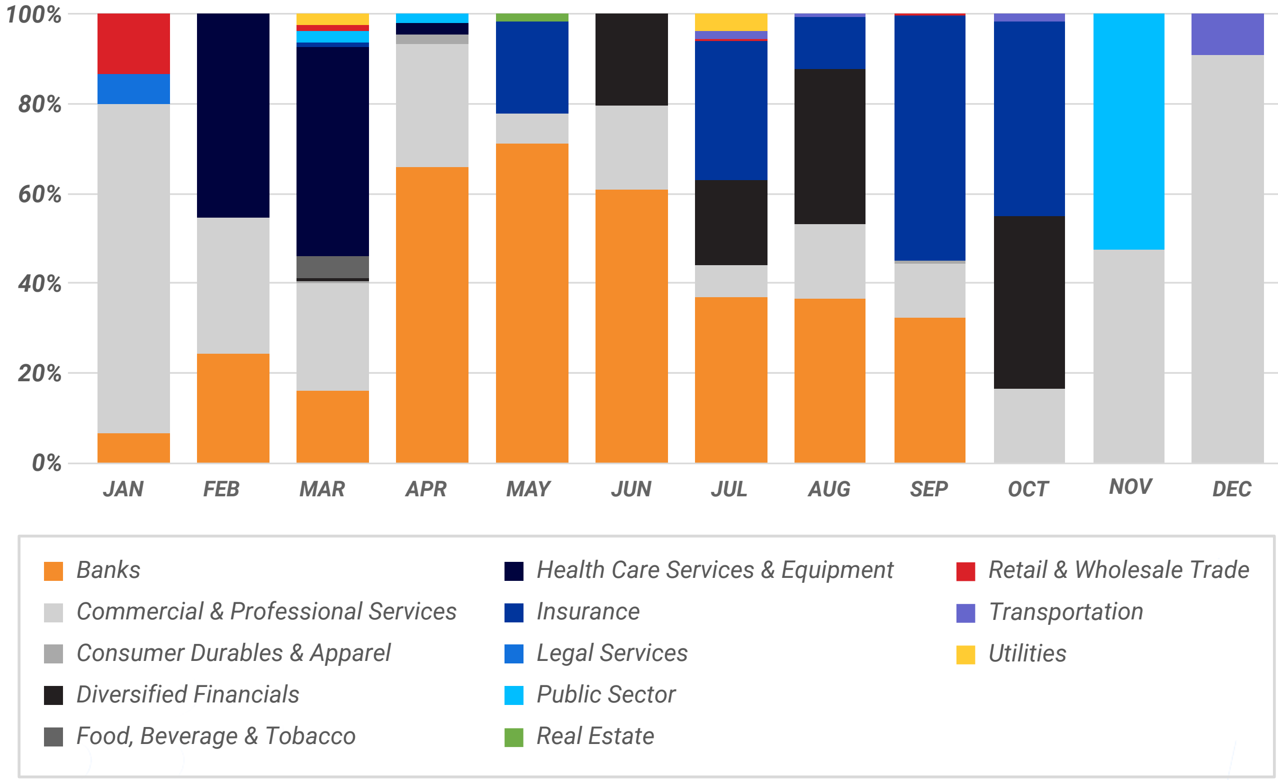


Figure 12 - Industries attacked by REvil, 2021

DARKSIDE

The DarkSide ransomware variant first appeared in mid-2020. It is distributed as a RaaS that is used to conduct targeted attacks. DarkSide targets machines running both Windows and Linux. It made headlines in 2021 with its attack on the U.S. fuel pipeline system, Colonial Pipeline.

DarkSide uses a double extortion scheme, where data is both encrypted locally and exfiltrated before the ransom demand is made. If the victim refuses to pay, their data is published to a site located on the dark web.

After the Colonial Pipeline attack, the DarkSide Group stated that it did not intend to affect hospitals or medical facilities, education, not-for-profit, or government systems. The DarkSide Group was reportedly shut down in May 2021, possibly by the U.S. military's Cyber Command.

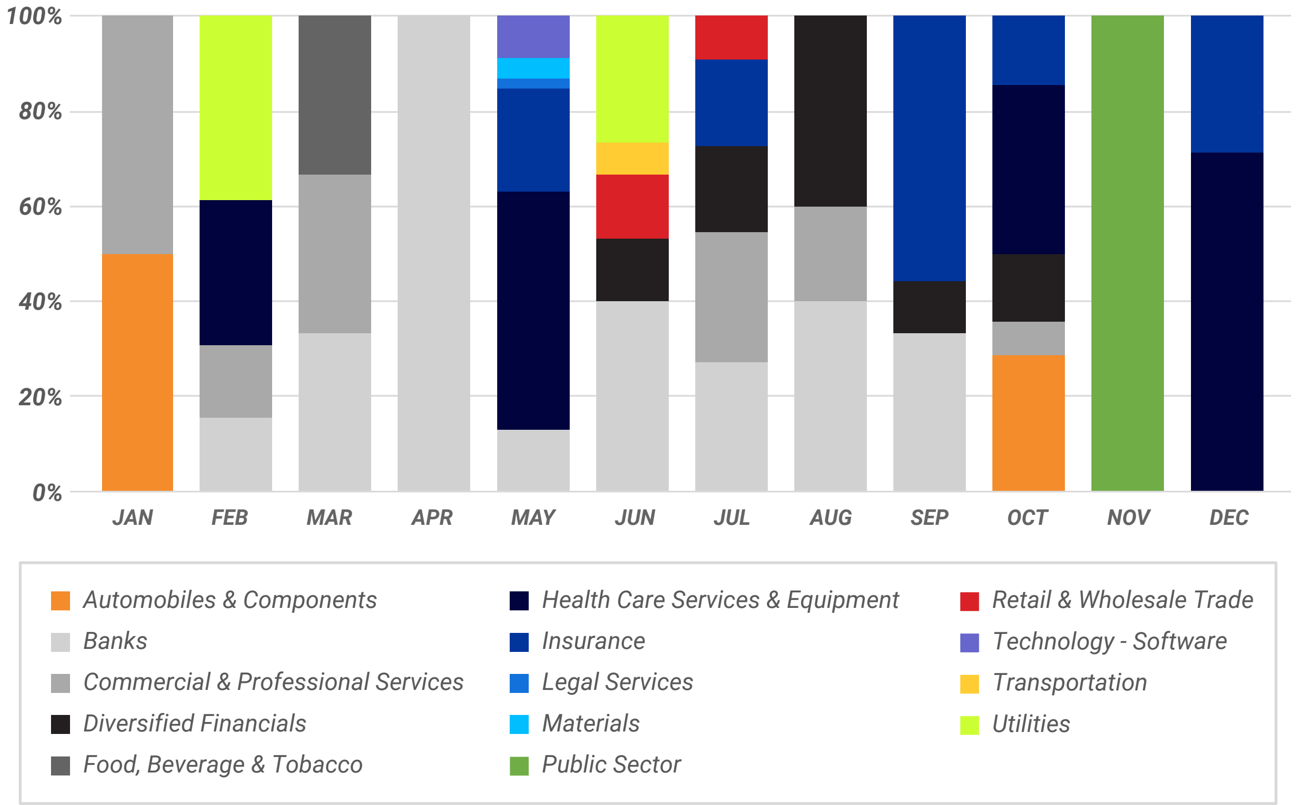


Figure 13 - Industries attacked by DarkSide, 2021

Many analysts regard Conti as the ransomware that replaced Ryuk, and consider it to be one of the most troubling ransomware threats in the wild.

CONTI

Conti ransomware made international headlines after its initial discovery in mid-2020. BlackBerry researchers have observed Conti attacks against manufacturing, insurance, and healthcare service providers across Japan, Europe, and the U.S.

Conti is offered as a RaaS, which is a popular way for threat actors to distribute and sell their malicious services via underground forums. As this threat is offered as a saleable service, it is customizable and thus its functionality can be altered from one infection to another. Threat actors released a decryptor for this threat in May 2021, which can help recover files altered by a specific strain of Conti.

Conti has seen a rise in popularity since the infamous ransomware Ryuk apparently ceased operations. Many analysts regard Conti as the ransomware that replaced Ryuk, and consider it to be one of the most troubling ransomware threats in the wild.

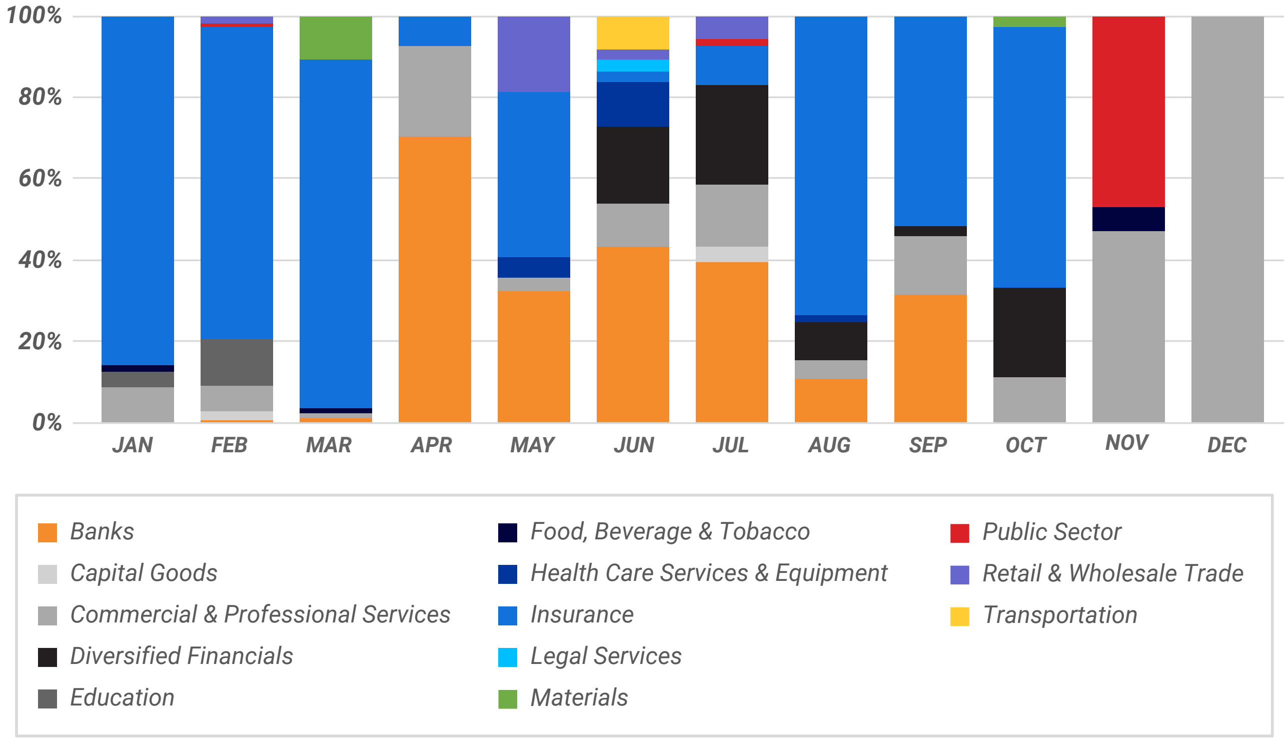


Figure 14 - Industries attacked by Conti, 2021

AVADDON

The Avaddon ransomware variant first appeared in early 2020. It made international headlines due to recent attacks against Australian organizations and the Asia-based cyber insurance company, AXA. Both the FBI and the Australian Cyber Security Center have released warnings regarding an ongoing attack by this malware family.

Like DarkSide and REvil ransomware, Avaddon also uses a double extortion scheme, where data is encrypted locally and exfiltrated before the ransom demand is made. If the victim refuses to pay, their data is published to a site located on the dark web. Avaddon, however, goes one step further. To further encourage compliance, attackers also subject victims to a distributed denial-of-service (DDoS) attack until the ransom is paid.

After drawing attention for its role in several high-profile ransomware incidents, the group behind Avaddon seems to be shuttering its current operations. Law enforcement efforts to track down malware operators visibly increased after the attack on Colonial Pipeline, which likewise prompted DarkSide to shut down operations. Avaddon has released the decryptors to the latest version of its threat.

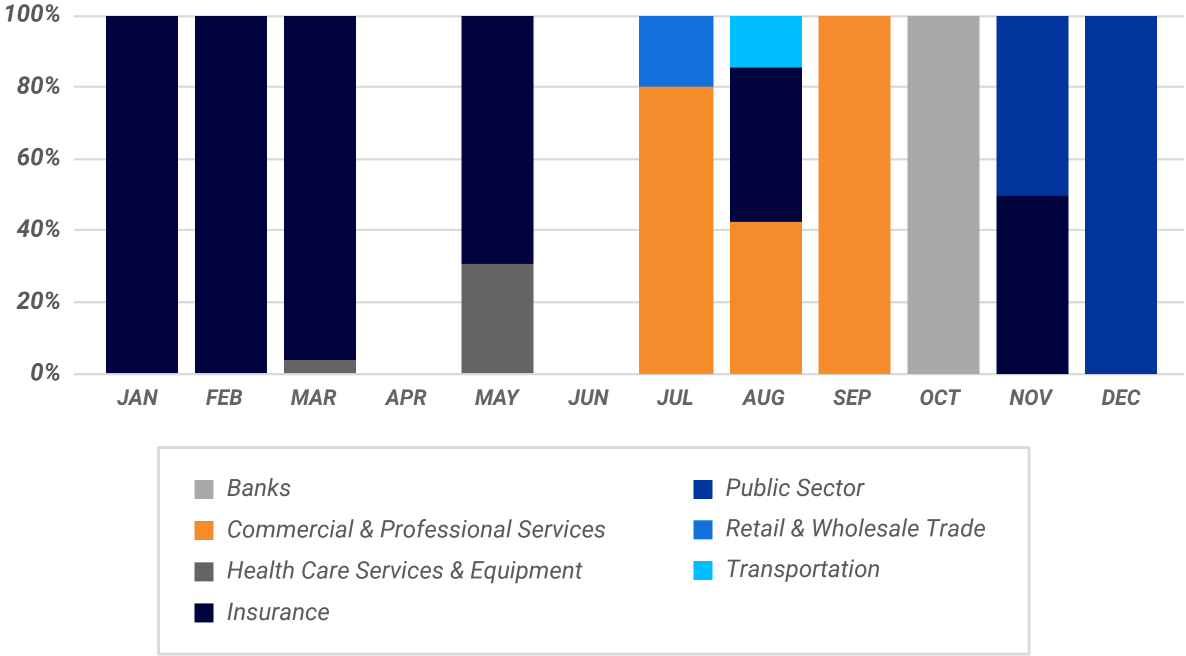


Figure 15 - Industries attacked by Avaddon, 2021

RAGNAR LOCKER

Ragnar Locker ransomware made international headlines for its attacks against a Taiwanese manufacturer of high-performance DRAM modules and NAND Flash products. The first variant of this family appeared in late 2019.

1.5TB

Ragnar Locker claims to have exfiltrated 1.5TB of data from a single high-profile victim.

Like many other well-known ransomware variants (such as DarkSide, Avaddon, and REvil), the current variant of Ragnar Locker also uses a double extortion technique to encourage victims to pay.

Ragnar Locker's dark website lists its latest victims on a self-dubbed "wall of shame". The threat group currently claims to have exfiltrated 1.5TB of data from a high-profile victim. According to the website, this information has been stealthily gathered over a long period of time.

HIVE

First seen in June 2021, the Hive ransomware family made headlines for attacking commercial real estate software company Altus Group. This threat also employs double extortion techniques. Victims refusing to cooperate with the threat actor risk having their data published to group's site, Hive Leaks.

Hive samples are written in the Go programming language and compiled for both 32-bit and 64-bit machines. The samples themselves are UPX packed to reduce their size, as Go binaries tend to be quite large.

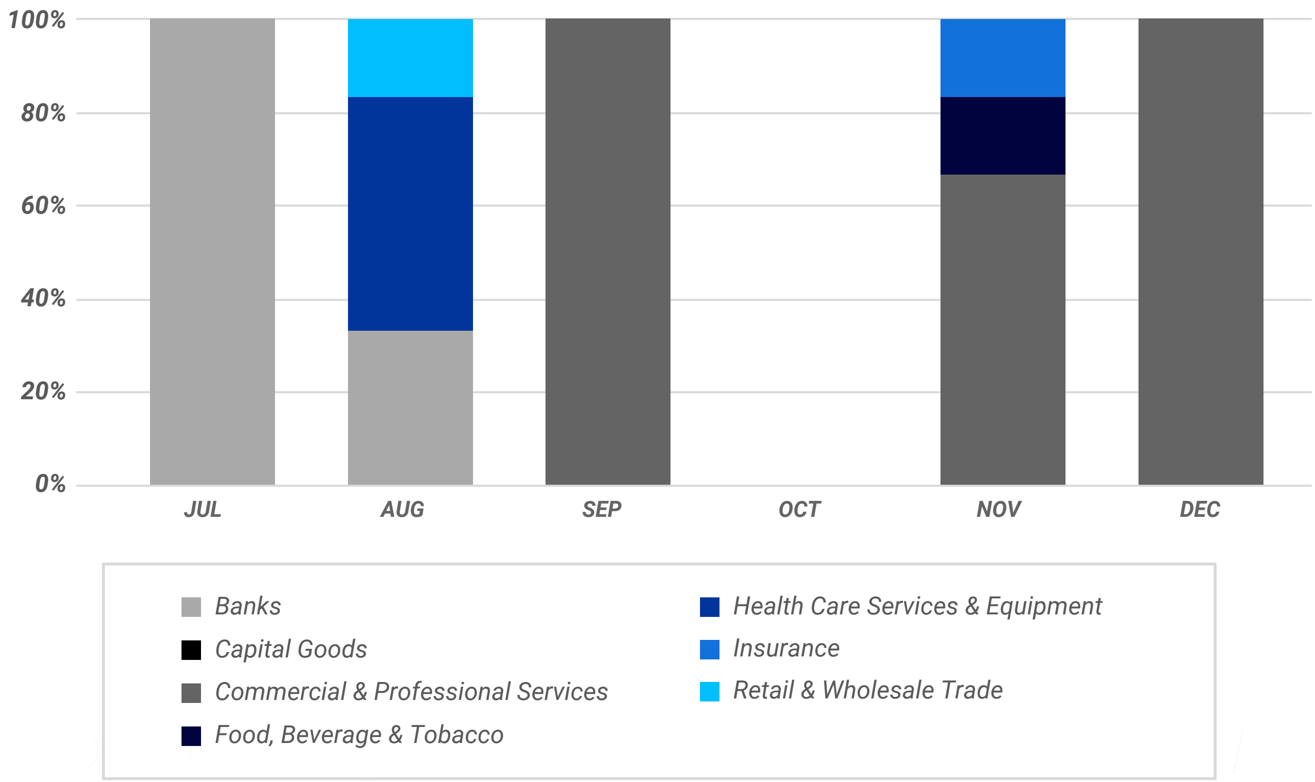


Figure 16 - Industries attacked by Hive, 2021

INFOSTEALERS

REDLINE

RedLine is an infostealer malware family that is distributed via COVID-19-themed phishing email campaigns.

RedLine is an infostealer malware family that is distributed via COVID-19-themed phishing email campaigns. It was an active threat throughout 2020. In 2021, it was delivered through malicious Google advertisements and spear phishing campaigns against 3D or digital artists using nonfungible tokens (NFTs). NFTs are digital tokens tied to assets that can be bought, sold, and traded.

RedLine is extremely versatile and has appeared as various trojanized services, games, cracks, and tools. Many samples of RedLine also appear with legitimate-looking digital certificates.

Once connection to its C2 panel is established, RedLine malware has a wide range of applications and services. In all cases, it attempts to perform illicit exfiltration of victims' data. The malware gathers information from web-browsers, file transfer protocol (FTP) clients, instant messengers, cryptocurrency wallets, virtual private network (VPN) services, and gaming clients. It also has remote functionality to drop and execute further malware onto the victim machine.

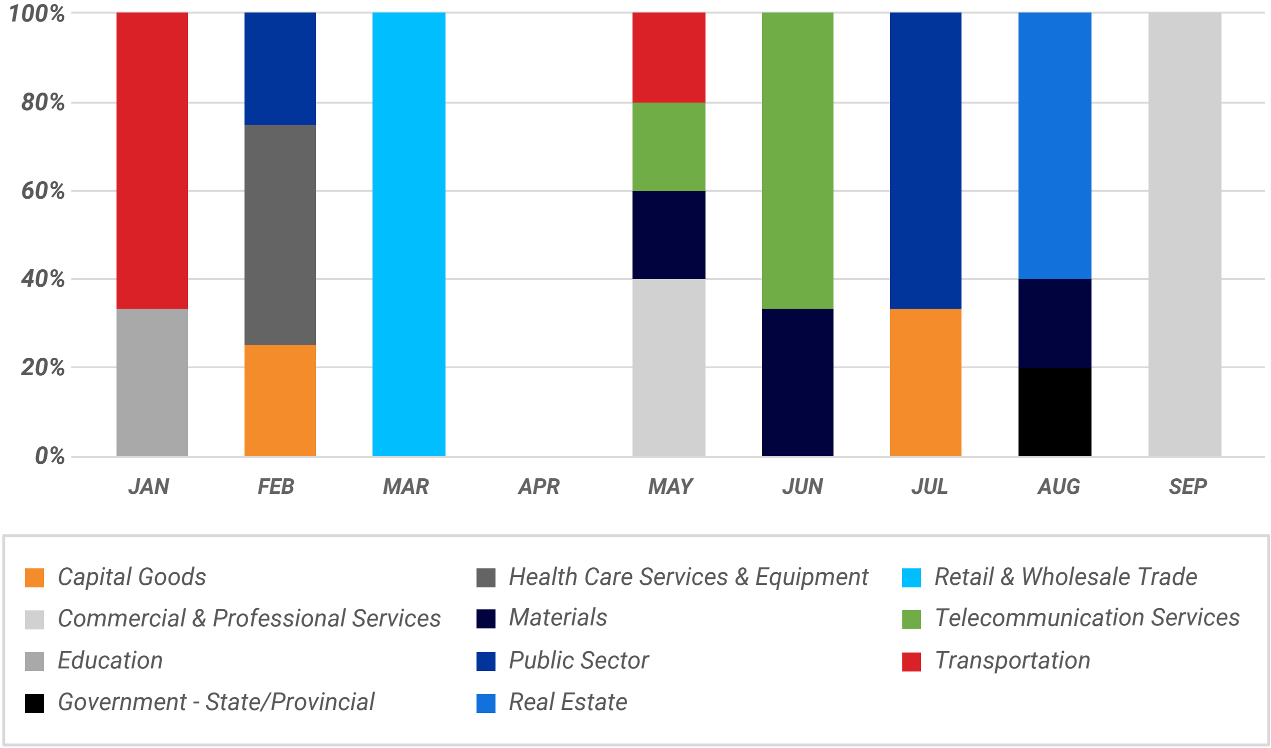


Figure 17 - Industries attacked by RedLine, 2021

AGENT TESLA

First seen in the wild in 2014, Agent Tesla is .NET-compiled and contains an array of powerful infostealing features. It was initially available for purchase through a website, with the malware's author offering several fixed-term licenses for its use.

Since then, the Agent Tesla infostealer has been consistently employed by cyber criminals in various campaigns, often using spam emails to facilitate infection.

The malware has evolved to gather information regarding a user's Wi-Fi profile, potentially as a propagation mechanism. This upgrade follows a similar enhancement to the Emotet malware variant, which also received a Wi-Fi spreader module.

The Agent Tesla infostealer has been consistently employed by cyber criminals in various campaigns, often using spam emails to facilitate infection.

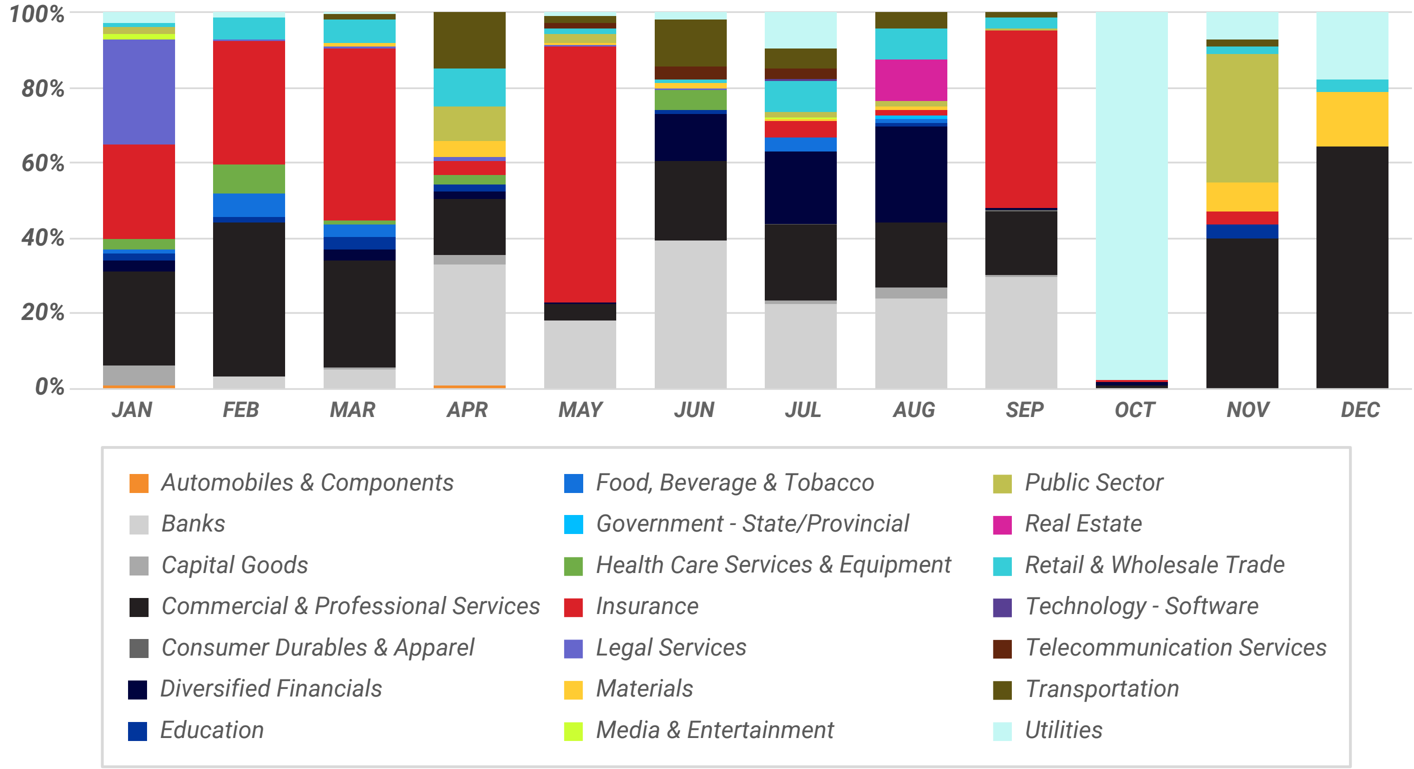


Figure 18 - Industries attacked by Agent Tesla, 2021

FICKER

Ficker is a malicious infostealer that is sold and distributed on underground Russian forums by a threat actor using the alias [at]ficker. This MaaS was first discovered in the wild in 2020.

Ficker has been previously distributed via trojanized web links and compromised websites. For example, it could direct victims to pages purportedly offering free downloads of legitimate paid services like Spotify and YouTube Premium™. It has also been deployed via the known malware downloader, Hancitor.

Notably written in Rust, Ficker has several targets for its information stealing activities, including:

- Web browsers
- Credit card information
- Crypto wallets
- FTP clients
- Other applications

Ficker uses anti-analysis checks, and can deploy further functionality and download additional malware once a system is successfully compromised.

Ficker is a malicious infostealer that directs victims to pages purportedly offering free downloads of legitimate paid services like Spotify and YouTube Premium™.

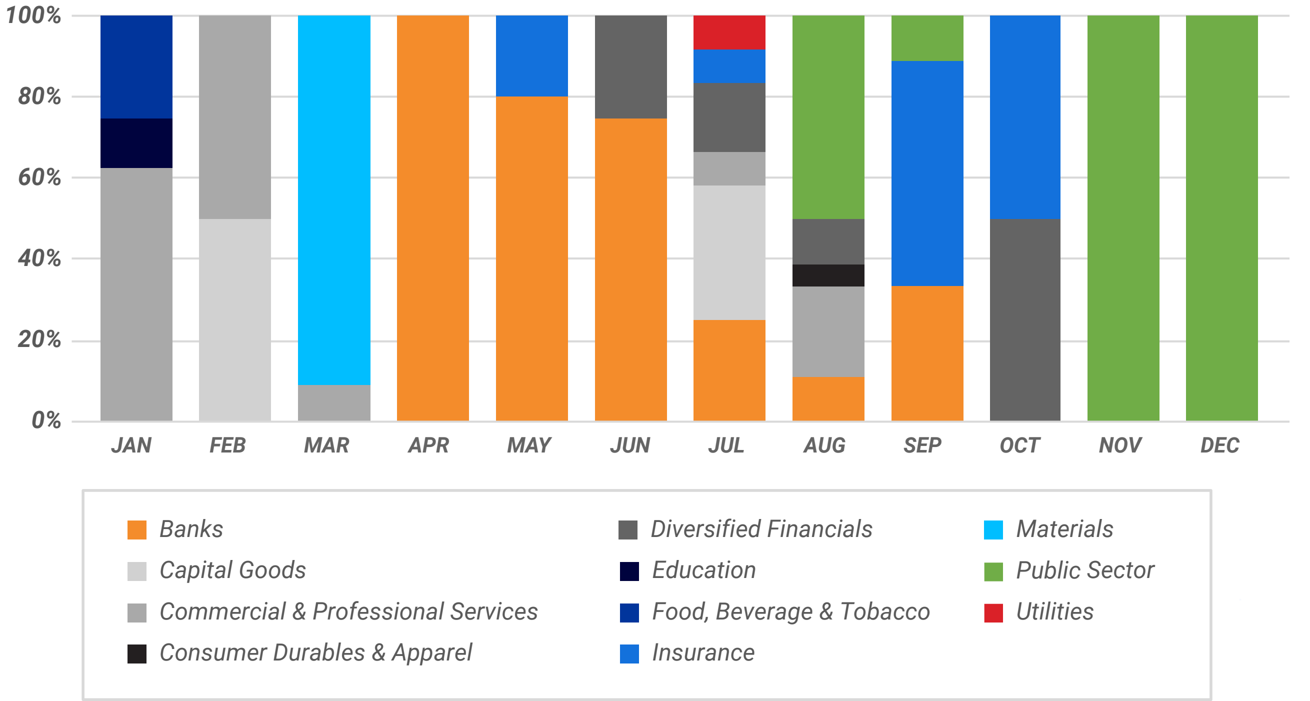


Figure 19 - Industries attacked by Ficker, 2021

HANCITOR

Hancitor (aka, Chanitor) was first discovered in the wild in 2013. It spreads via social engineering techniques, such as appearing to be from the legitimate document-signing service DocuSign®. Once victims are deceived into allowing its malicious macro code to execute, it infects their systems.

Hancitor then connects with its C2 infrastructure and attempts to download a wide range of malicious components, according to the needs of the operators' campaign. This year, Hancitor has been observed downloading known-malware family Ficker (aka, FickerStealer), as well as a Cobalt Strike Beacon payload.

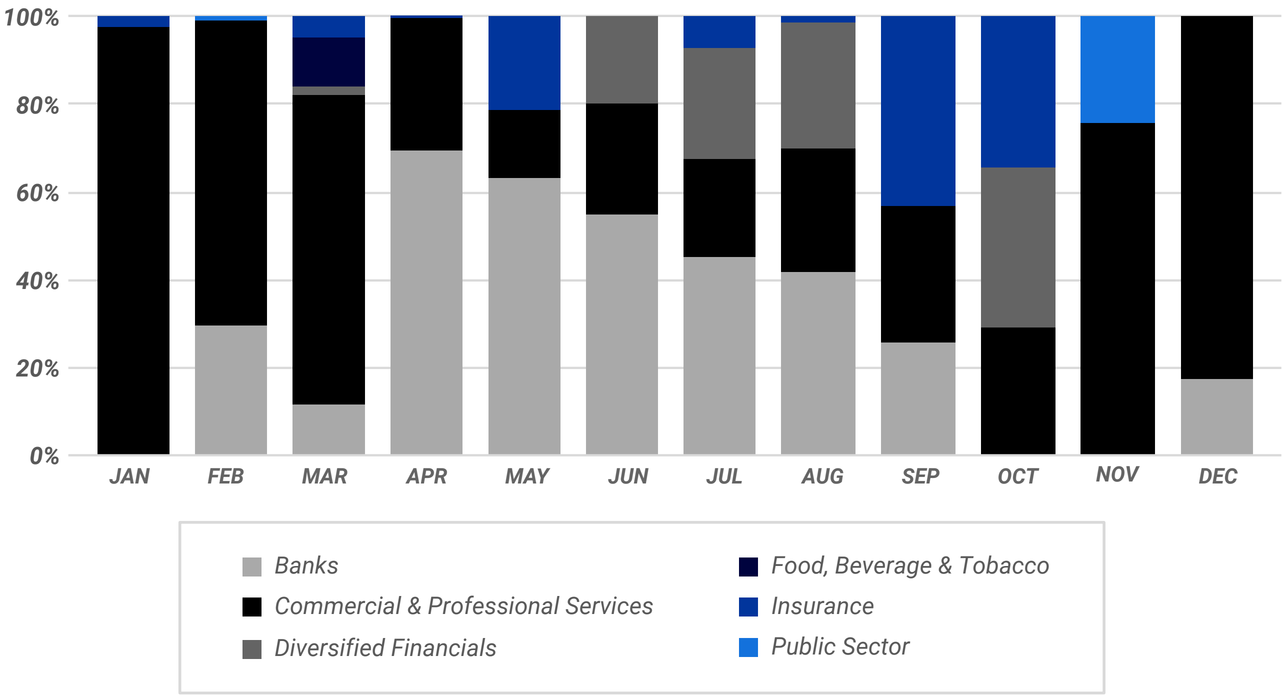


Figure 20 - Industries attacked by Hancitor, 2021

ALL TOP 10 THREATS

OCCURRENCES OF THE TOP 10 THREATS IN 2021

Figure 21 shows the monthly prevalence of each of the malware families according to BlackBerry's internal data.

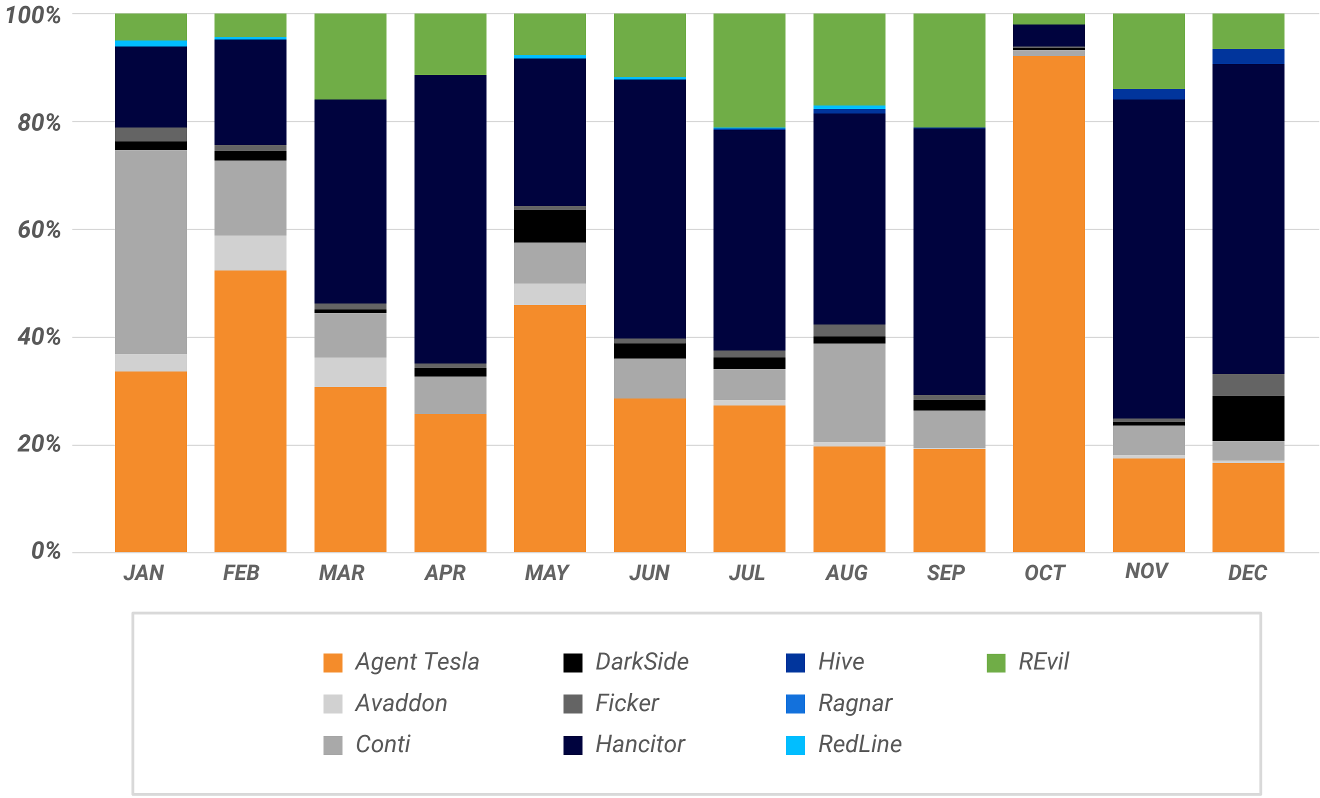


Figure 21 - Prevalence of the top 10 malware threats, 2021

TOP 10 VS. THE BLACKBERRY PREDICTIVE ADVANTAGE

No one wants to be patient zero for a new threat. By learning everyday lessons from the wide world of threats, organizations don't have to be.

With predictive threat detection models, forward-leaning cybersecurity models have moved from legacy detection methods to techniques driven by machine learning (ML). Training ML models extensively on current malware allows AI-driven solutions to predict how threats will appear and behave in the future. BlackBerry® solutions, built using Cylance® AI, learn to predict emerging malware families and variants by training on existing samples drawn from the threat landscape. This approach gives AI-driven cybersecurity the ability to detect both known and zero-day threats before they can impact their targets.

Predictive Advantage retroactively measures the period of time an AI-driven model would have detected and prevented a new threat prior to its discovery.

WHAT IS PREDICTIVE ADVANTAGE?

Predictive Advantage retroactively measures the period of time an AI-driven model would have detected and prevented a new threat prior to its discovery. For example, if an ML model protects against a threat that appears one year after the model's creation, it scores a predictive advantage of 12 months. The measurement uses an offline local prediction algorithm for testing, without any updates or an Internet connection. This ensures the ML model performs exactly as it did upon its original release date, without enhancements or upgrades.

BlackBerry has performed a predictive advantage test to score our detections against the top 10 malware families described in this annual report. This illustrates how far in advance the AI model offered protection against the largest threats facing our customers in 2021.

The AI model represented in this test was created in October 2015. It was deployed with the BlackBerry® Protect agent version 1320. The numbers in Figure 22 show how many months in advance our model could have protected customers from each threat before it was discovered.

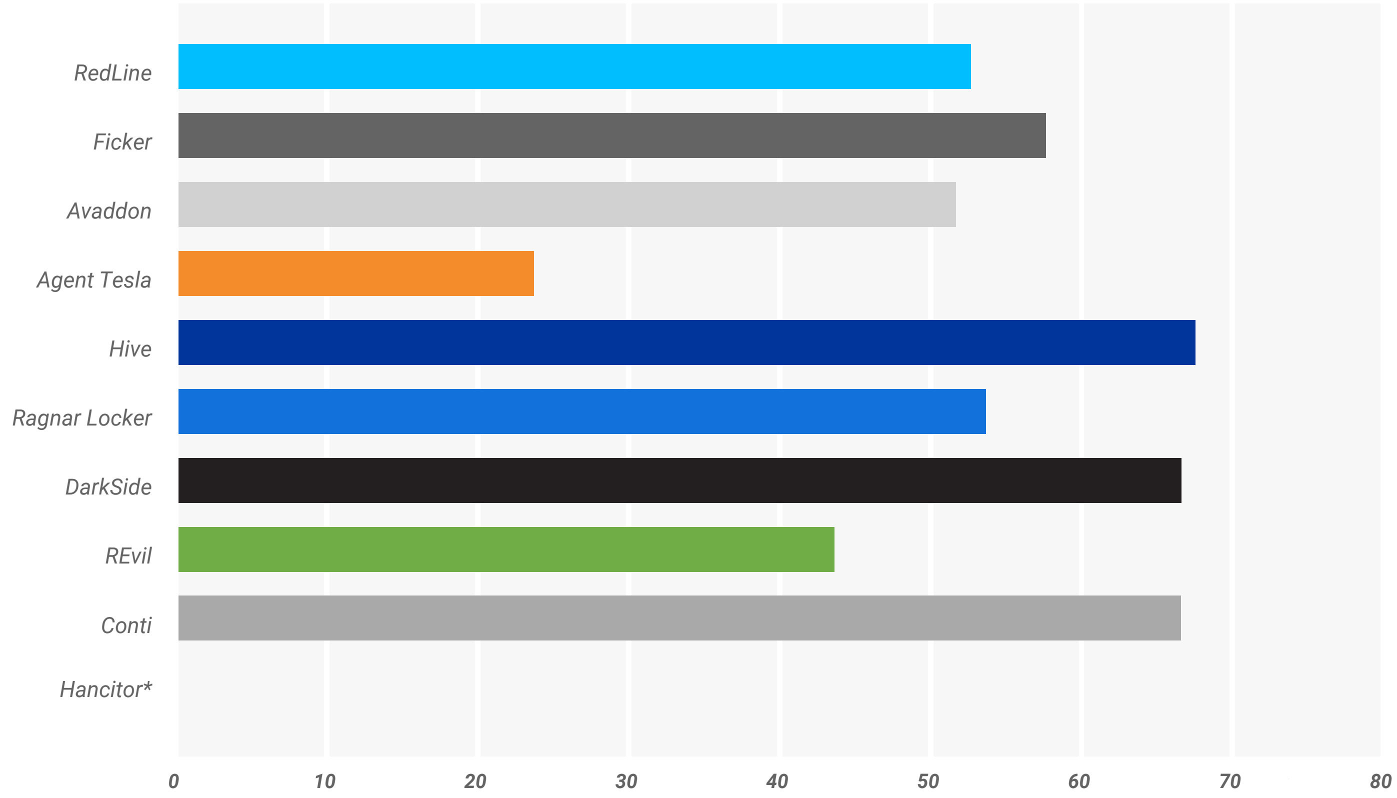
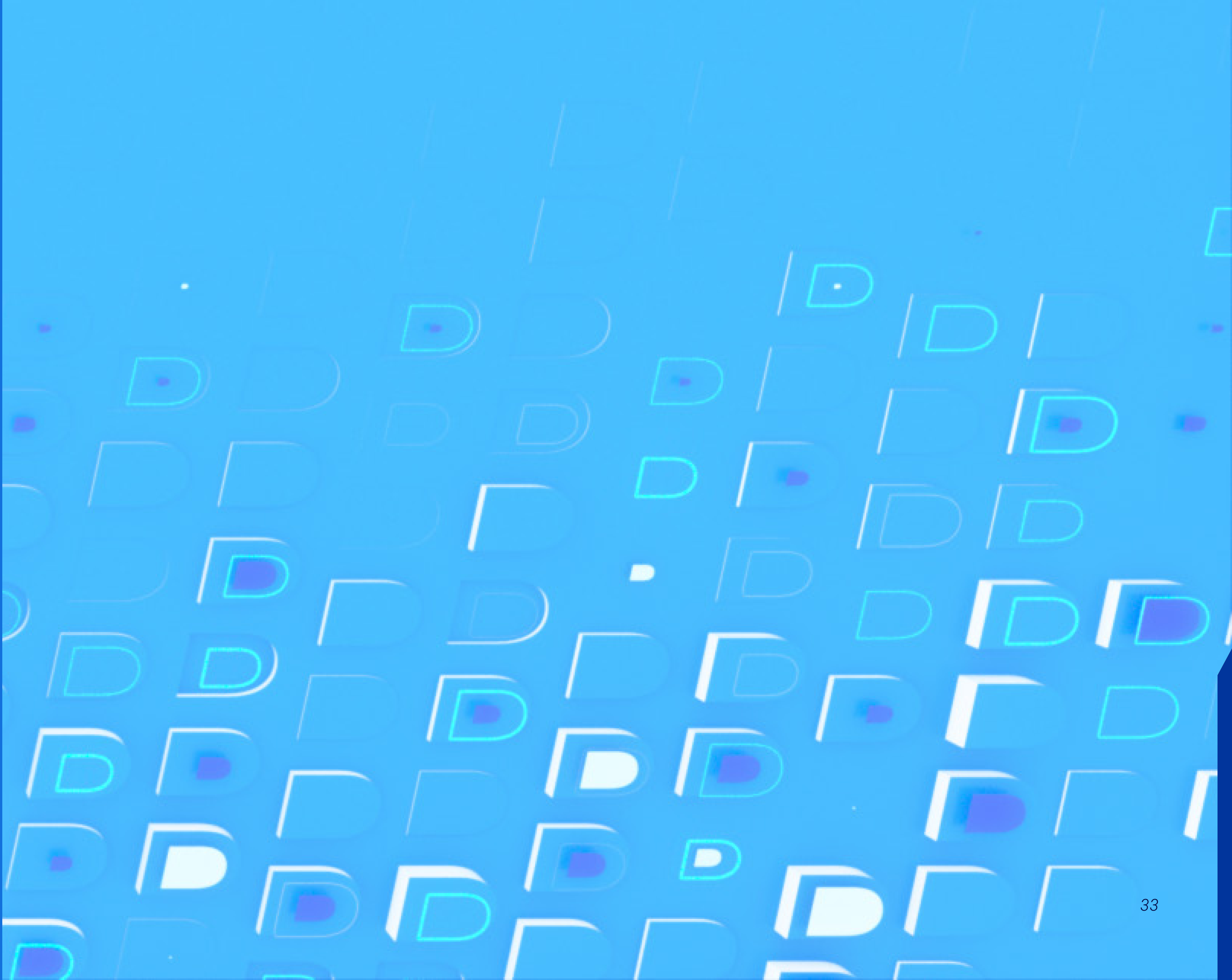


Figure 22 - BlackBerry Predictive Advantage, in months, over the top 10 threats to our customers
**NOTE: Hancitor is not represented in the chart as its discovery pre-dates October 2015.*

DATA SCIENCE



AI AND ADVERSARIAL ATTACKS

As the previous examples of Predictive Advantage indicate, artificial intelligence and machine learning can be mighty weapons in the fight against cyber crime. Unfortunately, they also have the potential for misuse or abuse at the hands of sophisticated and unscrupulous actors with malicious intent.

Consider the case of deep learning, one of the most hyped technologies of the past decade. Despite its promise for industry, it also introduces another target for threat actors to compromise.

DEEP LEARNING AND ADVERSARIAL ATTACKS

Over the past decade, the rise of deep learning (aka, neural networks) has provided a massive boon to technical industries. This disruptive technology has enabled companies to improve products and optimize key performance indicators by uncovering patterns previously hidden in their internal data. These algorithms have allowed companies to reallocate manpower away from tedious analytics tasks: specifically, those tasks in which huge quantities of rule sets or other heuristics were manually generated.

Unfortunately, this progress has come at a cost. An entire field known as adversarial learning has emerged as a threat to all products employing predictive algorithms. The primary goal of this field is to discover ways neural networks can be taught to fool other predictive algorithms by subtly changing input data. As an example, adversarial algorithms have been used to determine how to apply small patches of tape to a stop sign to render it invisible to classification algorithms. For imagery or audio, adversarial attacks can be used to make nearly undetectable changes to a sample to fool otherwise highly accurate prediction algorithms.

An entire field known as adversarial learning has emerged as a threat to all products employing predictive algorithms.

In cybersecurity, these algorithms have been used to modify malicious files to allow them to bypass both heuristic and ML-aided defenses. It is not simple to make arbitrary changes to files (which have their own structure and structural rules), so most of these attacks use a bulk iterative strategy. Using this technique, algorithms make thousands (or even hundreds of thousands) of small additions to a file that individually have no impact on its functionality. However, each change can nudge a predictive algorithm's decisions on threat classification in the benign direction. Concerningly, the files generated by these adversarial algorithms seem to be capable of being transferred between models. This means an attack trained on one defense might be capable of bypassing dozens of commercial cybersecurity products.

In spite of the danger posed by these algorithms, the pace of research in this area is accelerating, largely due to misaligned incentives. Deep learning is an extremely competitive and popular field, giving academics and large technology companies strong motivation to publish as much research as possible. As a result, the field of adversarial attacks is extremely active. For example, a search for adversarial attacks on Google Scholar™ for 2020 returns thousands of entries, of which a few hundred focus on cybersecurity.

Similarly, ML engineers looking to interview at high-level tech companies are usually encouraged to create useful open-source packages to demonstrate their skills. A quick search for adversarial learning across GitHub yields nearly 5,000 separate repositories, some with over 1,000 stars (or likes). Career-based incentives have had the net effect of democratizing and commoditizing adversarial algorithms, making them ubiquitous and reducing their barrier to entry.

ALGORITHMIC DEFENSES

A secondary field dubbed adversarial learning or adversarial defenses was created not long after adversarial attacks were discovered. These defenses often focus on ways to architect or train models, or preprocess data beforehand, to mitigate the effects of adversarial attacks.

This field is still playing catch-up in terms of its overall efficacy. No adversarial defense appears to be robust in white-box attacks where the attacker has full knowledge of the type of model and defense(s) being employed. However, many adversarial defenses appear to be fairly robust to black-box attacks. Thus, organizations can prevent white-box attacks and force attackers to rely on less efficient black-box attacks by using a couple of techniques. They can obfuscate the output of a defense, typically by reducing its precision, or throttle the ability of attackers to bulk query a defense.

As mentioned previously, adversarial examples are often transferable, and are potentially capable of evading numerous defenses, as recent publications have confirmed.

However, these attacks only evaded products that didn’t employ adversarial defenses generated by deep learning. BlackBerry has internally verified that attacks generated in this manner are unlikely to bypass models utilizing multiple robust deep learning defensive schemes.

Also, adversarial attacks on files need to rely on iterative approaches that are not typically used in other areas (such as on visual or auditory models). As a result, many open-source adversarial attack toolkits cannot be easily modified to focus on cybersecurity defenses. Unfortunately, a perusal of GitHub yields a few pages containing what appear to be amateur efforts at generating adversarial examples. This does not bode well for what may follow as the field matures.

OUTLOOK

In the near term, the outlook in this area is mixed. The field of adversarial attacks is still white-hot, and open-source software has greatly lowered the barrier to entry for people looking to generate adversarial examples. The amount of expertise necessary to generate bypasses is still quite high. Given this, we do not expect widespread use of this technology in the next one to two years.

Any open-source adversarial packages will still likely need to rely on bulk approaches to generating attacks. This means cybersecurity companies have a reasonable path forward, which can be summarized as follows:

- Hire people who understand adversarial deep learning
- Employ multiple robust defensive schemes (even for products using heuristic defenses)
- Keep defensive schemes secret / internal-only
- Prevent attackers from rapidly querying defenses to find subtle holes

> *Nothing in security is guaranteed. However, for organizations that follow these rules, adversarial attacks should prove to be a manageable threat vector in the near term.*

CYBERSECURITY INSIGHTS

INCIDENT RESPONSE YEAR IN REVIEW AND TRENDS

Ransomware has continued to take center stage for the BlackBerry Incident Response Team over the last year. As discussed in the BlackBerry 2021 Threat Report, the double extortion strategy of ransom and data exfiltration has now become the norm. In fact, the trend has escalated, with instances of triple (adding harassment) and quadruple (disruptive attacks such as DDoS) extortion occurring. As a result of these expanding threat actor strategies, there is an increasing spike in public data leakage.

Evolving extortion methods have created a close alignment between the tactics used by nation-state APT threat actors and profit-seeking criminal organizations. Their approaches and operational goals are strikingly similar, although their core motivations, levels of technical expertise and methods of execution often vary. As such, the vast majority of attacks that occur today follow a similar attack pattern, as detailed in Figure 23.

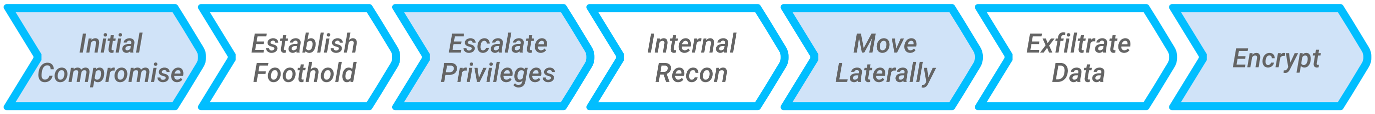


Figure 23 - Typical threat actor attack flow

One main difference between APT groups and ransomware organizations is how long each group plans to stay active in the environment. This, in turn, affects how covertly they behave. APT groups frequently plan for long-term residence in a victim's environment. Ransomware groups are more like smash-and-grab home invaders.

For example, APTs often prefer to "live off the land" by using legitimate system resources so their activity is hard to distinguish from daily operations. They take their time to carefully study an environment and understand the security measures in place before executing any malicious actions. Ransomware attacks are more opportunistic and therefore operate more quickly and recklessly. As a result, they typically generate more noise for an endpoint protection platform (EPP) and endpoint detect and response (EDR) tooling to detect. For example, they may use tools such as PowerShell, Windows batch scripting, or WMI to attempt to disable antivirus products, backup solutions, and other system processes.

Another key difference is that nation-state groups are often looking for specific information to exfiltrate. They may use it for intelligence purposes, often in pursuit of political or economic advantage. Conversely, ransomware groups often look for anything valuable that could increase the likelihood of getting paid. Frequent favorites include targeting databases that may contain customer or financial information.

In the public eye, size really does matter when it comes to headlines and data leakage. Therefore, profit-seeking threat actors will attempt to grab as much as they can while they are in the system or network.

As a result, BlackBerry has observed some automated “scatter-gun” approaches to data exfiltration by ransomware groups over the last year. Some showcase nicely engineered scripts targeting specific file types to collect: typically Microsoft® Word, Excel®, and PDF documents that are under a year old. Stolen data is then uploaded to the attacker’s infrastructure. In other instances, BlackBerry identified threat actors attempting to compress entire shared drives from the top level within corporations in attempts to grab everything available.

Along with ransomware groups like Conti, DarkSide, BlackMatter, and others currently making headlines, there is a new influx of ransomware operations occurring through RaaS. BlackBerry has observed several incidents where companies were attacked using a variant of a well-known ransomware. However, the tactics, techniques, and procedures (TTPs) utilized by the attacker lacked sophistication or depth. In multiple incidents, BlackBerry identified threat actors leaving behind playbook text files containing IOCs with exact commands, IP addresses, target lists, and more. This suggests that the authors of these sophisticated ransomware families are not the ones actually carrying out the attacks.

Financially motivated attackers still focus on low-hanging fruit when it comes to the initial compromise phase of their attack.

Financially motivated attackers still focus on low-hanging fruit when it comes to the initial compromise phase of their attack. Unfortunately, there was an overabundance of targets last year due to continued use of older technologies and infrastructure in victim environments, such as on-premises servers. For example, ProxyLogon and ProxyShell, common names for two sets of vulnerabilities impacting many on-premises Microsoft Exchange Servers, were widely exploited throughout 2021. The HAFNIUM APT group was first to exploit the vulnerabilities in multiple organizations. After publication of the ProxyLogon vulnerability and proof-of-concept exploits, other threat actors began rapidly scanning and infecting numerous on-premises Exchange hosts. Threat actors exploiting these vulnerabilities often implanted additional backdoors, commonly in the form of China Chopper web shells, an increasingly popular web shell that packs a powerful punch in a small package.

Externally accessible RDP continues to be an enduring favorite, however it is becoming less common compared to other techniques. Vulnerabilities impacting vendor appliances, especially VPNs, firewalls, and perimeter network devices, remain the root cause for many incidents. While these vulnerabilities are often dated and well documented, BlackBerry observed several incidents where devices remained unpatched.

In other cases, previously vulnerable network appliances were patched, but not until after they were already compromised. These incidents resulted in credentials being stolen or back doors being installed. The sheer number of compromised environments and credentials have bolstered flourishing dark web marketplaces, where premiums are placed on domain administrator accounts. However, it is not difficult to find company or private credentials that are available for free, as well.

In addition to the previously mentioned techniques, BlackBerry observed multiple incidents involving watering hole attacks. Watering hole attacks provide threat actors with a unique way to obtain a foothold and establish persistent access into an environment. These attacks targeted users performing legitimate searches for business-related material, a common workplace practice. In these incidents, search results returned the watering hole URL near the top of the first page of Google™ search. The watering hole site presented the user with what appeared to be a helpful forum post containing a link to exactly what they needed. It included several fake comments claiming that the linked-to file was an exact match to their query.

If users open the weaponized document, however, malware would download and install a Cobalt Strike Beacon, giving threat actors a foothold in the environment.

REvil is one of the best-known attack groups currently using this ploy. This threat group was initially identified in 2019. They are one of the dominant ransomware groups, claiming responsibility for some of the more infamous ransomware attacks of the past few years. They were also closely linked to the DarkSide Group, which was responsible for the Colonial Pipeline attack. The Russia-linked group has been under scrutiny recently and has gone underground on numerous occasions, only to reemerge.

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence

The increasing use of Cobalt Strike is another trend observed over the last year. BlackBerry has witnessed it being leveraged as a highly effective and popular post-exploitation toolkit for several years. Its abuse has continued to increase to the point that it is not uncommon to find evidence of its usage during an incident response engagement. For those unfamiliar with it, BlackBerry recommends reviewing our authoritative new book on Cobalt Strike, published by the BlackBerry Threat Research and Intelligence Team in November 2021.

ATTACK LIFECYCLE

The BlackBerry Red Team analyzes the entire attack lifecycle as part of our mission and portfolio of service offerings. Our end-to-end adversarial simulation provides a unique threat actor perspective, by allowing us to observe the effectiveness of different defenses in a variety of organizations. These experiences have prompted us to reveal some of the most common attacks and effective defenses we encounter.

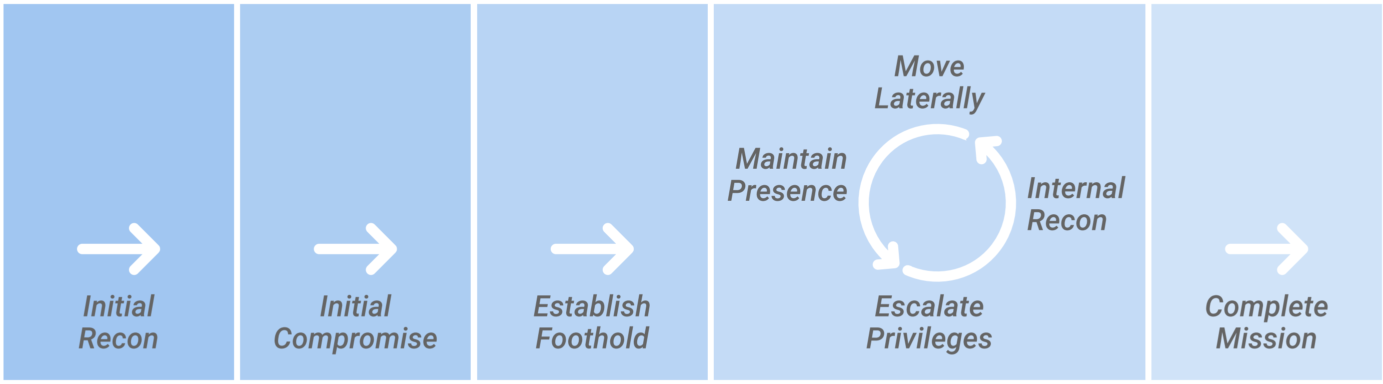


Figure 24 - Typical attack lifecycle

INITIAL RECONNAISSANCE

The initial recon that an attacker performs can be passive, active, or both. Since passive recon does not touch any of the target's systems, it can be difficult to detect. However, once the recon moves to more active and intrusive activities, such as probing systems for vulnerabilities, defenders should be alerted. Key defensive strategies for this phase involve knowing your organization's assets, proactive scanning, patching, monitoring, and attack surface reduction.

INITIAL COMPROMISE AND ESTABLISHING THE FOOTHOLD

Once a vulnerability is discovered during the recon phase, attackers exploit the vulnerability and establish presence on the host. From there, threat actors can regain entry at a later point and pivot to other systems in the network. This activity is something that organizations should detect and block via a layered defense of AI-based network and host visibility, and blocking.

ESCALATION

Attackers typically gain access equivalent to that of the application they exploited, and use that to compromise the host. This is one of many reasons why the principle of least privilege matters. In addition to following best practices, EPP software should contain layers of defense to include script blocking and memory protection. The goal is to make it extremely difficult for an attacker to achieve each step in the attack lifecycle. Slowing the adversary's progress also buys time for the defenders to detect and block the attack.

INTERNAL RECON AND LATERAL MOVEMENT

Once an attacker gains sufficient privileges, they will move through the network and position themselves to achieve their goal. One of the best defenses in this situation is to employ network segmentation and watch for anomalies resulting from the use of stolen credentials. In this phase, defensive teams can greatly benefit from using AI-powered defensive technology, such as continuous authentication using passive biometrics. These passive biometrics are low user-burden activities–such as keyboard and mouse usage patterns–that uniquely identify users. An ML algorithm can be applied to this metadata to create a risk score. Organizations can then utilize actions, such as force re-authentication or block user, when the risk score exceeds the organizationally defined threshold.

COMPLETE THE MISSION

Before the BlackBerry Red Team conducts an adversarial simulation exercise, we jointly define the goals with our clients. This almost always includes some sort of data (or flag) exfiltration, since many threat actors are financially motivated. Threat actors can get paid in many ways, such as selling stolen data, threatening to sell stolen data, or unlocking encrypted data.

Ways threat actors can get paid

Selling stolen data

Threatening to sell stolen data

Unlocking encrypted data

TAKEAWAY

Here are some helpful universal truths to remember regarding the attack lifecycle and cyber kill-chain:

- Be proactive. The "further to the left" you are in the attack lifecycle (see Figure 24), the easier and cheaper it is to discover and fend off an attack.
- Anything less than around-the-clock monitoring is not sufficient.
- The mission of most threat actors today is to exfiltrate data and launch ransomware for profit.
- AI-based defenses help organizations avoid becoming patient zero and are immune to the lag time from signature writing that occurs with traditional defenses.
- Defensive efforts must always be continuous, due to newly discovered vulnerabilities and an ever-evolving threat landscape.
- Prevention is key. The ability to recover from backups does not address the double extortion tactic derived from attackers threatening to sell stolen data.

PROTECTING CRITICAL INFRASTRUCTURE

Every organization, in every vertical industry sector, runs the risk of breach, ransomware deployment, and extortion. However, few carry the same real-world risk from cyberattacks as those in the critical infrastructure sector. The public expects that utilities such as power, gas, water, and waste treatment will always be able to provide these necessary services. As a result, these organizations are significantly motivated to meet these expectations, which makes them lucrative targets for ransom and extortion.

Unfortunately, the challenges for this sector don't stop at being high-value targets. The following factors often compound the problem:

- Older, inherently vulnerable, and sensitive devices
- Legacy operating systems
- The need for offline/disconnected environments

Many critical infrastructure systems and devices have been around for a long time and were originally designed for serial communication, but later adapted to ubiquitous TCP/IP networks. This adaptation of connectivity may not necessarily include a security upgrade. Since these environments can be difficult and expensive to modernize, they typically run older, and usually unsupported, operating systems.

Often, the need to protect the environments results in segmentation from other networks, and hopefully the Internet as well. However, this segmentation poses additional management and protection challenges.

In summary, protections need to be extended to older devices, running legacy operating systems, that are disconnected from networks and the Internet. One possible solution is the use of machine-learning-based endpoint protection that lives on the endpoint itself. This type of endpoint protection platform (EPP) software can run on legacy operating systems such as Windows XP/2003. If it is lightweight, it won't overtax antiquated hardware. The localized math model must be designed to avoid the constant need for deploying signature updates.

Legacy AV software requires signatures to be written for the latest threats and released as often as every hour. This is difficult to keep up to date, even on modern hardware and Internet-connected hosts. This makes it a poor fit for critical infrastructure that is disconnected and would require a "sneakernet" approach to distribute signature updates. AI-based defenses allow a much longer wait time before requiring updates, as they identify threats using millions of attributes, not through known signatures.

Critical infrastructure is a challenging environment to secure, but the situation is not hopeless. Like other industry sectors, it simply needs to evolve beyond reliance on legacy defensive technology that cannot scale to prevent modern cyberattacks.

Every organization, in every vertical industry sector, runs the risk of breach, ransomware deployment, and extortion. However, few carry the same real-world risk from cyberattacks as those in the critical infrastructure sector.

PREVENTION-FIRST AI

AI and ML offer many capabilities and advantages for protecting organizations from cyberattacks. While the terms AI and ML are often used interchangeably, they are different concepts in certain key aspects. AI describes the ability of computers and machines to perform activities that imitate intelligent human behavior. ML is a subset of AI that relies on mathematical algorithms to achieve AI behavior and functionality. The process behind training ML requires access to vast amounts of historical data as a base for its learning. Through multiple phases, new data is introduced to improve the ML model's learning functions before it ultimately becomes a component of AI.

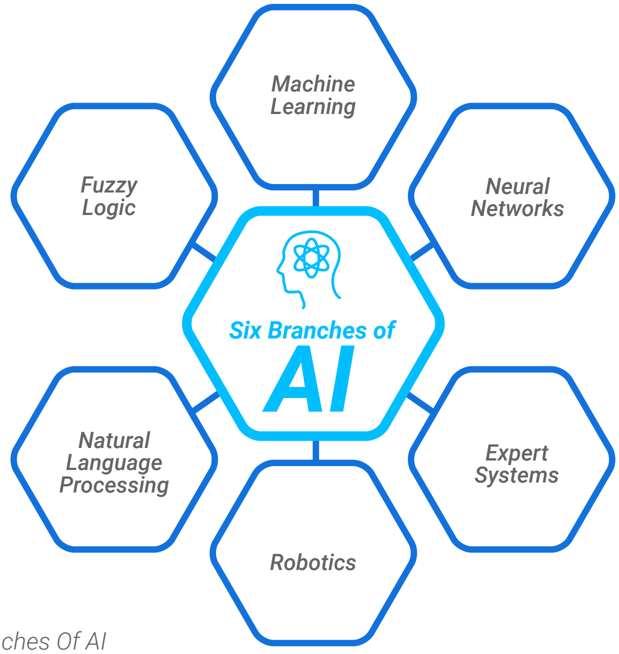


Figure 25 - Six Branches Of AI

In fact, ML is only one of six branches of AI. The other branches are neural networks, expert systems, natural language processing, fuzzy logic, and robotics. BlackBerry's Cylance AI, for example, combines ML and neural networks to identify and prevent cyberattacks before they execute. Because the AI security agents are well-trained and extremely lightweight, they can reside upon users' endpoints without impacting resources. These on-device security agents protect devices whether they are online or offline. BlackBerry has put considerable research and development funding and effort into developing its Cylance AI. We hold hundreds of patents in AI, ML, security, and forensics, which puts us alongside other leading AI-centric companies such as Google, Facebook, and Amazon.

ML is classified into two different categories: supervised and unsupervised. These classifications describe the ways ML models learn to classify input data into the correct output assumptions–in other words, how they make accurate predictions.

Supervised learning is an assisted process where the math algorithm is guided to predict the outcomes from the input of a data training set. With this method, humans supervise the ML by manually labeling the training data sets. Supervised ML is like a child learning to ride a bike with training wheels. The parent offers guidance until the child is ready to remove the training wheels and ride on their own. Supervised learning requires incredibly large amounts of training data and guidance before the math models can assess the inputs and return the desired outputs.

Unsupervised ML classifies data into the correct output assumptions without human intervention or labelled data. Unsupervised learning is usually the second stage of training math models, after they ingest vast amounts of input data from supervised training sets. This phase allows data scientists to see how math models run on their own, and how well they create the desired outputs. Going back to the bicycle allegory, unsupervised learning is the parent removing the training wheels and seeing how well a child rides the bike unassisted.

AI + ML

At BlackBerry, our AI math models use both supervised and unsupervised ML to train on identifying a good binary, and differentiating it from a bad one.

At BlackBerry, our AI math models use both supervised and unsupervised ML to train on identifying a good binary, and differentiating it from a bad one. The data sets are extensive and based upon millions of file features. When determining the danger posed by a file, its features (everything that makes up the file) are extracted to essentially provide its digital DNA. These features are correlated across approximately 2.7 million others that our math models have previously trained upon. By training on such a large set of file features, Cylance AI has learned to quickly identify what is a good or a bad (aka, malicious) file.

BlackBerry Protect, built using Cylance AI, can perform this feature correlation within 100 milliseconds or less, and, most importantly, it can do it pre-execution. That means it stops the threat before it can run. This allows BlackBerry Protect to stop malicious files from executing, whether they are known malware or a never-before-seen threat. This ability to stop emerging and zero-day malware is called the BlackBerry Predictive Advantage. It is achieved by the accuracy of our math models, which can correctly identify malicious files, often years before they are seen in the wild.

HOW IS FEATURE EXTRACTION/VECTORIZATION ACCOMPLISHED?

For machines to interpret the ML associations of feature extraction and produce an output, vectorization has to occur. Vectorization is the process of converting input data into mathematical vectors using a format readable by ML algorithms and computers.

Vectorization has been around since computers were first built. It is how ML math models can correlate and cluster good file features from bad. It formats file feature information in a way computers and math models understand, and allows them to provide output. When a file feature, such as code expected in a specific area of memory, is extracted from a file, it is converted into a mathematical value of 1s and 0s. This allows the ML algorithms in BlackBerry Protect to determine whether a file is safe. If so, it is cleared for execution, but malicious ones are blocked and quarantined.

It should be noted that BlackBerry Protect, in the beginning phases of the algorithm learning process, identified approximately 300 million file features. This has since been distilled down to 2.7 million critical features it can use to categorize and label file safety. Features refer to both what is found in files and what is expected. For example, if particular data is expected to appear in a specific part of a file's DNA but is not there, that is also a feature.

Well-trained AI offers an incredible advantage over human counterparts for performing this type of analysis and predictive work. A human analyst might take considerable time to identify 150 to 200 features of a file. Trained ML algorithms can identify, correlate, and assess millions of file features and determine a file's threat probability within milliseconds.

A PREVENTION-FIRST APPROACH TO SECURING AN INCREASINGLY HYBRID WORKFORCE

It's tempting to blame the massive increase in cyberattacks over the past 18 months on the COVID-19 pandemic and resulting shift to a distributed workforce. A recent IBM survey seems to support this view:

$1.07M

Increase in breach costs (from $3.89M to $4.96M) when remote work was a factor.

58 Days

Longer to identify and contain a breach when 50% or more of employees work remotely.

It's true that expanding the corporate network to encompass the home environment and personally-owned devices creates new security gaps for adversaries to exploit. But if our current security technologies and practices were robust enough to scale gracefully, the transition could have been much less disruptive for many organizations than it turned out to be.

Spear phishing and credential abuse were major problems before the pandemic. They continue to account for most breaches today. VPN and virtual desktop infrastructure products were vulnerable to exploitation before COVID-19. They still are today. It's the same story with unpatched servers and threats caused by malicious insiders, or by users practicing poor cyber hygiene.

The real problem is that current security approaches are unsustainable because they are inherently reactive and unrealistic. A human resources employee responsible for examining resumes all day should not be expected to know when a document is weaponized, and avoid opening it. SecOps and NetOps professionals responsible for protecting a complex and rapidly changing infrastructure should not be expected to anticipate and manually quash every possible attack.

The problem cannot be solved by training every employee to also become a cybersecurity expert. It cannot be fixed by adding yet another security tool or layer to a fundamentally reactive security architecture. BlackBerry believes that a more realistic solution is to transition to a prevention-first security strategy. By leveraging intelligent solutions that focus on impairing and impeding cyberattacks, employees can focus on the jobs they were hired to do.

At the device level, this means traditional blocking and tackling. Vulnerable systems should be patched and updated. Reactive, signature-based defenses should be replaced with AI-powered endpoint protection that prevents the execution of known and zero-day malware.

Next, user-focused security controls should be deployed at every enterprise network and cloud application ingress point that prevent remote employees from intentionally or accidentally abusing their credentials or violating security policies. Each user's access to resources should be controlled dynamically, based on real-time risk assessments of their current behavior. To preserve productivity, this continuous authentication process should be as transparent to users as possible, but permit no workarounds or evasions.

Tools that rely on static rules-based analysis cannot achieve this. It's simply not possible to devise rules that anticipate every gradation of risky or anomalous behavior. And the retrospective analysis they often produce comes too late to prevent exploitation. That requires solutions built with AI that learn how to assess risks and prevent exploitation proactively, not respond after the fact when damage is already underway.

Properly implemented, a prevention-first strategy preserves the flexibility and productivity benefits of having a remote or hybrid workforce in the first place.

Prevention and productivity in balance: The best of both worlds.

EXTENDED DETECTION AND RESPONSE

Security teams today face numerous challenges. Attackers are swiftly executing more sophisticated, stealthy, multi-vector attacks across multiple attack surfaces including endpoints, the cloud, networks, apps, and mobile devices. Endpoint detection and response (EDR) solutions created a defensive blueprint by delivering powerful threat detection and incident response capability for endpoints. However, a more proactive and comprehensive protection is needed across the entire attack surface.

This demand has driven the creation of XDR. It is an evolution of EDR, unifying protection at the endpoint with other security tooling. It gives security analysts improved visibility and high-efficacy detection, as well as more effective correlation, investigation, and response.

XDR is an evolution of EDR, unifying protection at the endpoint with other security tooling. It gives security analysts improved visibility and high-efficacy detection, as well as more effective correlation, investigation, and response.

WHAT IS XDR?

XDR products are, at their core, about data inclusion and enrichment strategies. This means that they incorporate information gleaned from their own product platforms, and integrate it with telemetry ingested from partners and other sources. This data is combined to create additional context, which is shared as actionable cyberthreat intelligence (CTI) within their product.

When leveraged for threat hunting, combining this novel intelligence allows XDR vendors to improve product capabilities and increase market opportunities. This threat intelligence enables products to proactively remediate risks, and then inform customers of the actions taken to protect their organizations. Better threat intelligence also allows product development to be proactive to customer needs and asks.

WHAT ARE THE BENEFITS OF XDR?

Enriched threat intelligence, gathered across the entire attack surface, can be contextualized to improve human and automated response actions. For example, a security analyst may lose considerable time sifting through alerts and threat data reported from multiple sources. An XDR platform could intelligently correlate threat data from across the environment and forward high-value information to analysts while filtering out noise. With enriched XDR data, the analyst has a better understanding of the environment and more time to make informed and effective security decisions.

XDR vendors like BlackBerry understand data and its meaning to the security community and to our customers, regardless of structure, origin, or location. We persist data in a structure that supports easy shared access and processing, so it can be utilized by all portions of our platform.

XDR vendors can ensure they offer the highest fidelity event alerting by having experts who understand and vet the data flowing in from multiple sensors. Professionally curated data allows for automated responses to prevent threats and provide remediation that continues to improve even as attacks grow more sophisticated.

HOW IS XDR DIFFERENT FROM SIEM?

The security operation center (SOC) team's typical approach of having security information and event management (SIEM) on top of all detection products has many shortcomings. SIEM solutions are good for collecting and storing logs to help with compliance and forensic use cases, but cannot generate high-fidelity detection alerts.

SIEM solutions do not produce and collect data natively. They simply consume data, without gathering or considering context. SOC teams must manually collect and correlate telemetry produced in silos, which results in low-fidelity alerts.

A new architectural approach is required to solve some of these modern SOC issues. This is where XDR comes into play. A vendor's sensor and security agent produce and collect most of the telemetry across the attack surface and centralize it into a cloud platform. This provides a repository of valuable threat data without requiring manual data ingestion, correlation, and enrichment.

When incidents occur, SOC analysts are often forced to squander critical response time manually stitching telemetry to build a timeline summary necessary for determining an attacker's intent. XDR solutions can enable automated threat hunting with pre-built attack stories. This automation reduces the time needed to detect and respond.

WHAT SHOULD A GOOD XDR SOLUTION HAVE?

XDR is a platform that unifies the capabilities of numerous disparate products into a single, simple, robust, and customizable experience. It represents the amalgamation of intelligence across native and third-party products, allowing for necessary response capabilities. In short, effective XDR products should:

- *Be customizable*
- *Allow aggregation of alerts*
- *Have response capabilities*
- *Have pertinent integrations*
- *Allow both native and cross telemetry*
- *Provide an excellent user experience*

Of course, even the best XDR solutions cannot stop threats by themselves. Some XDR platforms may include prevention-first technologies, AI-assisted analysis, and automation, but human specialists must still determine what qualifies as a threat in their environment.

All of the threat telemetry XDR gathers from primary and third-party solutions must ultimately be interpreted by trained analysts. This can make managed XDR services an appealing option to organizations operating with smaller cybersecurity budgets.

600%

Amount of increase in cyber crimes due to COVID-19.

THE EVOLUTION OF MANAGED DETECTION AND RESPONSE SERVICES

Increasingly complex and sophisticated cyberthreats are changing the way organizations approach cybersecurity. Some attackers are shifting their target focus from compromising infrastructure to exploiting individuals through increases in targeted phishing campaigns. This change, among others, means traditional defenses are inadequate for addressing the myriad of threat vectors exploited by contemporary adversaries. Organizations looking for detection and response partners today need vendors who can address a wide variety of advanced cyberattacks. A brief look at the threat landscape shows that organizations face an uphill battle:

- 667 million new malware detections were discovered worldwide in 2020.
- There was a 600% increase in cyber crimes due to the COVID-19 pandemic.
- 4 million additional cybersecurity workers are needed globally.
- 1 million daily security alerts are seen in 25% of SOCs.

Organizations are operating in an environment of constant change while threat actors quietly stalk them, looking for an opportunity to strike. Organizations must find a way to forge ahead without leaving themselves open to opportunistic cyberattacks. Managed detection and response (MDR) services can help organizations safely navigate the troubled waters of insecure technology and a hybrid or mobile workforce. MDR platforms offer 365x24x7 professional support for intrusion detection, incident response, and threat elimination.

The HAFNIUM attack of January 2021 offers a perfect example of how MDR assists organizations. During the campaign, at least 30,000 organizations in the U.S. were compromised by a Chinese cyber espionage unit, known as HAFNIUM. These attacks were largely automated, and targeted unpatched Microsoft Exchange Servers.

An MDR team could combat HAFNIUM by gathering and extensively researching all available threat intel feeds. Collected information might include IOCs, command lines, running processes, registry keys, DNS requests, and more. The MDR team would then perform additional threat hunting. For example, BlackBerry teams would continue searching for threats by using tools like InstaQuery, which is carried out via API.

Through information gathering and threat hunting, an experienced MDR team can quickly identify a specific cyberthreat. They quickly provide their customers with remediation instructions and best practices, as well as offer updates as more information becomes available. Proactive MDR teams could even set up a series of HAFNIUM-specific rules directly in an EDR tool–rules applying the techniques found in the MITRE ATT&CK® framework, for example.

Given the evolving and sophisticated threat landscape, the need for analysts to have holistic visibility and telemetry across security tools has increased. Managed XDR builds on the MDR services framework by incorporating XDR visibility across the enterprise. XDR platforms unify security-relevant endpoint detections by collecting and contextualizing threat telemetry across third-party tools. For example, an XDR platform might collect and analyze data from network sources and SIEM, email security, identity and access management, next-generation firewall, and more. Managed XDR is cloud-native and built on a Big Data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation. A managed XDR can offer SMBs a level of protection that few organizations can otherwise afford. For example, a managed XDR may provide:

Technical experts and experienced cybersecurity analysts

Advanced cybersecurity solutions that harness the predictive power of AI and ML

365x24x7 threat monitoring across the environment, endpoints, and users

Rapid incident investigation and mitigation

Expert threat identification and hunting across all attack surfaces

Managed XDR can offer organizations around-the-clock access to seasoned cybersecurity professionals using state-of-the-art threat detection and response tools. This can give organizations considerable peace of mind and allow them to focus on their primary mission instead of worrying about cyberattacks.

EXPANDING THE ROLE OF NETWORK SECURITY AND AI/ML IN PREVENTING ZERO-DAY ATTACKS

The network has been the carrier of the most targeted and highly exploited vulnerabilities of 2020 and 2021. In 2020, several of these vulnerabilities affected remote work, VPNs, or cloud-based technologies. In 2021, malicious cyber actors continued to target and compromise perimeter-type devices. Highly exploited vulnerabilities were discovered in many popular cyber platforms, including those of Microsoft, Pulse, Accellion, VMware, and Fortinet. This run of successful attacks resulted in an increased focus on securing and protecting network connectivity.

Organizations are turning to newer cybersecurity approaches such as Zero Trust Network Access (ZTNA), Secure Access Service Edge, and XDR. At a macro level, the MITRE ATT&CK framework has also provided resources that improve the attack coverage for network-specific vulnerabilities. Zero-day attacks have encouraged security analysts to combine defenses and technologies to strengthen security measures. Among the approaches being used are:

- Prevention-first technology
- Protection-first approaches
- Signature-based analysis
- AI- and ML-based anomaly and threat detection in the network layer
- Advanced correlation across multiple telemetry sources

The network fabric is also facing major changes. VPN solutions that are IPSec-based have been a flash point for several recent exploits, highlighting the necessity for secure and modern TCP/IP stacks. Similarly, a purely signature-based approach to malware requires at least one user to become infected so a malicious sample can be obtained. This has driven the rise of AI and ML approaches, which can analyze threats in the network layer and prevent zero-day attacks.

THE ROLE OF AI AND ML

In network threat detection, AI and ML play an important role by modeling the normal behavior of the organization and its users. They then detect anomalies that do not match the behavior of any authorized user. They can also predict whether a particular networking behavior has lower or higher probability of being associated with a specific user. This provides an effective way to identify C2 beacons, for example, and differentiate them from benign process and user-initiated network usage. This AI-driven, model-based anomaly detection and user-specific prediction capability can reduce both false positives and false negatives.

THE MALICIOUS INSIDER

For malicious insiders, anomalous access detection and predictive behavior modeling on their own may be less effective. The malicious insider will often conform with their own past behavior and may share many characteristics with otherwise normal user and organizational access. However, overtly malicious, aberrant, or suspicious behavior may still draw attention.

THE MALICIOUS OUTSIDER

AI modeling is highly effective against malicious outsiders, like those who access an unlocked device surreptitiously or obtain illicit access to legitimate user credentials. It is much less likely that a malicious outsider's behavior will continuously conform to the compromised user's modeled behavior. It is also likely the outsider's behavior will conflict with those of the organization as a whole. They may log in outside of normal work hours, access new resources, or perform atypical actions such as attempting to download databases that quickly identify them as threats.

MALWARE

As with malicious outsiders, anomalous or low-probability endpoint access by malware can trigger detections. Alerting the legitimate user to the malicious activity allows them to halt access and report the issue to their SOC. In addition, malware and its associated C2 exhibit networking patterns that are atypical of legitimate, user-driven behavior. For additional protection, threat behavior may be separately modeled for increased detection. Configuring automated response actions to modeled threat behavior protects the environment in cases where the legitimate user does not reject suspicious access attempts.

RULES-BASED NETWORK THREAT DETECTION

Holistic network protection includes a combination of AI and ML technology and rules-based network threat detection. For example, IDS/IPS traffic can be used to analyze, assess, and filter communications. Traffic can be assessed by pre-created rules, like SNORT, then deployed to prevent and detect malicious traffic. A rule can be associated with a corresponding response action such as alert, allow, or block. Typically, SOC admins maintain visibility into the actions performed by SNORT or similar rules. Rules-based detection by itself can significantly increase the MITRE ATT&CK coverage in areas such as privilege escalation, lateral movement, command-and-control, data exfiltration, etc.

MICROSOFT HAFNIUM

The state-sponsored threat actor HAFNIUM utilized patch vulnerabilities in on-premises Microsoft Exchange Servers to compromise email accounts. Within days, malicious actors beyond HAFNIUM began targeting unpatched systems and installing malware to ensure long-term access to compromised environments.

A combination of prevention-first cybersecurity and fast detection technology can thwart HAFNIUM-style attacks. Specifically, the vulnerabilities exploited by HAFNIUM could have been protected by:

- ZTNA principles
- A least-privilege approach to access
- An identity-aware network platform
- Continuous authentication and adaptive access technology
- Remote work solutions that authenticate access to individual applications, not the entire network

VPN EXPLOITS

Zero-day VPN exploits hammered the industry in 2021, from Sonic VPN, to Pulse Secure, to Fortinet VPN. While several of these vulnerabilities have existed for a while, recent work-from-home and remote access trends have brought them increased attention. As a technology attracts more users and organizations, it becomes increasingly valuable to threat actors.

To avoid VPN exploits while supporting a remote and mobile workforce, organizations should consider adopting:

- A software-defined Zero Trust network architecture
- A network built upon a robust TCP/IP stack
- Securing connectivity using the principles of least privilege access
- Solutions offering segmented network access control to separate professional and personal network traffic
- Dynamic access controls that can provide just-in-time access to a platform that offers full visibility into network traffic across on-premises and cloud resources

MOBILE THREATS AND SECURITY

76%

According to recent studies, a staggering 76% of tested mobile applications store data insecurely.

Mobile device security should be a serious concern for every organization. Consider the current state of the smartphone market, which is divided between Android™ and iPhone® devices. According to recent studies, a staggering 76% of tested mobile applications store data insecurely. Insecure apps threaten organizations with BYOD policies, and those supporting mobile or remote workers. The danger arises from employees increasingly using unmanaged personal devices to perform professional tasks. When business resources and vulnerable apps occupy the same device and connect to multiple networks, there are many opportunities for disaster.

Vulnerable apps are not the only mobile threat facing organizations. When personal devices store or access organizational resources, there is a risk that enterprise data may be unintentionally exposed. Leaks could be as simple as forwarding sensitive emails to the wrong address, or as serious as revealing user credentials and personally identifiable information. Data leakage can occur through other avenues as well, paired Internet of things (IoT) devices and unmanaged network access points (such as public Wi-Fi), for example.

Unpatched and out-of-date software also poses a serious risk to mobile devices. In March 2021, Android file-sharing app SHAREit was revealed to contain vulnerabilities allowing remote code execution. Threat researchers were aware of the problem and notified the developers in December 2020, but no updates were issued. By the time threat researchers revealed the vulnerabilities publicly, SHAREit had over one billion downloads.

Mobile devices in North America saw a 300% increase in smishing attacks, or phishing attacks via SMS, during the third quarter of 2020. This increase jumped to 700% in the first six months of 2021. Smishing attacks arrive as an SMS text message, allegedly coming from a trusted contact, and often contain malicious links. For example, a victim could receive a text claiming to come from their bank, that states their account is overdrawn. The text contains a malicious link and urges the victim to tap it for details. If the link is clicked, the victim may initiate a malware download or have their information captured. These attacks are easy to perform since all the attacker requires is the victim's phone number. SMS messages also truncate URLs, making them harder to visually inspect for warning signs.

Recently, the deceptive practices of phishing and smishing have evolved into an even greater threat–malicious applications posing as legitimate programs. This trend has been particularly noticeable with banking, cryptocurrency, and trading apps. Malicious applications installed by users enjoy the benefits of implicit user trust. Since the app receives the user's permission to install and execute, it can be difficult for traditional cybersecurity approaches to detect. Detection may be further complicated when malicious apps are downloaded from trusted platforms.

AI TACKLES MOBILE THREATS

Organizations faced many security challenges trying to support a remote and mobile workforce in the wake of COVID-19 lockdowns. Since then, the workforce has remained in flux, leaving many organizations searching for effective ways to combat mobile threats.

One promising approach is adopting AI-driven solutions that use mathematical modeling and predictive analysis to detect and prevent numerous types of threats. For example:

- **Vulnerable code in apps.** AI can extract file features from an application before it executes, and block those containing malicious or exploitable code. This protects users from malware as well as buggy applications relying on vulnerable open-source or third-party code.
- **Data leakage.** Intelligent gateway platforms can offer full/split tunnel capabilities that encrypt communications for sensitive data but leave trivial communications open. AI plays a vital role in selecting how network traffic is classified, removing the risk of human error causing unintentional data leaks.
- **Out-of-date software.** AI can monitor devices for outdated software versions and misconfigurations. These checks ensure the OS, system libraries, and firmware remain updated.
- **Vulnerable access points.** AI can analyze the security of Wi-Fi access points to ensure mobile traffic does not traverse insecure public or private networks.
- **Phishing/smishing attacks.** AI can quickly determine the safety of URLs, preventing users from unknowingly browsing to unsafe locations.
- **Malicious apps.** AI can detect malicious apps before they are loaded or execute on a mobile device. This proactive ability to stop malware is a feature of prevention-first cybersecurity.

While no solution is 100% effective against all attacks, AI can effectively address many of the threats facing mobile technology. AI can continuously make informed security-related decisions in the background, allowing users to focus on productivity. AI can also monitor connections and network traffic to ensure communications remain protected while users travel wherever their jobs require–or work wherever their travel requires. Because AI is an adaptive technology, it is well-suited to respond to both known threats and those which emerge during times of disruption.

CONNECTED VEHICLES–MOVING TOWARD SECURITY

The transformational changes occurring in personal transportation underscore the need to address the security requirements of these rolling network data platforms. The auto industry is exploring constructive uses for AI, including its ability to perform critical cybersecurity tasks.

Understanding how prevention-first AI cybersecurity integrates into connected driving is best done by breaking the technology down into the individual elements of prevention and AI. Each can be implemented independently of the other. Likewise, there is work that must go into each element in order to properly deploy them in connected driving.

PREVENTION OF CYBERSECURITY ATTACKS

The first step in securing any system is designing and building it in a way that minimizes the likelihood of security vulnerabilities. This sentiment is reflected in some recent guidelines set forth by ISO and the UN:

- ISO/SAE 21434, published in August 2021, sets the standard for handling security during vehicle design, manufacturing, use, and decommissioning.
- UN R155 enforces that cybersecurity be considered, not just in the automotive platforms, but in the surrounding infrastructure, as well.

Prevention and detection of threats, however, are not diametrically opposed. There are vulnerabilities which will not be found during system design and development. Preventing these unidentified vulnerabilities from being exploited involves detecting an attack against the system and preventing it from progressing. The possibilities for preventing malicious behavior will be impacted by whether the electronic system is safety critical.

Some electronic systems in modern vehicles must be safety certified. ISO 26262 defines Automotive Safety Integrity Levels (ASIL) A through D. Hazardous events are classified according to their severity, exposure, and ability to control the vehicle if the event occurs. For these safety-critical electronic systems, any modification to their behavior to prevent malicious attacks (including introducing a new prevention) requires a re-certification of the system. Re-certification involves performing a hazard analysis for every prevention action that might be taken. For electronic systems that are not safety-critical, changing system behavior to prevent ongoing malicious activity is more straightforward.

For safety-critical electronic systems, any modification to their behavior to prevent malicious attacks (including introducing a new prevention) requires a re-certification of the system.

Typically, the implementation of intrusion detection precedes intrusion prevention in new environments. It allows monitoring and refinement of the system without adverse consequences, until we are confident in its operation and can enable prevention-based approaches.

USE OF AI

With AI, the same important distinction between safety-critical systems and other vehicle systems arises. The use of AI within safety-critical systems is still being debated. One of the challenges of using AI in a safety context is in understanding the resulting system behavior. Safety assurance relies on understanding how the system will respond to its inputs. An ML-based AI system, where the behavior is not well understood, introduces intellectual debt. A system with intellectual debt is deeply concerning for safety engineers responsible for certification. Attacks such as adversarial machine learning highlight the designer's inability to fully understand how all inputs may affect the actions of the AI system. Data used to train the system might also be the target of attack, or not representative of changing real-world conditions. It is, therefore, critical to not treat new AI systems as infallible, and to understand why they fail when they do.

Reconstructing the state of a system using AI to perform post-incident analysis and discover why it failed will require significantly more resources in many areas. Considerable work still needs to be done in reducing the intellectual debt related to AI. The Safety of Autonomous Systems Working Group has published guidance on safety assurance of autonomous systems. ISO TC 22/SC 32 has several working groups (WG13 and WG14) which are examining the safety of AI and autonomous driving. Issues with using ML-based AI in a safety critical system include threats to the AI itself and to the data used for training or in production.

We expect, therefore, that AI-based cybersecurity will find inroads outside the safety-critical components of the vehicle before inclusion in safety-critical components. The BlackBerry IVY™ platform is designed to facilitate the introduction of AI into the vehicle, providing intelligent insights to enhance driver and passenger experiences.

The vehicle is only one component in the connected vehicle network. Other systems include charging infrastructure, connected intersections, and even route finding.

ADDITIONAL AREAS REQUIRING ATTENTION

The vehicle is only one component in the connected vehicle network. Other systems in the connected vehicle network include charging infrastructure, connected intersections, and even route finding. Currently, most route finding is done through smartphones as opposed to being integrated into the vehicle. Autonomous driving at higher levels is going to require route finding be built into the vehicle. In all of these support networks, AI can be used to make decisions based on the data. There is the potential for cyberattacks on these networks as well. Factors such as safety will continue to influence decisions on how to best protect these networks against cybersecurity threats.

Prevention-first AI cybersecurity does not need to focus exclusively on production environments. Preventing the introduction of vulnerabilities during software design and development, including those of AI systems, is another avenue through which cybersecurity can be improved. The use of AI continues to be researched for fuzzing and other static/dynamic application security testing (SAST/DAST) analysis tools.

Work is underway within ISO and SAE to determine the necessary cybersecurity assurance level for various components in the vehicle, based on the cyberthreats they may face. Higher assurance comes from an increased focus in the proper design, development, and testing of systems. This will ensure that the chance of vulnerabilities remaining undiscovered is minimized.

The increased focus on the proper design, development, and testing of software is not unique to just connected vehicles. With malicious cyber campaigns increasingly being waged against the private and public sector, the focus on improving cybersecurity extends to all critical software.

CRITICAL EVENT MANAGEMENT–BE PREPARED FOR ANYTHING

For many organizations, the pandemic brought home the reality that massively disruptive critical events can happen at any time. The pandemic, however, wasn't the only disruption in the last 12 months. Supply chain disruptions, civil unrest, utility outages, natural and man-made disasters, and even extreme weather were consistently occurring throughout the year, and throughout the world. In addition to physical events, cyberattacks and other IT disruptions have pummeled business-critical systems, according to a report by Aberdeen. Supply chain and utility disruptions of the past were often the result of "upstream and downstream" logistic or power transmission issues. Today, cyberattacks increasingly play a role in such disruptions.

A number of high-profile cybersecurity incidents were reported in the first half of 2021, including:

- **Colonial Pipeline.** The Colonial Pipeline Company, owners of the largest fuel pipeline in the U.S., fell victim to DarkSide ransomware in May 2021. The attacks disrupted operations and forced the company to shut down its pipeline system for several days. Colonial Pipeline paid $5 million in ransom, of which $2.3 million was later recovered.
- **Florida's water supply.** In February 2021, a cyber criminal infiltrated the water plant system for the town of Oldsmar. The attacker tried to poison town residents by increasing the sodium hydroxide content in the water supply to dangerous levels. A plant operator noticed the increasing sodium hydroxide levels and reversed the attack before anyone was harmed. Federal authorities are still looking for the attacker.

Colonial Pipeline Company, owners of the largest fuel pipeline in the U.S., fell victim to DarkSide ransomware in May 2021, forcing the company to shut down its pipeline system for several days.

- **Australia's Channel Nine.** The Australian broadcaster, Channel Nine, had its programs taken off the air by a cyberattack in March 2021. The company struggled with the issue for several hours before finding a workaround allowing it to broadcast again.
- **Accellion supply chain attack.** Attackers breached the Accellion file transfer system early in 2021. Through this breach, cyber criminals were able to steal data from multiple organizations.

Many organizations, unfortunately, are ill-prepared for these kinds of critical events. The headline-grabbing attacks on supply chains and critical infrastructure in 2021 raised some serious questions for organizations worldwide. Can these types of incidents be prevented in the future? If so, how? What steps could organizations have taken to be better prepared to respond to them?

To address similar cyber incidents, forward-looking organizations are investing in recruitment, training, and equipping their security analysts to staff "fusion" operation centers. These centers handle critical events related to cybersecurity and IT as well as non-technical issues. Their fused responsibilities extend to critical events traditionally managed by an emergency operations center, such as civil unrest, natural disasters, and safety incidents. They work around the clock performing important functions, including:

Intelligence Gathering

Threat Assessment

Impact Analysis

Situation Monitoring

Incident Management

Operating a well-staffed fusion operation center is just one aspect of critical event response. There are other challenges to consider. Organizations still need to ensure there are reliable processes for reaching stakeholders, interoperable response systems, and integrated non-SOC systems.

Successful critical event management (CEM) relies on swift communication and collaboration with all affected stakeholders. All involved staff and third-party vendors need to be familiar with the organization's standard operating procedures prior to a critical event occurrence. Conducting simulated crisis management exercises can raise awareness, preparedness, and ultimately reduce the impacts of critical events.

CEM isn't confined to large-scale disasters, but includes addressing events with a potential to deteriorate and escalate into serious situations. Having a secure, reliable, end-to-end CEM platform can help to mitigate any potential oversights that could later prove costly. It ensures risks are understood and addressed, stakeholders are adequately prepared, threat monitoring feeds are effectively integrated, and resources can be quickly deployed.

Critical Event Management (CEM) isn't confined to large-scale disasters, but includes addressing events with a potential to deteriorate and escalate into serious situations.

Consider the escalating frequency and severity of ransomware attacks. During such an attack, an organization's critical data is encrypted and, in some instances, exfiltrated. Threat actors demand a ransom payment for the encryption key to unlock the data, and an assurance the data will not be further circulated. If an organization does not comply, the attackers may use the data for blackmail, leave it encrypted, or release it to the public. Whether the threat actors keep their end of the bargain after a ransom is paid is, of course, a gamble.

Using a CEM platform in this situation, pre-identified stakeholders would already be familiar with the expected response procedures. As the incident unfolds, security analysts will attempt to trace the initial source and identify affected endpoints. An automated workflow can send out notifications to potentially impacted users. These notifications may include the nature of the incident, specific warning signs, ways to report issues, and any workaround measures. A progress status could even be incorporated to provide a quick overview to assist the incident manager.

Externally, regulators, law enforcement, identified service users, or other partners could be notified on the current progress of the incident. Suppose the affected organization is a critical care provider, such as a hospital, or a public safety organization. A CEM platform would mean having the capacity to effectively ensure that critical services can continue to operate. For example, an ambulance's on-board mobile data terminal could be integrated to ensure continuous dispatch of critical information such as patient location and data. This could happen while the organization is simultaneously struggling to contain and resolve a major disruptive event, like a cyber incident. A CEM platform provides the capability to better manage operational disruptions and ensures continuous service delivery when threats materialize.

According to Gartner's 2021 CIO survey, 64% of employees are able to work from home and 40% are already doing so. For this group of stakeholders, the ability to communicate and receive vital information during a cyber incident or other critical event is crucial. While risks cannot be totally eliminated, adopting CEM technology helps augment current preparedness and prevention initiatives, and improves organizational resilience.

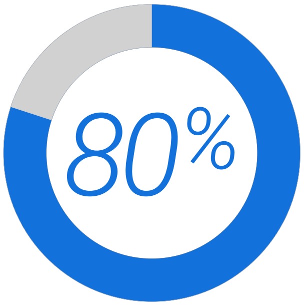
For organizations without a CEM platform, or those wishing to augment their capabilities, acquiring CEM capabilities as a managed service may be an attractive option.

NEW CYBERSECURITY LEGISLATIVE AND REGULATORY INITIATIVES AND FORECAST

Cybersecurity is now at the top of the public policy agenda for G7 countries and NATO allies. Successive and increasing cyberattacks on pipelines, hospitals, airlines, supply chains, and essential services, highlight the urgent need to protect critical infrastructure, businesses and citizens. In 2020/21, governments in the U.S., U.K., France, Japan, Italy, Australia and Germany collectively pledged billions of dollars and introduced new measures to strengthen their cyber resilience.

In the U.S., the Biden Administration issued an Executive Order in May 2021 designed to bolster cybersecurity initiatives across the federal government. President Biden nominated a national cyber director to oversee digital security policy and issued new measures to protect and secure Federal Information Systems. He also strengthened the authority of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to respond to major cyber incidents. Meanwhile, Congress has passed legislation to codify and fund some of these efforts.

The European Union is considering broad cybersecurity legislation covering networks, critical infrastructure, and new security certifications for IoT products. In Canada, the Federal government has committed to draft a new national cybersecurity strategy, pass new legislation to bring cyber criminals to justice, and boost Federal cyber capabilities. However, businesses and industry groups are calling on the Federal government to do more by making cybersecurity a top policy priority. The support for stronger measures is high, with 92% of Canadians saying that the government should prioritize cybersecurity investment. More than 80% of Canadian CEOs cite cybersecurity as a major threat to their company's growth prospects.



More than 80% of Canadian CEOs cite cybersecurity as a major threat to their company's growth prospects.

Indeed, implementation of laws enacted in 2021, including the rollout of significant cybersecurity investments, will continue into 2022 and include:

- Software supply chain security requirements
- Consumer-oriented cybersecurity labeling programs
- Compliance related to securing critical infrastructure sectors
- Measures to protect government networks and critical infrastructure from cyberattacks
- Improvements to public-private collaboration on cybersecurity initiatives
- Accelerating efforts to equip government agencies with the cyber capabilities that they need to respond to rapidly evolving cyber risks and cyberthreats

Government contractors and companies in regulated industries such as energy, transportation, finance, healthcare, and defense are likely to see additional cybersecurity requirements implemented first. Governments tend to deem these sectors highest risk for cyberthreats that could result in widespread economic, national security, and societal impact.

UNITED STATES

2021, like 2020, was another landmark year for cybersecurity incidents and, therefore, cybersecurity policy initiatives in the U.S. As noted above, President Biden issued an Executive Order on "Improving the Nation's Cybersecurity" (EO 14028). The EO called for and has led to new guidance on enhancing software supply chain security, among other key cybersecurity initiatives. It launched a multi-federal agency process to determine the appropriate framework for requiring a Software Bill of Materials for software sold to the federal government. The EO also instructed federal government agencies to transition to a more secure, Zero Trust IT architecture, among other things.

Additional U.S. government action in 2021 included new cybersecurity requirements for critical pipeline owners and operators, high-risk passenger, freight rail, and rail transit operators, large airports, and aircraft operators; an Industrial Control Systems Cybersecurity Initiative by DHS, in coordination with the Department of Commerce; establishment of a Ransomware and Digital Extortion Task Force by the Department of Justice; and a series of 60-day sprints to tackle ransomware and cybersecurity workforce issues. The President also convened representatives from 30 countries for a White House summit to discuss collaborative actions to counter ransomware.

In the wake of massive cyber vulnerabilities exposed by SolarWinds, Microsoft Exchange, JBS Foods, Colonial Pipeline, Log4j, and other high profile and high impact cyberattacks, Congress remains keen to raise the bar on cybersecurity to protect both the public and private sectors.

Some of the most notable U.S. public policy developments for enterprise security decisionmakers to consider include:

- **Cybersecurity-related provisions in the FY22 National Defense Authorization Act** designed to improve the ability of the Department of Defense (DOD) and DHS to identify, deter, protect against, detect, and respond to malicious cyber campaigns threatening the public sector as well as privately-owned critical infrastructure. This includes requiring DOD to develop a Zero Trust strategy and model architecture for its Information Network and expanding eligibility for DOD funding and technical support to owners of critical infrastructure. DHS, including CISA, will also expand efforts to address cyber risks and enhance cyber incident response, particularly concerning industrial control systems. It will roll out a program that provides continuous monitoring and detection of cybersecurity risks to critical infrastructure entities, and establish a national cyber exercise program designed to aid both government and industry incident response planning.
- **Cybersecurity requirements to harden the pipeline, railroad, and aviation sectors** against threats in cyber space. For example, in December 2021, the Transportation Security Administration rolled out new rules requiring high-risk rail, large airports, and aircraft operators to adopt new processes. These include reporting cyber

incidents to CISA, identifying a cybersecurity coordinator, conducting vulnerability assessments, and developing contingency recovery plans to be implemented in the event of a cyberattack.

- **New software supply chain security requirements** included in the President's Executive Order are starting to take shape as multiple government agencies are beginning to tackle this challenging issue. These rules will initially affect federal contactors. While focused on federal procurement, heightened software security requirements are likely to spill over into private sector practices and requirements as well.

Government initiatives likely to pick up steam in 2022 include the development of additional cybersecurity requirements for the transportation, energy, telecommunications, and financial sectors. Should new rules or laws materialize, owners and operators across these sectors will be obliged to dedicate more resources to meet new cybersecurity requirements. Some Members of Congress will press for increased federal consultation with industry stakeholders in the development of these requirements. Industry should also expect bipartisan proposals to enact cybersecurity incident notification and reporting mandates for critical infrastructure operators and owners, and possibly others. Multiple such proposals were debated in 2021 and are likely to be revisited in 2022.

$1B

Amount authorized in the Infrastructure Investment and Jobs Act to fund cybersecurity grants for State and Local governments.

Finally, government at all levels is expected to continue to move quickly to invest in IT modernization, including cybersecurity. These funds are flowing via the American Rescue Plan Act signed into law in March 2021, which enlarged the Technology Modernization Fund, and the Infrastructure Investment and Jobs Act signed into law in November 2021. Several provisions of this new law make infrastructure funding contingent on investment in and planning for cybersecurity for the very first time. Local and state governments, likewise, will benefit from $1 billion authorized in the Infrastructure Investment and Jobs Act to fund cybersecurity grants for State and Local governments.

CANADA

Like the U.S., cybersecurity is one of the most pressing challenges facing Canada. For decades, experts have warned about the dangers of cyberattacks. Today, cyber breaches have become disconcertingly routine. Rightfully, Canadians are worried. Notably, falling victim to a cyberattack now ranks second behind job loss on the list of things Canadians worry about most. In the past year, Canadian businesses, hospitals, universities, transit systems, cities, and government services all have experienced significant cyberattacks.

Addressing cybersecurity shortfalls is a high priority for Canadians, as integral to building a more resilient, innovative, inclusive, and vibrant economy. Industry groups are raising concerns about the ever-growing set of cyberthreats. They are calling on the government to invest in cybersecurity at a level on par with Canada's G7 peers, and have produced detailed recommendations on how the public and private sectors can collaborate to enhance cybersecurity in Canada.

The Trudeau government has committed to draft a new National Cyber Security Strategy and develop a National Cyber Security Action Plan. It will advance legislation to counter cyber crime and enhance privacy safeguards, and equip the Canadian Security Establishment with the tools it needs to respond to a rapidly evolving cyberthreat landscape. However, many in industry, including the Canadian Chamber of Commerce, are pressing the Government of Canada to do more to protect critical infrastructure, businesses and communities. Among these recommendations are calls for the government to:

- **Increase the cyber resiliency of critical infrastructure.** As noted in BlackBerry's 2021 Threat Report, Canada's Critical Infrastructure Strategy is old, dating back to 2009. Public Safety Canada has initiated consultations to renew and update this strategy, but this could take several years to finalize. In the meantime, Infrastructure Canada is moving forward with a National Infrastructure Assessment, which sets government priorities for infrastructure investment for years to come. Cyberattacks on Newfoundland and Labrador's health system and on Toronto's transit authority in 2021, served as an 'alarm bell' for Canada to increase investment in cybersecurity for critical infrastructure. Transport Canada has made progress on vehicle cybersecurity by issuing concrete guidance and characterizing cybersecurity as a foundational element of road safety and security. However, more cybersecurity-related guidance and regulation are expected for rail, marine and aviation sectors given the lack of attention to date.
- **Help Canadian businesses invest in cybersecurity.** In April 2021, the Federal government pledged $4 billion dollars to the Canada Digital Adoption Program. These funds are intended to help 160,000 small and medium-sized businesses buy and adopt the new technologies they need to grow. This was a welcome initiative for many, as COVID-19 thrust businesses into an unprecedented reliance on digital technology to support remote work and e-commerce. However, these same businesses experienced an unprecedented spike in cyberattacks. To fully harness the potential of the Digital Adoption Program, cybersecurity must be made an essential element of this program. By leveraging the deep expertise and talent of Canada's private sector, Canada can raise the cybersecurity bar and equip small and medium-sized businesses with best practices and tools they need to thrive in a data-driven economy. This will also help Canadian businesses comply with a new federal privacy and data protection law, which is likely to be proposed in 2022.
- **Improve government-wide coherence and action on cybersecurity.** As it stands today, cyber responsibilities in the Federal Government are distributed across at least 12 Federal departments and agencies. Creating coherence across government to ensure that all departments operate with a unity of effort and purpose is

essential to fostering cyber resilience. BlackBerry, together with other leading technology companies, has called on Canada to consider establishing a senior government position like the new U.S. National Cyber Director. This office would help elevate cybersecurity in government policy and foster cyber resilience by enhancing coherence and collaboration across government. In 2022, we expect increased attention to the development of strategies and mechanisms that facilitate the implementation of a cohesive cybersecurity strategy across the whole of government. Doing so will help the government move from a reactive incident response mindset to a prevention-first approach that will position Canada as a leader in cybersecurity.

EUROPEAN UNION

In 2021, the EU continued its proactive approach to address cybersecurity vulnerabilities. The EU Cybersecurity Strategy, published at the end of 2020, introduced new measures to enhance collective cyber capabilities. Steps included the creation of a new security operations center called the Joint Cyber Unit where public authorities in the EU can network and collaborate to respond to cyberattacks. In addition to new cybersecurity initiatives and requirements for government, industry will be impacted by revisions to the EU Network and Information Security (NIS) Directive and legislation regulating cyber incident reporting requirements for critical operators.

In 2022, there will be a continued focus on:

- A Commission proposal to address the deficiencies of the Network and Information Security (NIS) directive. Notable changes include an expansion in the scope of entities covered under the directive. These will now include providers of cloud-based services, telecom and electronic communications, intelligent transport systems and autonomous vehicles, as well as space technology. The directive also will include more restrictive cybersecurity and risk management standards. Changes impact encryption and supply chain security, as well as requiring mandatory cyber incident reporting within strict timelines. New cybersecurity product certification measures for the private sector also are anticipated. Non-compliance could result in GDPR-equivalent fines.
- An EU-wide cybersecurity certification framework, which will specify security assurance levels for ICT-based products and services for both consumer and industrial applications. Current focus areas include cloud security, 5G security, IoT, and artificial intelligence.
- The EU is also expected to announce a new *EU Cyber-Resilience Act* aimed at setting new duty of care requirements for software and data in ICT devices for manufacturers. This proposal includes IoT devices and software. The goal is to ensure security throughout the lifecycle of ICT products, from development to end-of-life.

PREDICTIONS: LOOKING AHEAD TO 2022 AND BEYOND

While it is impossible to predict the future, we asked our experienced BlackBerry experts to share their thoughts on issues that may soon impact cybersecurity. Here are some of the topics our professionals will be watching as we enter 2022.

QUANTUM COMPUTING

The continued advancement of quantum computing may be as disruptive to the cybersecurity space as AI is today, particularly when future quantum computers can crack modern encryption schemes in minutes or seconds. Envisioning the overall impact of quantum computing on cybersecurity is difficult, but one could begin by imagining encryption no longer being a factor. This could be catastrophic, as private and public organizations would lose a valuable tool for protecting stolen data from attackers.

Yet, there is another way to look at this problem. Data and communications are usually encrypted because of the general belief that motivated attackers will get to them. This ignores the possibility that other aspects of cybersecurity may improve to the point where data remains fully protected. For example, consider technologies fostering a strong prevention-first approach to security, one which identifies and shuts down attacks before they execute. If the attackers can never reach the data, then it does not matter whether it is encrypted or not. In this way, the advancement of other technologies could offset the impending loss of encryption due to quantum computing.

COVID-19-THEMED ATTACKS

It is not difficult to predict a continuation of COVID-19-themed attacks persisting for the duration of the pandemic. When a disruptive event occurs, there will always be some opportunistic element trying to profit or gain from the ensuing chaos. What is more difficult is forecasting what the COVID-19-inspired attacks of 2022 may look like when they arrive. One possibility is to consider the new COVID-19-related technologies that will emerge, and anticipate cyberattacks on those fronts.

For example, it is not unreasonable to assume that COVID tracking technologies will continue to be developed throughout the pandemic. These new technologies will have been quickly developed and implemented, making them tempting targets for threat actors. Likewise, should immunization passports or similar policies take hold in regions, the technological infrastructure behind them may draw the attention of threat actors.

It’s not unreasonable to assume that COVID tracking technologies, which have been quickly developed and implemented, make for tempting targets for threat actors.

GOVERNMENTS UNDER PRESSURE TO ADAPT

Governments are facing increasing pressure to change their approach to combating cyberattacks. Attackers are quickly adopting new TTPs to obfuscate their operations and exploit their targets. Hostile nation states, once content to conduct their own cyber warfare, now frequently outsource their attacks to third-party services or groups. This makes attributing a particular attack to a specific threat actor increasingly difficult. Likewise, some threat groups study the TTPs of other adversaries, and then mimic their behaviors and use their tools to foster misidentification.

Governments relying on legacy technology and approaches to cybersecurity are finding themselves continuously playing defense. Faced with a situation where their assailants are unknown and their technology is reactive, it becomes increasingly likely governments will adopt more aggressive measures. What these measures may be is unclear, but could include prevention-first security tools, Zero Trust frameworks, and more intrusive monitoring.

Future changes to the SOC will likely come down to two separate but intertwined components: people and technology.

CHANGES TO THE SOC

Future changes to the SOC will likely come down to two separate but intertwined components: people and technology. Driving the changes relating to people, cyberattacks have become increasingly sophisticated, which means the analysts employed to detect them must likewise evolve. The days when security personnel could be considered qualified for simply understanding how to interpret an SHA-256 are gone. The SOC analysts of today and tomorrow need a deeper understanding of adversarial techniques. They must not only be able to spot an attack, but also understand where it came from and where it is going.

This need for increased knowledge will drive the change in SOC technology. For example, modern SOCs focus less on singular products and more on capabilities. This is why XDR and managed XDR is commanding more attention. The capability of a platform to integrate threat telemetry from multiple sources, including third-party solutions, and deliver it to analysts is crucial. You need both analysts that understand sophisticated attacks and solutions that identify and deliver relevant information, regardless of where the threat data resides. We predict the SOC will continue to favor highly trained analysts and security platforms that prioritize capabilities over individual product strength in 2022.

SECURITY IN THE METAVERSE

Much could be said about the wisdom of creating a hybrid-reality where human interactions and status largely exists in a virtual capacity. From a security perspective, it is important to remember one simple truism: People will trade security for convenience. A prime example of this can be seen in the GPS functionality of smartphones. Anyone can deny an attacker (or company) information on their geographical location by simply turning off their phone's GPS location services. Yet, anyone trying this quickly discovers many of their applications simply stop working. This means, for the sake of convenience, people leave GPS enabled on their phone, even though mobile apps are notoriously insecure.

Now, consider how much greater the risk becomes when it is not simply a cellphone location, but one's entire life being monitored. If information can be misused for profit or gain, there will always be an element of society waiting to steal or exploit it. The Metaverse requires considerably more user interaction than a cellphone. Therefore, it is not unreasonable to assume it would collect much more information and attract many more attackers as well. For security to succeed in the Metaverse, it will have to be implemented in a way that is robust without negatively impacting user convenience.

For security to succeed in the Metaverse, it will have to be implemented in a way that is robust without negatively impacting user convenience.

FUTURE OF CYBERTHREATS

Attackers will continue to exploit events that cause organizations to be more vulnerable than usual. This applies to both unforeseen global crises like COVID-19 and more predictable occurrences like natural disasters or scheduled holidays. When an organization's security operations are disrupted, it is more likely to draw the attention of threat actors who sense an opportunity.

Threat actors will also continue mimicking the successful strategies and trends they observe in the business world. For example, we are seeing more malware built to run in cloud architecture. Offerings like RaaS and malicious IaaS are growing. IABs have emerged to help common criminals execute more successful campaigns, and to aid nation states and other powerful organizations seeking to conduct cyberattacks surreptitiously and maintain plausible deniability. Threat organizations are becoming increasingly resilient, as we can see from Emotet, which has returned after a complete international government takedown in January of 2021. Based on these factors, we predict technologies and trends increasingly favored by organizations are likely to remain prime targets for threat actors in 2022.

CONCLUSION

CONCLUSION

Organized attacks on critical infrastructure and large organizations made headlines throughout 2021, with ransomware playing a key role. Threat actors demonstrated their ability to adopt and mimic the private sector capabilities by leveraging malicious services (RaaS, IaaS, MaaS, etc.) and using IABs. As attackers continue to rapidly adopt new technologies and exploit changing circumstances, it becomes increasingly critical for threat analysts to keep pace. This may require investing in XDR-style platforms or managed XDR services that can collect threat telemetry across products and devices while separating useful intel from noise.

Attacks on the supply chain were another major factor shaping the threat landscape in 2021. Threat actors turned their attention to service providers, compromising them to launch downstream attacks on their customers. Two supply chain attacks, SolarWinds and Kaseya, brought the problem to the public's attention, but dozens of others occurred throughout the past year. Almost two-thirds of these attacks relied on exploiting the customer's trust in their service provider–yet another reason organizations should consider adopting a Zero Trust framework.

One particular vulnerability, the Microsoft Exchange Server flaw, wreaked havoc around the globe. First exploited by HAFNIUM, several other groups quickly zeroed in on the flaw and launched attacks using the same tactics against multiple organizations. While these attacks relied on zero-day exploits, they could have been prevented with a few existing technologies. An identity-aware network platform, continuous authentication, adaptive access, and remote work solutions that authenticate per-application, greatly reduce the risks of this type of vulnerability.

Governments remain actively engaged in the cybersecurity space, with G7 countries and NATO allies putting it at the top of their public policy agendas. An Executive Order on Improving the Nation's Cybersecurity was issued in the U.S., creating new requirements for incident reporting and software supply chain security. The Department of Justice established a Ransomware and Digital Extortion Task Force. The European Union continues the work set forth in the EU Cybersecurity Strategy of 2020. Measures include creating a Joint Cyber Unit security operations center and standardizing a common cybersecurity certification framework. Transport Canada declared cybersecurity a foundational element of road safety. Automakers received cybersecurity guidelines from ISO, SAE, and the UN regarding the design, manufacture, and use of connected vehicles.

The events of 2021 serve as a reminder that there is zero immunity to cyberattacks, and no one is safe. SMBs in particular suffered countless financially painful attacks that never made headlines. Attacks affecting organizations of all sizes were inflicted both directly and through their supply chains. Mobile devices, used by a growing population of world citizens, feature apps that are overwhelmingly insecure. The vulnerable SHAREit app for Android devices, allowing remote code execution, was downloaded over one billion times before its flaws were revealed. Every participant in the digital space, from international corporations down to the individual smartphone owner, remains exposed to cyber risks.

BlackBerry is dedicated to providing advanced cybersecurity solutions to people and organizations worldwide. We continue to train and deploy increasingly effective and advanced AI models that predict threats and use prevention-first technology to stop them from executing. Our Cylance AI security models, first deployed on endpoints, have been adapted to detect threats in the network, user behavior, and beyond.

TO LEARN MORE ABOUT HOW BLACKBERRY CAN SECURE YOUR ORGANIZATION, VISIT US AT BLACKBERRY.COM.

ACKNOWLEDGEMENTS:

The BlackBerry 2022 Threat Report represents the collaborative efforts of our talented teams and individuals. In particular, we would like to recognize:

Adam Lancaster
Baldeep Dogra
Brent Nicorvo
Brian Robison
Dan Ballmer
David Relyea
Dean Given
Eoin Wickens
Eric Milam
Ethan Fleisher
Gary Ng
Gina Regan
Ginger Espanola
Glenn Wurster
Goran Gotev
Grace Hu
Heather Spring
Ieva Rutkovska
Jim Simpson
John McClurg
John de Boer
Kristofer Vandercook
Lysa Myers
Marc Cormier
Marisa Goodrich
Marjorie Dickman
Mark Mariani
Mark Stevens
Marta Janus
Michelle Haynes
Natasha Rohner
Nigel Thompson
Patrick Slattery
Rajesh Rajamani
Robert Nusink
Sabrina Forgione
Samuel Spector
Sriram Krishnan
Steve Kovsky
Thom Ables
Tony Lee
Tom Bonner
Tracey Swanson
William L. Savastano
Willy Vega
Yi Zheng

The information contained in the BlackBerry 2022 Threat Report is intended for educational purposes only. BlackBerry 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 does not condone any malicious use or misuse of information presented in this report.

BlackBerry. Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.