CYBER

Threat Landscape Report

2022

CYBLE

Table Of Contents

Executive Summary

The Cyber Threat Landscape and Threat Predictions Report is an annual evaluation that provides an overview of the current state of cyber threats, highlighting the key threats, trends and patterns, Threat Actors (TA), and attack methodologies.

Cyble Research & Intelligence Labs (CRIL) examines the cyber threat landscape and assists enterprises in identifying emerging threats, associated potential risks, and how to prioritize cybersecurity activities.

The threat landscape is constantly evolving, with new threats emerging every time. In 2022, various cyber adversaries remained active and managed to adapt to changes in their target landscape.

In 2022, new ransomware groups such as **BianLian, Royal**, and several others were identified using new methods of extortion. It was noted that there was **a 15% decrease** in the number of publicly disclosed victims in comparison to the previous year, 2021.

With regard to Ransomware, America was the most frequently targeted region, followed by Europe and CIS nations.

APT groups have taken advantage of the ongoing **Russia-Ukraine** conflict to improve the effectiveness of their spear-phishing campaigns.

In 2022, APT groups like **Gamaredon, Lazarus**, and **Transparent Tribe** were among the most active, with newly discovered groups such as **DarkPink** and **Adastrea** also emerging.

In 2022, cyber adversaries continued to improve their methods by developing new malware and updating existing ones to target different operating systems. They also implemented more sophisticated techniques such as DLL side-loading, Stegosploit, **Fileless Execution**, Blindside, etc., and increased the complexity of malware to evade detection.

New stealers such as **Loli stealer, Prynt stealer, Ducklogs, Mini Stealer**, and many others were identified in 2022.

In 2022, there was a significant increase in the number resurfaced of banking trojans, including **ERMAC, SOVA, Hydra, OCTO**, and many others. These trojans actively targeted Android users, along with new banking trojans such as **Zanubis**.

New third-party services for Android malware, such as **Zombinder** and various **Dropper-as-a-Service** (DaaS), were actively being used by Threat Actors.

APT groups, Hacktivists, and Threat Actors conducted targeted attacks by scanning the internet-connected devices to infiltrate and compromise industrial control systems (ICS) and operational technology (OT) assets and deployed malware like **Industroyer2** to perform other malicious activities.

The number of vulnerabilities continues to rise, with **25,226** reported in 2022 alone - the highest number reported in the last six years.

Attackers are increasingly exploiting vulnerabilities in sensitive infrastructure such as Operational Technology (OT), internet-facing apps, and network devices to infiltrate corporate networks and launch devastating attacks.

In 2022, there was a substantial **rise of over 60%** in phishing attacks compared to 2021. These attacks targeted the healthcare, professional and scientific services, and information technology sectors.

Ransomware Trends

Cyble Research and Intelligence Labs (CRIL) identified multiple new ransomware groups in 2022. BianLian, Royal, and Play were the most active among these new groups. CRIL reported 2228 publicly disclosed victims in 2022, as compared to 2624 in 2021, which represents a 15% decrease year over year. The highest number of publicly reported victims was observed in the fourth quarter of 2022.

2022 Ransomware Highlights

Figure 1 - 2022 Ransomware Highlights

In 2022, CRIL monitored the activities of over **50** different ransomware groups, with **LOCKBIT, ALPHV, Conti, Black Basta, and HiveLeaks** being among the most active. These groups targeted victims in more than 100 countries worldwide, with the **United States, United Kingdom, Germany, Canada, and France** being among the most frequently targeted. The figure below shows the prevalence of prominent ransomware families in the five most affected countries

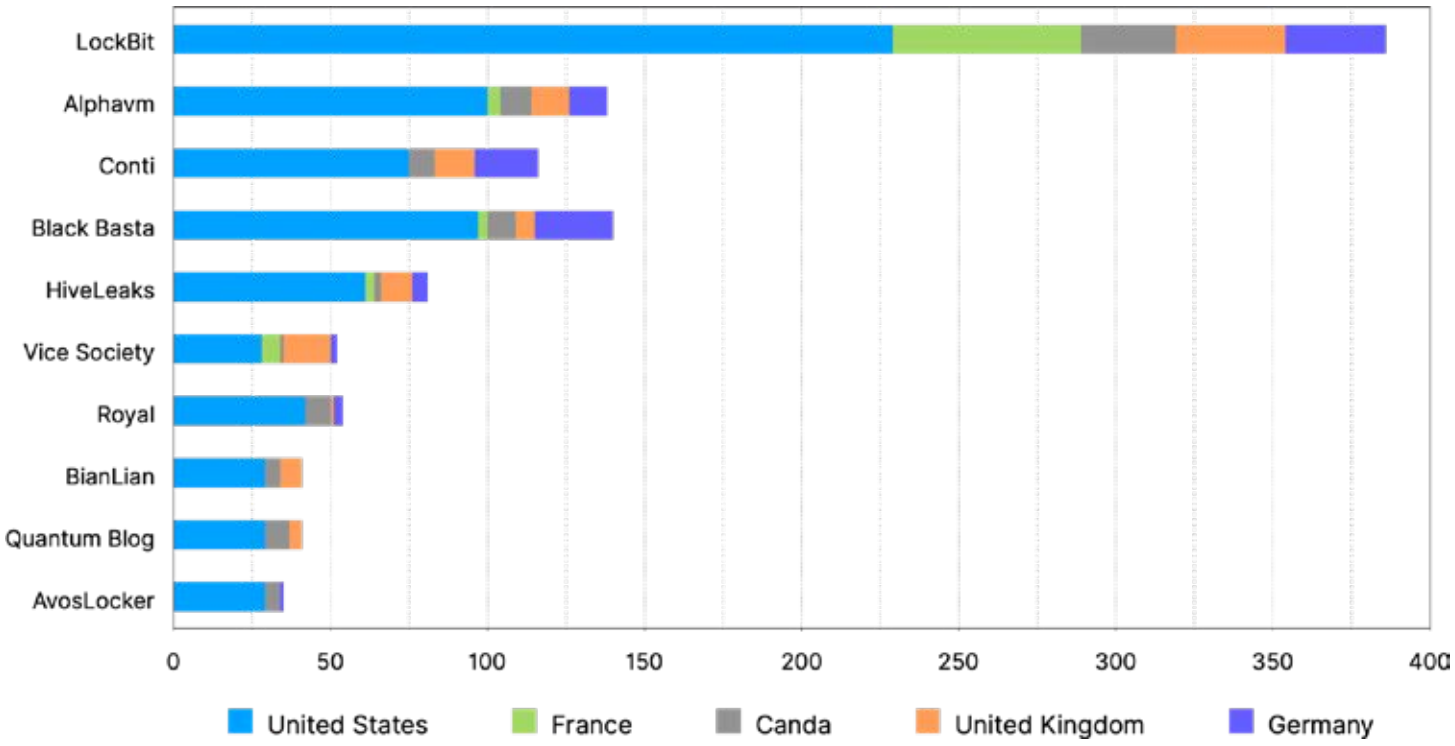


Figure 2 - Distribution of Ransomware within most targeted nations

Ransomware attacks affected several industries within these countries, including **Professional Services, Manufacturing, Construction, Healthcare, and the Banking and Financial Services industry**. The figure below shows the top 10 industries attacked by ransomware attacks

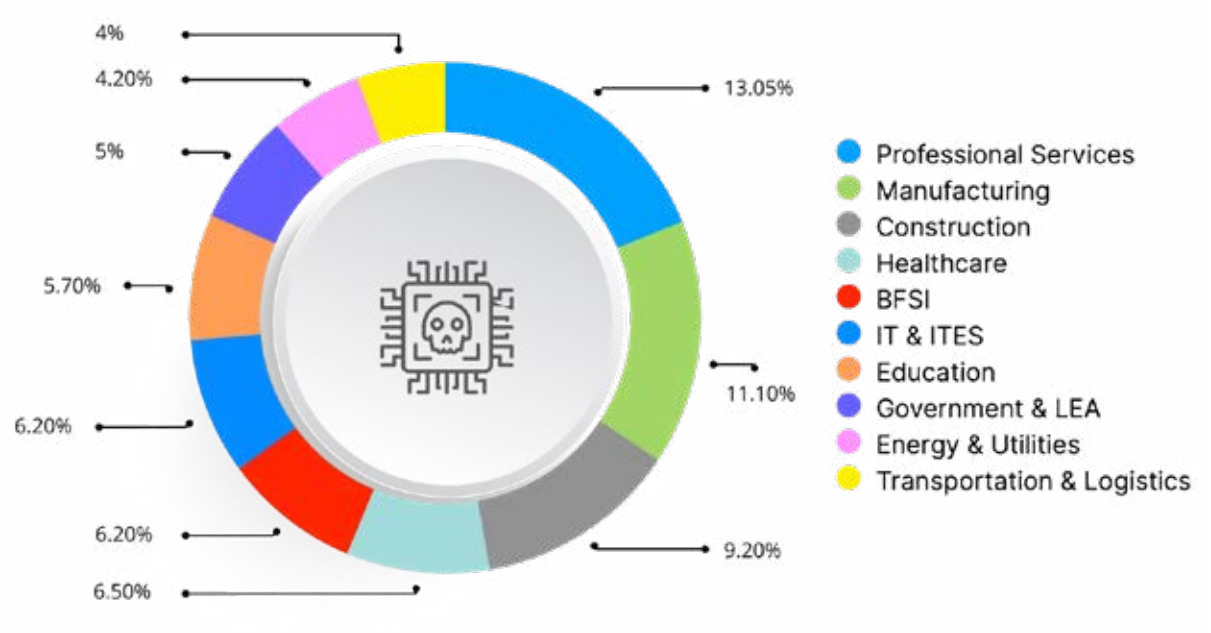


Figure 3 - Most attacked industries

It appears that countries with specialized industries are more susceptible to ransomware attacks in those specific sectors. For example, **Taiwan, known for its technology industry, has many victims in that field.**

Similarly, the Service, Finance, Insurance, and Healthcare sectors in the United States are frequently targeted, indicating that ransomware groups are not attacking industries indiscriminately. Instead, they are focusing on industries that play a substantial role in a country's GDP.

.

Americas was the most targeted region in 2022, followed by Europe & CIS. Professional Services, Manufacturing, Construction, Healthcare, BFSI, IT & ITES, Technology, and Government & LEA were the most targeted industries globally. The figure below shows the region-wise distribution of ransomware attacks on industries in 2022.

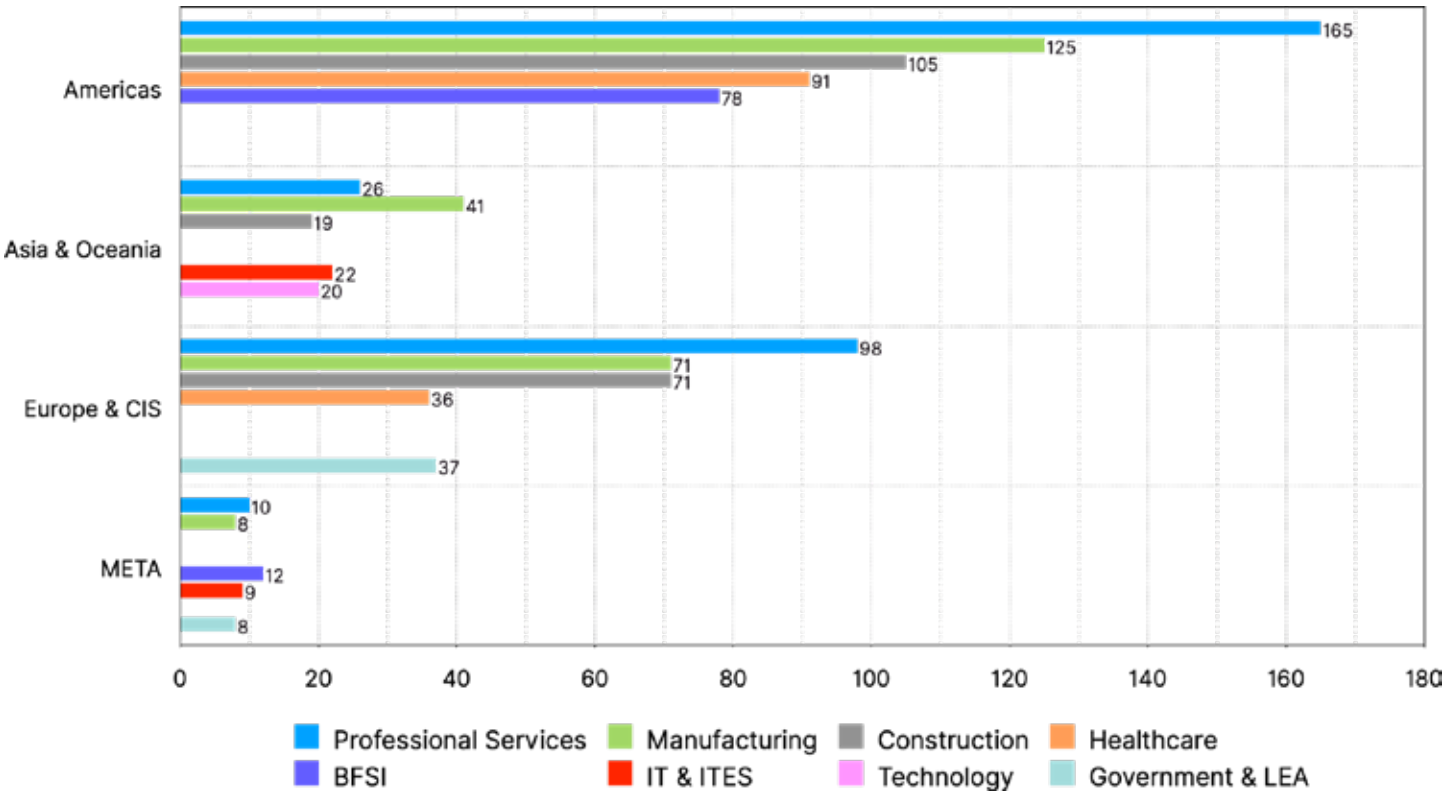


Figure 4 - Most Targeted Industries by Region

Some estimates suggest that ransomware attacks have generated billions of dollars in revenue for cybercriminals in recent years. In an advisory released by the FBI and CISA, it was reported that **Hive ransomware actors had extorted over $100M from victims.**

In a similar advisory, it was reported that **Cuba ransomware demanded 145 Million U.S. Dollars (USD) and received 60 Million USD in total ransom payments**. The figure below shows the ransomware earnings by different ransomware groups to date.

- Note: The ransom earnings shown in the figure below are taken from crowdsourced data and might not be precise.

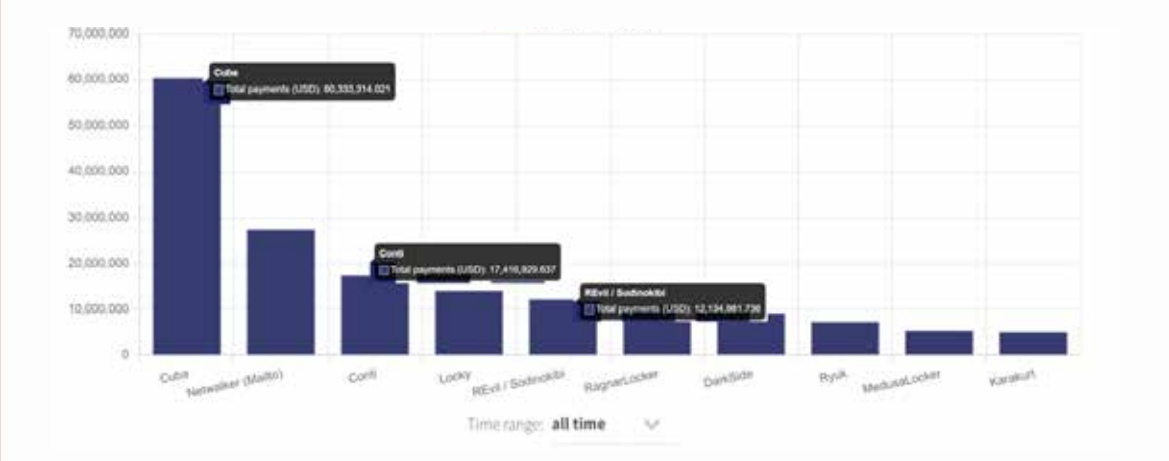


Figure 5 - Ransomware Payment (source: ransomwhe.re)

2022 Ransomware Upshots

Hampered Ransomware Operations

In 2022, several major ransomware groups faced significant disruptions to their operations due to Law Enforcement actions and internal conflicts. For example, in January 2022, 15 members of the **REvil ransomware** group were arrested by the Federal Security Service (FSB) in Russia.

In February, there were reports of internal strife within the **Conti ransomware group**, ultimately leading to the group's shutdown. Additionally, in October, a high-value target known for their involvement in numerous high-profile ransomware cases was arrested in Canada, as per Europol. The individual, a Russian and Canadian national, had been known to make ransom demands ranging from €5 to €70 million and was identified as an affiliate of the **LOCKBIT ransomware** group.

Public-Facing Infrastructure Under Siege

Multiple ransomware groups have been reported frequently exploiting public-facing infrastructure. The most common of those are **Exchange servers and RDP**. Exchange servers are a common target for ransomware attacks because they often contain sensitive business data and are critical to the operation of an organization.

One of the recent vulnerabilities related to exchange servers is ProxyNotShell, a Windows Exchange email servers vulnerability tracked as CVE-2022–41040 and CVE-2022–41082. Exploiting this vulnerability could result in Remote Code Execution (RCE) on the Exchange server. Play ransomware group also exploited this vulnerability in the Rackspace ransomware attack.

Remote Desktop Protocol (RDP) is used to remotely connect to a computer or device. Ransomware attacks often target RDP because it allows an attacker to gain access to a victim's network and infect multiple devices.

Intelligence gained from **Cyble Global Sensor Intelligence (CGSI)** indicates a surge in the number of RDP exploitation attempts in the past few months. **Over 4,783,842 exploitation attempts were made in Q4-2022**, with a peak in exploitation attempts being observed in September-end and mid-November. CRIL carried out an investigation and found multiple ransomware groups targeting open RDP to gain initial access to corporate networks.

The figure below shows the exploitation of RDP mentioned by Hive ransomware.

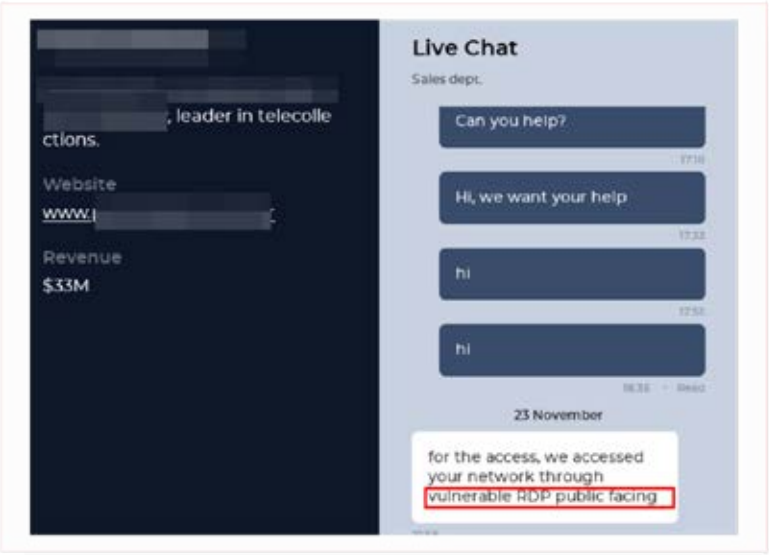


Figure 6 - Vulnerable RDP targeted by Hive ransomware

Does the concept of 'Average Ransom' exist?

During our routine threat-hunting exercises, CRIL found that the ransomware group does not demand ransom from their victims, considering an average ransom amount. Instead, the ransom amount is decided through the revenue of a company.

We encountered multiple instances where ransomware groups demanded relatively higher ransoms simply because the victim was a high-revenue organization. A similar instance is shown in the figure below.

In this case, **Hive ransomware demanded USD 5M from victim1 with a revenue of $1000M and USD 700K from victim2 with a revenue of USD 33M**.

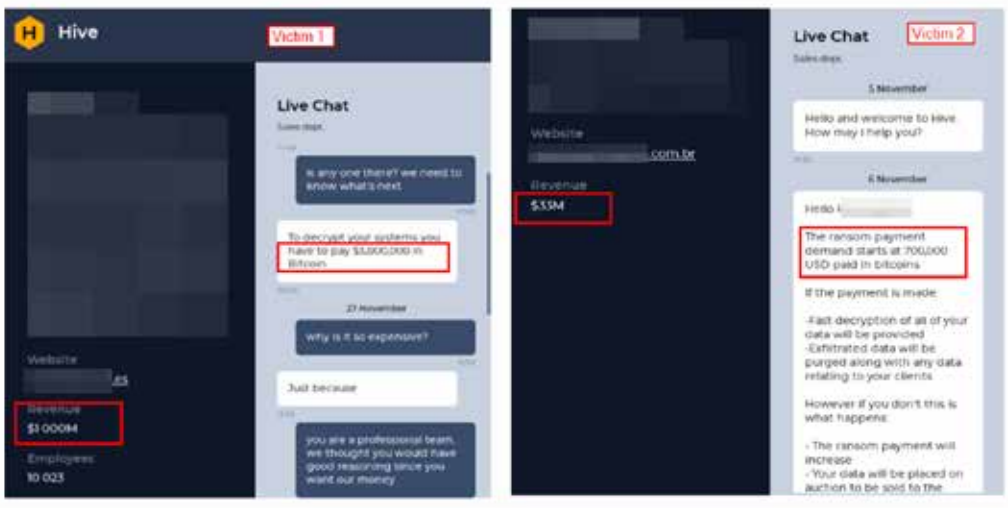


Figure 7 - Comparison of Ransom demand

Ransomware Collaboration

Ransomware collaborations are a significant concern as they allow multiple groups to pool their resources and carry out more potent attacks. The leaked data from the Conti group provided evidence of collaborations with other ransomware groups.

In one instance, the **HARON/MIDAS** and **ALPHV** ransomware groups posted the same victim data on their leak sites, raising suspicions of possible association or cooperation between them.

The REvil ransomware group's leak site was taken down in the first quarter of 2022 following the arrests of REvil affiliates. However, in October 2022, REvil claimed credit for an attack against Australia-based Medibank on the **REvil leak site** by an affiliate claiming to be a member of **REvil, ALPHV**, and **Hive** Ransomware groups.

Technical Advancement

Ransomware groups are rapidly evolving their attack techniques. In 2022, Ransomware strains such as **LOCKBIT** added a feature of Network Propagation which could make the attack much more devastating by encrypting all the files on a network.

In 2022, we witnessed prominent ransomware families shifting towards using **Rust** or **GoLang-based** binaries. Multiple ransomware groups use intermittent encryption to speed up the encryption process and make it more difficult to detect. Intermittent encryption was first observed with the **LockFile ransomware** variant in mid-2021.

Since then, intermittent encryption has been adopted by several prominent ransomware groups, including **PLAY, Qilin, Black Basta, and ALPHV**. The technique allows these groups to operate stealthily and evade traditional detection methods.

CRIL also investigated multiple new extortion techniques adopted by ransomware groups, such as searchable databases, spoofed domains, and leaking of the victim's negotiation chats.

Windows Malware Trends

Windows malware refers to any malicious software intended to run on computers using the Microsoft Windows operating system. This includes various types of malware, such as trojans, backdoors, stealers, ransomware, adware, and spyware.

These programs can infect a computer via various means, such as email attachments, files downloaded from phishing websites, or exploiting software vulnerabilities. Once inside, malware can cause harm by stealing personal information, damaging or erasing data, or using the infected computer to launch attacks on other systems.

In this report, CRIL presents an overview of the current threat landscape for Microsoft Windows, including information about prevalent banking trojans, information stealers, Remote Access Trojans (RAT), etc.

Prevalent Threats

Emotet

Emotet is a widely known malware variant that was first identified in 2014. Initially, it was utilized as a banking trojan, but it has since been adapted to deliver other types of malware, such as TrickBot and IcedID.

In 2022, the Emotet botnet was found to have been reactivated by the **Conti ransomware group**, which used it to gain initial access to corporate networks.

During the U.S. tax season in 2022, the Emotet botnet sent out malicious emails masquerading **as the Internal Revenue Service (IRS)**. The Emotet malware operators also switched to using 64-bit loaders and stealer modules. They were found to be using Windows shortcut files (LNK) containing PowerShell commands to infect victims' computers, moving away from the Microsoft Office macros that are disabled by default.

In June, the Emotet botnet attempted to infect potential victims with a **credit card stealer** module designed to collect credit card information stored in Google Chrome user profiles.

Emotet campaigns were less active in July, but in September, security researchers discovered that the **Quantum and BlackCat ransomware** gangs were utilizing the malware to deploy their payloads. In November, the Emotet group again sent malicious emails that downloaded the Bumblebee malware onto victim systems.

Qakbot

QBot, also known as Qakbot or Pinkslipbot, is a malicious software that has been active since 2007, primarily targeting financial institutions and designed to steal sensitive information such as login credentials and personal details.

In 2022, Qakbot was observed conducting rapid attacks, with analysts reporting that it only takes around 30 minutes for the malware to steal sensitive data after the initial infection.

In April, Qakbot began spreading malware payloads through phishing emails with password-protected ZIP archive attachments containing malicious **MSI Windows Installer** packages, a change in tactics from the previous method of delivering malware through phishing emails with **Microsoft Office documents** containing malicious macros.

Later, the **Black Basta** ransomware gang partnered with QBot to spread laterally through hacked corporate environments. The malware operators were also found to be using DLL Side-loading in Windows Calculator to infect computers, thereby aiding in evading detection by security software.

In November, new phishing attacks were observed utilizing a Windows zero-day vulnerability to drop the QBot malware without displaying security warnings. Additionally, phishing emails distributing QBot were found to be using a DLL hijacking flaw in the **Windows 10 Control Panel** for infection.

In December, QBot malware phishing campaigns adopted a new distribution method using **SVG** files to perform **HTML smuggling**, creating a malicious installer for Windows locally.

The below figure depicts the evolution of the Tactics, Techniques, and Procedures (TTPs) used by the Qakbot malware in 2022.

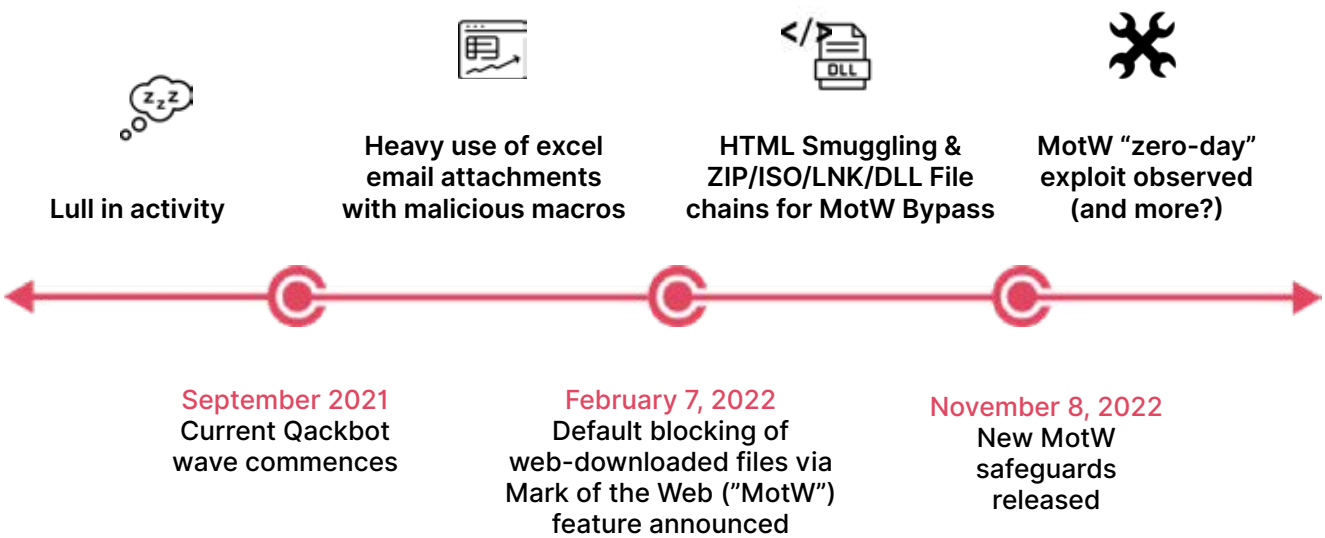


Figure 1 – Qakbot TTP Evolution in 2022 (Source: Tidal)

IcedID

IcedID is a modular banking trojan that was initially spotted in 2017 and primarily used to deploy secondary malware such as loaders or ransomware. In 2022, there was a significant increase in the distribution of IcedID malware, particularly in March, due to a new campaign that alters existing email conversations and inserts malicious payloads that are challenging to detect. The operators behind IcedID are suspected to be **Initial Access Brokers** who infiltrate networks and then sell access to other cybercriminals.

In April, Ukrainian government agencies were targeted with new attacks that exploited **Zimbra vulnerabilities** and phishing campaigns distributing IcedID.

In July, website owners were targeted with fake copyright infringement complaints using Yandex Forms to spread the IcedID malware. The threat actors behind IcedID malware phishing campaigns were found utilizing a wide range of distribution methods, likely to determine what works best against different targets.

Starting in September, Microsoft identified **Raspberry Robin worm** infections deploying IcedID malware. The resurgence of Emotet in the fall season also led to an increase in the distribution of IcedID as a secondary malware.

BumbleBee

In April 2022, a new malware loader called Bumblebee was discovered. It is believed to be the latest creation of the **Conti syndicate** and is intended to replace the **BazarLoader** backdoor to deliver ransomware.

Later, a new version of Bumblebee was seen in the wild, utilizing the PowerSploit framework for stealthily injecting a DLL payload into memory. Threat actors have also been found to use the **Sliver toolkit** as an alternative to Cobalt Strike to deploy the Bumblebee (Coldtrain) malware loader in recent attacks. Researchers have also identified the **Raspberry Robin** worm being used to deliver other second-stage payloads, including Bumblebee and other malware, onto compromised devices.

Growing Stealers

Threat actors use various methods, including stealer malware, to steal sensitive information from victims' devices, focusing on banking information and other important files.

In 2022, CRIL identified several of these types of malware, which have become a major concern for individuals and organizations due to their increasing prevalence. Some of the most well-known stealer malware include:

RedLine Stealer

Initially identified in 2020, RedLine is a widely-used information-stealing malware designed to steal sensitive information from a victim's computer. Throughout 2022, various cybercrime groups have been using RedLine in various distribution campaigns, such as using fake COVID-19 Omicron stat counters, Windows 11 upgrade installers, Valorant cheat lures, and fake Binance NFT mystery box bots on YouTube, Fake Express VPN Sites, Online File Converter phishing page, as well as the RIG Exploit Kit.

In August, cybercriminals created a fake 'Cthulhu World' play-to-earn community to distribute RedLine and other malware through websites, Discord groups, social media accounts, and the Medium developer site.

Additionally, self-propagating RedLine malware was also distributed on YouTube. At the end of the year, Windows gamers and power users were targeted through fake MSI Afterburner download portals that infected their devices with both cryptocurrency miners and RedLine malware.

Vidar Stealer

Vidar Stealer is a dangerous malware strain that first appeared in 2018 as a fork of another malware called Arkei Stealer. During 2022, multiple reports of malicious campaigns using techniques such as fake websites, malware droppers, typosquatting domains, and YouTube campaigns to deliver Vidar Stealer malware to unsuspecting victims.

One such campaign was found to be using a **fake Pixelmon** website to lure fans with free tokens and collectibles. However, it also infected their devices with malware that could steal their cryptocurrency wallets.

At least 34 Russian-speaking cybercrime groups using malware such as RedLine and Raccoon collectively stole over 50 million account passwords from infected individuals in 2022.

Another malware dropper named **'NullMixer'** was discovered infecting Windows devices with various malware families, including Vidar Stealer and Raccoon Stealer.

Fake **Zoom** websites were also found to be spreading Vidar Stealer malware. Cybercriminals also used typosquatting domains that mimic well-known brands such as **Notepad++, Thunderbird, and Codevisualstudio** to trick users into downloading malware.

In November, a large-scale **campaign** was reported using YouTube to target more than 100 applications and deliver the Vidar info stealer malware. Furthermore, in December, it was reported that malware operators were increasingly using the **Google Ads** platform to spread malware such as Vidar to individuals searching for popular software products.

Raccoon Stealer

The Raccoon Stealer malware first appeared in April 2019, advertised as a "Malware-as-a-Service" (MaaS) on various cybercriminal forums. It can steal sensitive information from a victim's computer, including browser credentials, credit card data, cryptocurrency wallet data, email data, and more.

In March 2022, the cybercrime group behind the development of Raccoon Stealer announced that it had suspended its operations, claiming that one of its developers had died during the invasion of Ukraine.

However, the same year, a phishing campaign was discovered targeting German automotive companies, attempting to infect their systems with Raccoon Stealer and other info-stealers.

In June 2022, a new version of Raccoon Stealer was discovered, named "**Recordbreaker**", later identified as a revised version of Raccoon (Raccoon V2) that includes additional features such as fileless data exfiltration and support for stealing data through the Telegram messaging platform.

Additionally, WordPress sites were hacked to display fake Cloudflare DDoS protection pages to distribute malware that installs the **NetSupport RAT** and the Raccoon Stealer password-stealing Trojan.

Other Stealer Malware

Cyble Research & Intelligence Labs (CRIL) has identified various types of stealer malware that are being advertised and sold on cybercrime forums and distributed through phishing websites. These include malware such as:

Jester Stealer

Jester Stealer is a malware strain that steals sensitive information such as login credentials, cookies, and credit card information and sends it to the attackers. It first appeared on cybercrime forums in July 2021. As of 2022, it has undergone seven updates, each time attempting to improve its capabilities

Ducklogs

In 2022, a new Malware-as-a-Service (MaaS) operation called 'DuckLogs' surfaced, providing low-skilled or non-technical attackers with easy access to various modules designed to steal information, log keystrokes, access clipboard data, and provide remote access to compromised hosts. This service is entirely web-based and claims to have thousands of subscribers who use its platform to generate and launch over 4,000 malware builds

Mini Stealer

Cyble security analysts uncovered a threat actor on a cybercrime forum offering MiniStealer's builder and panel for free. MiniStealer's builder helps less experienced hackers to create malicious payloads, primarily to attack FTP applications and Chromium-based browsers.

Loli stealer

The LOLI Stealer malware, first identified in June 2022, is a Golang-based malware designed to steal sensitive information from a victim's device, including passwords, cookies, screenshots, cryptocurrency wallet information, and session data from Telegram and Steam applications.

Mitsu Stealer

Cybercriminals have created a fake version of the AnyDesk website, which is being used to distribute a custom malware called "Mitsu Stealer", specifically designed to steal valuable user data.

Mars Stealer

Mars Stealer is a Malware-as-a-Service (MaaS) designed to steal data. It allows cybercriminals to rent access to its infrastructure to launch their own attacks. It is frequently distributed through email attachments, malicious ads, and phishing sites and bundled with torrented files on file-sharing sites.

Prynt Stealer

Security experts have identified a new malware called **Prynt Stealer**, which belongs to the category of info-stealer malware. It has powerful features and additional modules for keylogging and clipboard data collection.

Typhon Stealer

Cyble Research Labs has discovered a new malware, called **Typhon Stealer**, that is being offered as a service for hire. The malware can extract a wide variety of data from different applications. It also has the ability to collect data from messenger apps, VPNs, gaming software, and FTPs, such as usernames, passwords, tokens, and sessions.

Remote Access Trojans (RATs) are dangerous because they provide the attacker with a high level of access and control over the compromised system, allowing them to see and do anything they want on the infected machine. They are designed to hide on infected systems and provide secret access to the attacker. In 2022, some popular RATs that were spreading included:

NetSupport RAT

A modified version of NetSupport Manager, known as the NetSupport RAT, has been used in various malicious campaigns. Cybercriminals were hacking WordPress sites to display fake Cloudflare DDoS protection pages as a medium to distribute malware, including the NetSupport RAT and other malware.

Another tactic used by the cybercriminals is a campaign known as "sczriptzzbn inject", in which they inject a script using a variable named “sczriptzzbn” into files returned from compromised websites.

This script causes a fake browser update page to appear on the victim's browser and prompts them to download the NetSupport RAT malware payload. This tactic is often used by SocGholish threat actors, who use fake browser updates, and USPS-themed malspam was also used to deliver this RAT.

Borat RAT

Cyble researchers have discovered a new malware named Borat, which has been available on darkweb markets since 2022. This malware can be used for DDoS attacks, bypassing UAC, and deploying ransomware. It allows attackers to control the victim's mouse and keyboard, access files and network points, and conceal their presence.

Borat has various features such as keylogging, **encryption, decryption of files**, creating ransom notes, and launching **DDoS** attacks on targeted servers. It also gathers system information and sends it to the attacker's Command & Control server.

Remcos RAT

In 2022, cybercriminals were using phishing tactics related to the invasion of Ukraine to distribute malware, specifically Remote Access Trojans such as Agent Tesla and Remcos RAT.

In April, African banks were identified to be particularly vulnerable to these attacks, which use techniques such as **HTML smuggling and typo-squatted domains** to drop the Remcos. The attackers may use Remcos to access transaction details, steal credentials, move within the bank's network, and gain information for business email compromise attacks.

In November, the threat group known as **OPERA1ER** was using open-source tools, commonly-used malware, and frameworks like Metasploit and Cobalt Strike to target company servers. They gain initial access through spear-phishing emails that use popular topics such as invoices or postal delivery notifications. The emails have attachments that deliver the first stage of malware, including the Remcos and other malicious RATs.

AgentTesla RAT

Agent Tesla is a .NET-based keylogger and Remote Access Trojan (RAT) that has been active since 2014. In 2022, we observed phishing campaigns using malicious PowerPoint documents to distribute various malware payloads. The specific malware families used in this campaign are Warzone and AgentTesla. In June, a new distribution method was observed, using Windows Help files (*.chm) to spread AgentTesla.

In July, CERT-UA issued an alert warning of a cyber-attack targeting Ukrainian government entities, abusing the war-related topic and spreading the notorious RAT AgentTesla. In September, a large-scale phishing campaign was reported among Ukrainian, Austrian, and German organizations. The hackers were exploiting the email attachment vector to spread AgentTesla. Additionally, the RAT is delivered by Quantum Builder with new TTPs.

Other RATs

In 2022, a variety of other popular RATs were also spreading, including:

Venom RAT

Venom RAT is malicious software that was discovered in 2020 and allows cybercriminals to remotely control infected systems. The latest version, identified in 2022, has added a module that can steal sensitive information and send it to the attackers' command and control server. Older versions of Venom RAT have features such as remote access and HVNC (Hidden Virtual Network Computing).

ASyncRAT

Threat actors are using phishing emails with HTML attachments to deliver AsyncRAT, a Remote Access Trojan that can monitor and control infected computers remotely. The latest campaign for this RAT is particularly clever as it uses JavaScript to create an ISO file from a Base64-encoded string, mimicking the download process. Additionally, recent AsyncRAT campaigns have been observed to use a new version of the 3LOSH crypter.

Nanocore RAT

In 2022, security researchers uncovered an attack campaign in which cybercriminals used public cloud infrastructure such as Azure and AWS to deliver variants of Nanocore, NetWire, and AsyncRAT malware. These RATs are deployed to target users' data.

Notable Malware Threats Observed

In 2022, Cyble Research and Intelligence Labs identified various malware threats, including:

Coinminer

Coinminer is a type of malware that uses a victim's computer resources, such as CPU and RAM, to mine for cryptocurrency without the victim's knowledge. In 2022, Cyble researchers identified an attack where fake MSI Afterburner sites were being used to distribute coin-mining malware. In another campaign, the attackers used Coinminer to deploy Clipper malware for rapid financial gain.

Matanbuchus

Security experts have discovered a new malware loader called Matanbuchus, which is delivered to victims via phishing emails. This malware loader operates on a Malware-as-a-Service (MaaS) model. It is designed to quietly download and run secondary malware payloads, such as Cobalt Strike Beacons and other executable files.

MikuBot

MikuBot is a malware strain discovered by Cyble Research & Intelligence Labs. It is designed to steal sensitive data or covertly establish VNC connections to steal it. Additionally, it allows the attacker to gain remote access to the infected computer and run malware without needing other third-party applications.

DarkTortilla

DarkTortilla is a sophisticated malware that has existed since 2015; it is written in .NET. It is known to drop malware stealers and RATs such as AgentTesla, AsyncRAT, and Nanocore. In 2022, researchers found that it spreads through phishing sites that pose as legitimate Grammarly and Cisco sites. These phishing sites can be accessed through spam emails or online ads, which infect users once clicked.

IBAN Clipper

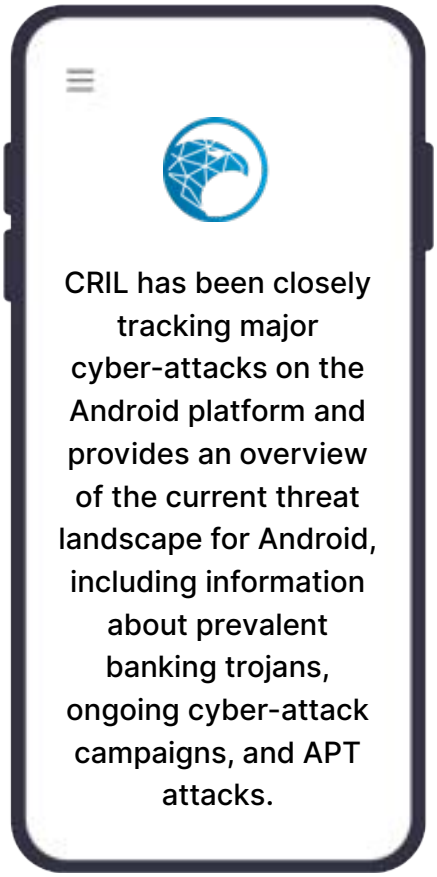
Cyble has identified a malware called 'IBAN Clipper' that replaces the victims' clipboard content without authorization. It is being sold on the underground forum with a subscription model designed to work on Windows systems. The malware is targeting International Bank Account Number (IBAN) specifically.

Mobile Malware Trends

Android is a widely used operating system with over 3 billion active users worldwide and holds a 70% mobile market share. According to a recent study, mobile users are predicted to reach 7.5 billion by 2026. As mobile users continue to grow, cyber-attacks targeting mobile devices also increase significantly.

In 2022, the majority of threats detected on Android platforms were Trojans, accounting for over 40% of all threats. These trojans included families like SOVA, Hydra, Sharkbot, and Ermac, among others.

In addition to Trojans, Potentially Unwanted Applications (PUAs) were commonly found on Android. The threat landscape on Android is largely dominated by Trojans and PUAs, as shown in the below chart.



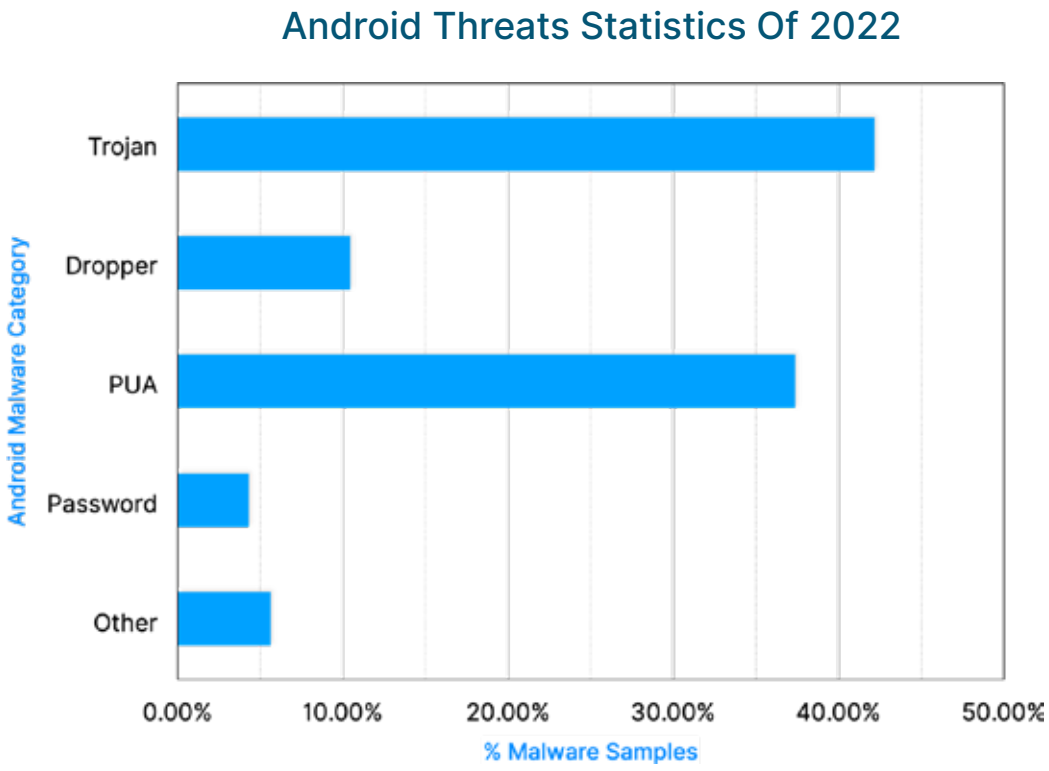


Figure 9 – Android malware statistics for 2022

Prevalent Banking Trojans targeting the Android platform

CRIL has identified several dangerous Android banking Trojans that have been actively targeting users and attempting to steal their sensitive information. These trojans, including **BRATA, ERMAC, Hydra**, SOVA, and **Sharkbot**, use techniques such as preventing uninstallation and auto-granting permissions to evade detection and effectively stealing user data. These trojans have been observed in high numbers in the wild, as shown by the statistics in the below figure.

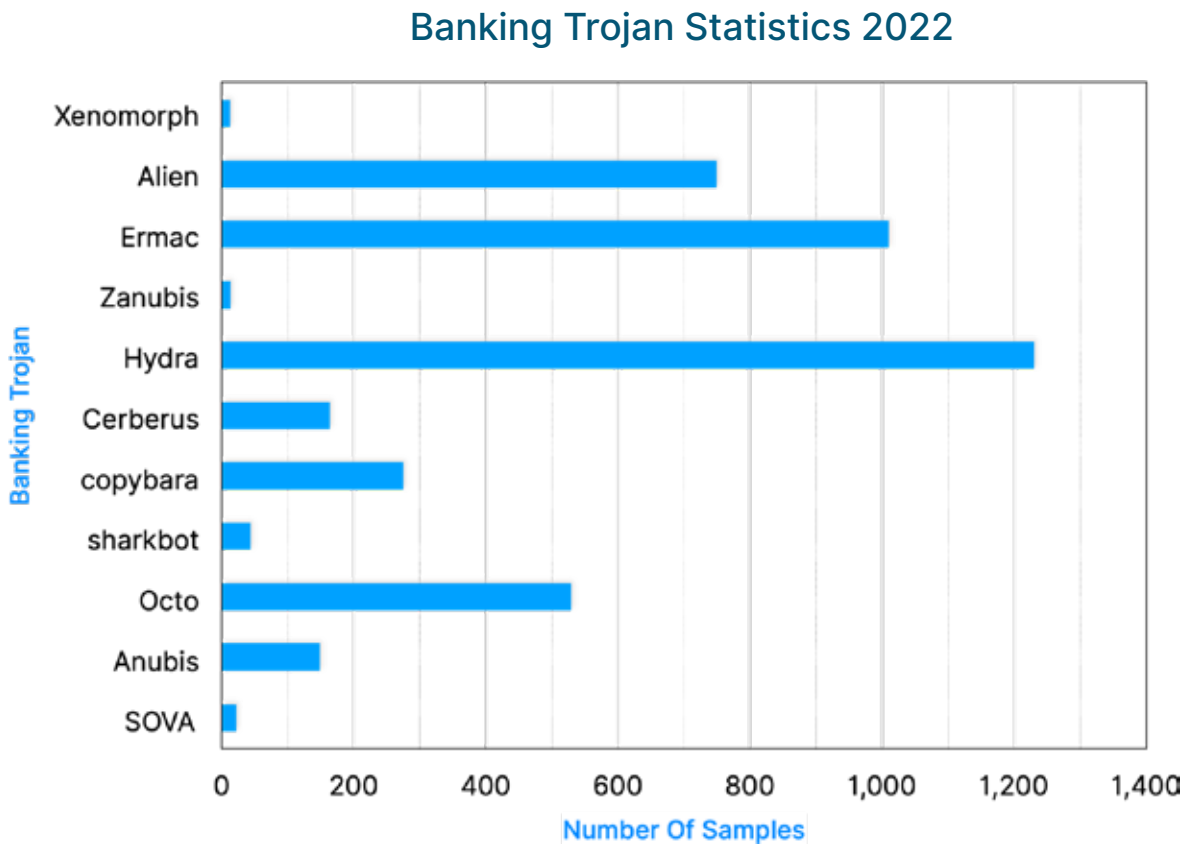


Figure 10 – Android Banking Trojan Statistics 2022

ERMAC Returned With New Features In 2022

According to the above banking trojan statistics, the ERMAC banking trojan was the second most dominant trojan in 2022. ERMAC 2.0 was identified in May 2022 and distributed via phishing sites.

It has been available on the underground market for rent at $5K/month and targeted over 400 applications using fake HTML overlay screens. In the recently upgraded version, ERMAC 2.0 continuously monitors victims' clipboard data and replaces the crypto wallet address with TA's wallet address to perform on-device fraud.

In October 2022, CRIL observed a spike in the phishing sites distributing the ERMAC banking trojan. The identified campaign used phishing sites impersonating legitimate entities such as **Google Play store, APK mirror, APK pure, Uber, Snapchat, and many others**. These typosquatted phishing sites were tricking victims into downloading ERMAC malware and infecting the victim's device.

New SharkBot variant found on Google Play Store

In October 2021, the Sharkbot Android banking Trojan was discovered targeting European banks. It utilized an Automatic Transfer System (ATS) to transfer money from infected devices. In March 2022, a new version of Sharkbot was detected being distributed through the Google Play Store.

Additionally, in September 2022, two new versions of the Sharkbot **malware (v2.25 and v2.26)** were discovered to be distributed through the Google Play Store. These variants include a cookie-stealing feature and have removed the ability to automatically reply to notifications.

The latest variant uses the logsCookie command to load a URL into WebView and collect the cookies from the loaded URLs using the onPageFinished method. The collected cookies are then sent to the attacker's Command & Control server.

Zanubis: A New Android Banking Trojan Targeting Peruvian Bank

Zanubis is an Android banking trojan that was first identified in September 2022. It disguises itself as a PDF reader app and uses fake overlays to steal sensitive information from targeted banking apps. It receives instructions from a Command and Control (C&C) server and has continuously evolved since its discovery.

Zanubis is currently targeting banks in **Peru**, and we suspect it will still be in the development phase, with the possibility of new variants and updated tactics being introduced in the future.

End Of Flubot Banking Trojan

The Flubot Android banking Trojan was first detected in late 2020 and primarily targeted users in Europe, Asia, and Oceania. It was distributed through fake text messages pretending to be from FedEx and Correos.

Flubot uses the Accessibility Service to steal victims' credentials by overlaying a fake window on top of genuine banking or cryptocurrency apps. It spreads mainly through smishing messages sent to the contacts of infected devices.

Flubot was active in various campaigns from late 2020 until April 2022, but its distribution was stopped in June 2022 due to the efforts of Europol, a law enforcement agency. They announced the takedown of Flubot in an operation spanning 11 countries, and the Dutch police took down its infrastructure in May 2022.

In addition to the prevalent baking trojans highlighted above, several other banking trojans have also been observed, such as **OCTO, Alien, and** Hydra targeting a significant number of Android users based on the number of samples observed in the wild. SOVA, in particular, has been observed with a new variant in 2022 that contains ransomware modules and a cookie stealer functionality.

Zombinder: New Dark Web Obfuscation Service Poisoned Legit App With Malware

In late 2022, security researchers discovered a darknet platform called "Zombinder" that provided binding services for Android and Windows malware. This campaign used various Trojans to target Android and Windows users, utilizing desktop malware such as Erbium, Aurora Stealer, and Laplas clipper, as well as the Android banking trojan **ERMAC**.

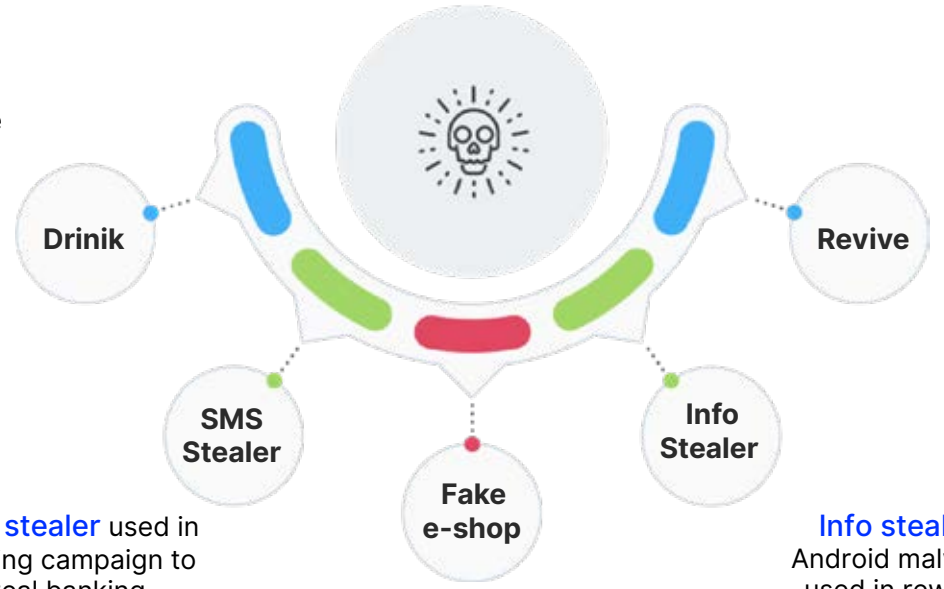
This campaign has resulted in the infection of over 1,000 victims, and the Erbium stealer, which was spread through this campaign, successfully obtained sensitive information from more than 1,300 victims.

Applications created using Zombinder often masquerade as modified versions of popular apps such as Instagram, WIFI Auto authenticator, and football streaming apps.

When a victim downloads one of these apps containing a malicious payload bound with Zombinder, they are presented with a fake update screen. This is meant to trick the victim into thinking they are updating a legitimate app, while in reality, a banking trojan payload is being downloaded in the background.

In 2022, we discovered various intriguing malware variants targeting Android users in a specific region, such as:

The Drinik malware identified in 2020 returned in 2022 with new capabilities, such as keylogging and screen recording features targeting Indian taxpayers.



Revive Banking Trojan Targeting Spanish Citizens enables threat actors to perform Account Takeover attacks.

SMS stealer used in phishing campaign to steal banking credentials targeting **BRI bank from Indonesia.**

Fake e-shop campaign used Android malware to steal net banking credentials, not targeting Southeast Asian countries like **Malaysia, Vietnam, and Myanmar.**

Info stealer Android malware used in reward campaign to target **Indian bank users.**

During 2022, we also observed that various APT groups used several Spyware variants with different capabilities for their malicious activities. These include a Spyware variant with new spying capabilities used by the Bahamut group to target the Middle East and South Asia. In August 2022, **Bitter APT** was identified using Dracarys Android Spyware.

Disguised as a messaging application, this spyware variant added malicious code to the genuine messaging app's source code. Also, we observed a new obfuscated version of Android malware, "Furball", disguised as a translation app used in the **Domestic Kitten campaign by the APT-C-50** group targeting Iranian Citizens.

Additionally, CRIL blogged about the Android Spyware masquerading as a PDF application and opening the popular book – "The China Freedom Trap" by Dolkun Isa. The Scarlet Mimic APT group used this malware to target the Uyghur community and steal sensitive information such as contact details, call logs, location, etc.

Linux Malware Trends

Linux is a popular operating system, especially for servers and other infrastructure, because it is open-source, stable, and secure. It is also highly customizable, which makes it easy to adapt to specific needs. As the use of Linux has increased, so have the capabilities of threat actors to create payloads that can infect Linux systems.

In 2022, there was a sharp rise, over 80%, in the usage of malware specifically designed to target Linux systems, with Trojans and Backdoors being the most commonly detected types, as the chart below illustrates.

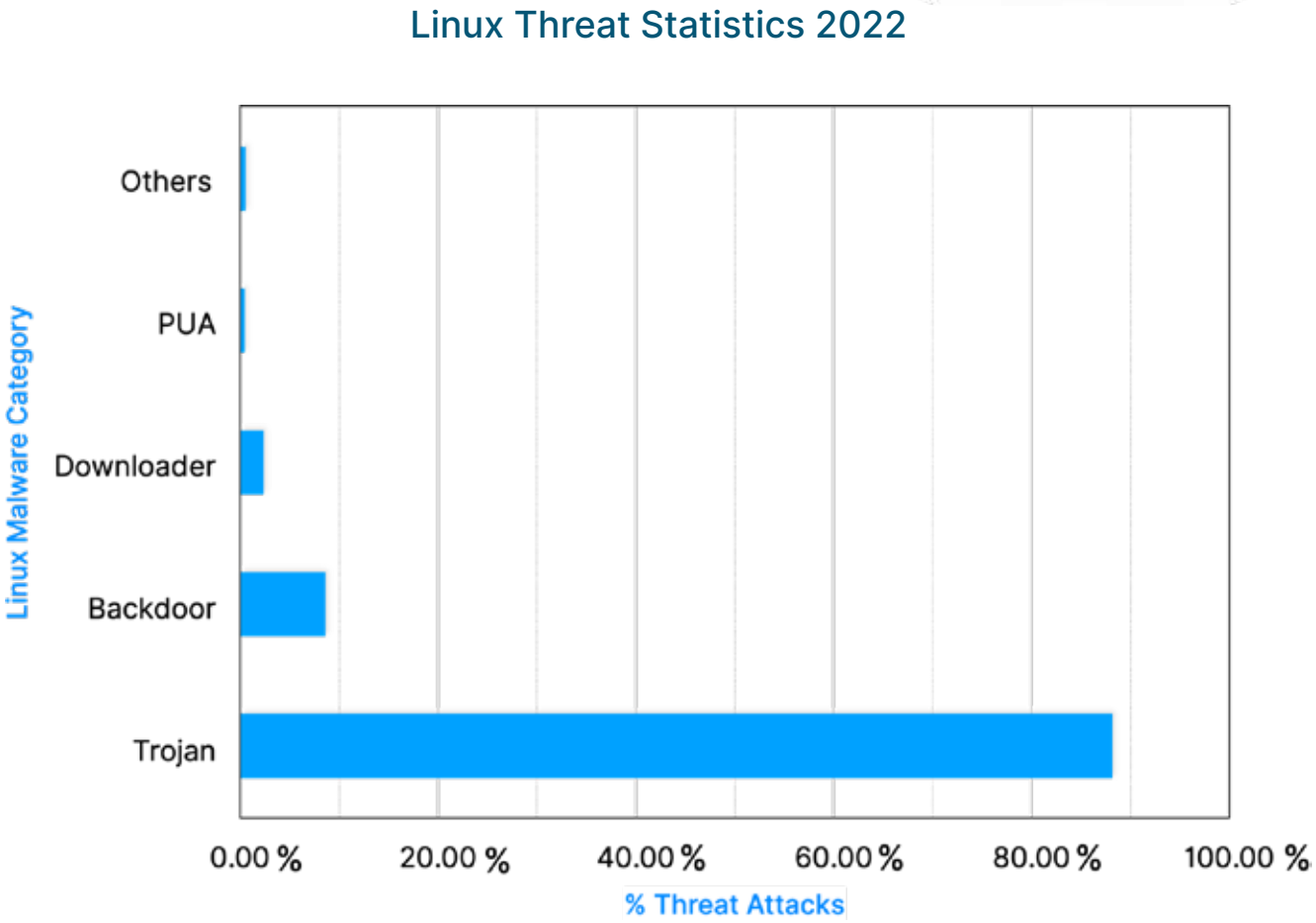


Figure 11 – Linux malware statistic for 2022 (source:av-atlas)

Predominant Malware Targeting the Linux Platform

Researchers have found several dangerous Trojans that specifically target Linux operating systems and aim to obtain users' personal information. These Trojans include **Mirai, BitConMiner, Gafgyt, Agent, Xorddos, and Tsunami**, among others, and have been widely detected in the wild, as shown below.

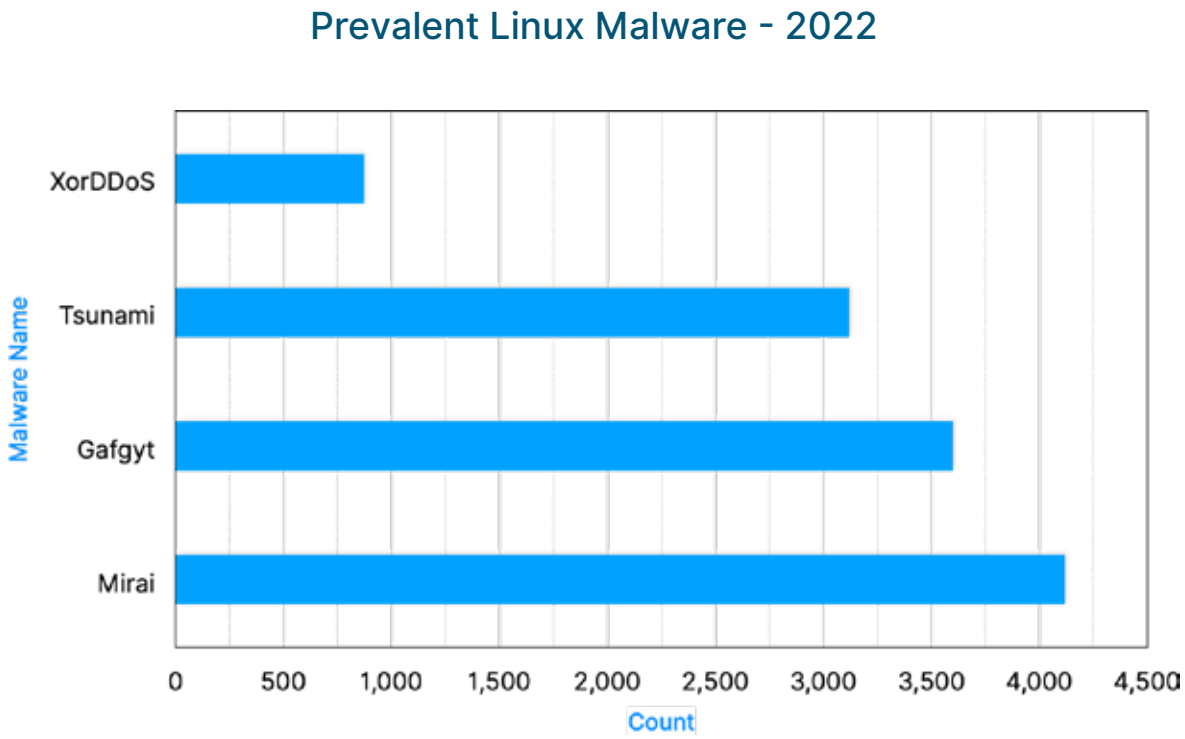


Figure 12 – Prevalent Linux Malware in 2022 (source: av-atlas)

Enemybot

In 2022, a new DDoS botnet known as Enemybot was discovered, which is derived from the leaked code of the malicious program **Gafgyt** and a few modules from **Mirai** to pursue crypto mining and Distributed-Denial-of-Service (DDoS) attacks.

Enemybot, which attributes itself to Kekses (a TA group specializing in crypto-mining and DDoS attacks), has been noticed targeting routers from **Seowon Intech and D-Link** and exploiting the **iRZ router** vulnerability to infect more devices.

Mirai

In April 2022, TrendMicro identified an active exploitation of the Spring4Shell vulnerability assigned as CVE-2022-22965 wherein malicious actors were able to weaponize and execute Mirai botnet malware on vulnerable servers, specifically in the **Singapore** region.

Chaos Malware

In April 2022, a new malware called Chaos was discovered, specifically targeting the Gaming, Financial Services, Technology, and Media & Entertainment industries. The malware offers **DDoS-as-a-service and a cryptocurrency exchange** service. Chaos malware focuses primarily on European regions, but some samples have also been found in the Americas and Asia Pacific regions.

SHC Loader

In 2022, a new malware SHC (Shell Script Compiler) loader was identified, targeting Korean users to infect systems with Monero cryptocurrency miners and DDoS **IRC bots**. According to researchers, the TAs used brute-force techniques to bypass weak administrator account credentials over SSH on a Linux server.

MCCrash

In December 2022, Microsoft identified a new Minecraft DDoS malware named MCCrash, targeting cross-platform to conduct Distributed Denial of Service (DDoS) attacks on Minecraft servers. This malware can also self-spread to other systems on the network by brute-forcing SSH credentials. Most of the devices infected by MCCrash are located in **Russia**, but there are also victims in **Mexico, Italy, India, Kazakhstan, and Singapore**.

BPFdoor

BPFdoor is a backdoor discovered in 2022 that remained undetected for more than five years while stealthily targeting Linux and Solaris systems. It allows TAs to remotely connect to a Linux shell to gain complete access to a compromised device. The BPFdoor attackers were mostly identified in the regions such as the **U.S., South Korea, Hong Kong, Turkey, India, Vietnam, and Myanmar**.

SideWalk

The SideWalk backdoor Linux version was identified in 2022, targeting East and Southeast Asia and other organizations outside these regions. APT group SparklingGoblin which is a State-backed Chinese Threat Actors group, is claimed to be behind the SideWalk backdoor's malicious campaign.

rshell

In 2022, multiple versions of a cross-platform instant messenger application focused on the Chinese market known as '**MiMi**' has been identified to deliver a new backdoor known as 'rshell' that can be used to steal data from Linux and macOS systems.

Researchers noticed unusual connections to this app while analyzing **Command-and-Control** (C&C) infrastructure for the HyperBro Remote Access Trojan (RAT) malware linked to the **APT27** Chinese-backed threat group.

More than a 75% increase in Ransomware Attacks on Linux Machines

In 2022, there was a significant uptick in the number of instances of ransomware malware being detected, including "LockBit" and "Conti". This spike in detections can be attributed to the rise of the "Ransomware-as-a-Service" business model, through which the creators of the ransomware and their affiliates have made significant profits.

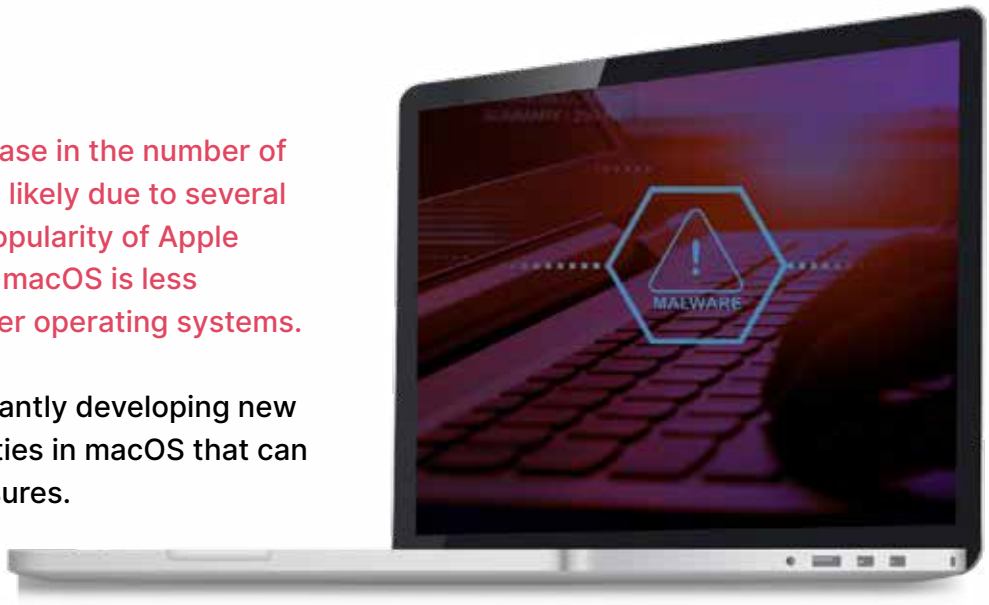
During the first half of 2022, a new type of ransomware called "Black Basta" was identified. It was successful in targeting over 50 different organizations. This group primarily relies on exploiting vulnerabilities in their attacks.

Cheerscrypt Linux ransomware with the capability of targeting ESXi servers was discovered.

A recently discovered malware known as "Shikitega" targets endpoints and IoT devices that operate on Linux systems. This malware downloads and runs the Metasploit's "Mettle" meterpreter to achieve maximum control over the infected machines. It takes advantage of system vulnerabilities to acquire elevated privileges, establishes persistence, performs crypto-mining activities, and misuses legitimate cloud services to store some of its C&C servers.

In 2022, the Hive ransomware developers converted their VMware ESXi Linux encryptor to the Rust programming language. They added new features to make it tougher for security researchers to investigate victims' ransom negotiations.

macOS Malware Trends



In 2022, there has been an increase in the number of attacks targeting macOS. This is likely due to several factors, including the growing popularity of Apple devices and the perception that macOS is less susceptible to malware than other operating systems.

Additionally, attackers are constantly developing new techniques to exploit vulnerabilities in macOS that can bypass traditional security measures.

We observed that the majority of threats detected on macOS systems were Potentially Unwanted Applications (PUAs), trojans, password stealers, downloaders, etc., as illustrated in the graph below. Additionally, there seemed to be a trend of using Go as a programming language among cybercriminals.

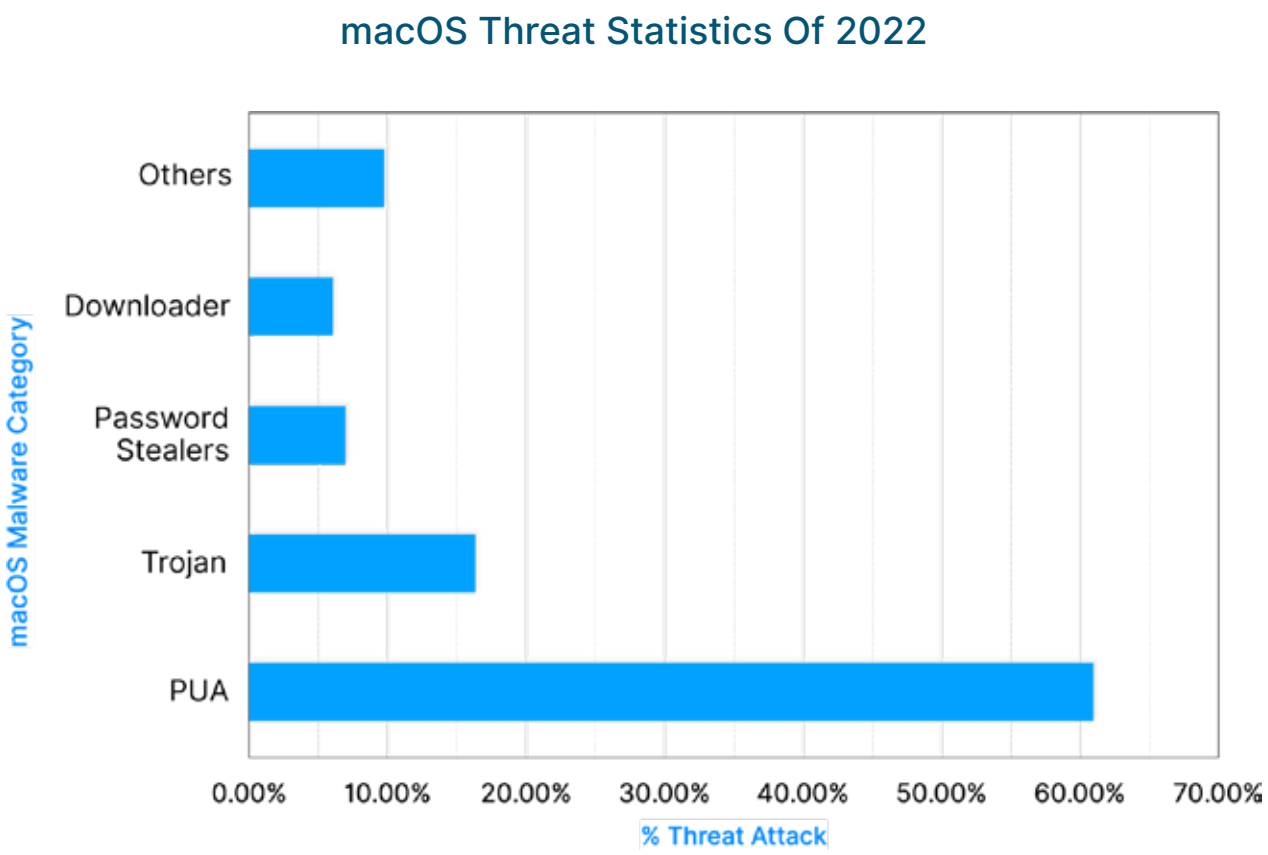


Figure 13 – macOS malware statistic for 2022 (source: av-atlas)

Predominant Malware Targeting the macOS Platform

Researchers have identified various harmful malware specifically designed to compromise macOS systems to obtain sensitive information from the affected individuals.

ChromeLoader

In January 2022, a malware called ChromeLoader, also known as ChromeBack or Choziosi Loader, was discovered by Paloaltonetworks. This malware quickly spread during the first half of 2022 through malvertising and spam campaigns. ChromeLoader disguises itself as a DMG file that contains a shell script.

The malware is either downloaded remotely from a specific URL or embedded in a separate file within the DMG and then installed by a Bash script. Once installed, the malware can deliver adware, steal information, and alter the victim's search engine results through the browser extension.

CloudMensis macOS spyware

ESET discovered CloudMensis in July 2022, a spyware downloader written in Objective-C and utilizes public cloud storage services such as **Dropbox, Yandex Disk, and pCloud** to communicate with its Command and Control server via access tokens.

The malware has various capabilities, including listing running processes, listing email messages and attachments, listing files on external storage, running arbitrary commands, exfiltrating files, and capturing screenshots.

Alchimist

In October 2022, Cisco Talos reported the discovery of Alchimist, a malware framework written in the Go programming language. The malware is designed as a cross-platform attack framework, with the primary objective of establishing a backdoor into the targeted system.

CrateDepression

In May 2022, SentinelLabs discovered CrateDepression malware which is written in the Go programming language. It has various features such as capturing screenshots, logging keystrokes, retrieving files remotely, exfiltrating data and maintaining persistence on the infected system.

DazzleSpy

ESET discovered DazzleSpy in January 2022, a highly sophisticated malware that employs advanced techniques to evade detection and maintain a foothold on infected devices.

oRAT

In January 2022, TrendMicro researchers identified a Go-based malware, named oRAT, that is a backdoor. An Advanced Persistent Threat (APT) group known as **GamblingPuppet** was behind this campaign to target gambling websites.

TraderTraitor

In August 2022, ESET identified malware targeting Coinbase users. Researchers discovered that this attack was conducted by a North-Korean APT group known as **Lazarus**.

APT Attacks Highlight for 2022

APT attacks allow Threat Actors to break into an organization's network without alerting security systems. Therefore, these pose considerable risks for all organizations, regardless of their scale.

The Russia-Ukraine conflict has given APT groups an edge in successfully conducting spear-phishing campaigns. People are inherently curious to know more about the developing situation around the conflict in Ukraine and typically do not think twice before opening an email linked to it.

In addition to the Russia-Ukraine conflict, some crucial geopolitical conditions, including countries initiating hostile actions against other countries, have also given rise to state-sponsored APT attacks for spying and cyber espionage.

The use of supply chain attacks and Zero-day vulnerabilities provides an edge to the Threat Actors while targeting organizations. We have curated some notable APT attacks of the year 2022.

The figure below shows certain remarkable APT attacks identified in each month of 2022.

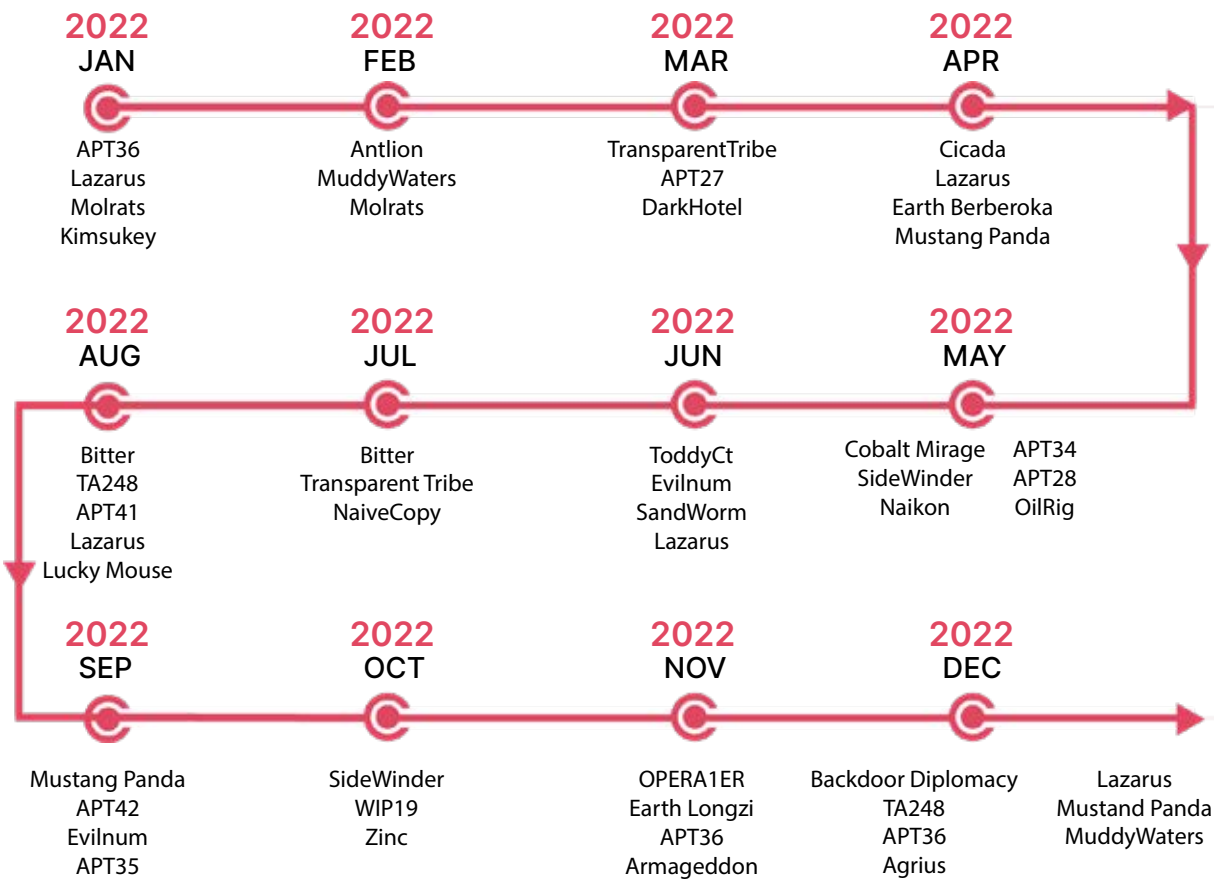


Figure 14 - APT Attack Timeline for 2022

We have put together an analysis of some critical APT campaigns that affected various victims globally in 2022. These state-sponsored attacks utilize techniques ranging from spear phishing to exploiting zero-day vulnerabilities.

Gamaredon APT

Gamaredon APT group is a state-sponsored APT group attributed to Russia and is involved in various information theft and cyber espionage operations. Gamaredon group is also known as Winterflounder, Primitive Bear, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, and Callisto.

In its global operations, Gamaredon APT has been targeting Defence, Government, Law enforcement, NGOs, diplomats, and journalists since 2013.

Gamaredon APT uses a spear-phishing campaign to attack victims for the initial infection stage. After penetrating the victims' system, Gamaredon deploys custom malware or **VNC tools** for lateral movement and data extraction. Such tools include Aversome infector, EvilGnome, FRAUDROP, Gamaredon, Pteranodon, RMS, Resetter, and UltraVNC.

In a recent campaign, Gamaredon APT targeted Ukrainian citizens, luring them with malicious document files containing a remote template embedded with a VBScript macro. This macro downloads a RAR file from a remote server with a malicious LNK file inside. The final malicious binaries are dropped in several stages to evade detection.

Lazarus Group

The Lazarus group has been one of the most active APT groups operating since 2009. Operating under various aliases, including Hidden Cobra, Whois Team, and ZINC, the Lazarus group has been attributed to North Korea by multiple agencies. Some other APT groups are also related to Lazarus, like Andariel, APT37, APT38, and Kimsuky.

Lazarus group has been behind various cyber-attacks since 2009's operation Troy, an unsophisticated DDoS attack against websites in the United States and South Korea. Other notable cyber-attacks are the **Sony breach** (2014), **Bangladesh Bank cyber heist** (2016), the **WannaCry Ransomware** attack, etc.

Lazarus group uses 1-day vulnerabilities and phishing campaigns for cyber-attacks. The Lazarus group uses multiple malware, including AppleJeus, DarkComet, DoublePulsar, EternalBlue, Gh0stRAT, Mimikatz, WannaCry, etc., and uses multiple malware tools. At the end of 2022, Lazarus conducted campaign operation interception using signed binaries.

Transparent Tribe

Transparent Tribe is an APT group attributed to Threat Actors in Pakistan. It is also known as APT 36, ProjectM, Mythic Leopard, Templatic, and Copper Fieldstone. Transparent Tribe started its operations in 2012, targeting Indian embassies in the Middle East. It has been highly active ever since, performing operations around the globe.

The group uses spear-phishing campaigns to compromise the victims utilizing current affairs topics such as defense news, resumes, CVs, military-related maldocs, and honey traps. In some cases, they have used compromised websites as well. Transparent Tribe also has employed tools like **CrimsonRAT**, **BreachRAT, LuminosityRAT, and QasarRAT** for cyber espionage in their past operations. The APT group continuously evolves its arsenal for new attacks. In recent attacks in 2022, it has used LimePad as the final payload.

The infection chain of the latest attack started with a phishing campaign using maldocs that contained a link to the compromised website. This compromised website hosts the **ObliqueRAT** payload, and once the victim clicks the download link, it drops the RAT into the system. This RAT has capabilities to identify anti-malware processes employed in the system. After the check, ObliqueRAT connects to the C&C server for further operations. ObliqueRAT has multiple versions and is continuously evolving.

New APT Groups

In addition to pre-existing APT groups, two notable groups have been identified by researchers.

Dark Pink

In the APAC region, a new sophisticated threat actor has been identified, which has been attacking government and military entities. This group, called Dark Pink or Saaiwc Group, uses custom malware to steal confidential data and employ uncommon TTPs. To spread malware and steal data, the actor has been observed using a custom toolkit and **DLL side-loading** and event-triggered execution methods.

According to a report from Group-IB, a cybersecurity firm, Dark Pink, an APT, successfully launched seven attacks between June and December of 2022. The objective of the threat actor is to collect data from the victim's browser, access messengers, extract documents, and record sound from the infected microphone.

Although Group-IB confirms with high confidence that Dark Pink is responsible for seven attacks, the researchers note that the number could be higher.

Adastrea

Adrastea, an online threat actor who claims to be a group of independent cybersecurity specialists and researchers, has allegedly hacked MBDA, a European multinational developer and manufacturer of missiles that was created through the merger of the main French, British and Italian missile systems companies (Aérospatiale–Matra, BAE Systems, and Finmeccanica (now Leonardo). The name MBDA is derived from the initialism of the names of these three missile companies: Matra, BAe Dynamics, and Alenia.

Adrastea declared that they have uncovered critical vulnerabilities in the company's infrastructure and have exfiltrated **60 GB of confidential** documents. They revealed that the stolen material includes details of the company's personnel involved in military ventures, trade dealings, contract accords, and communication with various other businesses.

Tools and Tactics Used by APT groups in 2022

With the ongoing Russia-Ukraine conflict, TAs have also started weaponizing this information by targeting their victims via maliciously crafted documents. There are multiple recorded instances of APT groups using the various ongoing advancements and other related information to target government employees. This way, APT can infiltrate into organizations and establish persistence for future operations.

Nation-states have been known to use cyberattacks for the purposes of espionage and information theft. In particular, state-sponsored APT groups have crafted attacks to target nations seen as enemies. An example of this is the Lazarus APT group, which has been known to target Ukrainian Military and Government stakeholders. This is a particularly concerning matter due to the multiple conflict zones and highly volatile geopolitical situations worldwide.

Ransomware gangs are seeking out affiliates with access to corporations or essential infrastructure in Western countries, offering them a profit-sharing agreement. The threat of a ransomware attack, which could inflict serious damage, is made even more concerning when the perpetrators are APT groups, who have the capability to cripple essential national infrastructure.

Cobalt Strike is a post-exploit remote access tool employed by cybercriminals with a range of built-in capabilities for data exfiltration and lateral movement to other vulnerable systems on a network. The Cobalt Strike beacon is mostly used as a terminal payload for carrying out malicious operations on the targeted network. Additionally, APT groups have been known to deploy custom malware to steal sensitive information from the victim system.

Vulnerability Trends

There is a vulnerability behind almost every cyberattack that impacts every organization's security. We observed that the number of reported vulnerabilities is growing every year. There are remarkable data points to consider in the example of the last 6 years alone, with just 6,454 vulnerabilities reported in 2016. This number is 2022 stood at 25,226 vulnerabilities.

The figure below gives a comparison of vulnerabilities found from 2009 to 2022.

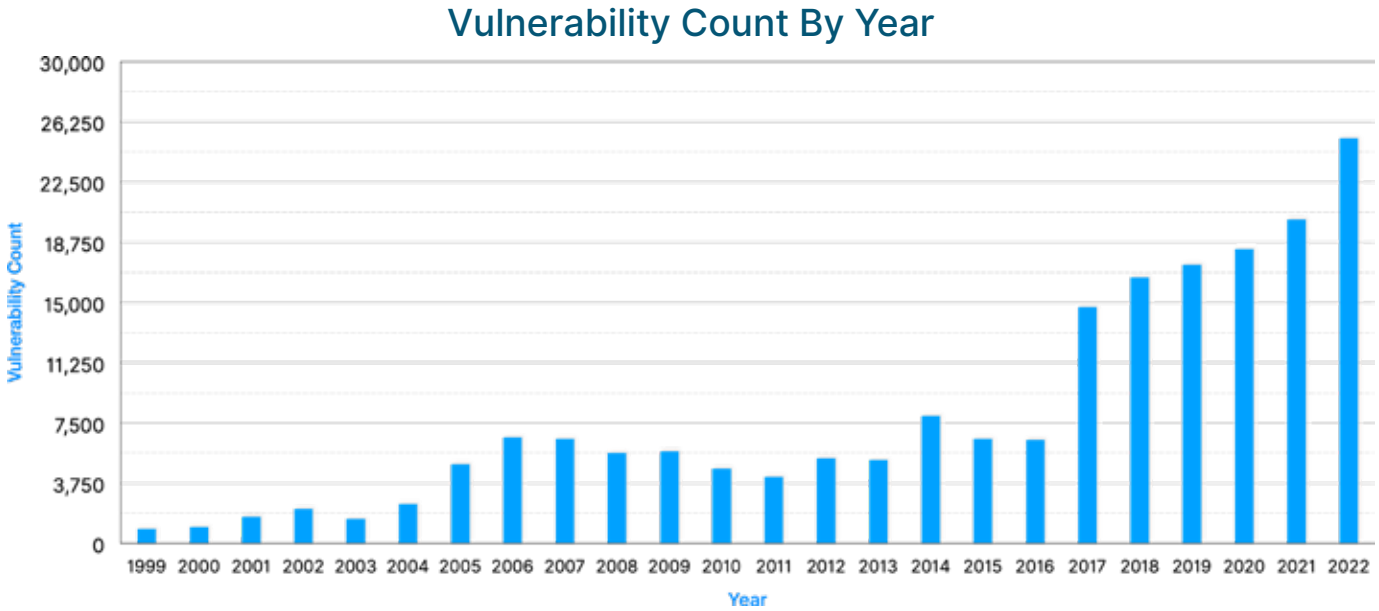


Figure 15 - Vulnerabilities Identified Since 1999 [Data Source: cvedetails]

Last year 25,226 vulnerabilities with an average weight of 3.7 CVSS (Common Vulnerability Scoring System) were reported, which is half of the previous year, which was 6.5. Out of the total vulnerabilities, 860 (3.40%) were given a CVSS score of 9-10. Our researchers found that, on average, 69 CVEs (Common Vulnerabilities and Exposures) are reported daily. Approximately 2,100 vulnerabilities are reported every month.

The figure below shows the monthly distribution of vulnerabilities discovered during the year 2022.

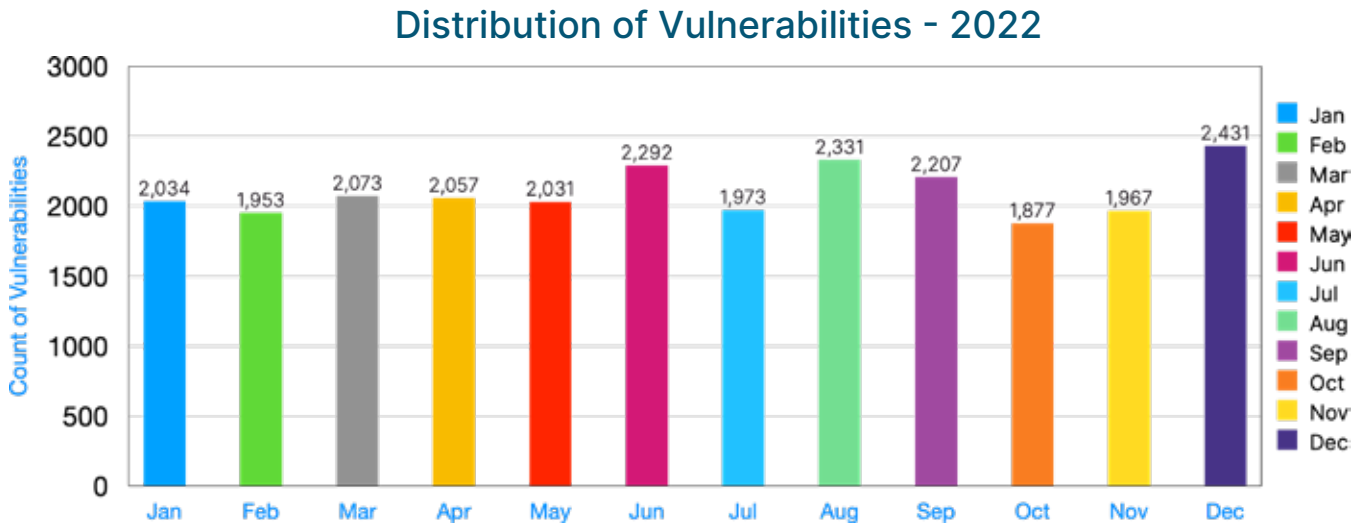


Figure 16 - Distribution of Vulnerabilities on a Monthly Basis [Data Source: cvedetails]

In 2022, most of the vulnerabilities (8,243) were reported in various products of **Microsoft** due to its vast user base, followed by **Oracle** with 8,043 CVEs reported.

The figure below depicts the count of vulnerabilities on the Top 10 products.

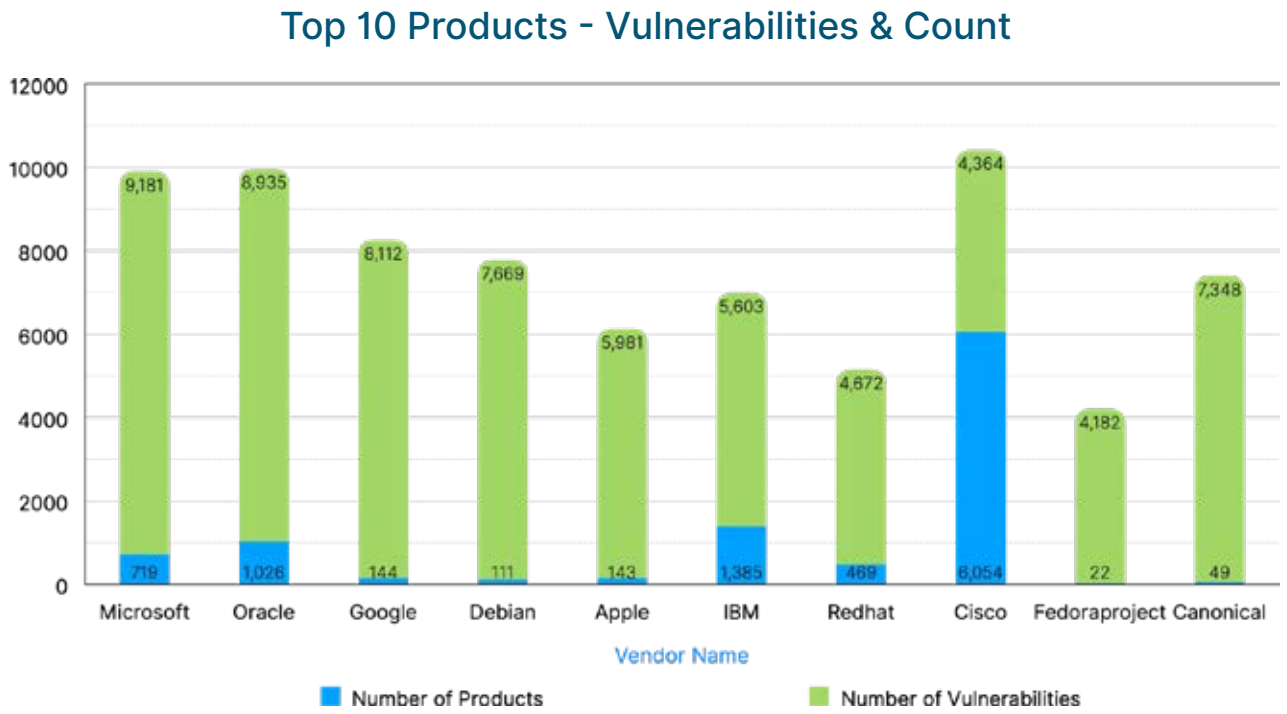


Figure 17: Vulnerabilities in Top 10 Products [Data Source: cvedetails]

Our observations indicated that **Debian Linux** was the most targeted product and reported the highest vulnerabilities in 2022, followed by **Android and Ubuntu Linux**.

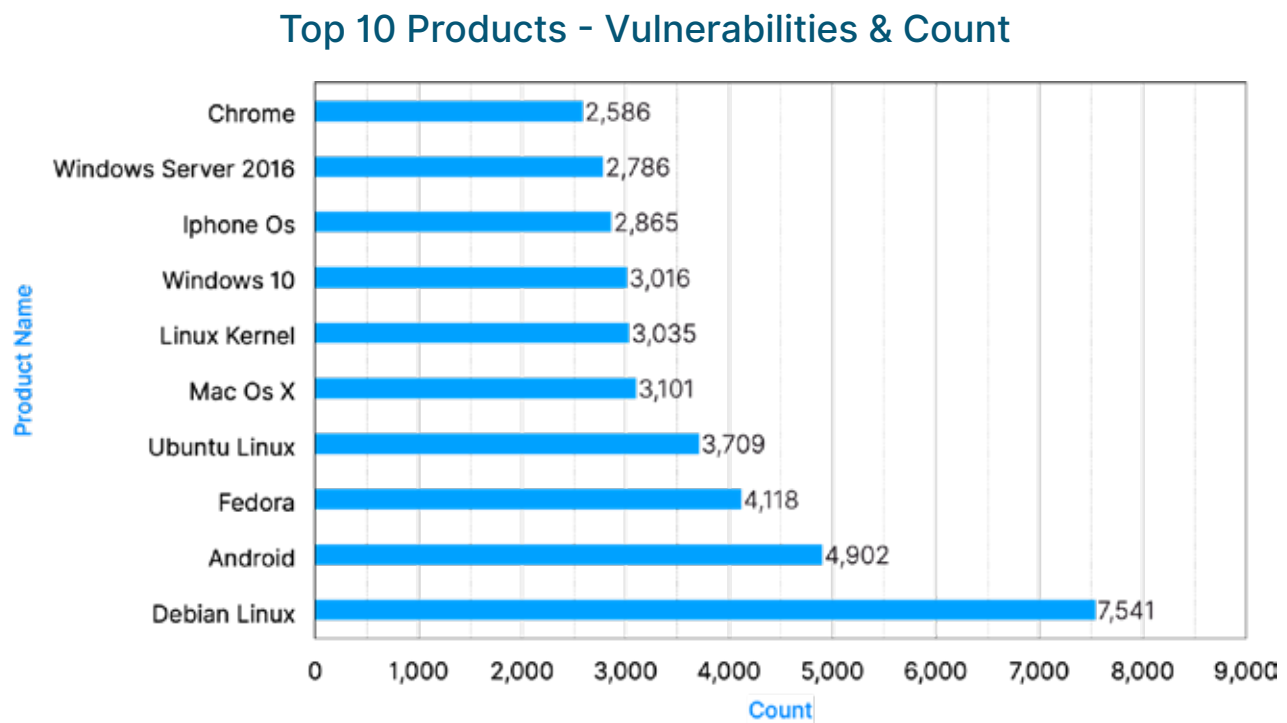


Figure 18 - Top 10 Products with Vulnerabilities in 2022 [Data Source: cvedetails]

Some of the top vulnerabilities of 2022 are discussed in the following sections.

Follina MSDT Bug (CVE-2022-30190)

This zero-day flaw was identified in the built-in MS URL handlers (ms-msdt:) that would trigger the **Microsoft Support Diagnostic Tool** (MSDT) process used to run code on the target system. It named the vulnerability '**Follina**' after the Italian city whose area code (0438) matched the numbers written on the malware sample file name(05-2022-0438.doc). This bug could be exploited even if Macros were turned off completely.

Spring4Shell/Springshell (CVE-2022-22965)

Spring4Shell affects spring framework applications running JDK 9+ versions that use a data-finding functionality, allowing an attacker to run unauthenticated **Remote Code Execution** (RCE). This issue was exploited in the wild and may still be the case.

BIG-IP iControl REST RCE (CVE-2022-1388)

The CVE-2022-1388 flaw enables Remote Code Execution on systems using affected versions of **F5 BIG-IP** running **iControl REST API** and gives the attacker full control over these servers. The vulnerability priority rating for this bug was rated critical due to the public-facing nature of this service and the high rate of exploitability combined with the nature of the issue (authentication bypass).

Google Chrome Use After Free in Animation (CVE-2022-0609)

In the affected Google Chrome versions (prior to 98.0.4758.102), a remote attacker may exploit **use after free** in an animation via a crafted HTML page. A use after free is a type of memory corruption flaw in which a program continues to use a memory address after the associated memory has been freed (deallocated).

ProxyNotShell(CVE-2022-41040 and CVE-2022-41082) in Exchange

The first of these two bugs, CVE-2022-41040, is an SSRF (**Server-side Request Forgery**) vulnerability. When exploited, it allows an authenticated user to remotely trigger the CVE-2022-41082, which allows RCE when PowerShell is accessible to a threat actor. Both vulnerabilities are part of the attack flow and require an authenticated session (standard email user credentials) for exploitation.

Zimbra RCE (CVE-2022-27925 and CVE-2022-41352)

Attackers could exploit these vulnerabilities by sending malicious emails containing specially crafted attachments or links that allow them access to a vulnerable system's files or user accounts. CVE-2022-27925 relates to an RCE vulnerability in ZCS that was patched in March 2022. CVE-2022-41352 related to unsafe usage of cpio utility where cpio is in use. In case of a pax utility in use (over cpio), the affected system can't be exploited because amavisd (**Zimbra's AV engine**) prefers pax, and pax is not vulnerable to this issue.

Atlassian Confluence Vulnerability (CVE-2022-26134)

As this flaw affected all supported versions of the confluence server, this vulnerability was exploited in the wild benefitting crypto-mining and other malware. Multiple proof of concepts were available on GitHub to exploit this critical unauthenticated OGNL injection Remote Code Execution vulnerability that affected the Confluence server and data center.

ZyXEL Vulnerability (CVE-2022-30525)

An unauthenticated remote command injection was identified by Rapid7 that affected **Zyxel firewalls** supporting ZTP (ATP, VPN, USG flex series). This flaw allowed an unauthenticated, remote attacker to achieve arbitrary code execution as a nobody user on the affected device.

A statistical view of vulnerabilities from Sensors

The statistical view from Cyble sensors shows the data perspective of the most targeted vulnerabilities and attacks from various locations. The figure below shows the timeline of various attacks on one of our sensors in the last quarter of 2022.

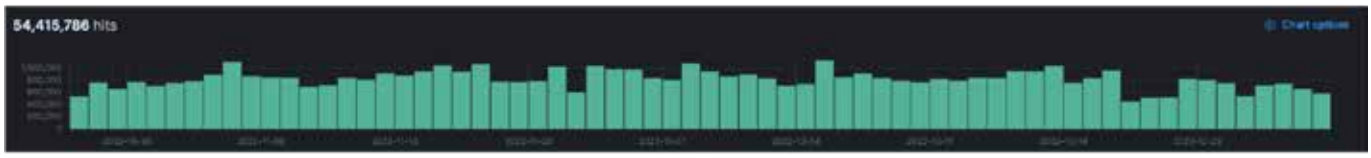


Figure 19 - Timeline of Various Attacks on our Sensors for Last Quarter of 2022

The most targeted vulnerabilities captured by our sensors are depicted in the figure below. One of the most targeted vulnerabilities found by the sensor is CVE-2020-11899 (Treck TCP/IP stack before 6.0.1.66 has an IPv6 'Out-of-bounds' read).

The figure below shows the targeted vulnerabilities in the last quarter of 2022.

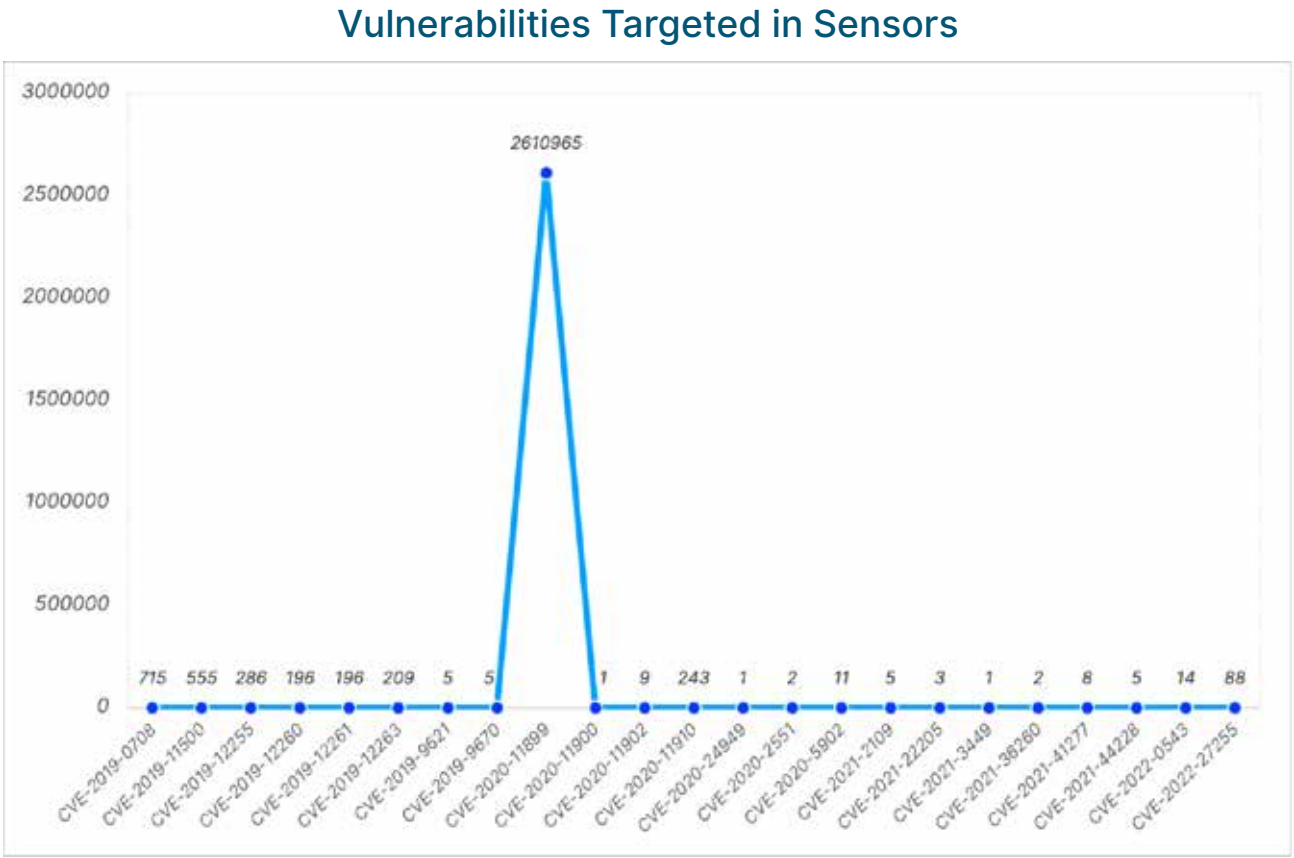


Figure 20 - Vulnerabilities Targeted in Our Sensors for Last Quarter of 2022

Operational Technology (OT)

Critical Infrastructure Sectors and devices used within this environment are critical to/ the functioning of modern societies, as they control and monitor processes in sectors such as energy, transportation, water, and manufacturing. Hence, Cyble actively monitors evolving threat landscape of Operational Technlogy.

Major Cyber Incidents targeting the Critical Infrastructure Sector

In 2022, there was a significant increase in cyber attacks targeting organizations in the critical infrastructure sector, with a notable increase in the complexity and advanced nature of these attacks. The barrage of attacks on Critical Infrastructure observed included:

- Multiple Ransomware Attacks were carried out for monetary gain, reputational damage to organizations, and operational loss.
- Deployment of ICS-specific malware and wipers (Pipedream, Industroyer2)
- Data leaks over the dark web containing sensitive documents, reports, blueprints, credentials, etc.
- Insider threats which involved leaking of sensitive intelligence and USB attacks.
- Targeted attacks on employees dealing in critical infrastructure
- Active scanning and exploitation of ICS-specific products, protocols, devices, etc.
- The exploitation of vulnerabilities in IT/OT/IoT devices to gain a foothold in the organization's environment.
- Use of default credentials, misconfigured devices, internet exposed devices by Threat Actors (TA) to gain access to Critical Infrastructure.
- Regional riots interrupting the operations of organizations dealing with critical infrastructure
- Military attacks involving the use of missiles and drones on Critical infrastructure such as substations, power generation units, healthcare facilities, etc.

Among numerous attacks on the Critical Infrastructure sector, below is a timeline of some notable incidents.

February 2022

Acid Wiper Malware targeted Viasat Ka-Sat Modems, which affected 5,800 wind turbines in Europe.

February 2022

CISA and FBI released an advisory for Indicators of Compromise (IOCs) related to BlackByte Ransomware Group in which they state, "BlackByte ransomware had compromised multiple US and foreign businesses, including entities in at least three US critical infrastructure sectors (government facilities, financial, and food & agriculture)."

March 2022

Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released an advisory stating "possible threats to U.S. and international satellite communication (SATCOM) networks".

March 2022

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Energy (DOE) released an advisory that provides information on multiple intrusion campaigns conducted by state-sponsored Russian cyber actors from 2011 to 2018 and targeted U.S. and international Energy Sector organizations.

March 2022

FBI released an alert stating that "52 entities across 10 critical infrastructure sectors affected by RagnarLocker ransomware, including entities in the Critical Manufacturing, Energy, Financial Services, Government, and Information Technology sectors."

March 2022

FBI and CISA released an advisory for Indicators of Compromise (IOC) related to AvosLocker Ransomware in which they state, "AvosLocker is a Ransomware as a Service (RaaS) affiliate-based group that has targeted victims across multiple critical infrastructure sectors in the United States including, but not limited to, the Financial Services, Critical Manufacturing, and Government Facilities sectors."

April 2022

Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) released a joint cybersecurity advisory to warn that certain Advanced Persistent Threat (APT) actors have exhibited the capability to gain full system access to multiple Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) devices.

April 2022

The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom released a joint cybersecurity advisory, this joint advisory intended to warn organizations of Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.

June 2022

CISA released an advisory providing details about People's Republic of China (PRC) state-sponsored cyber actors continuing to exploit publicly known vulnerabilities to establish a broad network of compromised infrastructure. The advisory details the targeting and compromise of major telecommunications companies and network service providers and the top vulnerabilities, primarily Common Vulnerabilities and Exposures (CVEs) associated with network devices routinely exploited by cyber actors since 2020.

June 2022

Iran's major crude steel production halted due to a cyber-attack.

July 2022

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of the Treasury (Treasury) released a joint advisory to provide information on Maui ransomware, which has been used by North Korean state-sponsored cyber actors since at least May 2021 to target Healthcare and Public Health (HPH) Sector organizations.

August 2022

Cyble Global Sensor Intelligence (CGSI) observed attackers actively exploiting Virtual Network Computing (VNC) and distributing intelligence over Darkweb and cybercrime forums.

September 2022

CISA and NSA released a joint advisory describing the TTPs malicious actors use to compromise OT/ICS assets. It also recommends mitigations that owners and operators can use to defend their systems.

September 2022

Cyble actively monitors sensitive leaks over the Darkweb and cybercrime forums. A major leak related to Iran Atomic Energy Organisation became public in September. Cyble Research & Intelligence Labs has published a blog detailing leaks related to the nuclear sector, "CyberThreats Mushrooming Over Global Nuclear Facilities".

September 2022 Threat Actors (TAs) targeted multiple industries in the Telecommunication sector, and Optus Breach was one of the major cyber incidents that affected a large population in Australia.

October 2022 The Hive ransomware group leaked sensitive data related to TATA power over the dark web.

November 2022 A cyber attack forced the Denmark train network to halt its operations.

December 2022 Voyager Worldwide, a Singapore-based provider of maritime technology solutions, was reportedly targeted by a cyber-attack in early December. All systems at the navigation services and solutions company were taken offline on December 2nd. Customers include over 1,000 shipping businesses from all around the world.

December 2022 Threat Actors targeted multiple hospitals in the last three months; AIIMS India was one of the recent victims of a cyber attack.

Vulnerability Overview for Industrial Control Systems (ICS) / Operational Technology (OT)

Integrating IT and OT systems in the Critical Infrastructure sector has increased the opportunities for targeted attacks by exploiting vulnerabilities. Organizations must prioritize protecting the most critical assets in their operations and safeguarding Cyber Crown Jewel.

The landscape of vulnerabilities in the OT sector involves cooperation between state and private organizations, who work together to detect and notify of vulnerabilities in various ICS components.

Organizations in the CI sector should take into account the use of a Software Bill of Materials (SBOM), darkweb leaks, and advisories released by state entities and official vendors when addressing vulnerabilities in their environment, as attackers are actively scanning for assets to perform lateral movement and target specific assets.

OT Vulnerability Severity Overview

The figure below illustrates the severity of vulnerabilities affecting various ICS components used in Critical Infrastructure sectors, as reported by the top 10 vendors for the year 2022.

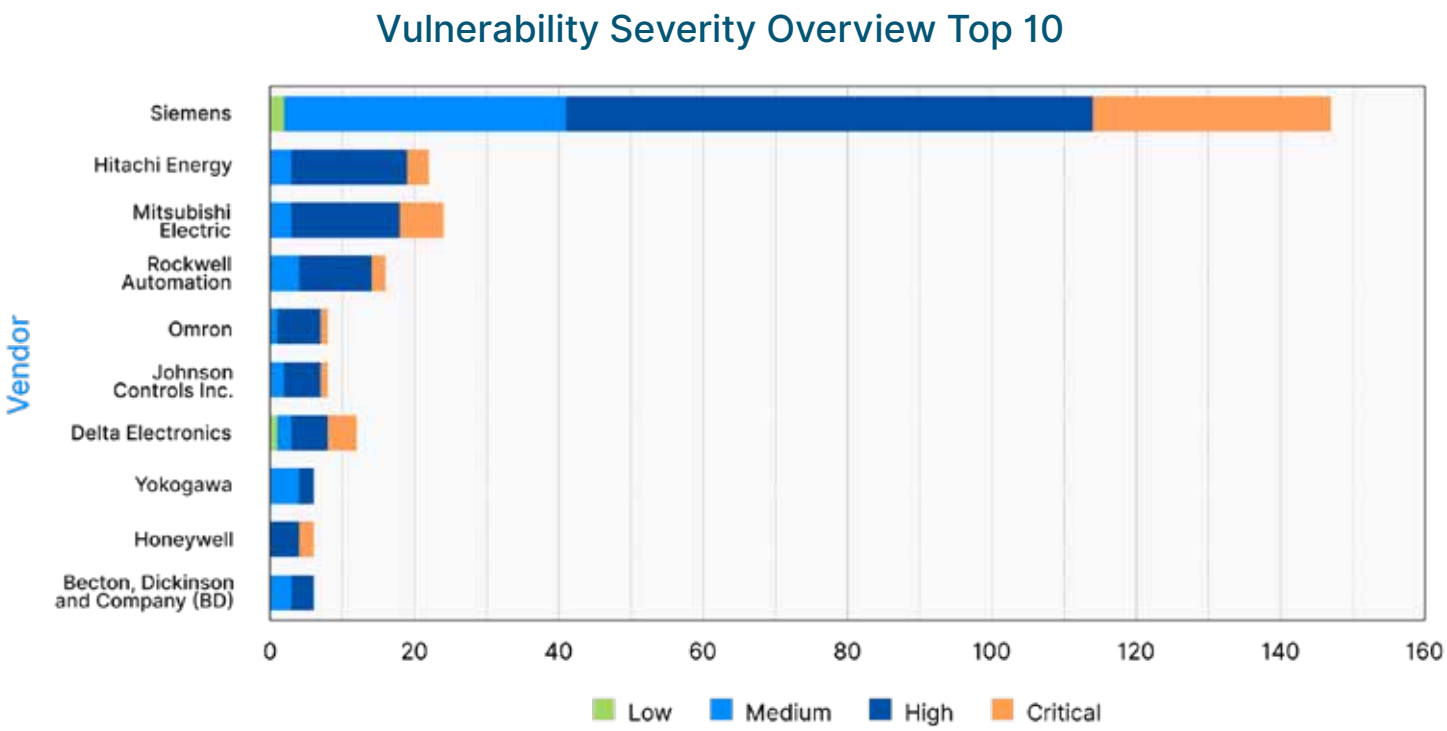


Figure 21 – Vulnerability Severity Overview – Top 10 Vendors

OT Advisory Overview for 2022

The following figure represents the number of alerts and advisories released by vendors operating in different Critical Infrastructure sectors.

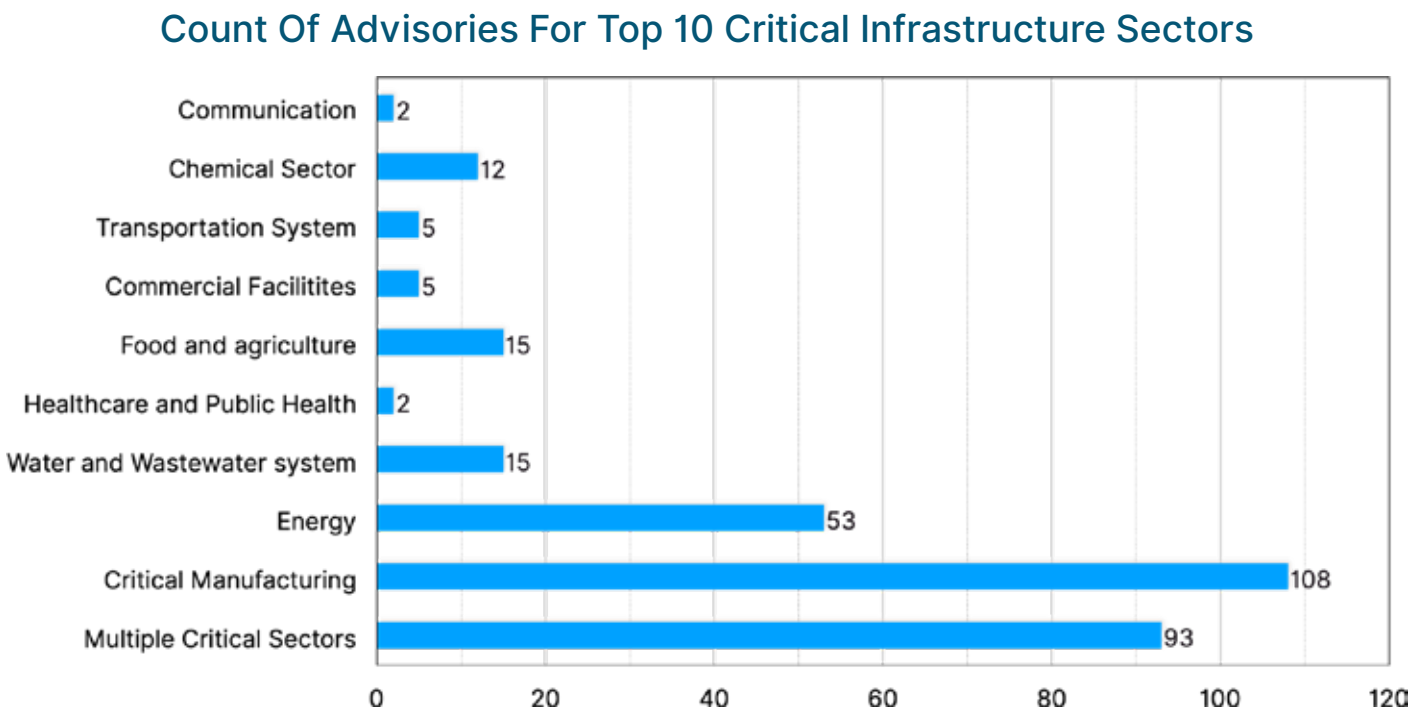


Figure 22 – Count of Advisories released for Top 10 CI sectors (Source: ICS Advisory Project)

Critical Infrastructure (CI) Sector-Specific Exploitation Attempts

In previous years, we saw a surge in hacktivist groups targeting Industrial Specific protocols and assets exposed over the internet. Cyble actively monitors Industrial Control System (ICS) exploitation and scanning attempts by Threat Actors (TAs) through its extensive network of Global Sensors.
The figure below shows industry-specific exploitation attempts observed by our ICS/OT sensor network.

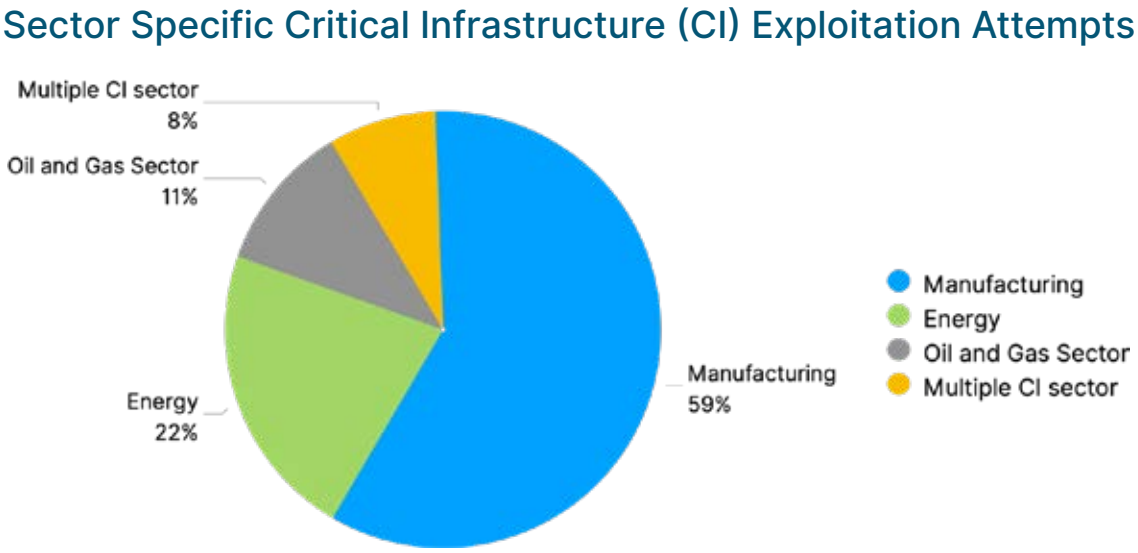


Figure 23 – Sector-specific CI exploitation attempts

Phishing Attacks

Cybercriminals commonly use phishing to gain access to victims' systems, often used as a primary method of infection. Phishing is a well-established method used by Threat Actors and APT groups to infiltrate victims' systems and networks, as it doesn't require technical knowledge. Combating phishing attacks has proven difficult for cybersecurity professionals, as individuals remain the primary target of Threat Actors. Phishing can be conducted through various means, such as email, text messaging, and social media platforms.

In 2022, there was a significant increase of more than 60% in the number of phishing attacks when compared to the previous year. The industries most targeted by the phishing attacks were Healthcare, Professional and Scientific Services, and Information Technology. According to our research, 76% of all attacks were focused on spear-phishing to obtain login credentials.

SlashNext researchers recorded a 50% increase in attacks on **mobile devices**, with scams and credential theft at the top of the list of payloads. In 2022, researchers found an 80% growth in threats from reputable services like **Microsoft, Amazon Web Services, or Google**.

Around 32% of all threats are now being hosted on these trusted services, according to the research. The figure below shows the statistics of top-level domains abused in 2022.

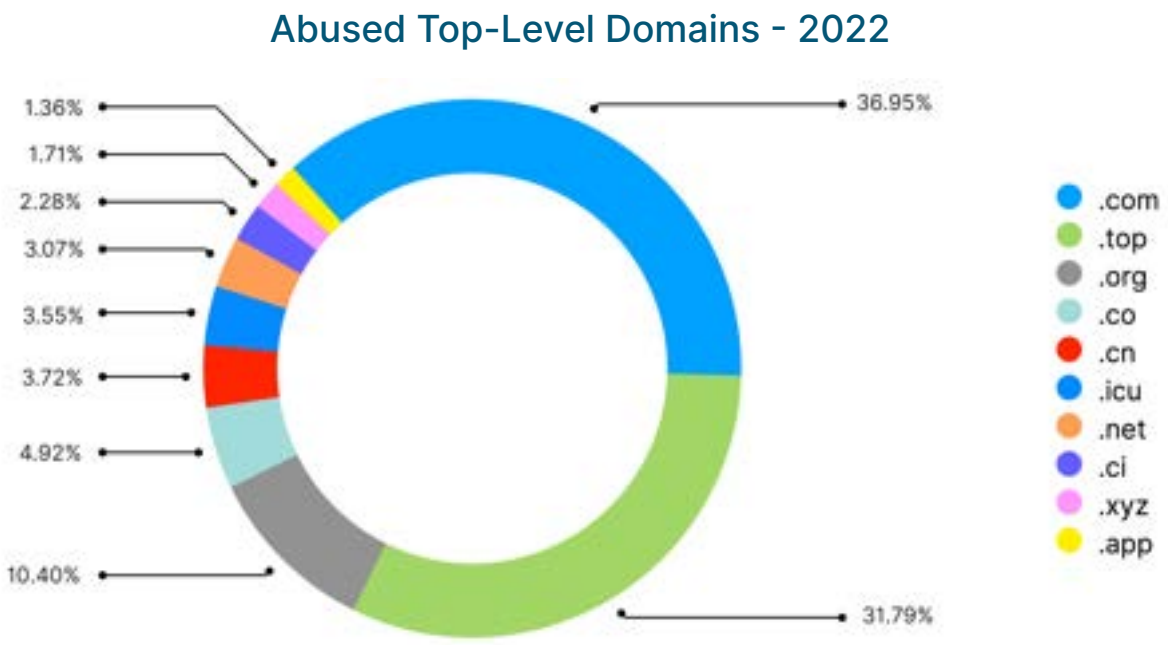


Figure 24 - Statistical View of TLD's Abused in 2022 Phishing Attacks (source: phishstats)

Phishing attacks are typically targeted at countries with a high concentration of individuals and organizations with valuable personal and financial information. These countries also tend to have a high level of internet penetration, making it easier for attackers to reach potential victims. Additionally, many phishing attacks are targeted at specific industries, such as **Banking and Finance, Healthcare, and Technology**, which are also more prevalent in developed countries.

The statistics below show the most targeted countries in 2022.

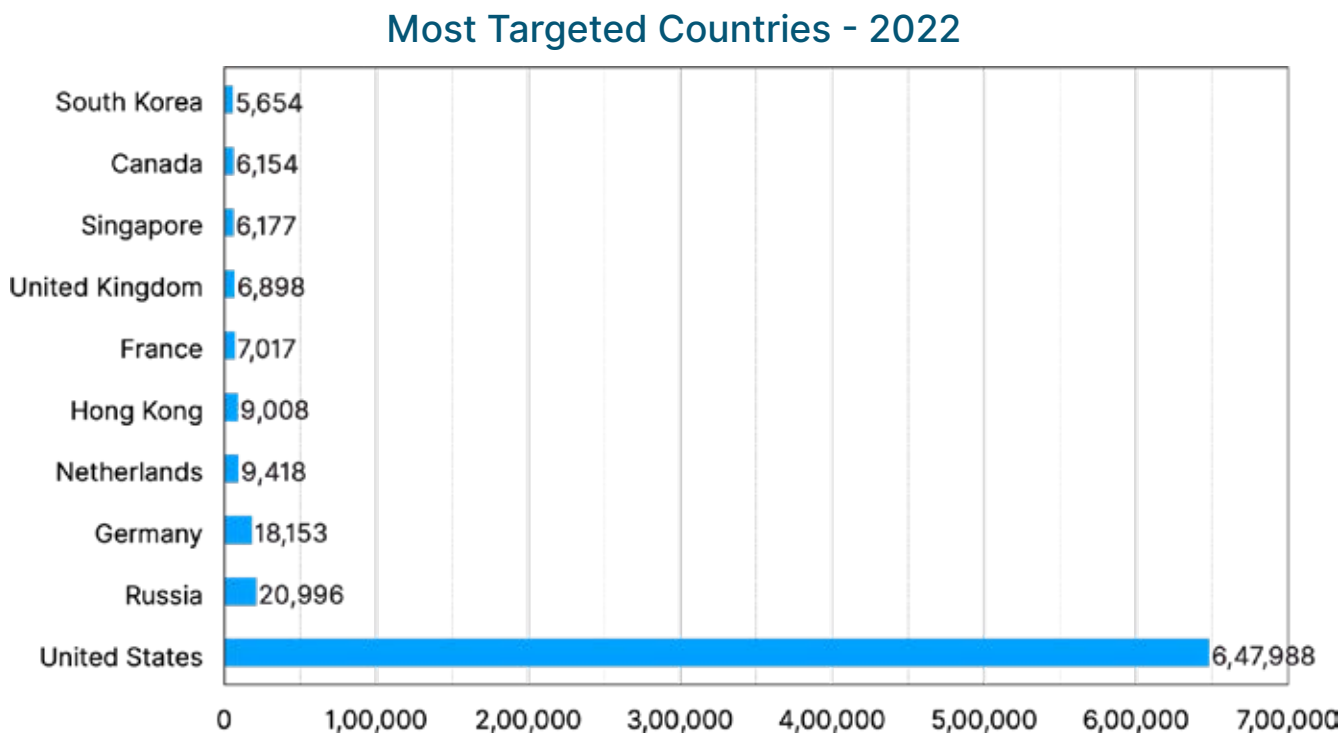


Figure 25 - Statistical View of Most Targeted Countries in 2022 (source: phishstats)

Predominant Phishing Attacks in 2022

Acorn Financial Services

In August 2022, an Acorn employee fell victim to a phishing attack, where their email credentials were stolen. As a result, the attackers gained access to internal information in the employee's email account, including sensitive information such as names, addresses, financial account numbers, and Social Security Numbers of customers. Acorn launched an investigation and informed its impacted customers of the breach. To prevent similar incidents in the future, Acorn should consider implementing a phishing detection and takedown service.

Twilio

In August 2022, Twilio experienced a data breach due to an SMS phishing attack. The attackers used this method to steal employee credentials by redirecting them to a fake website resembling Twilio's authentic site. As a result, the attackers were able to gain access to internal company resources and steal customer data. The attackers also compromised 93 Authy accounts, impacting approximately 75 million users, and potentially exposed 1,900 accounts on Signal's encrypted communication app by initiating account takeovers. To prevent similar incidents in the future, Twilio could have implemented measures to proactively identify and take down fake authentication sites before employee credentials were stolen, which would have helped mitigate the attack's impact.

Allegheny Health Network

In July 2022, the Allegheny Health Network suffered a data breach due to a phishing campaign where employee credentials were stolen. The attackers used these credentials to access the sensitive personal and health information of about 8,000 patients, including names, medical history, addresses, phone numbers, driver's license numbers, and email addresses. To prevent similar incidents in the future, the network could have implemented measures to automate the detection and takedown of digital risks online, which would have helped identify the phishing campaign and stop further damage. Given the permanent nature of medical history, protecting the integrity of patient data should be treated as a top priority.

Mailchimp

In March 2022, Mailchimp fell victim to a cyber-attack where the attackers used social engineering tactics to trick employees into giving away their credentials. With these credentials, the attackers gained unauthorized access to 319 Mailchimp customer accounts and exported mailing lists from 102 of those accounts. The attackers then used these accounts to launch phishing attacks that appeared legitimate due to them coming from Mailchimp emails. The attackers may have also gained access to API keys that could be used for further automated email-based phishing campaigns. This incident highlights the importance of employee awareness training and monitoring for suspicious activity to detect and prevent such attacks.

Targeted Phishing Attacks

Threat Actors Leveraging FIFA to Launch Phishing campaigns

In 2022, CRIL analyzed a phishing campaign where Threat Actors targeted individuals primarily in the Middle East by creating fake websites related to FIFA and sending emails with FIFA themes.

For example, a phishing website named "football-balance[.]com" was created to impersonate the Binance cryptocurrency website to trick users into providing sensitive information by offering free Non-Fungible Tokens (NFTs) as bait.

Figure 3 – FIFA-Themed Website Offering NFT

When scanned, the QR code displayed on the phishing website would compromise the user's wallet, allowing the attacker to steal funds from it.

Figure 4 - QR code displayed by phishing sites

Threat Actors Targeting Japanese National Tax Agency

In September 2022, CRIL analyzed a phishing campaign imitating the National Tax Agency's page, which targets Japanese users by tricking users into sharing sensitive information with the Threat Actors.

The figure below shows the comparison of fake and legitimate websites of the National Tax Agency.

Figure 5 - Fake and Legitimate websites of the "National Tax Agency"

Threat Actors Targeting Geek Banking Users

In September 2022, the CRIL discovered multiple URLs hosting fake websites pretending to be Greece's tax refund websites. The websites falsely state the refund amount and ask users to provide their net banking credentials by confirming their account number for the supposed transfer of funds. The attackers use this method to trick users into revealing their net banking credentials.

Figure 6 - Greek Tax Refund Phishing Page

Data Leaks Trends

0ktapus Data breach: Phishing Attacks Compromised 130+ companies

A group of attackers known as "0ktapus" carried out a phishing attack by pretending to be the Okta authentication service. They sent text messages to victims, directing them to a fake authentication page.

Once victims entered their login credentials, the attackers would gain unauthorized access to the victim's account. The attack mainly targeted companies like Cloudflare, Doordash, Mailchimp, and Twilio.

Figure 7 - Oktapus Attack Process (source: GROUP-IB)

American Airlines Discloses Data Breach in September 2022

On September 16, American Airlines informed its customers and legal officials that a data breach occurred in July 2022 as a result of a phishing attack. The company stated that the number of affected individuals was minimal. However, a legal filing revealed that about 1,708 customers and employees had their information exposed in the attack.

Breach of Microsoft by the Lapsus$ Hacker Group

On March 22, Microsoft confirmed an attack by the TA group Lapsus$ who had posted a screenshot on their Telegram channel claiming that they had breached Microsoft. The screenshot, taken within Azure DevOps, showed that Bing, Cortana, and other projects had been compromised in the attack. The group's motive for this attack was purely financial.

Data Breach from the Texas Department of Insurance uncovered

In May 2022, a state audit revealed a data leak at the Texas Department of Insurance, which exposed the personal information of 1.8 million Texans. The data included social security numbers and other sensitive information and was easily accessible on the department's website from March 2019 to January 2022.

The issue was identified in January and resolved soon after. The state audit was conducted in March, and the results were made public in May 2022. The auditors stated that unauthorized parties had not accessed the breached data.

The 20 GB data breach confirmed by Marriott

In July 2022, Marriott International announced that an anonymous TA group had stolen 20 gigabytes of sensitive data in June 2022. The breach appeared to have occurred due to a social engineering attack in which the TA group convinced an employee to grant them access. Marriott stated that the group had only gained access to a single employee's computer and that the extent of the breach was limited.

The stolen data included internal business documents, flight information, and corporate credit card numbers, and the company planned to alert the 300-400 individuals whose data had been exposed. The company also stated that unauthorized parties had not accessed their data.

Cyber Threat Predictions for 2023

The threat landscape has been evolved significantly over the past year, yet the Threat Actors likely to develop new techniques to bypass security measures and plan more organized cyber-attacks in 2023.

With the widespread availability of leaked source code and builders of multiple ransomware strains, we might see attacks from unknown and unsophisticated groups. A recession in 2023 might bring down the monetary gains made by ransomware groups, as victims might decline to pay ransom due to financial constraints.

Ransomware groups could attack Managed Service Providers more, as MSPs often have access to multiple client networks and systems, making them a valuable target for attackers who can potentially encrypt and demand payment from multiple clients at once.

The Windows threat landscape for 2023 is anticipated to be shaped by both the continuation of existing threats and the emergence of new ones. **The use of malware as a service offerings is expected to rise, providing easy access for cybercriminals with limited skills to deploy malware.** Weaponized phishing attacks targeted toward popular business communication services and apps such as Microsoft Teams and Zoom will also become more prevalent.

Furthermore, **the difficulty of protecting against Multi-Factor Authentication (MFA) attacks is expected to rise** as cybercriminals use stolen personal data and social engineering techniques to bypass MFA security measures. Ransomware and information stealer malware will remain a major concern, with cybercriminals using stolen credentials and social engineering to carry out high-profile breaches.

Remote Administration Tools (RATs) will continue to be a powerful tool for malware. They will be in high demand in the darkweb, providing various attack capabilities such as data theft, system monitoring, and silent execution. Additionally, there will be a significant emergence of malware loaders and botnets in the wild.

Mobile threats are expected to increase in 2023 as the use of mobile applications has increased over the past few years. As more and more people use mobile banking, we may see a resurgence of known banking trojans such as Sharkbot, SOVA, Hydra, etc., with new features and targets, as well as the emergence of new banking trojans like Zanubis.

In 2022, we observed that cybercriminals had already started selling services like "Dropper-as-a-Service" and Zombinder (APK binding service) to create harmful mobile applications. These third-party services make it easier for threat actors to bypass security measures and develop malware.

In 2023, we will likely see an increase in the use of these "as-a-service" offerings by cybercriminals to simplify the development of Android malware.

It is expected that in 2023, the number of malware threats targeting Linux systems will rise as the usage of Linux continues to increase. Known malware such as Mirai, Gafgyt, Tsunami, and XorDDoS may also resurface with new features and targets. In 2022, it was observed that cybercriminals were offering services such as "Ransomware-as-a-Service" and “DDoS-as-a-service”, which make it easier for TAs to target Linux users. In 2023, there will likely be an uptick in the use of these types of services by cybercriminals, making it simpler to utilize Linux malware.

As the usage of macOS systems continues to grow, it is predicted that the number of malware threats targeting these systems will also increase in 2023. Known malware such as ChromeLoader, CloudMensis, Alchimist, and DazzleSpy may also reappear with new capabilities and targets. Furthermore, new forms of malware may also emerge. In 2022, it was observed that cybercriminals were targeting macOS systems using malware such as backdoors and spyware to steal sensitive information. As a result, it is likely that in 2023, cybercriminals will continue to use these types of malware to financially harm users and damage their credibility.

Phishing attacks are expected to remain a significant threat to organizations and individuals in 2023 as TAs continuously improve their methods and make phishing campaigns more advanced and targeted.

In 2022, it was observed that TAs used themes such as ongoing FIFA tournaments, Japanese National Tax Agency websites, and Greek Banking websites to create phishing pages and steal sensitive information from victims. In 2023, cybercriminals will likely continue to use similar tactics to financially harm users and damage their credibility. Additionally, TAs may also use global events as themes for their phishing attacks to trick victims into providing sensitive information or clicking on malicious links.

In the coming year, supply chain attacks on organizations dealing in critical infrastructure will become even more prevalent, as these attacks can potentially disrupt various national services across the globe. As countries become more dependent on technology, the potential consequences of these attacks will become even more severe.

One of the major drivers of this trend will be the increasing number of geopolitical events and regional disturbances. These events will lead to more Hacktivist groups and Threat Actors (TA) targeting exposed ICS assets and protocols. These groups will be motivated by various factors, including political ideologies, financial gain, disinformation campaigns, etc.

Devices used with satellite communications, which are critical for the Telecommunications sector, Transportation sector, and Military operations are more likely to be targeted as growing vulnerabilities at the hardware and code level are at high frequency, creating more difficulties for teams involved in patch management. These devices will often be difficult to secure and maintain, making them easy targets for TAs.

Advanced Persistent Threat groups will also become more prevalent as they create customized malware targeting various products from various vendors dealing in Industrial Control System equipment and software. These groups will be highly skilled and well-funded, and they will be able to infiltrate even the most secure networks.

Advanced Persistent Threat rely on vulnerabilities and spear phishing emails for initial compromise. APT groups are using N-day vulnerabilities to compromise unpatched public-facing assets. Spear phishing campaigns are crafted using current affairs related to the target organizations. The attacks are multi-staged to maintain stealth and leave little or no traces of their activities. We may observe similar trends for further campaigns as well.

Data leaks and the distribution of confidential blueprints will also become a major concern, as they will provide more value to attackers while targeting critical infrastructures. This will be particularly true in the case of organizations dealing in critical infrastructure, as confidential information will be used to plan and execute sophisticated attacks.

More vulnerabilities have been identified since last year, but the count of critical vulnerabilities has decreased. Because of various bug bounty programs, the volume of vulnerability identification is increased.

TAs are using the already detected vulnerabilities to target their potential victims. TAs also utilize chaining multiple low-impact vulnerabilities to compromise the possible victim. We will observe similar trends for 2023 as well.

References

https://blogs.blackberry.com/en/2022/11/gamaredon-leverages-microsoft-office-docs-to-target-ukraine-government

https://labs.k7computing.com/index.php/lazarus-apts-operation-interception-uses-signed-binary/

https://www.zscaler.com/blogs/security-research/apt-36-uses-new-ttps-and-new-tools-target-indian-governmental-organizations

https://securityaffairs.co/133881/data-breach/mbda-alleged-data-breach.html

https://socradar.io/sensitive-data-of-65000-entities-in-111-countries-leaked-due-to-a-single-misconfigured-data-bucket/

https://www.databreaches.net/exclusive-marriott-hacked-again-yes-heres-what-we-know/

https://tdi.texas.gov/news/2022/tdi03242022.html

https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

https://www.slashnext.com/the-state-of-phishing-2022/

https://unit42.paloaltonetworks.com/chromeloader-malware/#post-123828-_mpyacggxtibk

https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/

https://www.uptycs.com/blog/black-basta-ransomware-goes-cross-platform-now-targets-esxi-systems

https://www.trendmicro.com/en_us/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html

https://www.microsoft.com/en-us/security/blog/2022/12/15/mcrash-cross-platform-ddos-botnet-targets-private-minecraft-servers/

https://www.securonix.com/blog/detecting-the-enemybot-botnet-advisory/

https://www.cleafy.com/cleafy-labs/revive-from-spyware-to-android-banking-trojan

https://www.threatfabric.com/blogs/zombinder-ermac-and-desktop-stealers.html

https://blog.fox-it.com/2022/06/29/flubot-the-evolution-of-a-notorious-android-banking-malware/

https://www.bleepingcomputer.com/news/security/exploited-windows-zero-day-lets-javascript-files-bypass-security-warnings/

https://www.bleepingcomputer.com/news/security/over-60-000-exchange-servers-vulnerable-to-proxynotshell-attacks/

https://www.infosecurity-magazine.com/blogs/top-security-vulnerabilities/

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2022 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups to Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence.

To learn more about Cyble, visit www.cyble.com