Quick Heal
Security Simplified

SEQRITE

QUICK HEAL
QUARTERLY THREAT REPORT | Q2 2018

www.quickheal.com

Contributors

- Quick Heal Security Labs
- Quick Heal Marketing Team

Table of contents

Introduction

In the second quarter of 2018, Quick Heal Security Labs detected over 180 million Windows malware. May clocked the highest detection - on a daily basis, Quick Heal detected around 2,004,728 malware, 16,165 ransomware, 141,079 exploits, and 40,488 PUA & adware. The Trojan horse family retained its position as the most dominant malware in the entire quarter. It grew 4.03% compared with its detection in Q1 2018. The top malware of the year is a destructive Trojan called Trojan.Starter.YY4. Quick Heal Security Labs noticed a spike in EternalBlue exploit (used in the biggest ransomware attack in 2017 – WannaCry). Other important trends include the increase of MBR (Master Boot Record) infecting ransomware and cryptocurrency mining. The most worrying trend, however, is cryptojacking – experts are calling it the new ransomware.

Quick Heal Security Labs recorded over 631,000 detection (malware + PUA + adware) on the Android OS in Q2 2018. The PUA (Potentially Unwanted Application) family comprised 46.2% of the total detection of the year. The main trends observed in the Android threat landscape include the rise in cryptocurrency mining malware and banking Trojans that are targeting popular banking and social media apps.

About Quick Heal

Quick Heal Technologies Ltd. (Formerly Known as Quick Heal Technologies Pvt. 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

Quick Heal Detection on Windows Q2 2018

Malware

Per Day: **2,004,728**
Per Hour: **83,530**
Per Minute: **1,392**

Ransomware

Per Day: **16,165**
Per Hour: **674**
Per Minute: **11**

Exploit

Per Day: **141,079**
Per Hour: **5,878**
Per Minute: **98**

PUA and Adware

Per Day: **40,488**
Per Hour: **1,687**
Per Minute: **28**

Cryptojacking Malware

Per Day: **13,427**
Per Hour: **559**
Per Minute: **9**

Source: Quick Heal Security Labs

Windows Malware Detection in Q2 2018

The below graph represents the statistics of the total count of malware detected by Quick Heal during the period of April to June in 2018.

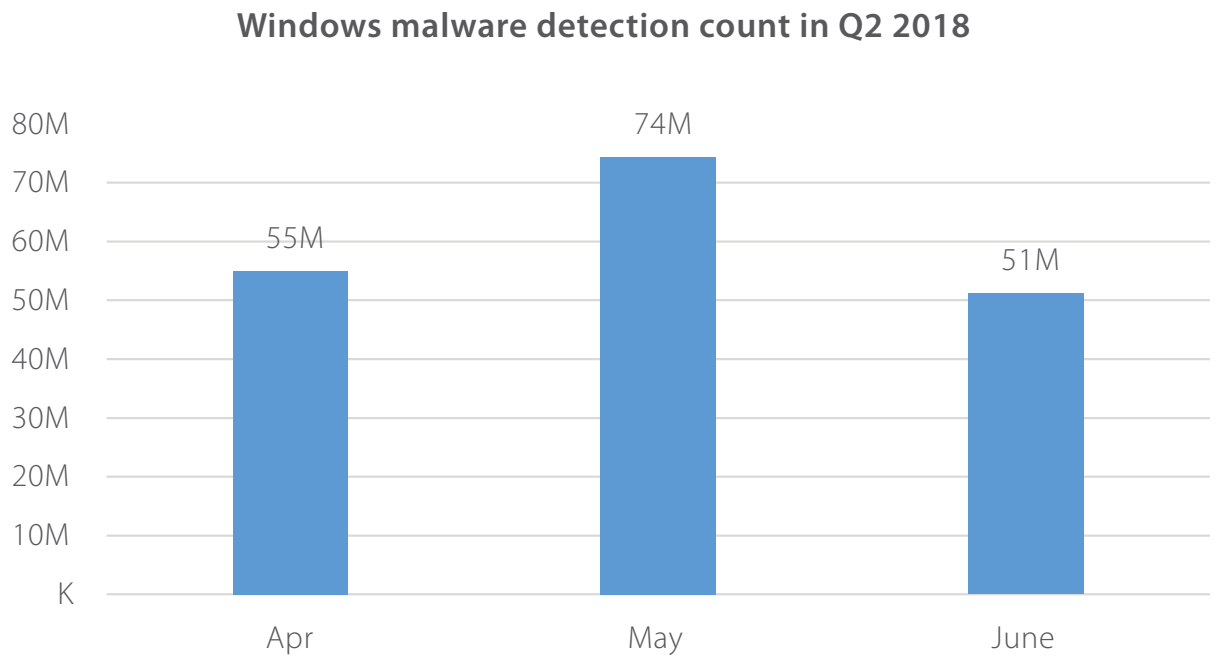


Fig 1

Observations

- Quick Heal detected over 180 million Windows malware in Q2 2018.
- May clocked the highest detection of Windows malware.

Top 10 Windows Malware

Fig 2 represents the top 10 Windows malware of Q2 2018. These malware have made it to this list based upon their rate of detection from April to June.

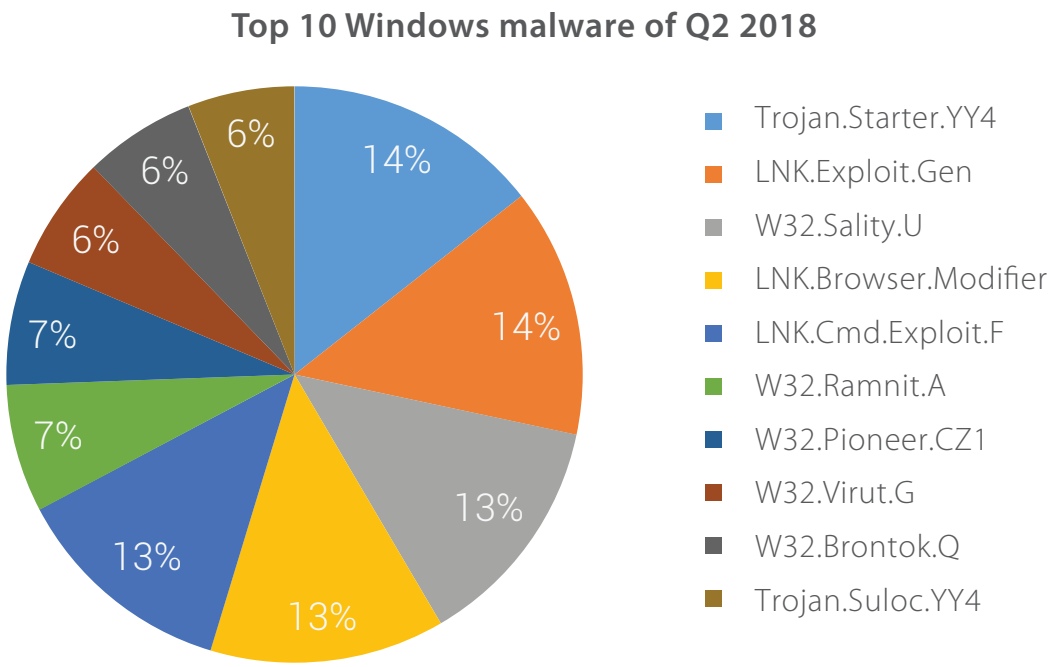


Fig 2

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.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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. W32.Virut.G

Threat Level: Medium
Category: File infector
Method of Propagation: Bundled software and freeware
Behavior:

- Creates a botnet that is used for Distributed Denial of Service (DDoS) attacks, spam frauds, data theft, and pay-per-install activities.
- Opens a backdoor entry that allows a remote attacker to perform malicious operations on the infected computer.
- The backdoor functionality allows additional files to be downloaded and executed on the infected system.

9. W32.Brontok.Q

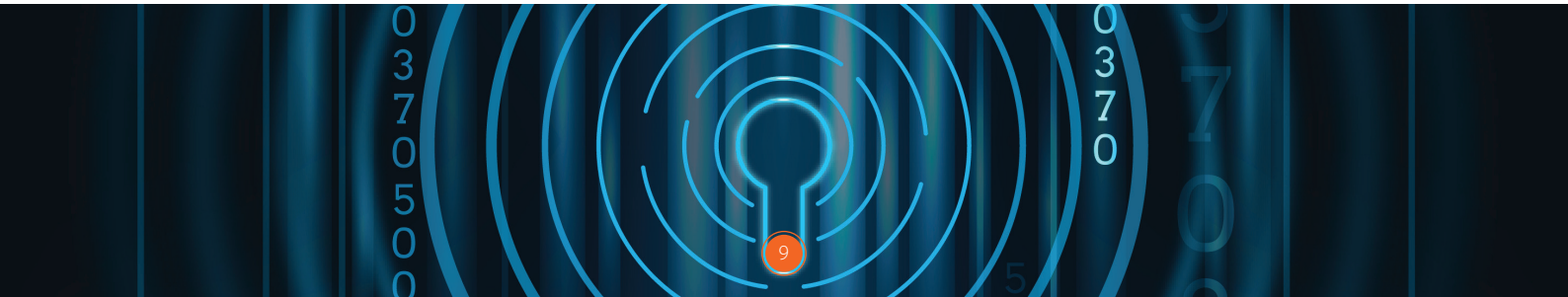
Threat Level: Medium
Category: Worm
Method of Propagation: Spreads through emails or infected USB & network drives
Behavior:

- This worm spreads through emails or infected USB drives.
- It stores several copies of itself on different places on the hard disk, including system directories.
- It gains persistence by modifying registry keys and creating an entry in the Startup directory.
- It modifies several system configuration parameters to disable the registry editor and command prompt.
- It also modifies the safe boot shell to prevent the user from cleaning the machine.

10. Trojan.Suloc.YY4

Threat Level: Medium
Category: Trojan
Method of Propagation: Bundled software and malicious websites
Behavior:

- Copies itself on the targeted drive, and startup drive.
- Modifies registry entries to execute itself automatically and hides file extensions.
- Nested process continuously queries the information of dropped files and copies itself in download folder.



Category-wise Windows Malware Detection

Fig 3 represents the various categories of Windows malware detected by Quick Heal in Q2 2018.

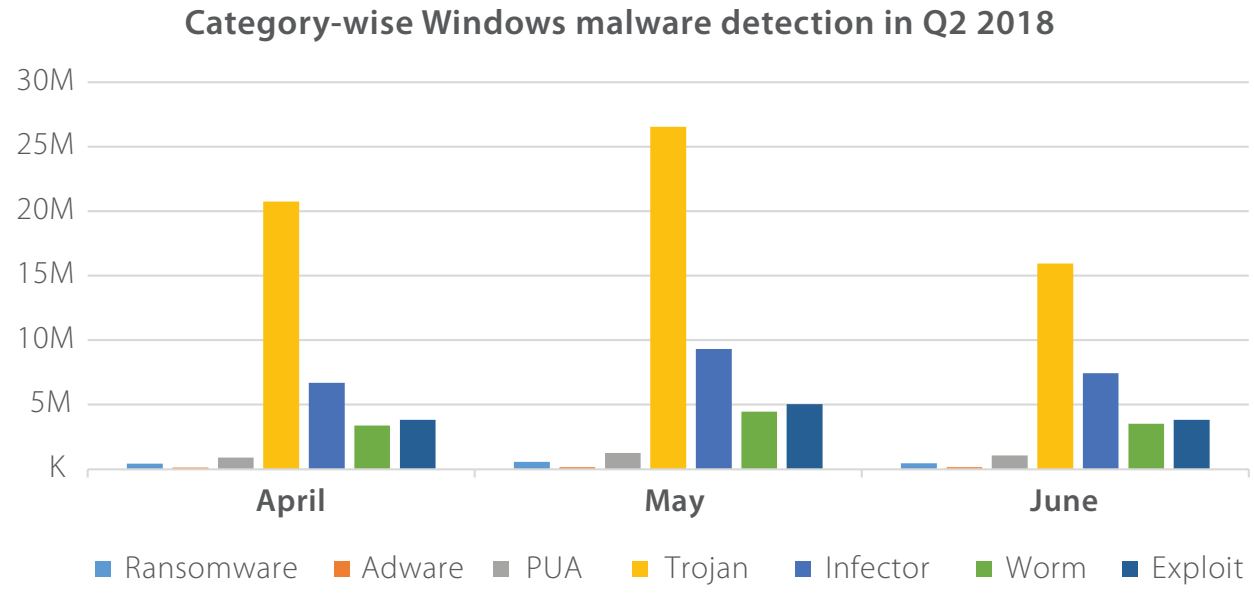


Fig 3

Observations

- The Trojan Horse family clocked the highest detection in the entire quarter.
- Following is a comparative analysis between the detection count of Q2 2018 and Q1 2018.

Detection Count			
Malware Category	**Q1 2018**	**Q2 2018**	**Growth**
Trojan	60,797,318	63,249,214	4.03% increase
Infectors	27,526,654	23,457,813	14% decrease
Exploit	17,055,455	12,697,113	25% decrease
Worm	13,313,316	11,371,699	14% decrease
PUA	4,499,151	3,226,738	28% decrease
Ransomware	2,861,095	1,454,820	49% decrease
Adware	799,530	417,152	47% decrease

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.

Fig 4 represents the top 10 PUAs and Adware detected by Quick Heal in Q2 2018.

Top 10 PUA & Adware of Q2 2018

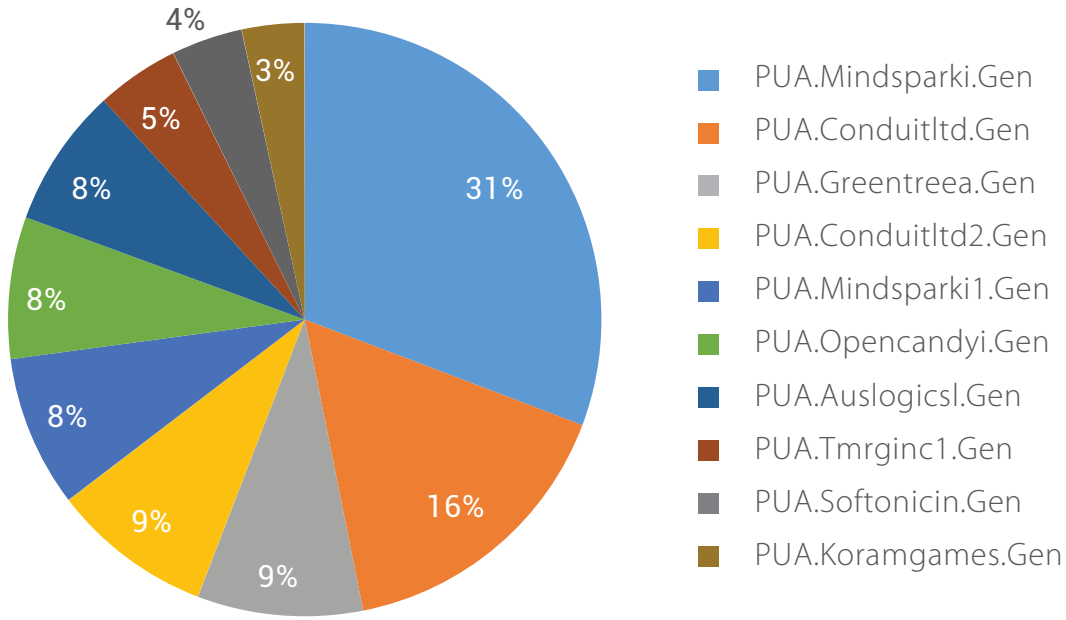


Fig 4

Observations

PUA.Mindsparki.Gen was registered as the top PUA in Q1 2018 and it continues to be so in Q2 2018.

Top 10 Windows Exploits

A computer exploit is an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. Fig 5 and 6 represent the top 10 Windows exploits (host-based and network-based) of Q2 2018.

Top 10 host-based exploits of Q2 2018

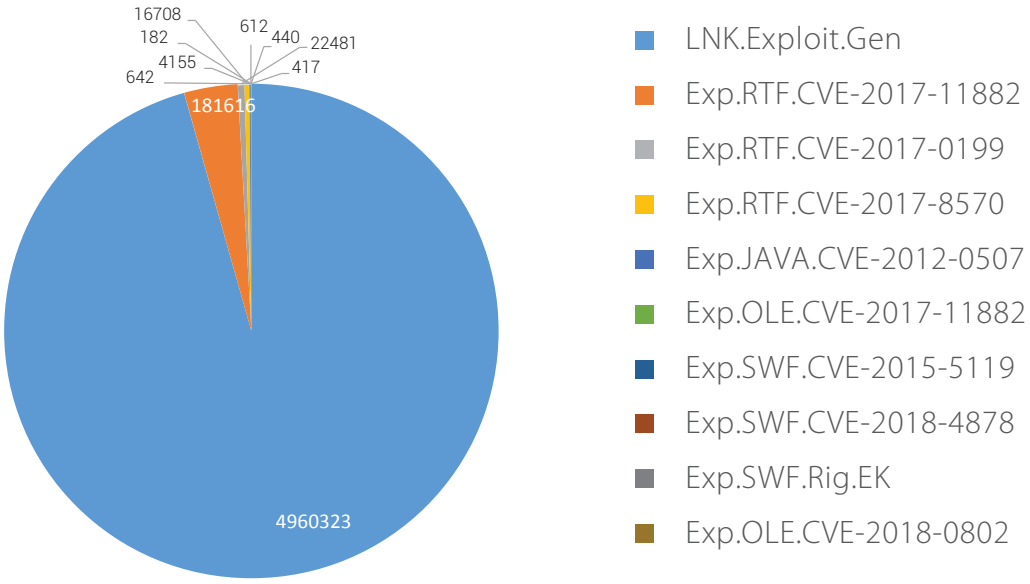


Fig 5

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.

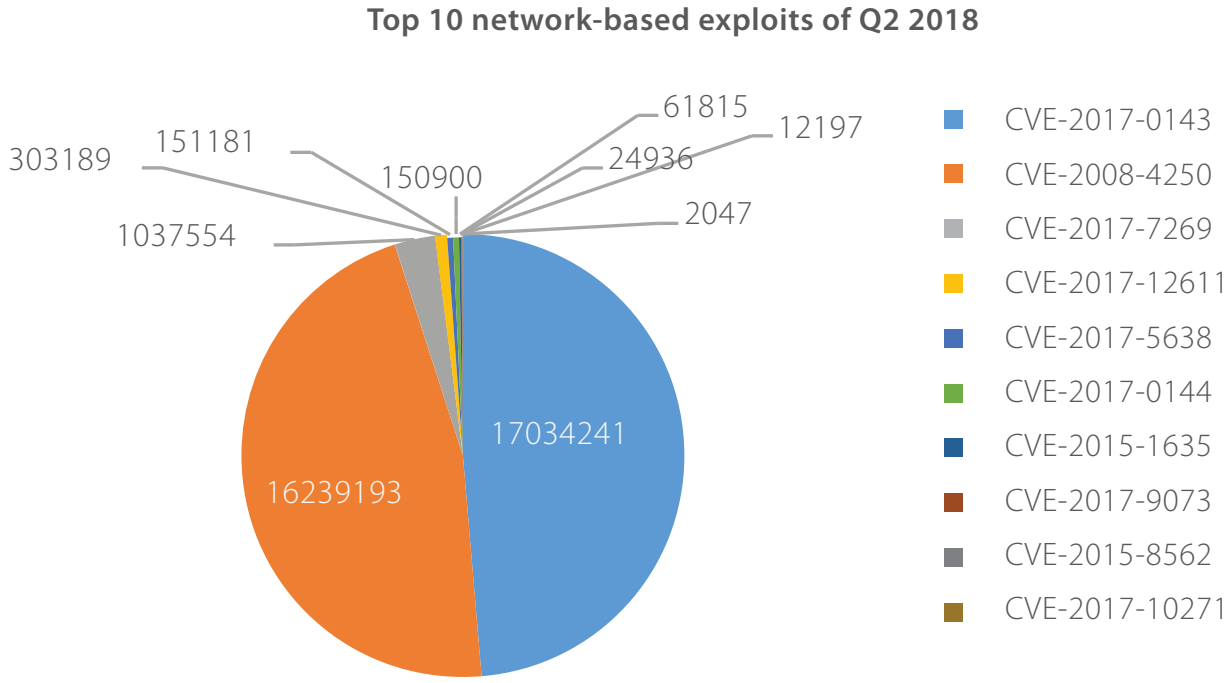


Fig 6

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

I. EternalBlue - A prominent threat

In Q2 2018, Quick Heal Security Labs again witnessed spike in EternalBlue exploit which is a SMB protocol vulnerability leaked by Shadow Broker group in April 2017. It was adopted in many ransomware campaigns as well as cryptocurrency miner campaigns. Quick Heal Security Labs has released an in-depth technical research paper which reveals EternalBlue exploit and DoublePulsar payload. The research paper featured on Virus Bulletin.

Read more:

https://quickheal.co.in/documents/technical-paper/201806-EternalBlue-Final.pdf

https://www.virusbulletin.com/blog/2018/06/paper-eternalblue-prominent-threat-actor-20172018/

II. Breed of MBR Infecting Ransomware

Ransomware is becoming one of the most perilous cyberattack methods and the most habitual techniques for cybercriminals to earn money. It appears to have added new weapons to its arsenal over time - aimed towards boosting its strength and enhancing its business. As if encrypting files and restricting user access is not enough, ransomware also infect the master boot record and prevent the operating system from loading. As the operating system is not loaded, none of the ransomware tool or antivirus work on these types of ransomware. Even though this technique was noticed last year (in case of PETYA ransomware), this year there has been an exponential increase in MBR infection by ransomware. MBR infection extends the scope for deep infection and controls the infected computers, which make the attack more severe. The ransomware copies the original MBR and overwrites it with its own malicious code. After that, it automatically restarts the system for the infection to take place. When the system restarts, the user is locked out and the ransomware displays its note and asks for a ransom.

Read more:

https://blogs.quickheal.com/breed-mbr-infecting-ransomware-analysis-quick-heal-security-labs/

III. Cryptocurrency mining rampage throttles Linux machines

Quick Heal Security Labs recently came across a Linux-based Monero (XMR) miner. Monero (XMR) is one of the top 15 cryptocurrencies. It can be mined easily on any machine using its CPU computation power. This is one of the reasons why it is preferred to Bitcoin or Ethereum which are more famous than Monero. A shell script file is the source for this Monero mining campaign which is injected into the targeted machine through SHH brute force attack. Using the "nproc" command, the shell script checks for the number of CPU cores present in the user's system. If it is less than or equal to 4, then the script will terminate otherwise it will perform further tasks.

It is a myth that Linux is safe from malware and the fact is attackers are well prepared to use Linux machines for mining. The market for cryptocurrencies is large and we can expect a rise in the attacks on Linux machines to mine cryptocurrencies.

Read more:

https://blogs.quickheal.com/cryptocurrency-mining-rampage-throttles-linux-machines/

Trends in Windows Security Threats

IV. Cryptojacking

Till recently, ransomware was the ultimate cash cow for attackers – kidnap critical data and ask a ransom in exchange. However, now, there is even a bigger source of income than ransomware. It is called cryptojacking – using someone else's computer to generate digital cash called cryptocurrency. While a ransomware is detected after a time and is short-lived, cryptojacking can run almost undetected on users' systems minting money for attackers for as long as they want. Due to its ease of deployment and an instant return of investments, cryptojacking has replaced ransomware as the number.

Read more:

https://blogs.quickheal.com/cryptojacking-is-when-someone-illegally-uses-your-pc-to-make-digital-money-8-facts/

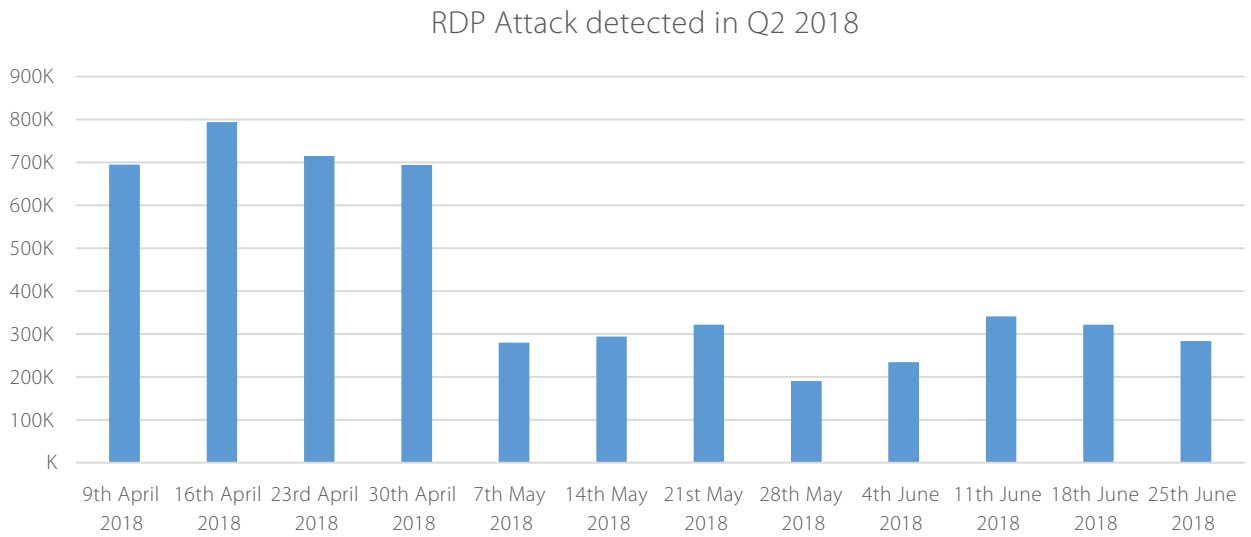
V. Dharma ransomware outbreak

In Q2, 2018, we observed a sudden spike in Dharma ransomware detection. Even though Dharma ransomware is old, we observed its new variant which is encrypting files and appending the ".arrow" extension to it. Previously, the encrypted files were having the ".dharma" extension. Largely, we will categorize these infection vectors into two categories.

- Vector 1 – RDP Brute Force Attack
- Vector 2 – Other Suspicious means

Vector 1 – RDP Brute Force Attack

In this vector, the Remote Desktop Protocol (RDP) running on port 3389, is targeted with a typical brute force attack. As a result of the brute force, the attacker gets hold of victim's administrative user credentials. Once credentials are obtained, they get the ability to carry out any type of attack. In this case, ransomware is used to infect the system. Also, it's observed, before executing the ransomware payload it uninstalls the security software installed on the system.



Vector 2 – Other suspicious means

Here the source of infection is unknown but when we started analyzing the attack chain, it took us to an interesting set of entries in the victim's registry. These were autorun PowerShell script entries in the registry under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services which drop and execute multiple malicious components.

- Inf.exe – It enables RDP and runs sticky key exploit.
- i.exe – Gets the list of IP addressed from APR cache and sends to CnC server.
- ipcheck.exe – It also finds out the list of IP address and passes on to 'sc.exe'.
- sc.exe – This is WannaCry scanner tool which runs on the list of IP address passed by 'ipcheck.exe'. This gives a list of vulnerable machines. This list is sent to CnC server by 'ipcheck.exe'.
- rc.exe – This is main payload i.e Dharma ransomware

The 'inf.exe' component is mainly used to enable the Remote Desktop Protocol (RDP) on the victim's machine. Once RDP is enabled, it creates a new user from one of the hardcoded username list and randomly generates a password for it. Further, it gives administrative privileges to the newly created user account and enables this account for the remote session. The rc.exe is main payload i.e., Dharma ransomware. This variant appends the extension '.arrow' to the files it encrypts. If the file size is greater than 98304 bytes, the ransomware overwrites this file with encrypted content else creates a new file with encrypted content and deletes the old one. The ransomware encrypts all the above-mentioned extension files using AES 256 algorithm. The AES key is further encrypted with an RSA 1024. This encrypted AES key is kept at the end of the encrypted file.

Read more:

https://blogs.quickheal.com/analysis-dharma-ransomware-outbreak-quick-heal-security-labs/

ANDROID

Quick Heal Detection on Android Q2 2018

Malware

Per Day: **2,632**
Per Hour: **110**
Per Minute: **2**

Adware

Per Day: **1,101**
Per Hour: **46**
Per Minute: **1**

Potentially Unwanted Application (PUA)

Per Day: **3,207**
Per Hour: **134**
Per Minute: **2**

Source: Quick Heal Security Labs

Top 10 Android Malware of Q2 2018

Fig 1 represents the top 10 Android malware of Q2 2018. These malware have made it to this list based upon their rate of detection during the period of April to June in 2018.

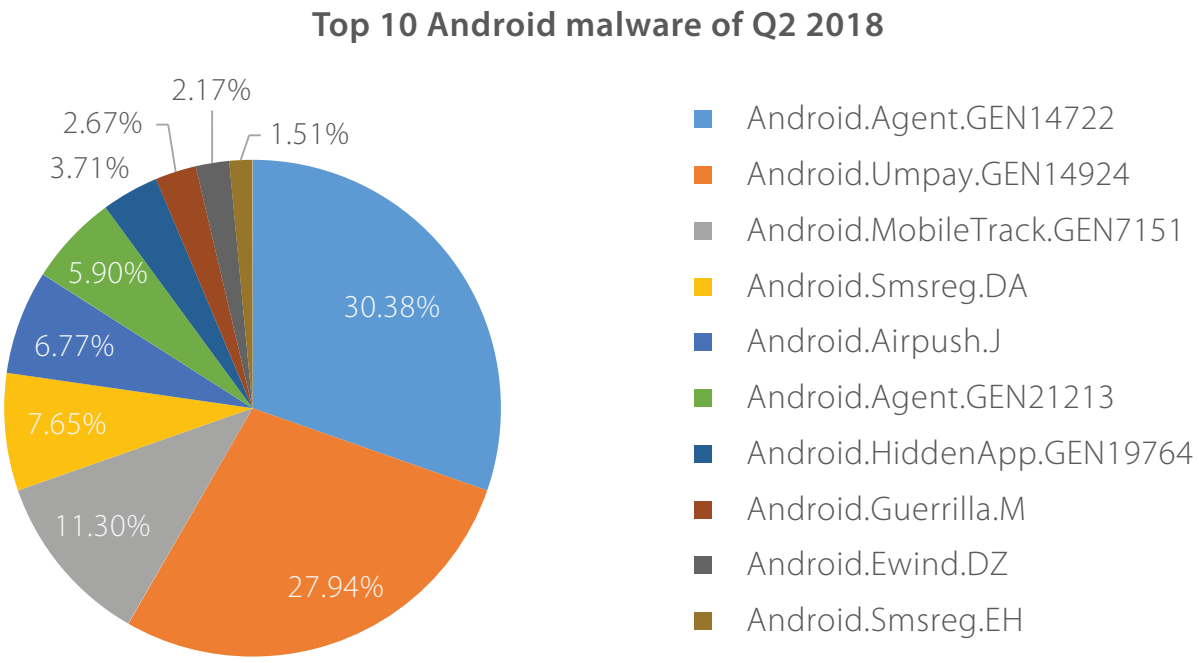


Fig 1

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.Umpay.GEN14924

Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app storess

Behavior:
- Umpay is a Chinese mobile payment SDK, which allows developers to request payments through Web, WAP, and 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.

3. 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.

4. 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.

5. 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.

6. Android.Agent.GEN21213

Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores
Behavior:

- This malware receives commands via SMS from specified numbers and performs malicious activities as directed in the SMS.
- It sets the device's ringer volume to silent mode.
- It can pick up and end the call without user knowledge.
- It can install other apps silently in the background.

7. Android.HiddenApp.GEN19764

Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores
Behavior:

- It disguises as a 'Settings' app. After launching, it hides its icon and runs in the background.
- This Trojan's activity is to visit the web pages in a hidden way that it receives from its C&C server.

8. Android.Guerrilla.M

Threat Level: High
Category: Malware
Method of Propagation: Third-party app stores
Behavior:

- After first launch, it hides its icon and runs in the background.
- It collects system information like account type, model, IMEI, etc.
- It runs its own processes and kills other processes in the background.
- It connects to malicious C&C server and downloads other malicious apps from it.
- The downloaded malicious apps perform further malicious activities.

9. Android.Ewind.DZ

Threat Level: Low
Category: Adware
Method of Propagation: Third-party app stores and repacked apps
Behavior:

- It displays unwanted ads on the infected device.
- It decrypts the malicious file from the asset file.
- It collects device data like SDK version, brand, model, IMEI, screen height, time zone, etc.

10. 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.

Android Security Vulnerabilities Discovered in Q2 2018

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. Fig 2 shows the type of Android security vulnerabilities and their growth from April to June of 2018.

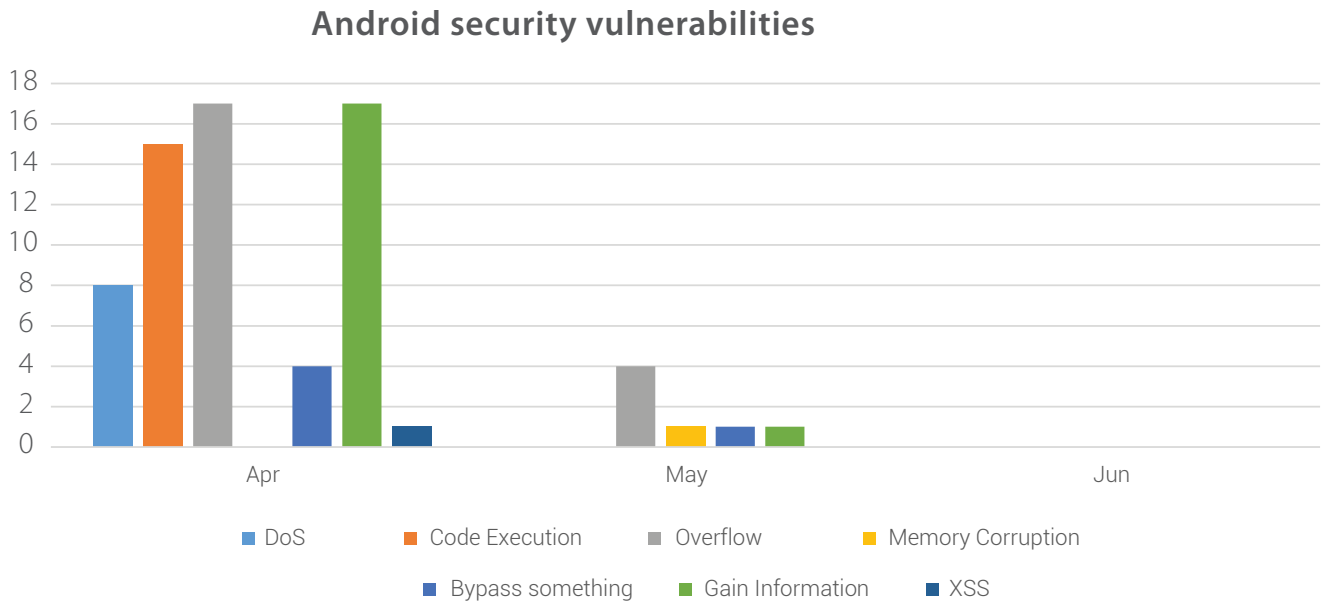


Fig 2

Source: cvedetails.com

Trends in Android Security Threats

I. Rise in cryptocurrency mining malware

Quick Heal Security Labs has observed a rise in cryptocurrency mining malware in Q2 as compared to Q1 & further we may see a rise in this. In general, these malware use techniques to remain hidden from users and perform mining without their knowledge. They use anti-emulation to bypass detection and automated analysis techniques. These malware make excessive use of device resources, which cause over heating & drains device battery.

II. Banking Trojans imitating popular social media and banking apps in India

Quick Heal Security Labs spotted two banking Trojan malware. These malware imitate some popular social and banking apps. While doing so, they gain access to some security permissions on the infected device which allow them to steal the user's banking credentials. The malware are able to do this by displaying a fake window that asks for a debit/credit card number.

Read more:
https://blogs.quickheal.com/quick-heal-detects-another-banking-trojan-imitating-popular-banking-apps-india/

Conclusion

What attracts more than a magnet? You might have guessed it right – it is money! And where there is easy money, there is a lot of hustle and bustle. Till now, ransomware was seen as the ultimate cash cow for attackers – kidnap critical data and ask a ransom in exchange. But, now, there is even a bigger cash cow than ransomware. It is called cryptojacking – using someone else's computer to generate digital cash called cryptocurrency. While a ransomware gets detected after a time and is short-lived, cryptojacking can run almost undetected on users' systems minting money for attackers for as long as they want. Due to its ease of deployment and an instant return of investments, cryptojacking has replaced ransomware as the number one threat for consumers and enterprises. This trend easily sends out a message that time, technology and digital threats wait for no man. Till a few months ago, we thought ransomware was here to stay and it will only grow nastier with time. But, the arrival of cryptojacking proves that we haven't figured it all. We are still not fully capable of predicting what is going to happen in the near future. What we can do is strengthen our defenses, draw our swords, and put up a good fight when the enemy strikes. Hope for the best but prepare for the worst!