Quick Heal

Security Simplified

QUARTERLY THREAT REPORT Q3-2021

www.quickheal.com

QUARTERLY THREAT REPORT Q3-2021

Contributors

Quick Heal Security Labs
Quick Heal Marketing Team

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

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

Follow us on:

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

Cybercriminals upped their game over the last quarter—increasing the number of credential phishing attacks, coin miner and ransomware attacks, and account takeover attempts.

In the first half of this year, cybersecurity strongholds were surrounded by cyber criminals waiting to pounce at the sight of even the slightest crack in defenses to ravage valuable assets. These security issues include high-profile modern ransomware attacks, active campaigns, critical vulnerabilities, Covid-19-related scams, and other threats, not to mention developing threats in the cloud and the internet of things (IoT).

Last quarter also witnessed a rise in all types of advanced email attacks, with significant increases in the number of brute force attacks.

Q3 was certainly interesting and certainly not calm: contrary to our expectations. The Quick Heal Q3 2021 Threat Report covers observed trends in attackers' ever-evolving tactics, insights into windows and android malware, ransomware, and other cybersecurity threats from the threat research team.

WINDOWS

147 Million

Windows Malware detected in Q3

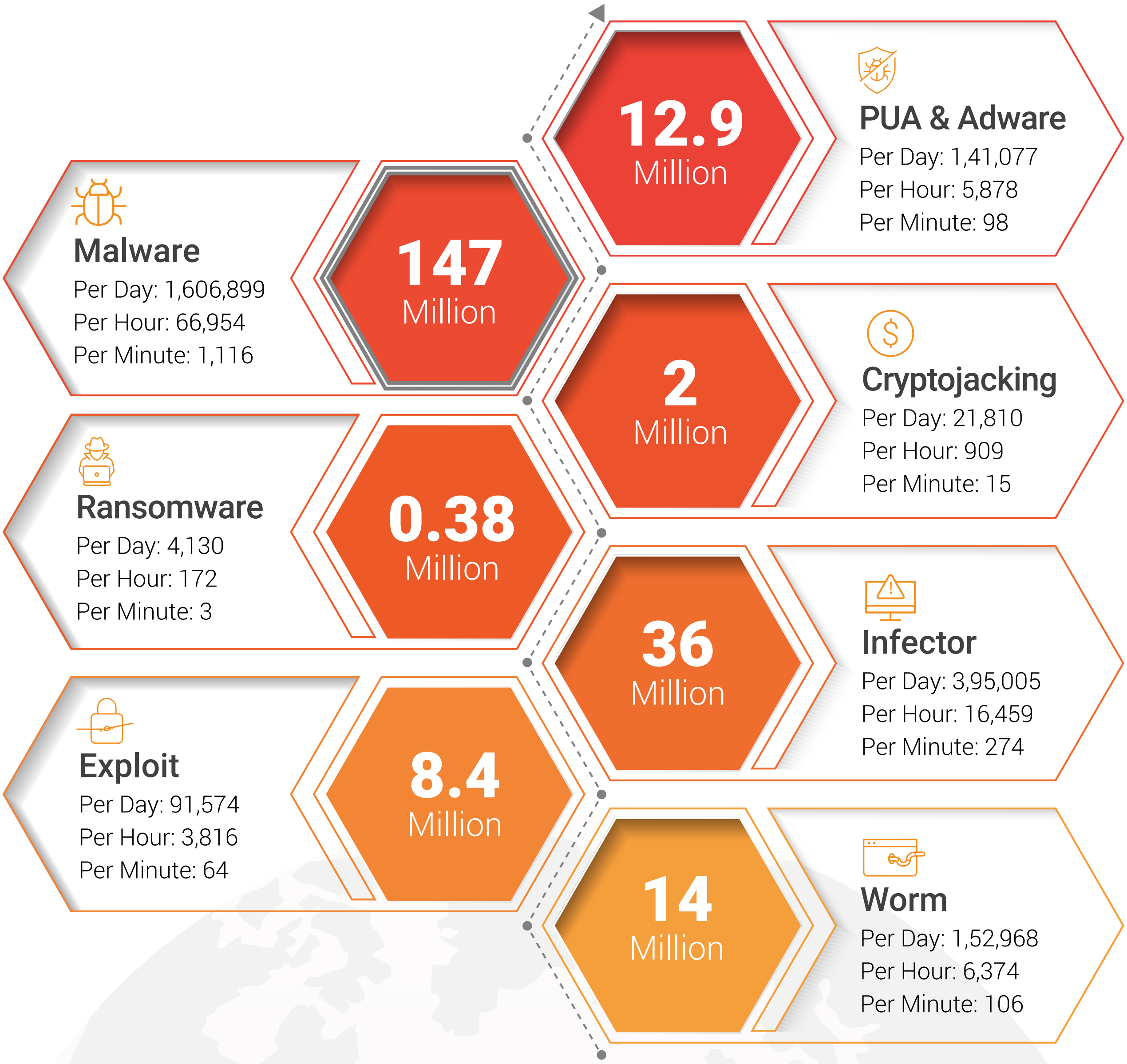
50 Million

Windows Malware detected in Aug’21

1.6 Million

Malware detected daily in Q3

Windows Detection Statistics **Q3 2021**



147 Million

Malware
Per Day: 1,606,899
Per Hour: 66,954
Per Minute: 1,116

0.38 Million

Ransomware
Per Day: 4,130
Per Hour: 172
Per Minute: 3

8.4 Million

Exploit
Per Day: 91,574
Per Hour: 3,816
Per Minute: 64

12.9 Million

PUA & Adware
Per Day: 1,41,077
Per Hour: 5,878
Per Minute: 98

2 Million

Cryptojacking
Per Day: 21,810
Per Hour: 909
Per Minute: 15

36 Million

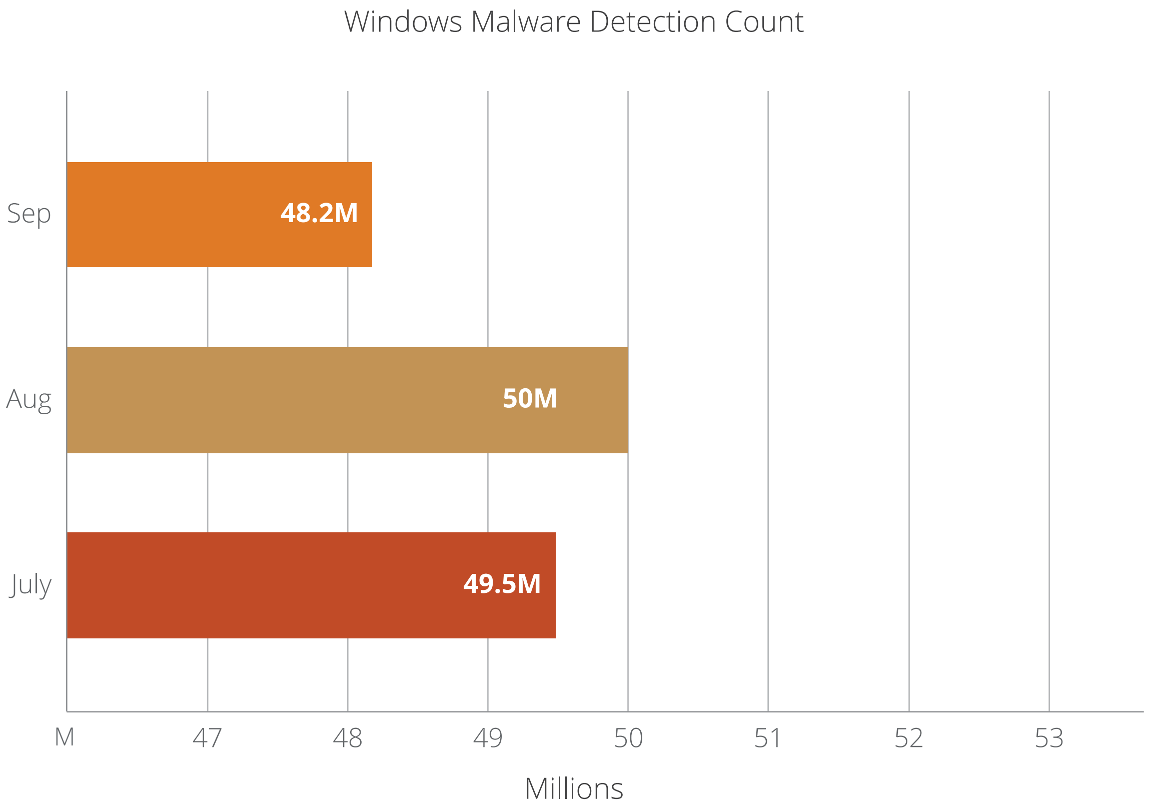
Infector
Per Day: 3,95,005
Per Hour: 16,459
Per Minute: 274

14 Million

Worm
Per Day: 1,52,968
Per Hour: 6,374
Per Minute: 106

Detection Statistics – Month Wise Q3 2021

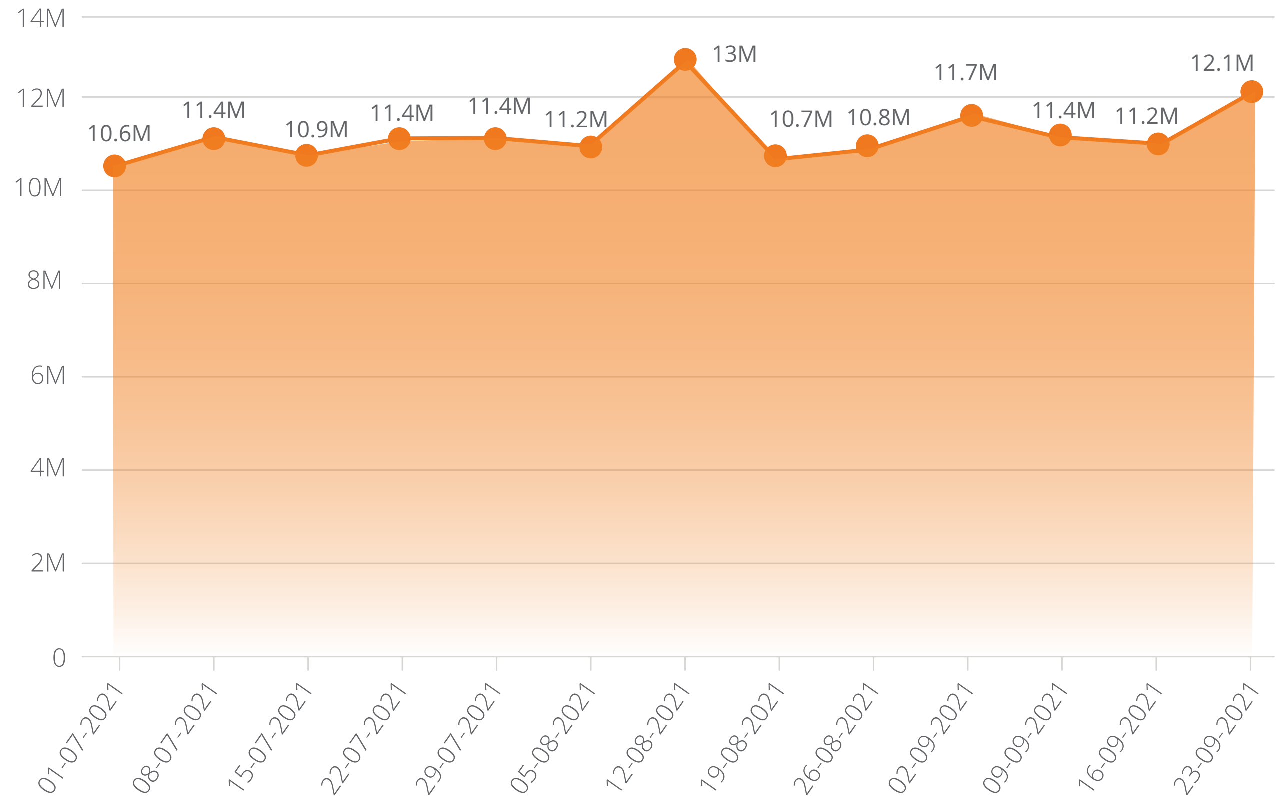
The below graph represents the statistics of the total count of Malware detected by Quick Heal from Jul to Sep 2021.



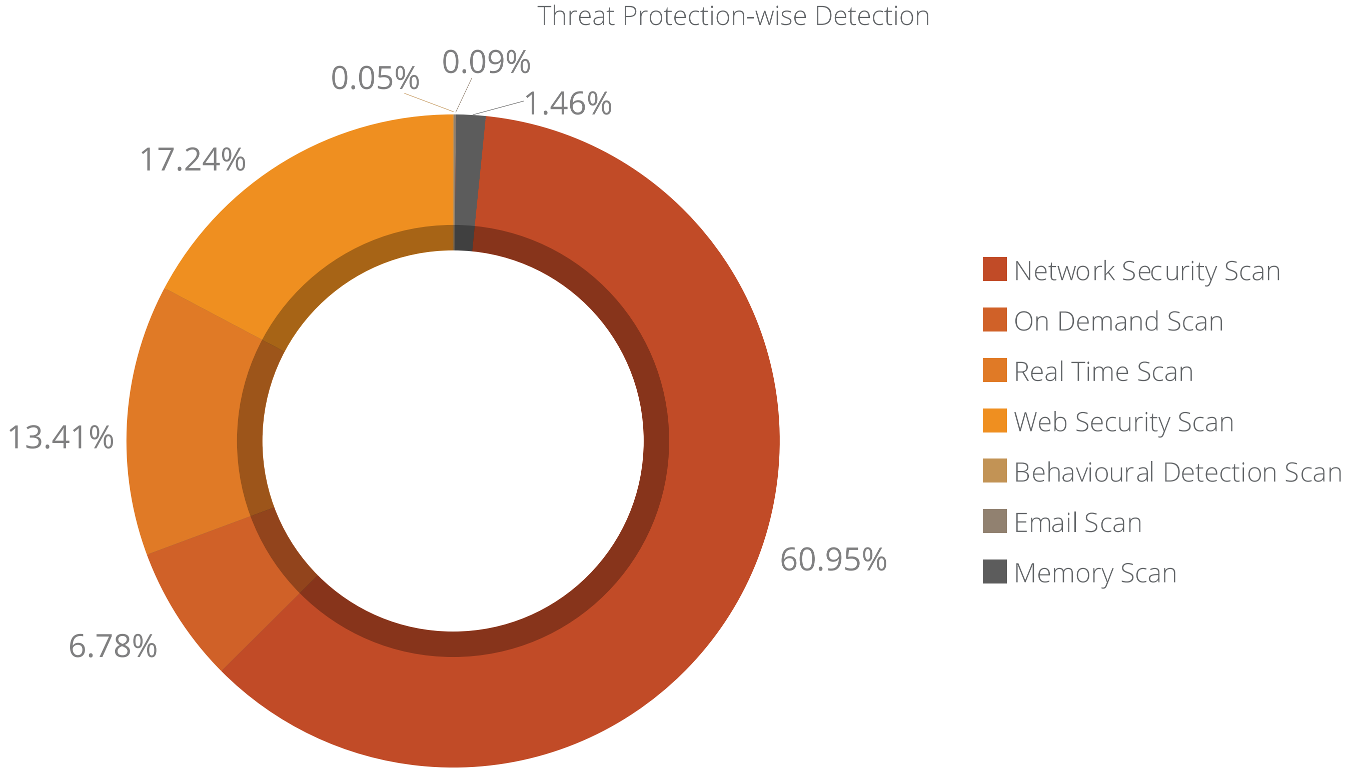
Observations

- Quick Heal detected over 147 Million Windows malware in Q3 2021. August clocked the highest detection.

Detection Statistics – Week-Over-Week



Detection Statistics – Protection Wise



Observations

- Maximum malware detections were made through Network Security Scan, which analyses network traffic to identify known cyberattacks & stops the packet being delivered to the system.

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

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

Behavioural Detection Scan

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

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.

Web Security Scan

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

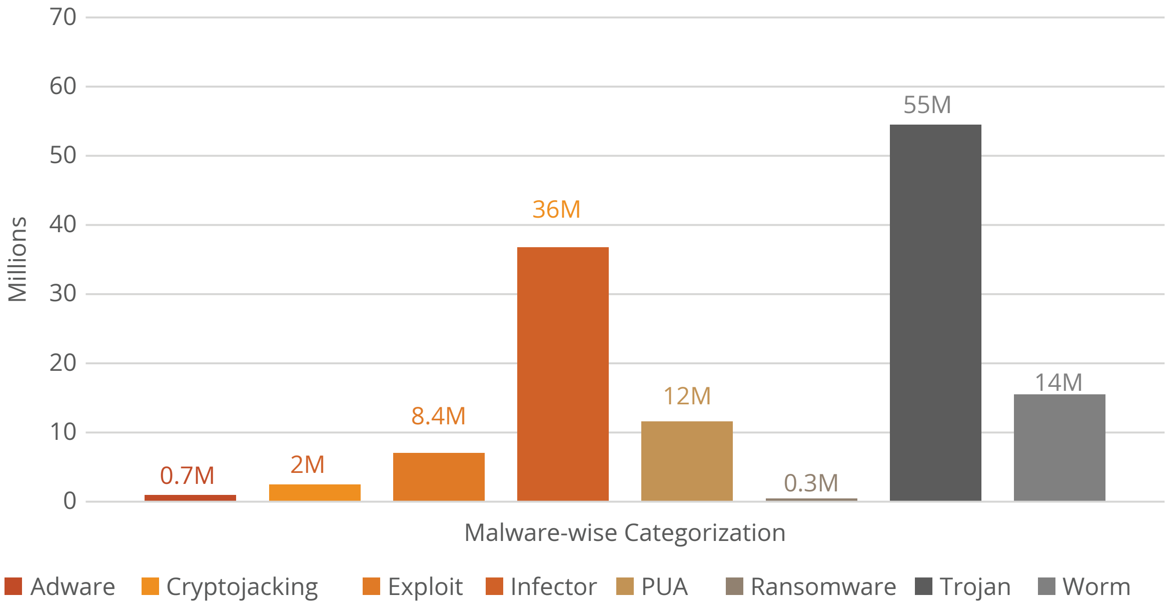
Network Security Scan

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

Detection Statistics - Category Wise

Categorization based on various Windows malware detected by Quick Heal in Q3 2021

A) Malware-wise Categorization



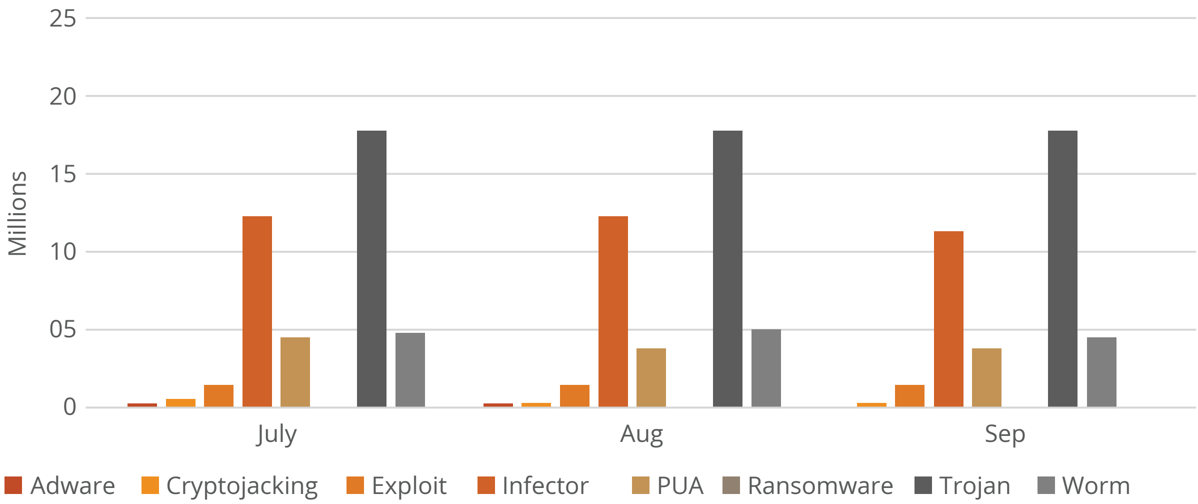
What is Trojan Malware?

A Trojan horse or simply a Trojan is a malware that misleads users about its true intent. It disguises itself as legitimate software and fools the user to take an action.

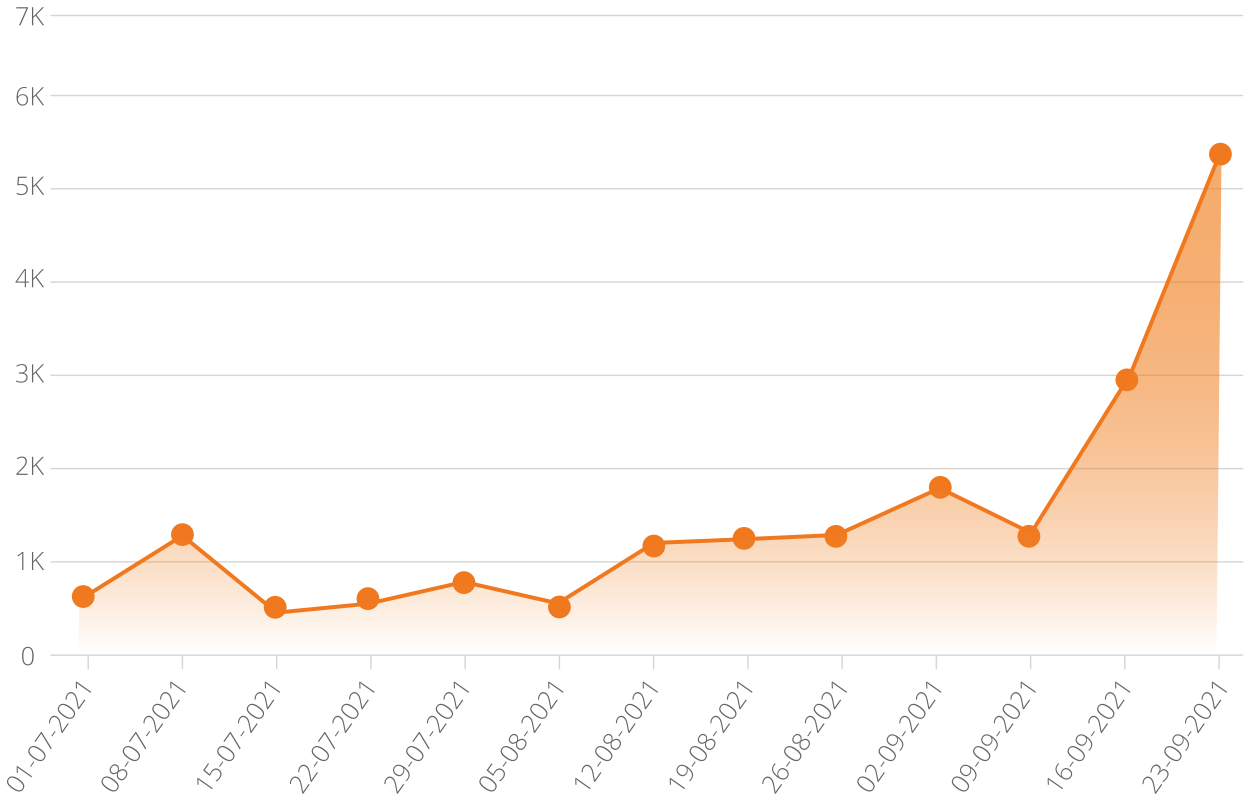
Observation

- Trojan malware was found to clock the maximum detection with 19 Million in September 2021

B) Month-wise Categorization



Coin Miner Detection Statistics

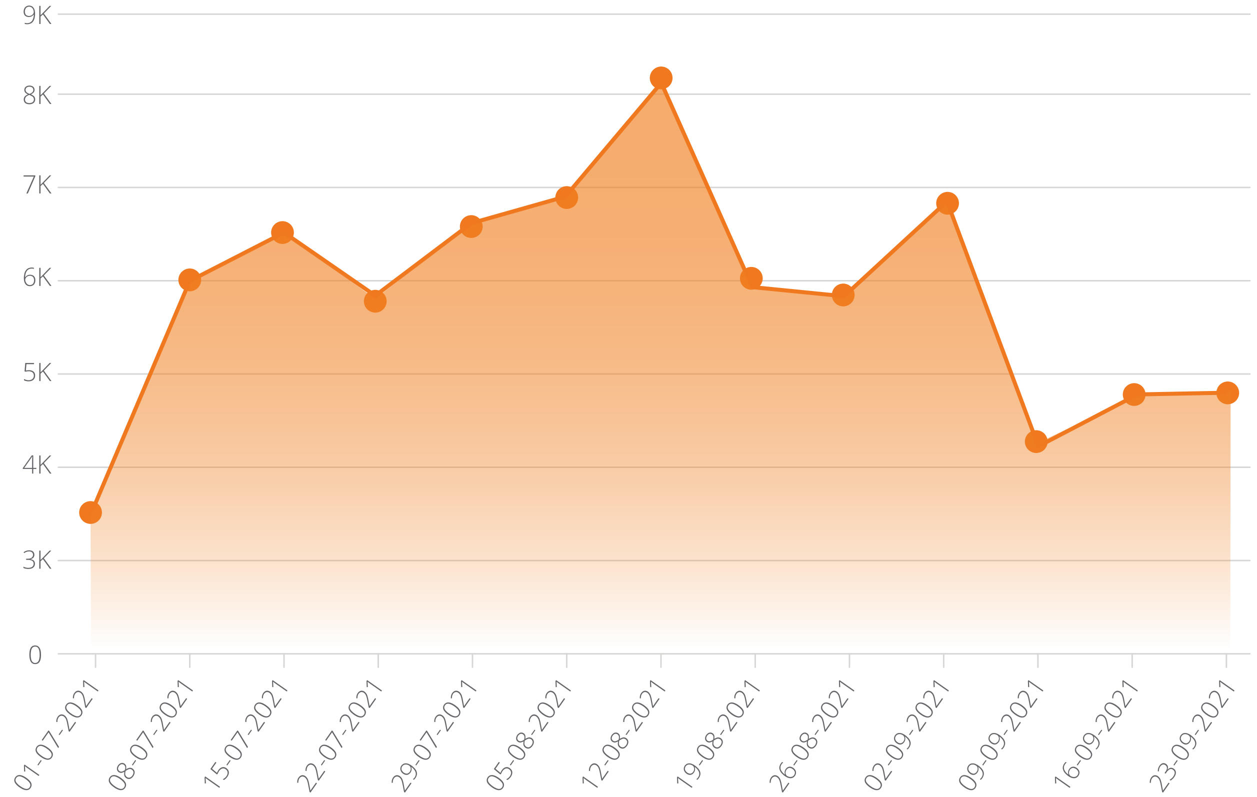


What is Coin Miner Malware?

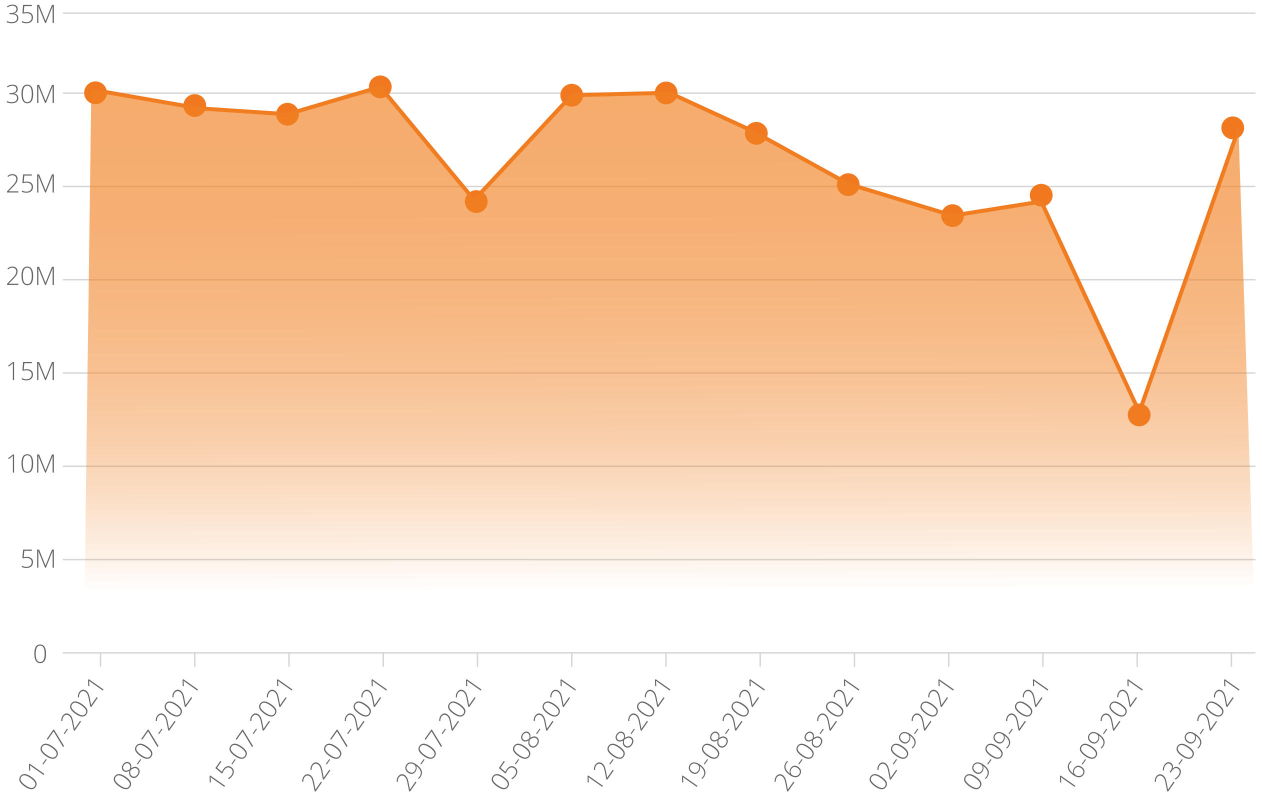
Coin Miners (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income.
Cyber criminals have created threats and viruses which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

Phishing Attack Statistics

A) Phishing Email Attacks

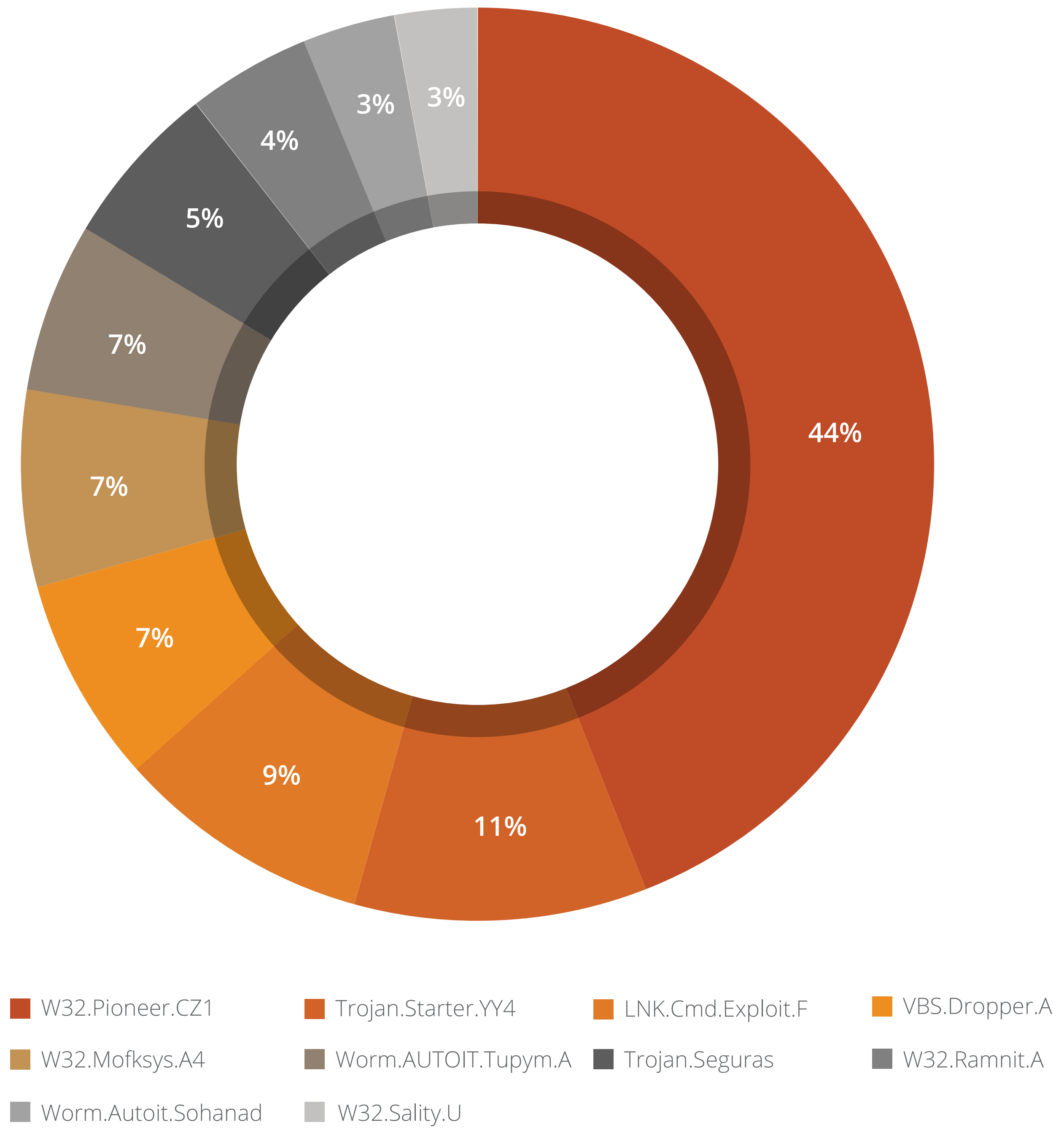


B) Phishing URL Attacks



Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q3 2021.
These malware have made it to this list based upon their rate of detection from July to September.



Top 10 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 which may cause a system crash.
- Downloads other malwares like key loggers.
- Slows down the booting and while shutting down the 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 a 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

VBS.Dropper.A

Threat Level: Medium

Category: Dropper

Method of Propagation: Web page

Behaviour:

- Spreads via malicious web pages and contains embedded PE file.
- It drops that PE file to specific folder & launches the file to perform malicious activities.

05

W32.Mofksys

Threat Level: High

Category: Worm

Method of Propagation: Removable or network drives

Behaviour:

- It copies itself to following paths:
  - <System>\explorer.exe
  - <Windows>\svchost.exe
  - <Windows>\spoolsv.exe
- It adds these paths to RunOnce registry.
- It can capture the activity like keyboard/mouse inputs, including screen capturing and pass it to the remote intruder.
- Drops a copy of itself on other machines in network through writable shared drives and further uses sc.exe to remotely execute as a service.

06

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.

07

Trojan.Seguras

Threat Level: Low

Category: Trojan

Method of Propagation: Bundled Applications

Behaviour:

- It often shows fake scan results luring users to purchase its full version.
- May download other malware that can infect the system.
- Degrades performance of the machine

08

W32.Ramnit

Threat Level: Medium

Category: File Infector

Method of Propagation: USB Drives, other malware, Exploit Kits, Spoofing the URL, and Bundled applications

Behaviour:

- This malware has several components embedded within it. After installer is dropped or downloaded, it drops its various components in memory or disk. Each component has specified task. This will also speed up the process of infection.
- It infects all running processes.
- It also infects HTML files by appending script in it while in the case of PE file infection it appends itself in the file.
- It modifies registry entries to ensure.

09

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.

10

W32.Sality.U

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

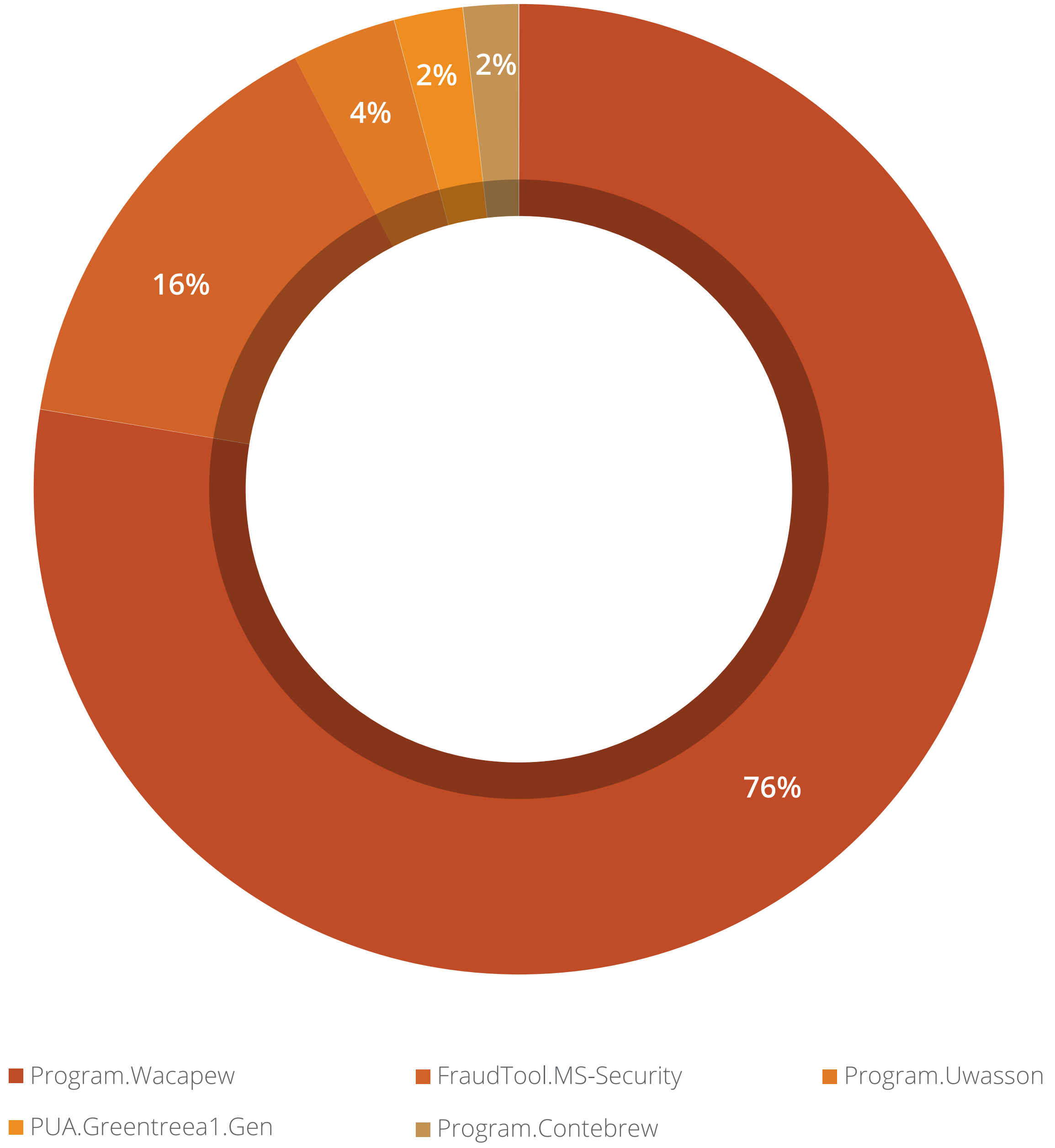
Behaviour:

- Injects its code into all running system processes. It then spreads further by infecting the executable files on local, removable, and remote shared drives.
- Tries to terminate security applications and deletes all files related to any security software installed on the system.
- Steals confidential information from the infected system.

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. 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 2021.

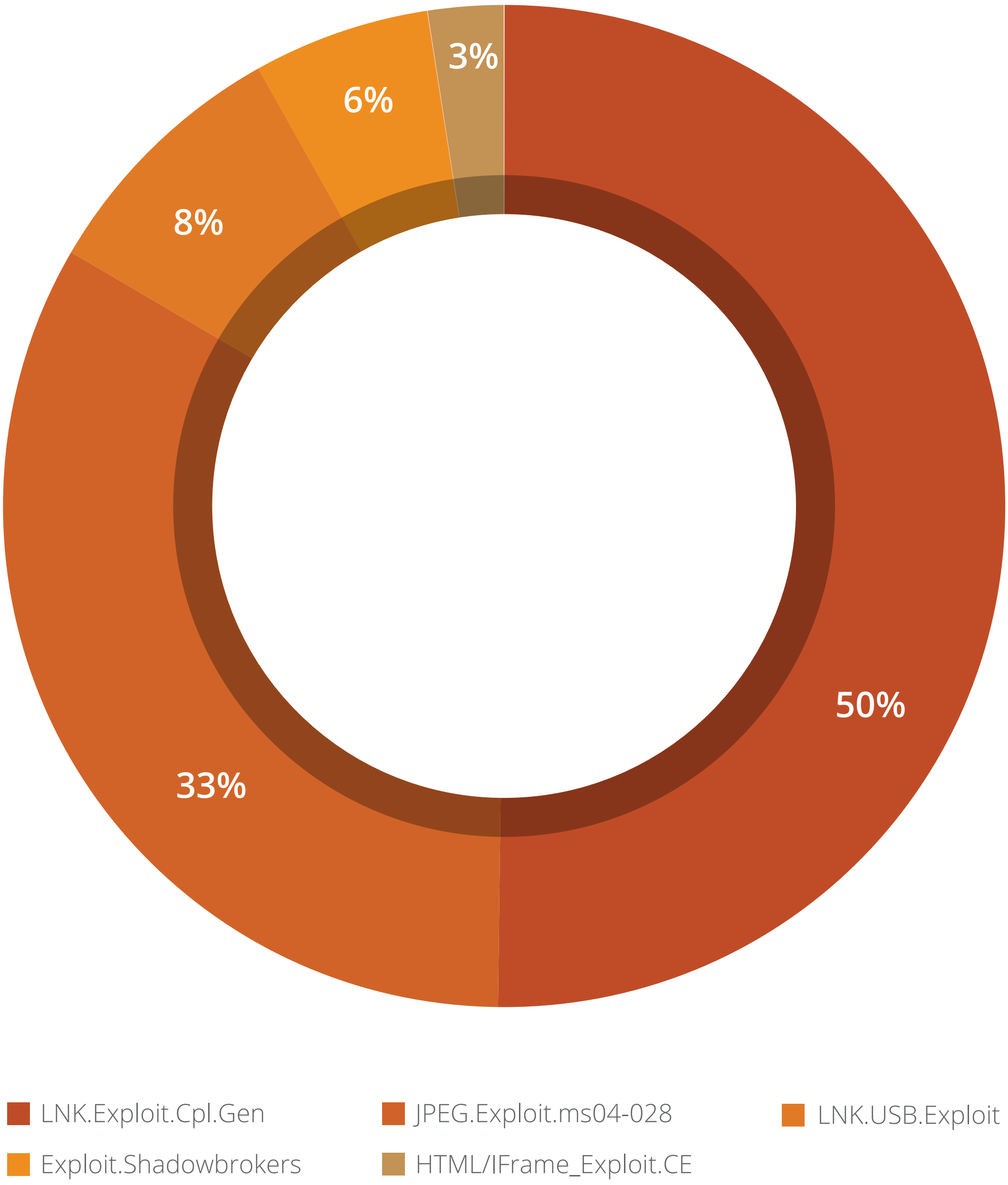


Observations

- Program.Wacapew was detected to be the top PUA, with 7.2 Million detections.

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.



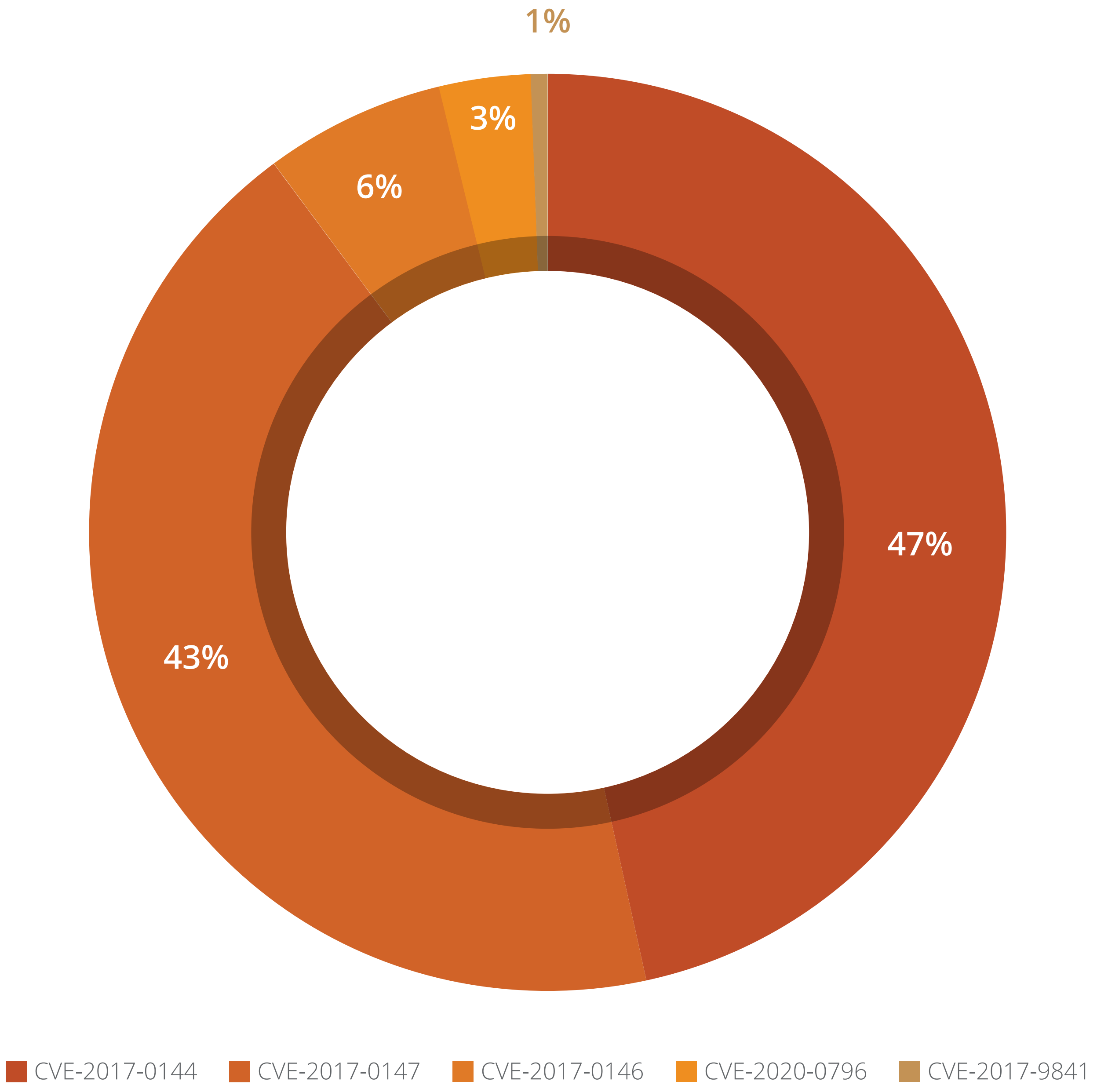
What are host-based exploits?
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection,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

Observations

- LNK.Exploit.Cpl.Gen was detected to be the top host-based exploit, with 0.6 Million detections.

Top 5 Network-Based Exploits

Below figure represents the top 5 Network-Based Windows exploits of Q3 2021



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)

Observation

- CVE-2017-0144 was detected to be the top network-based exploit, with 40 Million detections.

Trends in Windows Security Threats

01 FormBook Malware Returns: New Variant Uses Steganography

Quick Heal Security Labs has come across several malware like Agent Tesla, Racoon Stealer, Netwire, etc., using crypto named Onion crypter that uses multiple layers before delivering the final payload. One such family is the formbook which uses steganography in two of its layers. The interim layers are not written on disk, and they are present in memory only.

The final payload is injected in either itself or some targeted process like chrome.exe, iexplorer.exe, etc. Apart from stealing regular passwords, it also focuses on stealing discord tokens, telegram, and steam data. We have seen an increase in formbook malware activity in the past few months, and it's expected to increase in the coming days.

02 Targeted WSL by Deploying ELF As Stealth Windows Loaders

The Windows Subsystem for Linux (WSL) - the latest Windows Operating System version feature, allows users to execute Linux commands on the Windows operating system. The Windows Subsystem for Linux uses an application known as Bash.exe, which launches a Linux dialogue box within the interface. This might be considered as a "shell" application that runs within Windows. The WSL feature is introduced to leverage open-source software. It is also a new attack surface threat actors will try to exploit.

There was a recent attack reported on the WSL environment. The original payload script was written in Python 3 and then, with the help of PyInstaller, converted into an ELF executable for Debian Linux. This ELF binary acts as a loader running a payload that was either embedded inside the sample or retrieved from a remote server, and it is then injected into a running process. This would enable an actor to obtain an unnoticed footing on a compromised machine. The ELF loader has two variants: the first one was written entirely in Python.

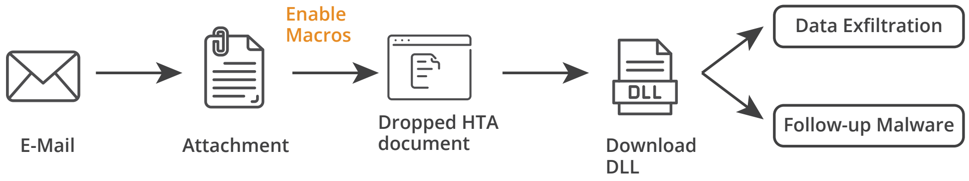
In contrast, the second uses Python to call several Windows APIs via ctypes and launch a PowerShell script to perform further operations on the host machine. Some of the samples included lightweight payloads generated by open-source tools like MSFVenom or Meterpreter. In other situations, the files tried to download shellcode from a remote C2. We advise users to enable WSL support only when they need it and otherwise limit the attack surface.

03 Bazarloader: Use of old technique to remain undetected

This year a new malware campaign dubbed Bazarloader is observed. This campaign is very diverse in its delivery mechanism. Last quarter it was seen making use of Excel 4 macro. This quarter, it used an old technique known as "WordProcessingML." WordProcessingML or Word 2003 XML Document is an XML-based format introduced in Microsoft Office 2003 as one of the formats that could be chosen in the "Save As" feature to save Word documents, though not the default format (e.g., DOC, a proprietary binary format). This is different from the "Microsoft Office Open XML File Format" introduced in Office 2007, which consists of a ZIP archive of various files, including XML.

In contrast, WordProcessingML is a single uncompressed XML file. This XML file contains Ole VBA macro and payload encoded in Base64 and obfuscated format, respectively. Executing this file will drop an HTA file that other downloads DLL files dropped at the "C:\Users\Public" location. This malware also used to spread other modules of different malware families like Trickbot, Ryuk Ransomware, and Cobalt Strike.

Infection Chain:



04 CVE-2021-40444: Zero Day Exploit in the Wild

Microsoft disclosed a new 0-day vulnerability, "CVE-2021-40444," a Remote Code Execution Vulnerability in MSHTML that affects Microsoft Windows machines and many other servers. Malicious Office Documents exploit this vulnerability. An attacker could trick a malicious ActiveX control into using a Microsoft Office document that hosts the browser rendering engine. The attacker should then have to convince the user to open that malicious document.

The exploit document is used as an external object relationship to download exploitative JavaScript. This javascript would be responsible for downloading a CAB file containing a DLL bearing an INF file extension and then decompression of that CAB file and execution of a function within that DLL. The DLL retrieves remotely hosted shellcode which will result in the execution of malware families such as Cobalt Strike Payload or Formbook malware.

05 Different Phishing Attack Techniques use to steal data

Phishing is a technique used to steal sensitive data such as login credentials, personal information & financial details of a user. Attackers' most prevalent ways to attempt phishing are social networking sites, SMS, and email notifications. Some of the purchased resources like Phish kits are used by attackers in phishing attacks that come with ready-to-use email phishing templates designed to evade detection.

The different techniques prevalent are emails with phishing attachments and embedded links, hidden text in phishing emails, messaging services (SMS, WhatsApp etc.), encoded phishing pages in scripts.

If the victim is accessing the phishing link from the mail, it will redirect to fake pages that look similar to the legitimate one, such as a fake Microsoft login page. In spear phishing or whale phishing, the victim is not prompted to input their email address as it is already embedded, so the victim is asked for their password before being redirected to the legitimate page. Generally, when the password is provided, it will not throw an error for the first time. Instead, it accepts the entered password. After clicking on the sign-in option, it again redirects to the legitimate page, but in the background, targeted email ID and entered password are sent in POST request to phishing URL. As a result, the victim has no idea that they entered their password on a fake site. In this way, attackers harvest credentials.

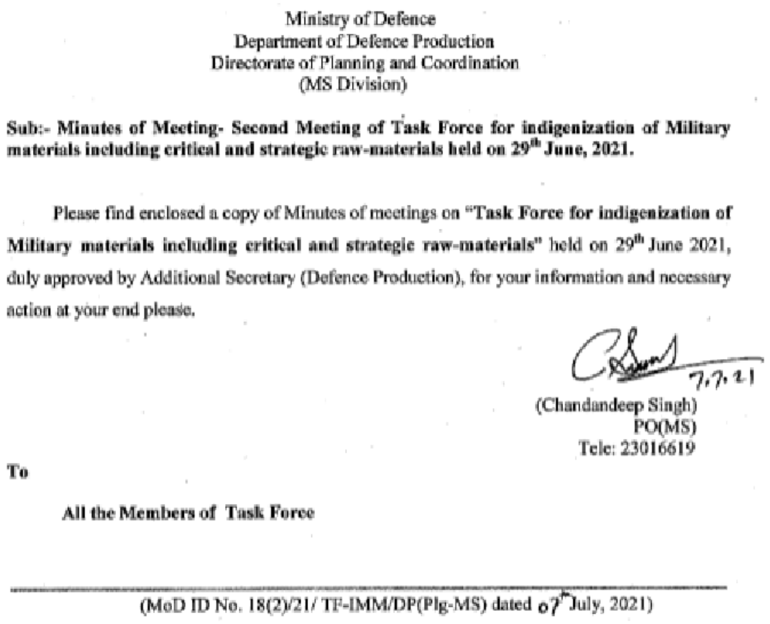
06 Sextortion email scams demand payment to bitcoin wallet

Sextortion is an emerging online scam that takes advantage of people's fear to blackmail the victim and threatens to expose private data like photos, web browsing history, chat history, and so on. Generally, these sextortion scammers send emails & claim that they have gained access to the victim's device, installed a trojan virus by logging into an email account. The sexual leverage is then applied, claiming that your activity is being recorded through the controller of your devices like camera, microphone, etc. Finally, the attacker makes an extortion pitch, telling the targeted victim to avoid leaking personal/sensitive data by paying USD 1550 in bitcoin.

If a sextortion email appears in your inbox, stay calm and do not reply to the scammers. Without further ado, you should change your password to avoid unauthorized access to your accounts. In addition, nobody is going to blackmail you. It's just spam. However, it can be a clue that your data leaked during various data breaches, such as your email address.

07 Crimson RAT predominantly used for info-stealing in targeted attacks

Crimson Rat is a . NET-based RAT and has been used by APT36 for the past five years to target its victims across multiple countries, mainly India. The attacks are not very sophisticated and are carried out by sending spear-phishing emails containing malicious attachments. Attachments are usually MS Office files containing macros. After execution, a decoy document is presented to the user while the PE file is executed in the background. It has the functionality to check system info, spy on victims, steal credentials, and exfiltrate sensitive file.



Ministry of Defence
Department of Defence Production
Directorate of Planning and Coordination
(MS Division)

Sub:- Minutes of Meeting- Second Meeting of Task Force for indigenization of Military materials including critical and strategic raw-materials held on 29th June, 2021.

Please find enclosed a copy of Minutes of meetings on **"Task Force for indigenization of Military materials including critical and strategic raw-materials"** held on 29th June 2021, duly approved by Additional Secretary (Defence Production), for your information and necessary action at your end please.

7.7.21

(Chandandeep Singh)
PO(MS)
Tele: 23016619

To

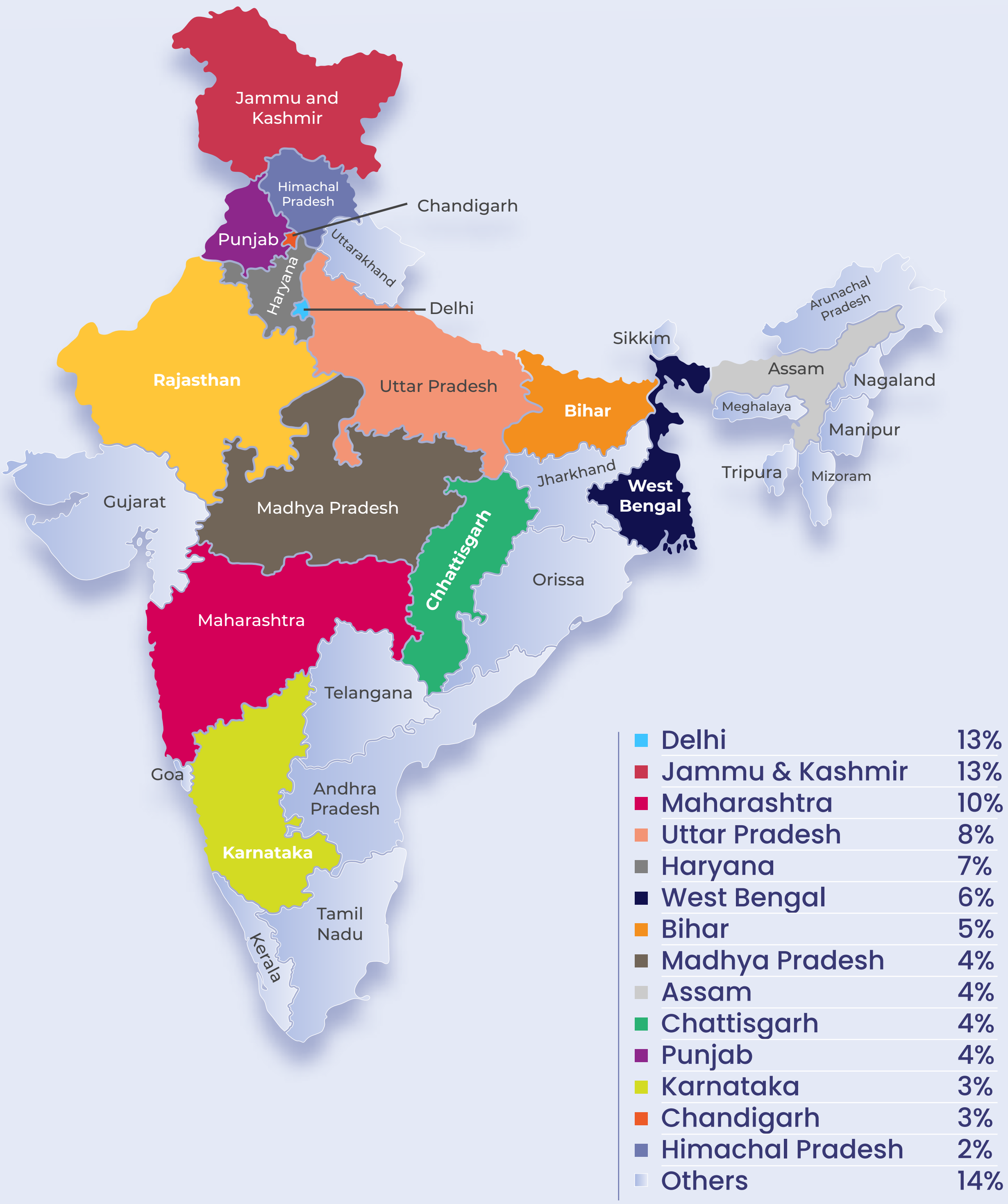
All the Members of Task Force

(MoD ID No. 18(2)/21/ TF-IMM/DP(Plg-MS) dated 07 July, 2021)

Fig. 1: Sample Decoy Document

Crimson RAT has a definite pattern of communicating with its C2. It has one server IP hardcoded in the binary along with five distinct server ports. The client expresses with the C2 server IP on the 5 TCP ports in a round-robin way. In Q3 2021, we observed multiple Crimson RAT campaigns over 19 different C2 IPs targeting government employees across other states. 36% of attacks were spread in Delhi, Jammu & Kashmir, and Maharashtra regions. Below is the detailed state-wise distribution of attacks.

CRIMSON RAT Target Regions

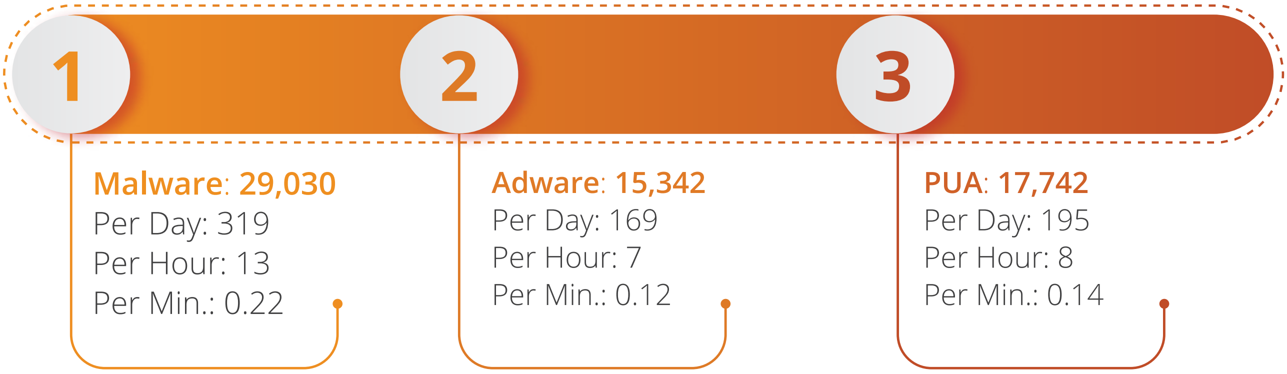


🟦	Delhi	13%
🟥	Jammu & Kashmir	13%
🟥	Maharashtra	10%
🟧	Uttar Pradesh	8%
⬛	Haryana	7%
⬛	West Bengal	6%
🟧	Bihar	5%
🟫	Madhya Pradesh	4%
⬜	Assam	4%
🟩	Chattisgarh	4%
🟪	Punjab	4%
🟨	Karnataka	3%
🟥	Chandigarh	3%
🟦	Himachal Pradesh	2%
⬜	Others	14%

ANDROID

47% of total Android detection in Q3 2021 was Malware

Android malware detections for Q3 2021



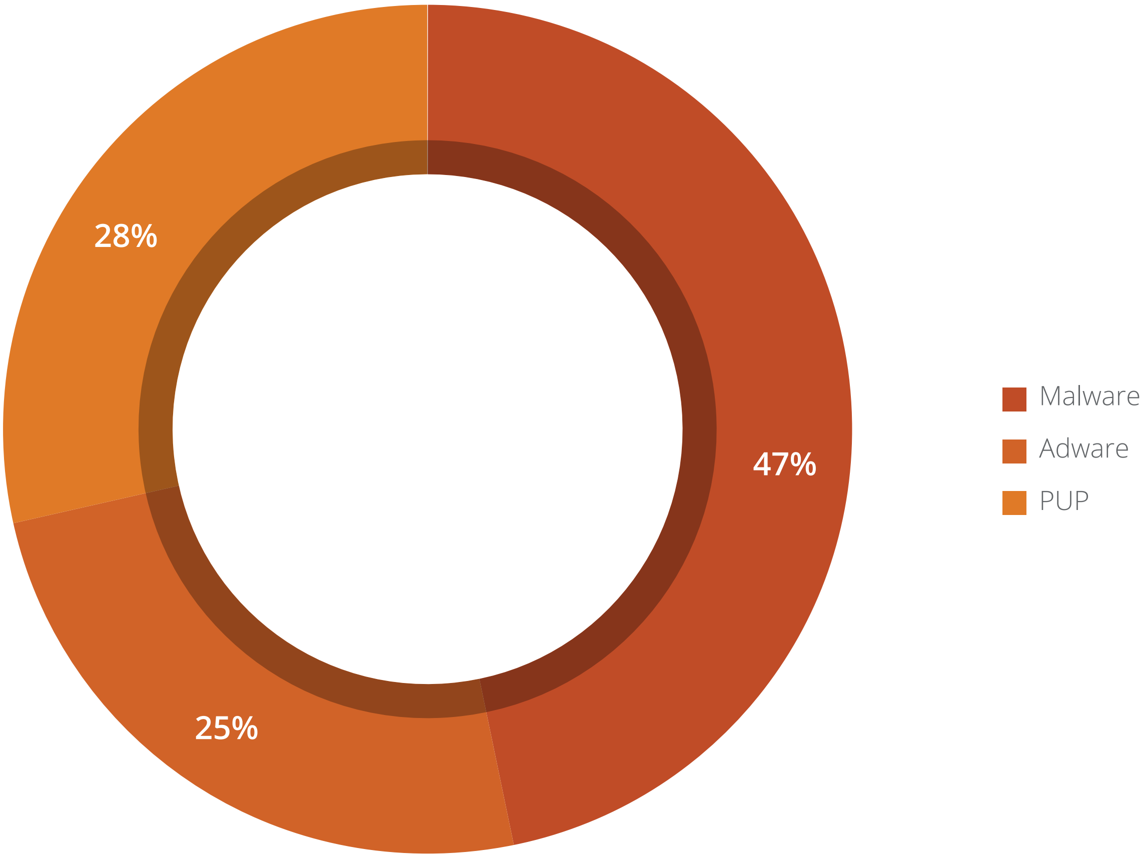
Malware: 29,030
Per Day: 319
Per Hour: 13
Per Min.: 0.22

Adware: 15,342
Per Day: 169
Per Hour: 7
Per Min.: 0.12

PUA: 17,742
Per Day: 195
Per Hour: 8
Per Min.: 0.14

Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q3 2021.

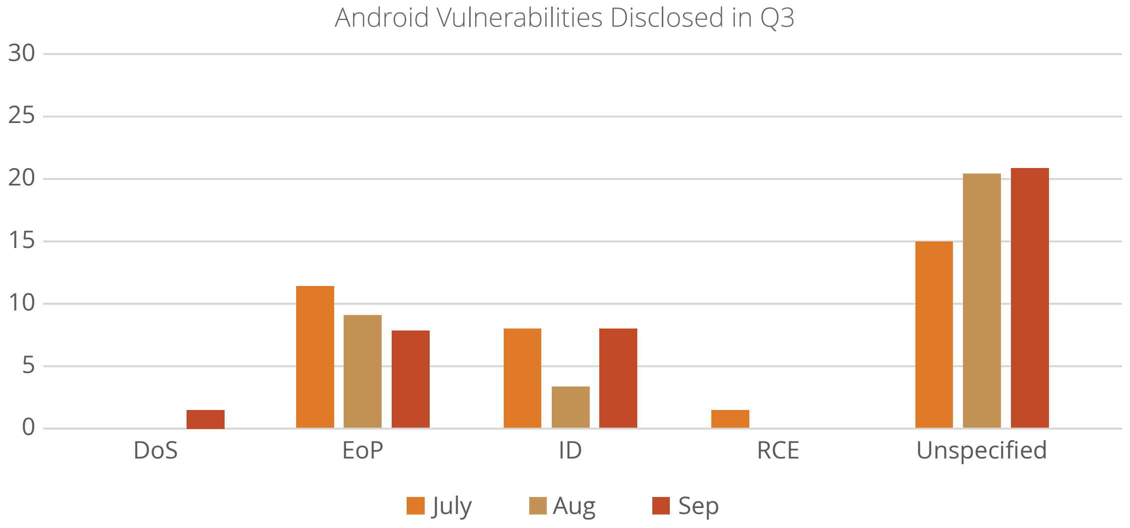


Observations

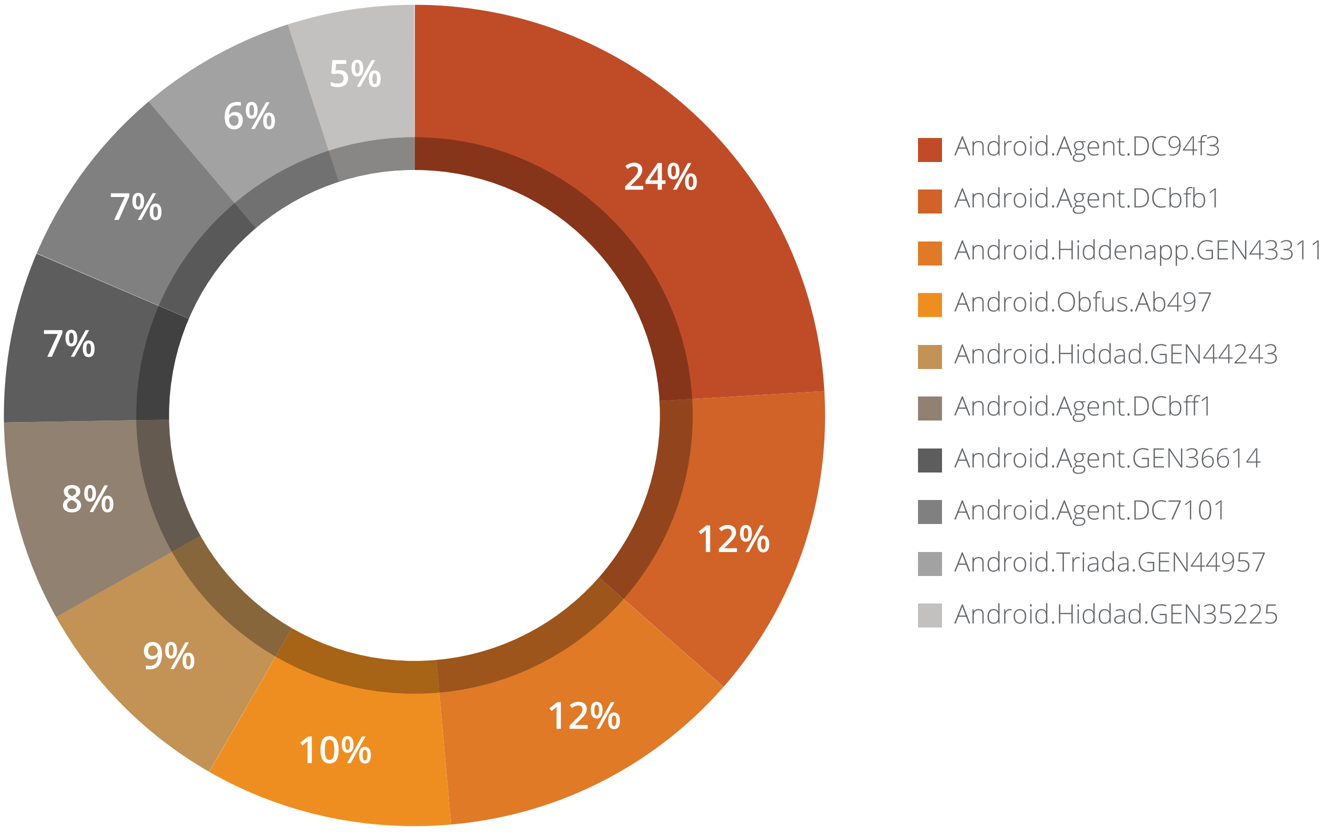
- Malware clocked 47% of the total Android detections in Q3 2021.

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 July to September 2021.



Top 10 Android Malware for Q3 2021



Top 10 Threat Details

01

Android. Obfus.Ab497

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behaviour:

- This malware loads a payload from the assets folder and converts it into an Android executable file. Its code is highly obfuscated, so it becomes hard to detect. It has a list of specific apps of whose package info is shown in alert dialogue.

02

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 folder.
- Encrypted payload has advertised SDK which shows full screen advertisements.

03

Android.Agent.DCbfb1

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behaviour:

- It disguises as a genuine app. After launching, it hides its icon and runs in the background.
- This malware's activity is to visit the web pages in a hidden way and display advertisement that it receives from its C&C server.

04

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.

05

Android.Agent.DCbff1

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behaviour:

- It is from the Trojan-Downloader family.
- It collects device details like country code, model, IMEI, SIM details, phone number, installed packages list, running process info, etc.
- It collects contact list, call logs, SMS data and send all collected information to the C&C server.
- It downloads the malicious application and installs it.

06

Android.Hiddad.GEN44243

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behaviour:

- It hides its icon on the first launch.
- Shows message like 'Application is unavailable in your country'
- Runs services in the background and shows full screen advertisements.
- It collects device information like Country code, IMEI, phone number, etc.
- It then sends collected information in an encrypted format to a remote server.

07

Android. Hiddenapp.GEN43311

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores and protector plug-ins

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 user to unnecessary services, downloads other malicious applications & enables browser notification.
- Request users to visit the different websites and download an application called "Adblock," which has nothing to do with the legitimate application and does the opposite of blocking ads.

08

Android. Agent.GEN36614

Threat Level: High

Category: Potentially Unwanted Applications (PUA)

Method of Propagation: Third-party app stores

Behaviour:

- It is a remote administration tool that is used to hack any android device.
- It enables hackers to collect personal information like user messages and contacts.
- It also gains access to the camera and microphone of the infected device and spies on infected users.
- The hackers can even make calls using infected devices.

09

Android.Agent.DC7101

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behaviour:

- This malware is from the Trojan-dropper category.
- It looks like a legitimate application like RAM cleaner.
- It carries an encrypted malicious payload with it.
- It uses an encrypted Chinese string to decrypt the payload for further malicious activity.

10

Android.Triada.GEN44957

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behaviour:

- It hides its icon and runs silently in the background.
- On execution, it asks the user to grant device admin permission.
- It displays a pop-up prompt and asks the user to download other applications. The prompt cannot be dismissed and shows up continuously on the mobile screen.
- In the background, it downloads and installs several other malicious apps.
- Records device information and sends it to a remote server.

Trends in Android Security Threats

01 Malware Targeting Indian Taxpayers

Quick Heal security labs observed a few Android malware applications which are targeting Indian taxpayers. These applications spread through fake text SMSs in the name of the Income-tax department of India. These applications have used the income tax department's original logo to trap users.

This Malware collects sensitive information like SMS data, phone number, E-mail address, etc. Attackers behind this have exposed this sensitive data on the internet. Quick heal detects these malware applications with the detection name **Android.Agent.DCc127**.

02 How unlimited internet data has changed the face of cybercrime?

Voice over LTE is a high-speed wireless communication standard for mobile phones. It has up to three times more voice and data capacity than older 3G UMTS and up to six times more than 2G GSM. With its increased data capacity, users don't need to use the data very judiciously, and they can keep the internet connection on every time. Due to this, internet-connected devices are always at a higher risk of infection and online fraud.

That is the reason users who use VoLTE are the preferred target of threat actors around the world. Jio is one of the mobile operators which uses VoLTE technology. Quick Heal Security Labs has gone through multiple scams, fake messages, and fake applications that exploit Jio users and published one blog over the last few years. This malware uses different ways like fake apps on the Google play store using the name of JIO, fake WhatsApp messages about JIO prime offers, fake Jiocoin apps on Google Play Store, fake JIO apps offering free data but only shows advertisements, fake messages targeting JIO users to spread adware.

Quick heal detects such applications under the variants of **Android.Fakeapp** and **Android.GoodNews**.

03 Aggressive evolution in banking Trojan

Quick Heal Security Labs has seen a considerable rise in banking trojan in the last three months. Banking trojan primarily targets Banking apps, Cryptocurrency Apps, and Crypto wallets. It steals the credential using the overlay technique. These Malware masquerades as Legitimate Applications for spreading.

- **SOVA banking malware** -

We have seen different banking trojans target some groups of countries like SOVA, a banking trojan capable of stealing credentials through overlay attacks and manipulating clipboards and notifications. It targets banks from Spain and USA region primarily. Quick Heal detects these kinds of malware by threat name **Android.ScytheSCF.QJ, Android.Agent.GEN.**

- **Coper** -

The Coper banking trojan targeting Colombian users loads encrypted dex files from the asset folder at runtime, which is responsible for tricking users for Accessibility Service and overlay attacks. Quick Heal detects these kinds of malware by threat name **Android. Agent.A.Android.Banker.A.**

- **Hydra** -

Hydra is resurfaced with a new variant targeting European banking users. It also uses the overlay technique to steal the credentials with different encryption techniques and team viewer features. Quick Heal detects these kinds of malware by threat name **Android.Agent.A.**

- **ERMAC** -

Recently found ERMAC banking trojan uses the code of Cerberus banking trojan discovered in 2019; It uses different encryption schemes in communication with the server. It is masquerading as a banking and media player application. Quick Heal detects these kinds of malware by threat name **Android.Agent.GEN45035**.

04 Fake Crypto mining Applications

There has been increased interest of many in crypto mining in recent times. Crypto mining uses the processing power of computers to solve complex mathematical problems that verify cryptocurrency transactions, and the miners are rewarded with a small amount of cryptocurrency. A typical mining strategy is called mining pools, where individuals can contribute computing power to get cryptocurrency in return that is proportional to what they contributed. Cloud mining is the evolution of mining pools, just like cloud computing. There are legitimate apps for this service.

These fake applications claim to offer this service to users for money. Users buy these services. Then these applications show a fake count of cryptocurrency as a reward. These applications have the option of paid upgrades and paid subscriptions. These applications are not doing any malicious activity. They are just taking money from users and showing fake UI to users. Quick heal detects these fake applications with detection **Android.Scamapp.A**

05 Facebook credential stealing Malware

FlyTrap and Facestealer malware spread through both Google Play and third-party application stores. These malicious applications take victims' Facebook account information like Facebook ID, email address, Location, and cookie and tokens associated with the Facebook account. This attacker has used various social engineering techniques.

This Trojan exploits one such process known as JavaScript injection. Using this technique, the application opens the legit URL inside a WebView configured to inject JavaScript code and extract all the necessary information. The attacker used login credentials for authorizing access and harvesting data. Quick heal detects these applications with detection **Android.Facestealer.A**

Inference

Q3 proved unexpectedly fast-paced for various sophisticated attacks: our records show several thousand attacks per day on some days. In Q3, the new ransomware groups quickly capitalized on some of the most dangerous vulnerabilities in the wild.

Our research underscores that ransomware continues to evolve and is becoming more dangerous based on the catastrophic damage it can inflict on target organizations. We continued to see ransomware attacks, coin miner attacks, and phishing attacks aggressively increase in sophistication and frequency in Q3.

The report showed a rise in activities compared to Q2 data and threat actors targeting perimeter devices.

It seems cybercriminals are training for a marathon—time to break a leg. We would recommend our customers increase their cybersecurity and incorporate threat intelligence into their daily operations.

You should also use a firewall, patch your systems, and monitor security news to keep up-to-date. Take a layered approach to security with Quick Heal advanced antivirus solutions and prevent tomorrow's threat today!

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