Quick Heal

Security Simplified

QUARTERLY THREAT REPORT Q1-2019

www.quickheal.com

Table of Contents

Contributors

- Quick Heal Security Labs
- Quick Heal Marketing Team

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

Introduction

The very first quarter of 2019 seemed to bring in some significant detections with Quick Heal Security Labs detecting over 434 Million Windows malware. The year started on a high note with January clocking the highest detection of 162 Million windows malware. On a daily basis, Quick Heal detected around 4 Million malware including 22K Ransomware, 0.5 Million exploits, 0.4 Million PUA and Adware and 69K Cryptojacking malware.

The Trojan horse category retained its position as the most dominant malware in the first quarter of 2019. Trojan.Starter.YY4 was detected to be the topmost Windows Malware, with around 25 Million detections made in Q1 of 2019 while PUA.Elex topped the list of PUA and Adware, with around 5 Million detections.

Cryptojacking & Ransomware is a dangerous threat, which threatens to cause havoc in 2019. Our threat report suggests that over 69K Cryptojacking & 22K Ransomware malware were detected in Q1 2019 every single day. Considering the widespread popularity of crypto-currency, this threat is likely to become even more popular among cyber criminals in the time ahead.

Our threat report suggests that every minute 3K malware were detected by Quick Heal. Quick Heal Security Labs observed continued attack using RDP and SMB brute force. Criminals constantly look for unsecured RDP, SMB services to exploit and access system & networks. Ransomware like Dharma, CrySis were distributed through hacked RDP or SMB share by brute forcing.

The first quarter of the year also witnessed Quick Heal Security Labs detecting over 0.15 Million malware, PUA and Adware on Android OS. Android.Agent.GEN14722 was detected to be the topmost Android malware of Q1.

A significant trend observed right in the beginning of the year on the Android front where the fake apps including fake antivirus apps on play store that easily recompile other genuine apps and share user information with a remote server. Quick Heal Security Lab observed around 28 fake apps & 24 fake antivirus apps on Google Play Store.

Yet another trending android malware was the Trojan banker malware that is designed to achieve goals like steal credentials and gain access to SMS messages received on the compromised devices to bypass SMS-based 2-factor authentication.

Word of caution – “User’s sensitive information will always be the target, no matter from which device the user is connected to the internet.”

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

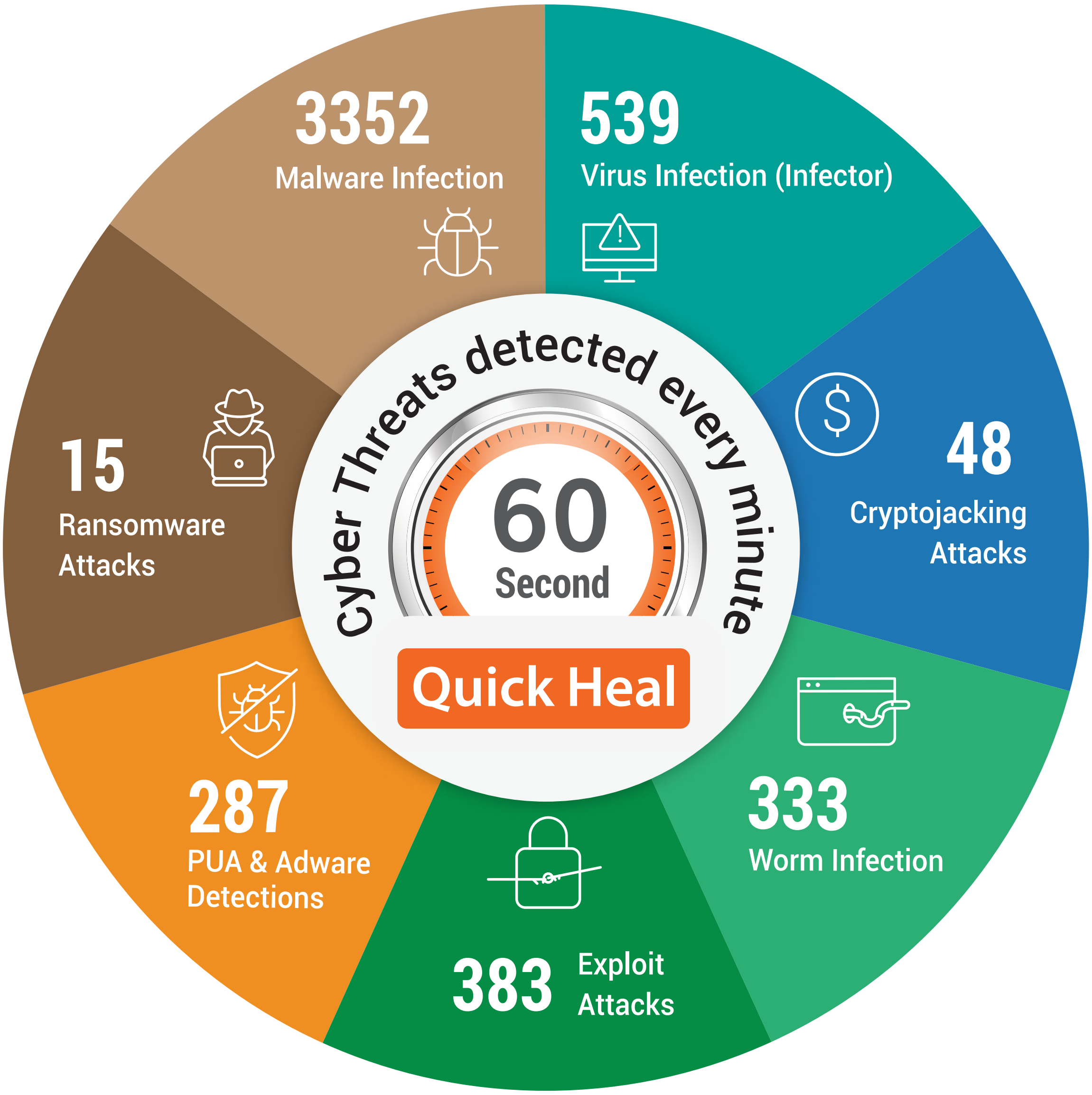
A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

www.quickheal.com

Follow us on:

WINDOWS

Malware Detections Highlights – Q1 2019



Cyber Threats detected every minute

60 Second

Quick Heal

3352 Malware Infection

539 Virus Infection (Infector)

48 Cryptojacking Attacks

333 Worm Infection

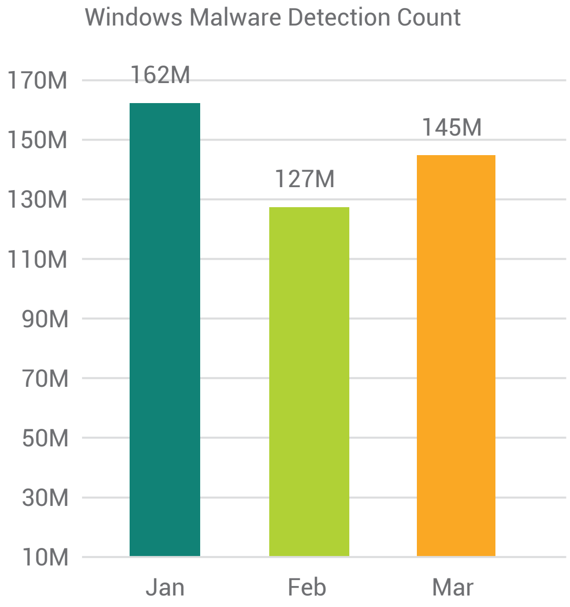
383 Exploit Attacks

287 PUA & Adware Detections

15 Ransomware Attacks

Malware Detection Statistics - Month Wise

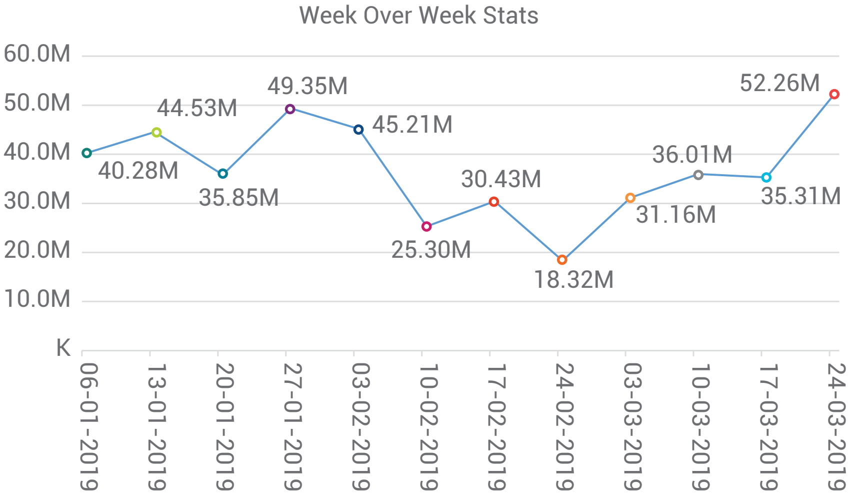
The below graph represents the statistics of the total count of malware detected by Quick Heal during the period of Jan to Mar in 2019.



Observations

- Quick Heal detected over 434 million Windows malware in Q1 2019.
- Jan clocked the highest detection of Windows malware.

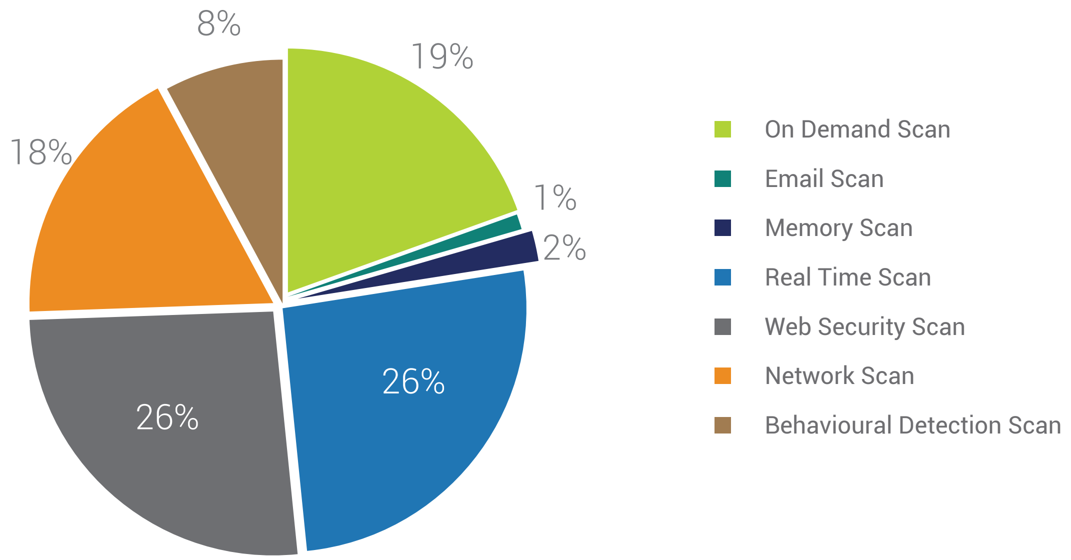
Malware Detection Statistics – Week-Over-Week



Observations

- While the month of Feb showed a major dip in malware detection count, the detections began to rise thereon with the last week of March clocking the highest detections.

Malware Detection Statistics - Protection Wise



Observations

- Maximum malware detections were made through Real Time Scan and Web Security Scan.

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 program running & cleans it.

Email Scan

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

Web Security Scan

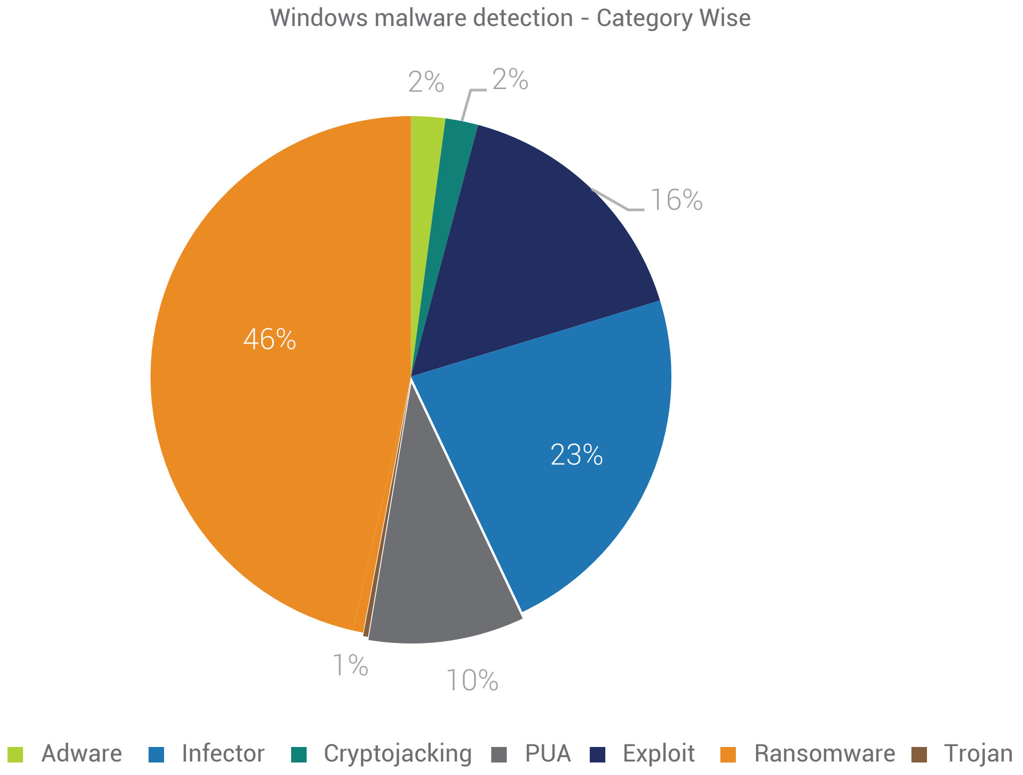
Automatically detects unsafe and potentially dangerous websites, and prevents you from visiting them.

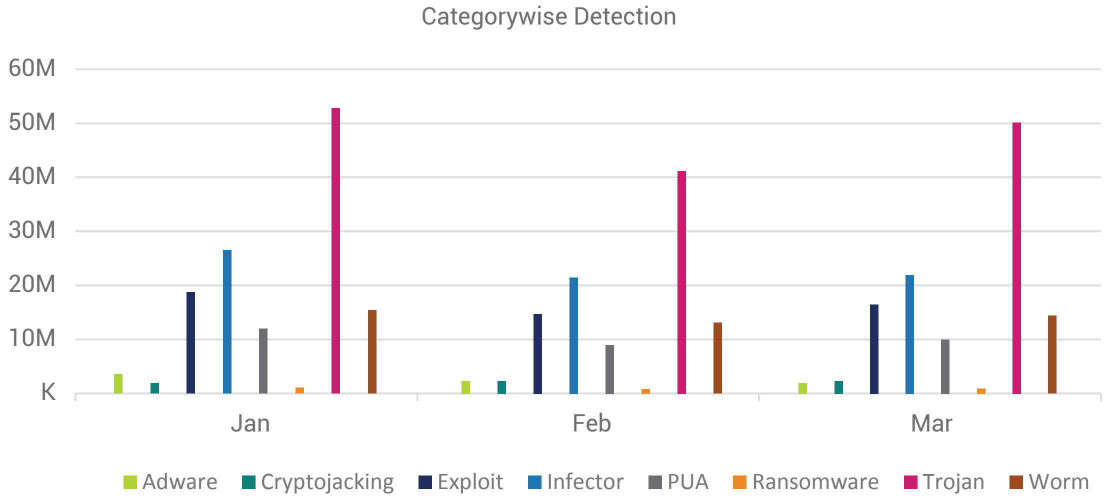
Network Scan

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

Malware Detection Statistics – Category Wise

Below figure represents the various categories of Windows malware detected by Quick Heal in Q1 2019.



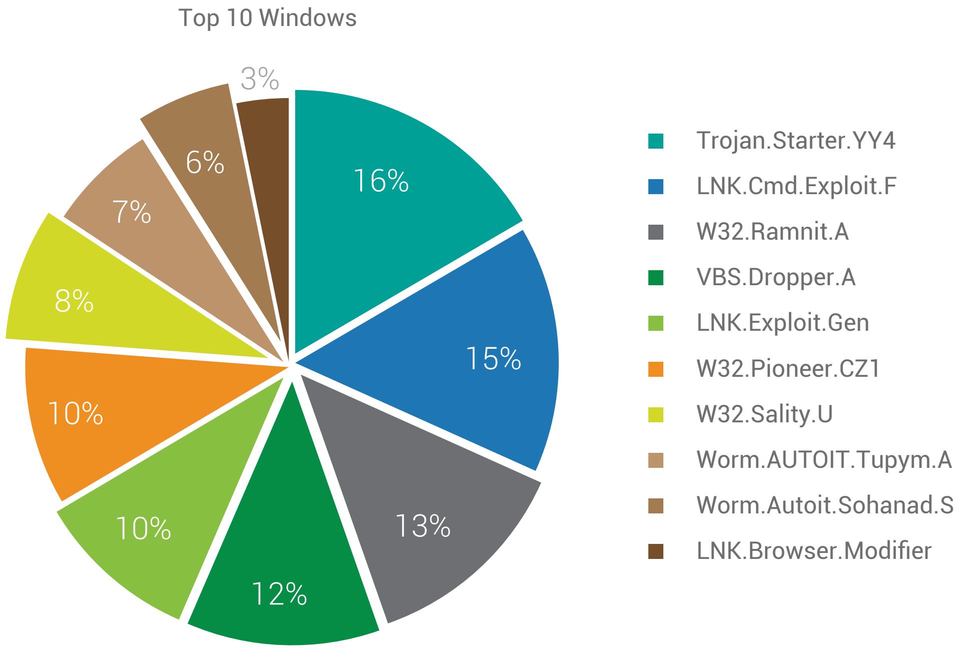


Observations

- Trojan malware was found to clock the maximum detection of 46% in Q1 2019.

Top 10 Malware

The below figure represents the Top 10 Windows malware of Q1 2019. These malware have made it to this list based upon their rate of detection from Jan to March.



Observations

- In 2019, Trojan.Starter.YY4 was detected to be the top Windows Malware, with around 25 Million detections made in Q1 of 2019.

1. 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 the infected system to crash.
- Downloads other malware like keyloggers and file infectors.
- Slows down the booting and shutting down process of the infected computer.
- Allows hackers to steal confidential data like credit card details and personal information from the infected system.

2. LNK.Cmd.Exploit.F

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.

3. W32.Ramnit.A

Threat Level: Medium

Category: Virus

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 modifies registry entries to ensure its automatic execution at every system start up.

4. VBS.Dropper.A

Threat Level: Medium

Category: Dropper

Method of Propagation: Web page

Behavior:

- 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.

5. LNK.Exploit.Gen

Threat Level: High

Category: Trojan

Method of Propagation: Bundled software and freeware

Behavior:

- It is a destructive Trojan virus that could hide in spam email attachments, malicious websites and suspicious pop-ups.
- This kind of virus can be installed on Windows systems by using illegal browser extensions.
- It changes some of the system files without the user knowing about it. Next time the user launches the Windows system, this virus will run in the system background and spy on their activities. In order to redirect the user to dubious websites, the virus modifies system hosts file and hijacks the IP address.

6. W32.Pioneer.CZ1

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behavior:

- Malware injects its code to files present on disk and shared network. It decrypts malicious dll present in the file & drops it. This dll perform malicious activity and collect system information & send it to CNC server.

7. W32.Sality.U

Threat Level: Medium

Category: Polymorphic 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.

8. 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.

9. Worm.Autoit.Sohanad.S

Threat Level: Medium

Category: Worm

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

Behavior:

- It arrives to your computer through Messaging apps, infected USB or network. It has ability to spread quickly. After arrival it creates copy of itself as exe with typical windows folder icon. User mistakenly executes this exe assuming it as a folder and then it spreads over network. It infects every connected USB drive too.

10. LNK.Browser.Modi¬er

Threat Level: High

Category: Trojan

Method of Propagation: Bundled software and freeware

Behavior:

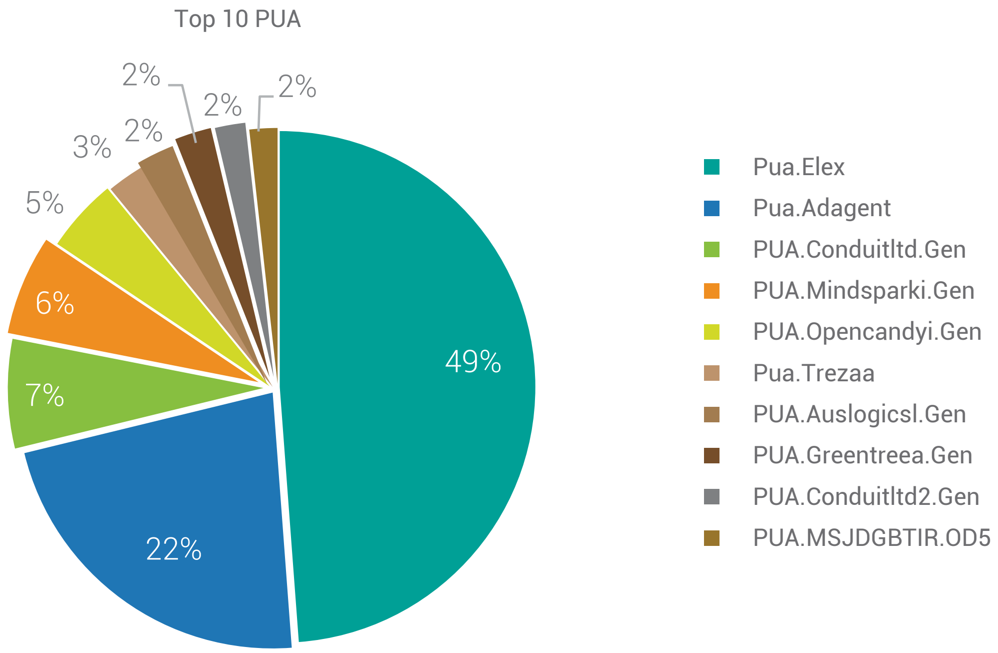
- Injects malicious codes into the browser which redirects the user to malicious links.
- Makes changes to the browser's default settings without user knowledge.
- Generates ads to cause the browser to malfunction.
- Steals the user's information while browsing like banking credentials for further misuse.

Top 10 Potentially Unwanted Applications (PUA) and Adware

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 by Quick Heal in Q1 2019.

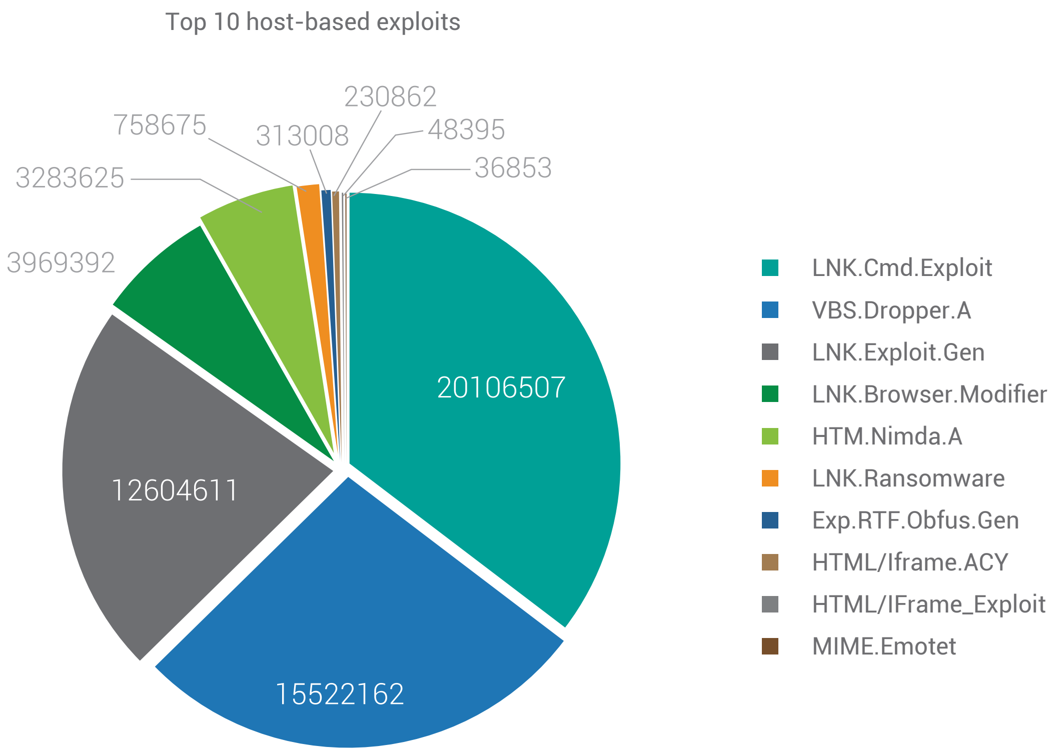


Observations

- In 2019, PUA.Elex was detected to be the top PUA, with around 5 Million detections made in 2019.

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 Windows exploits of Q1 2019.

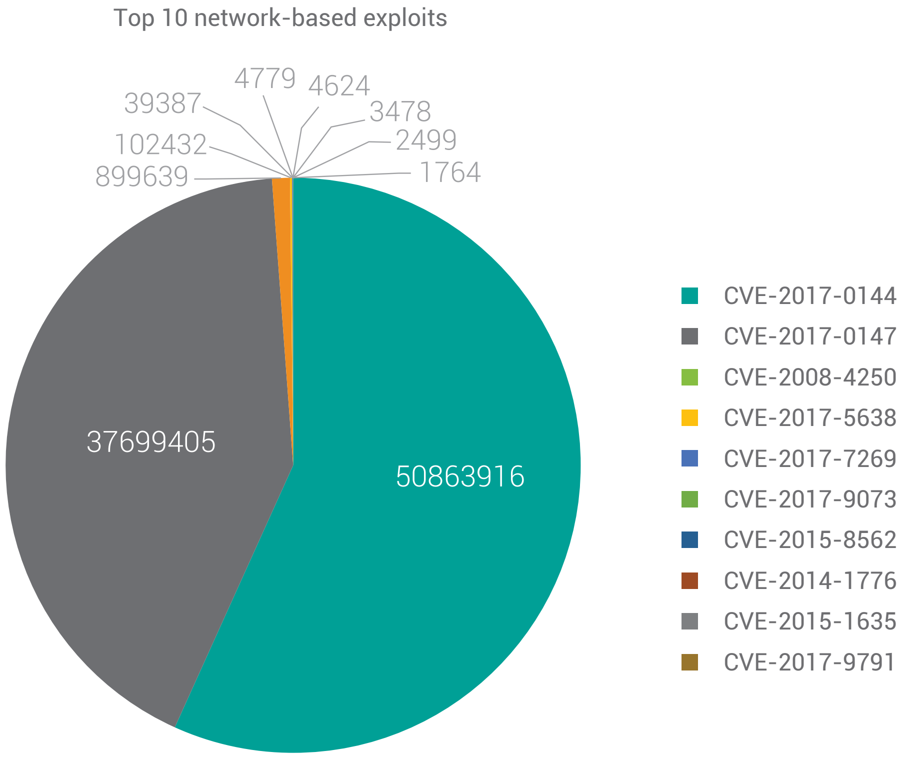


What are host-based exploits?

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 10 Network-Based Exploits

Below figure represents the top 10 Network-Based Windows exploits of Q1 2019.



What are host-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).

Trends in Windows Security Threats

1. Insecure Remote Desktop & SMB

Quick Heal Security lab observed continuous attack using RDP and SMB brute force. Criminals look for unsecured RDP, SMB services to exploit and access enterprise networks. Ransomware like Dharma, CrySis distributed through hacked RDP or SMB share by brute forcing. RemoteDesktop Protocol (RDP) is widely used for remotely connecting to Windows systems, whereas, Server Message Block (SMB) Protocol is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.

Brute Force Attack: A brute force attack is a trial-and-error method used to retrieve critical information such as usernames and passwords. A brute force attack is generally carried out through automated scripts.

RDP Brute Force Attack: The Remote Desktop Protocol (RDP) running on default port 3389. By brute forcing the user credentials to access the RDP on a victim's machine, attackers can uncover usernames and passwords. Once credentials are obtained, attacker gets the ability to carry out any type of attack.

SMB Brute Force Attack: The Server Message Block (SMB) Protocol running on port 445, is targeted with a typical brute force attack using Metaspolite. As a result of the brute force, the attacker gets reverse meterpreter shell. Then attacker can create new user with administrative rights on victim's machine. Once attacker creates user, he gets the ability to carry out any type of attack.

Many organizations fail to secure RDP services against unauthorized access. It is strongly advised to protect it by setting up appropriate configuration (For eg. Firewall, Do not keep RDP over Public Network). Keep Operating System up to date. Along with setting up complex password; password expiration & account lockout policies should also be implemented. Most important – ***Keep backup of important data.***

2. A 19-year-old vulnerability in WinRAR (CVE-2018-20250)

Few days back, researchers at Israel based cyber security vendor reported a 19 year old code execution vulnerability in the WinRAR tool. WinRAR is widely used tool for compression and decompression of multiple archives. This vulnerability affected over 500 million users of this program. This vulnerability is absolute path traversal bug while extracting ACE archives. Attacker can craft and embed malware payload in ACE archive with rar extension. When a vulnerable version of WinRAR is used to extract such crafted ACE archive, the malicious payload by attacker is extracted in start-up folder and executed by system next time when system restarts.

Past discloser of this vulnerability, attackers have started exploiting this vulnerability to distribute ransomwares. According to security forums, many APT campaigns have started exploiting this vulnerability to distribute their payload.

3. GandCrab Riding Emotet's Bus!

Emotet is known for constantly changing its payload and infection vectors like spam mail, malicious doc and even malicious JS files. It compromised a very high number of websites on the internet. Emotet malware campaign has existed since 2014. Most of the websites are genuine but somehow tricked into delivering Emotet. But this time, some of these websites were seen delivering the infamous GandCrab Ransomware V 5.1 for some time. The payload was downloaded through a malicious doc on the victim's computer using VBA macro. The PowerShell script from macro connected to the compromised website and downloaded GandCrab Ransomware from the URL. The GandCrab v5 ransomware has started using task scheduler ALPC vulnerability to gain System privileges on an infected computer. After encryption, it asks for $700 in dash/bitcoin cryptocurrency; also 10% charges are applicable for miner fees/commission.

Ref - https://blogs.quickheal.com/gandcrab-riding-emotets-bus/

4. Anatova, A modular ransomware

Recently, Quick Heal Security Labs has observed the first ransomware of 2019 — 'Anatova'. During our analysis, we found that Anatova is not just ransomware but a modular one. By modular ransomware we mean, though the main activity of this ransomware will be encrypting the data. Once the ransomware enters the system, it uses anti-analysis technique in which, it checks user name and compares the user name with the stored blacklisted user names. If a user name is not in the list, it starts the encryption of files. Unlike other Ransomware, Anatova encrypts the files but, it doesn't add any extension to the encrypted files. To save the hassle and not to encrypt the same file again, it adds a marker to the encrypted content of 4 bytes at the end of the file. Smartly, this ransomware encrypts files whose size is =<1MB, and if the size is more than 1 MB then it will only encrypt the data of 1 MB from that file. Anatova not only encrypts system drives but also checks remote location to encrypt. It checks for all instances, DRIVE_FIXED to check the local drives and DRIVE_REMOTE to verify remote (network) location. After encryption and deletion of the shadow copies, ransomware deletes itself. Anatova demands ransom payment in crypto currency of 10 DASH which calculates to somewhere around $700 USD.

Ref - https://blogs.quickheal.com/anatova/

ANDROID

Quick Heal Detection on Android

Quick Heal Detection on Android

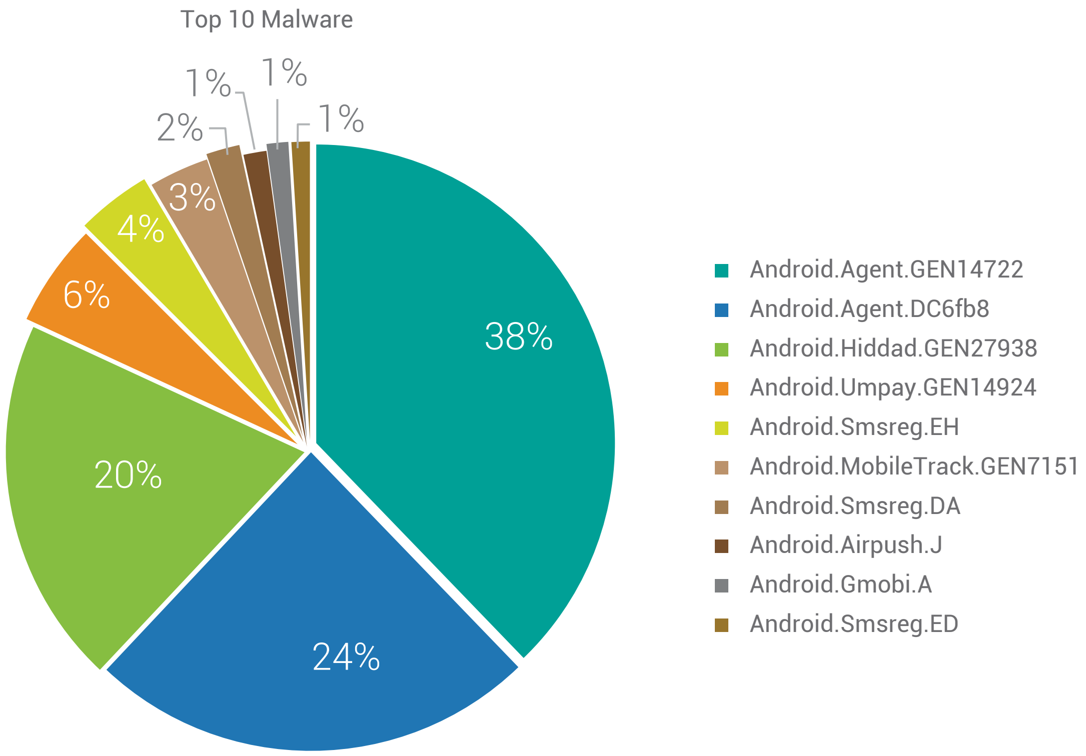
Malware: 116K
Per Day: 1294
Per Hour: 54

Adware: 5K
Per Day: 56
Per Hour: 2

Potentially Unwanted Application (PUA): 32K
Per Day: 359
Per Hour: 15

Top 10 Malware

Below figure represents the top 10 Android malware of Q1 2019. These malwares have made it to this list based upon their rate of detection during the period of Jan to March in 2019.



1. Android.Agent.GEN14722

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores (Other than Google Play Store)

Behavior:

- Once launched, it hides its icon and works in the background.
- It can download other applications and prompt to install them.
- The downloaded applications can be malicious and infect the device further.
- Downloaded application may steal user information and send it to a malicious server.

2. Android.Agent.DC6fb8

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- Hide its icon after installation & disguise itself as system update.
- Connects to advertisement URLs to show advertisement.
- It sends the infected device's information such as country, model, vendor, OS version IMEI, IMSI, model number, and location to a remote server.

3. Android.Hiddad.GEN27938

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- Hide its icon after installation.
- Connects to advertisement URLs and sends the infected device's information such as IMEI, IMSI, model number, and location to a remote server.

4. Android.Umpay.GEN14924

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- Umpay is a Chinese mobile payment SDK, which allows developers to request payments through Web, WAP & SMS.
- The SDK has many capabilities to make payment process easier & secure for app developers.
- Capabilities include sending SMS, collecting GPS location, intercept SMS, and checking if a device is rooted or not. It has been observed that some apps are misusing this SDK to earn money.
- It is used to send SMSs to premium numbers without user consent & for the collection of user information.

5. Android.Smsreg.EH

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- It sends device IMEI and IMSI to premium rate numbers via SMS.
- It collects device data like SDK type, SDK version, phone company, phone number, etc.

  It sends the collected data to a remote server

6. Android.MobileTrack.GEN7151

Threat Level: Low

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- It's a mobile tracker application.
- Sends the user's device location via SMS to an external server.
- Checks if the device's SIM is changed or not by identifying the IMSI number.
- Sends a SMS after SIM change or phone reboot with specific keywords in the body.
- Collects device information such as IMEI and IMSI numbers

7. Android.Smsreg.DA

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- Asks targeted Android users to make payments through premium rate SMSs in order to complete their registration.
- Collects personal information such as phone numbers, incoming SMS details, device ID, contacts list, etc., and sends it to a remote server.

8. Android.Airpush.J

Threat Level: Low

Category: Adware

Method of Propagation: Third-party app stores and repacked apps

Behavior:

- Displays multiple ads while it is running.
- When the user clicks on one of these ads, they get redirected to a third-party server where they are prompted to download and install other apps.
- Shares information about the user's device location with a third-party server.

9. Android.Gmobi.A

Threat Level: High

Category: Adware

Method of Propagation: Third-party app stores and repacked apps

Behavior:

- Makes use of SDK (Software Development Kit) to easily recompile other genuine apps.
- Downloads other apps on the device causing unnecessary memory usage.
- Shares the infected device's information such as location and email account with a remote server.
- Displays unnecessary ads.

10. Android.Smsreg.ED

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

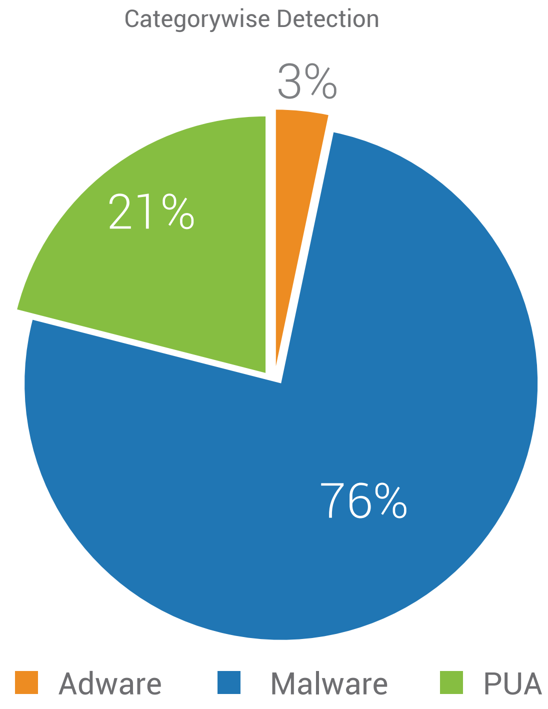
Method of Propagation: Third-party app stores

Behavior:

- Masquerades as a gaming app. Asks money from the player via premium-rated SMSs to play the next stage or to get extra lives in the game.
- Collects personal information such as device ID, phone number, and incoming messages before transmitting the stolen data to a remote server.

Android Detection Statistics: Category Wise

Below figure represents the top 10 Android malware of Q1 2019. These malwares have made it to this list based upon their rate of detection during the period of Jan to March in 2019.

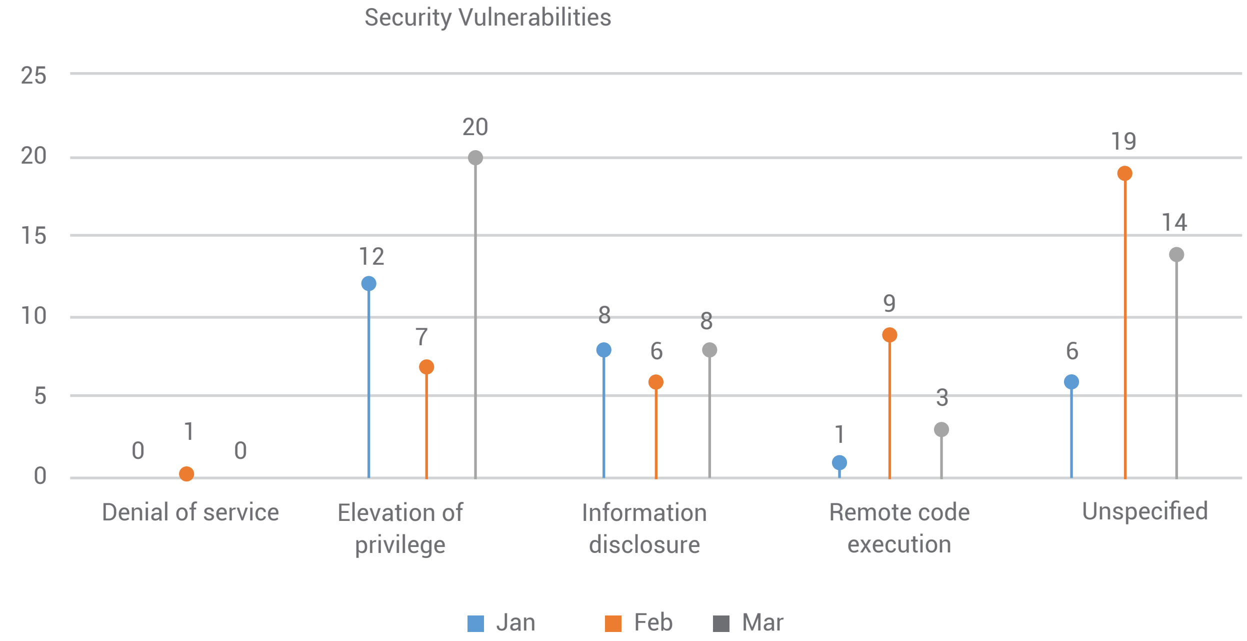


Observations

- Malware clocked 76% of the total Android malware detectons in Q1 2019.

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 Jan to March of 2019.



Source: https://source.android.com/security/bulletin/2019

Trends in Android Security Threats

1. A Rising trend in Android - Fake applications

Fake Apps have increased in recent years. These apps use similar icon, app name, developer name and even their description to manipulate users into downloading them and to deceive users. Some fake apps even have good ratings and high download counts as compared to the original app. Android fake applications use the fame of other genuine popular apps to attract more users. There are fake apps for almost every popular app, including Google Play, WhatsApp, Flash Player Some of them make their way to Google Play also.

Quick Heal Security Labs had reported to Google Play Store about 28 Fake Apps, which were then removed from Google Play Store. These apps don't have any legitimate functionality related to App name. Developer develop these apps only for earning money by showing advertisements.

Additionally, Quick Heal Security Lab also observed around 24 fake antiviruses on Google Play Store. These Fake AV looks like genuine one but detect them self as well as other clean applications as a malware. They have maintained a whitelist and blacklist application. If application does not come under whitelist they declare the installed application malicious.

Malicious author keeps on uploading such fake application just to get revenue through advertisement and to increase install count or just can led to any financial fraud.

Read more: https://blogs.quickheal.com/28-fake-apps-removed-google-play-store-post-quick-heal-security-lab-reports/

2. Banking malwares found on play

Another trend in Android malware from previous few months is the banking Trojan. Android banking trojan on Google Play store have increased. There are two main types of banking malware - sophisticated banking Trojans and fake banking apps. Malware in both these categories is designed to achieve the same goals like steal credentials and gain access to SMS messages received on the compromised devices to bypass SMS-based 2-factor authentication. Last year, three fake credit card apps were removed from Google play store.

3. Vulnerability detected!

Google has reported a serious bug in the Android security bulletin. It reveals a new method which can allow hackers to attack Android smartphone by using malicious PNG files. The flaw found in Android deals with one of the three vulnerabilities identified in the Android framework and it is one of the most critical security issues for this month's security update, that affect millions of devices running recent versions of Google's mobile operating system. One of the three vulnerabilities, which Google considered to be the most severe one is a major flaw in Android's framework that allows an attacker to execute computer code remotely by using a maliciously crafted PNG image file that could allow a maliciously crafted Portable Network Graphics (.PNG) image file to execute arbitrary code on the vulnerable Android devices to smuggle the code. The malware can start running on the device with high-level privileges just by opening the evil PNG file on a chat app or email.

However, several third-party device makers take weeks or months to roll out security patches to their phones, so it leaves your device vulnerable until handset receives the 2019 February update. The vulnerabilities, identified as CVE-2019-1986, CVE-2019-1987, and CVE-2019-1988, have been patched in Android Open Source Project (AOSP) by Google as part of its February Android Security Updates.

Since Google hasn't released the technical details of the flaw, so it won't be easy for anyone to abuse this hacking method. Also, no cases have been reported yet of anyone exploiting the vulnerability. This isn't the first time when PNG files are flagged as dangerous because they can be rigged easily. And it is very easy to send a harmless-looking PNG file to victims over chat, email or social media which in turn triggers the device to download malware.

4. Malwares can intercept copied data

We all know the addresses of cryptocurrency wallets are long strings of characters. Instead of typing them, we very casually copy this address and paste it in respective applications using the clipboard. Clipper malware takes advantage of this. It intercepts the content of the clipboard and replaces it with the attacker cryptocurrency address. Previously, this type of malware was seen in Windows and now it is also found for android. This malware was seen for the first time in February 2019 on Google Play.

Conclusion

The first quarter of 2019 started on an exciting note with Quick Heal Security Labs observing an upswing in Ransomware activity and banking malwares. In fact, a new form of malware has been detected known as the "clipper malware" that intercepts the content of the clipboard where the address of cryptocurrency wallets is usually pasted and replaces it with the attacker cryptocurrency address.

While Ransomware continues to be the preferred money-maker for cyber criminals, it is soon getting replaced by Cryptojacking. According to reports by Quick heal Security Labs, there were total 6 Million Cryptojacking detections made in Q1 of 2019 as against just 1 Million Ransomware detections.

These facts and figures go on to explain that while the counts of Ransomware and Cryptojacking detections may continue to vary across the quarters, there's no denying the fact that both of them are here to last for long and will continue to evolve.

And, so it is extremely important that we gear up our security systems and upgrade to robust antivirus software to put up a strong fight against the evolving threat landscape.

Additionally, it is also a good practice to take regular backups of your work, so that your critical data does not get compromised in the event of a malware attack. Today, data is most important factor, may it be an individual or a business. Modern businesses depend heavily on the continuous availability of data, be it of the customer, product, employee or financial. Data backups, in such cases, are the life savers for business. There are many instances where businesses have suffered the loss of data but were able to get back on their feet very quickly because they were wise enough to back-up their data. Backups restore the data quickly and enable the business to continue its operations.

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