Quick Heal
Security Simplified

SEQRITE

QUICK HEAL
QUARTERLY THREAT REPORT | Q1 2018

www.quickheal.com

Contributors

- Quick Heal Security Labs
- Quick Heal Marketing Team

Table of contents

Introduction

In the first quarter of 2018, Quick Heal Security Labs detected over 181million Windows malware. March clocked the highest detection. On a daily basis, Quick Heal detected around 2,017,722 malware, 31,790 ransomware, 189,505 exploits, and 58,874 PUA & Adware. The Trojan horse family retained its position as the most dominant malware in the entire quarter. It grew 13.9% compared with its detection in Q4 2017. The top malware of the year is a destructive Trojan called LNK.Exploit.Gen. Quick Heal Security Labs noticed a worrying trend in the distribution of ransomware. It involves the heavy use of .NET framework by ransomware authors. Case in points include SamSam ransomware, BlackRuby ransomware, Lime ransomware, and Ransomware-as-a-Service.

Quick Heal Security Labs recorded over 1 million detection (malware + PUA + adware) on the Android OS in Q1 2018. The PUA (Potentially Unwanted Application) family comprised 47% of the total detection of the year. This is evident by the fact that the top Android malware of the quarter was a PUA named Android.Umpay.GEN14924. The main trends observed in the Android threat landscape include the persistent growth in fake Android apps, banking Trojans heavily targeting banking apps, cryptomining apps, and hidden adware.

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 Q1 2018

Malware

Per Day: **2,017,722**
Per Hour: **84,071**
Per Minute: **1,401**

Ransomware

Per Day: **31,790**
Per Hour: **1,325**
Per Minute: **22**

Exploit

Per Day: **189,505**
Per Hour: **7,896**
Per Minute: **132**

PUA and Adware

Per Day: **58,874**
Per Hour: **2,453**
Per Minute: **41**

Source: Quick Heal Security Labs

Windows Malware Detection in Q1 2018

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

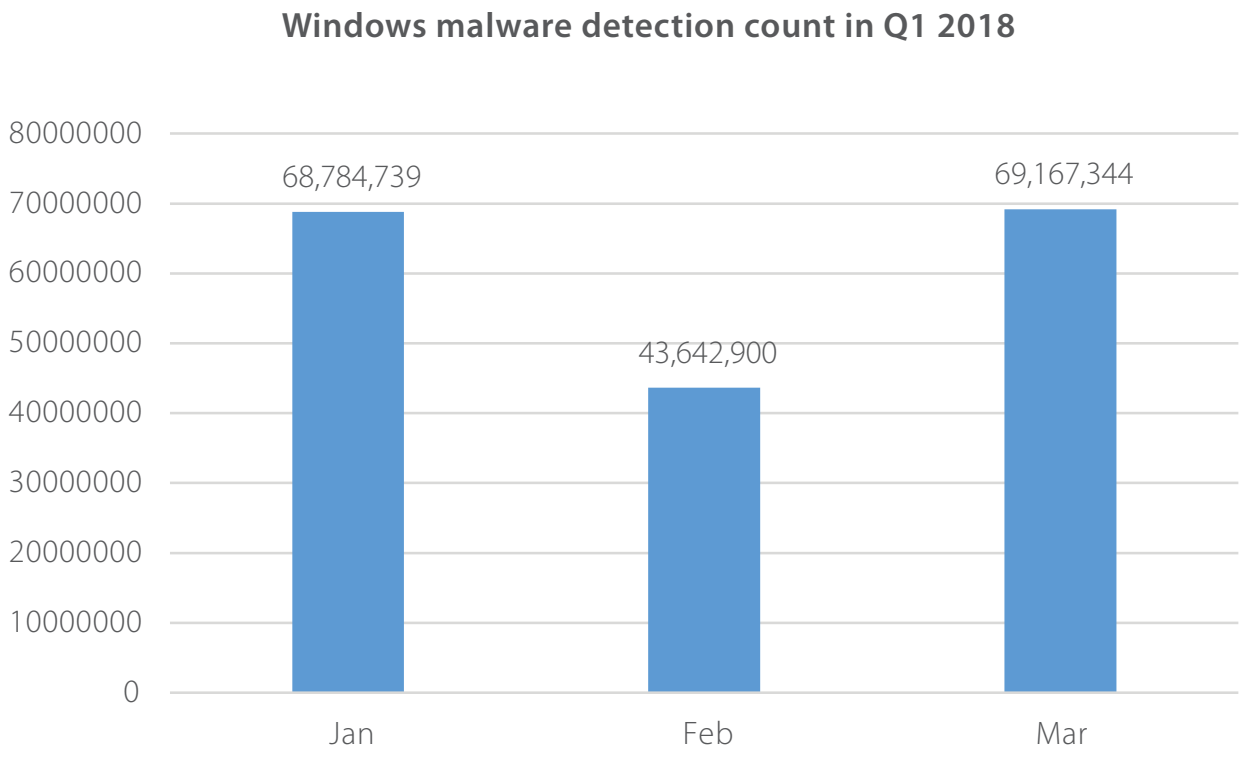


Fig 1

Observations

- Quick Heal detected over 181 million Windows malware in Q1 2018.
- March clocked the highest detection of Windows malware in 2018.

Top 10 Windows Malware

Fig 2 represents the top 10 Windows malware of Q1 2018. These malware have made it to this list based upon their rate of detection from Jan to March.

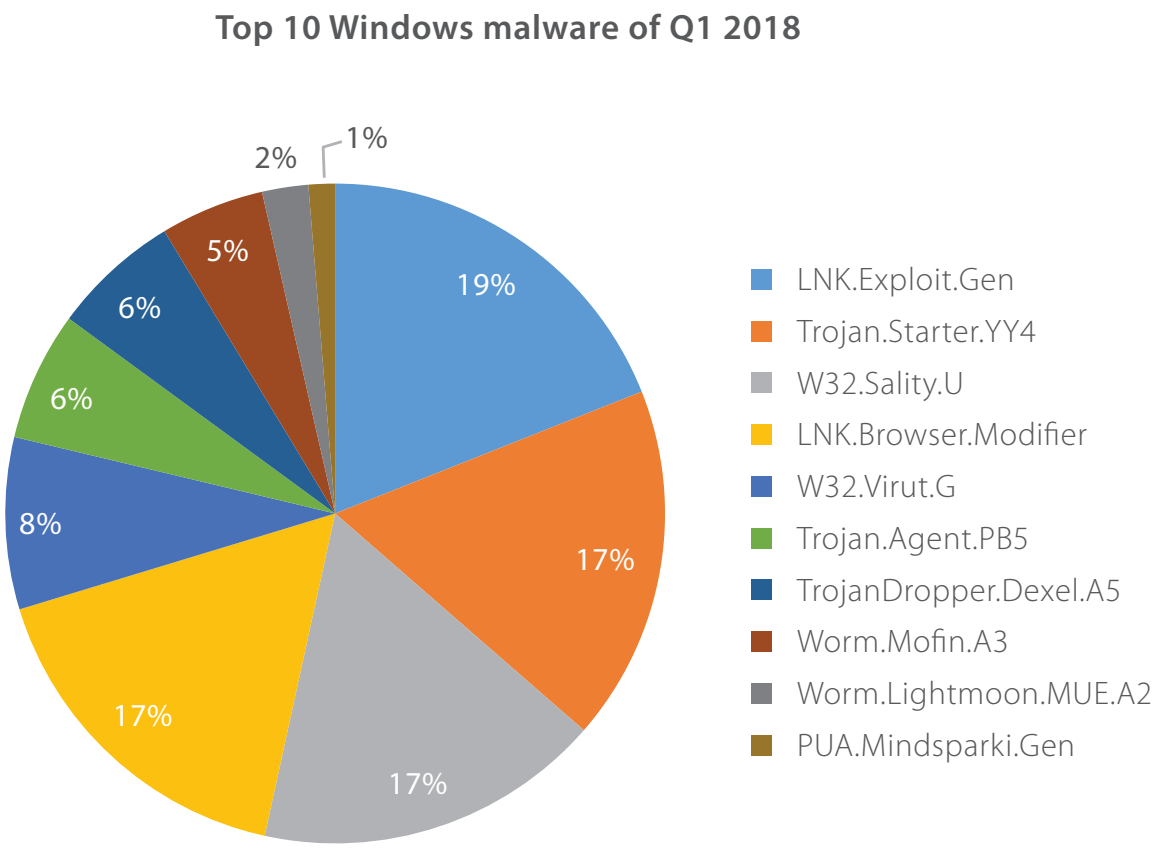


Fig 2

1. 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.

2. 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.

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. 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.

6. Trojan.Agent.PB5

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

- This is a component of a multi-component malware.
- It uses the Windows shortcut file functionality and spreads via removable drives.
- This shortcut file contains instructions to launch the malware automatically and open a hidden folder where all the data is stored.
- Its components are "desktop.ini", Thumbs.db", and a random extension dll file.

7. 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.

8. 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.

9. Worm.Lightmoon.MUE.A2

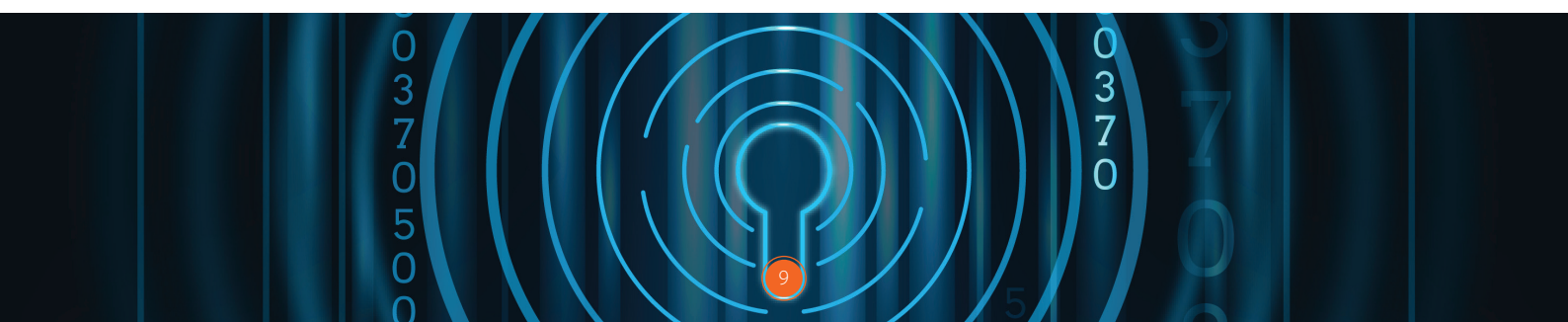
Threat Level: Low
Category: Worm
Method of Propagation: Spam emails and P2P (Peer to Peer) sharing applications
Behavior:

- Arrives in the system as an attachment in spam emails.
- Modifies the system settings and registry entries.
- Monitors keystrokes entered by the user and further sends the logged data to a remote site.
- System information such as drive, folder, and file names can also be sent to the remote attacker by this malware.

10. PUA.Mindsparki.Gen

Threat Level: Medium
Category: Potentially Unwanted Application
Method of Propagation: Bundled software and malicious websites
Behavior:

- Changes the infected system's Internet browser homepage and default search engine to ask.com or yahoo.com.
- Installs a toolbar powered by ask.com.
- Asks the user to download software mentioned on the toolbar.



Category-wise Windows Malware Detection

Fig 3 represents the various categories of Windows malware detected by Quick Heal in Q1 2018.

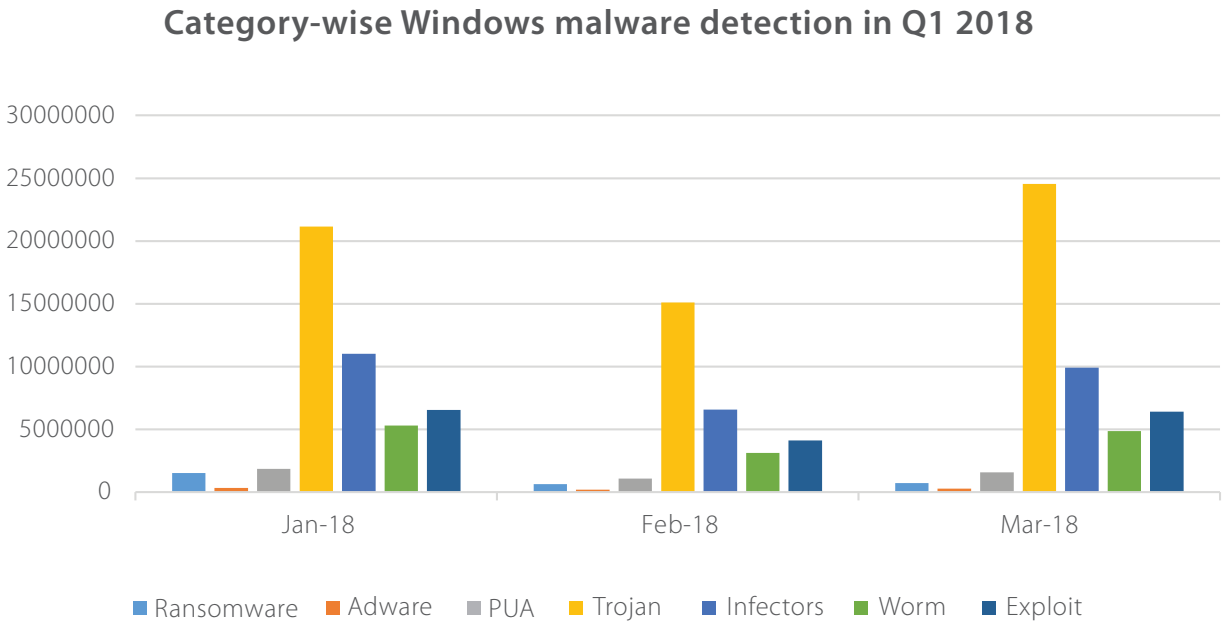


Fig 3

Observations

- The Trojan Horse family clocked the highest detection in the entire quarter.
- Following is a comparative analysis between the detection count of Q1 2018 and Q4 2017.

Detection Count			
Malware Category	**Q4 2017**	**Q1 2018**	**Growth**
Trojan	53,360,142	60,797,318	13.9% increase
Infectors	28,863,738	27,526,654	4.6% decrease
Exploit	19,827,915	17,055,455	13.9% decrease
Worm	13,770,170	13,313,316	3.3% decrease
PUA	5,415,412	4,499,151	16.9% decrease
Ransomware	3,325,829	2,861,095	13.9% decrease
Adware	1,100,839	799,530	27.3% 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 Q1 2018.

Top 10 PUA & Adware of Q1 2018

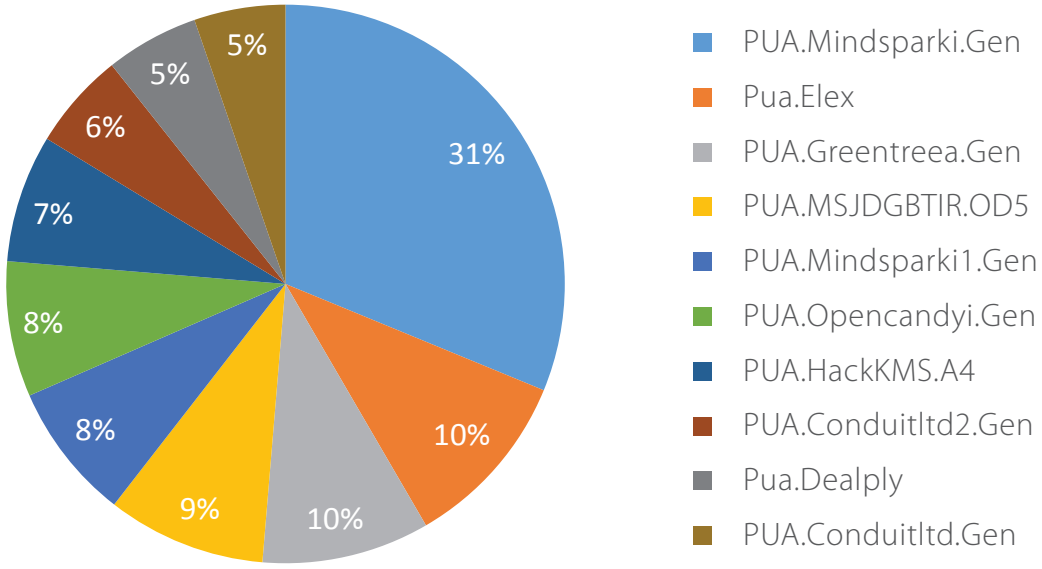


Fig 4

Observations

PUA.Mindsparki.Gen was registered as the top PUA in 2017 and it continues to be so in Q1 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 Q1 2018.

Top 10 host-based exploits of Q1 2018

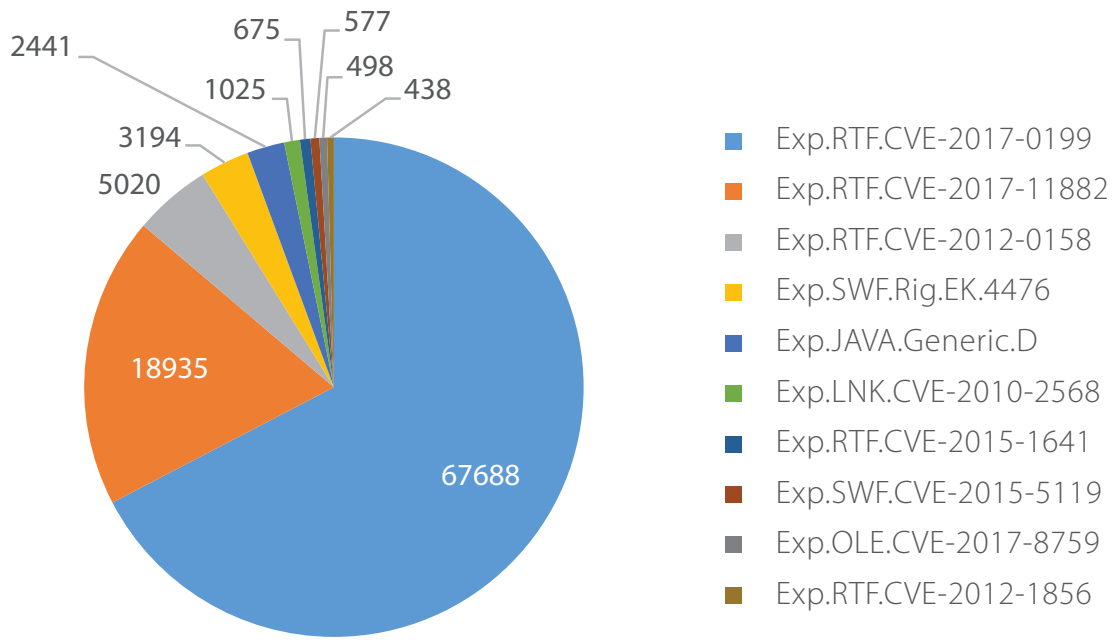


Fig 5

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.

Top 10 network-based exploits of Q1 2018

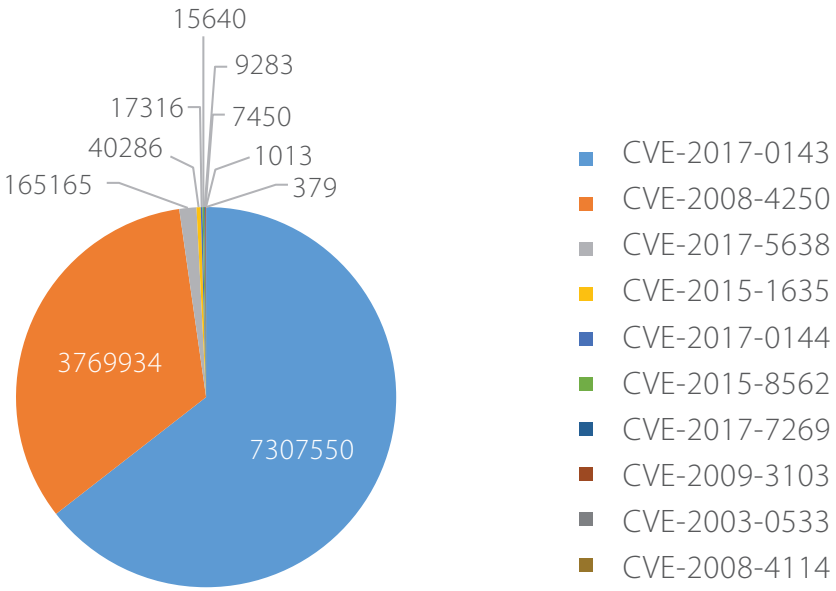


Fig 6

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. Rise in .NET ransomware

In Q1 2018, ransomware maintained its dominance as the most destructive malware. We observed the use of .NET framework in the development of ransomware – this is a new trend in the malware's implementation. Below are some case in points.

- The component 'Runner' that decrypts the main SamSam ransomware payload was found to have been developed in .NET. In late March 2018, the city of Atlanta battled with the SamSam ransomware for over a week. Major government offices, hospitals, educational institutions, and industrial control services were targeted. Read more about this here - http://blogs.quickheal.com/runner-key-component-samsam-ransomware-campaign/
- The BlackRuby ransomware, bundled with Monero miner, was developed in the .NET framework. The executable was further obscured using "Babel Obfuscator" to protect it against reverse engineering.
- The Lime ransomware was discovered in Q1 2018 and it spread through spam email; it was a .NET executable. Read more about this here - http://blogs.quickheal.com/beware-new-net-ransomware-encrypting-files-lime/
- RaaS (Ransomware-as-a-Service) components are also being developed in the .NET framework. RaaS is an ecosystem for ransomware generation and distribution. The latest addition to RaaS league is Data Keeper. It's available on the black market for free and it offers various services.

Why .NET?

.NET is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It has a huge collection of predefined class libraries that has support for simple and complex data structures. Ransomware creators are leveraging the power of the .NET framework to create new payloads which takes lesser time with fewer efforts. This is a tell-tale sign of a steady rise in the number of .NET ransomware.

II. MIRUS - a cryptomining virus

In Q1 2018, Quick Heal Security Labs came across a malware which not only infected files but could also perform cryptomining by injecting CoinHive JavaScript into HTML files. This interesting but new modification creates additional challenges for security researchers. In case of MIRUS, its malware authors used miner scripts as the payload of the virus thus making mining on users' machine possible and consistent in time and space frame. Read more about this here - http://blogs.quickheal.com/mirus-cryptomining-virus/

III. New attack vector ".url"

In Q1 2018, Quick Heal Security Labs witnessed the emergence of a new attack vector ".url". We observed a spam campaign that uses .url files as a first-stage downloader to spread malware. The .url attack vector is currently being used by the Quant Loader malware family. We may see a rise in the use of this novice attack vector .url by other malware families in the coming days.Further reading on this:

- http://blogs.quickheal.com/depth-analysis-new-emerging-url-malware-campaign-analysis-quick-heal-security-labs/
- http://blogs.quickheal.com/email-campaign-using-url-extensions-abuse-internet-explorer-vulnerabilities-cve-2016-3353/

ANDROID

Quick Heal Detection on Android Q1 2018

Malware

Per Day: **2,741**
Per Hour: **114**
Per Minute: **2**

Adware

Per Day: **4,733**
Per Hour: **197**
Per Minute: **3**

Potentially Unwanted Application (PUA)

Per Day: **6,580**
Per Hour: **274**
Per Minute: **5**

Source: Quick Heal Security Labs

Top 10 Android Malware of Q1 2018

Fig 1 represents the top 10 Android malware of Q1 2018. These malware have made it to this list based upon their rate of detection during the period of Jan to March in 2018.

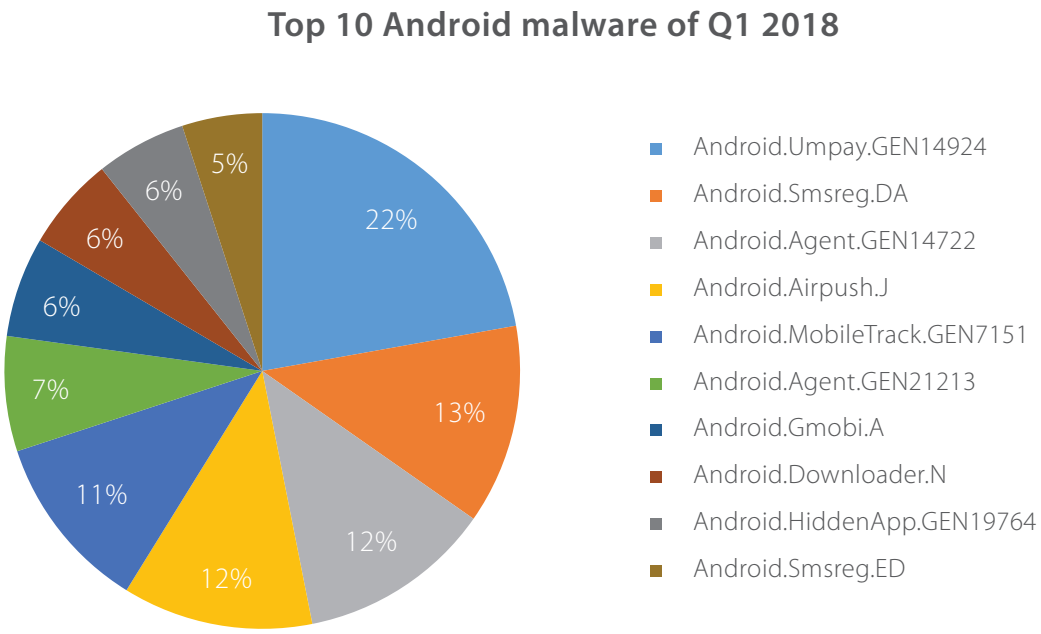


Fig 1

1. 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.

2. 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.

3. 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.

4. Android.Airpush.J

Threat Level: Low
Category: Malware
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.

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.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.Gmobi.A

Threat Level: High
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.

8. Android.Downloader.N

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

- Looks like a genuine app but when launched, it redirects the user to the Google Settings web page.
- In the background, the app connects to a third-party server.
- Downloads malicious apps from the server it connects to after a specific interval of time.
- The downloaded malicious apps can infect the device further or may steal user information before sending it to the external server.

9. Android.HiddenApp.GEN19764

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.

10. Android.Smsreg.ED

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

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

Android Security Vulnerabilities Discovered in Q1 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 Jan to March of this year.

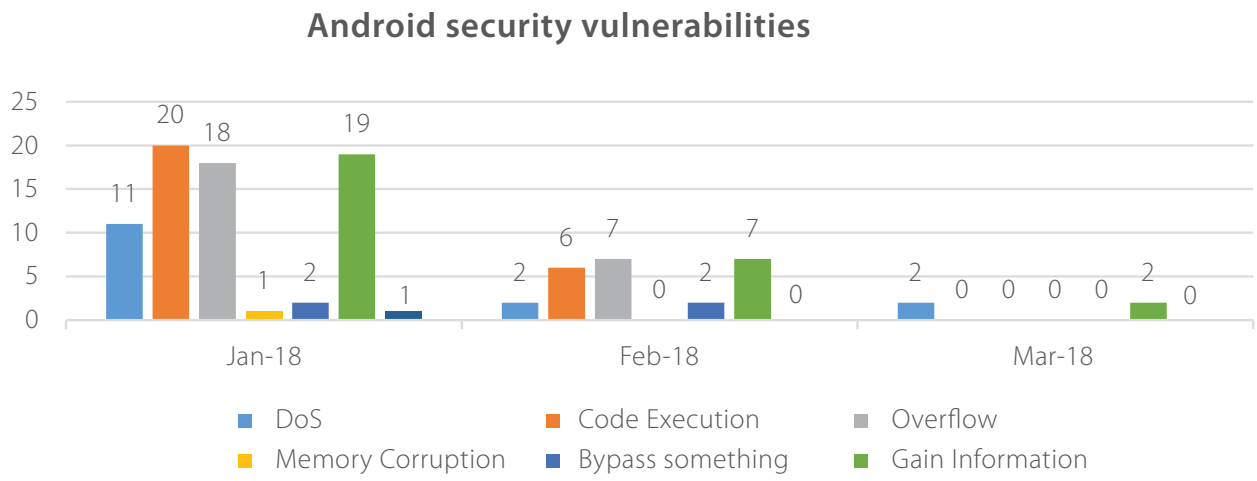


Fig 2

Source: cvedetails.com

Trends in Android Security Threats

The persistent growth of fake Android apps

As predicted in the Quick Heal Annual Threat Report 2018, incidences of fake apps on Google Play Store are increasing. In Q1 2018, Quick Heal Security Labs reported several fake apps to Google. Fake apps are crafted to look like genuine apps to misguide and trick users.

One case in point was an incident involving a fake app that claimed to help users invest in JioCoin. You may read its analysis by Quick Heal Security Labs here - http://blogs.quickheal.com/beware-fake-apps-claim-help-invest-jiocoin/

It is worth noting that some fake apps manage to gain good ratings and more download counts than their original counterparts. More than 35 apps that claimed to be antivirus apps were removed from Google Play. They searched for user apps from a blacklist and whitelist prepared on the base of a package name and permissions; the interesting part is, they detect themselves as malicious apps. AV Comparatives is a well-known organization which conducts independent tests of antivirus software. It had recently released a report on the premise of a fake antivirus app called Virus Shield. This app was on sale on Google Play and did nothing as it claimed to (scam mobile devices for malware). So, the report was released to help users distinguish between genuine and fake antivirus apps. Read the complete report here - https://www.av-comparatives.org/wp-content/uploads/2018/03/avc_android_201802_en.pdf

Banking Trojan

In Jan 2018, Quick Heal Security Labs detected an Android Banking Trojan malware targeting more than 232 apps including apps offered by Indian banks. Like most other Android banking malware, even this one was designed to steal login credentials, hijack SMSs, upload contact lists and SMSs on a malicious server. The most concerning part, however, was that the malware was designed to display an overlay screen on top of legitimate apps to capture sensitive information such as net banking details, credit/debit card numbers and so on. Read more about his malware here - http://blogs.quickheal.com/android-banking-trojan-targets-232-apps-including-indian-banks

Monero-mining malware

The Monero-mining malware app's icon is identical to the Google Play Store update app. When the app is downloaded, the user receives an "Activate Device Administrator" pop-up. On selecting the 'Cancel' option, it does not disappear and keeps popping up until the user selects 'Activate'. Once the permission is granted, the app hides and starts mining Monero in the background. It also checks whether the app is running on the device/emulator. If it finds the device running on the emulator, it doesn't start its activity.

Hidden adware

As a way to make revenue, advertising companies are getting more aggressive by including functionality in their apps to display ads. Recently, seven apps (six QR reader apps and one smart compass) were found on Google Play. These apps wait for six hours to start their activity by flooding the user's mobile screen with ads, opening web pages full of ads and relay ads-related notifications.

Conclusion

With heavy penetration of the Internet into almost every household, data privacy has had its day. The Facebook data leak scandal which rocked the tech industry is a blistering example of the way our privacy is getting compromised at the cost of our obsession with social networking. To give you a brief recap, Facebook exposed data of 87 million users to a researcher hired by Cambridge Analytica (a personality profiling company involved in the Donald Trump presidential campaign, 2016). Among the affected were half a million users in India. This researcher built a Facebook app based on a personality quiz. The app not only collected the data of people who took the quiz but also the data of the friends of these people (which adds up to 87 million users). And in 2015, the researcher sold this data to Cambridge Analytica. And this very Facebook data leak has been alleged to have played a decisive role in U.S. President Donald Trump's victory in 2016. Who would have guessed it? This story goes deeper than you can think; a simple search on Google about the Facebook-Cambridge incident will help you get the entire picture of what happened and how it happened. So, while it may seem that such incidents do not concern you, it actually does but on a subliminal level - you won't catch the drift. If firms can use/misuse your data to unethically calibrate the course of an event as big as a democratic election, then there is no saying what other monumental changes can occur. What we are trying to say here is, data is the new oil. Our data must stay in our hands and used exactly like the way we want it while being complete aware about how it is being used. Let's not give the security of our data the back burner treatment anymore. Our data is us; if we lose it, if someone misuses it; it is us who will take the fall. With that thought, be careful of apps and websites you decide to willingly share your personal data with and stay away from those who are after it. Your data is you; keep it safe.