Quick Heal

Security Simplified

QUICK HEAL THREAT REPORT

QUARTER 3 2022

102 Million Windows Malware detected in Q3 2022
32 Million Windows Malware detected in Sep'22
1.12 Million Malware daily average detected in Q3 2022

Follow us

Quick Heal
Security Simplified

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.

Contributors

Quick Heal **Security Labs** | Quick Heal **Marketing Team**

About Quick Heal Security Labs

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.

www.quickheal.com

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**

THREAT REPORT Q3-2022

Contents

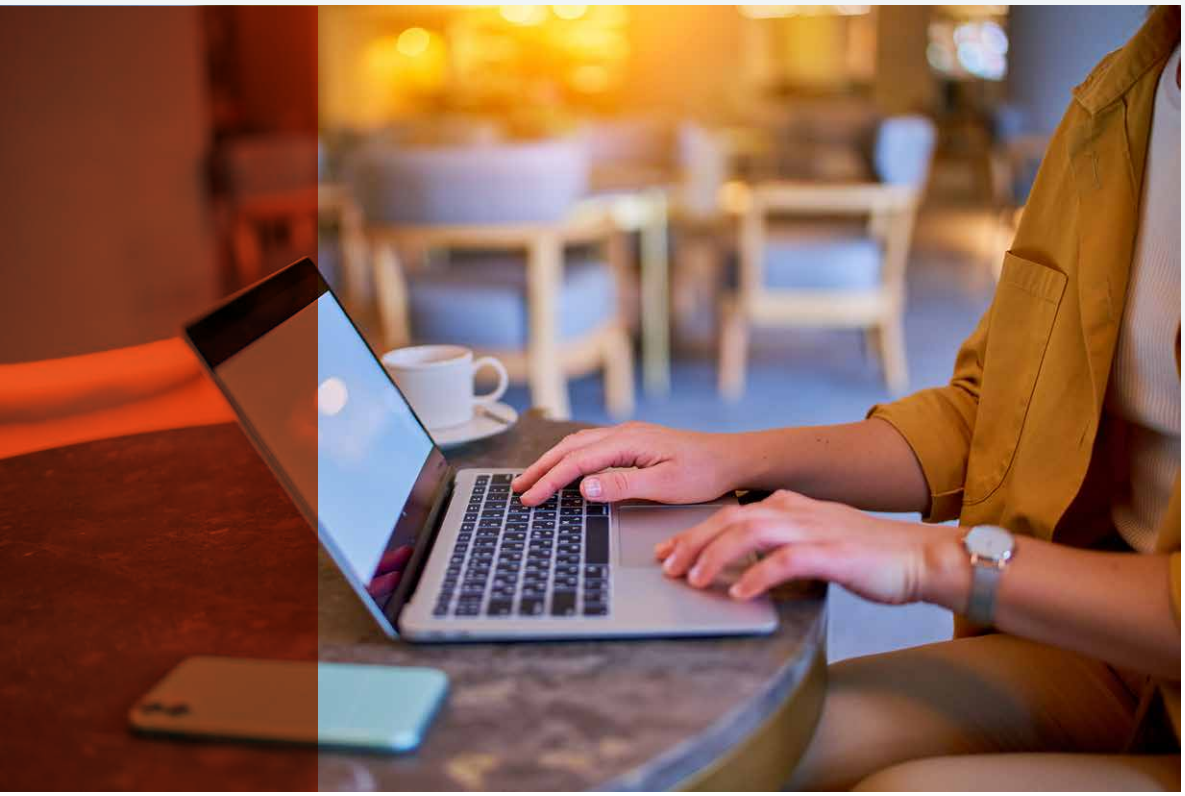
Foreword

Quick Heal quarterly threat reports include information on new threats, detection statistics, and major trends observed in that quarter. The report also captures any new threat actors and attack techniques that were identified in the quarter.

Q3 CY 2022 continued from the previous quarter. We witnessed increasing complexity of attacks – primarily ransomware and phishing attacks. To learn more, read on.

WINDOWS

102 Million Windows Malware detected in Q3 2022
32 Million Windows Malware detected in Sep'22
1.12 Million Malware daily average detected in Q3 2022



Windows Detection

Statistics Q3 2022

Malware:
102 Million
Per Day: 1,119,107
Per Hour: 46,629
Per Minute: 777

Ransomware:
0.19 Million
Per Day: 2,036
Per Hour: 85
Per Minute: 1

Exploit:
4.98 Million
Per Day: 54,759
Per Hour: 2,282
Per Minute: 38

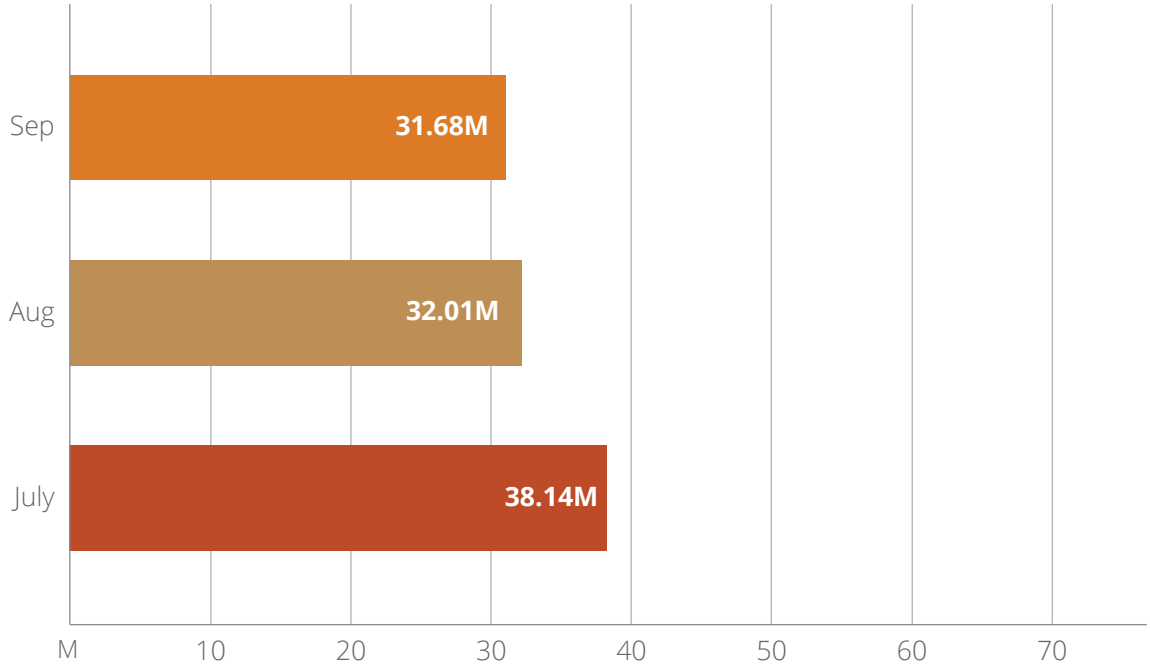
PUA & Adware:
5.50 Million
Per Day: 60,431
Per Hour: 2,518
Per Minute: 42

Cryptojacking:
0.73 Million
Per Day: 7,968
Per Hour: 332
Per Minute: 06

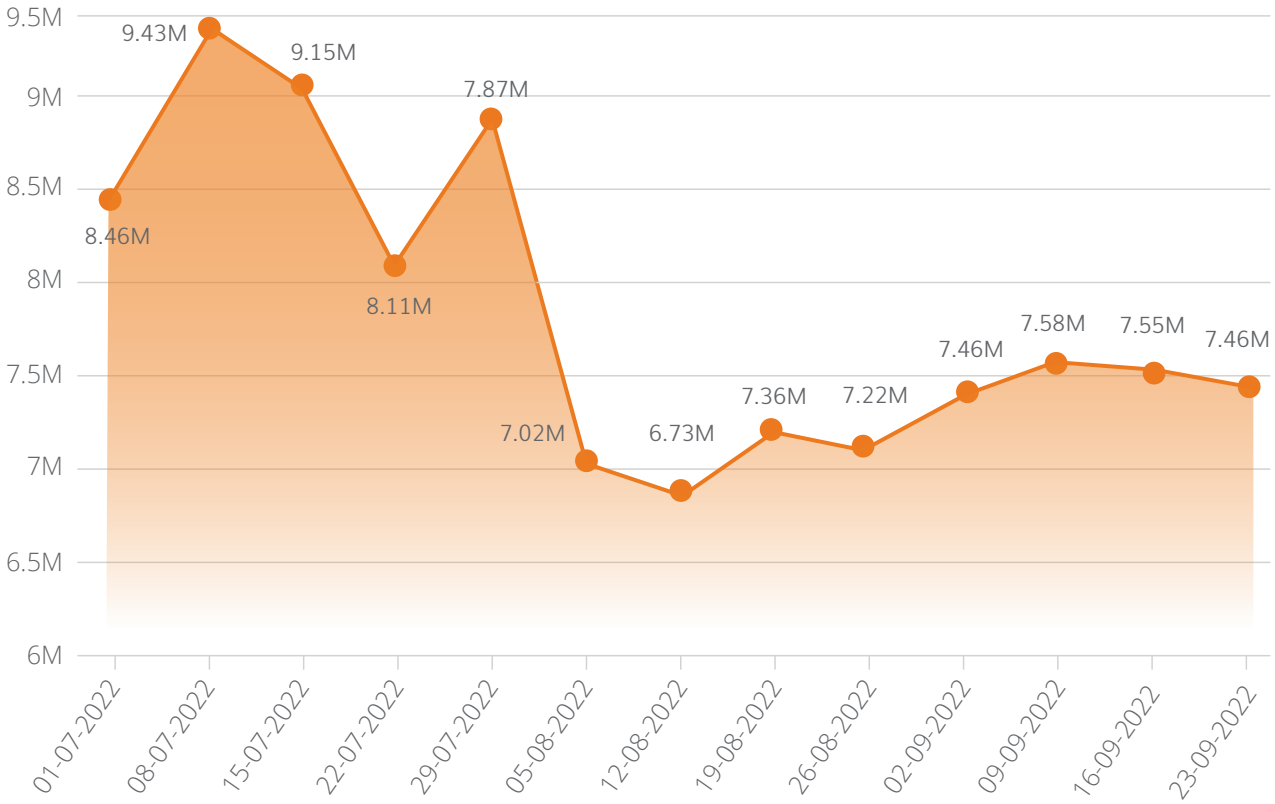
Infector:
26.05 Million
Per Day: 286,312
Per Hour: 11,930
Per Minute: 199

Worm:
10.21 Million
Per Day: 112,143
Per Hour: 4,673
Per Minute: 78

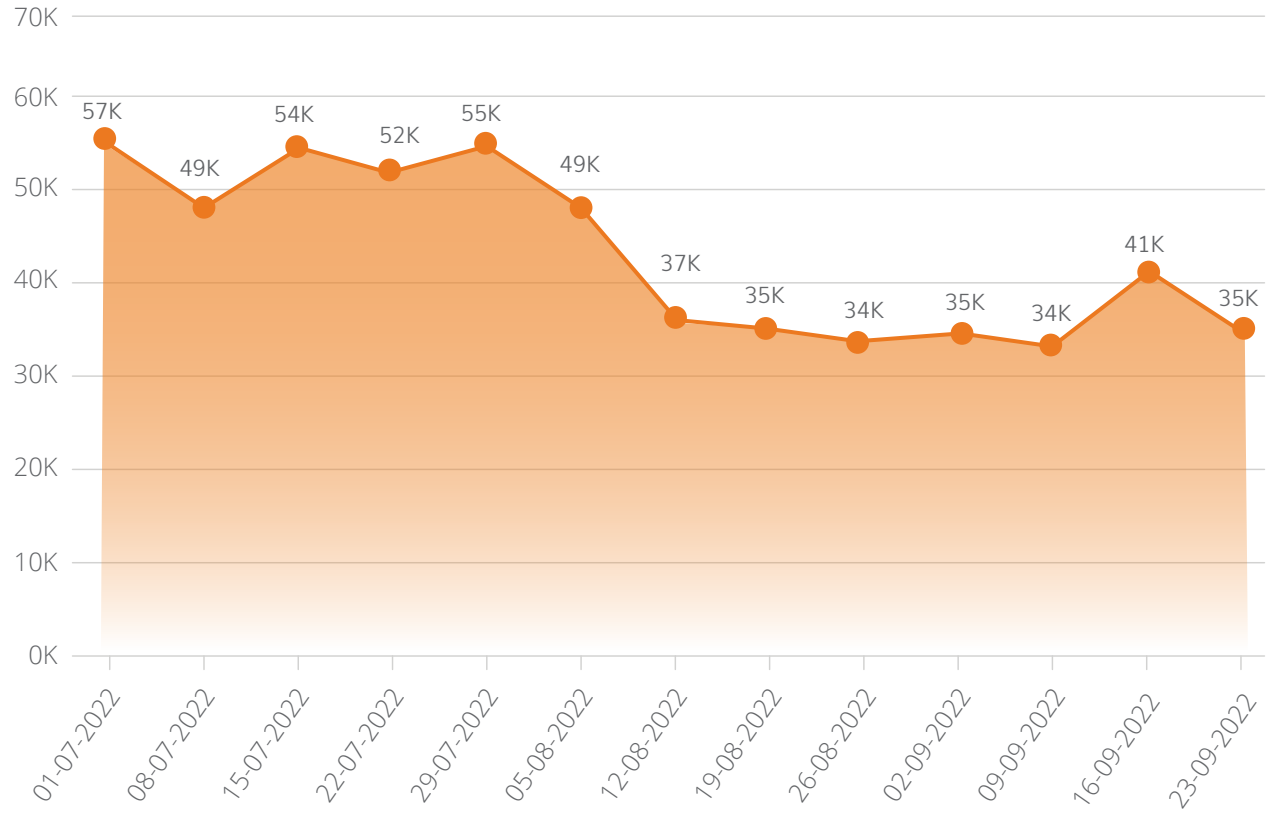
Detection Statistics – Month Wise Q3 2022



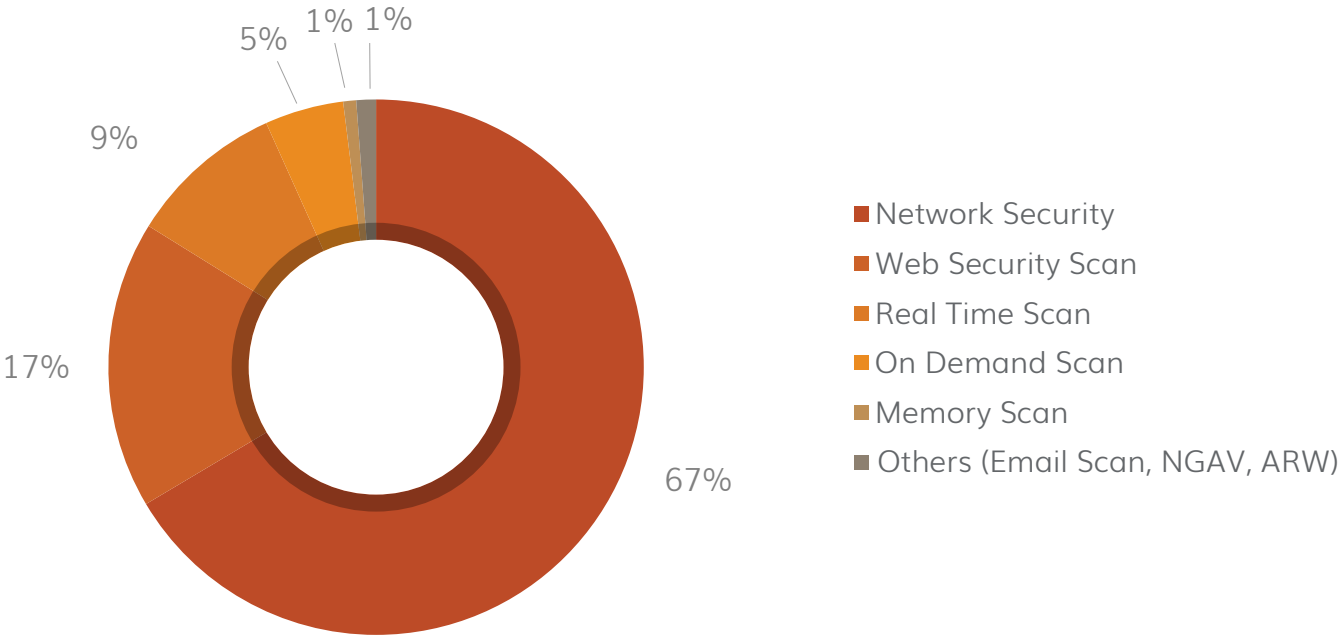
Detection Statistics – Week-Over-Week



Ransomware – Week-Over-Week



Detection Statistics – Protection Wise



Brief description about

various threat protection mechanisms

Network Scan

Network scan (IDS/IPS) analyses network traffic to identify known cyber-attacks & stops the packet from being delivered to the system.

Web Security Scan

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

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

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

Memory Scan

Scans memory for malicious programs running & cleans it.

Email Scan

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

NGAV

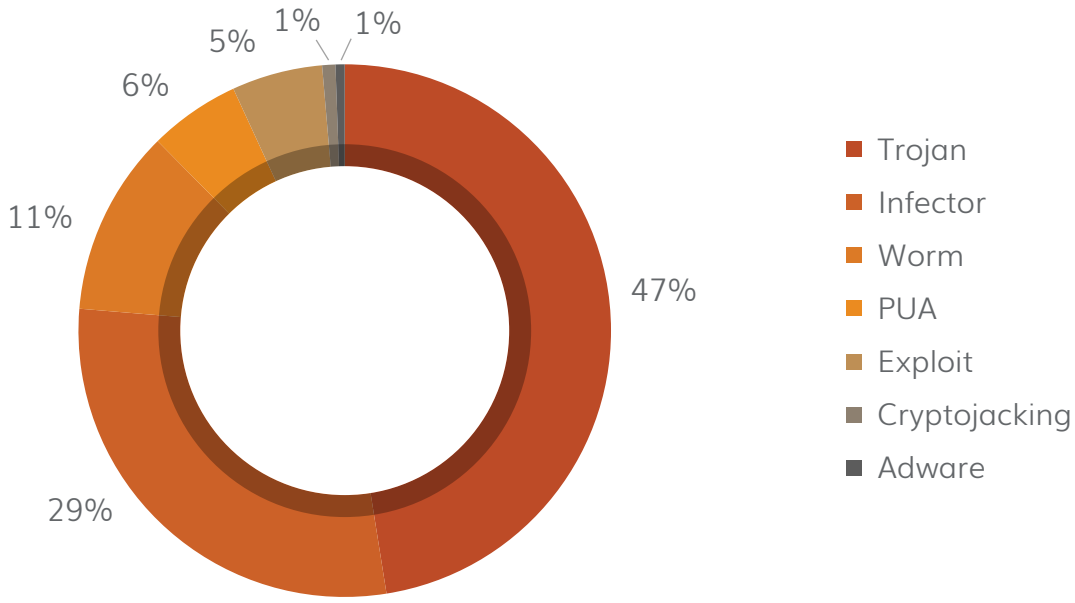
It detects and eliminates new and unknown malicious threats based on their behaviour.

ARW

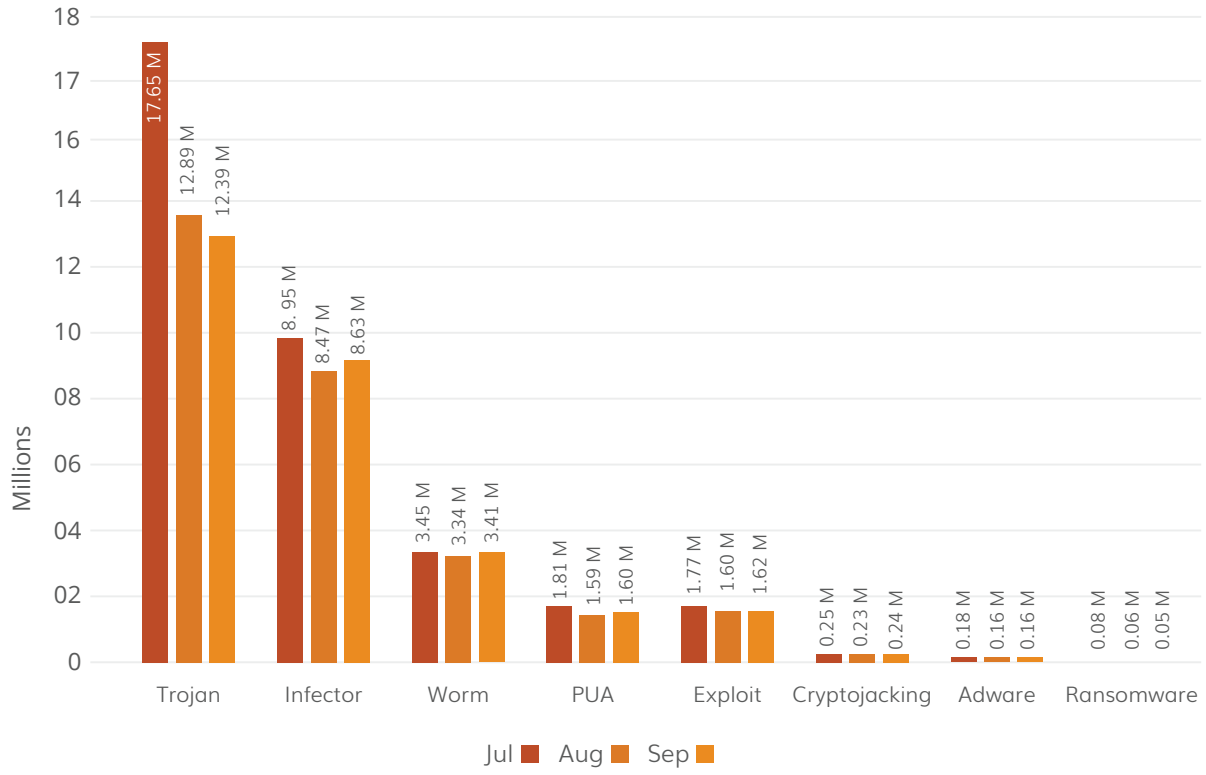
ARW is our anti ransomware module for protection against ransomwares.

Detection Statistics - Category Wise

A) Malware-wise Categorization



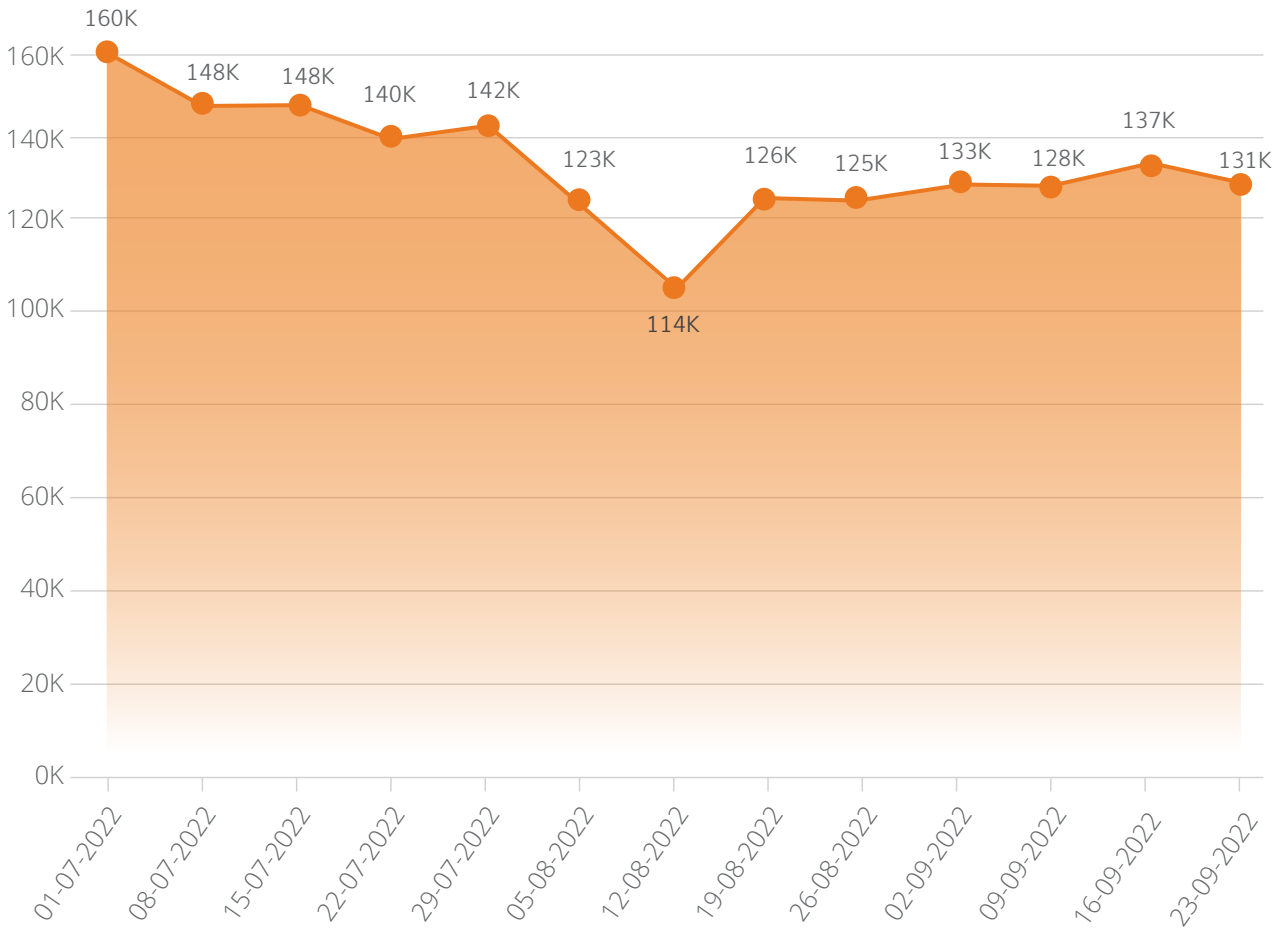
B) Month-wise Categorization



What is Trojan Malware?

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

Coin Miner Detection Statistics

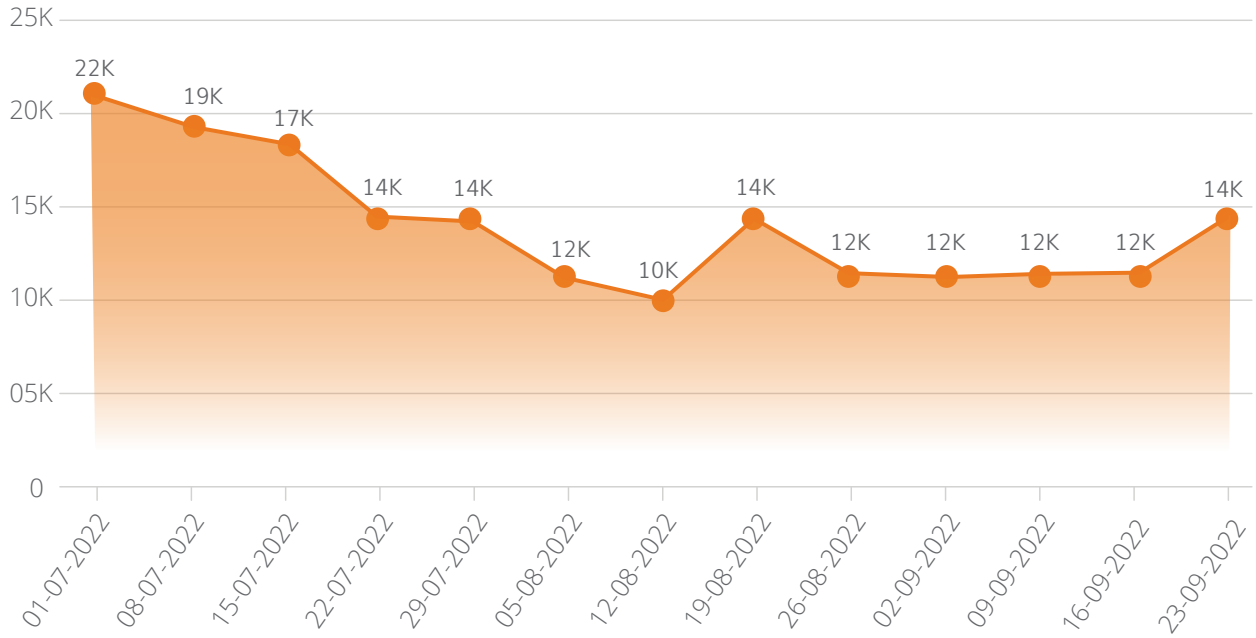


What is Coin Miner Malware?

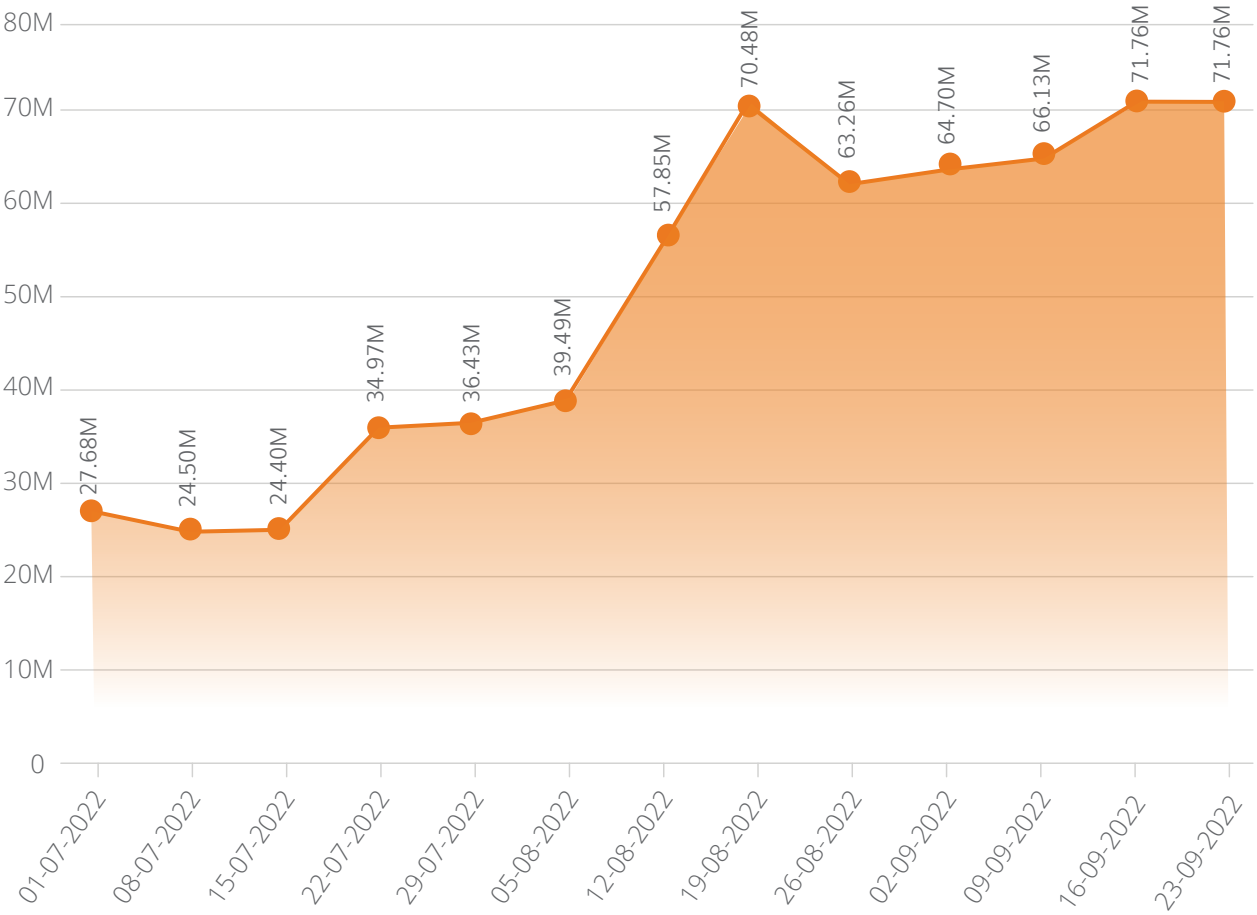
Coin Miners (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income.
Cyber criminals have created threats and viruses which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

A) Phishing Email Attacks

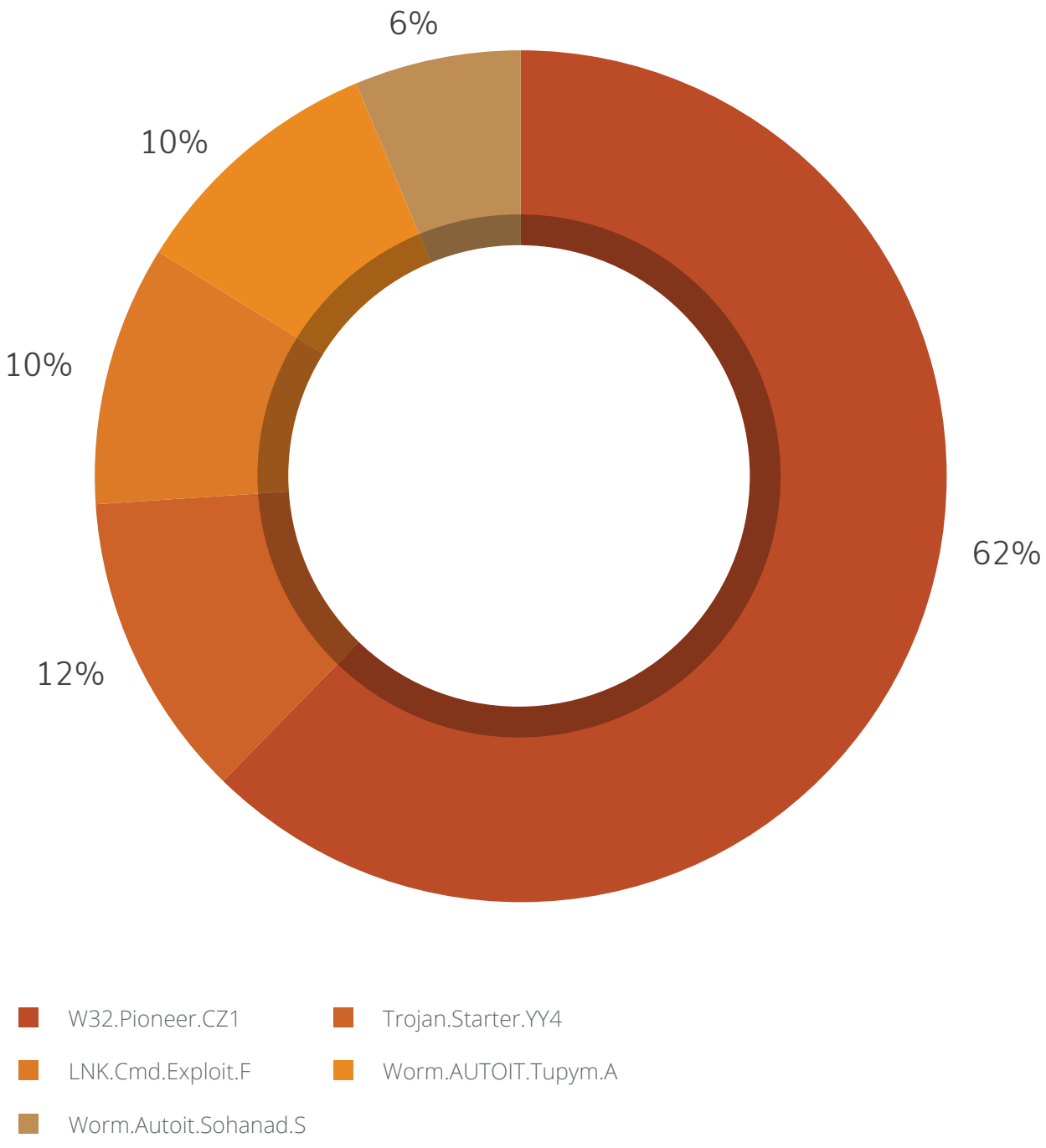


B) Phishing URL Attacks



Top 5 Windows Malware

The below figure represents the Top 5 Windows malware of Q3 2022.
These malwares have made it to this list based upon their rate of detection from July to Sep of current calendar year.



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

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.

03

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.

04

Worm.AUTOIT.Tupym.A
Threat Level: Medium
Category: Worm
Method of Propagation: Malicious links in instant messenger

Behaviour:

- Malware drops file in system32 folder and executes it from dropped location.
- It connects to malicious website, also modifies start page of browser to another site through registry entry. Also Creates Run entry for same dropped file for persistence.

05

Worm.Autoit.Sohanad

Threat Level: Medium

Category: Worm

Method of Propagation: Spreads through mails, IM apps, infected USB & network drives

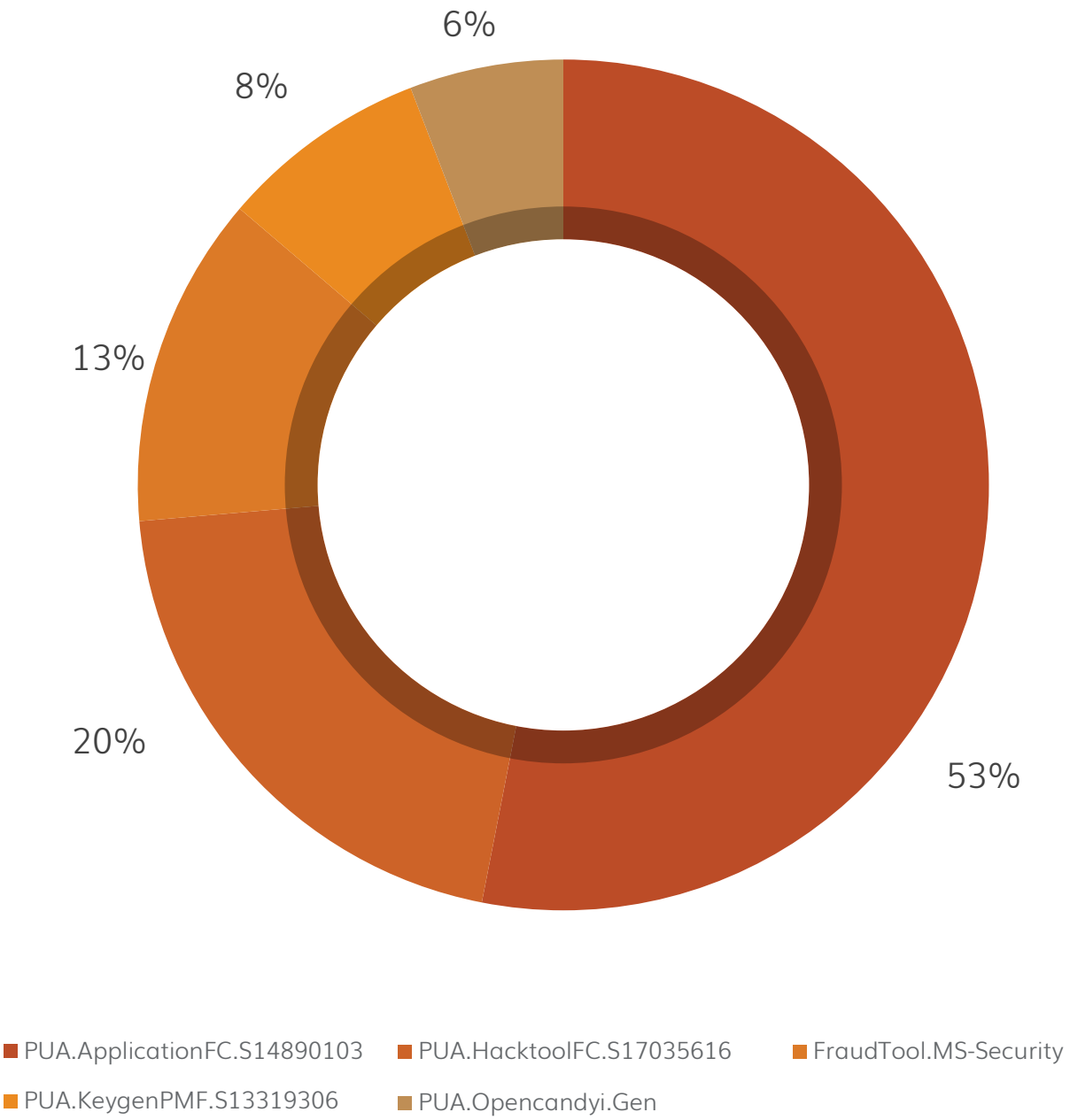
Behaviour:

- It arrives on your computer through Messaging apps, infected USB, or network and can spread quickly.
- After arrival, it creates a copy of itself as .exe with a typical Windows folder icon.
- User mistakenly executes this .exe assuming it as a folder, then it spreads over the network.
- It infects every connected USB drive too

Top 5 PUA (Potentially Unwanted Applications and Adware)

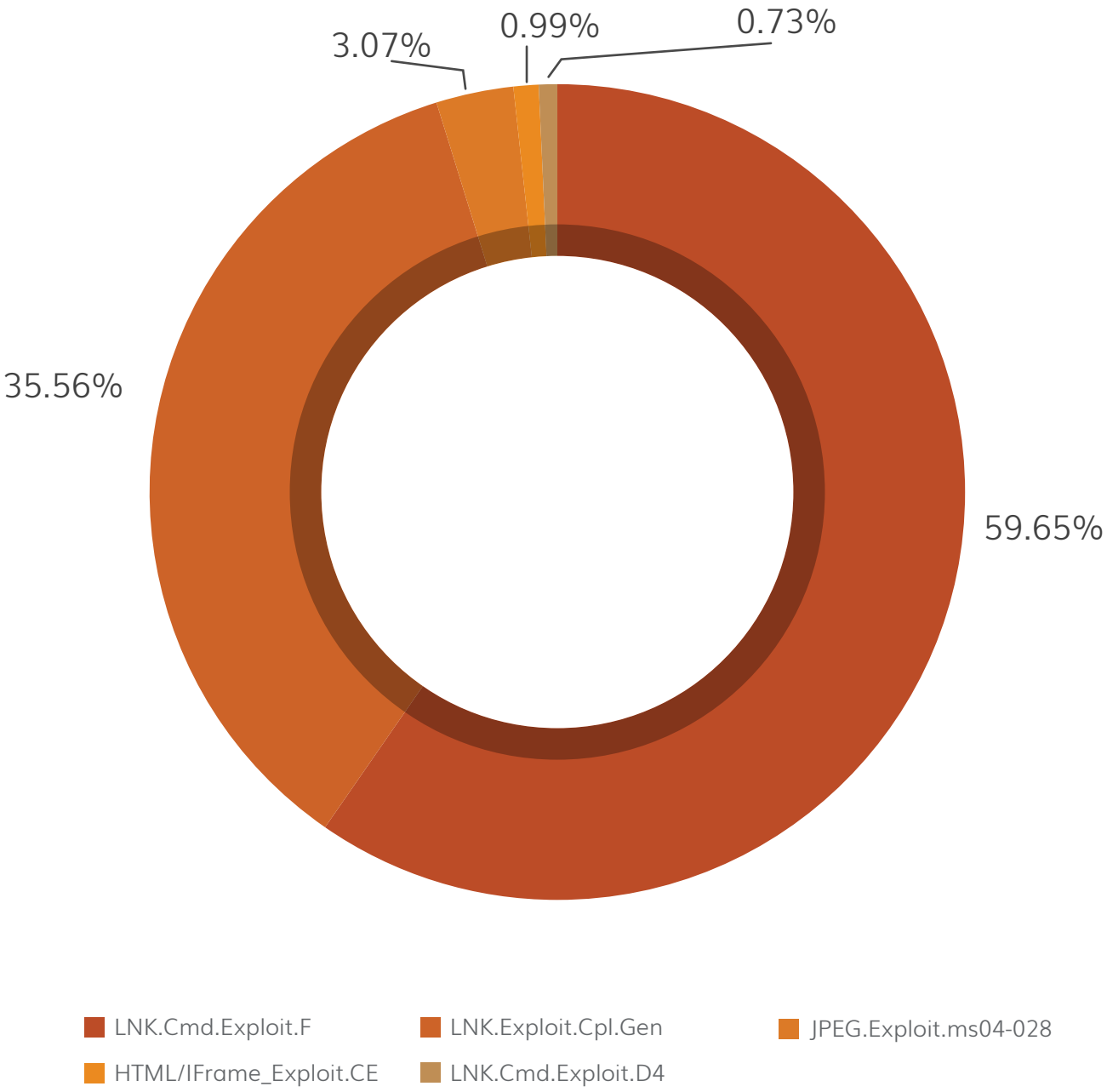
Potentially Unwanted Applications (PUA) and Adware programs are not necessarily harmful but using them might lead to security risks. Adware are software used to display ads to users; some are legitimate while some are used to drop spyware that steals user information.

Below figure represents the top 5 PUAs and Adware detected by Quick Heal in Q3 2022.



Top 5 Host-Based Exploits

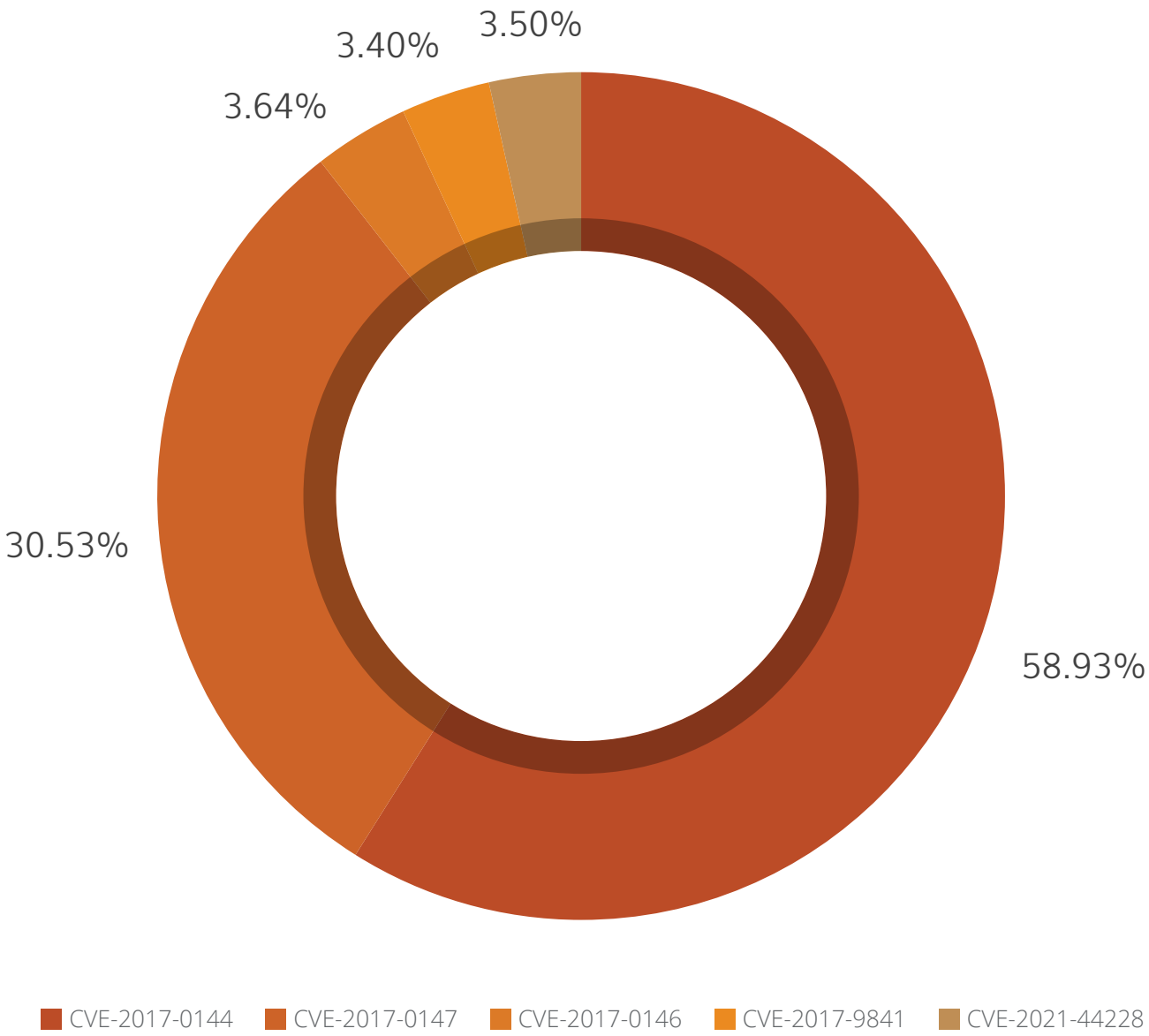
An exploit is a piece of code or crafted data that takes advantage of a bug or vulnerability in the targeted system or an application running on it.



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

Below figure represents the top 5 Network-Based Windows exploits of Q3 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

1. CVE-2017-0144

Microsoft Windows SMB Remote Code Execution Vulnerability
This vulnerability enables the attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server

2. CVE-2017-0147

Microsoft Windows SMB Information Disclosure Vulnerability
An attacker who successfully exploited this vulnerability could craft a particular packet, leading to information disclosure from the server.

3. CVE-2017-0146

Windows SMB (SMBv1) Remote Code Execution Vulnerability
A remote code execution vulnerability exists in how the Microsoft Server Message Block 1.0 (SMBv1) server handles specific requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.

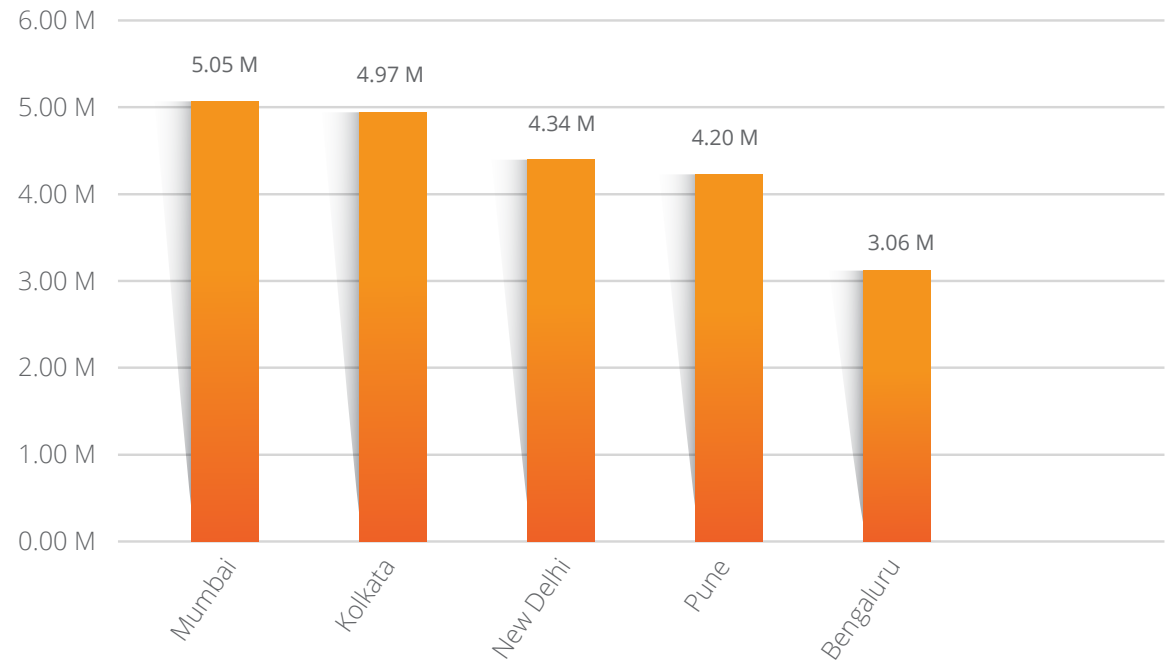
4. CVE-2017-9841

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

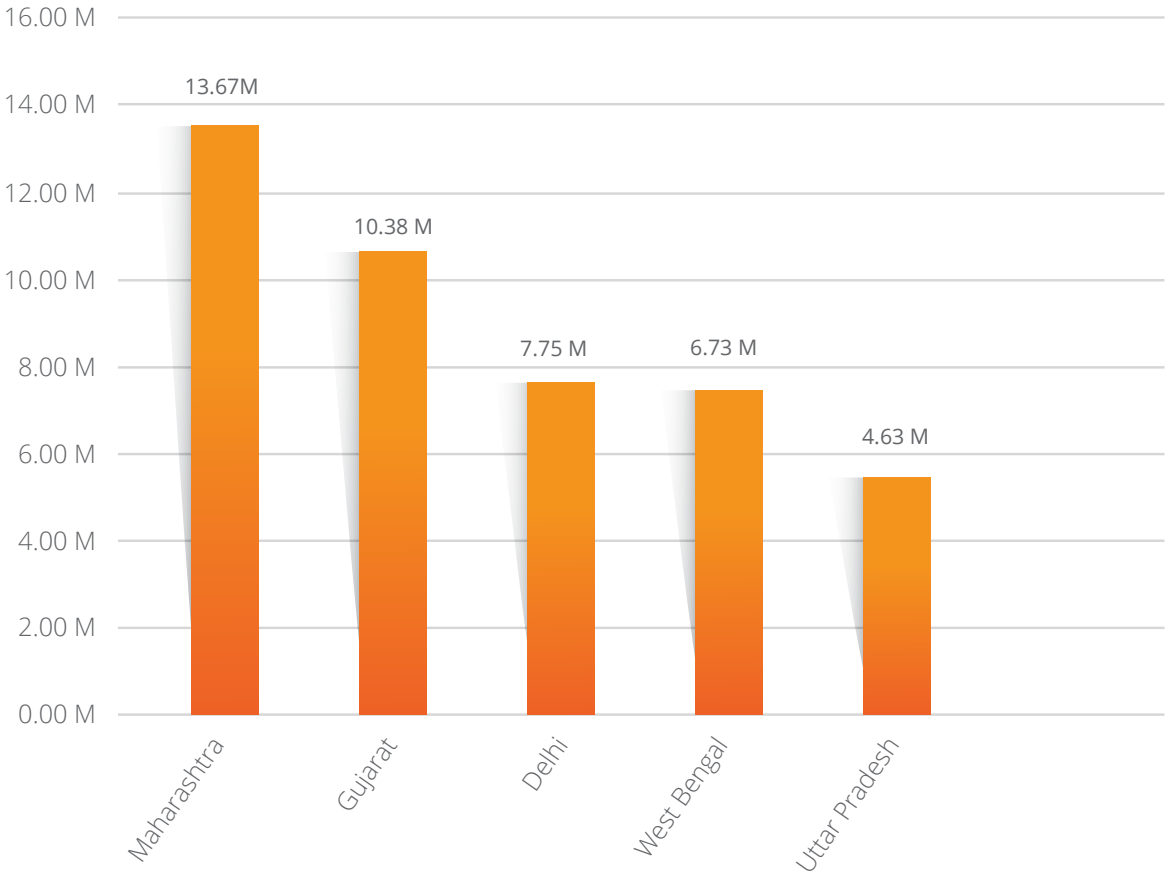
5. CVE-2021-44228

Apache log4j-core vulnerability
An attacker who can control log messages or parameters can execute arbitrary code loaded from LDAP servers and other JNDI-related endpoints when message lookup substitution is enabled.

Top 5 Affected Cities



Top 5 Affected States



Trends in Windows Security Threats

1. POWERSHELL: AN ATTACKER'S PARADISE

PowerShell was originally intended as a task automation and configuration management program for system administrators. However, it didn't take long for attackers to realize their potential for carrying out offensive operations without being detected. Due to PowerShell's versatility, it can be seen in all stages of attacks.

Why attackers use PowerShell?

- PowerShell is a reputed tool signed by Microsoft and is virtually present on every Windows system.
- Its input can be encoded commands which can be decrypted without the need to drop any files on the disk, making the attack stealthier.
- PowerShell can be used in all stages of the attack, from malicious macros of MS Office documents for initial infection to dumping credentials in post-exploitation using mimikatz, etc.
- Malicious operators can manipulate PowerShell by using various bitwise operators and string operations to achieve a high level of obfuscation.
- More advanced use cases like reflective dll-injection and shellcode execution can be performed quite easily.

Defending against PowerShell attacks is complicated. Due to its availability and ease of use, it provides cybercriminals and adversarial groups with a large attack surface. There is no silver bullet for detecting and preventing PowerShell attacks. However, the protection provided by various detection technologies can help us mitigate its risks.

The best way that you can protect yourself against malicious use is to adhere to all of the standard best practices for Windows security and keep your Anti-malware product updated.

2. Indian Power Sector Targeted with latest LockBit 3.0 Variant

After the infamous Conti ransomware group was disbanded, the LockBit group has claimed dominance over other groups this year. Conti's former members split up, joining already existing cybercrime groups, and started to target the energy and power sectors. Proactive monitoring of this sector led to the identification of one of our premium entities getting attacked. Investigation and analysis determined that the new LockBit 3.0 (Black) ransomware variant caused the infection that exhibited huge anti-forensic activity with similarities to other variants. Unprotected systems in the network were brute forced to execute ransomware payload laterally across the systems using the sys-internal tool PSEXEC. Only the shared drives were found to be encrypted, and telemetry shows the payload dropped got detected at multiple endpoints on protected systems.

LockBit Black's builder was leaked recently by one of its programmers, who was upset with their leadership as these reputed cybercrime groups work as an

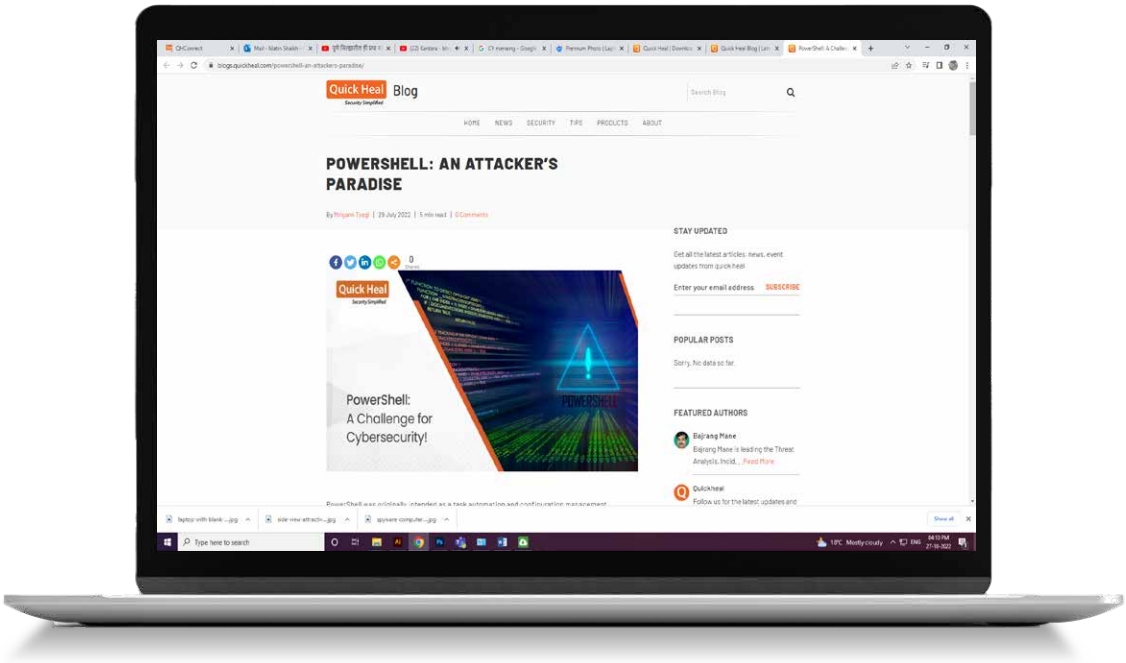
organization with salaries, employees, and HRs. Necessary precautions must be taken as threat actors (Bl00dy Ransomware Group) are already taking advantage of this leaked builder, with LockBit now adopting triple extortion techniques.

3. Swachhta Platform Hacked by Threat Actor "LeakBase"

Threat Actor LeakBase (a moderator on LeakBase[.]cc) has shared 16 million Indian citizen's PII on BreachForums from the Swachhata Platform, a Swachh Bharat Mission initiative governed by the Ministry of Housing and Urban Affairs (MoHUA), Government of India. The platform is used to submit and follow up on municipal complaints.

They have compromised several prominent financial institutions in India prior to this leak. 6 GB of leaked data was stolen from SQL DB "swachh_manch," where the impacted infrastructure was running on outdated versions of the phpMyAdmin & Ubuntu 16.04.1 OS. The compromise was made via a custom brute forcing method with credentials being weak password strings.

This incident is yet another reminder of the acute need to have strong and complex passwords – without which we are prone to such cyber-attacks.



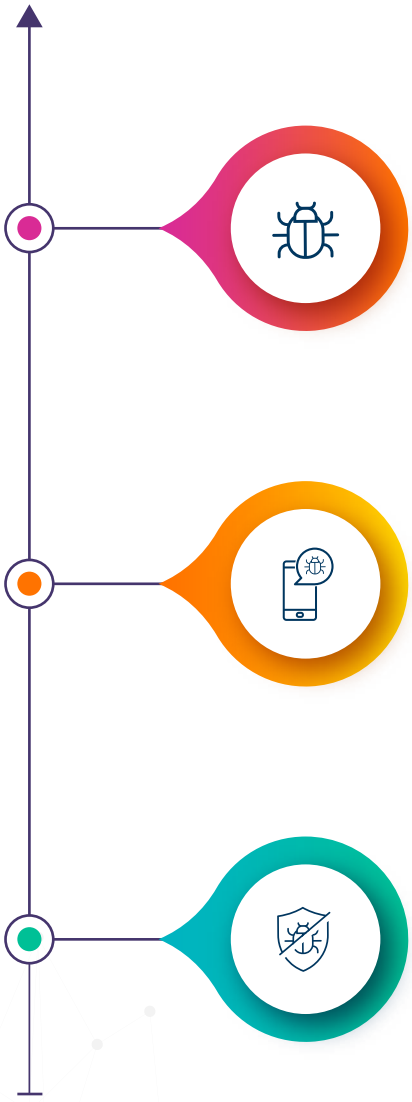
ANDROID

65.5%

of total Android detections
in Q3 2022 were Malware.

ANDROID MALWARE DETECTIONS

FOR Q3 2022



20,248

Malware

Per Day: 222
Per Hour: 9
Per Minute: 0

5,487

Adware

Per Day: 60
Per Hour: 2
Per Minute: 0

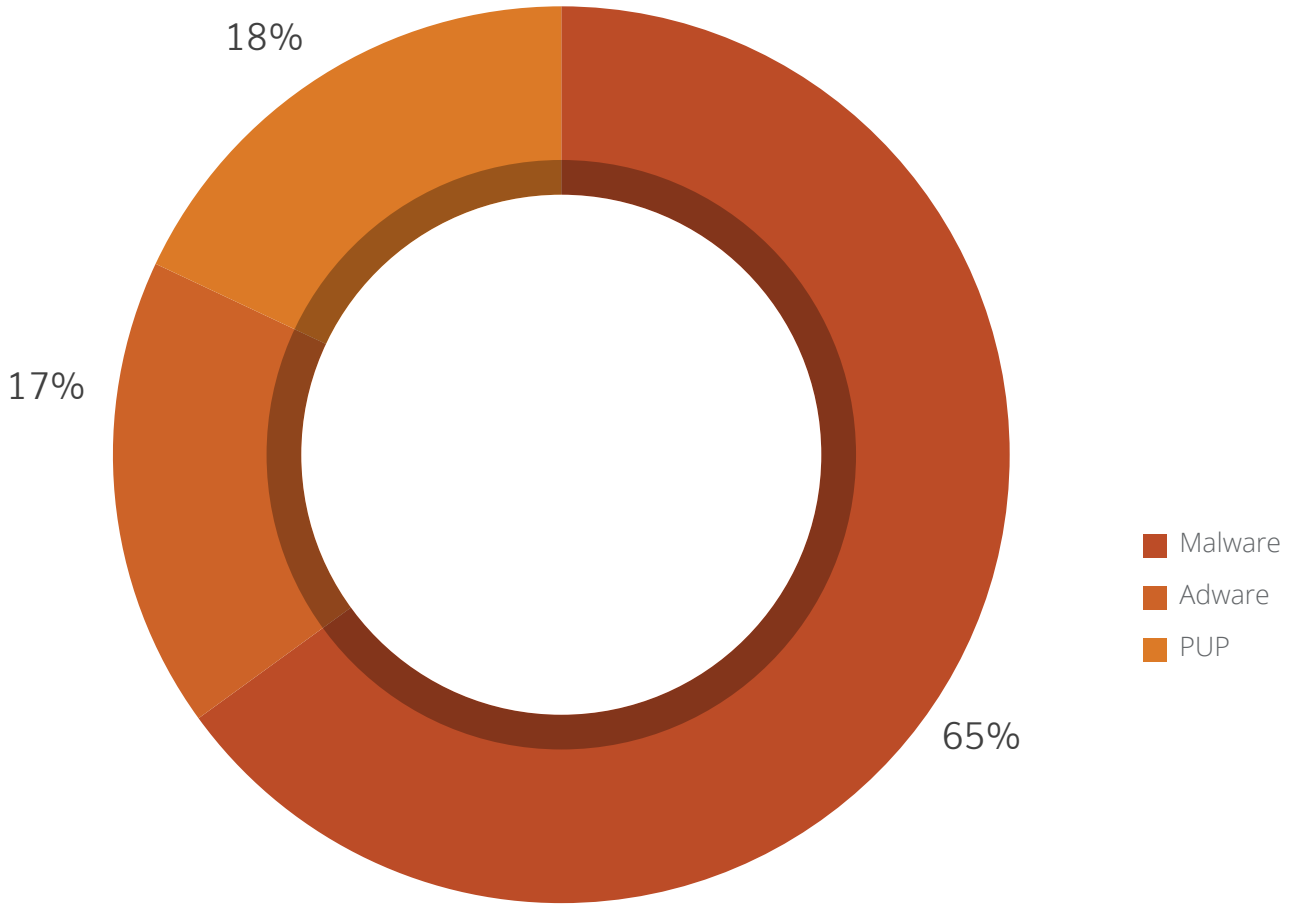
5,178

Potentially Unwanted Application (PUA)

Per Day: 56
Per Hour: 2
Per Minute: 0

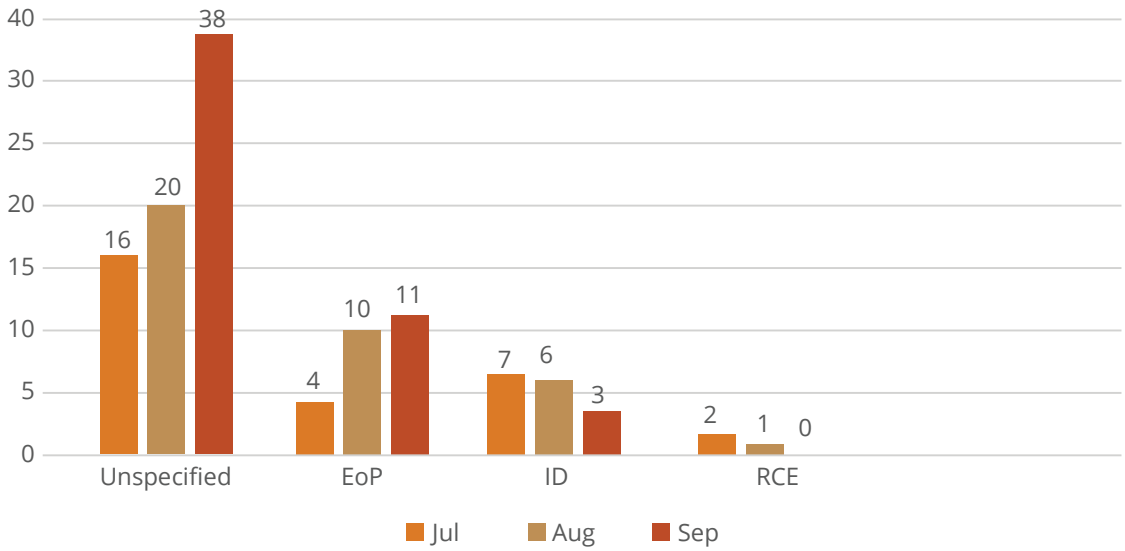
Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q3 2022.

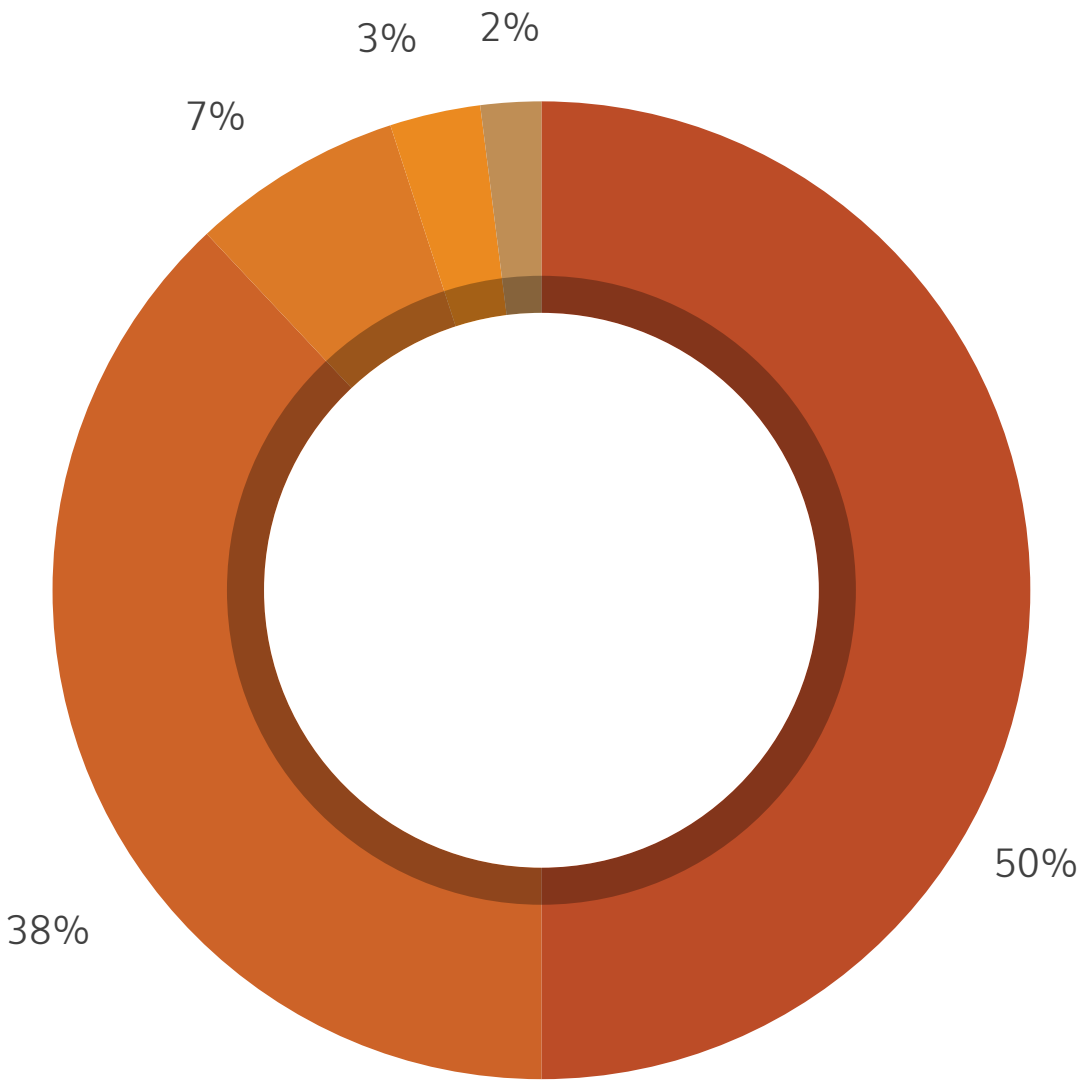


Security Vulnerabilities Discovered

A security vulnerability (also known as a security hole) is a security flaw detected in a product that may leave it open to hackers and malware. Below figure shows the type of Android security vulnerabilities and their growth from Jul to Sep 2022.



Top 5 Android Malware for Q3 2022



Top 5 Android Malware Details

01

Android.Agent.DC94f3
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It is a Trojan-Dropper malware, it drops malicious Android file in background.
- It looks like a legitimate application such as settings or messaging.
- On its first launch, it hides its presence and loads encrypted payload from Resources.
- Encrypted payload has advertised SDK which shows full screen advertisements.

02

Android.BAB.A84a2
Threat Level: Low
Category: PUA
Method of Propagation: Third-party app stores

Behaviour:

- These apps are modified version of WhatsApp and known as GB WhatsApp.
- These apps are 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. But there are no security checks in place.
- Original WhatsApp issues the warning about such unofficial apps developed by third parties and violate its Terms of Service.

03

Android.Agent.GEN49494
Threat Level: Medium
Category: PUA
Method of Propagation: Third-party app stores

Behaviour:

- These applications are spyloan
- This offer small loans without requiring much pa
- These applications asks for contact, SMS, storag
- This data used by threat actors to harass users.

04

Android.Agent.GEN51659
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It is a Trojan-Dropper that looks like a legitimate application such as settings or messaging.
- On its first launch, it hides its presence and loads encrypted payload from the resources folder.
- Encrypted payload has advertised SDK, which shows full screen advertisements.

05

Android.Hiddad.GEN35225
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- All these apps use a standard SDK (Software Development Kit) for advertising.
- Capabilities of this malware family include showing ads, opening URLs in the browser & receiving commands from C&C (Command & Control) server to perform activities.
- It can also hide its icon in the app launcher, making it difficult to notice its existence but runs in the background even after the device restarts.
- The intention of these apps seems to generate as much Ad revenue as possible.

Trends in Android Security Threats

1] 14 Auto-launching HiddAd malware found on Google has more than 6 million downloads.

The prime motive of HiddAd is to generate revenue through aggressive advertisements. As long as HiddAd remains on the device, it will generate revenue for the malware author. To make uninstalling difficult, malware authors hide the application's icon from the application drawer. They also use different deceptive techniques to make uninstallation less intuitive to the users. In this quarter, Quick Heal found 14 such applications on Google Play Store. The download count of all these applications is more than 6 million, and Google removed these applications after being reported by Quick Heal. These applications are HiddAd malware and execute themselves without user interaction. **Quick Heal Security Labs detects these apps with variants of Android.Hiddad**. We also published blog about the same - https://blogs.quickheal.com/auto-launching-hiddad-on-google-play-store-found-in-more-than-6-million-downloads/

2] Android banking Trojans are again on hit -

Recently Quick Heal analyzed many banking malware which targeted banking sector badly-

I] SOVA Android Trojan-

SOVA is an Android banking Trojan with significant capabilities like credential theft, capturing keystrokes, taking screenshots, etc., that can inflict acute harm to the devices that become victims of this malware. Since last year, SOVA has been found to be targeting Russian and Philippine banks. Since its inception, we have seen its three versions, which had 2FA interception, cookie stealing, and injection capabilities. These versions have the capability to steal credentials and session cookies through overlay attacks, keylogging, hiding notifications, and manipulating the clipboard to insert modified cryptocurrency wallet addresses.

The latest version seems to have evolved with new features like the ability to operate screen clicks, swipes, and copy/paste remotely using commands. The latest version has VNC (virtual network computing) capability, ransomware capabilities for encrypting files, showing an overlay screen on other apps, communicating with a C2 server to exfiltrate a list of installed applications, stealing cookies and keylogging, and intercepting with multi-factor authentication (MFA) tokens. These latest versions mimic icons of Amazon and Google Chrome to trick users into downloading. At the launch time, it asks for accessibility permission and forces the user to allow it.

Quick Heal detects this with variants of "**Android.Agent.A**", "**Android.ScytheSCF.QJ**", "**Android.HqwarSCF.EH**"

II] Fake banking reward applications posing threat to user-

These applications use icons of Indian Banks and spread through SMS. It has remote access trojan (RAT) capabilities. It steals call_logs, SMS, and 2FA messages for email accounts and sends this collected data in an encrypted format to the C2 server.

These perform malicious activities like-

- Collecting contact information.
- Intercepting OTPs from the infected device.
- Managing the list of installed applications from the device.
- Sending SMSs to the contacts based on the commands received from the C2 server.
- Stealing credentials of social media accounts and Banking portals.
- Monitoring the victim device by leveraging the BIND_ACCESSIBILITY_SERVICE.
- Using Telegram API to communicate with the C&C server hosted on a Telegram bot account.

Quick Heal detects this with variants of "**Android.Agent.GEN**"

III] Dawdropper:

DawDropper is Android banking Trojan that steals users' data like banking credentials. This malware can intercept communication and gets control of the affected device. It uses Firebase Realtime Database to obtain a payload and hosts malicious payloads on GitHub.

It Drops 4 types of banking trojans, i.e., Octo, Hydra, Ermac, and TeaBot.

The payload is having below capabilities-

- Overlay Attacks against multiple banks applications
- Steal login credentials, credit card information, email, passwords
- Send / intercept / hide SMS messages
- Enable keylogging functionalists
- Steal Google Authentication codes

These applications are detected by Quick Heal with the name "**Android.Banker**"

3] Spyloan - Instant LOAN applications harass users

These applications offer small loans without requiring much paperwork but charge heavy interest rates. These applications request contact, SMS, storage, and camera access permissions. This data is used by threat actors to harass users very inadequately. RBI issued new guidelines in September that state loan applications for not allowing apps to access irrelevant data. RBI is in the state to prepare a white list of legal loan applications. Simultaneously, Google Play Store also came with a new policy for such loan applications that states the developer to submit more information about their NBFC on Play Store. We detect such applications as PUA (Potentially Unwanted Applications) as **Android.Spyloan** and warn the user.

Android RAT targeting Indian Defense personnel

This malware spread via WhatsApp, with the name "CSO_SO on Deputation DRDO. Apk"and uses the Adobe reader icon. This malware collects location information like altitude, latitude, and longitude. And sends this data to the C2 server. It checks the victim's phone for a list of mobile security products and, in the future, may try to disable it. Quick Heal detects these applications with the name **Android.McalProtect.GEN**

Inference

This Q3 2022, the pendulum has swung harder in the direction of detection of threats in the current cyber world. This is where our security labs have played a successive role and never wavered from their mission to detect, block, and remove malicious code and instructions from devices.

This quarter 3 report provides holistic and multilayered cybersecurity trends highlighting numbers to protect people from increasing attacks. While we witness **1.12** Million Malware attacks on Windows and **222** Android Malware on a daily basis, it is advisable to proactively back up all your sensitive data on a separate storage device or on drives. If attackers are up for targeting with more attacks, it's time to stay extra cautious and safe. Hence, we highly recommend that all our users include cyber intelligence while browsing the digital world.

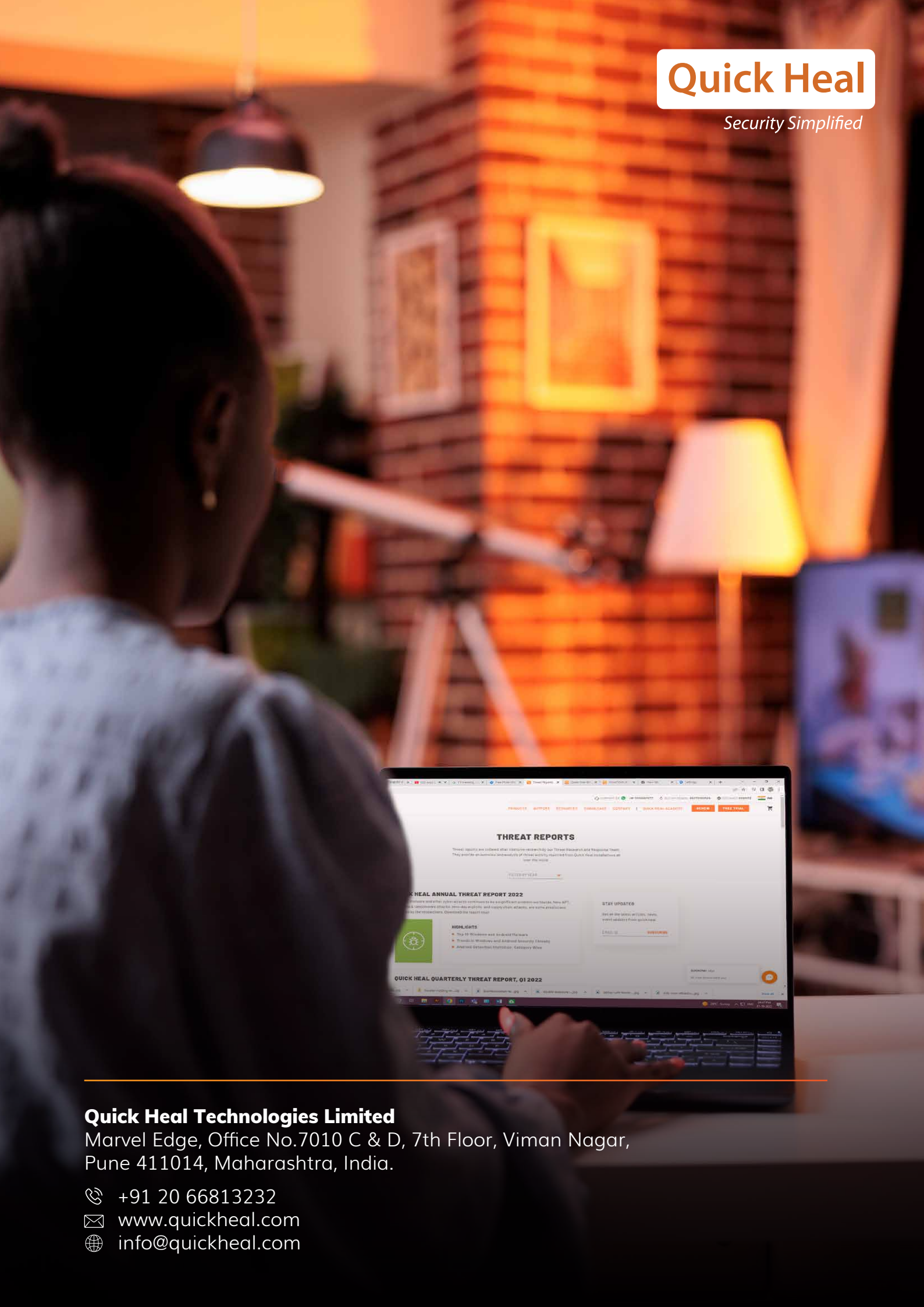
Tips to be secured:

- Use a firewall
- Keep your systems up to date
- Report any suspicious activity
- Stay cautious while downloading any new application

It's important to follow the steps and take a layered approach to security with Quick Heal Cyber security solutions while preventing upcoming threats!

Quick Heal

Security Simplified



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

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