Quick Heal

Security Simplified

QUICK HEAL
QUARTERLY THREAT REPORT | Q3 2018

www.quickheal.com

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

Table of contents

Introduction

In the third quarter of 2018, Quick Heal Security Labs detected over 288 million Windows malware. August clocked the highest detection. On a daily basis, Quick Heal detected around 3 Million malware including 7K ransomware, 0.2 Million exploits, 0.1 Million PUA & Adware and 33K Cryptojacking malware. The Trojan horse category retained its position as the most dominant malware in the entire quarter. W32.Ramnit.A was the topmost Windows malware while PUA.Conduitltd.Gen topped the list of PUA and Adware.

A significant and critical observation by Quick Heal Security Labs has been the increase in cryptocurrency mining & banking trojan – **Emotet**. This can be a threat for users of banking apps, especially during this festive season, when online transactions are on the rise.

There has also been a significant increase in Ransomware attacks over this past quarter, especially via **Remote Desktop Protocol (RDP) using brute-force technique**. RDP brute-force attack is basically a kind of ransomware attack that makes use of RDP. Attackers scan a list of IPs to find the default RDP port 3389 that is open for connection. Once the port is discovered, the attacker launches the brute-force attack. This is basically a trial & error technique of User name and password guessing, where the attacker tries a series of commonly used credentials, common word combinations and dictionary words to break through weak passwords. To make things easier for attackers, there are numerous tools readily available that can perform these RDP brute forcing and port scanning with ease. Once attackers gain access, they can bypass your system's antivirus (even if updated) and infect your system.

The third quarter also witnessed Quick Heal Security Labs detecting over 0.9 Million malware, PUA and Adware on Android OS. Android.Umpay.GEN14924 continued to retain its position as the topmost android malware of Q3. A significant trend observed in the third quarter were the apps on play store, which hide themselves after installation and display full screen ads after specific time interval. The most trending scam of Q3 however was the WhatsApp scam message

- **Cadbury 70th anniversary scam**.

Disclaimer: We have made some improvements in the way we calculate our telemetry data. Hence, an increment in detection counts may be observed in this quarter, as compared to the previous quarters.

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

Quick Heal Detection on Windows Q3 2018

Malware
Per Day: **3,130,946**
Per Hour: **130,456**
Per Minute: **2,174**

Ransomware
Per Day: **7,246**
Per Hour: **302**
Per Minute: **5**

Exploit
Per Day: **250,063**
Per Hour: **10,419**
Per Minute: **174**

PUA & Adware
Per Day: **130,409**
Per Hour: **5,434**
Per Minute: **91**

Cryptojacking
Per Day: **33,433**
Per Hour: **1393**
Per Minute: **23**

Infector
Per Day: **414,205**
Per Hour: **17,259**
Per Minute: **288**

Worm
Per Day: **290,215**
Per Hour: **12,092**
Per Minute: **202**

Source: Quick Heal Security Labs

Windows Malware Detection in Q3 2018

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

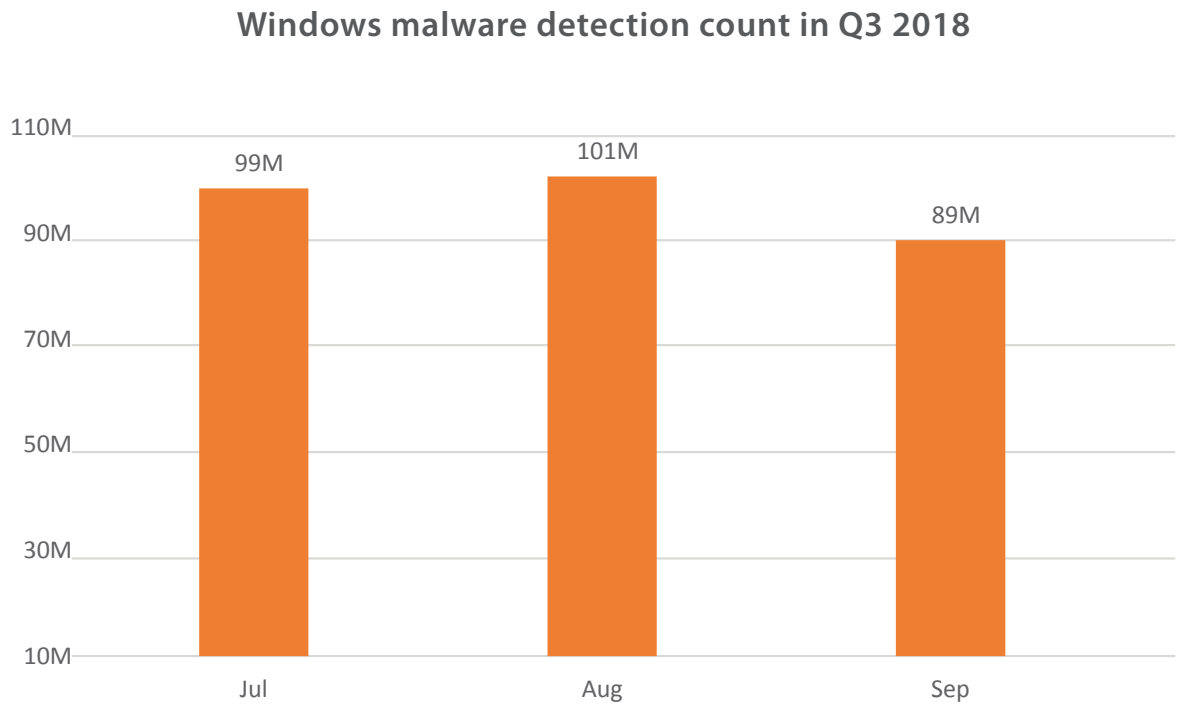

Fig 1

Observations

- Quick Heal detected over 288 million Windows malware in Q3 2018.
- August clocked the highest detection of Windows malware.

Top 10 Windows Malware

Fig 2 represents the top 10 Windows malware of Q3 2018. These malwares have made it to this list based upon their rate of detection from July to September.

Top 10 Windows malware of Q3 2018

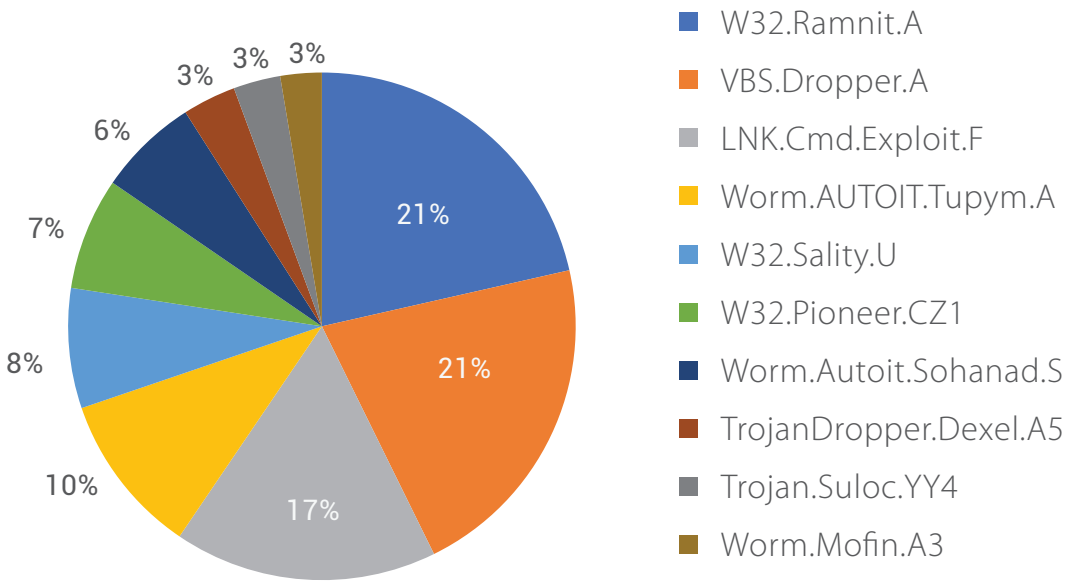

Fig 2

1. W32.Ramnit.A

Threat Level: Medium
Category: Infector
Method of Propagation: USB Drives, Other malware, Exploit Kits, Spoofing the URL, Bundled application
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 speeds 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 it's automatic execution at every system start up.

2. VBS.Dropper.A.

Threat Level: Medium
Category: Dropper
Method of Propagation: Web page
Behavior:

- This malware is spreading 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.

3. 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.

4. 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.

5. W32.Sality.U

Threat Level: Medium
Category: 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.
- It tries to terminate security applications and deletes all files related to any security software installed on the system.
- It steals confidential information from the infected system.

6. W32.Pioneer.CZ1

Threat Level: Medium
Category: Infector
Method of Propagation: Removable or network drives
Behavior:

- Malware attaches its code to files present on disk and shared network. It decrypts malicious dll present in the file & drops it.
- This dll performs malicious activity and collects system information & sends it to CNC server.

7. 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.

8. TrojanDropper.Dexel.A5

Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites
Behavior:

- Allows entry of other malware into the infected system. Changes registry and browser settings.
- Automatically redirects the user to malicious websites to drop more Trojan malware on the system.

- Steals confidential data from the infected system and can also destroy the data.
- Slows down system performance by consuming more resources.

9. Trojan.Suloc.YY4

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

- Copies itself on the targeted drive, and start-up folder.
- 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.

10. Worm.Mofin.A3

Threat Level: Medium
Category: Worm
Method of Propagation: Removable or network drives
Behavior:

- Uses the Windows Autorun function to spread via removable drives. Creates an autorun.inf file on infected drives.
- This file contains instructions to launch the malware automatically when the removable drive is connected to a system. Searches for documents with extensions such as .doc, .docx, .pdf, .xls, and .xlsx. It copies the files it finds and sends them via SMTP (Simple Mail Transfer Protocol) to the attacker.

Category-wise Windows Malware Detection

Fig 3 represents the various categories of Windows malware detected by Quick Heal in Q3 2018.

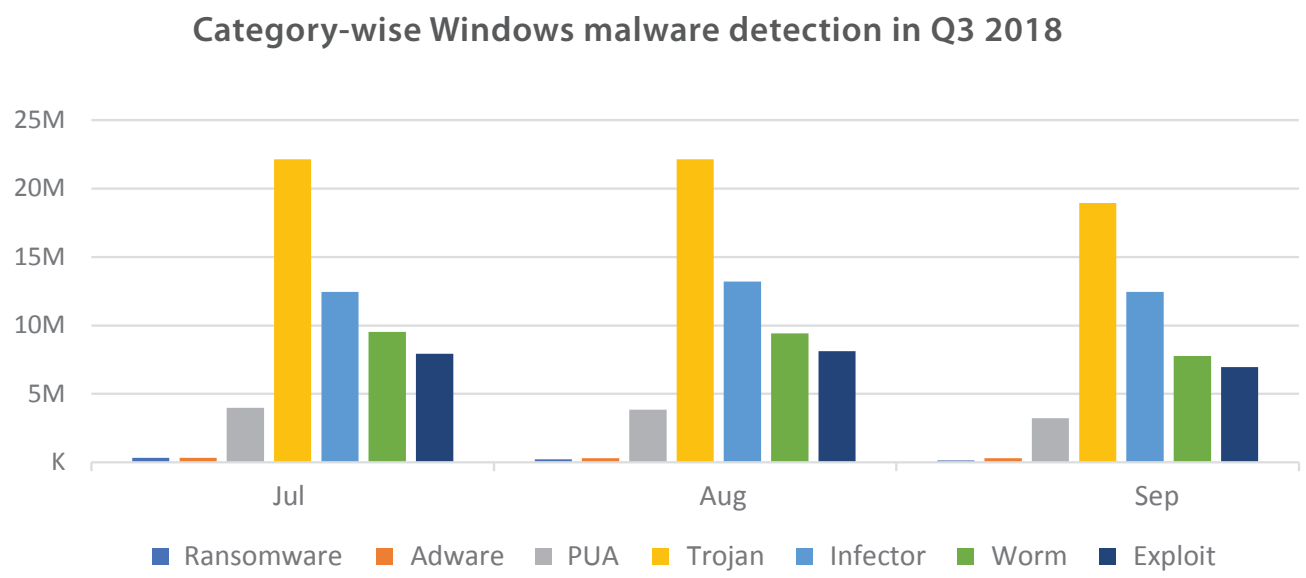

Fig 3

Observations

- The Trojan Horse family clocked the highest detection in the entire quarter.
- Following is a comparative analysis between the detection count of Q3 2018 and Q2 2018.

Detection Count			
Malware Category	**Q2 2018**	**Q3 2018**	**Growth**
Trojan	63,249,214	63,209,397	0.06% decrease
Infectors	23,457,813	38,106,864	62.4% increase
Exploit	12,697,113	23,005,760	81.1% increase
Worm	11,371,699	26,699,811	134.7% increase
PUA	3,226,738	11,065,332	242.9 % increase
Ransomware	1,454,820	666,618	54.1% decrease
Adware	417,152	932,336	123.5% increase

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 Q3 2018.

Top 10 PUA & Adware of Q3 2018

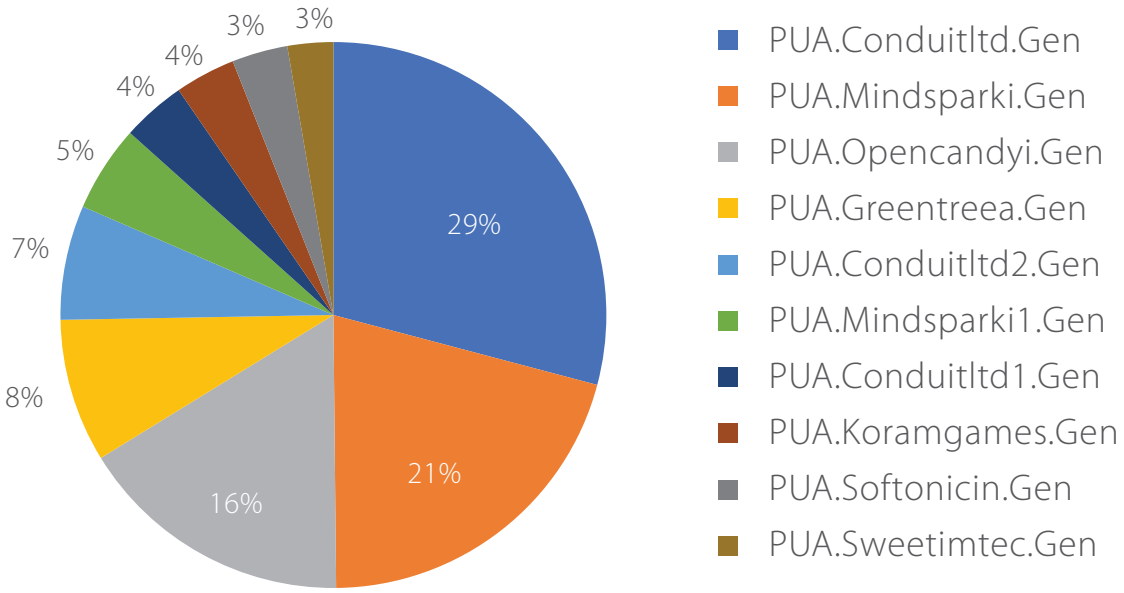

Fig 4

Observations

As against Q2 in which PUA.Mindsparki.Gen was the top PUA, in Q3 2018 PUA.Conduitltd.Gen was registered as the top PUA.

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 Q3 2018.

Top 10 host-based exploits of Q3 2018

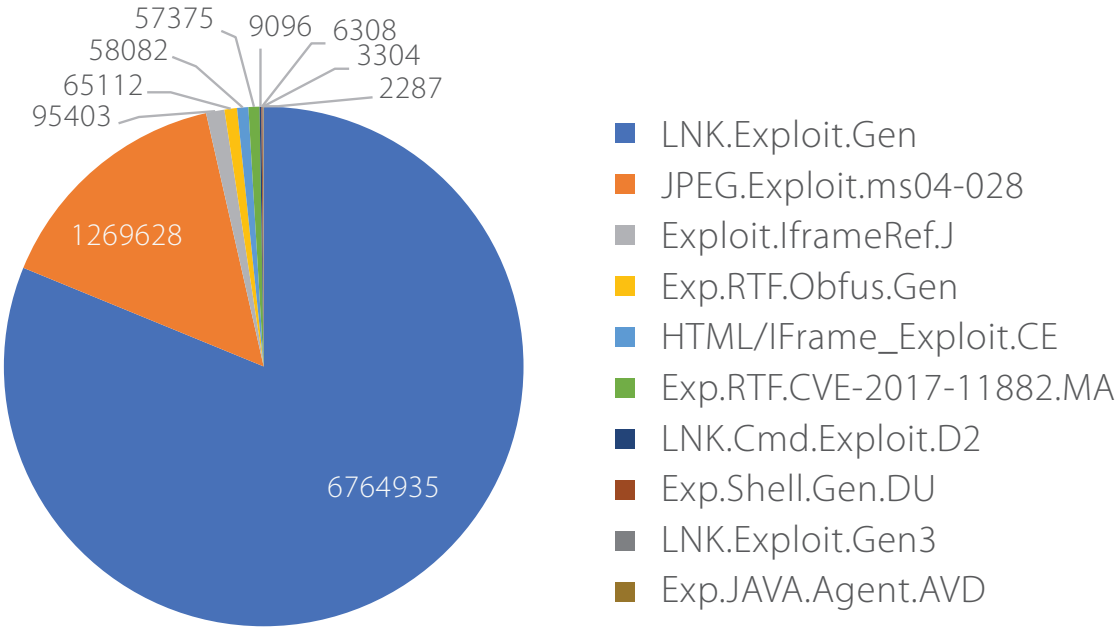

Fig 5

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.

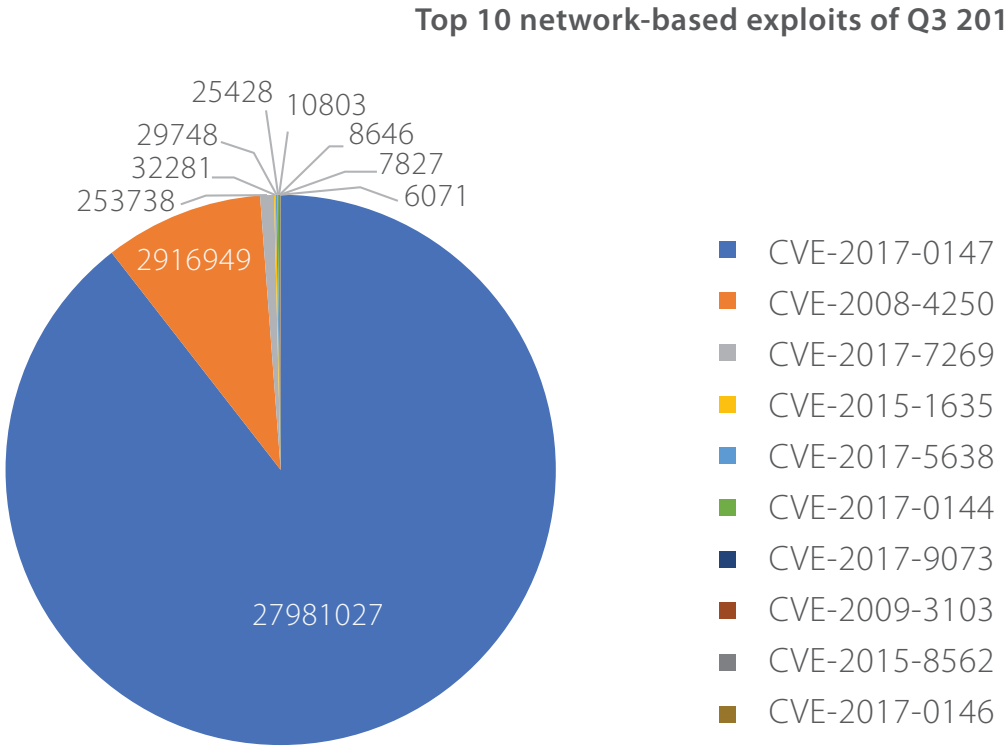

Fig 6

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

1. I am invisible – Monero (XMR) Miner

From the last one year, Quick Heal Security Labs has been observing a boost in the number of mining malware. Nowadays malware authors are using mining as a replacement for Ransomware to make money. Recently Quick Heal Security Labs came across a malware which mines Monero (XMR). This miner has many different components in it. The infection vector of this mining malware is still unconfirmed, but based on attribution this miner arrives on the system via spear phishing, malvertising etc. As the price and appreciation of digital currencies has grown exponentially, mining malware too have increased over the last year. In fact, miners are so common that thousands of computers are already infected. The number of mining malware has increased, and they have also become more complex.

Read more:
https://blogs.quickheal.com/invisible-monero-xmr-miner/

2. A new ransomware campaign in the wild,Ryuk!!

Recently, Quick Heal Security Labs observed a new destructive ransomware named 'Ryuk. Ransomware'. This ransomware campaign has already affected many users worldwide and seems to be a spear phishing attack. The compelling thing, it encrypts victim files without appending any extension but making files unreadable. Ryuk uses robust military algorithms such as 'RSA4096' and 'AES-256' to encrypt files. We have seen that the infection vector of this ransomware is exploit kits and spam emails. This ransomware demands a ransom ranging from 15 BTC to 50 BTC in the form of Bitcoin to decrypt the files.

Read more:
https://blogs.quickheal.com/new-ransomware-campaign-wildryuk/

3. Again! A New .NET Ransomware Shrug2

For several months, Quick Heal Security Labs has been observing an increase in ransomware which are built in .NET framework. Ransomware like SamSam, Lime and now Shrug was found to be built in .NET framework. Malware authors are finding it very easy to build and obfuscate malware in .NET framework rather than making them in other compilers. Quick Heal Security Labs has found a new ransomware named Shrug2. This ransomware demands a ransom of 70$ in the form of Bitcoin for decrypting files. The infection vector of this ransomware is still unknown, but this file may arrive on the victim's machine via phishing emails, RDP brute force attacks, malvertising, bundled with other files, etc.

Read more:
https://blogs.quickheal.com/new-net-ransomware-shrug2/

ANDROID

Quick Heal Detection on Android Q3 2018

Malware
Per Day: **3514**
Per Hour: **146**
Per Minute: **2**

Adware
Per Day: **1134**
Per Hour: **47**
Per Minute: **1**

Potentially Unwanted Application (PUA)
Per Day: **6031**
Per Hour: **251**
Per Minute: **4**

Top 10 Android Malware of Q3 2018

Fig 1 represents the top 10 Android malware of Q3 2018. These malwares have made it to this list based upon their rate of detection during the period of July to September in 2018.

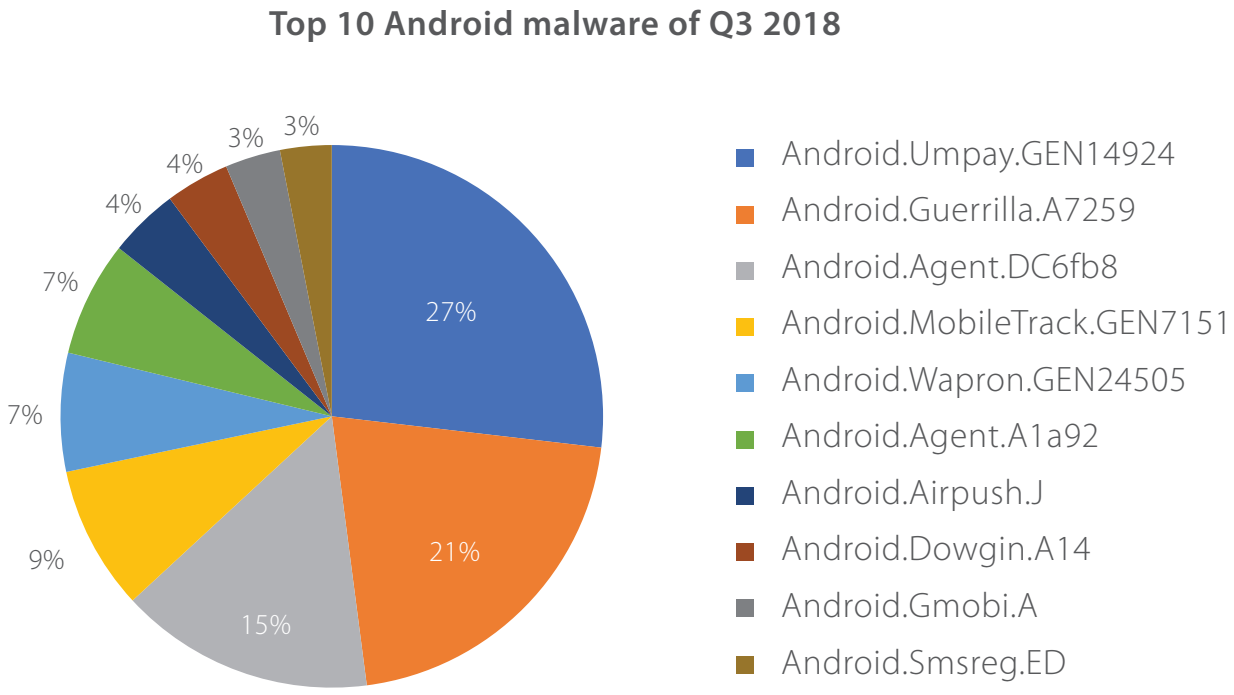

Fig 1

1. 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.

2. Android.Guerrilla.A7259

Threat Level: High
Category: PUP
Method of Propagation: Third-party app storess
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.

3. 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.

4. 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

5. Android.Wapron.GEN24505

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

- This family uses the 'Jiagu' Android app protector.
- This protector is commonly used by developers to prevent their apps from being tampered or decompiled.

- This technique makes it difficult to run reverse engineering on the malicious app because it encrypts the dex files and saves it in native files.
- It releases the data into memory and decrypts it while runtime.
- Decrypted DEX file may be a malicious or a clean file.

6. Android.Agent.A1a92

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

- It Carries another malicious file in an encrypted format, decrypts it at runtime and drops it at a later time on the infected phone.
- The decrypted file is nothing but banker malware.
- This trojan displays an overlay phishing login form over targeted apps window, where it asks the user to enter a username, password, and other sensitive data.
- Apart from this it also reads SMS, contacts and uploads it to C&C server.
- It receives commands from C&C server and perform malicious activity according to this.

7. 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.

8. Android.Dowgin.A14

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

- It is an advertising module that comes with other android applications.
- This is used to generate revenue for the software developers.
- It sends the infected device's information such as IMEI, IMSI, network operator name, screen size etc.
- It may download other applications by using user's mobile data.

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 SMS in order to play the next stage or to get extra lives in the game.
- Collects personal information such as device ID, phone number, incoming message, and sends the stolen data to a remote server.

Android Security Vulnerabilities Discovered in Q3 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 July to September of 2018.

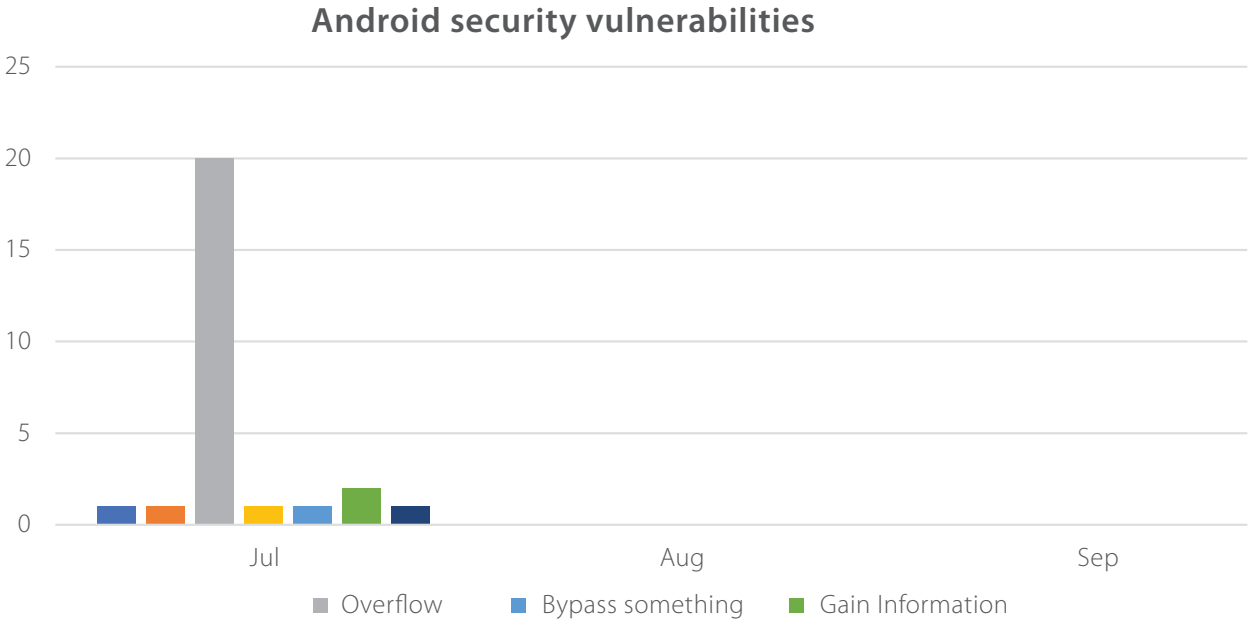

Fig 2

Source: https://www.cvedetails.com/

Trends in Android Security Threats

1. Be aware! Hiddad Malware present on Google Play Store.

Quick Heal Security Lab has spotted a couple of applications on play store 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.

Even if users want to uninstall these applications, they won't be able to find in the app manager as it was installed with the name 'Google Play Service, Google Play Store' and uses icon of genuine apps such as Google Play Store, default Android icon or YouTube.

After hiding itself, it interrupts user by frequently showing advertisements while using other applications. This type of malwares is present on Google Play store with more than 50k+ downloads. Quick Heal Security Lab reported this to Google and those applications have been removed from Play store now.

Read more: https://blogs.quickheal.com/aware-hiddad-malware-present-google-play-store/

2. Android malware that combines a Banking Trojan, Keylogger, and Ransomware in one package

This malware has all basic functionalities of the Android banker along with additional features like call forwarding, sound recording, keylogging and ransomware activities. It has ability to launch user's browser with URL received from the C&C server.

It repeatedly opens the accessibility setting page until the user switches ON the 'AccessibilityService'. The AccessibilityService allowing the Trojan to enable and abuse any required permission without user concern. After launching one of the targeted application, the Trojan displays an overlay phishing login form of confidential information over its window where it asks the user to enter a username, password, and other sensitive data.

Read more:
https://blogs.quickheal.com/android-malware-combines-banking-trojan-keylogger-ransomware-one-package/

3. Beware of the Cadbury 70th anniversary scam on WhatsApp!

WhatsApp currently has over 200 million monthly active users in India. No wonder it has become a popular tool for scammers and they want to exploit this opportunity. Almost all aspects of life like family affairs, latest news, awareness are organized and discussed in WhatsApp groups. It is easy way to get information and connect many people at a time. This anniversary scam on WhatsApp is a scam because Cadbury hasn't announced any kind of anniversary offers on its official website. And link mentioned in this scam is fake link. After clicking on it. It took user to a website that asked 4 questions. After answered all the questions, it showed a congratulatory message followed by instructions on how to proceed. In which it asks user to share it with other 15 contacts via WhatsApp. After sharing it asked user to install 1 app and run it for 30 second and only then user would be able to claim the free basket.

Read more: https://blogs.quickheal.com/beware-cadbury-70th-anniversary-scam-whatsapp/

Conclusion

The past quarter witnessed ransomware attacks moving altogether to a new and critical level. With Quick Heal Security Labs observing a significant increase in cryptocurrency mining and ransomware attacks via RDP, it is important for users to be on the alert at all times.

To start with, ensure that all the protection levels on your security software are ON for the first line of protection. Take care to back up your data on a frequent basis, so that you do not lose any important data in the occurrence of an attack. As a general practice, turn OFF RDP if not in use or use strong and unique password combinations making it hard for attackers to guess user IDs and passwords. This can save your system from critical threats like RDP brute-force attacks.

Most importantly, if you are inclined to do a lot of online shopping and online transactions during this festive season, make sure to use Multi/Two Factor authentication to prevent attacks from banking trojan – Emotet. Remember, an ounce of prevention is worth a pound of cure!!

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