Quick Heal

Security Simplified

QUARTERLY THREAT REPORT Q2-2019

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 second quarter of 2019 had comparatively lesser detections of around 242 million Windows malware as compared to Q1 of 2019. The quarter started on a high note with April clocking the highest detection of 82 Million windows malware. On a daily basis, Quick Heal detected around 2.5 Million malware including 10K Ransomware, 0.2 Million exploits, 0.2 Million PUA and Adware and 35K Cryptojacking malware.

The quarter started with some unpleasant incidences of phishing attacks, data breach and data leaks like the breach of Indian IT outsourcing giant Wipro Ltd. Phishing scams were back in trend with Quick Heal Security Lab noticing a sudden increase in Spear Phishing attacks. Also trending were the RDP (Remote Desktop Protocol) based attack, specially using botnet. A latest botnet - ***GoldBrute*** has attacked more than 1.5 million systems.

The Trojan horse category continued to top the chart as the most dominant malware in the second quarter of 2019. Trojan.Starter.YY4 was detected to be the topmost Windows Malware, with around 13 Million detections made in Q2 of 2019 while PUA.Elex topped the list of PUA and Adware, with around 2 Million detections.

Our threat report suggests a rise in Ransomware attacks with around 10k Ransomware being detected every day. Quick Heal Security Labs have observed a rise in ***Stop Ransomware*** which was initially discovered in December 2017 and new variants have started reappearing since August 2018. The STOP Ransomware is distributed using spam emails, MS office attachments, repackaged and infected installers of popular programs and pirated activators etc.

The second quarter of the year also witnessed Quick Heal Security Labs detecting over 0.13 Million malware, PUA and Adware on Android OS. Android.Agent.GEN14722 was detected to be the topmost Android malware of Q2.

The second quarter of the year witnessed malware's ability to convert clean applications into malicious one, with the help of vulnerabilities in the Android OS. Mid May witnessed a vulnerability discovered in ***WhatsApp*** that allows hacker to install a spyware remotely with single VoIP call on target phone. While the vulnerability has been patched, users are advised to update installed applications.

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

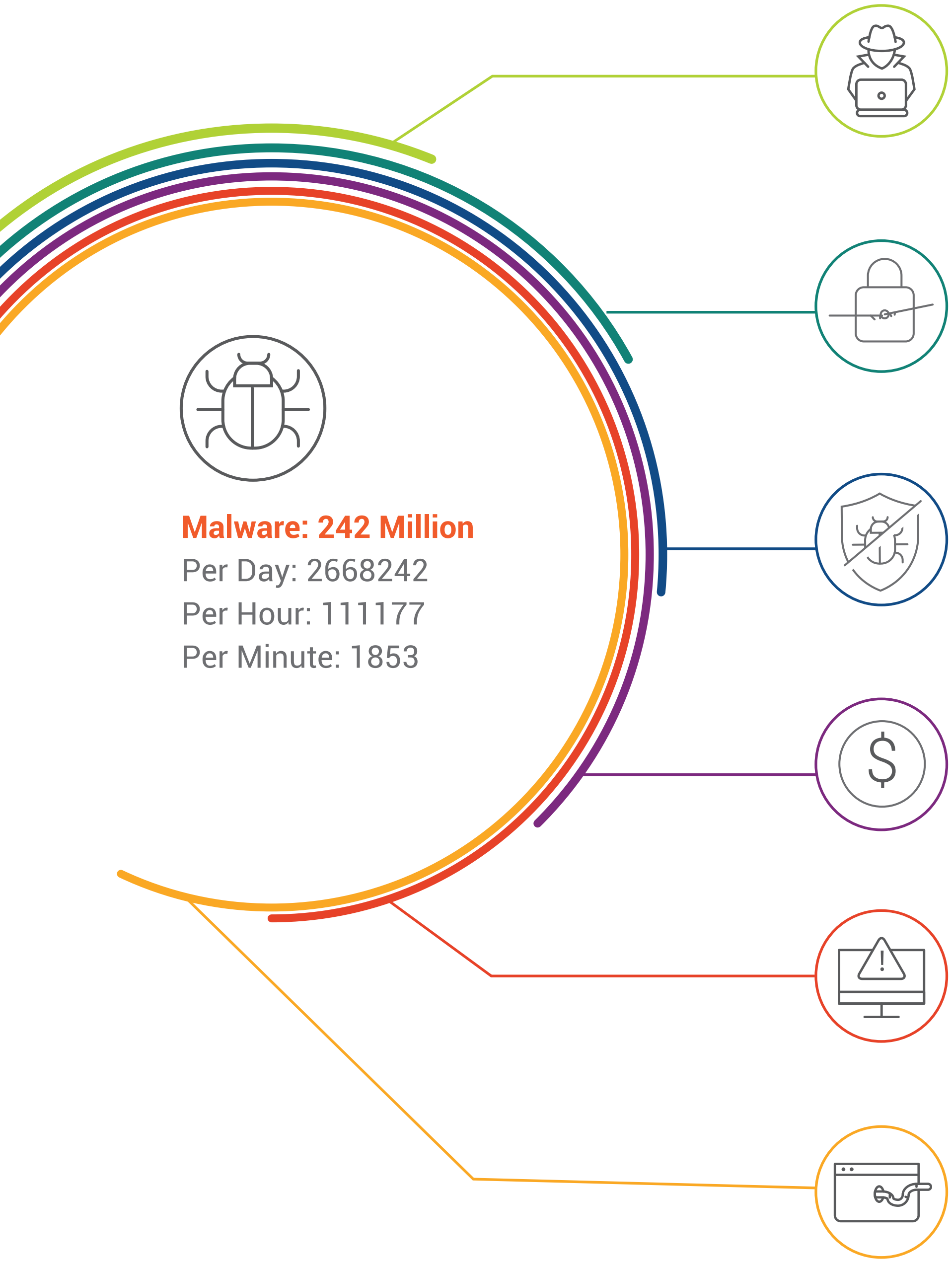
A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

www.quickheal.com

Follow us on:

WINDOWS

Detections Highlights - Q2 2019



Malware: 242 Million
Per Day: 2668242
Per Hour: 111177
Per Minute: 1853

Ransomware: 0.9 Million
Per Day: 10260
Per Hour: 428
Per Minute: 7

Exploit: 23 Million
Per Day: 263386
Per Hour: 10974
Per Minute: 183

PUA & Adware: 19 Million
Per Day: 215653
Per Hour: 8986
Per Minute: 150

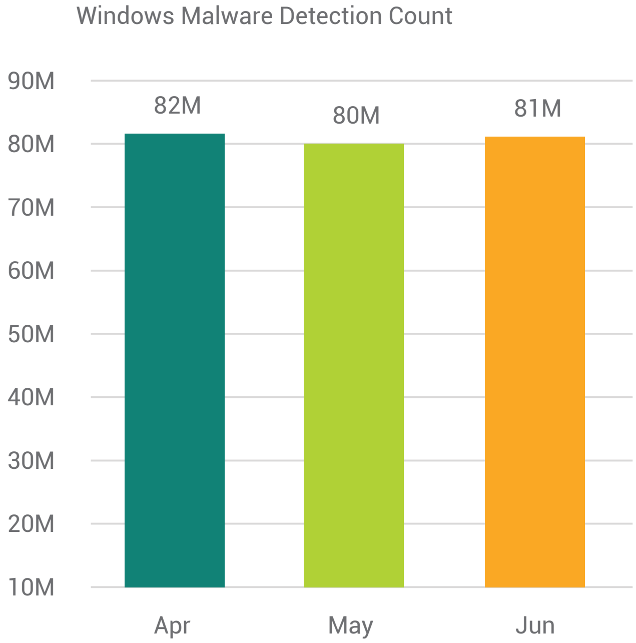
Cryptojacking: 3 Million
Per Day: 35923
Per Hour: 1497
Per Minute: 25

Infector: 37 Million
Per Day: 415176
Per Hour: 17299
Per Minute: 288

Worm: 23 Million
Per Day: 256811
Per Hour: 10700
Per Minute: 178

Detection Statistics - Month Wise

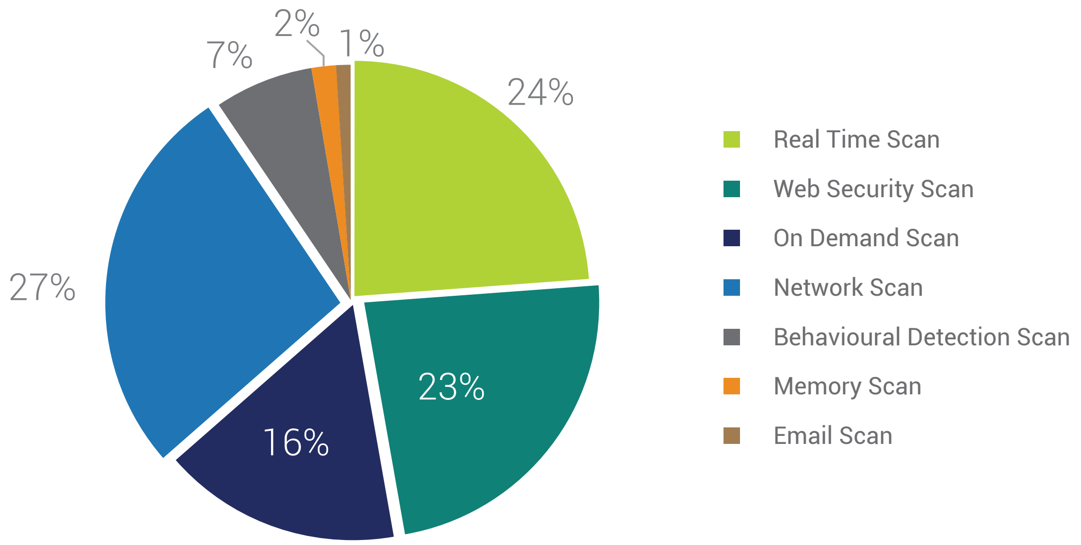
The below graph represents the statistics of the total count of malware detected by Quick Heal during the period of Apr to Jun in 2019.



Observations

- Quick Heal detected over 242 million Windows malware in Q2 2019.
- April clocked the highest detection of Windows malware.

Detection Statistics Protection Wise



Observations

- Maximum malware detections were made through Network Scan and Real Time 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

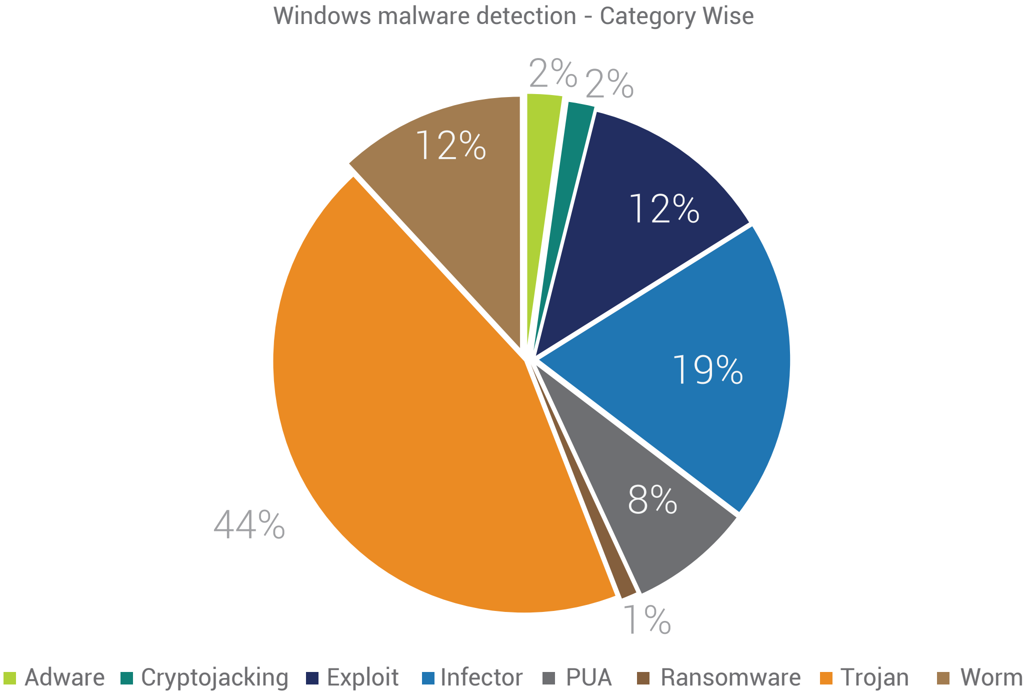
Automatically detects unsafe and potentially dangerous websites and prevents you from visiting them.

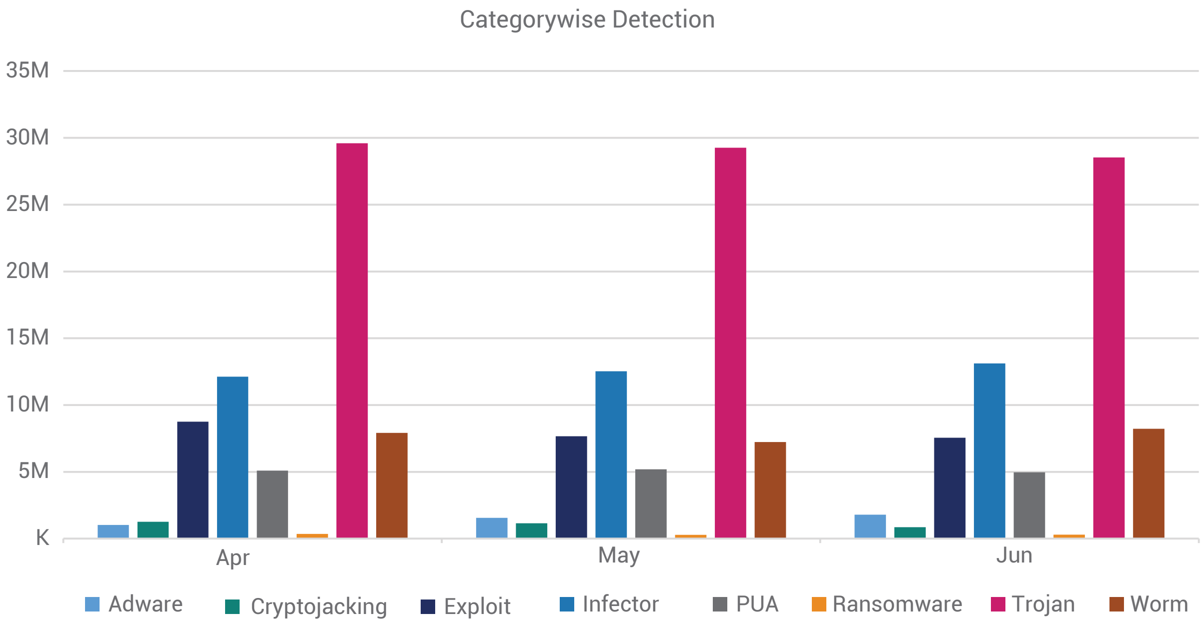
Network Scan

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

Detection Statistics - Category Wise

Below figure represents the various categories of Windows malware detected by Quick Heal in Q2 2019.



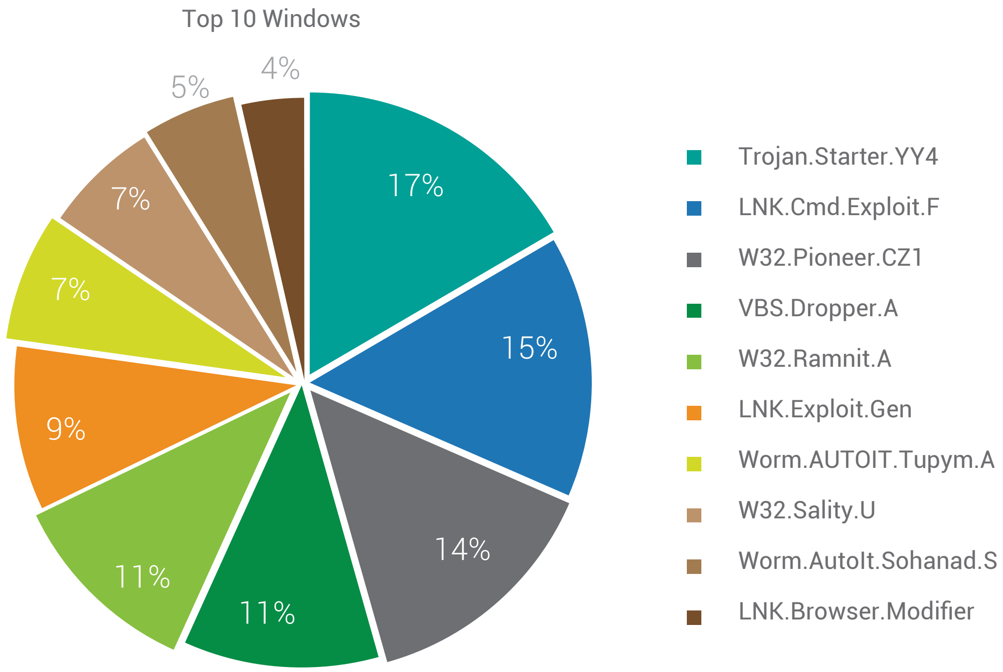


Observations

- Trojan malware was found to clock the maximum detection of 44% in Q2 2019.

Top 10 Malware

The below figure represents the Top 10 Windows malware of Q2 2019. These malware have made it to this list based upon their rate of detection from Apr to Jun.



Observations

- Trojan.Starter.YY4 was detected to be the top Windows Malware, with around 13 Million detections made in Q2 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 a system crash.
- Downloads other malwares like keyloggers.
- 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.Pioneer.CZ1

Threat Level: Medium

Category: File Infector

Method of Propagation: Removable or network drives

Behavior:

- The malware injects its code to files present on disk and shared network.
- It decrypt malicious dll present in the file & drops it.
- This dll performs malicious activities and collects system information & sends it to a CNC server.

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. W32.Ramnit.A

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

6. 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.

7. 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.

8. 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.

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.Modifier

Threat Level: High

Category: Trojan

Method of Propagation: Bundled software and freeware

Behavior:

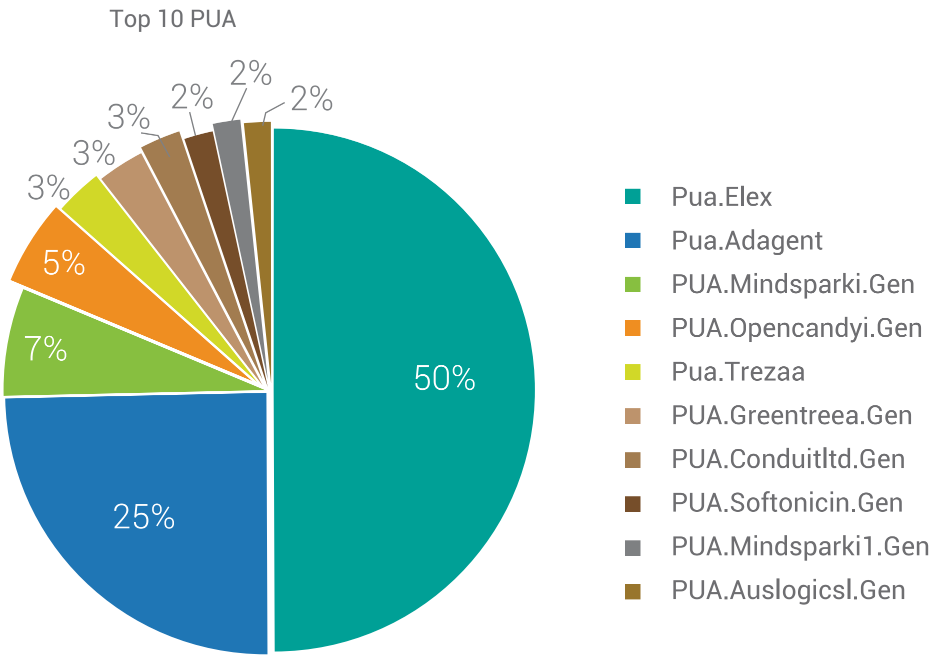
- Injects malicious codes into the browser which redirects the user to malicious links.
- Makes changes to the browser's default settings without user knowledge.
- Generates ads to cause the browser to malfunction.
- Steals the user's information while browsing like banking credentials for further misuse.

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 Q2 2019.

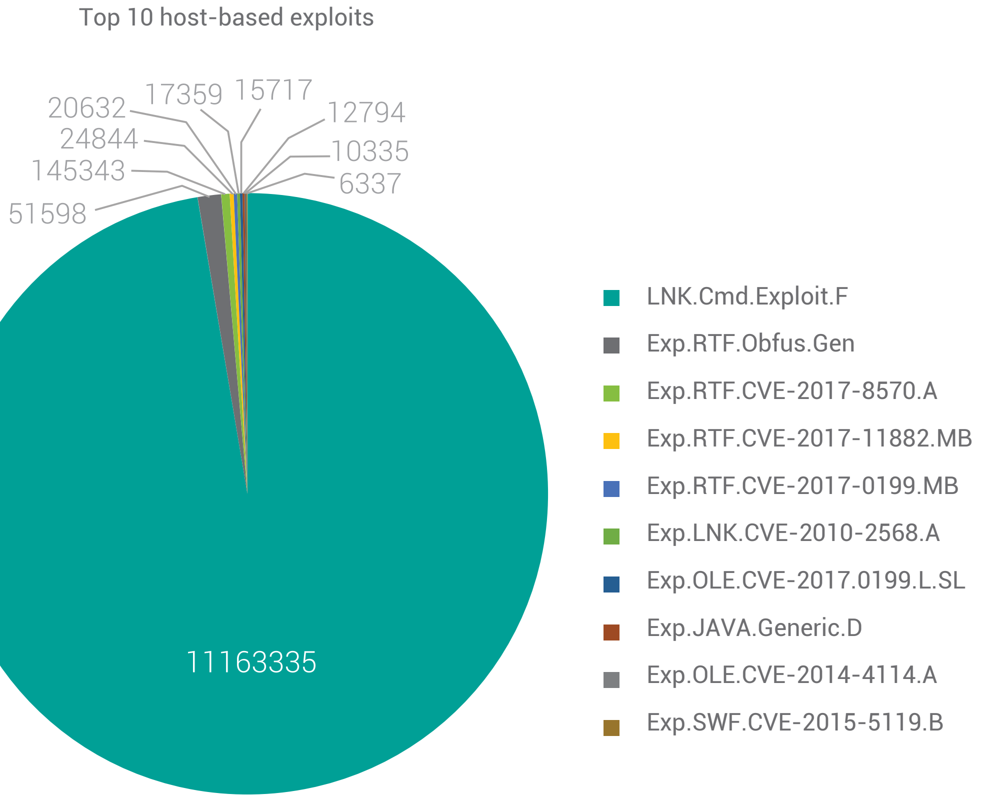


Observations

- PUA.Elex was detected to be the top PUA, with around 2 Million detections made in Q2 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 Q2 2019.

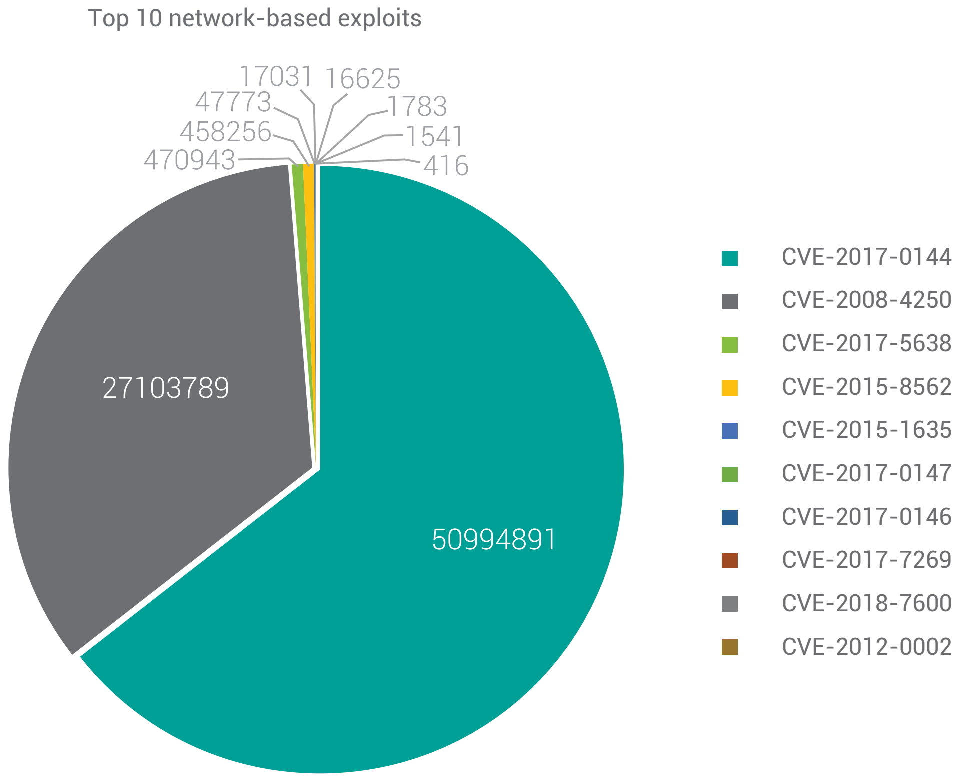


What are host-based exploits?

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 Q2 2019.



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).

Trends in Windows Security Threats

1. CVE-2019-0708 – A Critical "Wormable" Remote Code Execution Vulnerability in Windows RDP

Microsoft recently released a patch for Critical Remote Code execution vulnerability found in Microsoft Windows Remote Desktop Service (RDP). The vulnerability is identified as "CVE-2019-0708 – Remote Desktop Services Remote Code Execution Vulnerability". As mentioned in the MSRC blog "This vulnerability is pre-authentication and requires no user interaction. In other words, the vulnerability is 'wormable', meaning that any future malware that exploits this vulnerability could propagate from one vulnerable computer to another vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017. While we have observed no exploitation of this vulnerability, it is highly likely that malicious actors will write an exploit for this vulnerability and incorporate it into their malware." This vulnerability is a special case, as Microsoft went out of the way to patch this vulnerability in Windows 2003 and Windows XP as well, which have reached End of Support quite a long time ago. Given the 'wormable' nature of this vulnerability, once a host is infected, it can infect other vulnerable hosts in the same network really fast. We've few IPS signatures addressing this vulnerability through our AV. At the time of publishing this report, there were no known cases of this vulnerability getting exploited in the wild.

Ref: https://blogs.quickheal.com/cve-2019-0708-critical-wormable-remote-code-execution-vulnerability-windows-rdp/

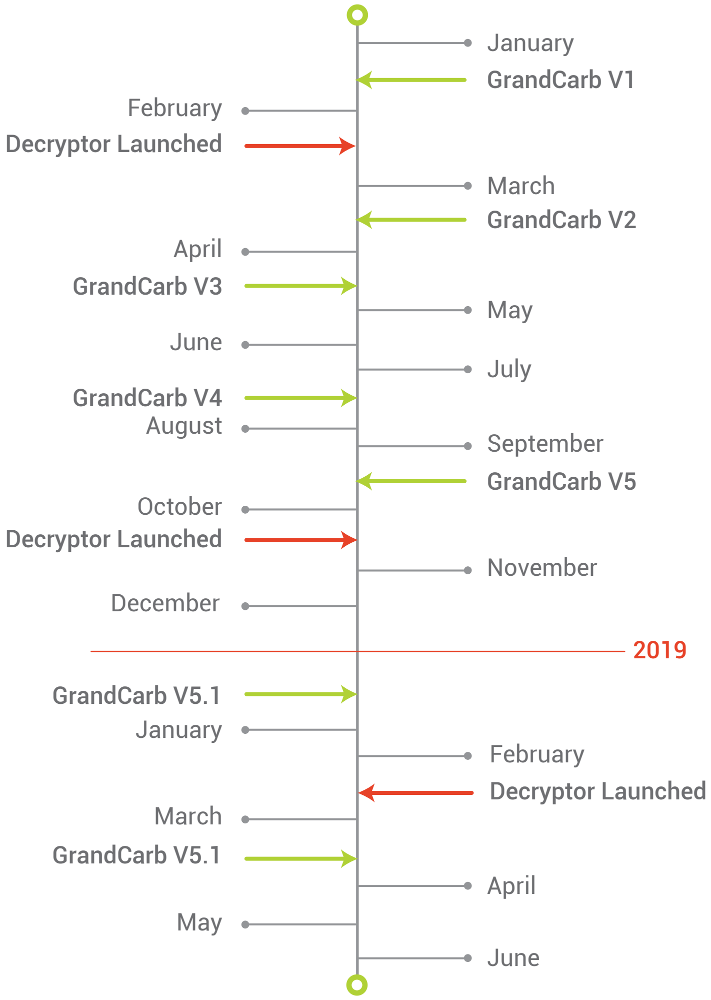
2. GandCrab retired?

One of the most prominent RaaS (Ransomware as a Service) ever, the evolving Ransomware GandCrab has announced its end this year after one and half year since its inception!

Since beginning, GandCrab had used almost every possible way to spread, like spam emails, malicious attachments, social engineering, various exploits in wild and bots to penetrate the systems etc. Over the period they changed their way of encryption, extension generation, moved to secure C&C servers and almost everything which antivirus vendors tried to detect. The malware authors were continuously monitoring the solutions provided by various AV vendors and malware researchers. Also, they evaded those tricks and made fun of those vendors and researchers on the forum or through next versions of GandCrab.

The retirement of Gandcrab also indicates that decryption keys will no more be available as infrastructure will shut down (?). The official page of Gandcrab RaaS on exploit.in was used to announce retirement of GandCrab. The message stated in sarcastic way with the phrase: "All the good things come to end!"

The figures announced by authors will definitely amaze you. People who used this RaaS are believed to earn more than $2 billion with the average of $2.5 million per week. The authors themselves, earned more than $150 million per year which sums up to $225 million for the period of their existence. And the best part is, the money earned by authors is already legalized!



GrandCarb Has Retired, or Has It?

3. Be aware of email attachments!

In the last few months, Quick Heal Security Labs have seen a sudden increase in Spear Phishing attacks. Spear phishing is a variation of a phishing scam wherein hackers send a targeted email to an individual which appears to be from a trusted source. In this type of attacks, attacker uses social engineering tricks and some business transactions or deals to entice the customer in believing that the email is genuine and from a known person or contact. The agenda of these emails, like any other cyber fraud, is to either gain access to the user's system or obtain other classified information. Spear phishing is considered one of the most successful cyber-attack techniques because of the superior level of personalization done to attack users, which makes it highly believable.

The emails which we analysed have different MS Office documents (.xls and/or .doc) as attachments and these attachments have some personalized names. When the email recipient opens the XLS attachment, it prompts the user to enable macro. After user clicks on "Enable Macros" button, the XLS file is opened for viewing. This XLS file has a malicious macro inside it, which is responsible to extract other files in a destination folder. This macro first checks the OS version of the victim's host and then drops .zip file which contains an executable file inside it. The contents of the dropped executable file are different based on the OS version, but the name remains same. The macro further loads the PE file directly (without any user intervention) and then connects to a remote Command and Control (CnC) Server.

After connecting to CnC Server, we observed that CnC Server sends few commands to the victim host. The CnC Server collects information about the current running processes from the victim host. It then commands the victim host to share victim's personal data which contains screen-shots of the host taken at regular intervals, few random files from the victim host, etc. Quick Heal Security Lab is monitoring this Spear Phishing attack to further identify the motive behind these attacks.

Ref: https://blogs.quickheal.com/beware-email-attachments-can-make-victim-spear-phishing-attacks/

4. Beware! The padlock icon and HTTPS are no more indicators of safe website

The recent past shows a startling rise in the number of incidences of phishing attacks, where visitors have been lured into clicking fraudulent links, under the cover of security marks like padlock icon and 'HTTPS'. Until now, the padlock icon and HTTPS in web link, were considered as safety indications that the link is secure to be browsed and visitors can safely share their data. The HTTPS protocol especially meant that the website is secure against hackers and spying agents, but nowhere did it ensure that the website is benign. However, off recently, cyber criminals are breaching people's trust on the padlock icon and HTTPS. As per reports, more than 15,000 TLS certificates have been unveiled containing the word 'PayPal' that hackers are using to carry out malicious attacks, while playing with the trust of people. The fact that new domains and sub-domains are springing up every now and then, has made it more difficult for people to differentiate a legitimate site from a fraud one. This means you need to take precautions while visiting any website and once you are absolutely confident and satisfied that the website belongs to the domain of the company that you intended to visit, only then enter your credentials or personal data. In short, do your research before you trust any website, as precaution is always better than cure!

Ref - https://blogs.quickheal.com/beware-padlock-icon-https-no-indicators-safe-website/

5. GoldBrute: Brute Forcing the Internet!

Recently CVE-2019-0708, also known as Bluekeep vulnerability made buzz in RDP (Remote Desktop Protocol) based attacks. As RDP gives attacker full control of system, attackers are continuously in search of ways to exploit RDP. Special type of Botnets are designed to scan RDP exposed systems over internet and then using brute force it tries to gains access. The GoldBrute botnet is one of the latest botnet of this category. According to popular internet resource, this aggressive brute force botnet attacked more than 1.5 million RDP servers.

How does it work?

GoldBrute is designed in a way to add new compromised servers hence, continuously increasing its network. It uses these compromised systems to find new vulnerable systems and brute force them. It gives the system in same network a set of multiple user names and passwords to brute force millions of servers which can be attacked. Because of this the system faces brute force attack from a different IP every-time. Due to this the security tools and malware analyst are not alerted. After gaining control of system through RDP, it downloads a payload i.e. a zip file containing JAVA based 'GoldBrute' code. It then communicates with the system by establishing a connection to CnC via WebSocket port 8333. It is an AES encrypted communication. Then the system is assigned a task to scan and return a list of minimum 80 IP's of server which can be infected. This list is added to the database. Brute Forcing is then materialized as the system receives IP list along with the username and password to use while attacking. If the attack is successful, the machine sends the username and password to the CnC server. The infected machine keeps on getting the list of systems to attack.

How to prevent it?

1. It is advised to keep your RDP off if it is not required OR allow specific systems.
2. Instead of exposing RDP over internet, use alternative like VPN or other remote access tools.
3. Account lockout & password expiration could also help to prevent brute force (but not always)

GoldBrute remains dangerous as the result of all these attacks is still unknown. This can be converted into a mass exploitation, but to reach that level it will take time and until then we all have time to act accordingly and secure our systems.

6. STOP…Please Stop!

Quick Heal Security Labs have been observing a rise in Stop Ransomware. The STOP ransomware was initially discovered in December 2017. However, new variants have started reappearing since August 2018. Although the behaviour shows similarity, different samples have different extensions, providing slightly different ransom notes and new contact email addresses. The initial version of malware were used to add '.STOP' extension to encrypted file, but now it keeps on changing the extension. Initially STOP ransomware used to encrypt all files and then it used to deliver ransom note in "!!! YourDataRestore !!! txt" file. The message tells victim to pay the ransom within 72 hours to avail 50% discount. The STOP Ransomware is distributed using spam emails, MS office attachments, repackaged and infected installers of popular programs and pirated activators etc. STOP might also be delivered by unprotected RDP configuration and exploits web injects. The recent version shows that the files are encrypted using SALSA20 algorithm with 256 bit key. STOP ransomware connects to C&C server, receives an encryption key along with an infection identifier for the victim's PC. Data is transmitted over simple HTTP in the form of a JSON file.
If C&C is not available, then it uses locally generated keys and performs offline encryption. In this case, it will be possible to decrypt the files without paying the ransom. From its inception till June 2019 the number of versions has already crossed the count of 100. It is always recommended to audit & follow security measures & harden it as much as possible. & keep backup of important data.

7. Miners snatching open source tools to strengthen their malevolent power!

Since last one year, Quick Heal Security Labs has been observing a boost in the number of mining malware. One of the ways to earn cryptocurrencies is to mine them. Nowadays cryptocurrency miner malware has become hot attack vector for cybercriminals due to its ease of deployment and instant return on investments. Attackers download original open source software and slightly modify them rather than completely writing their own module. The trend is observed especially in cryptojacking cases. Though cryptojacking is a direct source of income for cybercriminals, stolen information from the victim's systems can yield additional money for cybercriminals.

We received a miner downloader which downloads multiple components of the attack. This script may come to your system through spam mails, malicious URLs, free software bundler or any conventional method that is being used by all the malware variants. It contains the list of process to kill if it was running on victim machine. Then malware downloads a text file which contains the information of multiple payloads to be downloaded. Mimikatz, masscan, eternal blue vulnerability scanner seems to be popular tools among the malware authors. Similar techniques are being used for spreading ransomware too. In multiple cases attackers execute the Miner along with tools like mimikatz and dump the credential irrespective of execution Miners.

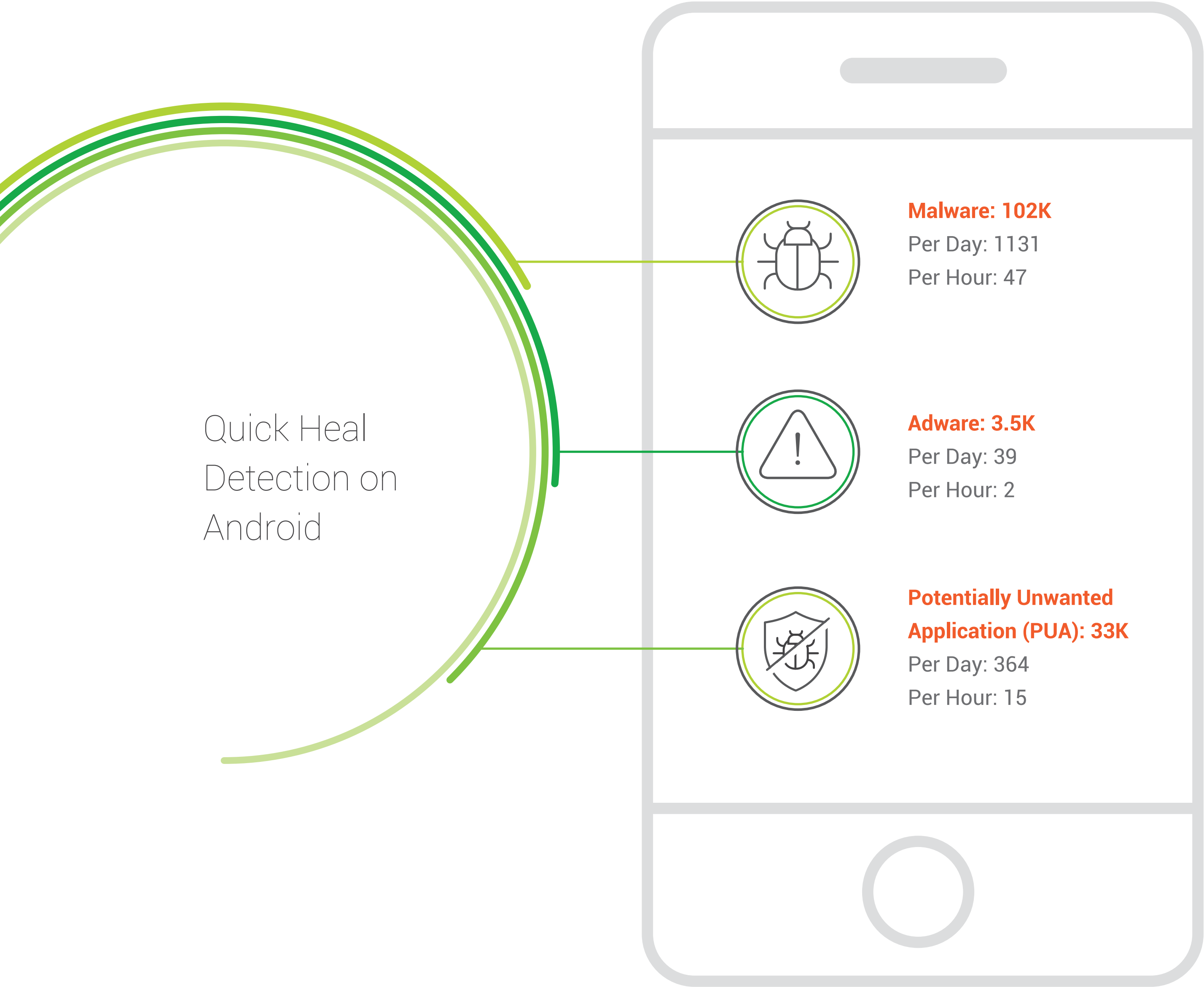
The malicious vector also enumerates the network addresses and checks for the IPs that are active and then scans these IPs to identify the systems which are vulnerable to MS17-010 (with Eternal Blue Scanner Script). The vulnerable machines in network will also get infected once vulnerability is confirmed.

Quick Heal detects such attacks at various detection levels.

Ref: https://blogs.quickheal.com/miners-snatching-open-source-tools-strengthen-malevolent-power/

ANDROID

Quick Heal Detection on Android



Quick Heal Detection on Android

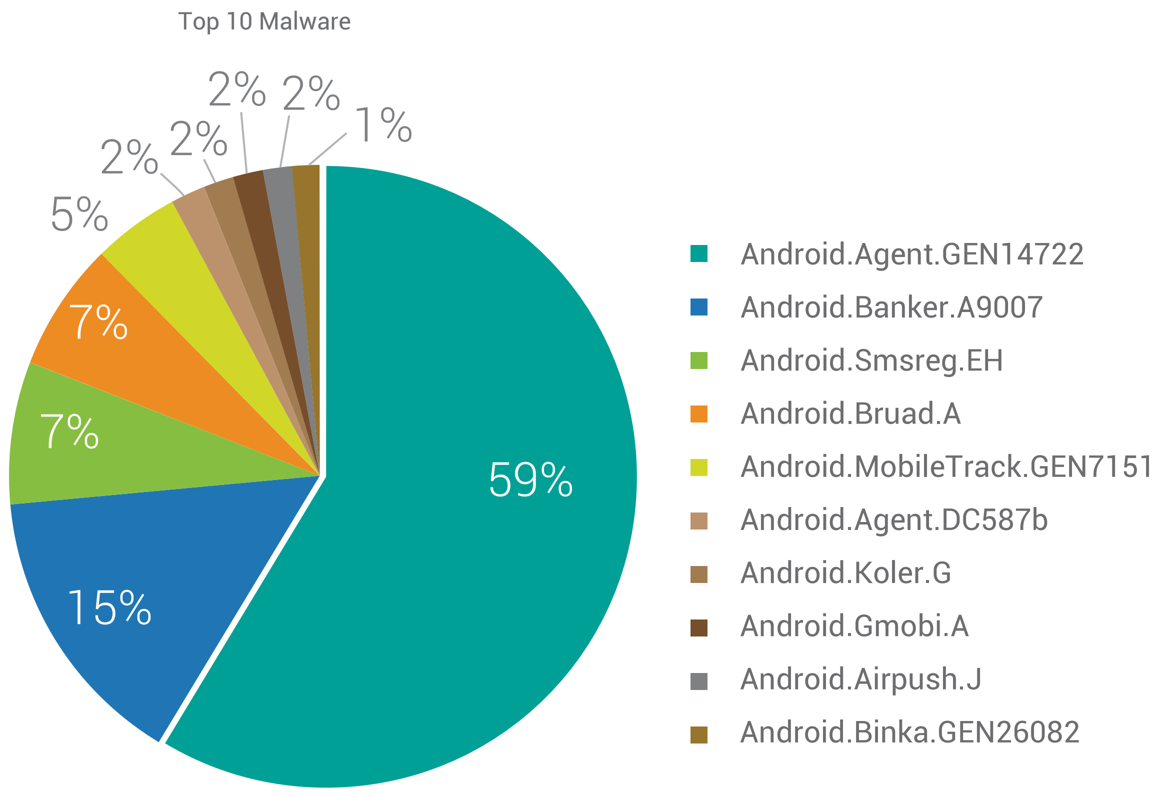
Malware: 102K
Per Day: 1131
Per Hour: 47

Adware: 3.5K
Per Day: 39
Per Hour: 2

Potentially Unwanted Application (PUA): 33K
Per Day: 364
Per Hour: 15

Top 10 Malware

Below figure represents the top 10 Android malware of Q2 2019. These malwares have made it to this list based upon their rate of detection during the period of Apr to Jun in 2019.



1. Android.Agent.GEN14722

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- After it's launched, it hides its icon and runs in the background.
- In the background, it downloads malicious apps from its C&C server.
- The downloaded malicious apps perform further malicious activities and may steal user information.

2. Android.Banker.A9007

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- After installation, It collects the data like vendor information, device fingerprint, System information etc.
- After launch it shows black window and hides its icon. It start running services in background.
- It downloads other applications by connecting to C&C server

3. 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

4. Android.Bruad.A

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

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.

5. 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 an SMS after SIM change or phone reboot with specific keywords in the body.
- Collects device information such as IMEI and IMSI numbers

6. Android.Agent.DC587b

Threat Level: High

Category: Malware

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

Behavior:

- This malware continuously asks user for accessibility services permission.
- After getting permission, it draws phishing overlay window on other banking apps and steal login credentials.
- It performs malicious activities like send/read SMS, make calls, read contacts and prevent itself from uninstallation.
- It is having ability to read keylogs, screen locking and demanding ransom.

7. Android.Koler.G

Threat Level: High

Category: Malware

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

Behavior:

- This malware continuously asks user for accessibility services permission.
- After getting permission, it draws phishing overlay window on other banking apps and steal login credentials.
- It performs malicious activities like send/read SMS, make calls, read contacts and prevent itself from uninstallation.
- It is having ability to read keylogs, screen locking and demanding ransom.

8. Android.Gmobi.A

Threat Level: Medium

Category: Adware

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

Behavior:

- Makes use of SDK to easily recompile other genuine apps.
- 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

9. 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 serve

10. Android.Binka.GEN26082

Threat Level: High

Category: Trojan

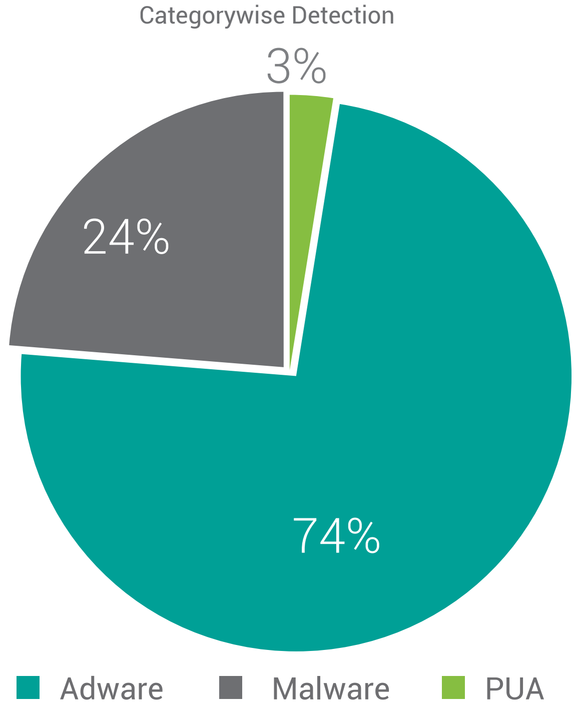
Method of Propagation: Third-party app stores and repacked apps

Behavior:

- It disguise as banking application.
- It collects device incoming SMSs and forward it.
- It record calls and send it to C&C server
- It collect device data like IMEI, manufacturer, model, device number, contacts from device and send it to server.

Android Detection Statistics: Category Wise

Below figure represents the top 10 Android malware of Q2 2019. These malwares have made it to this list based upon their rate of detection during the period of Apr to Jun in 2019.

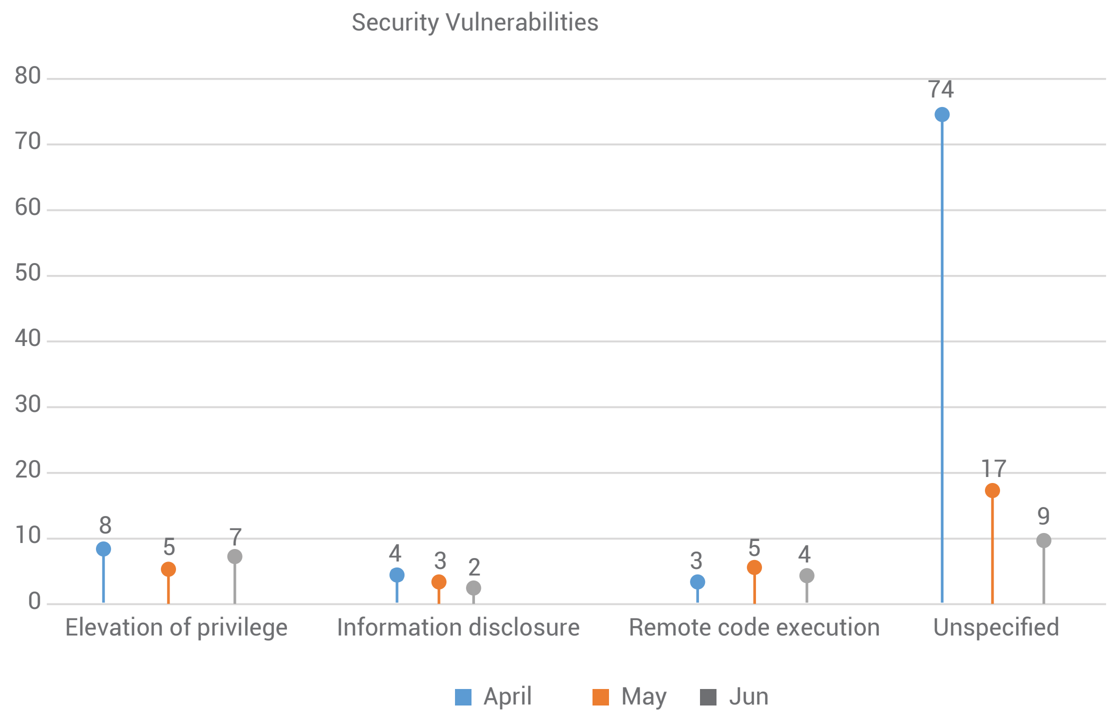


Observations

- Malware clocked 74% of the total Android malware detectons in Q2 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 Apr to Jun of 2019.



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

Trends in Android Security Threats

1. Malware has ability to convert clean application into malicious

An innocent looking application turns clean applications into malicious one, with the help of vulnerabilities in the Android OS. Recently attackers made some applications that makes use of Janus vulnerability which was discovered in 2017 to infect the clean applications & it helps the attackers to add its components in the targeted APK files without changing their digital signature.
After installation when the user launches this malicious application, it shows a pop-up "choose an account". After clicking on it, malware starts its activity in background by adding a patch on clean application. Due to this installed application shows a pop-up regarding update application, and innocent user accept the update and in result clean application won't be clean any more. Following are some of the malware related apps: HD Camera, Euro Farming Simulator 2018, Spollo player.

The patch contains module which display ads and steal the private massages. The primarily targeted applications are Opera Mini, WhatsApp Messenger, Daily-hunt, Ludo King, SHAREit and Truecaller. It uses the vulnerability CVE-2017-13156 and CVE-2017-13315. Following android versions 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0 have these vulnerabilities.

Quick Heal AV detects such malicious app as Android.Infdas.GEN29083.

2. Different techniques being used by banking malware

Use of twitter and telegram account

Previously Anubis banking malware used twitter account to collect C&C server address, but now Anubis abuses telegram also. Anubis uses this method to remain undetected as both are famous sites and uses this way to escape from URL classification.

To perform malicious activity, it connects to specific telegram account, then collects the Chinese string and further decrypts it with various decryption algorithm. Afterwards it then generates C&C server address & downloads the payload. Telegram has deleted the account now which was used to generate server address.

This payload targets various banks. It starts its malicious activity when user launches any bank application and then creates fake login overlay for same bank. Thus, it steals user's login credentials. Apart from this, it also has the capability to lock user's device and demand for ransom.

Quick Heal detects this malware as Android.Dropper.E and Android.Anubis.A1f34

Banking Trojan enters through SMS

Previously Anubis banking malware used twitter account to collect C&C server address, but now Anubis abuses telegram also. Anubis uses this method to remain undetected as both are famous sites and uses this way to escape from URL classification

Another banking malware that targets top international banks such as Bank of America, J.P.Morgan & 30 virtual currency apps, Coinbase, Bitcoin Wallet and BitPay. This malware looks like regular applications, but they start phishing to get login credentials, whenever user uses one of these applications. The malware also sends SMSs, screenshots, photos to C&C server. It can also reset device to factory settings. In advance versions this malware makes a use of accessibility features that can enable privileges itself and it can even turn off Google Protect. It collects contact list from victim mobile and spreads through SMS by sending APK installation link through SMS.

Quick Heal detects it as Android.SmsThief.GEN20741 And Android.Hqwar.M.

3. Trend of hiddad malware continues

Earlier this year, Quick Heal Security Labs had reported few applications to Google Play, which hide themselves after installation and display full screen ads after specific time interval. This trend is used by most of the developers these days to earn profit by displaying ads. After hiding itself, it interrupts user by frequently showing advertisements while using other applications. Quick Heal Security Labs reported this to Google and those applications have been removed from Play Store now. This trend continues in this quarter also.

Many PUA were present on Google Play. Combined installations of applications from this one family was 30 million before it was removed from Google Play. These applications were simple games, fitness, and photo editing applications. After installation they add multiple shortcuts on home screen and shows too many ads using a common library. This library drains the device battery, consumes mobile data and make the device slower. All of this is against Google's policies & rules for advertising. The ad library has multiple versions, and newer versions use complex packers to make analysis & AV detections difficult.

Quick Heal detects such apps as: **Android.Hiddad.GEN29671**

More than 200 apps were present on Google Play, working as an adware-backdoor. All of these apps use a common SDK (Software Development Kit) for advertising. Capabilities of this malware family include showing ads, opening URLs in browser & receiving commands from C&C (Command & Control) server to perform activities. It is also able to hide its icon in app launcher making it difficult to notice its existence but runs in the background even after device restarts. Intention of these apps seems to generate as much ad revenue as possible. Quick Heal detects such apps as: Android.Hiddad.ZL

4. WhatsApp Vulnerability used by hackers to infect with spyware

In mid-May a vulnerability was discovered in the WhatsApp that allows hacker to install a spyware with single VoIP call on target phone. The vulnerability CVE-2019-3568 allows attacker to install a spyware remotely. Once installed, it can turn on camera and microphone and collect the user data like messages, mails, Contacts, locations etc. This vulnerability is discovered in WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to v2.18.15. For now, according to Facebook, the owner of WhatsApp, the vulnerability is patched. Users are advised to update installed applications as and when there is an update available.

Conclusion

The second quarter of 2019 witnessed a comeback of several Ransomware and banking malware that had been discovered earlier and have started reappearing with newer and more destructive variants. This goes on to explain that these malware are here to stay for long and the chances of them creating a havoc cannot be ruled out easily.

While Ransomware continues to be the preferred choice for cyber criminals with new variants appearing, Cryptojacking is right on its tail. In fact, according to reports by Quick Heal Security Labs, there were total 3 Million Cryptojacking detections made in Q2 of 2019 as against just 0.9 Million Ransomware detections.

Considering this consistent evolution of Ransomware and Cryptojacking across the quarters, it would be fair enough to say that these malware will only continue to evolve. Thus, it is advisable to switch to a stronger and robust antivirus with advanced features that can put up a strong fight against both evolving and new malware types.

Most importantly, be aware of what you are doing and sharing on the internet unless you are absolutely sure about it. Learn to protect your personal data with a strong password and frequent backups and limit the amount of personal information you share on social media, as this information can easily be harvested to make you a victim of phishing scams and targeted attacks.

In addition, with cyber criminals increasingly using soft targets like emails for conducting targeted attacks and spear phishing scams, it is advisable to be cautious when clicking on URLs in emails or attachment. This comes after Quick Heal Security Lab witnessed a sudden increase in Spear Phishing attacks wherein hackers send a targeted email to an individual which appears to be from a trusted source. The agenda of these emails, like any other cyber fraud, is to either gain access to the user's system or obtain other classified information.

Thus, try to be cautious and suspicious to be safe… it costs nothing.

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