Quick Heal

Security Simplified

ANNUAL THREAT REPORT 2021

673.58
Million
Windows Malware detected in 2020

January
saw the highest Windows Malware attacks in **2020**

Trojan
was the highest detected malware across **2020**

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:

Seqrite Annual Threat Report

To know how the threat landscape targeting enterprise segment played out in 2020, please go through:

Seqrite Annual Threat Report 2021

Visit: www.seqrite.com

Contents

Foreword **01**
Category Wise Year on Year (YoY) Windows Malware Detection Statistics for 2020 02
Top Cyber-Attack Stories Of 2020 03
The Indian States Most At Risk 06
The Indian Cities Most At Risk 07

Windows **08**
Detection Highlights 2020 09
Monthly Malware Detection for 2020 10
Quarterly Malware Detection for 2020 11
Quarter on Quarter (QoQ) Malware Detection Statistics 11
Category Wise Quarter on Quarter (QoQ) Malware Detection Statistics 12
Protection Module Wise Detection Stats 13
Top Ten Malware in 2020 15
Top 10 Potentially Unwanted Applications (PUA) and Adware of 2020 19
Top 10 Host-Based Exploits 20
Top Five Network-Based Exploits 21
Trends in Windows 22

Android **25**
Android Detection Highlights 2020 26
Top Ten Android Malware in 2020 26
Category-Wise Android Detection Statistics 29
Trends in Android Security 30
Turn the Page: Predictions for 2021 and Beyond 31

Inference **35**

Foreword

Malware numbers have nearly halved in 2020 as against 2019! For a world coming to terms with the COVID-19 pandemic, this might sound like some really good news from a cybersecurity perspective. However, be warned that the drop in numbers is no sign of adversaries slowing down from their usual behaviour.

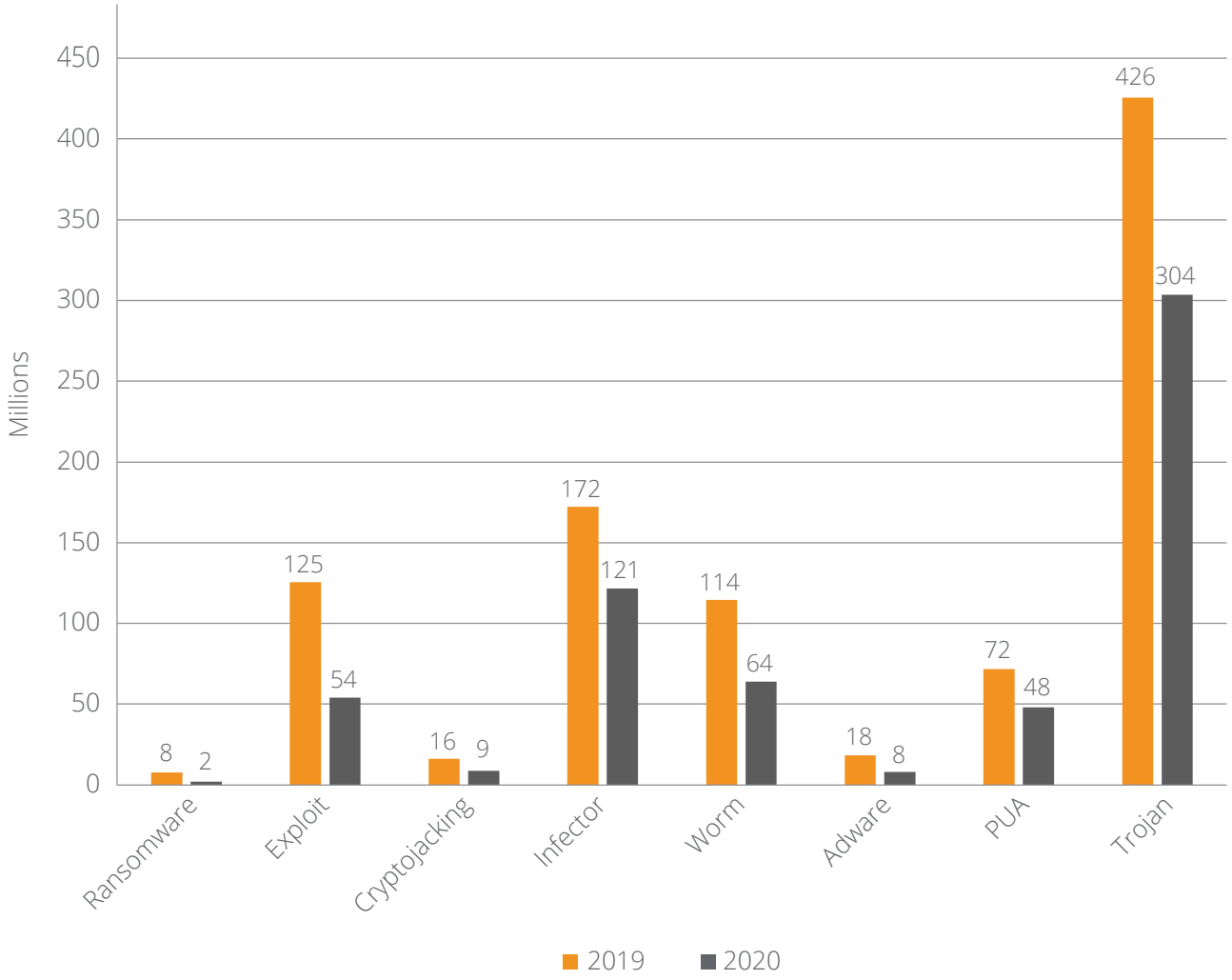
During the complete lockdown, personal devices were used professionally as well. The new normal forced adversaries to focus on shifting their strategies to align with a new attack surface. It looks nearly certain that the drop in numbers is due to this new environment, and not because of declining attack vectors.

The epidemic will overlap into 2021 and with attackers ready, it is predicted that the number of infiltration attempts will increase.

Malware numbers almost halve in 2020!

Category Wise Year on Year (YoY) Windows Malware Detection Statistics for 2020

The below graph represents year on year (YoY) category-wise Windows malware detection statistics.



Observation

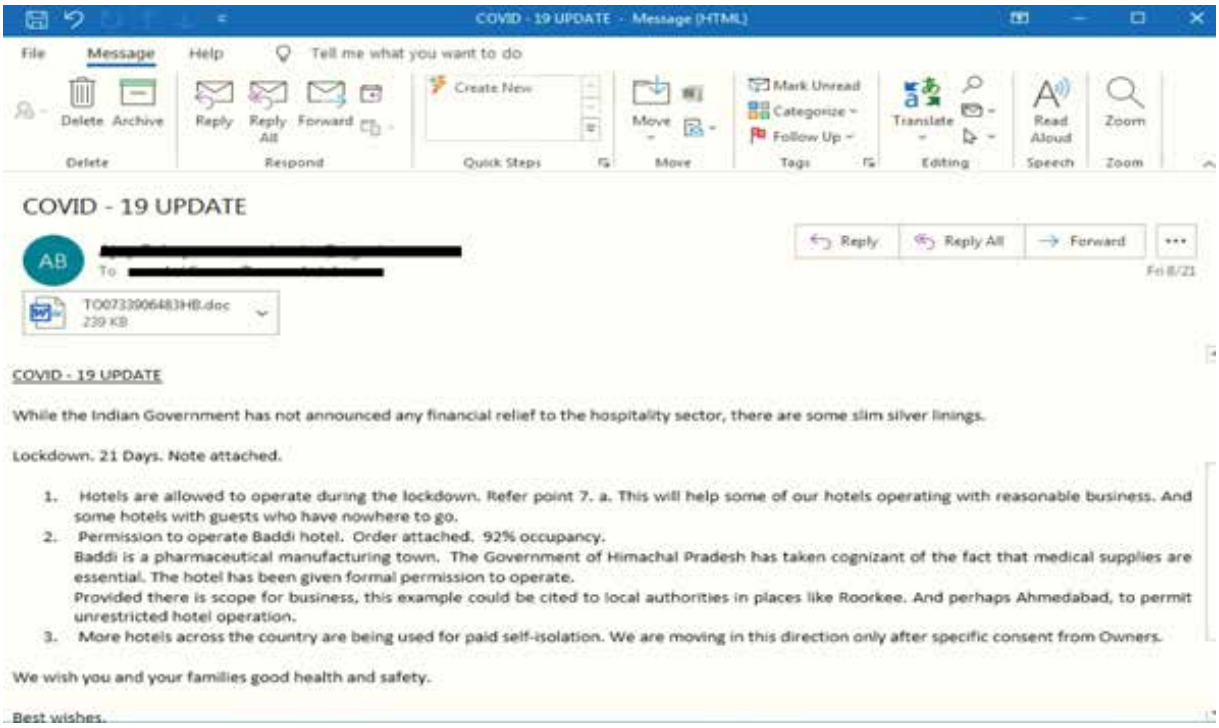
Trojan was the highest detected malware across 2019 & 2020 indicating its popularity with cyber attackers.

Top Cyber-Attack Stories Of 2020

01

Emotet is Back After Unlock!

Emotet Trojan has been a persistent threat actor for quite some time now and is considered highly successful in delivering malware through crafted emails with subject names containing hot keywords. A typical email sample from numerous instances we detected can be seen below.



02

Dharma Aka CrySIS: An Exhaustive Phenomena of Human Operated Ransomware!!!

Dharma aka CrySIS ransomware has been rampant from years leveraging infection mechanisms like spam emails, targeting public IPs with open RDP ports, etc. Human- operated and resilient in evading anti-virus software, Dharma attacks are prevalent in SMB organizations and critical service providers.

The attacks are typically staged in the manner mentioned below -

- Search for target systems with vulnerabilities
- Gain initial access using brute-force tools
- Disable security solutions
- Steal Credentials through tools such as Mimikatz
- Clear event logs using wevutil.exe
- Get privileges from local administrator to SYSTEM using 'Sticky Keys'
- Stop active services that might interfere with encryption
- Enable RDP connections with registry modifications using .bat or .reg files
- Create new local accounts and add them to the local administrator group
- Use tools such as vulnerability scanning tools to find more targets in a local network

Popular tools used to carry out these attacks are -

- Masscan
- NLBrute
- Advanced Port Scanner
- Defender Control
- Your Uninstaller
- PCHunter
- PowerTool x64
- GMER
- Obit Unlocker software
- Process Hacker

03 A New Era in Ransomware

Ransomware has evolved from being a simple screen locker to an advanced file infector which encrypts user's important files and mapped network drives. Ransomware authors always update their TTPs to attack a large number of systems and gain maximum benefit.

Essentially, they evolve in two directions, one being the use of different encryption techniques and the other, using different attack vectors to encrypt a large number of systems.

We have listed down a few techniques which are used in recent malware attacks, worldwide.

04 WoL (Wake on Lan) in Ryuk Ransomware

Wake on Lan (WoL) is a hardware feature that allows a computer to be switched on or awakened by a network packet.

05 Process Hollowing in Mailto aka Netwalker Ransomware

The Mailto or Netwalker performs process hollowing in explorer.exe - this helps in evading the Anti-Virus software (AVs) to easily perform encryption.

06

Exploiting Vulnerabilities in System/Products i.e., CVE-2020-0601 By HorseDeal Ransomware, CVE-2018-19320, Gigabyte by Robinhood Ransomware

This is a spoofing vulnerability in Windows CryptoAPI (Crypt32.dll) validation mechanism for Elliptic Curve Cryptography (ECC) certificates. HorseDeal leveraged this vulnerability by making use of a spoofed ECC certificate to evade detections.

07

RagnarLocker Ransomware Hides in Virtual Machine

Threat actors have developed a new type of ransomware attack that uses virtual machines to hide the malicious code from security products. Since ransomware application runs inside the virtual guest machine, its processes and behaviour can run unhindered, as they are out of the reach of security software on the physical host machine.

08

PonyFinal and Tycoon Ransomware used JAVA as the language/file format for Encryption

PonyFinal is Java-based ransomware which requires JRE (Java Run-Time Environment) in the system to specifically target enterprise organizations where JRE is available on almost all the systems.

09

Info-stealer hidden in the phishing emails!

Phishing emails directed to entice users into downloading malicious content and steal precious information are still on the rise. Details of the attack tactics can be found through our blog here.

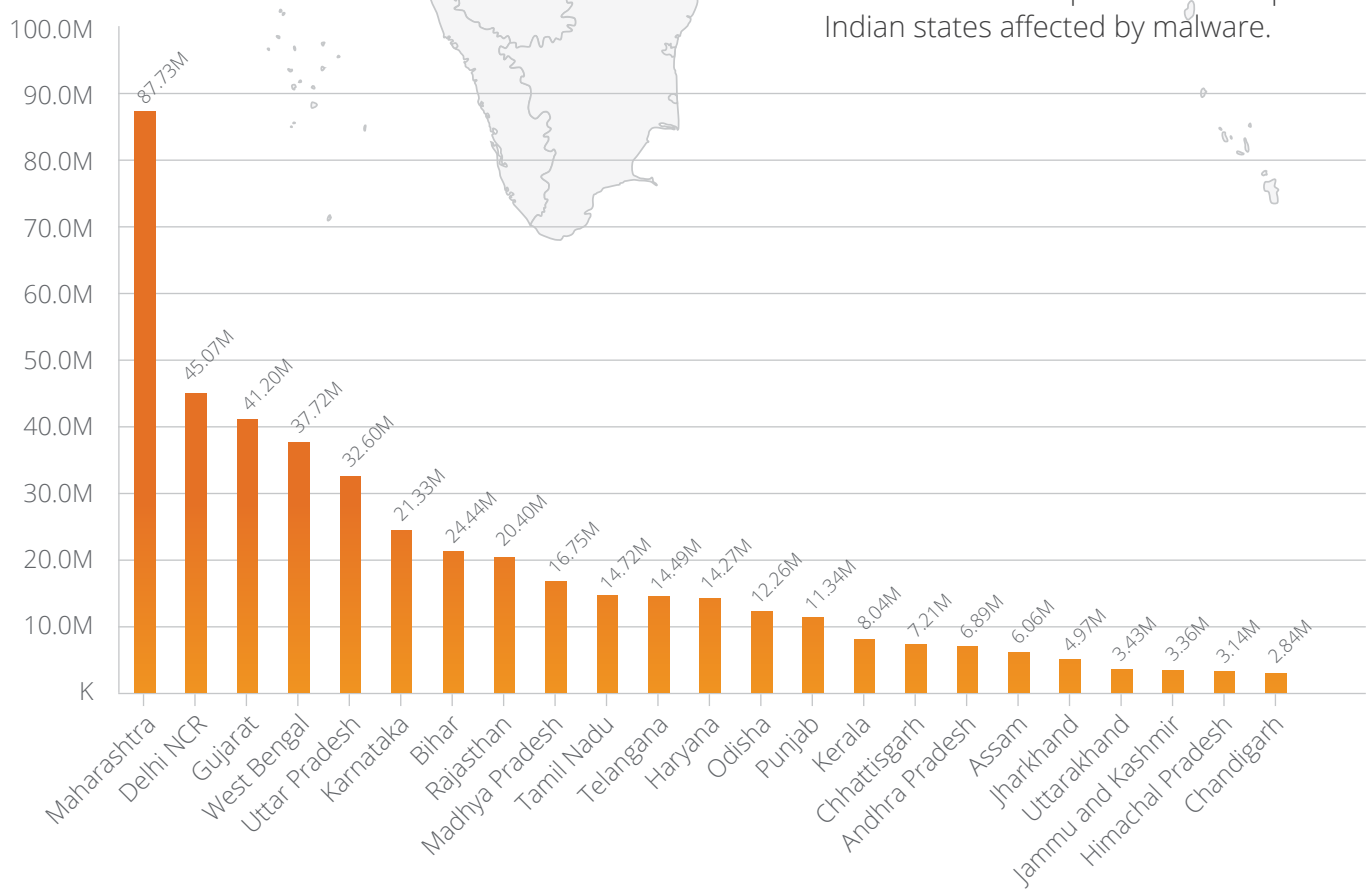
10

Poulight- An info-stealing trojan might be teaching you how to play Minecraft

Poulight, info-stealer Trojan, which in all likelihood originated in Russia is notoriously popular in collecting sensitive user information through Minecraft, a popular video game. Ever since its first appearance, it has been growing and taking different forms with the main infection vector remaining spear-phishing emails. Read our detailed blog for more information on Poulight.

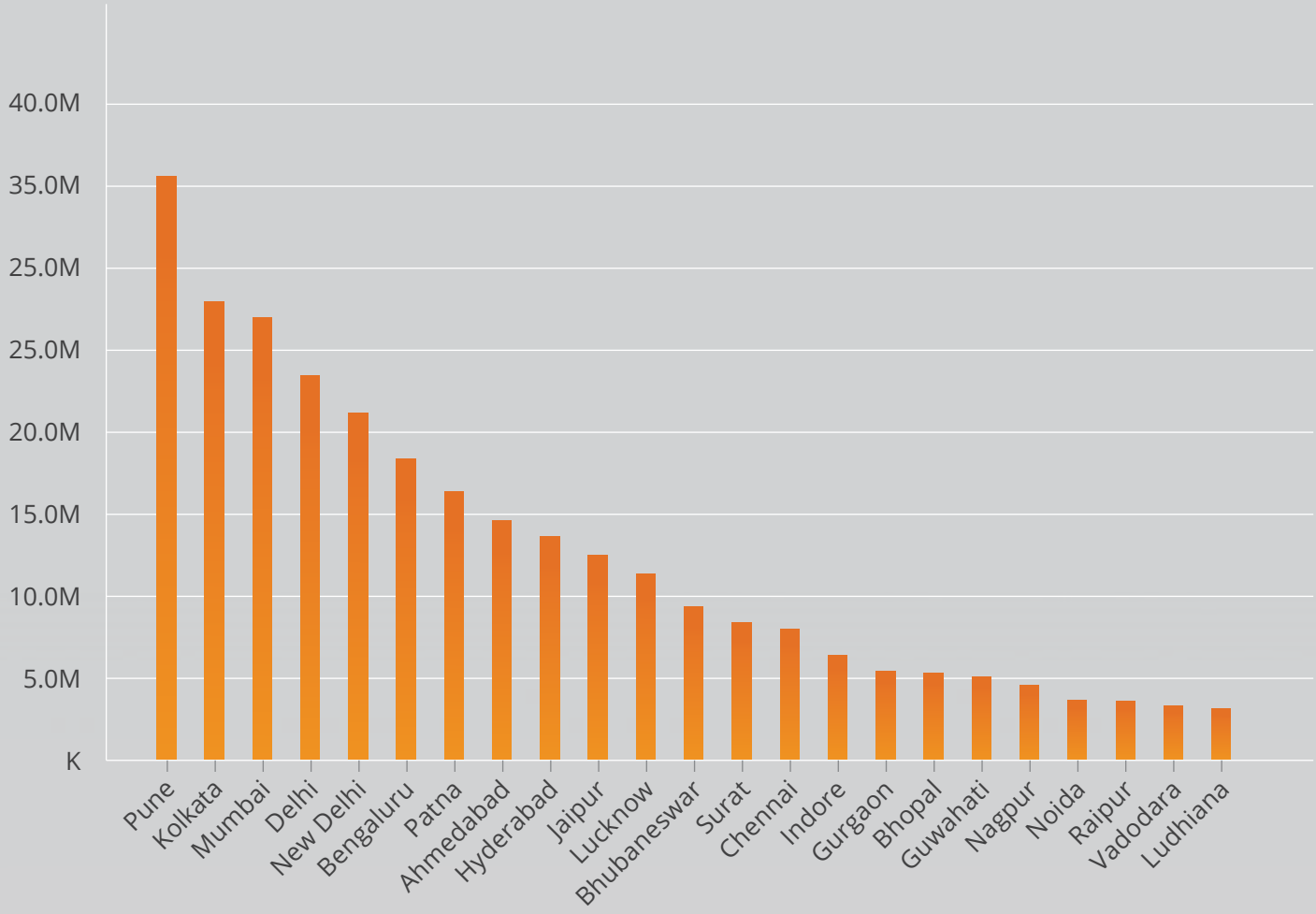
The Indian States Most at Risk

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



The Indian Cities Most at Risk

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



WINDOWS

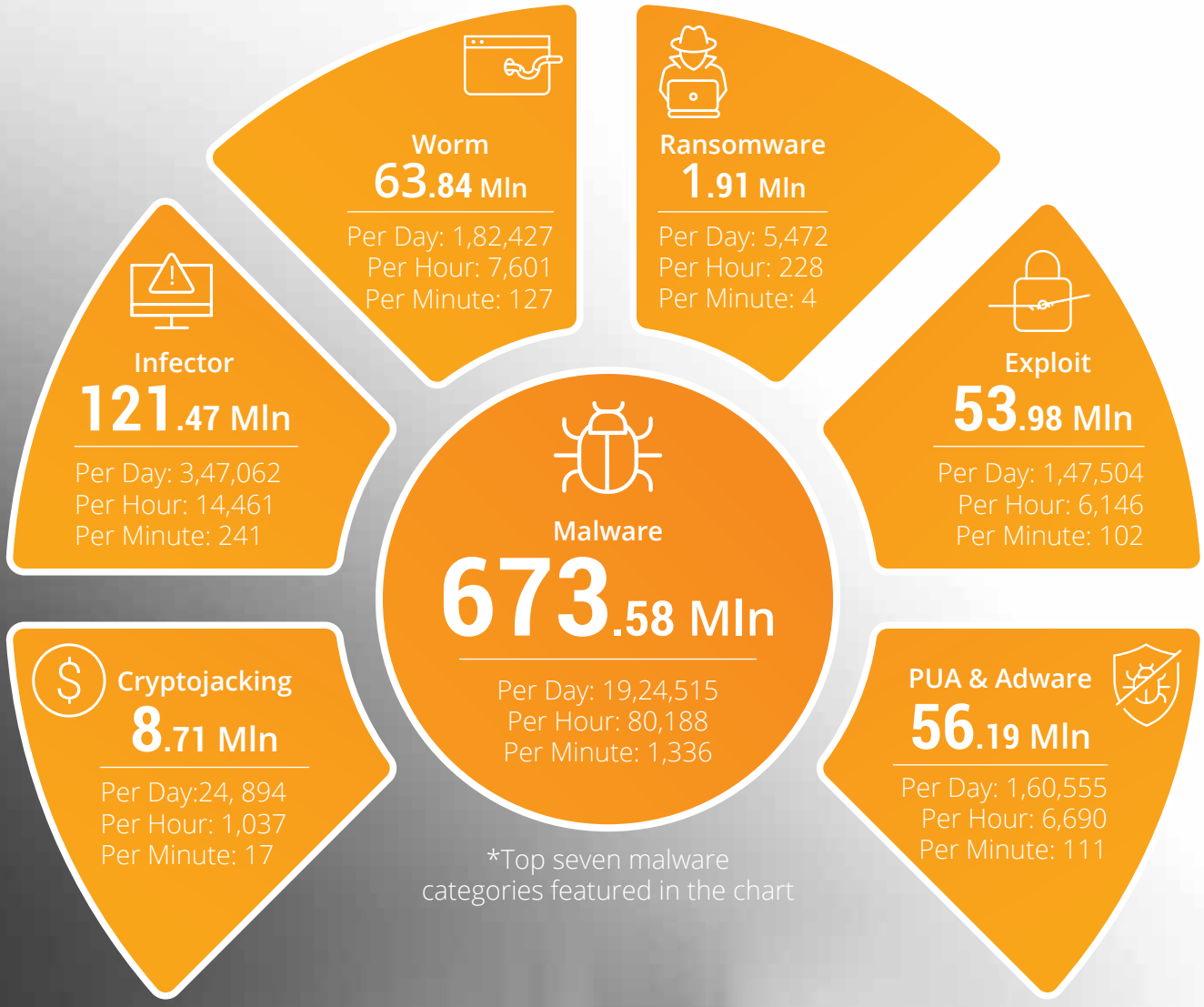
203

Million
Windows Malware detected in Q1, highest in 2020

Most malware were detected by Network Security Scan at

38%

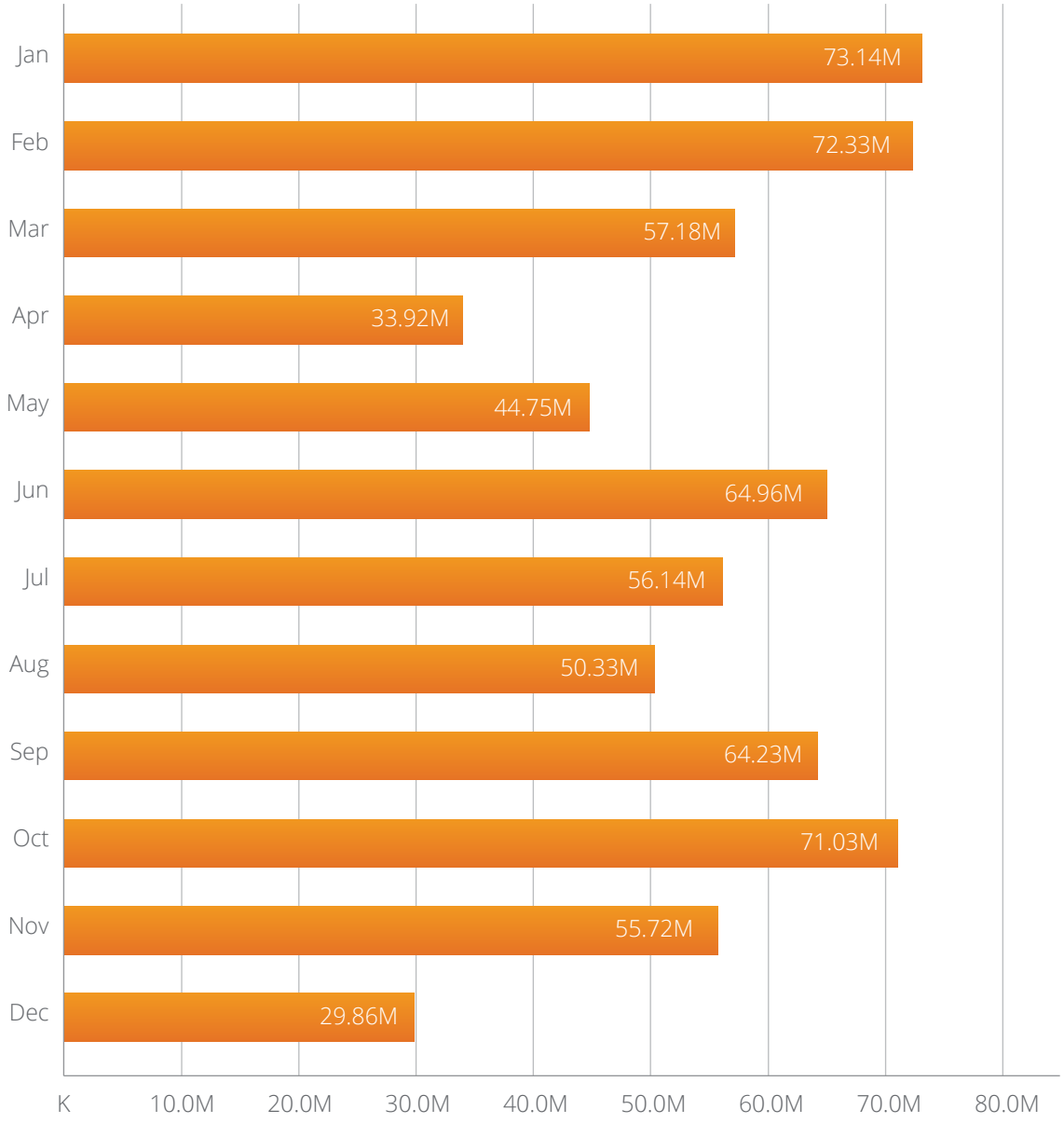
Detection Highlights 2020*



*Top seven malware categories featured in the chart

Monthly Malware Detection for 2020*

The graph below represents monthly malware detection for 2020.



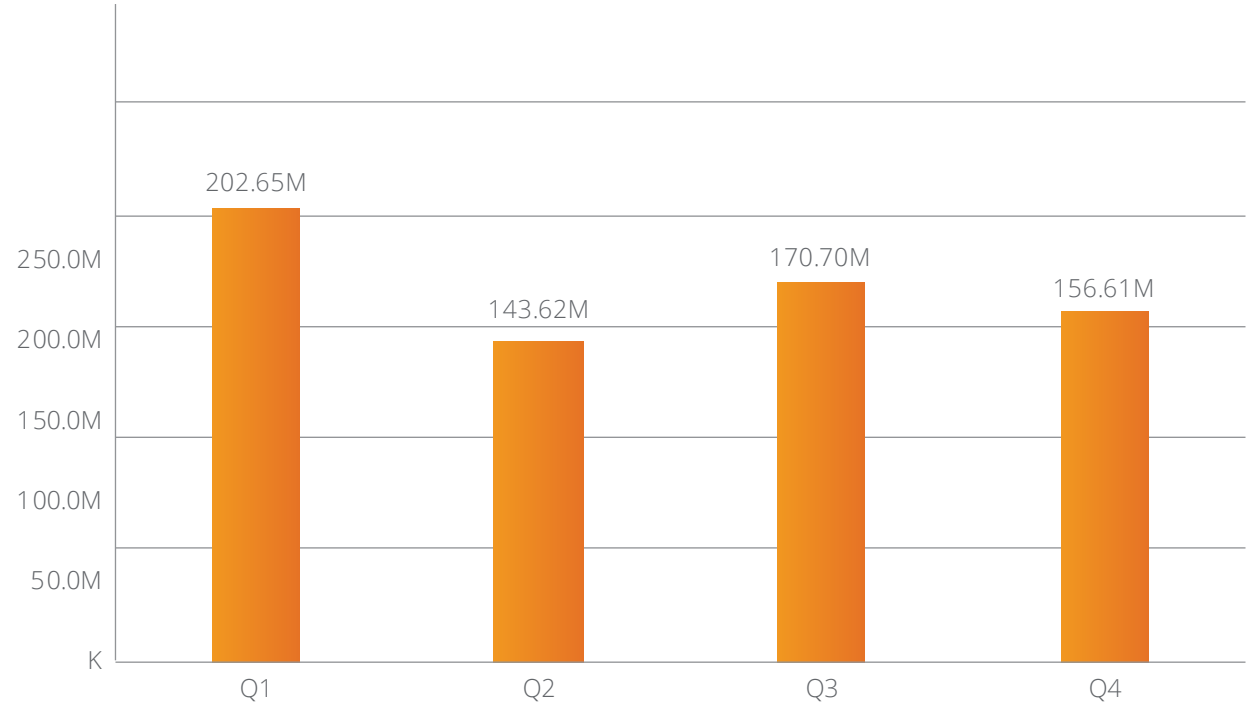
Observation

January 2020 saw maximum malware attacks.

**(The data for December 2020 has been extracted until the 15th of the month.)*

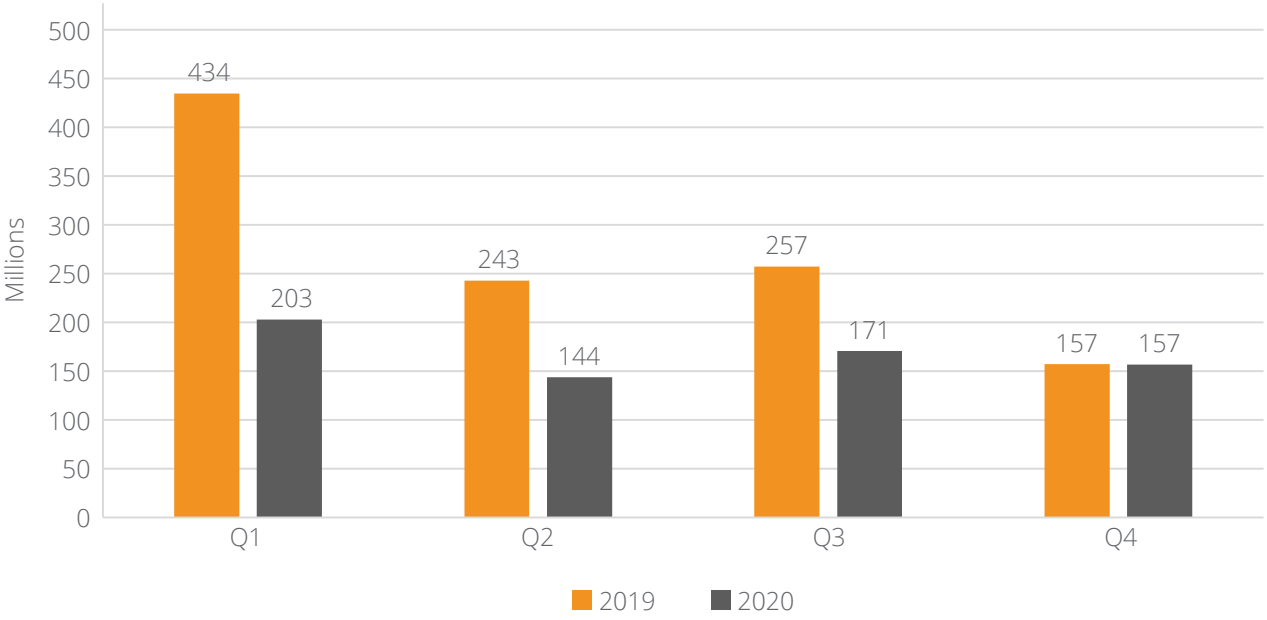
Quarterly Malware Detection for 2020

The graph below represents quarterly malware detection for 2020.



Quarter on Quarter (QoQ) Malware Detection Statistics

The below graph represents quarter on quarter (QoQ) malware detection statistics for 2020.

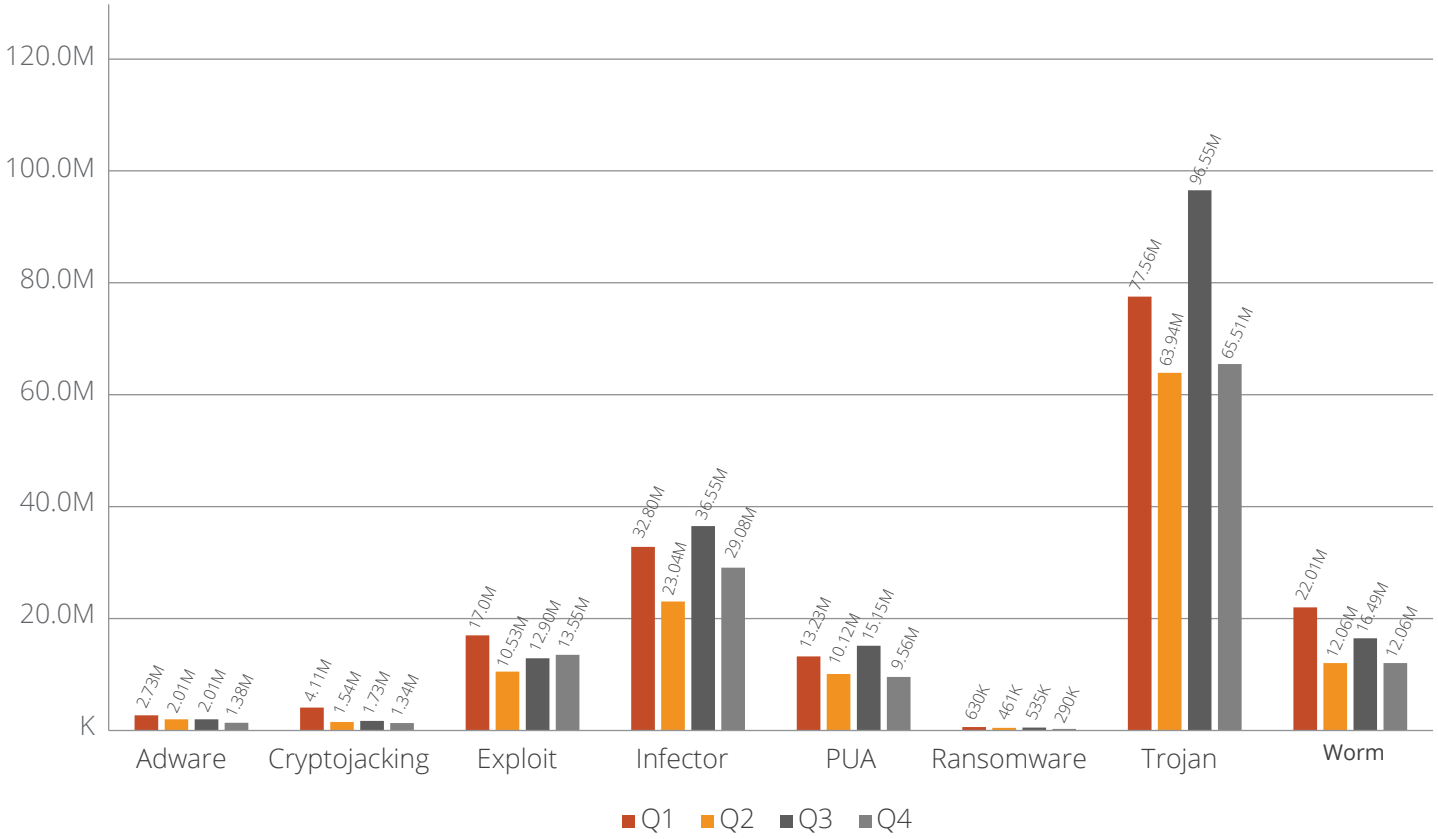


Observation

- 673.58 million malware were detected in 2020 as against 1.08 billion in 2019.
- Q1 - 2020 clocked the highest detection of malware at 203 million.

Category Wise Quarter on Quarter (QoQ) Malware Detection Statistics

The below graph represents quarter on quarter (QoQ) category-wise malware detection statistics for 2020.

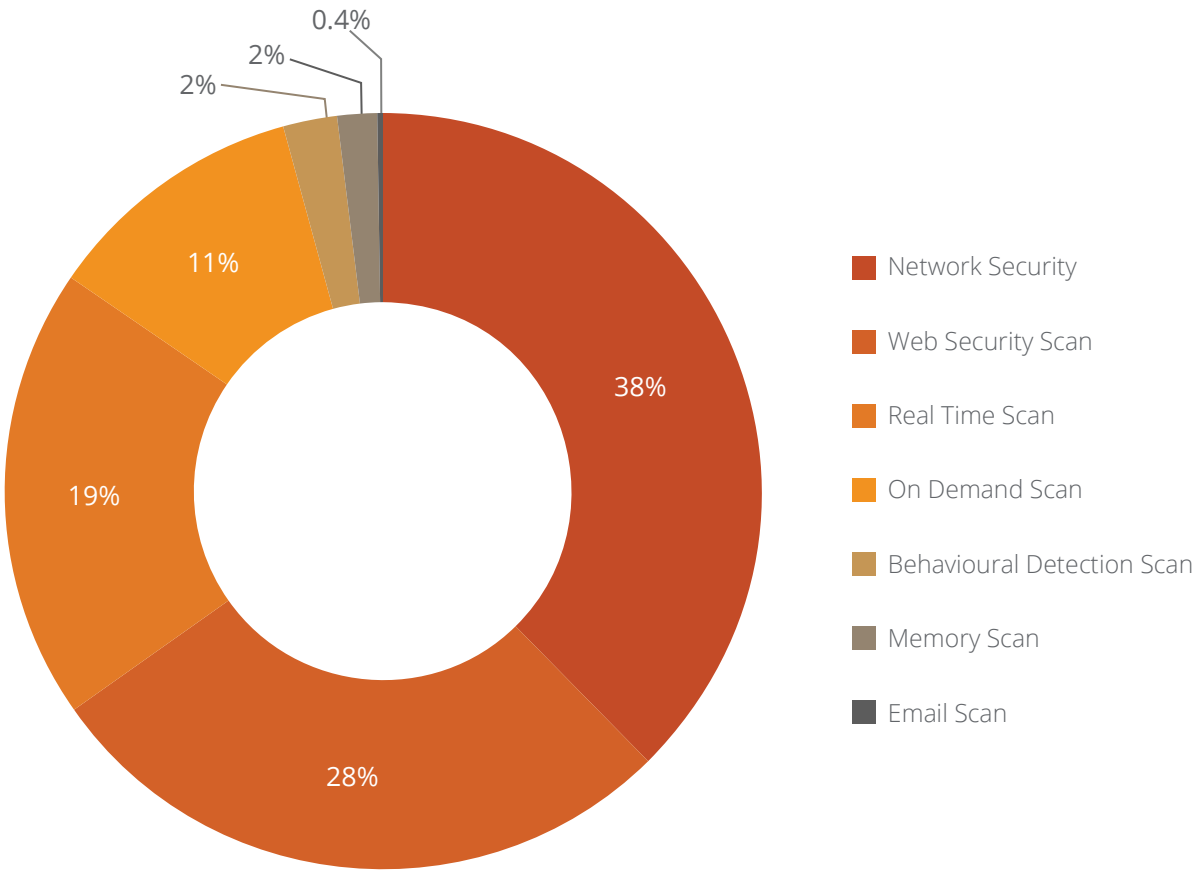


Observation

The Trojan malware dominated across all four quarters of 2020.

Protection Module Wise Detection Stats

This section features the various methodologies through which Quick Heal Security Labs detected malware in 2020.



Observation

Most malware were detected by Network Security Scan at 38% followed by Web Security Scan at 28%.

Here is a brief description of how various detection methods function -

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.

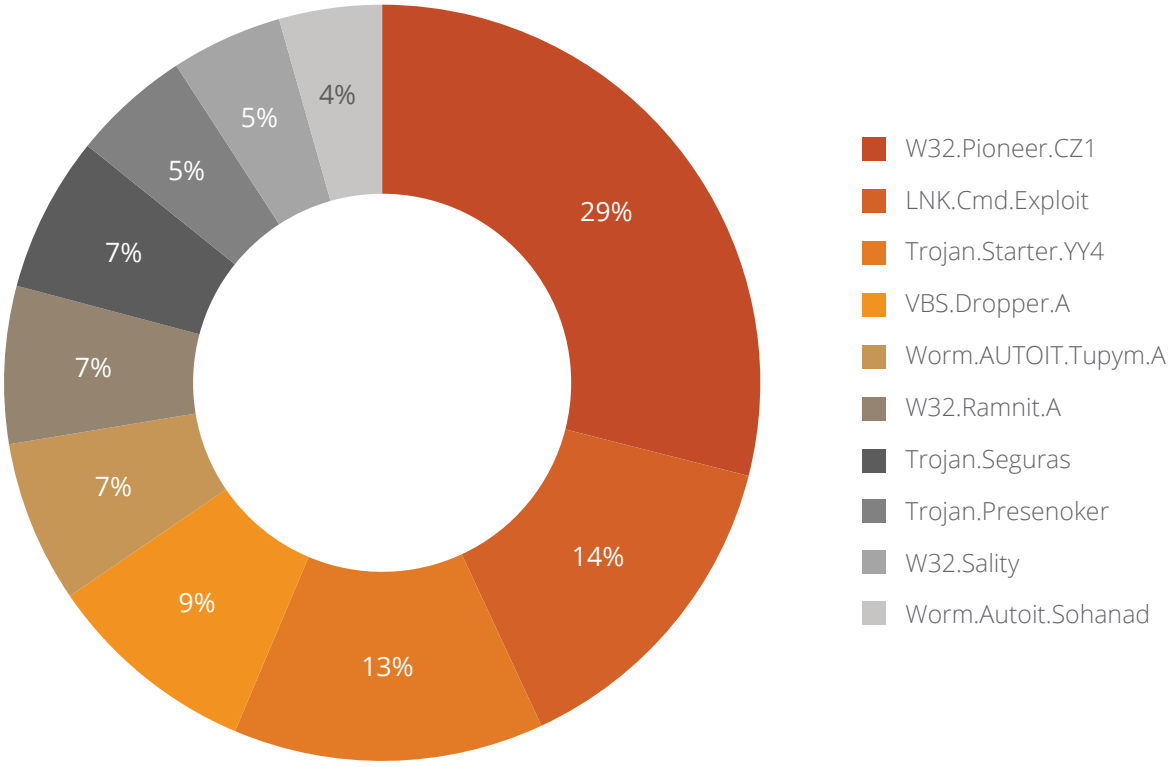
Email Scan
Blocks emails that carry infected attachments or links to compromised or fake and phishing websites.

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

Network Scan
Network scan (IDS/IPS) analyzes network traffic to identify known cyberattacks & stops the packet being delivered to the system.

Top Ten Malware in 2020

The below figure represents the top 10 Windows malware of 2020 based upon their rate of detection in the year.



Observation

The W32.Pioneer.CZ1 malware was detected the most in 2020.

Top 10 Windows Malware

01

W32.Pioneer.CZ1
Threat Level: Medium
Category: File Infector
Method of Propagation: Removable or network drives

Behaviour:

W32.Pioneer.CZ1 injects its code into files and maliciously collects system information sending it to attackers.

02

LNK.Cmd.Exploit
Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites

Behaviour:

LNK.Cmd.Exploit uses cmd.exe with "/c" command-line option to execute other malicious files simultaneously executing a malicious vbs file which uses Stratum mining protocol for Monero mining.

03

Trojan.Starter.YY4
Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites

Behaviour:

Trojan.Starter.YY4 creates a process to run the dropped executable file and modifies computer registry settings which may cause a system crash. It also downloads other malware like keyloggers, slows down the booting and shutting down process of the infected computer and allows hackers to steal confidential data like credit card details and personal information from the infected systems.

04

VBS.Dropper.A
Threat Level: Medium
Category: Dropper
Method of Propagation: Web page

Behaviour:

VBS.Dropper.Aspreads via malicious web pages — a web page contains an embedded PE file, so it drops that PE file to a specific folder & launches from there to perform malicious activity.

05

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

Behaviour:

Behaviour: Worm.AUTOIT.Tupym.A drops file in system32 folder and execute it from a dropped location. It connects to a malicious website, modifies start page of browser to another site and creates a run entry in the same (dropped) file for persistence.

06

W32.Ramnit
Threat Level: Medium
Category: File Infector
Method of Propagation: USB Drives, other malware, Exploit Kits, Spoofing the URL, and Bundled applications

Behaviour:

W32.Ramnit infects all running processes, more so, the HTML files by appending the script in. In the case of PE file infection,it appends itself in the file modifying registry entries to ensure the same.

07

Trojan.Seguras
Threat Level: Low
Category: Trojan
Method of Propagation: Bundled Applications

Behaviour:

Trojan.Segurasoften shows fake scan results to lure users in purchasing its full version. It causes substantial system degradation and may download other malware that can infect computer systems.

08

Trojan.Presenoker
Threat Level: Low
Category: PUA
Method of Propagation: Bundled Applications

Behaviour:

Trojan.Presenoker injects ads in web pages, changes browser settings and creates popups asking users to download fake software or update. It also degrades system performance.

09

W32.Sality.U
Threat Level: Medium
Category: File Infector
Method of Propagation: Removable or network drives

Behaviour:

W32.Sality.U injects its code into system processes and gathers confidential information from affected machines.

10

Worm.Autoit.Sohanad
Threat Level: Medium
Category: Worm
Method of Propagation: Spreads through mails, IM apps, infected USB & network drives

Behaviour:

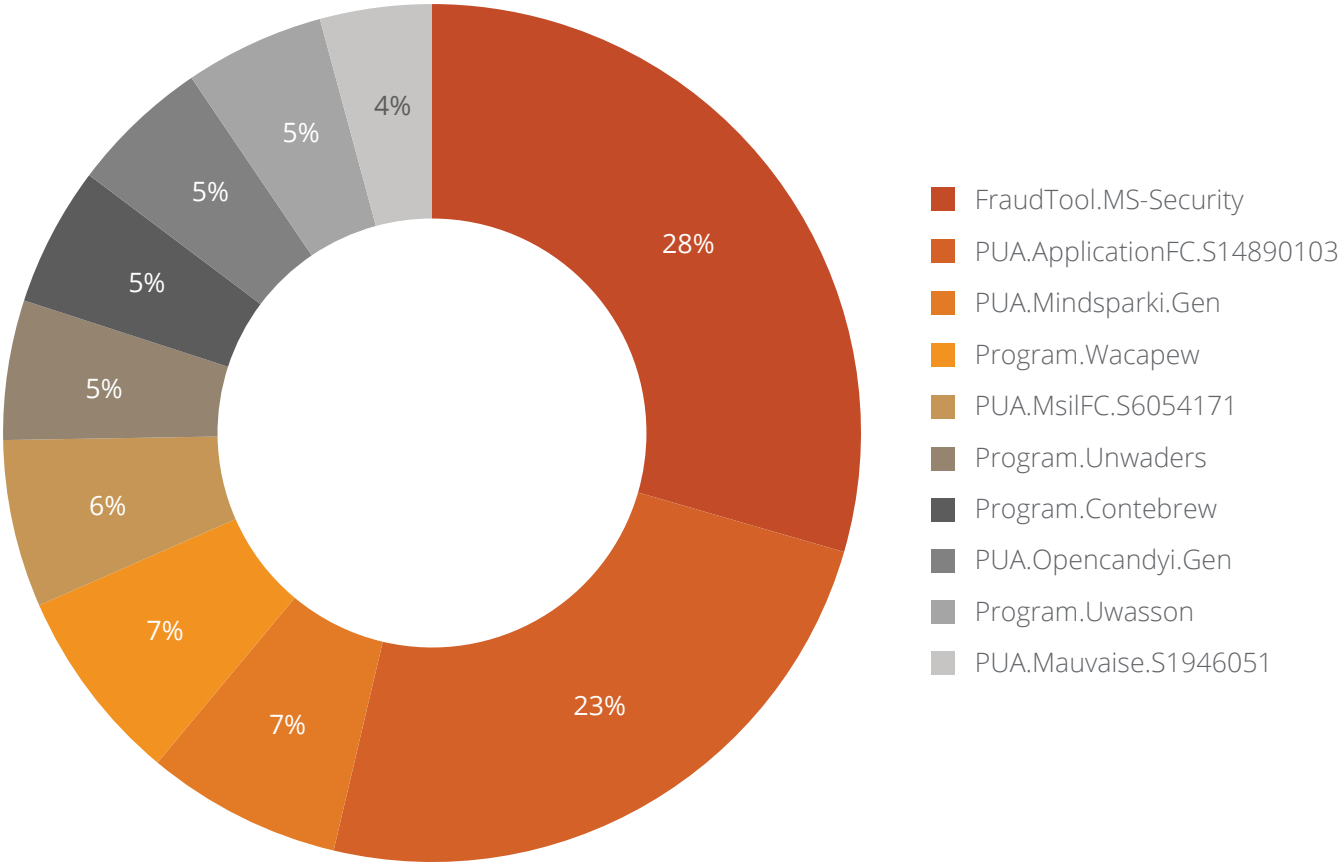
Worm.Autoit.Sohanad infiltrates computers through messaging apps, infected USB or network and spreads quickly. After arrival, it creates a copy of itself as exe with a typical Windows folder icon. Users mistakenly execute this exe assuming it as a folder — it infects every connected USB drive as well.

Top 10 Potentially Unwanted Applications (PUA) and Adware of 2020

Potentially Unwanted Applications (PUAs) are programs that 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 10 PUAs and Adware detected in 2020.

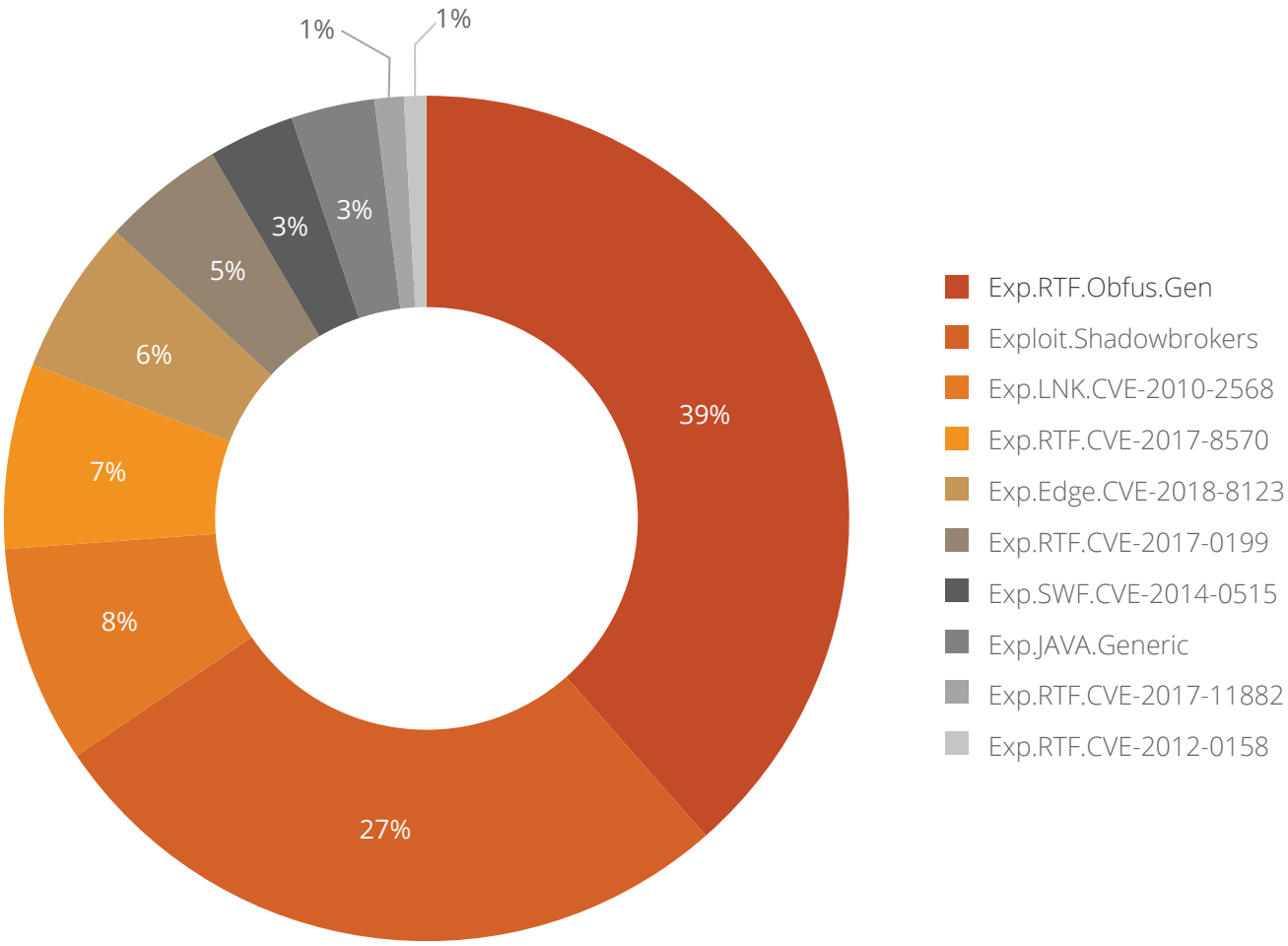


Observation

With 28% detection, FraudTool.MS-Security was the top PUA in 2020.

Top 10 Host-Based Exploits

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. Below figure represents the top 10 Host-Based exploits of 2020.



What are host-based exploits?

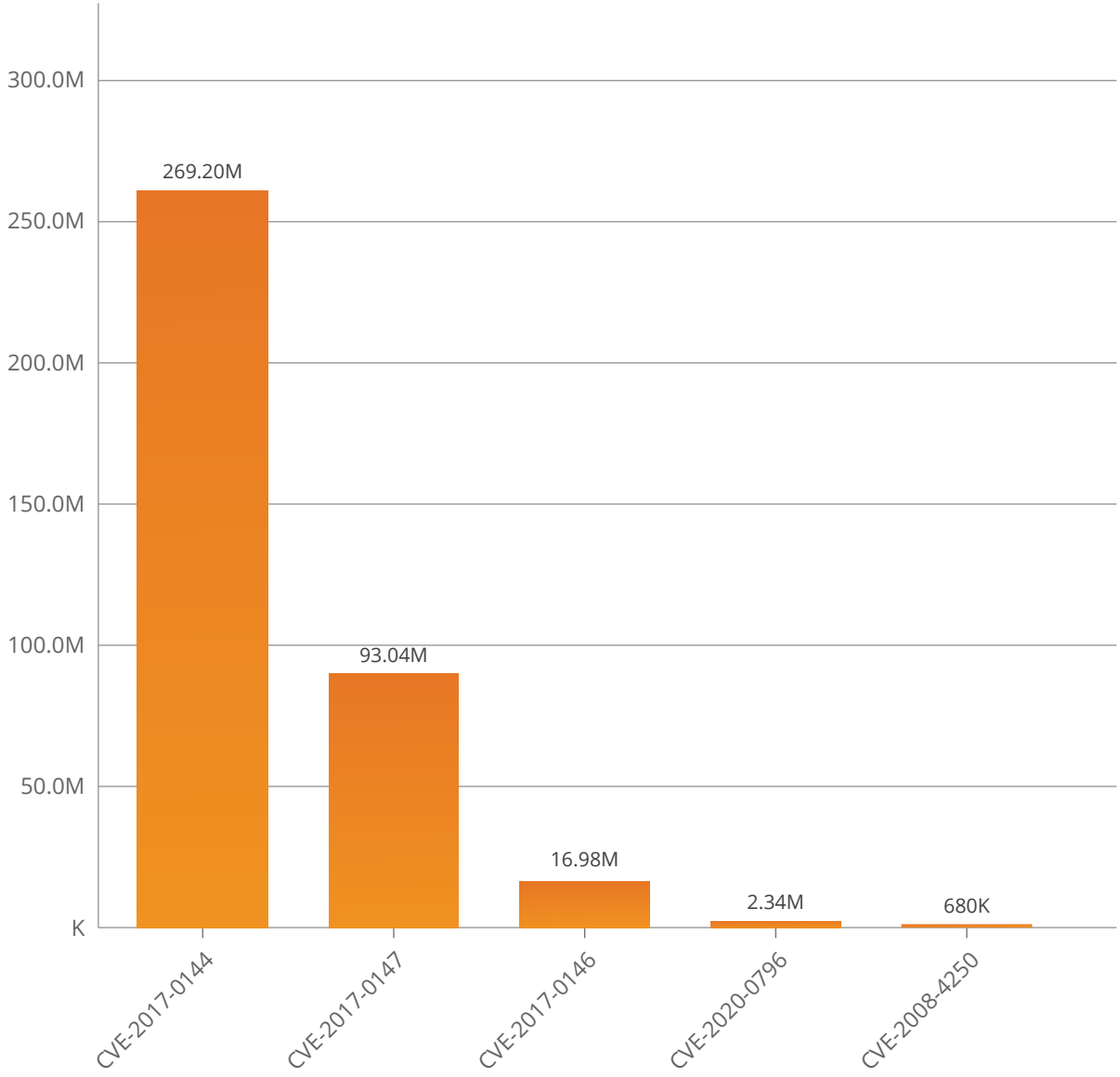
Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

Observation

With 39% attempts, the Exp.RTF.Obfus.Genwas the top detected host-based exploit of 2020.

Top Five Network-Based Exploits

Below figure represents the top five Network-Based exploits of 2020.



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

With 269 million attempts, the CVE-2017-0144was the top detected network-based exploit in 2020.

Trends in Windows

Excel 4.0 Macro (XLM) malware – Evolution

Surprisingly, adversaries have cycled back by attacking through XML Macros, launched by Microsoft in 1992. Using a variety of techniques, families like zloader, Dridex, Trickbot, Danabot use this feature to deliver malware through phishing xls/xlsm documents.

Excel Macro 4.0 was widely used by attackers in malspam campaigns with the below-mentioned file-names -

- req_data-6794349.xls
- Covey_Planning.xls
- Efa-4314.xls
- Rva-1968.xls
- price list 2020.xlsx
- inform-2020-06-01_7985395.xls
- FOH DAILY CASH- REMMITANCE 24-05-2020 NIGHT SHIFT (version 1).xls

Corona-Themed Malspam on the rise

Cyber-criminals are taking advantage of the COVID-19 pandemic for spreading malware — we have found cases where there are different initial attack vectors and varying payloads getting delivered.

Case 1

The attacker sends a document file as an initial attack vector containing exploits like CVE-2017-8570 and CVE-2017-11882. When the user opens this document, a .NET payload is dropped which further injects Agent Tesla in Windows Native process to collect data from victim machines.

Case 2

The attacker sends a compressed archive as an e-mail attachment to the user containing a malicious file which gets downloaded and extracted in some folder having a double extension (for ex. COVID19.pdf.exe, COVID-19 Supplier Notice.jpg.exe).

Case 3

The victim receives a compressed zip file containing a malicious JAR file which upon execution self-extracts again and drops another JAR file in %appdata% location.

Case 4

The victim receives a macro-enabled PowerPoint presentation which spawns mshta.exe to download malicious HTA script from “pastebin.com”.

The ultimate motive of all the campaigns mentioned above is to steal data and get sensitive information from the user or sell the stolen data on the Dark Web.

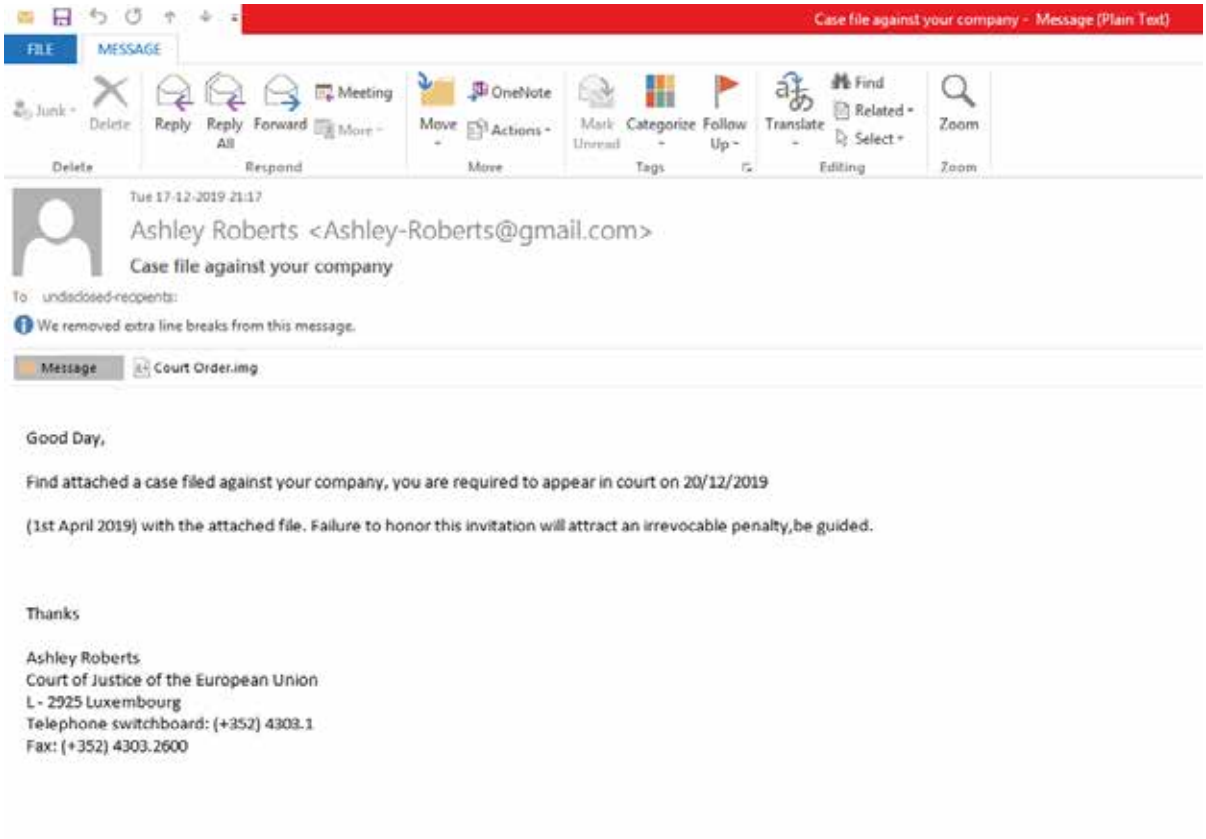
MassLogger: An Emerging Spyware and Keylogger

MassLogger is a new Spyware and advanced keylogger distributed through MalSpam attachments having more features than other present keylogger tools. It has been observed that this campaign is using several different file types as malicious attachments as the initial infection vector.

A new wave of mal-spam campaign attaching Disk Imaging Files.

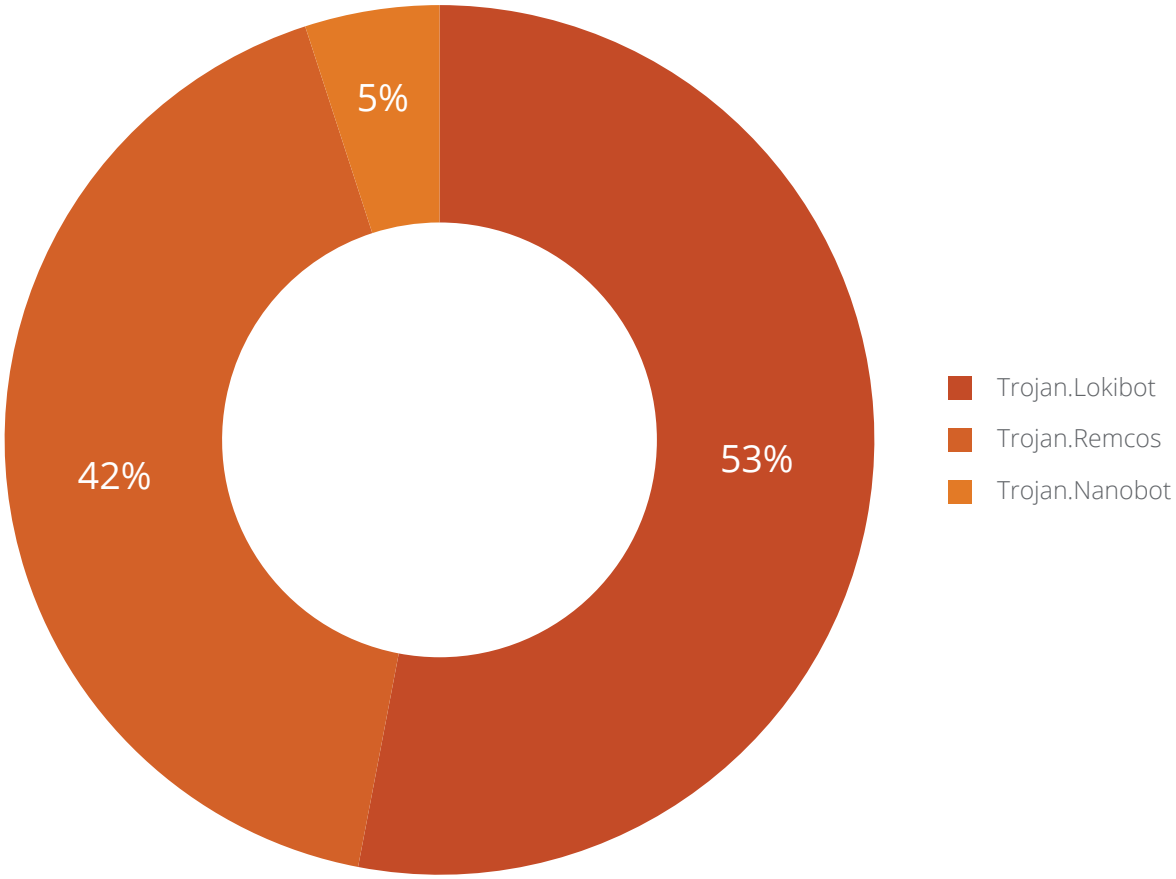
Since last year, we have been seeing a sudden rise in the use of disk imaging file formats in massive mal-spam campaigns to distribute various RATs attached in emails. The subject of these emails is made to appear as genuine as possible — 'case filed against your company' or 'AWB DHL SHIPMENT NOTICE AGAIN', etc. are few legitimate-sounding emails discovered. The attached files contain compressed malware (RAT's) which have many different names like 'Court Order.img', 'Product Order.img', etc.

The below image displays one such spam email.



Two of the most bashed disk imaging file formats are IMG and ISO as these files can be directly opened in explorer, automatically mounting them upon a user's system. The count of IMG and ISO files used in such campaigns was at a peak in January and has been declining since then but malware authors may use these file types in the future.

The most used RATs in this mal-spam campaign are shown in the below figure.



Present-day Ransomware imperil Enterprise

A new ransomware trend is being observed which not only encrypts files but also exfiltrates the private and sensitive files and threaten to release it in public if the ransom payment is not made. This is double trouble for organizations —according to the GDPR (General Data Protection Regulation), releasing sensitive data to the public can cause huge fines. In either case, the organization is likely to have to pay to move forward. This tactic is called RansomHack or Double extortion —Maze, DoppelPaymer, Ryuk, Lockbit, Netwalker, Mountlocker and Nefilim are few ransomware operators which use the double extortion technique and publish the exfiltrated data

ANDROID

220K

Potential Unwanted Apps detected in **2020**

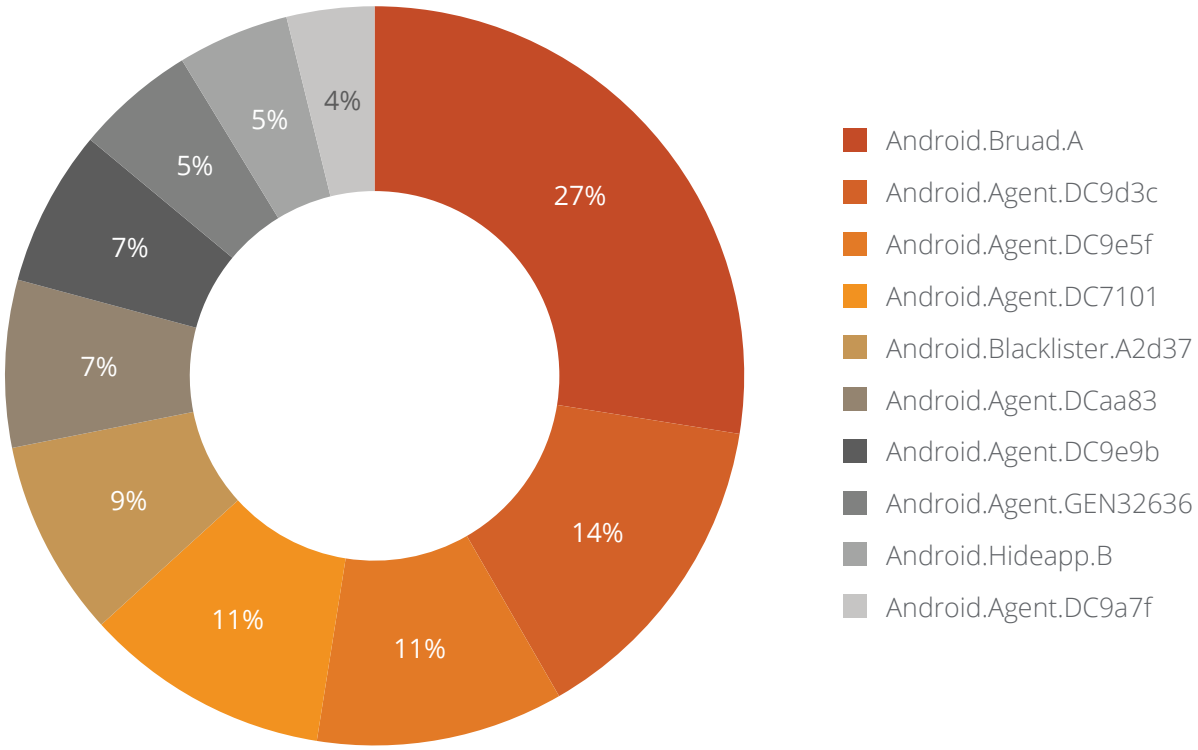
Malware and adware saw equal detections at

29%

Android Detection Highlights 2020

Top Ten Android Malware in 2020

The below figure represents the top 10 Android malware in 2020 based upon their rate of detection in the year.



Observation

Android.Braud.A malware was detected the most in 2020 on Android Operating Systems.

01

Android.Bruad.A (PUP)
Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores

Behaviour:

Android.Bruad.A (PUP) hides its icon after installation and connects to advertisement URLs and sending the infected device's information to a remote server.

02

Android.Agent.DC9d3c
Threat Level: Medium
Category: Malware
Method of Propagation: Third-party app stores and repacked apps

Behaviour:

Android.Agent.DC9d3c makes use of SDK to easily recompile other genuine apps and downloads other apps on the device causing unnecessary memory usage. It also sends the infected device's information to a remote server and displays unnecessary advertisements.

03

Android.Agent.DCaa83
Threat Level: High
Category: Malware
Method of Propagation: Google Play app store

Behaviour:

Android.Agent.DCaa83 attacks Android systems through malicious advertisements. It starts its malicious activity after a certain period to avoid detection

04

Android.Agent.DC9e5f
Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Google Play app store

Behaviour:

Android.Agent.DC9e5f spreads through video calling apps sending the infected device's sensitive information to a remote server after encrypting it.

05

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

Behaviour:

Android.Agent.DC7101 s from the Trojan-Dropper family that attempts infiltration as a genuine-looking application decrypting an encrypted payload to partake in malicious activity.

06

Android.Agent.DC9e9b
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores and repacked apps

Behaviour:

Android.Agent.DC9e9b can draw an overlay window on other applications along with sending the infected device's information to a CnC server.

07

Android.Blacklister.A2d37
Threat Level: Medium
Category: Adware
Method of Propagation: Google Play app store

Behaviour:

Android.Blacklister.A2d37 bombards users with advertisements by pretending to be a fake anti-virus app while having no such capabilities.

08

Android.Agent.GEN32636
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

Android.Agent.GEN32636 decrypts files from asset and drops another Android executable on the device. Dropped file is nothing but Android.Bruad.A adware which shows ads and collects device information to send it to a C&C server

09

Android.Agent.DC9a7f
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

Android.Agent.DC9a7f is from the Trojan-Dropper family collecting sensitive device information and sending it to a CnC server. It downloads malicious applications and installs it.

10

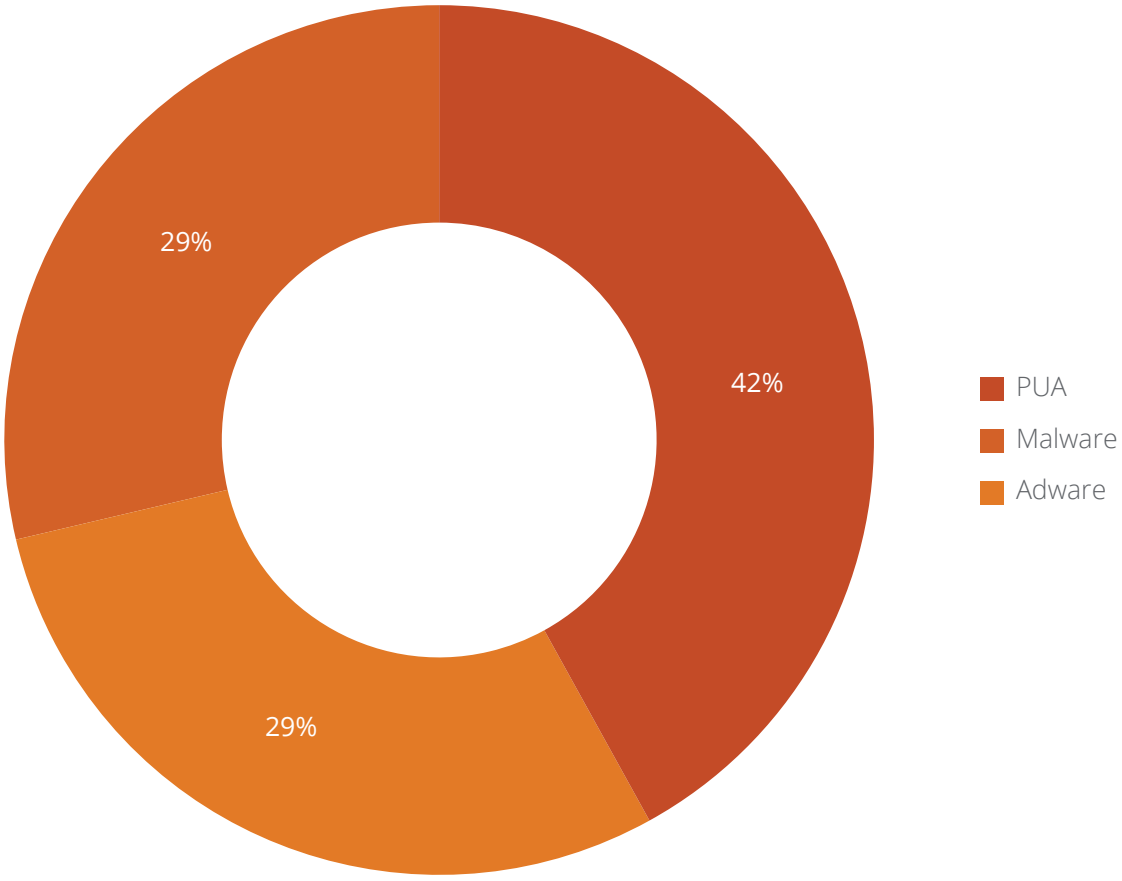
Android.Hideapp.B
Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores

Behaviour:

Android.Hideapp.B hides its icon when first-launched and shows a message like 'Application is unavailable in your country'. Then, it runs services in the background to show fullscreen advertisements, collects sensitive device information and sends it across to a remote server.

Android Detection Statistics

Below figure represents the various categories of Android malware detected by Quick Heal Security Labs in 2020.



Observation

Malware and adware saw equal detections at 29% on Android systems in 2020.

Trends in Android Security

01 Novel Coronavirus- A new way for cyberattacks

Adversaries took advantage of the fact that people all around the world wanted to stay on top of the
information about the omnipresent Coronavirus for most of 2020. Several cunning methods were
deployed by cyberattackers to rip-off unalarmed users. Here is a brief list of attacker tactics –

- Hiding ransomware in Android applications hosted on malicious websites promising to provide real-time information about Coronavirus patients
- Banking Trojans
- Misusing the name, 'AarogyaSetu App' to attempt infiltration
- Scheming under the disguise of providing free Netflix subscription
- Offering free data and free subscriptions
- Faking UPI ID of the 'PM Cares' fund

02 WAPDropper – Dropper with additional functionalities

WAPDropper, a two-part malware, wreaked havoc on Android users by subscribing them to premium services without their knowledge. The malware hides its icon to avoid detection and after performing device checks, send user information to a hard-coded CnC server. Quick Heal Mobile AV detects WAPDropper malware as variants of Android.Agent.DC.

03 Attack by Banking Trojan with additional features

CERBERUS

Cereberus starts with performing complete system integrity checks to avoid detection, sending this information to a CnC server. Depending on the response, it performs malicious activities such as draw overlay or phishing pages of the targeted application, dump user information and data, keylogging, push notifications, etc.

ALIEN

Alien, a part of the new baker family, replicates the behaviour of Cereberus Trojan with some additional features like getting notification content and taking remote access by abusing the team viewer application. Quick Heal mobile AV detects this malware as variants of Android.Hqwar.A.

GHIMOB

GHIMOB typically targets the FinTech sector and spreads through emails and malicious sites where it promotes its malicious apps. It mimics the official apps of Google Defender, Google docs, WhatsApp updater, etc. to get an entry on victims' device to steal sensitive information. Quick Heal Mobile AV detects GHIMOB malware as variants of Android.Agent.A.

Eventbot

Eventbot is a mobile Trojan that steals private and valuable information from mobile banking and financial apps in Android. It hacks into Android's in-built accessibility features and steals data by reading into SMSs, banking PINs, etc. and bypasses the two-factor authentication criteria that most banking apps have.

Predictions for 2021 and beyond

1 Threat Actors to switch from Ransomware to RansomHack: Double - Trouble for Enterprises

Previously, advanced ransomware attacks like WannaCry, Petya, Ryuk, Grandcrab etc. used to only encrypt disks or files and demand a ransom payment in return for a decryption key. Now a new ransomware trend is observed which not only encrypts user files but also exfiltrates private and sensitive information. On denial of ransom, adversaries threaten to release hijacked information in public.

This is double trouble for organizations – exposing sensitive data in public causes severe GDPR implications. In either case, businesses are likely to have to pay to move forward. This tactic is called RansomHack or Double Extortion.

Maze, DoppelPaymer, Ryuk, Lockbit, Netwalker, Mountlocker and Nefilim are few ransomware operators using double extortion techniques. We expect this trend to continue in 2021 as well.

2 Targeted Ransomware attacks on Healthcare and Pharma Sector to Surge

Healthcare and Pharma sector companies that have been in the front lines working to fight against the Coronavirus pandemic are also facing a new wave of ransomware attacks and extortion demands lately. Though few ransomware operators agreed to not attack the healthcare sector during the COVID-19 crisis, several other attack groups have continued to use ransomware against this sector, largely because of the sensitive and personal data of patients they store. Numerous hospitals, COVID-19 research firms and pharma companies have fallen victim to ransomware in the last quarter of '20, making it necessary for them to adopt or deploy a comprehensive set of security solutions.

3 Techniques similar to Operation SideCopy

In September 2020, Seqrite became the pioneer in discovering Operation SideCopy, an Advanced Persistent Threat (APT) attack targeting the Indian Defence Forces. The cunning nature of this attack had so far misled the security community in believing that this was in fact Transparent Tribe.

Similar to Operation SideCopy, which attempted to use techniques similar to some other state-sponsored APTs, there will be similar attacks in 2021 that will attempt to breach critical infrastructure.

4 CobaltStrike: Powerhouse of Ethical Hackers in the Hands of Cyber Criminals

Cobalt Strike is a threat emulation toolkit which is often being used for post-exploitation, covert communication, and browser pivoting, among

other malicious purposes. It can be repurposed to deploy any type of payload, be it ransomware or keylogger.

Ransomware attacks that are now relying on this are Egregor, Ryuk and Lockbit. We have also observed the involvement of 'CobaltStrike' beacons in the recent major backdoor and APT attacks. Recently, the source code of 'CobaltStrike' was leaked on GitHub. This will allow malware authors to make customized changes in the source code or tweak it to evade detections. So, the rise in the inclusion of 'CobaltStrike' beacons in major cyber-attacks will be observed in the coming future.

5 Increase in threats on Remote Work Infrastructure

With the Covid-19 pandemic, almost all organizations have rolled out a remote working model — businesses have introduced tools to facilitate employees to connect to office networks from home and collaborate. Typically, VPNs are used to connect to such networks, whereas video conferencing or chat applications are used to communicate with colleagues — many SMBs have also rolled-out BYOD (Bring Your Own Device).

This new infrastructure must be managed and configured with great precision. IT administrators need to update and patch the software, OS and Antivirus whenever required to defend against exploitation attempts made on this new attack surface. Any new vulnerabilities in such popular applications could be encashed by malware authors as soon as they are reported or discovered.

6 Next wave of Crypto-miners

The cryptocurrency prices are at an all-time high currently and are expected to rise even more in 2021. Cryptocurrencies like Bitcoin and Monero have almost tripled in value in 2020. The booming cryptocurrency values will invite even more threat actors towards developing stealthier crypto-miners and generate higher revenues in 2021.

7 Coronavirus themed threats to divert from precaution-based to prevention-based

In the initial timeframe of the pandemic outbreak, cyber threats were precaution-based where phishing sites, fake mobile apps and malware filenames were related to awareness of coronavirus, symptoms, precaution measures, PPE kits, test kits, lockdown and social distancing.

With the end of the year approaching, the big race among all the pharma companies has led to the creation of several vaccines which are at various stages of testing and approvals. The governments of different countries and states are gearing up for providing vaccines to all its citizens free of cost or at subsidized rates to prevent the virus from infecting and spreading. Hence, now the threats are forecasted to start diverting to a prevention-based theme.

8 New additions in exploits leveraging weak crypto implementations

This year we saw two critical exploits (Curveball and Zerologon) in Windows which were leveraging bugs in Microsoft's implementation of Cryptographic algorithms in different modules. Curveball (CVE-2020-0601) allowed attackers to sign a malware file with anyone's digital certificate, making it look legit.

Zerologon (CVE-2020-1472) made it possible for a low-privileged domain user to take full control of Active Directory domain without any authentication. These exploits were very quickly adopted by hackers in different malware attacks. Considering the high potential of such exploits, security researchers might come across more crypto vulnerabilities in different Windows modules.

9 Deep-fakes to cyber-frauds

Deep-fakes are fake/manipulated video or audio clips of a person, created using deep learning technology. This can be used to create fake news and carry out cyber frauds. A company's CEO featuring in a deep-fake video asking colleagues or employees to transfer funds is a classic example of deep-fake video. Expect more of these in 2021.

10 Automation in performing phishing attacks

Hackers have been increasingly seen using automation in performing phishing attacks. This trend will continue — a variety of social engineering tricks will be used to lure into giving up on sensitive information in 2021.

11 Attacks on Red Team tools

Cybersecurity vendor FireEye's Red Team tools were recently stolen in a massive cyberattack. These tools were used in 'Red Teaming Exercises' to demonstrate the "impacts of successful attacks" for clients. The stolen tools range from simple scripts used for automating reconnaissance to entire frameworks that are similar to publicly available technologies such as CobaltStrike and Metasploit.

Many of the Red Team tools have already been released to the community and are already distributed in the open-source virtual machine, CommandoVM. This will allow access to internal systems and fetch critical information of organizations. Attacks comprising the application of Red Team tools will be observed in the coming future.

12 Increase in attacks related to mobile banking

In September 2020, Cerberus mobile banking trojan's source code was released for free on underground hacking forums. Following this, an immediate rise in mobile app infections was seen. It is expected that far more advanced variants of mobile banking malware based on Cerebrus's code will emerge next year with new techniques and payloads.

Inference

Bidding farewell to an unforgiving 2020, the year has seen a completely different brand of attacks as compared to 2019. While both, Windows and Android users faced the onslaught of Coronavirus-themed attacks, Trojans, ransomware, adware, spyware and theft of sensitive information was common. With users forced to prioritize on establishing the new normal, adversaries took maximum advantage to breach the transition.

As the new year begins, it is presumed that adversaries have completed their transition and have synced-in to strategize cyberattackers through established and emerging channels. Our cybersecurity predictions for 2021 and beyond, forecasts a likely cybersecurity landscape for this year. The cunning ways of attackers however never lack the element of surprise and ensure that there is always room for more.

Stay protected in 2021 by leveraging a broad range of Quick Heal solutions to protect from advanced threats.