



Quick Heal

Security Simplified

QUICK HEAL **ANNUAL THREAT REPORT** 2022



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	01
WINDOWS	02
- Annual Windows Detection Statistics	03
- Detection Statistics – Month Wise	04
- Detection Statistics – Per Quarter	05
- Detection Statistics – Per Quarter Year-over-Year	05
- Per Quarter Detection Statistics – Category-wise	06
- Year-over-Year Detection Statistics – Category-wise	06
- Detection Statistics – Protection-wise	07
- Indian States Most At Risk in 2021	09
- Indian Cities Most At Risk in 2021	09
- Top 10 Windows Malware in 2021	10
- Top 10 Potentially Unwanted Applications (PUA) and Adware	13
- Top 5 Host-Based Exploits	14
- Top 5 Network-Based Exploits	15
- Annual Round-up of Windows Security Threat Trends in 2021	16
ANDROID	24
- Annual Android Detection Statistics	25
- Per Quarter Detection Statistics: Category-wise	26
- Android Vulnerabilities Discovered in 2021	26
- 2021 Top 10 Android Malware	27
- Annual Round-up of Android Security Threat Trends	30
INFERENCE	33

FOREWORD

Get ready for more phishing attacks, more scammers, and a more significant need for digital security in 2022. It is likely that cyber breadcrumbs from some of the last year's most notorious cyber-attacks would result in a rise in attacks in the new year.

Malware continues to be a significant problem worldwide, and the ever evolving nature of the attacks makes the problem even more challenging. Quick Heal Security Lab researchers have prepared a forecast and detailed analysis of the threats per quarter in 2021, outlining how the threat landscape will change in 2022.

The return of low-level attacks, an inflow of new APT actors, increase in phishing & ransomware attacks, wider use of zero-day exploits, and growth of supply chain attacks, are some of the predictions outlined by the researchers.

Read on to learn about the threat landscape in 2021 and how Cyber Attacks continue to evolve.





WINDOWS



507
Million
Windows
Malware
detected
in 2021



June
saw the highest
Windows
Malware attacks
with **56.5** Million
detections



Trojan
was
the highest
detected
malware
in 2021

Annual Windows Detection Statistics

**Malware:****507** Million

Per Day: 1,387,842

Per Hour: 57,827

Per Minute: 964

Ransomware:**1.4** Million

Per Day: 3,801

Per Hour: 158

Per Minute: 3

Exploit:**39** Million

Per Day: 109,212

Per Hour: 4,551

Per Minute: 76

PUA & Adware:**50.5** Million

Per Day: 138,525

Per Hour: 5,772

Per Minute: 96

Cryptojacking:**9.8** Million

Per Day: 26,925

Per Hour: 1,122

Per Minute: 19

Infector:**126.7** Million

Per Day: 347,385

Per Hour: 14,474

Per Minute: 241

Worm:**54** Million

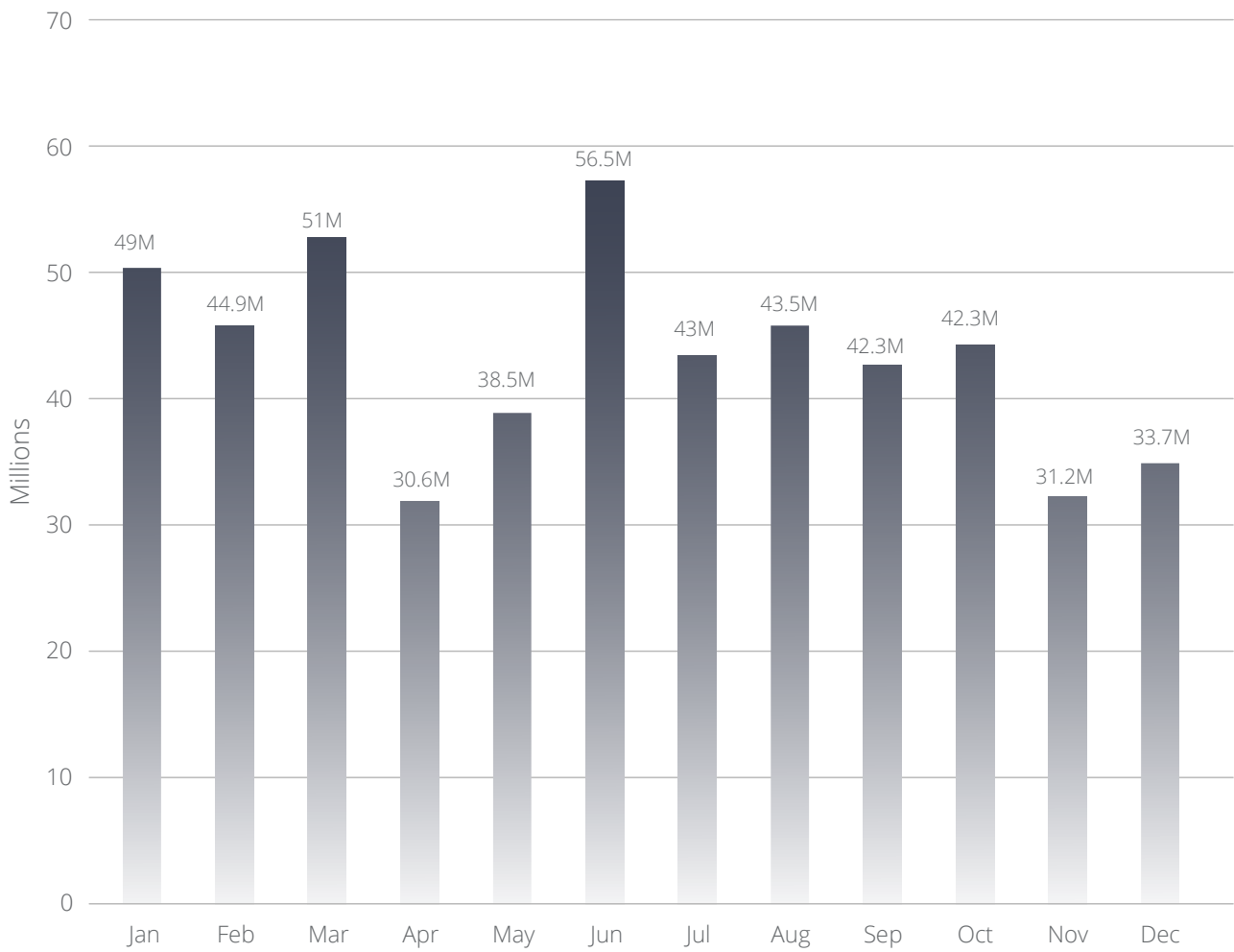
Per Day: 149,169

Per Hour: 6,215

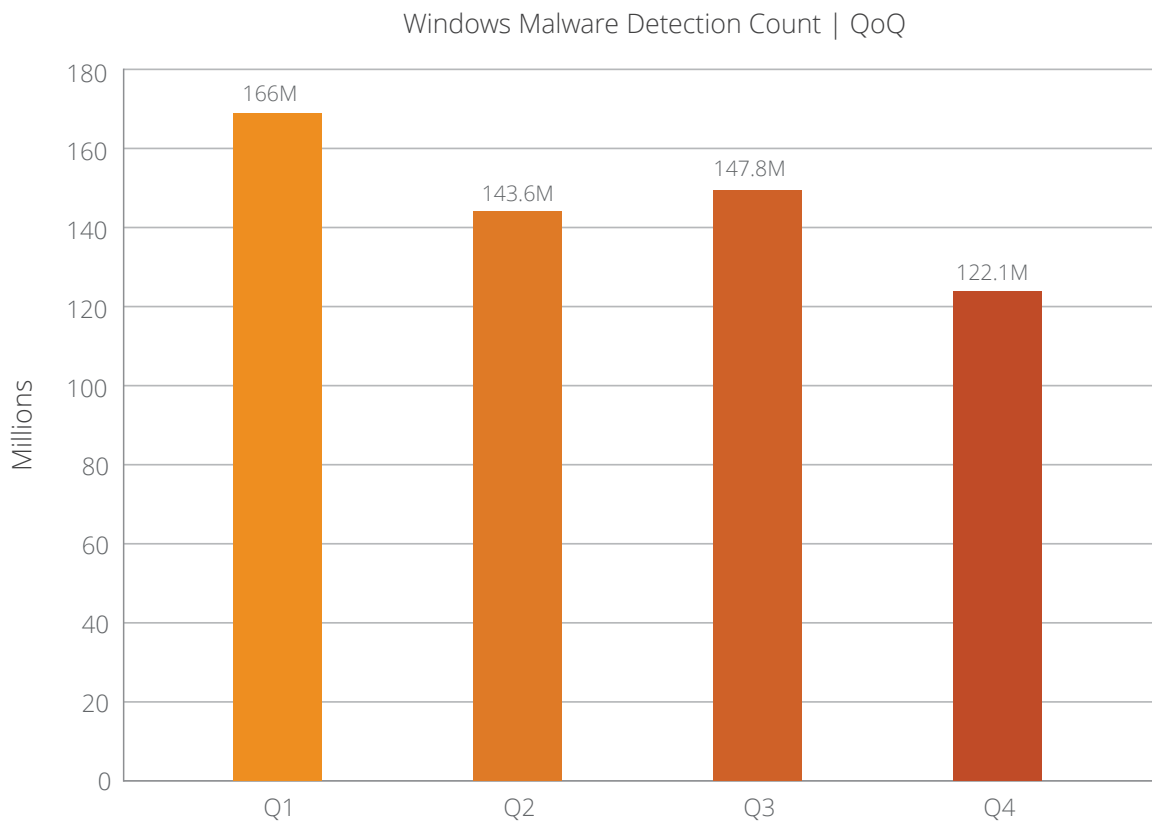
Per Minute: 104



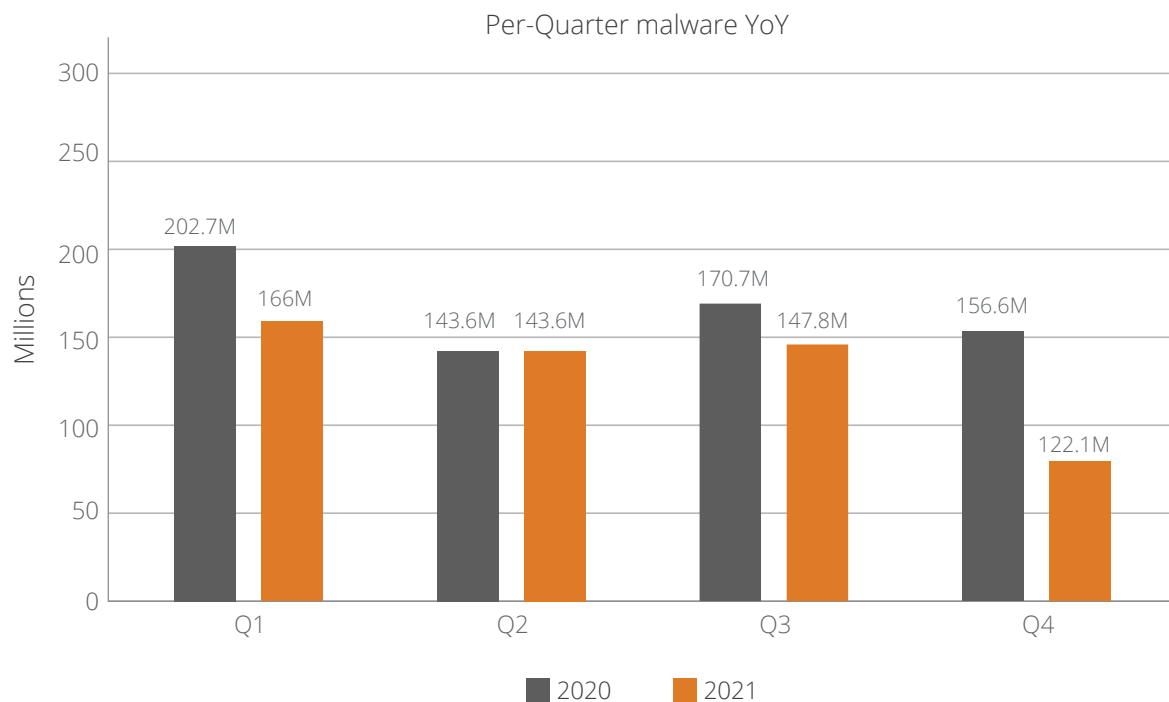
Annual Detection Statistics – Month Wise



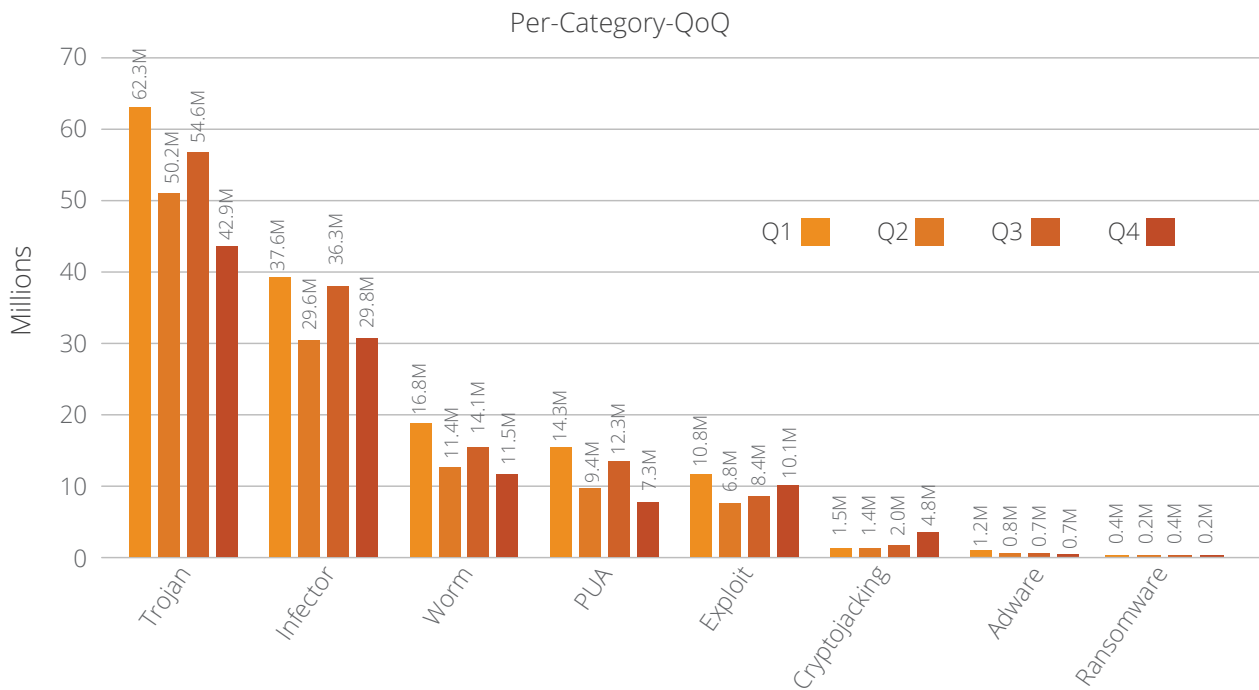
Detection Statistics – Per Quarter



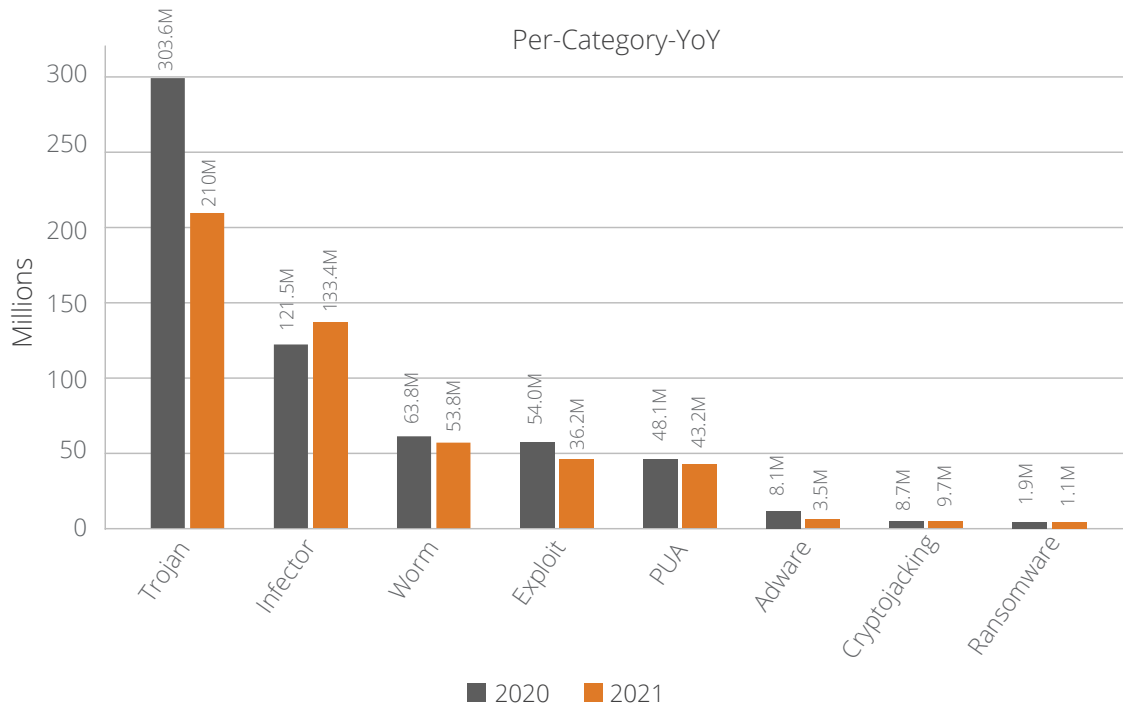
Detection Statistics – Per Quarter Year-over-Year



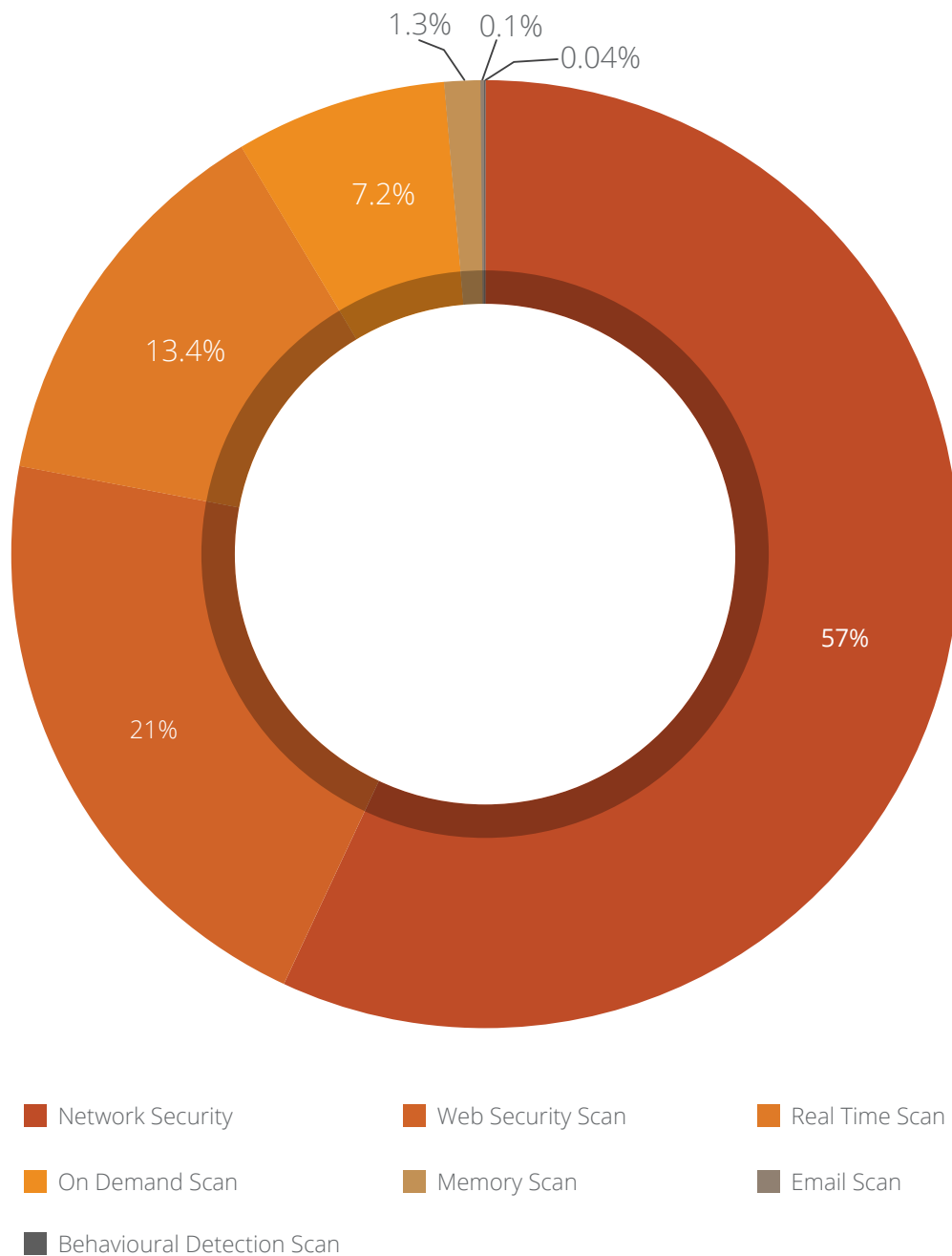
Per Quarter Detection Statistics – Category-wise



Year-over-Year Detection Statistics – Category-wise



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.

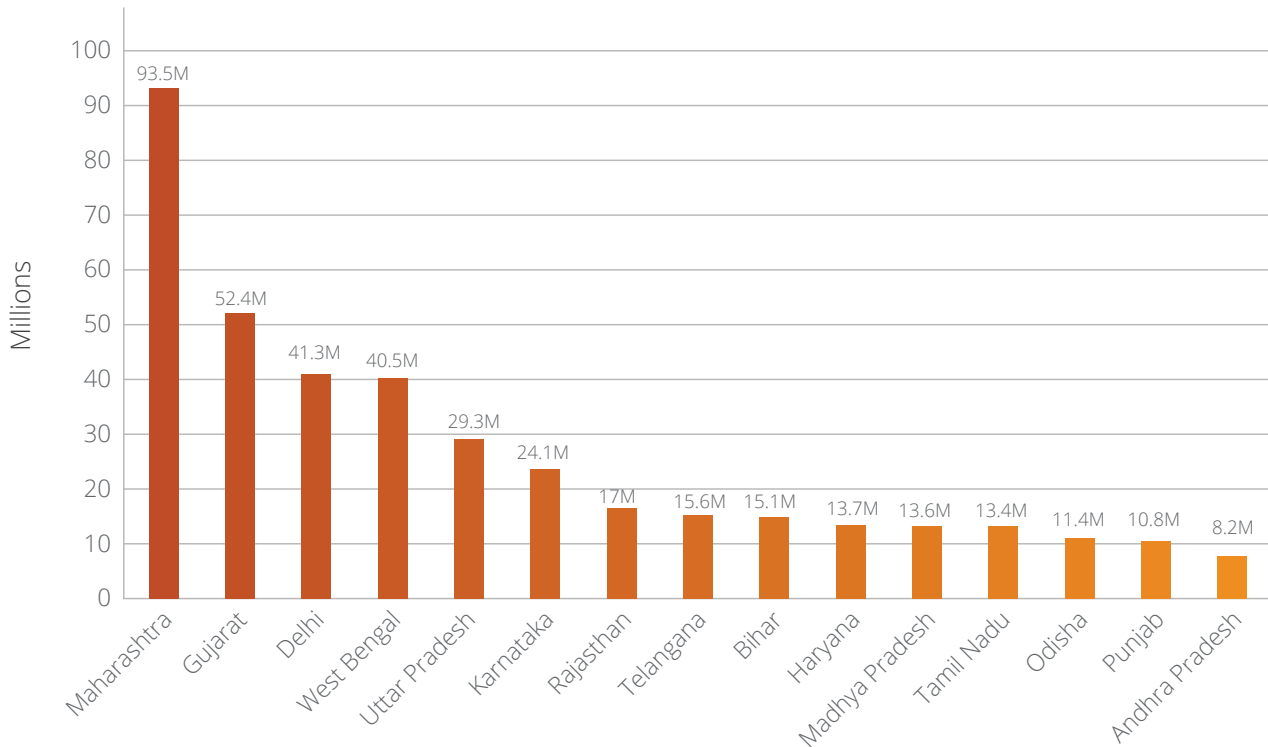


Network Scan

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

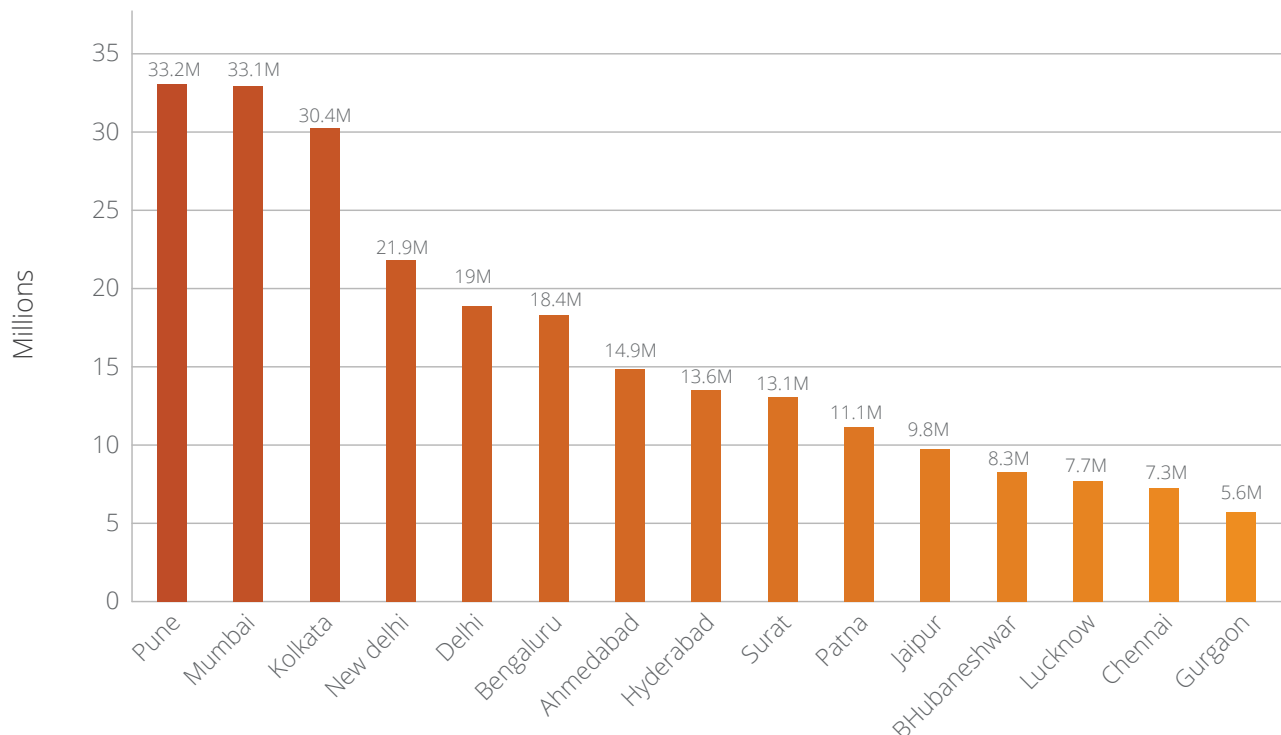
The Indian States Most at Risk in 2021

The below chart represents the top 15 Indian states affected by malware.



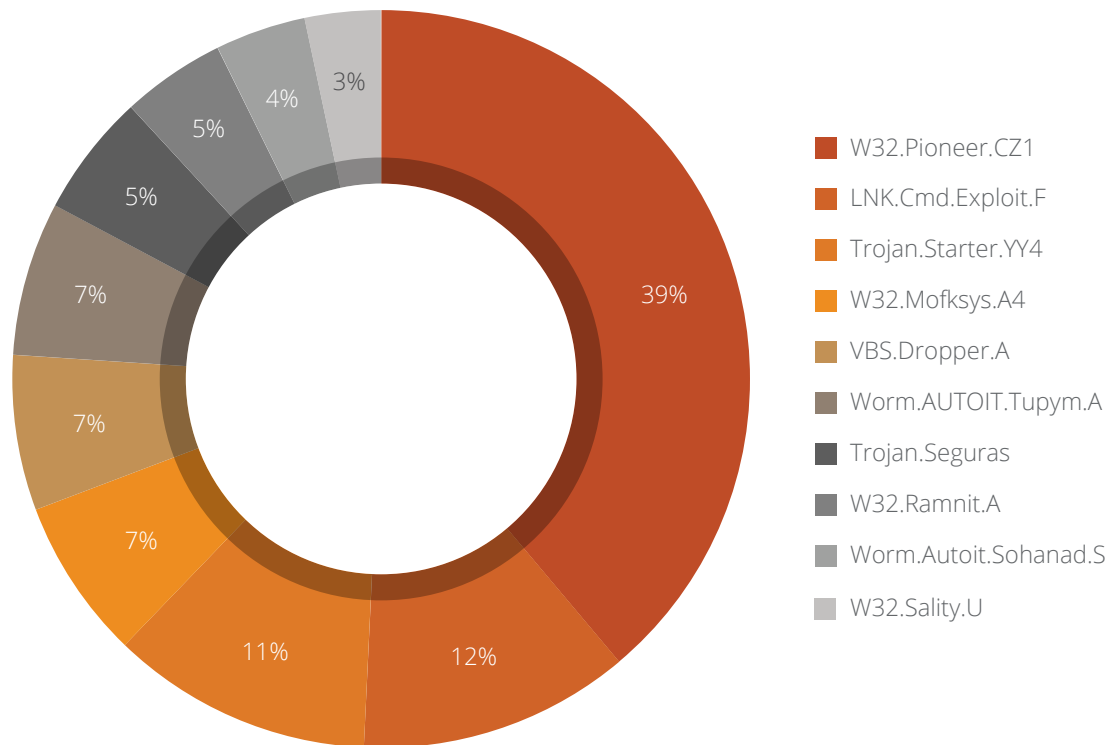
The Indian Cities Most at Risk in 2021

The below chart represents the top 15 Indian cities affected by malware



Top 10 Windows Malware in 2021

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



Top 10 Windows Malware Details

01

W32.Pioneer.CZ1

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behavior:

- 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

Behavior:

- 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

Behavior:

- 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

Behavior:

- 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

Behavior:

- 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

Behavior:

- 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

Behavior:

- It often shows fake scan results and lure 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

Behavior:

- 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 ensures modifies registry entries.

09

Worm.Autoit.Sohanad

Threat Level: Medium

Category: Worm

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

Behavior:

- 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

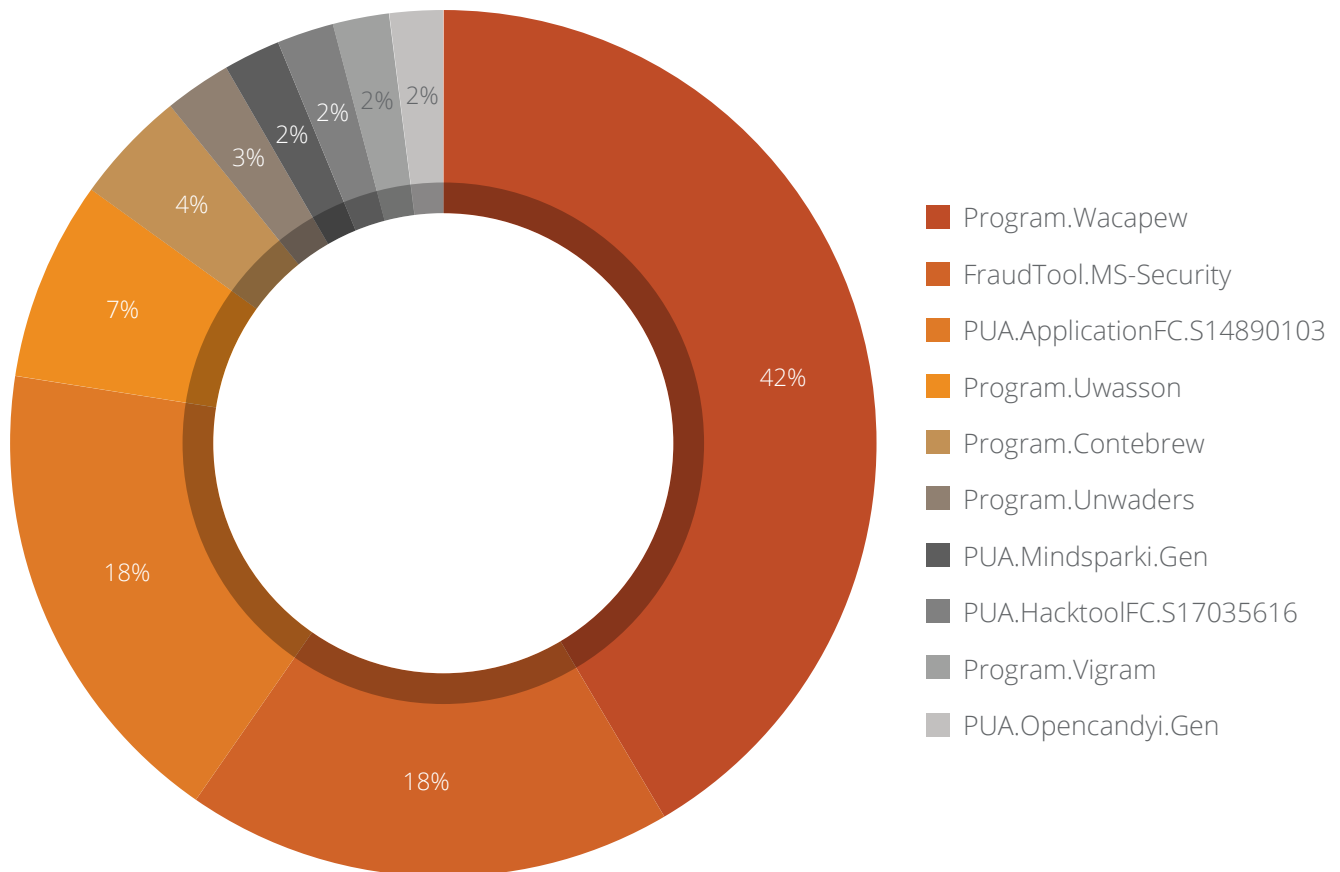
Behavior:

- 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 10 Potentially Unwanted Applications (PUA) and Adware

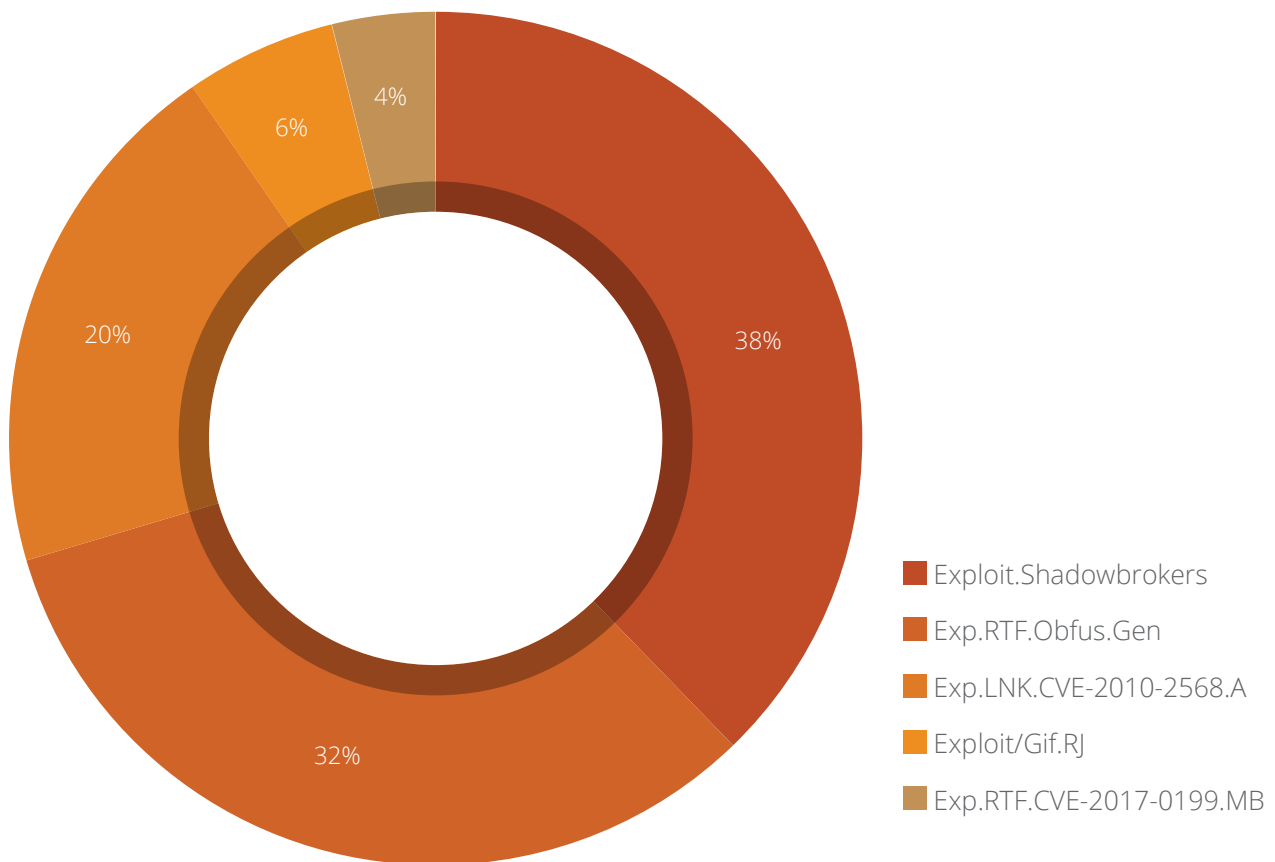
Potentially Unwanted Applications (PUA) and Adware programs are not necessarily harmful but using them might lead to security risks. Adware are software used to display ads to users; some are legitimate while some are used to drop spyware that steals user information.

Below figure represents the top 5 PUAs and Adware detected by Quick Heal in 2021.



Top 5 Host-Based Exploits

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

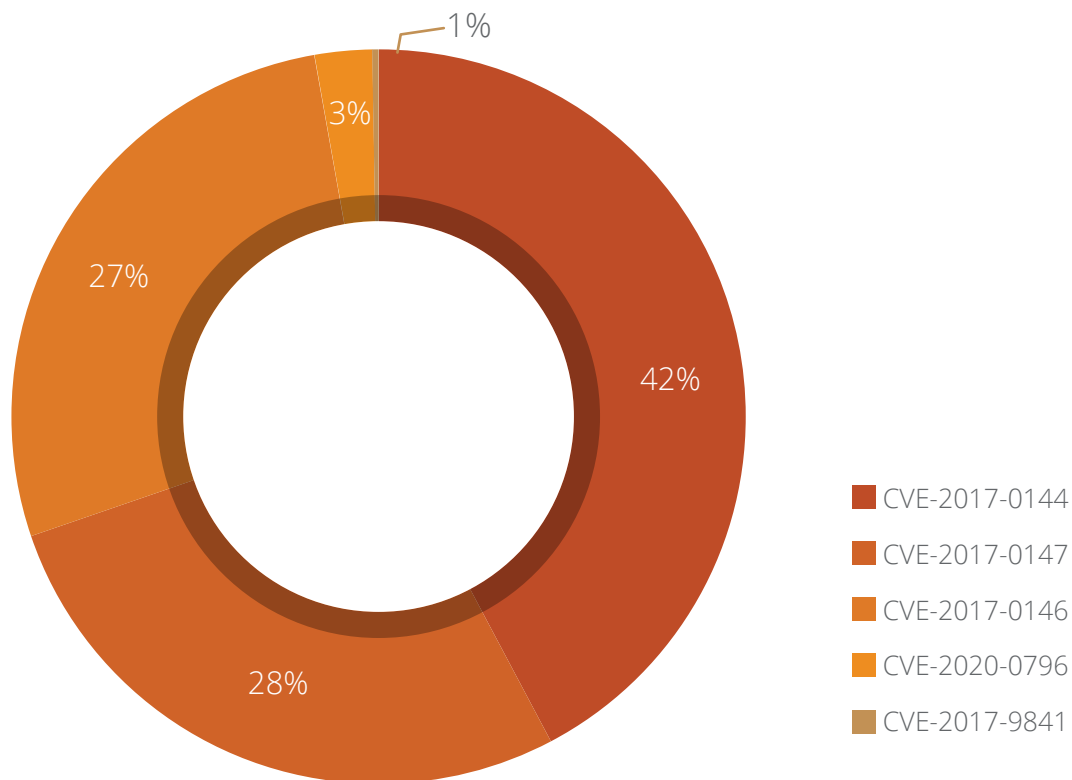


What are host-based exploits?

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

Top 5 Network-Based Exploits

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



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



CVE-2017-0147

Microsoft Windows SMB Information Disclosure Vulnerability

An attacker who successfully exploited this vulnerability could craft a special packet, which could lead to information disclosure from the server.



CVE-2017-0146

Windows SMB Remote Code Execution Vulnerability

An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server.



CVE-2020-0796

Windows SMBv3 Client/Server Remote Code Execution Vulnerability

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests



CVE-2017-9841

Code injection vulnerability in PHPUnit

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

Annual Round-up of Windows Security Threat Trends in 2021

01

First Dlang-based ransomware: Vovalex

Recently, Quick Heal Labs came across new a ransomware called Vovalex which is being distributed through pirated software disguised as popular Windows utilities, such as WinRAR, CCleaner, and uTorrent installers. The ransomware encrypts the device files and then drops a ransom note demanding payment in some form. Vovalex might be the primary ransomware written in D language, and it uses a single symmetric key to decrypt files. It is expected that ransomware will evolve and advance its encryption mechanisms.

02

Attack on Indian vaccine makers & Power Grid

A Chinese state-backed hacking group APT10 has been targeting the systems of Indian vaccine manufacturers, Bharat Biotech and Serum Institute (SII). Hackers have identified certain gaps in the IT infrastructure and supply chain software of these companies. The real motive was exfiltrating intellectual property and getting a competitive edge over Indian pharmaceutical companies. This is not the first time that Chinese hackers have targeted India. Last year, they had an alleged role in attacking India's power grid which caused a blackout in Mumbai.

03

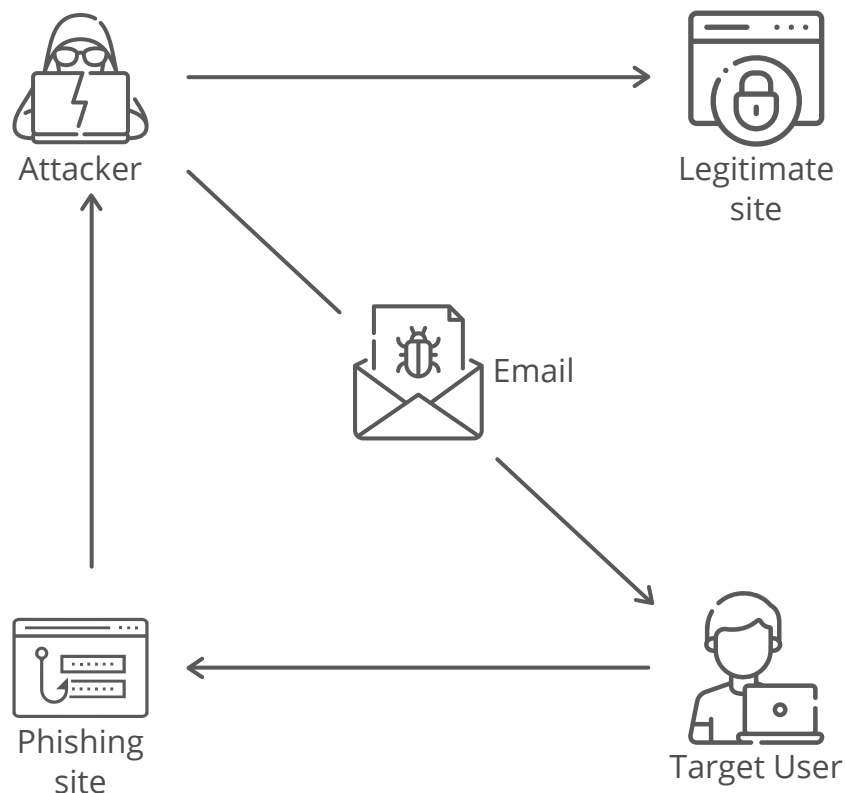
Discord becoming famous among malware authors

Cybercriminals step up efforts to target gamers on Discord – a popular app used to interact over voice calls, videos calls, or text messaging. It also allows users to set up servers or join pre-existing ones easily. Over 100 unique malicious malware are being served through Discord in zscaler cloud over the last two months alone. The attack usually starts with spam emails in which prospective marks are lured with legitimate-looking templates into downloading next-stage payloads. Another feature called Webhooks permits websites and external applications to send a message to the discord channel.

04

Spear Phishing targets Microsoft O365 users to gather credentials

There was a considerable amount of rise in Phishing Attacks during the COVID-19 pandemic. One such [Spear Phishing](#) Campaign targets high-profile individuals for credential harvesting. The analysed email links to a fake login page that resembles the victim's organization's Office 365 login. The fake phishing page looks exactly similar to the Microsoft Office login page. The redirected URL can target a substring in your organization to make users believe in the legitimacy of the website. The end goal of the attackers is to spoof the targeted victims to damage the organization's data and reputations, lead to scams, and steal critical information.

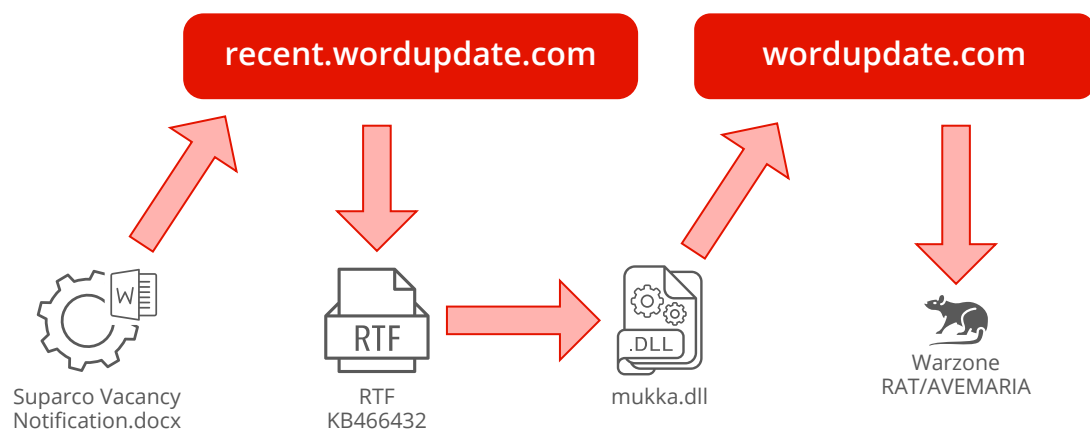


05

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.



06

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.

07

Side Loading Never Gets Outdated

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

08

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, while 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 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.

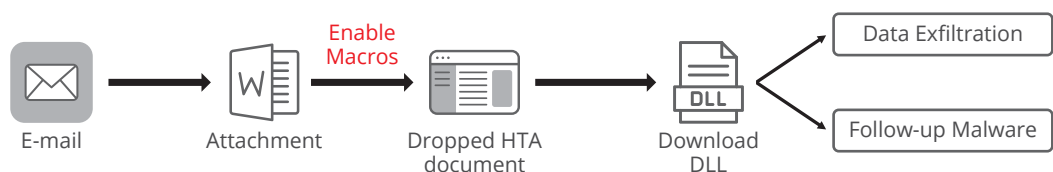
09

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:



10

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 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.

11


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 files.

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

Subj:- 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.


(Chandandeep Singh)
PO(MS)
Tele: 23016619

To

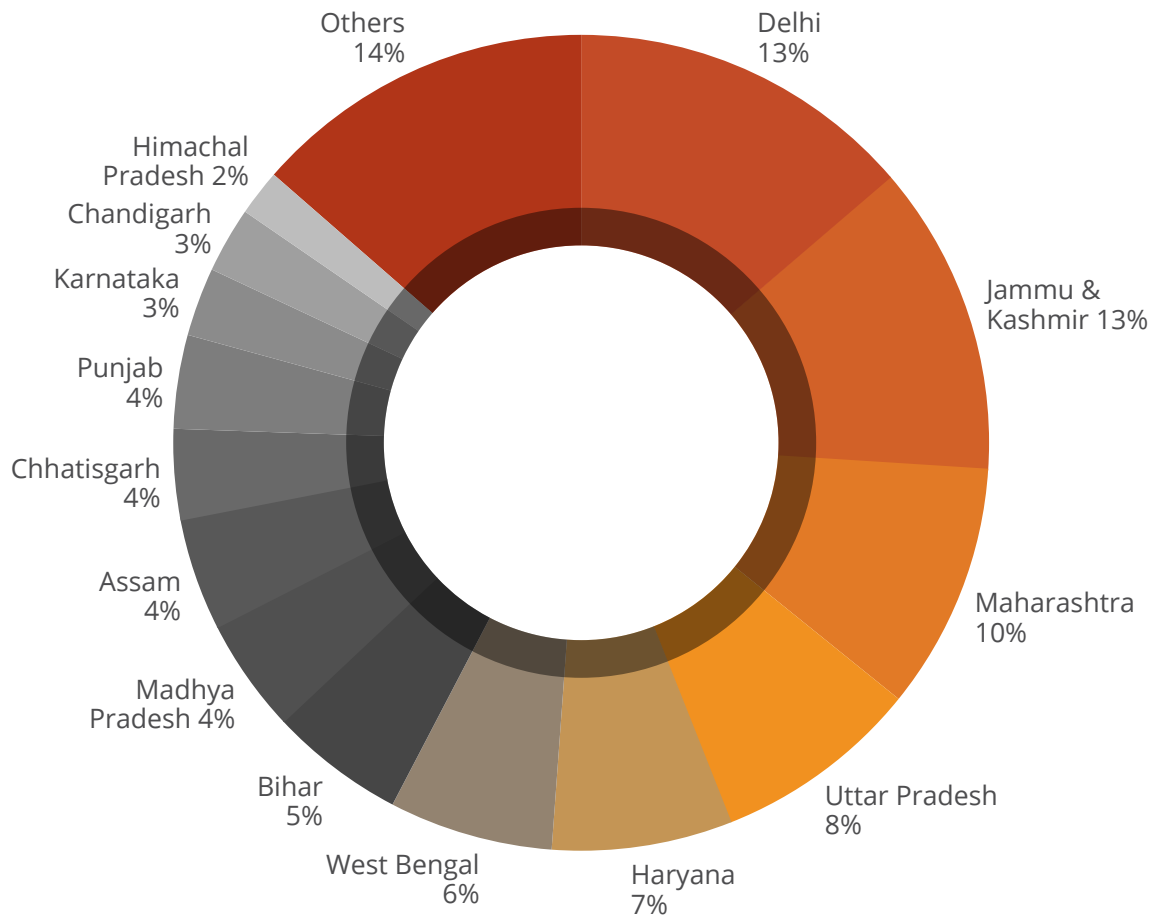
All the Members of Task Force

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

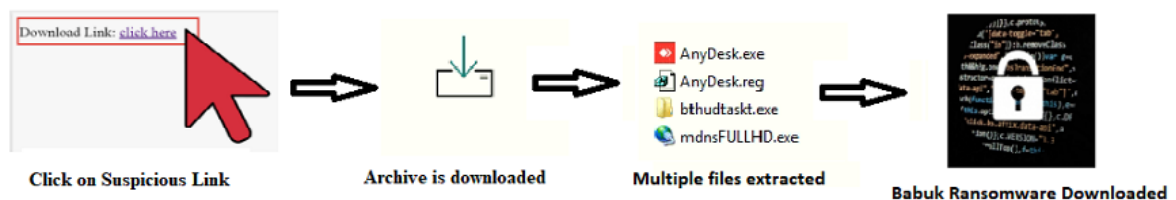


12

Anydesk software exploited to spread Babuk Ransomware

Ransomware attacks are deployed through exploits, unsolicited malicious emails (malspam), or malicious Microsoft Office documents. Attackers trick the unsuspecting users into enabling macros, etc. Apart from these usual attack techniques, we came across a new way of using Anydesk software fake websites to spread Babuk ransomware. Babuk Ransomware is recently very active. Its tactics for encryption are not much different from other ransomware families. Over time, ransomware releases new variants and improves its attack mechanisms to target new victims.

When the user tries to download the Anydesk software from an unknown suspicious link, a fake website appears, which allows you to download Anydesk software. This fake website looks like the original Anydesk website. When the user clicks for downloading Anydesk software, ransomware is also downloaded as it is bundled with Anydesk software in the form of a self-extracting archive.



When a user executes the downloaded archive, other files in the bundle get dropped silently, installing the Anydesk software. The above image shows an Allakore Rat client named bthudtask.exe, a Babuk downloader called mdnsFULLHD.exe, and one registry file named AnyDesk.reg is fallen in the Startup folder without user interaction. Clean Anydesk application is dropped at the desktop, and it gets installed. Babuk downloader downloads Babuk ransomware payload.

We believe that this type of infection affects a wide range of Anydesk users. Using tools like Anydesk or other administrative agencies, the malware authors can easily take administrative privileges of the victim's computer and perform malicious activity in the system.

ANDROID



0.12

Million Android
Malwares were
detected in 2021



Annual Android Malware Detections



Malware:
120,795

Per Day: 331
Per Hour: 14
Per Min.: 0.22



Adware:
50,580

Per Day: 139
Per Hour: 6
Per Min.: 0.09

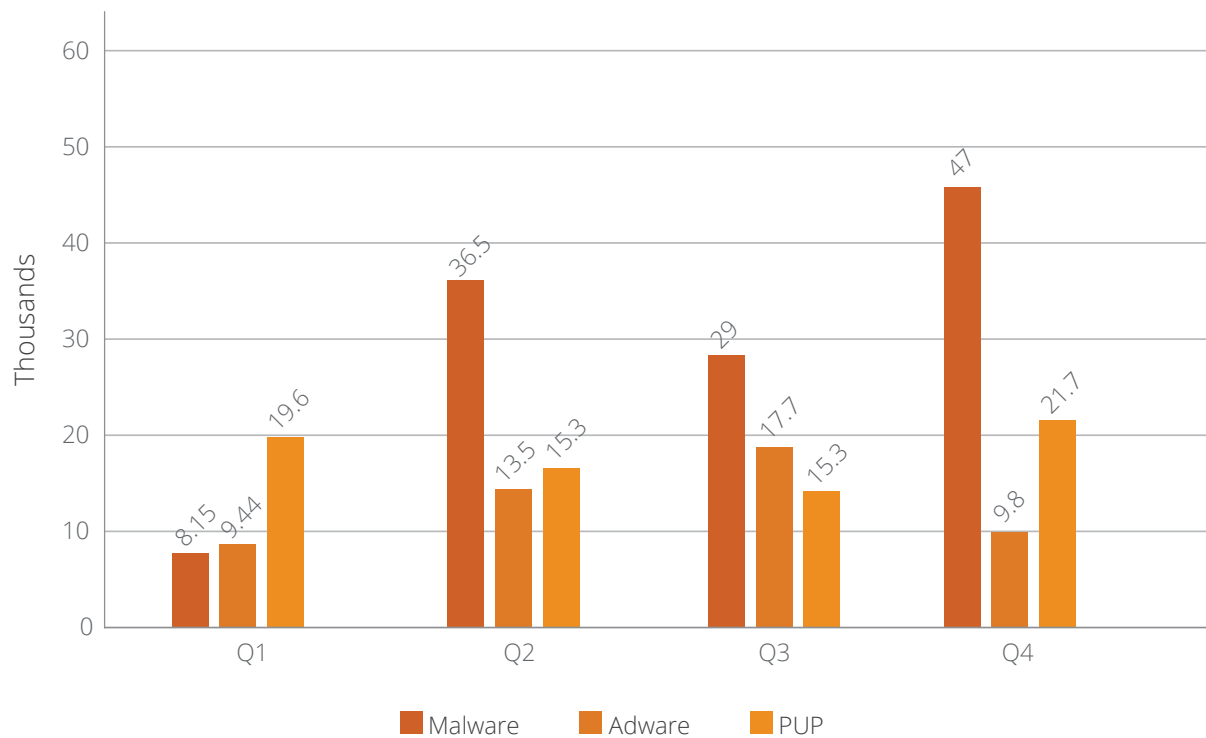


PUA:
71,978

Per Day: 197
Per Hour: 8
Per Min.: 0.14

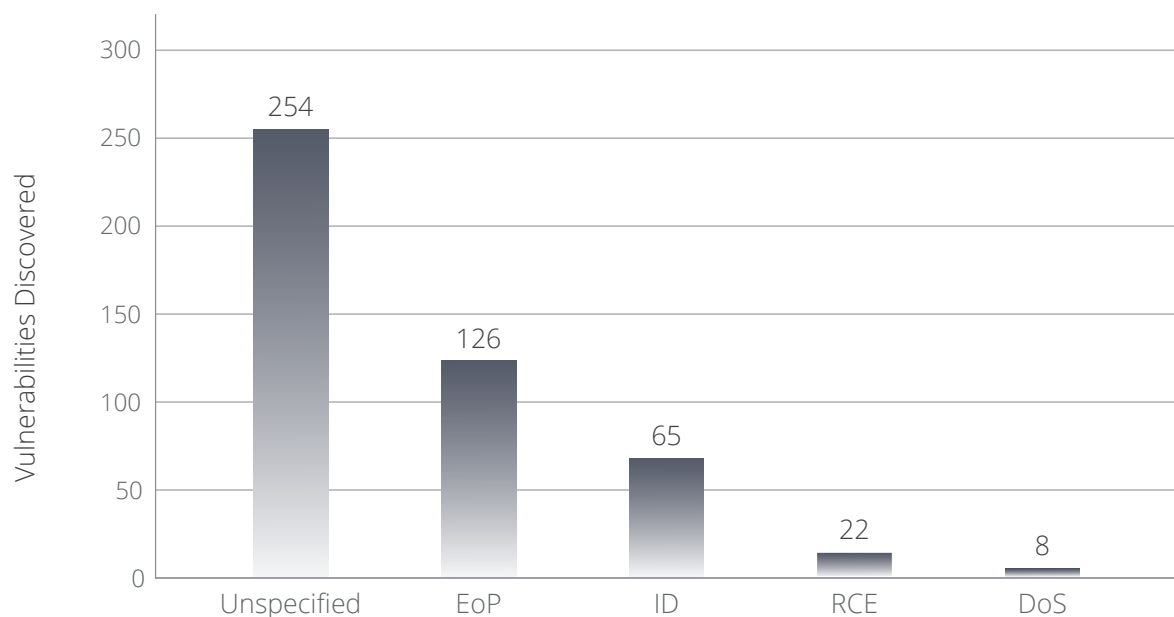


Per Quarter Detection Statistics: Category-wise



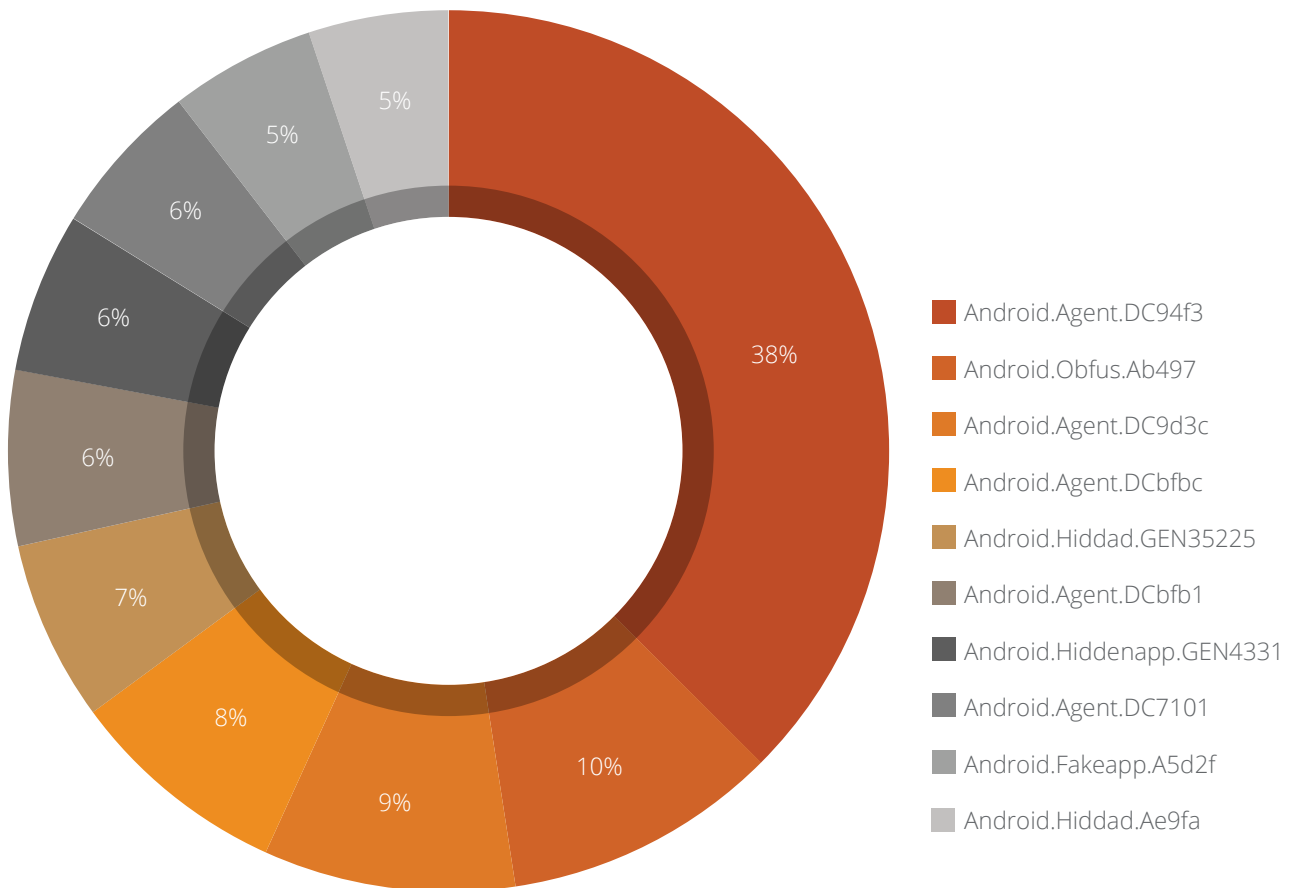
Android Vulnerabilities Discovered in 2021

An android 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 vulnerabilities and their growth in 2021.



Unspecified - Classification not available | EoP - Elevation of Privilege | ID - Information Disclosure
RCE - Remote Code Execution | DoS - Denial of Service

2021 Top 10 Android Malware Detections



Top 10 Threat Details

01

Android.Obfus.Ab497

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- 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

Behavior

- 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.DC9d3c

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores and re-packed apps

Behavior:

- Makes use of SDK to recompile other genuine apps easily
- Downloads other apps on the device, causing unnecessary memory usage
- Shares device information such as location and email account with a remote server
- Displays unnecessary advertisements

04

Android.Hiddad.GEN35225

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

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

05

Android.Agent.DCbfbf

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- 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.

06

Android.Agent.DCbfbf1

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- It disguises itself 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 hidden and display advertisements that it receives from its C&C server.

07

Android.Hiddenapp.GEN43311

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- 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.Fakeapp.A5d2f

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- It disguises itself as a genuine app. After launching, it hides its icon and runs in the background.
- It may steal users' sensitive information like banking details, SMS, passwords.
- Many times its purpose is to increase download count and rating.

09

Android.Agent.DC7101

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- 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.Hiddad.Ae9fa

Threat Level: High

Category: Malware

Method of Propagation: Third-part app stores

Behavior:

- These apps use a standard SDK (Software Development Kit) for advertising.
- Capabilities of this malware family include showing ads, opening URLs in the browser and 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.

Annual Round-up of Android Security Threat Trends

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

Android malware spreading through social media applications

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 cookies 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 harvest data. Quick heal detects these applications with detection "Android.Facestealer."

Similarly, 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"

03

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.

04

Use of Phishing campaign with respect to Current News

This year, we have seen many phishing campaigns carried out by the threat actors to spread Malware. Most of them took advantage of the pandemic situation and vaccination programs.

Hackers target users with fake COVID-19 vaccine registration apps for this purpose to spread the Fake vaccination registration application. The Android worm collects all contacts from the victim's device and distributes them through SMS. During the COVID-19 vaccination, a drive was started in India for everyone above 18. 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 circulated, tricking users into 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.GEN"

Quick Heal observed some malware applications targeting Indian taxpayers through phishing. They pretend to be the e-filing site that other downloads the fake application. These applications spread through fake text SMSs in the name of the Income-tax department of India. This application leads to stealing sensitive information like SMS data, phone number, e-mail address, etc. These applications have used the income tax department's original logo to trap users. The attacker behind this has exposed this sensitive data on the internet. Quick heal detects these malware applications with detection Android.GoodNews.GEN and Android.Agent.DC

05

New Smishing Malware targeting Android Users

SMS or WhatsApp messages containing malicious URLs or any other malicious content are spreading these days extensively with various attractive themes to lure in users. Such fake messages targeted recipients to click a link and send the attacker private information or download malicious programs to a smartphone. This kind of attack is called Smishing.

In 2021 we saw some malware using this attack vector. Flubot is targeting various countries with different versions of malware in DHL and FedEx delivery services. This was a banking Trojan spread in Europe, Australia, and some Middle East countries using fake SMS about delivery services companies. Oscorp was another banking Trojan that got distributed through Smishing. It was mainly targeting Spain, Poland, and some Asian countries. We also observed SMS phishing campaigns impersonating Iranian government services. We have recently seen Brata, an Android RAT, spread using the same vector. Quick Heal detects all of the malware mentioned above with our various detection -Android.Flubot.GEN, Android.Agent.A etc.



INFERENCE

2022 may be the time to add a cybersecurity resolution to your list to help protect the most overlooked commodities – your digital identity and privacy. Cybercrime continues to flourish in a hybrid-driven digital landscape that brings new opportunities for fraudulent activities, phishing campaigns, and malware attacks that take advantage of decreased cyber resilience among Windows and Android users.

It's time we take control of our digital life and monitor our digital footprint wherever we go or whatever we do!

The year 2021 has taught us that no matter how much adversity we face, the adversary will not rest. The increased integration of endpoints in hybrid working environment, combined with a rapidly growing and poorly controlled attack surface, poses a significant threat to the users. Protecting such complex and unknown threats is no easy task, especially when so many devices of varying types and security standards. It is estimated to only worsen in 2022 as connectivity grows.

Stay protected in 2022 by leveraging a broad range of Quick Heal solutions to safeguard your identity and privacy from advanced threats.



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