Quick Heal
Security Simplified

QUARTERLY **THREAT REPORT** Q2 - 2021

www.quickheal.com

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

Quarter 2 2021 saw a concerning amount of cyber activity, including ransomware and phishing attacks. Specific cyber-attacks like Joker Malware on applications in the Google Play Store, FormBook Malware, Warzone RAT, and more were seen repeated by the cybercriminals in an attempt to steal data and money from the users.

Ransomware continues to be a dominant threat even in this quarter and is expected to rise in the coming quarters. 2021 is proving to be 'an extraordinary year for vulnerabilities,' some experts are still predicting that the worst is yet to come.

Though the second quarter had comparatively lesser detections of around 125 Million, the quarter ended on a higher note, with June clocking the highest detection of 45 Million windows malware, including 0.22 Million Ransomware, 29 Million infectors, 12 Million Worm malware.

Tech Support Scams are back in trend wherein 7 out of 10 Indian consumers have encountered the scam in the past 12 months. The second quarter of the year witnessed malware's ability to convert clean applications into malicious ones with the help of vulnerabilities in the Android OS. While the vulnerability has been patched, users are advised to update installed applications.

The report details top malware in both Windows and Android and extensively discusses the top trends in cyberattacks.

WINDOWS

125 Million

Windows Malware detected in Q2

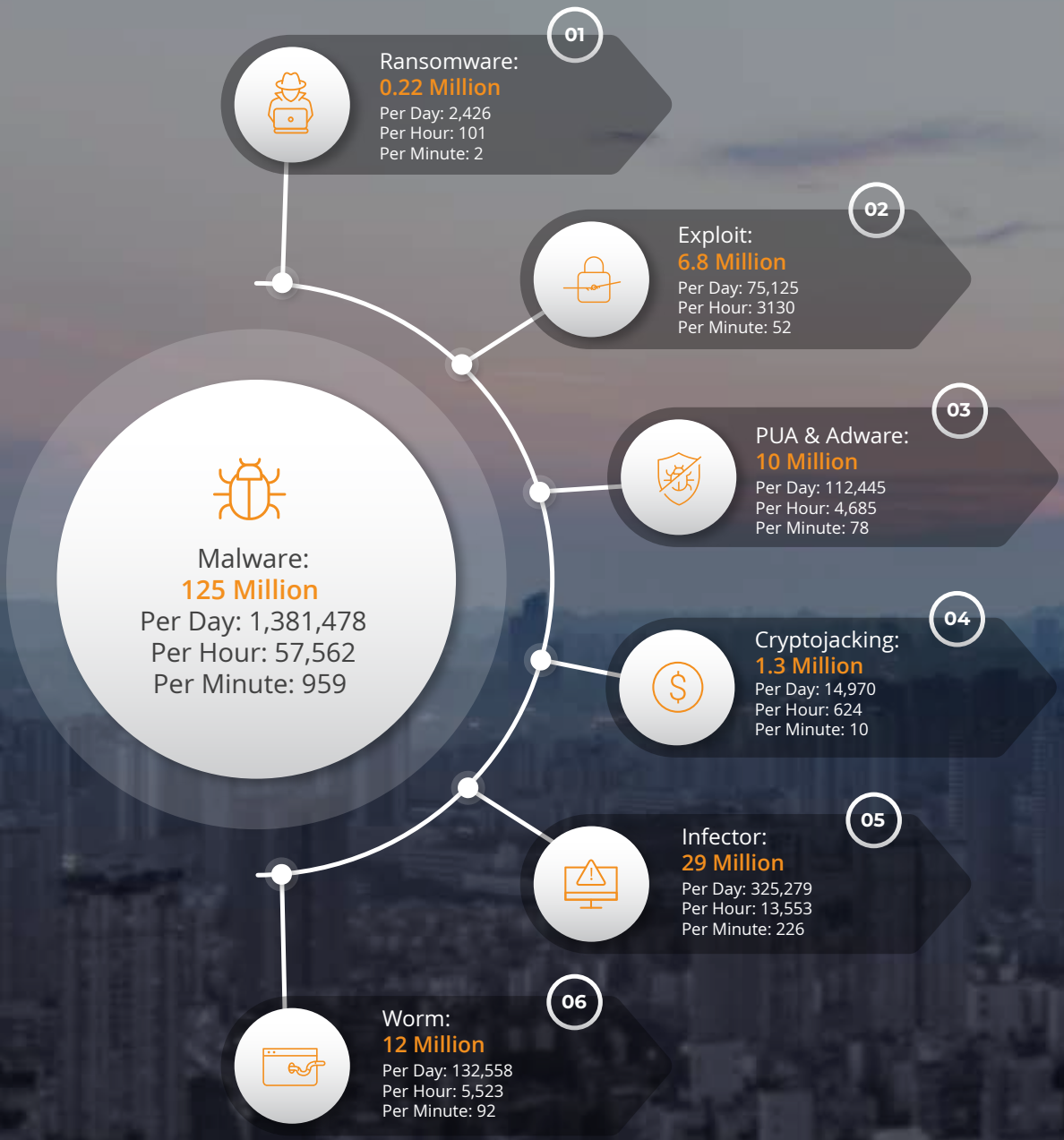
45 Million

Windows Malware detected in June'21

1.3 Million

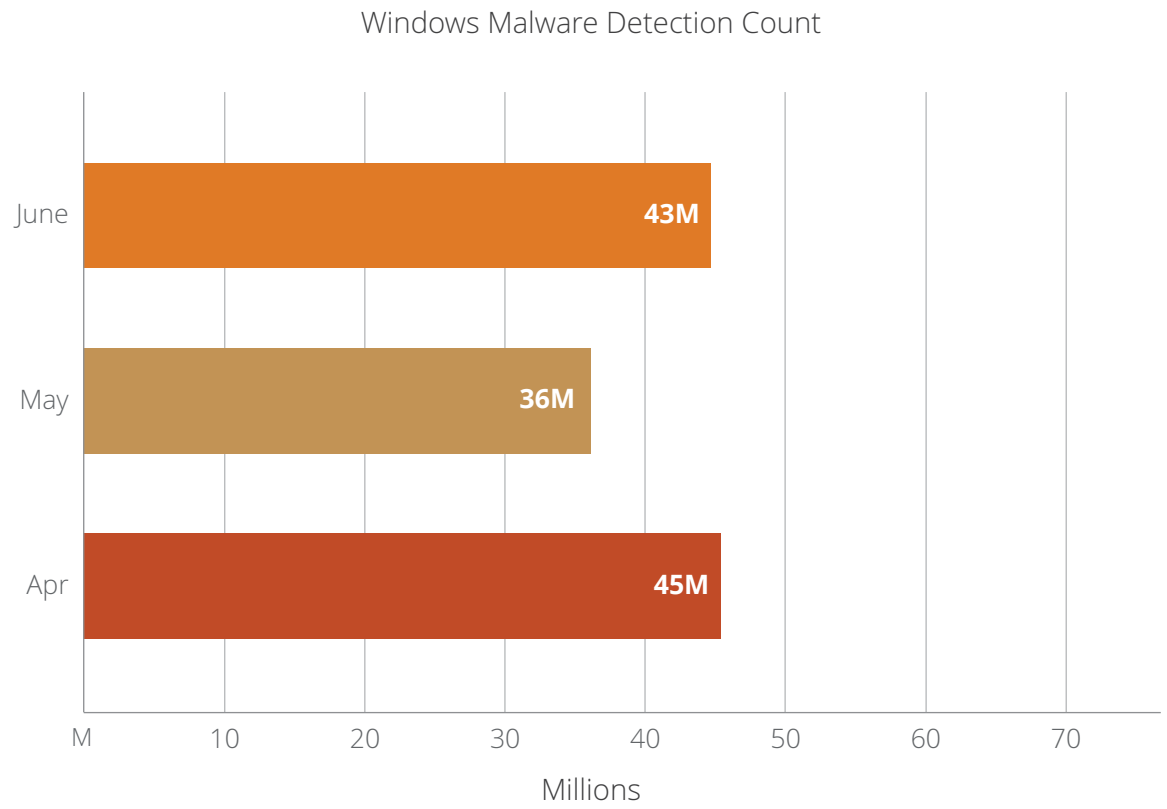
Malware detected daily in Q2

Windows Detection Statistics **Q2 2021**



Detection Statistics – Month Wise Q2 2021

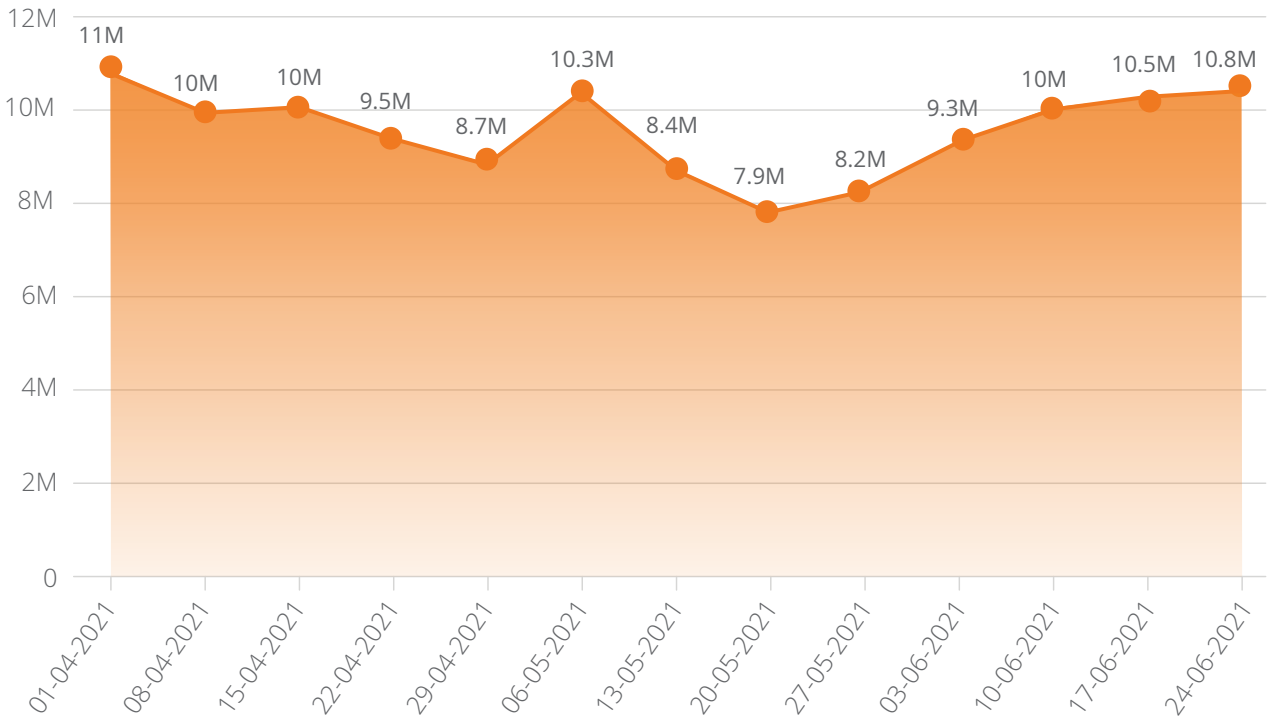
The below graph represents the statistics of the total count of Malware detected by Quick Heal from April to June 2021.



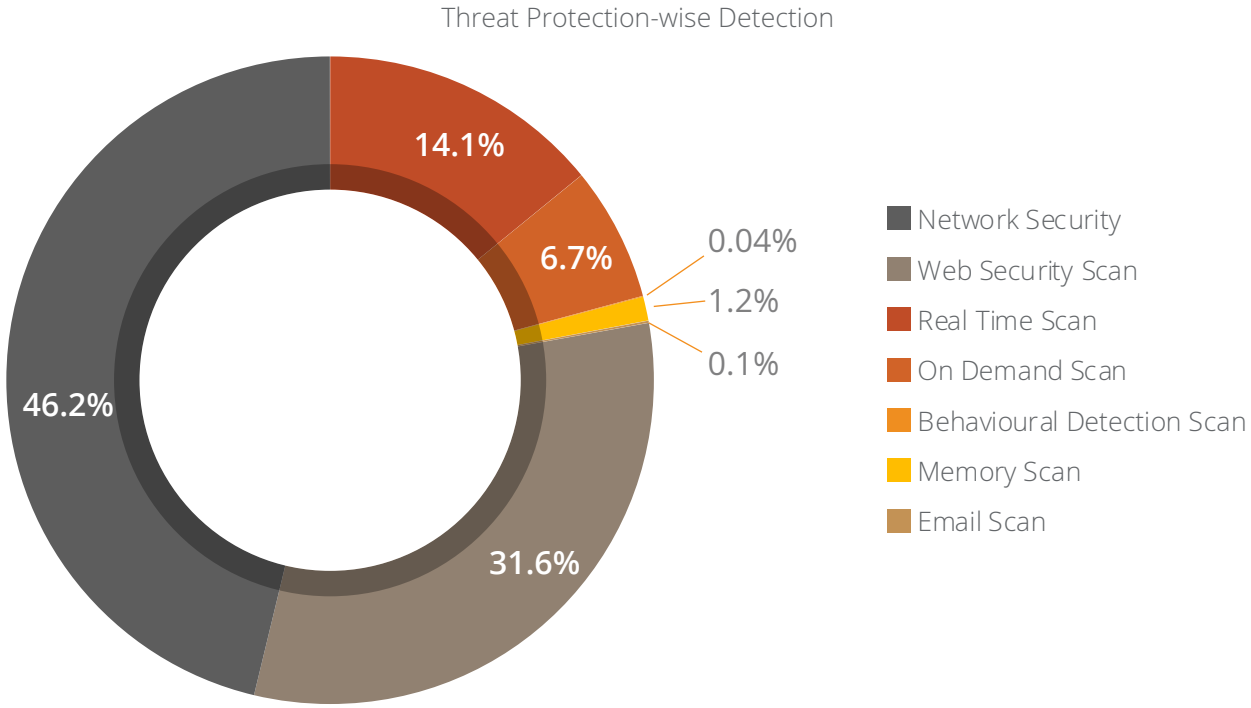
Observations

- Quick Heal detected over 125 Million Windows malware in Q2 2021. June 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.

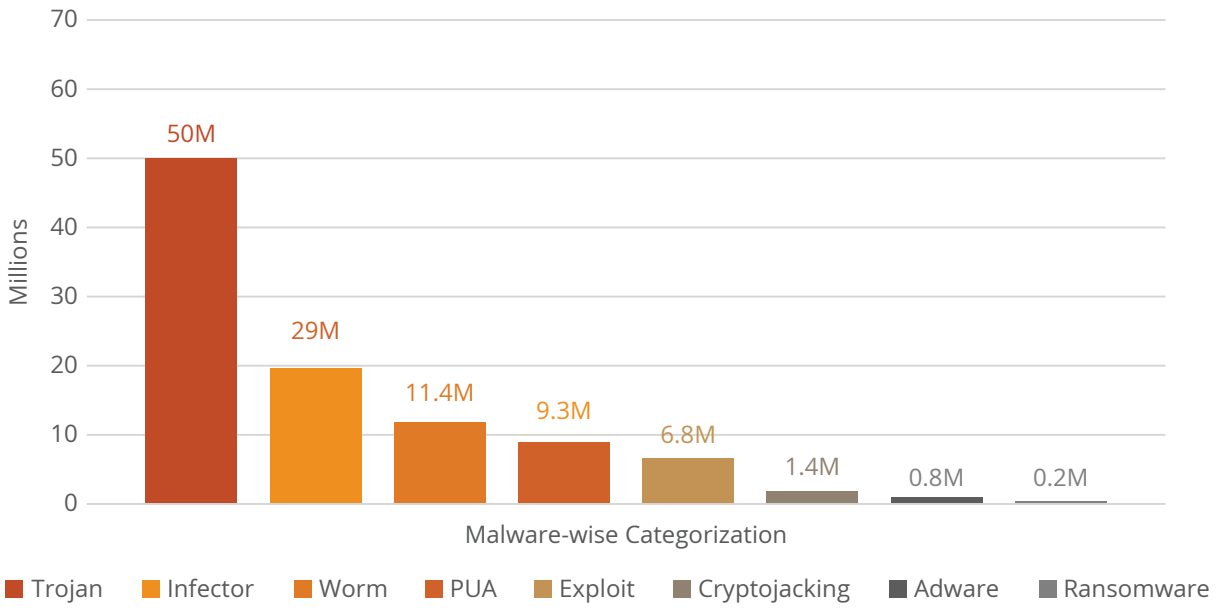
Web Security Scan
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

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

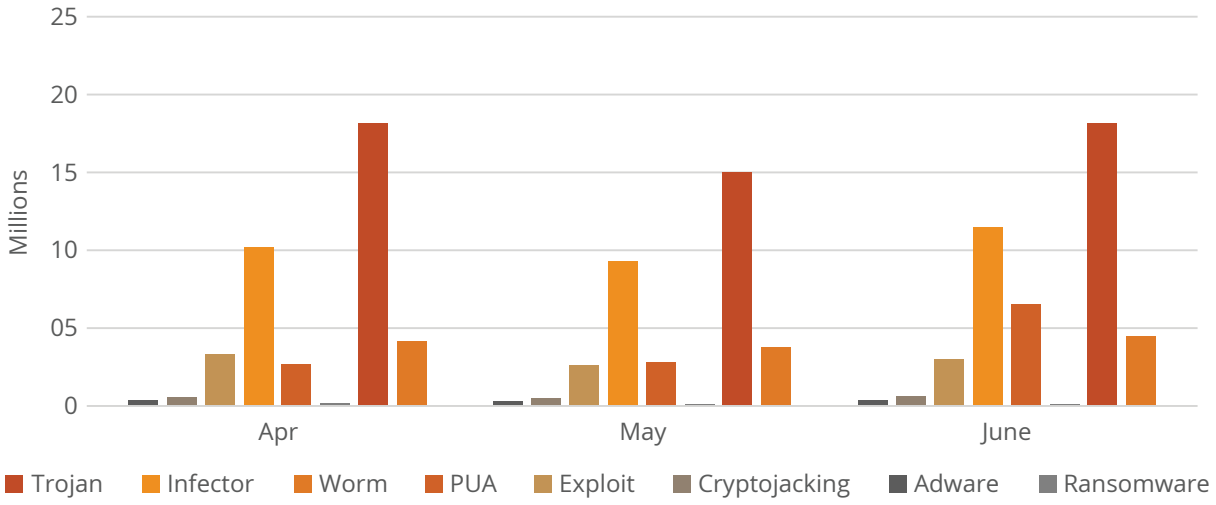
Detection Statistics - Category Wise

Categorization based on various Windows malware detected by Quick Heal in Q2 2021

A) Malware-wise Categorization



B) Month-wise Categorization



What Trojan Malware?

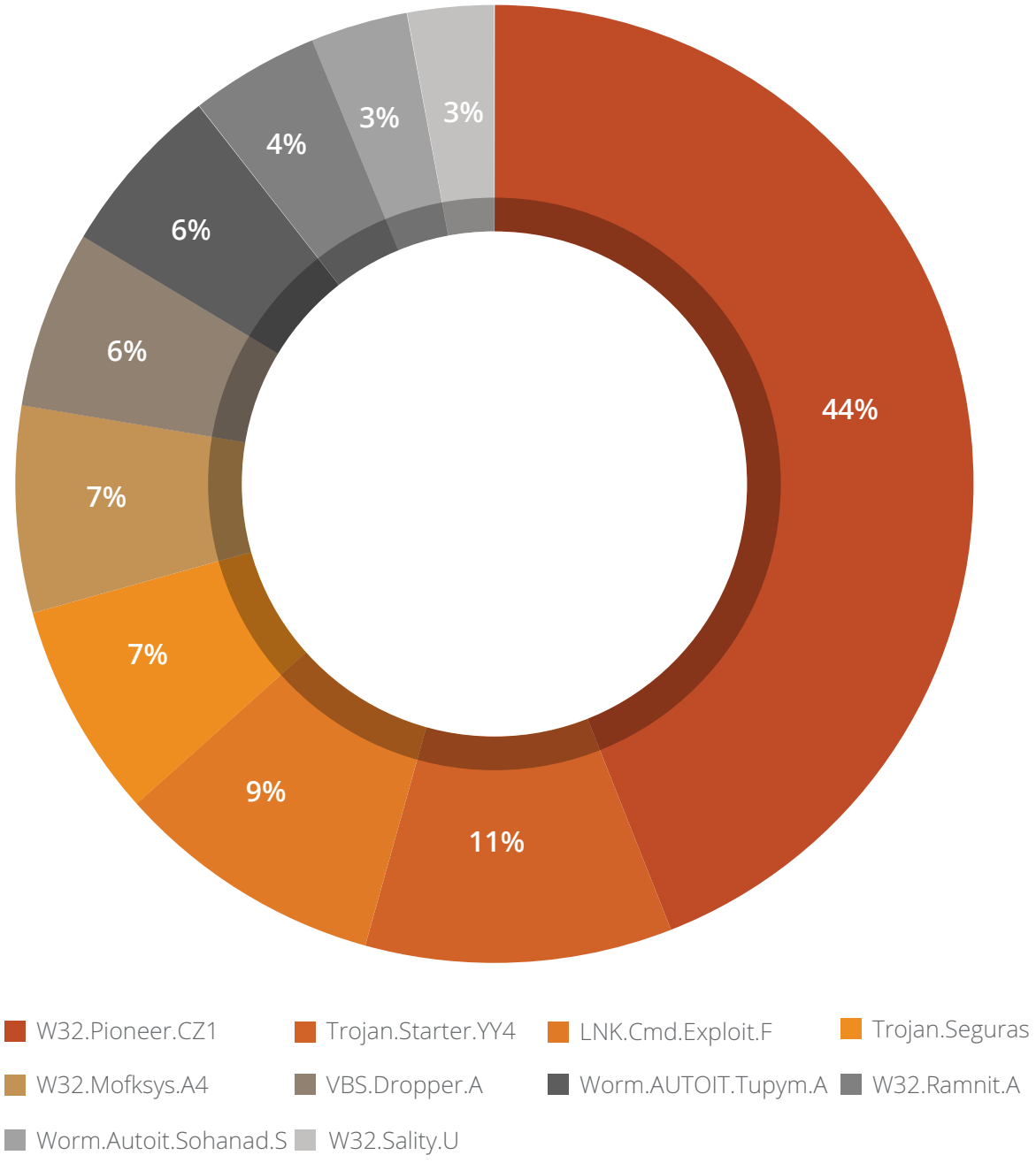
A Trojan horse or simply a Trojan is a malware that misleads users about its true intent. It disguises itself as legitimate software and fools the user to take an action.

Observation

- Trojan malware was found to clock the maximum detection with 17.7 Million in June 2021

Top 10 Windows Malware

The below figure represents the Top 10 Windows malware of Q2 2021.
These malware have made it to this list based upon their rate of detection from April to June.



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

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

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

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 embedded PE file.
- It drops that PE file to specific folder & launches that to perform malicious activity.

07

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.

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

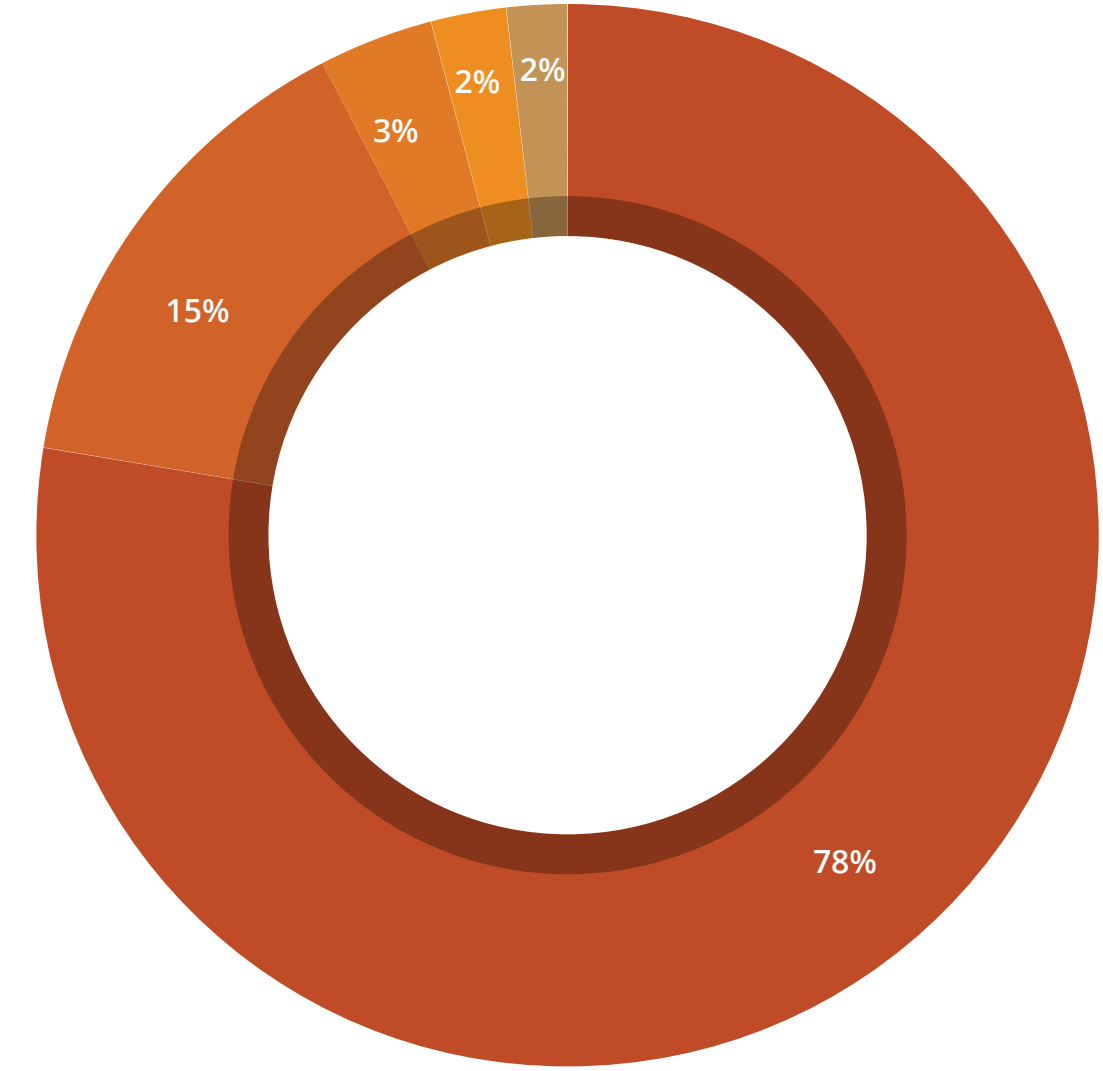
Behaviour:

- 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 Q2 2021.

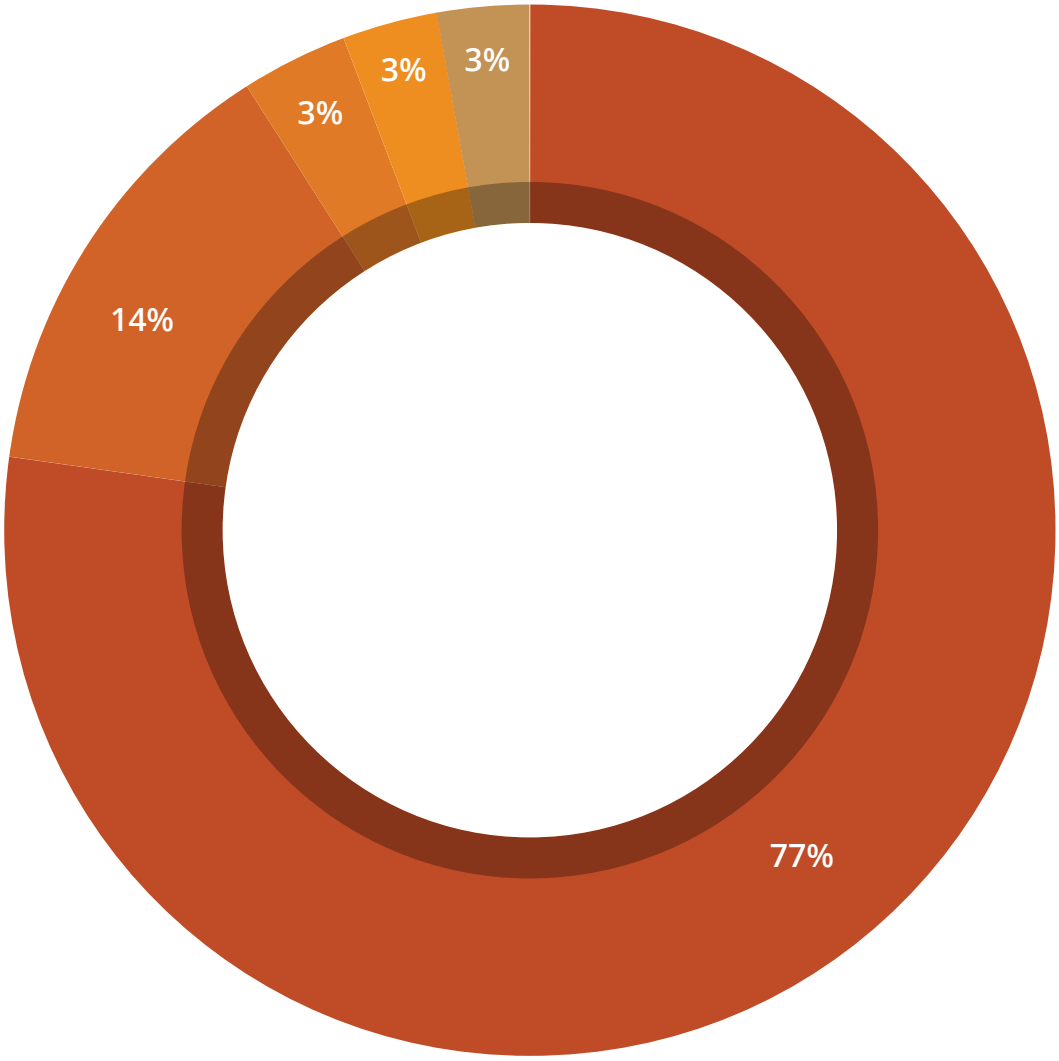


Observations

- 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?

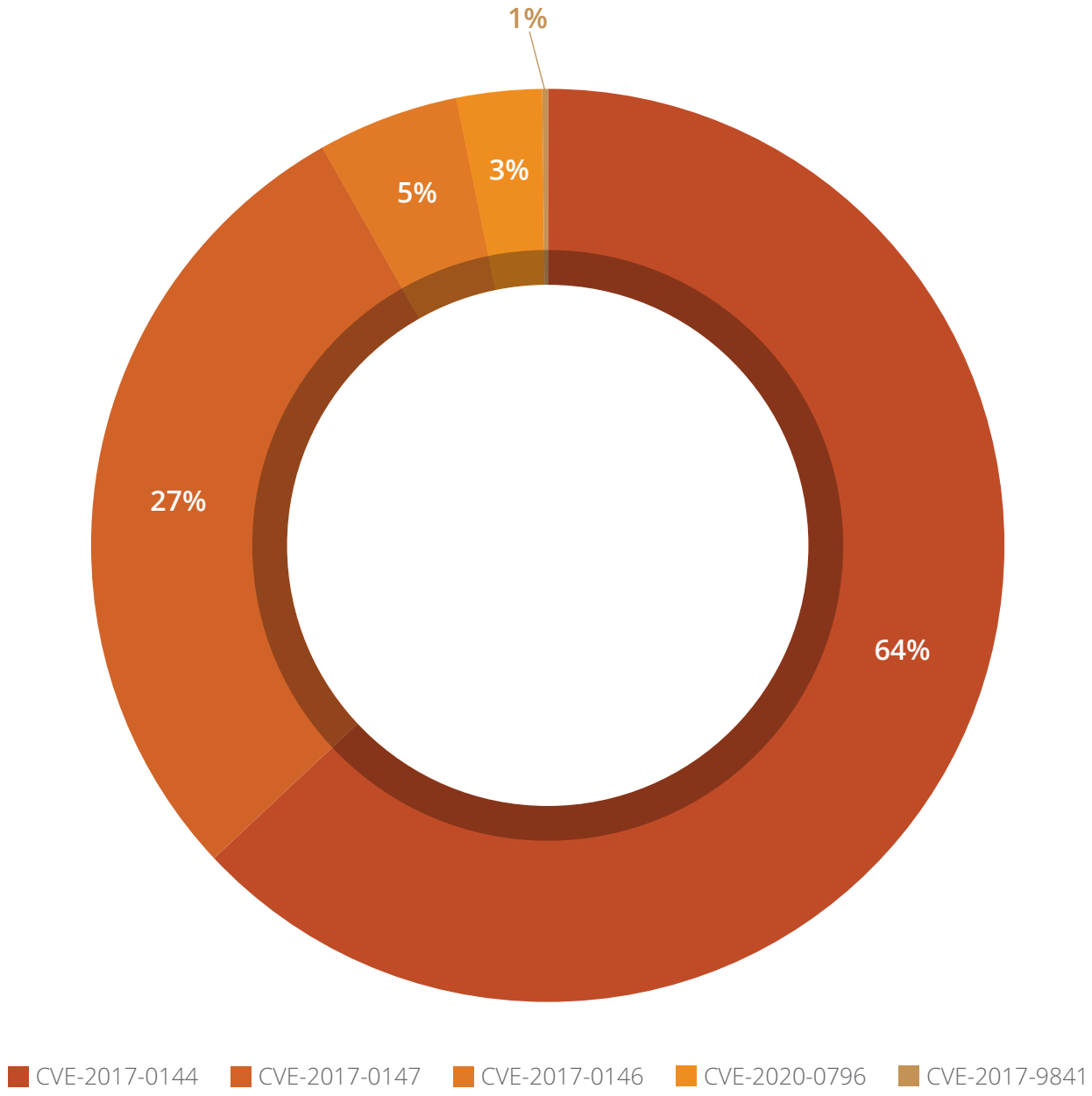
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Observations

- LNK.Exploit.Gen was detected to be the top host-based exploit, with 1.7 Million detections.

Top 5 Network-Based Exploits

Below figure represents the top 10 Network-Based Windows exploits of Q2 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

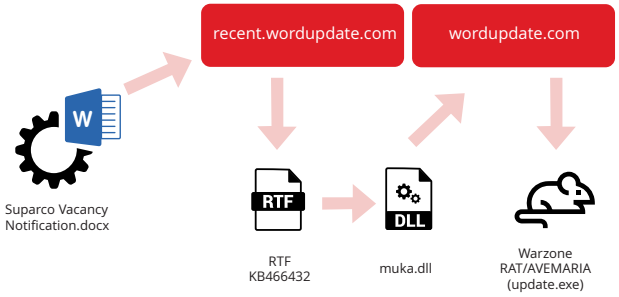
- CVE-2017-0144 was detected to be the top network-based exploit, with 62 Million detections.

Trends in Windows Security Threats

01 Warzone RAT – Data Stealing Trojan Malware Triggering from Office Documents

Warzone RAT is a part of an APT campaign named "Confucius" that targets government sectors of China and few other South Asian countries for credential stealing and keystrokes logging. It is known for its aggressive use of ".docx" files as its initial infection vector. This RAT performs various functionalities like Privilege Escalation - UAC Bypass, Remote Shell, Persistence and works as an info stealer malware.

The infection chain starts with sending malicious .docx files to the targeted organizations or persons, connects with C2, and exploits popular old vulnerability CVE-2017-11882. Further, it drops malicious .dll and connects with C2 again to deliver the final payload of Warzone RAT in the form of .exe. Attackers typically spread such malware through document files as an email attachment.



02 FickerStealer: A New Rust Player in the Market

Ficker Stealer is a family of information-stealing malware with various capabilities, including stealing sensitive information such as web browser passwords, cryptocurrency wallets, FTP client information, credentials stored by Windows Credential Manager, and session information from various chat and email clients. It is different from other stealers as it does not write the stolen data in any file. Instead, it sends the data to the server after each stealing operation.

This malware uses different techniques to get into the victim's computer, like malicious email attachments, malicious online advertisements, social engineering, etc. The infection process starts when Illegal activation tools ("cracks") are downloaded/installed instead of activating the licensed product. Malicious document downloaded as a file attachment that contains macros to run the malware in the system. In this quarter, Quick Heal Security Labs have seen that Hancitor malware delivers Ficker Stealer.

03 **FormBook Malware – A new variant delivered in phishing campaign**

Quick Heal Lab has observed a new variant of formbook malware using steganography to evade detection. But this specific variant uses the stenography technique in 2 stages. Both are loaders of other modules which are loaded in memory to avoid detections. The final payload is then self-injected. This variant is still in its development phase. So, we can expect an increase in formbook malware soon.

04 **Malicious DLL sideloading to execute the ransomware code**

Recently Quick Heal Security Lab has observed many malware scenarios that are using DLL sideloading. Sideloading takes advantage of the search order used by the loader, keeping the abused file and malicious DLL together. Malware authors are abusing genuine files by packing them with a spoofed malicious DLL. Dropping and executing genuine .exe will not raise any alarm, which can lead to persistence and evasion. If the victim's .exe has higher privilege, it can gain more access to the machine. One such case was seen in a recent REvil ransomware attack using Microsoft's MsMpEng.exe to load spoofed malicious MpSvc.dll.

05 **Nitro Ransomware asks for gift cards as ransom**

Nitro Ransomware is a new ransomware attack where hackers demand discord Nitro gift code from victims to decrypt their files. It has been distributed as a fake free Nitro gift code generator. Upon executing the ransomware, it encrypts the victim's file and gives them 3 hours to provide a valid discord Nitro.

The malware appends the ".givemenitro" extension to the filenames of the encrypted files. At the end of an encryption process, Nitro ransomware changes the wallpaper to an evil discord logo. The Nitro Ransomware performs other malicious activity on an infected device, such as stealing discord authentication tokens that are stored in the form of *.ldb files stored under "Local Storage\leveldb. The use of discord may evolve in the future.

06 **Phishing scam alert "domain name expiration"**

Quick Heal has observed an ongoing phishing attack named 'Domain Name Expiration Scam.' The goal of this scam is to trick targeted people with fake Domain Name Expiration mails to steal sensitive information & money via online payment. The victims receive multiple phishing emails on their registered mail from different Mail IDs. In such emails, the attackers mention "Domain Services Expiration Date" with fake Domain services expiration notices to the targeted users.

The mail also contains shorten bit.ly URL, which redirects the user to a phishing site and where attackers are asked to the user about sensitive information like email ID, Phone Number, and Digital signature, etc., to renew the domain plan. Once the targeted user fills & submits all the details, it will be redirected to the PayPal payment page to continue its Domain name plan. The scam would be successfully executed if the victim pays the amount.

56%
of total Android detection in Q2 2021 was Malware

ANDROID

Android malware detections for Q2 2021

1

Malware: 36,585
Per Day: 402
Per Hour: 17
Per Min.: 1

2

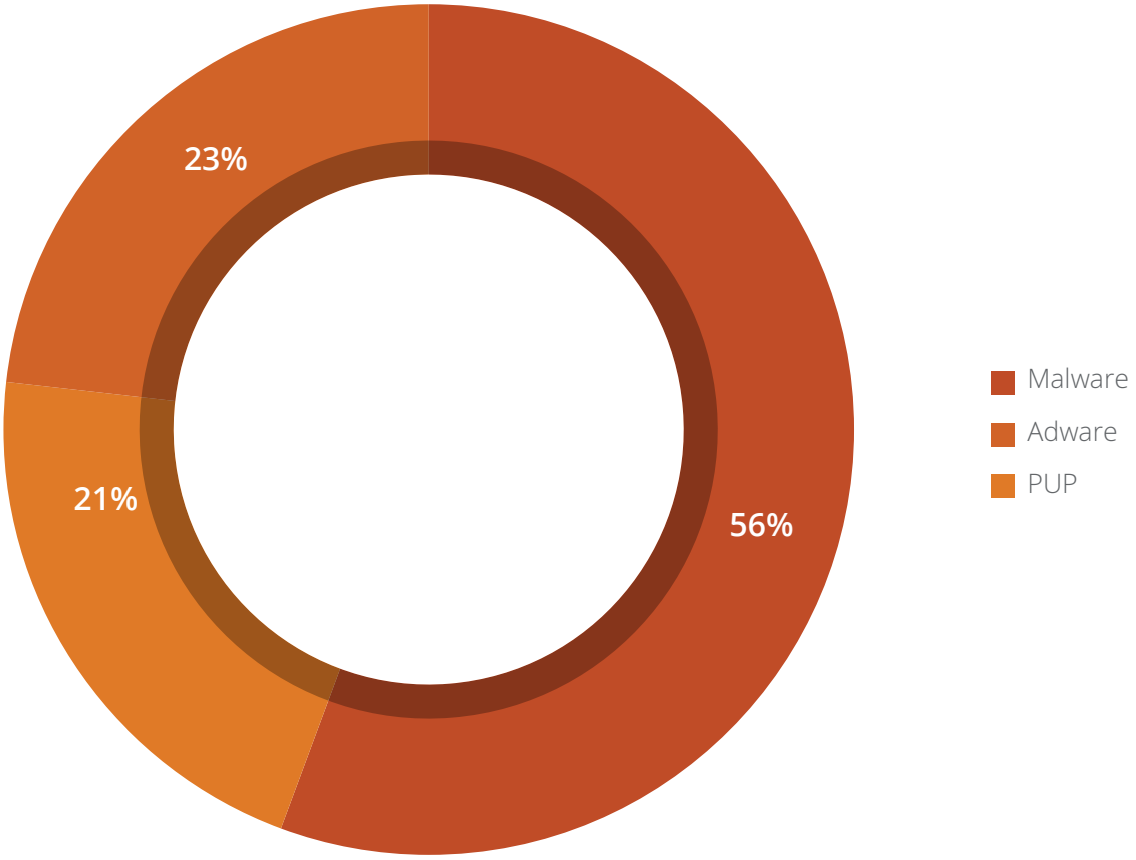
Adware: 13,553
Per Day: 145
Per Hour: 6
Per Min.: 0.10

3

PUA: 15,336
Per Day: 169
Per Hour: 7
Per Min.: 0.12

Detection Statistics: Category Wise

Below figure represents the various categories of Android malware detected by Quick Heal in Q2 2021.

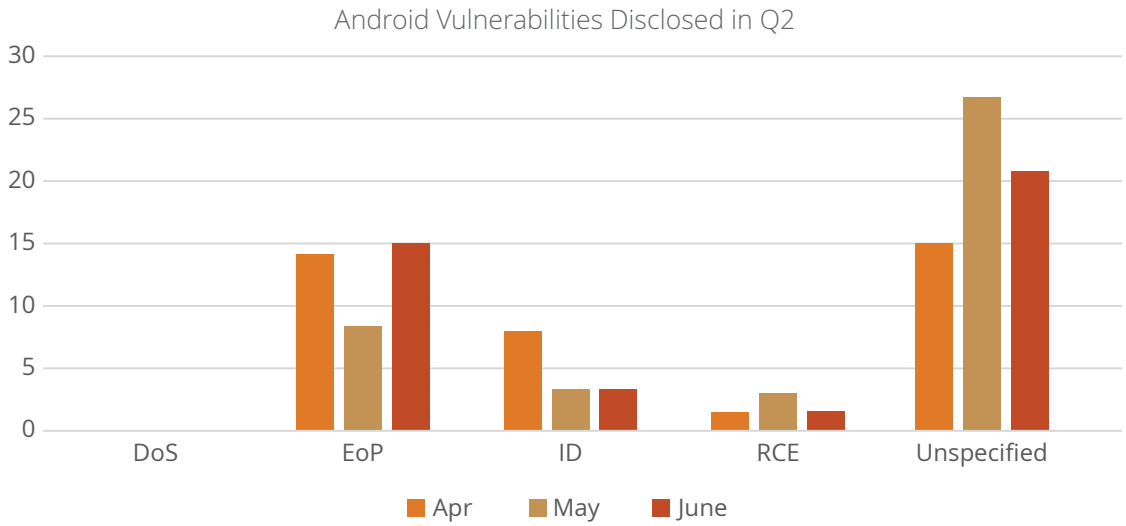


Observations

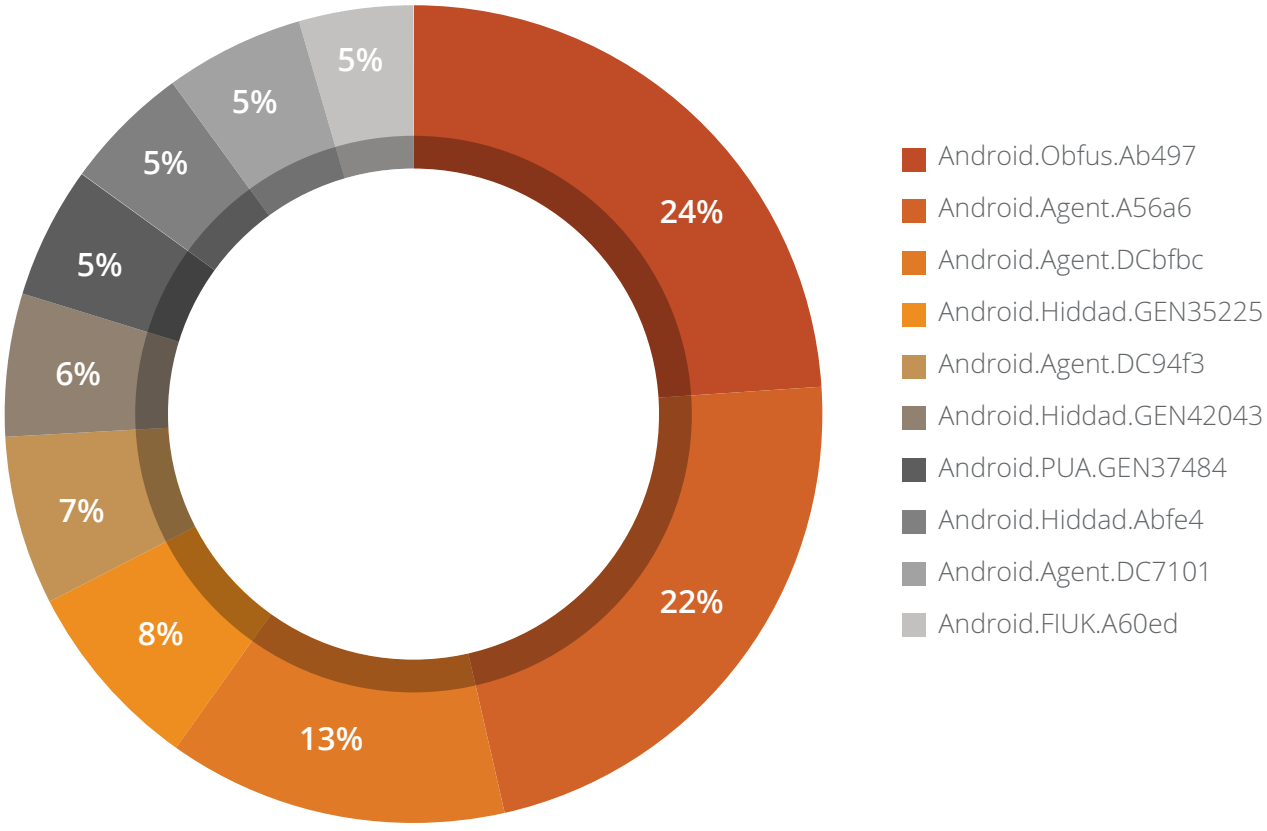
- Malware clocked 56% of the total Android detections in Q2 2021.

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 April to June 2021.



Top 10 Android Malware for Q2 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.A56a6
Threat Level: High
Category: Malware
Method of Propagation: Third-party app storest

Behaviour:

- This malware decrypts files from assets and creates Android executable files from them.
- This file has code to download another Android executable file on the device.
- This malware may download adware, spyware, or Trojans and harm the user's device.

03

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

Behaviour:

- After installation, it hides its icon and runs in the background.
- It collects device information, and further, it loads the payload.
- It shows a popup to activate the VPN service, and it starts displaying full screen ads while it is running.

04

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

Behaviour:

- It loads payload which contains different packages of advertisement.
- Further, it connects to advertisement URL, and shows the full screen ads.

05

Android.Agent.DC94f3
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.

06

Android.Hiddad.GEN42043
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It hides its icon on the first launch.
- Runs services in the background and shows Fullscreen 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.PUA.GEN37484
Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores and protector plug-ins

Behaviour:

- Developers use the 'Jiagu' Android app protector, commonly used to prevent apps from being tampered with 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.Hiddad.Abfe4
Threat Level: Medium
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- It uses string obfuscation to evade antivirus engines and to make reverse engineering difficult.
- Hides its icon after installation and displays advertisement
- Connects to advertisement URLs and sends the infected device's information to a remote server.

09

Android.Agent.DC7101
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

- This malware is from the dropper category.
- It drops malicious hidden Ad applications on users' phones.
- The dropped file hides its icon and shows pop-up ads after installation.
- It uses Chinese language strings and decrypts them to get malicious code at runtime.

10

Android.FIUK.A60ed
Threat Level: Medium
Category: Potentially Unwanted Application (PUA
Method of Propagation: Google Play Store

Behaviour:

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

Trends in Android Security Threats

01 Google Play store applications laced with Joker malware yet again

Quick Heal Security Labs spotted 8 Joker malware on the Google Play Store, which were removed after Quick Heal reported them. Joker is a spyware Trojan that steals data from the victim's device through SMS, contact lists, and device info. Then, it silently interacts with advertisement websites and subscribes the victim to premium services without their knowledge.

Malware authors had spread these malicious applications on the Google Play Store in scanner applications, wallpaper applications, message applications. These types of applications can quickly become a target. Quick Heal detects these apps with variants of "**Android.Joker.A"**

02 Fake Oximeter Apps Steal Banking Credentials

Recently, several applications were developed for easy management and tracking of COVID-19 cases. Quick Heal Security Labs have been tracking such applications to identify malware-laced apps misusing the official apps meant to ease the lives of people and authorities.

This quarter, we found fake oximeter apps imitating legitimate oximeter and vaccine registration apps that took user's fingerprint data for Google Pay, PhonePe, Paytm, and more. It asks for contact and SMS permission to check oxygen saturation levels and send the link of another application to every contact in the system. This is hosted on some mega account which on download turns out to be a banking Trojan-banker. Quick Heal detects these apps with variants of "**Android.Anubis.GEN30551**."

03 Hackers target users with fake COVID-19 vaccine registration app

COVID-19 vaccination drive had recently started across India for everyone above 18, but consumers were facing problems booking a slot due to vaccine shortage. To ease the process, several developers came up with notify-me websites that can tell the availability of the slots. However, the user still needs to use the official registration platform CoWIN API to complete the formalities.

Hackers took advantage of the situation with malicious elements. A fake SMS was in circulation, tricking users for vaccine registration via an app. The SMS primarily was a malicious link filled with Android Worm that reaches users via message app, asking them to register with the 'Vaccine Registration' app. Once the user downloads the app, it requests permission to access all the contacts and messages. The worm then uses the references listed in the infected Android device to spread to other devices via text messages. Quick Heal detects these apps with variants of "**Android.GoodNews.GEN41898**"

04 Android malware spreading through social media applications

Autoreply is a convenient feature through which users can send a custom message as an automatic reply for unanswered emails, SMS, WhatsApp messages, and more. There are many applications on Google Play Store which offer such functionality. We have recently noticed malicious applications which are abusing this functionality.

In many cases, these messages come from a trusted contact (who is already infected). As a result, users are likely to consider the message legitimate and follow the mentioned steps. The message then asks users to open a web link and download an application. The website displays lucrative offers such as Free Netflix, watch Free IPL, or Download New feature in WhatsApp like WhatsApp pink to lure users further. Quick Heal detects these apps with variants of "**Android.SpamsCAD.A**"

Inference

In yet another year filled with restrictions and lockdowns, cybercriminals were not deterred as nearly 125 Million malware were detected. In a recent Microsoft Research Report, India has been ranked #1 amongst 16 countries for tech support scams affecting 7 out of 10 consumers.

Phishing campaigns and ransomware attacks also remain the top threat to consumer safety, with top scams relating to vaccination, android apps laced with Joker malware, fake oximeter apps, gaming threats, and financial relief. All the cyber-attacks and scams were designed to trick consumers into sharing their passwords, personal and financial information in an attempt to steal money and data.

With relaxation on lockdown across the country, we can expect cybercriminals to tap into the gradual shift as people start to return to work, travel, and engage in social activities. Despite many consumers saying they are taking all the online precautions required online, they feel more vulnerable to cybercrimes than before the pandemic, and half aren't sure how to protect themselves.

With 2,426 ransomware detected per day in this quarter, too, it is advisable to proactively back up all your sensitive data in a separate storage device. Switch to a more vigorous and robust antivirus with advanced features that can put up an intense fight against both evolving and new malware types. Most importantly, be aware of what you are doing and sharing on the internet unless you are sure about it.

Quick Heal

Security Simplified

Quick Heal Technologies Limited
Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India
Phone: +91 20 66813232 | Email: info@quickheal.com | Website: www.quickheal.com