Quick Heal
Security Simplified

SEQRITE

Quick Heal Quarterly Threat Report | Q2 2017

www.quickheal.com

Contents

Contributors:

Anand Singh
Aniruddha Dolas
Anita Ladkat
Dipali Zure
Pallavi Pangavhane
Prachi Sudame
Pranali More
Prashant Kaam
Prashil Moon
Priyanka Dhasade
Sandip Borse
Sanket Temgire
Shraddha Khedkar
Swati Pharate

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.

www.quickheal.com
www.seqrite.com

About Quick Heal Security Labs

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

Introduction

In Q2 2017, over 224 million malware samples were detected on the systems of Quick Heal users – April had the highest count. Compared with Q1 2017, Q2 saw a drop of about 24% in the detection count. The top malware detected in this quarter is a Trojan that changes web browser settings and discreetly steals user information. Free software turns out to be the most common source of malware infection followed by spam emails and removable drives as other carriers. The talk of the town in Q2 has been the infamous WannaCry and NotPetya Ransomware – the biggest ransomware attack in history. The malware swooped over 230,000 computers in more than 150 countries. While the attack began on 12th May, Quick Heal started detecting the exploits used in the attack from May 5th onwards. We blocked over 1 million attempts made by the exploits used to spread this ransomware. Quick Heal Security Labs detected 8 new ransomware families in this quarter. OilRig Campaign and Industroyer Malware Campaign were the targeted attacks observed in Q2. After the Mirai botnet attack in Q1, Persirai botnet was seen attacking vulnerable IP camera devices. The Fireball Adware made some news after it infected millions of users – it was part of a Chinese adware campaign.

The detection of Android samples in Q2 also moved down the scale by 21%. Third-party app stores continue to be the top source of malicious apps. Android ransomware grew by 16% from Q1 through Q2 while Banking Trojans showed a massive jump of 166%.

Important trends and predictions to watch out for include evolution of ransomware, increase in adware and targeted attacks on IoT devices, fake Android apps, and mobile ransomware.

Key observations of Q2 2017

- Although malware detection in Windows and Android in Q2 receded compared with the last quarter, ransomware attacks have increased – there have been 5 attacks so far with WannaCry and Petya as the notable ones. This trend sets off an unmistakable sign that attackers are shifting their attention towards attacks that make them more money and in an easier way. Ransomware campaigns, truth be told, have higher returns compared with data stealing and other malicious campaigns. With Ransomware-as-a-Service (a service where malware authors sell ransomware for free or for a small fee) gaining grounds, even novice cybercriminals are infecting computers and extracting money from their victims. In short, the ransomware business is a booming one.
- The 166% increase in Banking Trojans on Android platform in this quarter could be a tell-tale sign of attackers taking advantage of the ever growing popularity of digital payments. As more users skew towards mobile banking apps, they get nearer to the attack perimeter of cybercriminals.

Quick Heal Detection | Q2 2017

Malware

Per Day	Per Minute	Every 1 second
2,498,121	1,734	28

Ransomware

Per Day	Per Minute	Every 3 seconds
25,765	17	1

Exploit

Per Day	Per Minute	Every 4 seconds
22,817	15	1

PUA and Adware

Per Day	Per Minute	Every 1 second
2,85,987	198	3

Windows Malware

Windows Malware Detection Statistics

In Q2 2017, we detected over 224 million malware samples on our users' machines.

Compared with Q1 2017, Q2 2017 registered a drop of 23% in the detection count of Windows malware samples.

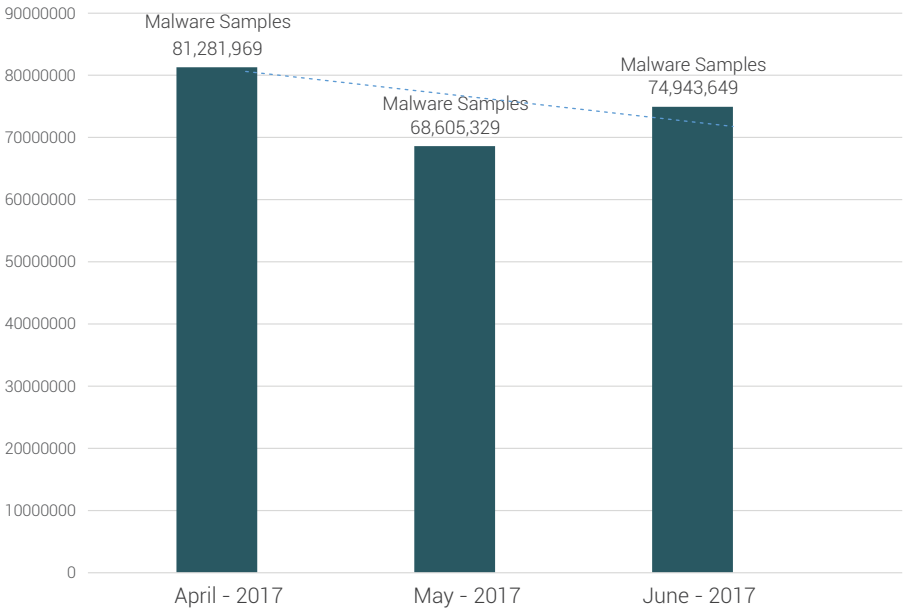


Fig 1

Ransomware formed 1.60% of the total malware samples detected in Q1 while in Q2 it's 1.78%.

Top 10 Windows Malware

These are the top 10 Windows malware detected by Quick Heal in Q2 2017.

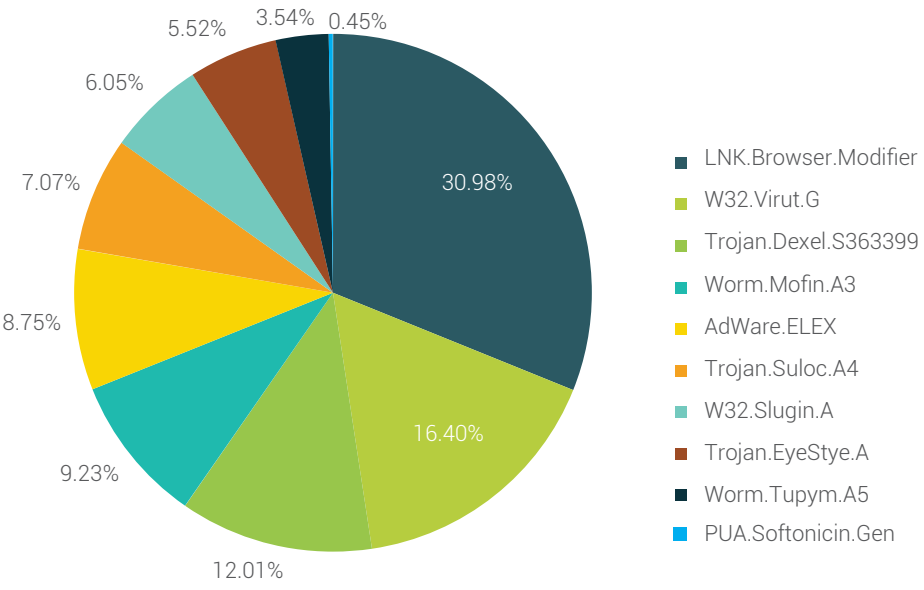


Fig 2

1.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.

2. 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.

3. Trojan.Dexel.S363399

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 where more Trojan malware are dropped on the system.
- Steals confidential data from the infected system and can also destroy the data.
- Slows down system performance by consuming more resources.

4. 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.

5. Adware.ELEX

Threat Level: Low
Category: Adware
Method of Propagation: Bundled software and freeware
Behavior:

- Displays ads when the user is browsing on the Internet.
- Modifies displayed pages or opens additional pages with ads.Adware.ELEX.
- Throws pop-ups, shows ads, and prompts fake update and software installation notifications.
- Redirects the user to malicious links while they are browsing.

6. Trojan.Suloc.A4

Threat Level: High
Category: Trojan
Method of Propagation: Bundled software and freeware
Behavior:

- Modifies system settings.
- Consumes system resources which slows down system performance.
- Invites other malware such as spyware and keyloggers into the infected system.
- Redirects search results to malicious websites where other malicious content gets downloaded on the user's computer.
- Can cause the system to crash or shut down abruptly.

7. W32.Slugin.A

Threat Level: High
Category: File infector
Method of Propagation: Spam email, removable or network drives
Behavior:

- Loads during system start-up and spreads through emails and infected files.
- Contains a backdoor component that can be remotely controlled by the attacker.
- Performs malicious activities such as changing system settings and redirecting the browser to malicious websites.

> There are only two types of companies: those that have been hacked and those that will be.
>
> – Robert S. Mueller

8. Trojan.EyeStye.A:

Threat Level: High
Category: Trojan
Method of Propagation: Removable and remote shared drives
Behavior:

- Copies itself on the targeted drive and modifies registry entries to execute itself automatically.
- Copies and uses autorun.inf files to execute automatically on the targeted system.
- Rapidly spreads from one system to another.
- Steals important data from the victim's computer and sends it remotely to the attacker.

9. Worm.Tupym.A5

Threat Level: Low
Category: Worm
Method of Propagation: Removable and remote shared drives
Behavior:

- Changes browser settings such as home page and search engine.
- Steals confidential information such as credit card details and bank account credentials.
- Looks for removable drives and network drives to replicate itself onto other systems in the network.
- Utilizes system resources to an extent that it degrades system performance.

LNK.Browser.Modifier, which modifies browser settings, has registered the highest detection count in Q2 2017. This means users should be more careful if they are downloading free software that have unverified publishers.

10. PUA.Softonicin.Gen

Threat Level: Low
Category: Potentially Unwanted Application
Method of Propagation: Bundled software and freeware
Behavior:

- Downloads software stubs (downloader executable) which then download installer setups from websites along with additional malicious setups.
- While downloading the software viz., "007-password-recovery" and "100-sudoku-puzzles", it triggers the download of other unwanted software such as VOpackage with vuupc and Site Finder. These software further change browser and search engine settings.

Malware Category-wise Detection Statistics

The below graph represents the statistics of the categories of Windows malware that were detected by Quick Heal in Q2 2017.

Detections in descending order (average):
Trojan: 37% | Infector: 25%
Worm: 15% | Adware & PUA: 19%

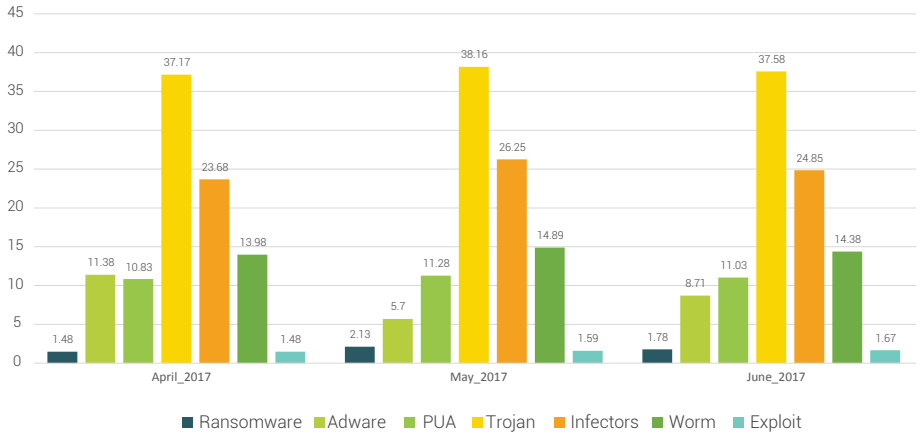


Fig 3

Top 10 Potentially Unwanted Applications (PUA) and Adware

These are the top 10 PUAs and Adware samples detected by Quick Heal in Q2 2017.

- 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.

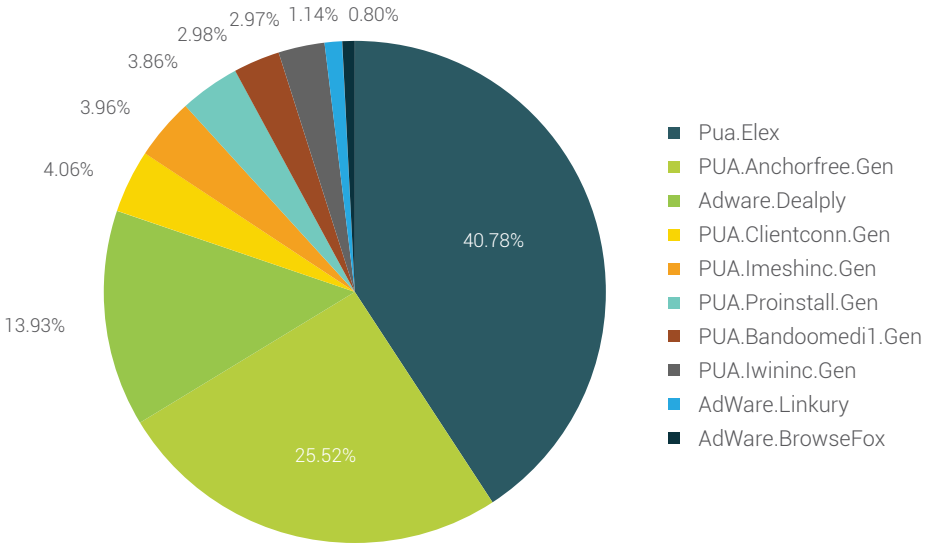
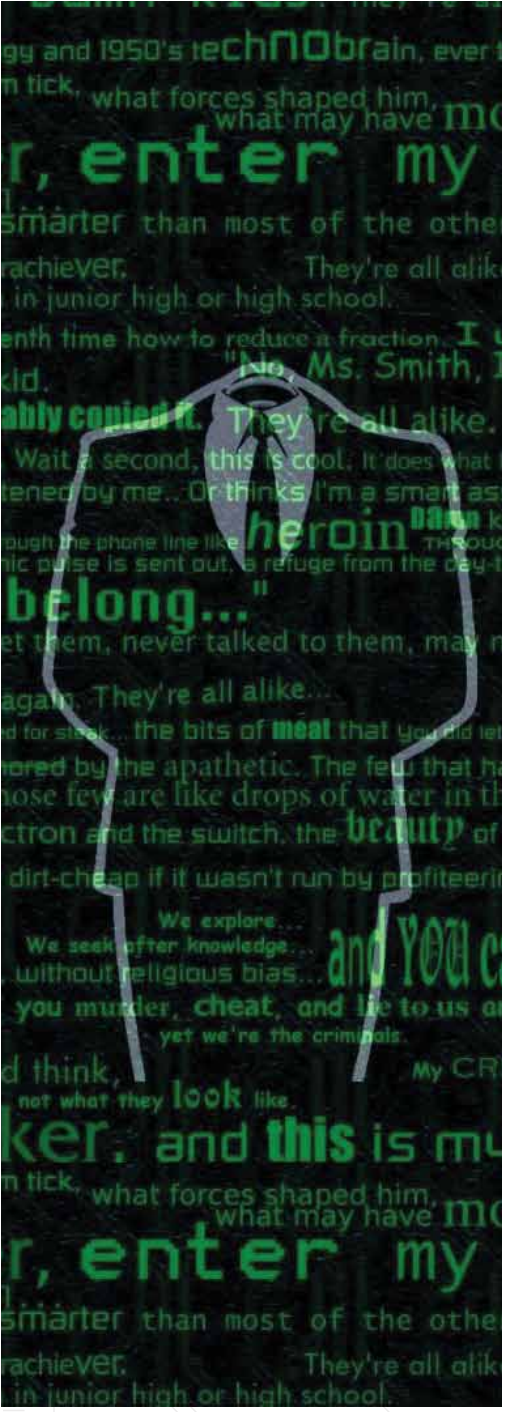


Fig 4



Top 10 Potentially Unwanted Applications and Adware

Newly observed Adware and PUAs in Q2 2017

Adware.Elex

Adware.Elex comes with third-party bundled installer applications. Once installed, it changes browser home page and shortcut path. It drops unwanted files that run at start-up.

PUA.Imeshinc.Gen

PUA.Imeshinc.Gen comes with third-party bundled installer applications and software downloaders. It changes browser home page and its settings. The malware also injects unwanted ads and pop-ups into the infected computer's web browser.

PUA.Proinstall.Gen

PUA.Proinstall.Gen triggers ads and pop-ups on the infected computer's web browser and redirects the user to unwanted sites.

PUA.Bandoomedi1.Gen

PUA.Bandoomedi1.Gen displays ads and pop-ups on web browsers, changes browser homepage and redirects the user to advertisement websites.

PUA.Iwininc.Gen

PUA.Iwininc.Gen changes browser settings such as homepage and search engine and also adds unwanted toolbars.

Top 10 Windows Exploits

A computer exploit is defined as an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has. These are the top 10 Windows exploits (host-based and network-based) of Q2 2017.

Top 10 host-based exploits

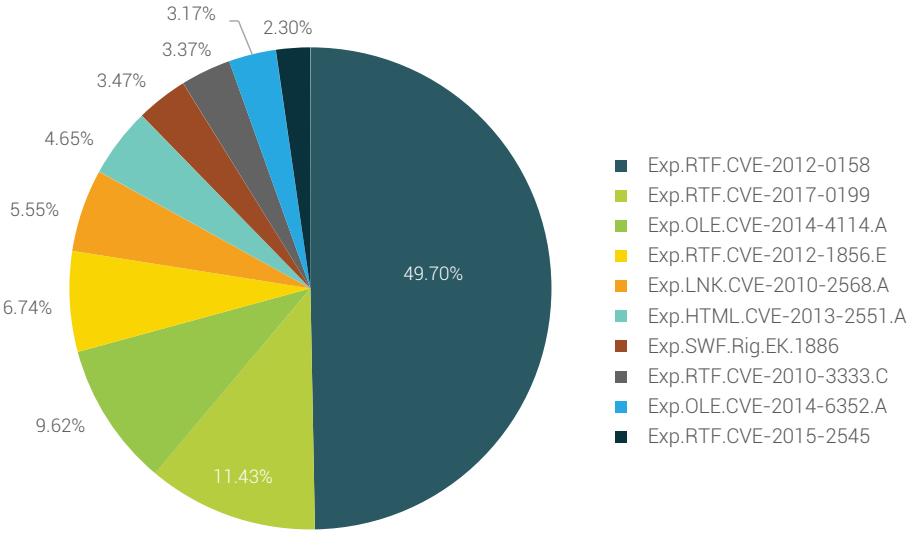


Fig 5

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).

Such exploits are detected by modules such as Virus Protection, Email Protection, and Scanner.

Network-based exploits are those that target security vulnerabilities found in network-based applications.

Such exploits are detected by (Intrusion Detection and Prevention) IDS/IPS module.

Top 10 network-based exploits

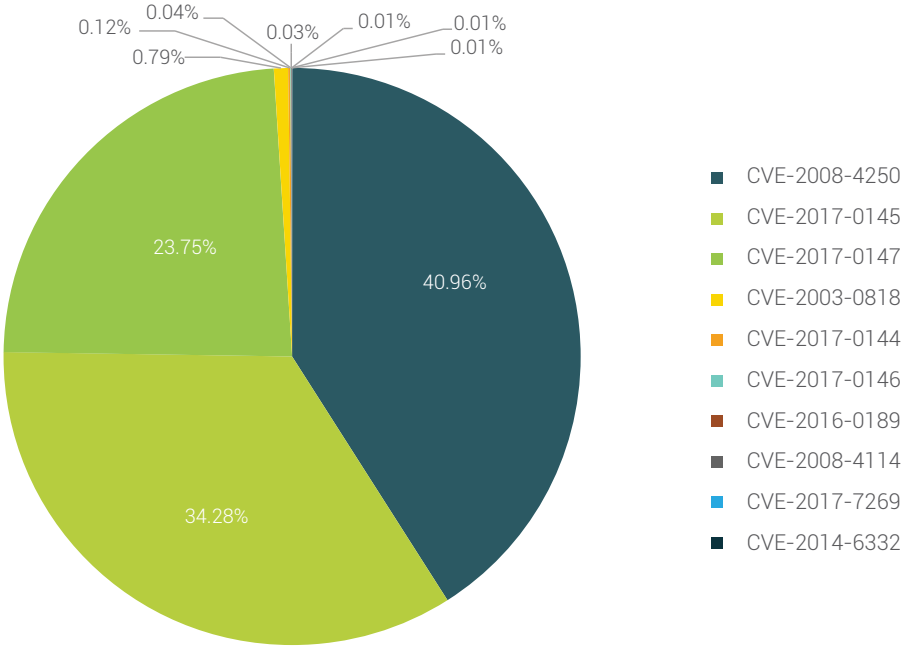


Fig 6

Major Windows Malware of the Quarter

Ransomware

1. WannaCry Ransomware

Q2 2017 witnessed the biggest ransomware attack in history – the WannaCry Ransomware. The attack begun on 12th May 2017 and within a day it managed to infect over 230,000 computers in more than 150 countries. Initially thought to have spread via spam emails, WannaCry was confirmed as a direct attack on systems running vulnerable SMB ports. The attackers targeted these systems with an exploit called EternalBlue. WannaCry is a self-propagating worm. This means, after it infects one computer, it searches for other computers in the network with the same vulnerability. If found, it can spread on its own without any user action.

High profile organizations including clinics and hospitals, telecom, gas, electricity and other utility providers in the UK and other countries were the main casualties in this attack. It caused an estimated loss of £100 million to UK business.

Read more on WannaCry Ransomware: http://bit.ly/2rQgldR

- Quick Heal started detecting the exploits used in the WannaCry Attack from May 5, 2017 onwards.
- Issued an immediate security advisory for users.
- 1,275,878 of these exploits were blocked (as of June 12, 2017).
- Setup an emergency hotline for customers and other users.

2. Jaff Ransomware

Jaff Ransomware surfaced after WannaCry and it came up with new versions. It spreads through spam emails containing a malicious PDF file as an attachment. This file contains an embedded word document with macros that downloads the malicious payload. Upon execution of the payload, it begins encrypting the files on the infected computer. After the encryption, names of the affected files are appended with a .jaff extension.

Read more on Jaff Ransomware: http://bit.ly/2rSiDZ0

3. Petya a.k.a. NotPetya Ransomware

Continuing the bout of ransomware outbreaks in Q2 2017, came along a new version of the Petya ransomware. The initial infection of the new version of this ransomware was spotted in Ukraine and within a few hours, it spread to Europe as well as some major parts of Asia including India. It uses the exploit called EternalBlue to target its users – the same exploit that was used by WannaCry.

This new version of Petya is known as **NotPetya** as it differs in its functionality and operations from the earlier one. This is a wiper which uses a random key to encrypt data and this makes it impossible to recover it.

In a few cases in Ukraine, it was found that Petya was getting delivered to the victims by a tax accounting software updater process. Petya also spreads via spam and phishing emails containing a malicious attachment.

Read more on Petya Ransomware: http://bit.ly/2skImZY

4. **Crisis Ransomware resurfaces with a new variant**
   A new variant of Crisis Ransomware was observed encrypting files to extensions '.wallet' and '.onion'. The master decryption keys for these variants were released by its authors. Quick Heal Security Labs updated its ransomware decryption tool with these keys to help users decrypt files which might have gotten encrypted by this new variant.

Quick Heal Security Labs was successful in decrypting files encrypted to pattern no. 2 as discussed under **Cry128/ Cry9 Ransomware**

The latest version of the **Free Ransomware Decryption** tool can be downloaded from the below link: http://bit.ly/2u8Ktp6

5. **Cry128/ Cry9 Ransomware**
   This is a variant of CryON Ransomware that infects systems via RDP (Remote Desktop Protocol) brute-force attack. Files encrypted by this ransomware are appended with extensions of the following patterns.
   1. ".id-<id>_[qg6m5wo7h3id55ym.onion.to].63vc4"
   2. ".fgb45ft3pqamyji7.onion.to._"
   3. ".id_<id>_gebdp3k7bolalnd4.onion._'"
   4. ".id_<id>_2irbar3mjvbap6gt.onion.to._"

6. **Other ransomware observed in Q2 2017:**
   - Mole
   - LMAOxUS
   - Karmen
   - xdata
   - Widia
   - FIXI
   - GLOBEIMPOSTER
   - AES-NI

Remote Desktop Services (RDS): A medium increasingly used by attackers

RDS is a feature of the Operating System that allows users to avail interactive sessions with graphical user interface implementing Remote Desktop Protocol. RDP ports are often left open and connected to the Internet making them more vulnerable to RDP brute-force attacks. Having acquired weak login credentials, password stealer software, and credential access techniques, attackers can easily get into the targeted systems.

In Q2 2017, most ransomware families such as Crysis, Cry9, Cryakl, and Amnesia were seen using RDP brute-force attack as their distribution vector. Having gained access to the victim's system, attackers are known to either disable or remove security software to extort money by encrypting the system's data.

Along with RDP, MSSQL server was seen to be targeted using brute-force attacks. Although no known damage was observed in these attacks, the possibility of a data breach and Denial of Service (DoS) attack by changing login credentials, cannot be denied.

Read more on brute-force attacks and its preventive measures: http://bit.ly/2tZmV5L

Java RAT

We are in close observation of a fast spreading malware called Java RAT (Remote Access Tool). It is mostly delivered through phishing emails as an attachment.

Of late, we've observed the following malicious attachments related to Java RAT:

- ITD_EFILING_FORM15CB_PR3.2.jar
- MVD_SHPMNT_VSL_0004048_pdf.jar
- Payment Swift Scan Copy 682017.pdf.jar
- SHIPPING DOCUMENTS PDF.jar
- SCAN DOC- 53862100.jar
- FINAL COMPLETE SET OF SHIPPING DOCS.jar
- PAYMENT_ADVISE_PDF.jar
- PAYMENT_APLICATION_PDF.jar

Behavior of Java RAT:

- Checks for the presence of any security solution on the infected system.
- Disables the security software and other analysis tools.
- Launches itself every time the system boots and downloads the executable malware file and infects the system again.

Quick Heal detects and blocks this malware with the name 'JAR.Suspicious.A'.

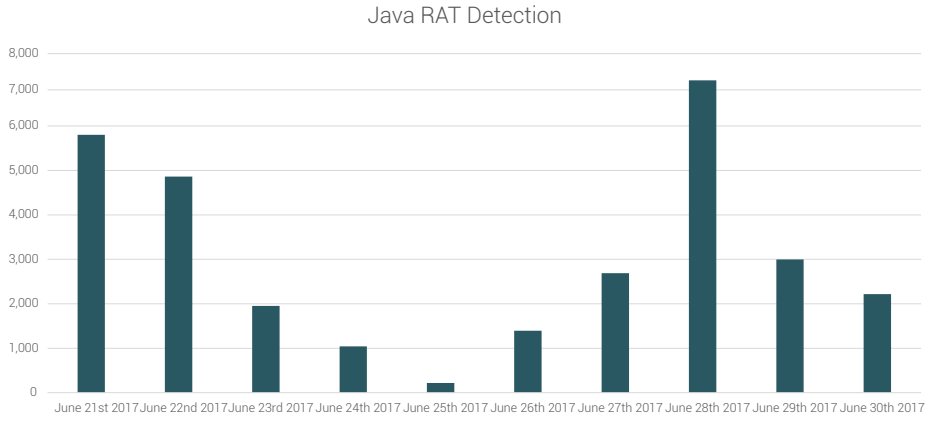


Fig 7

> Thinking of cyber security solely as an IT issue is like believing that a company's entire workforce, from the CEO down, is just one big HR issue.
>
> – Steven Chabinsky

Targeted Attacks

These are well-planned, systematic campaigns where attackers work with a motive to keep their presence hidden while stealing as much data as possible from the victim. A targeted attack usually goes undetected for months and sometimes even for years. Malicious emails, compromised websites, and exploits are some common channels used to carry out these attacks.

- The OilRig Campaign was such an attack where malicious MS-Excel files were used to infect its target. These Excel files were delivered to the victim via spam emails which when opened, triggered a malicious RAT (Remote Access Tool) to be downloaded on the victim's machine. This tool is capable of executing commands remotely and uploading or downloading files on the attacker's remote server.

- The Industroyer Malware Campaign was another targeted attack on Industrial Control System (ICS), especially ICS used in electrical substations. Malware used in this campaign were capable of handling circuit breakers and switches which may have been already used in a previous power outage incident in Ukraine. An organization-specific backdoor component was used to carry out its main activity. Interestingly, attackers could decide a particular time for this backdoor to be active.

- IoT (Internet of Things) devices are becoming a hot target for attackers. Earlier it was the Mirai Botnet that affected several IoT devices and now in Q2 2017, it is the Persirai Botnet. This malware targets vulnerable IP camera devices and uses them to carry out DDoS (Distribution Denial of Service) attacks on other vulnerable systems.

Potentially Unwanted Applications (PUA) and Adware

Browser hijackers are a type of unwanted software that are distributed with free programs. These software change web browser homepage or search engine settings without the user's permission. They also redirect the user to another search engine without their permission. Many browser hijackers display ads and pop-ups. Some also collect personal data such as credit card information, bank account details and login passwords.

In Q2 2017, one such browser hijacker was discovered as part of a Chinese adware campaign; it impacted millions of users. The adware used in this campaign is known as Fireball. It enters the victim's system with a free software.

Fireball performs the following activities:

- Creates a fake Google Chrome installation and profile automatically
- Modifies browser homepage by appending URLs in the browser shortcut
- Downloads and installs several other PUAs and adware components
- Connects to malicious CloudFront CDN (Content Delivery Networks)

Read more on the Fireball malware: http://bit.ly/2sGWZrO

Further Reading

Shadow Brokers' Exploits Leak

On 8 April 2017, a hacker group called the Shadow Brokers disclosed NSA (National Security Agency) leaked exploits. A few of these exploits were used to launch history's biggest ransomware attack called WannaCry. While Microsoft had already released the security patches against these exploits, many did not apply them. This resulted in a massive outbreak worldwide which has never been seen before. Many other campaigns emerged at the same time and were observed to be using the leaked exploits such as EnternalRocks, Adylkuzz, etc.

Windows exploits disclosed by Shadow Brokers:

Esteemaudit (CVE-2017-9073)
Explodingcan (CVE-2017-7269)
Eternalchampion (MS17-010)
Eternalromance (MS17-010)
Eternalblue (MS17-010)
EternalSynergy (MS17-010)
EskimoRoll (MS14-068)
EmeraldThread (MS10-061)
EducatedScholar (MS09-050)
EclipsedWing (MS08-067)
ErraticGopher (CVE-2017-8461) - addressed prior to the release of Windows Vista

Fig 8 shows the trend of how these leaked exploits were used.

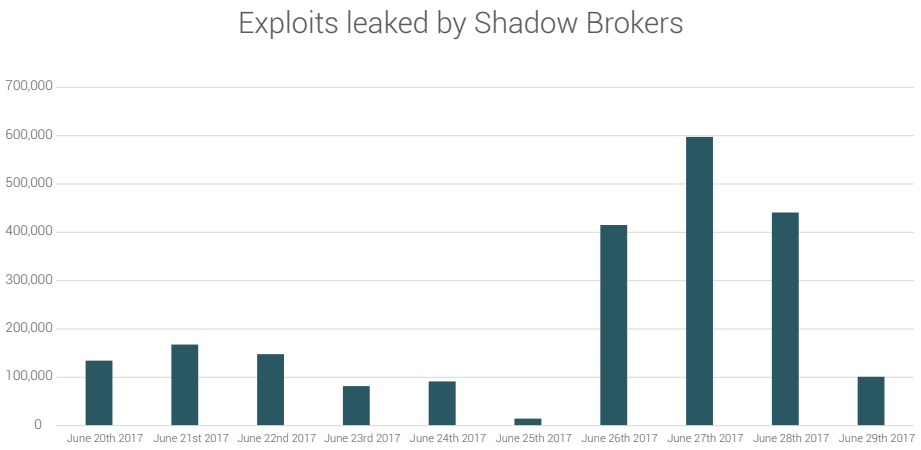


Fig 8

> Cybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we all are.
>
> – Jeh Johnson

IPS (Intrusion Prevention System) detections for Quick Heal and Seqrite products:

- VID-01714: Microsoft IIS Server Buffer Overflow Vulnerability
- VID-01901: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-01903: [MS08-067] Server Service Vulnerability
- VID-01906: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-01907: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-01911: DOUBELPULSER backdoor detection
- VID-01912: [MS17-010] Windows SMB Information Disclosure Vulnerability
- VID-01996: DOUBELPULSER backdoor detection
- VID-02013: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-02020: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-02021: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-02022: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-02042: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-02044: [MS17-010] Windows SMB Remote Code Execution Vulnerability
- VID-02069: Windows SMB MIBEntryGet Buffer Overflow Vulnerability
- VID-02083: Microsoft Windows RDP Remote Buffer Overflow Vulnerability
- VID-02121: [MS14-068] Microsoft Kerberos Checksum Validation Vulnerability
- VID-02375: Microsoft IIS Server Buffer Overflow Vulnerability

References:

http://bit.ly/2vOu8U1

Microsoft Office/WordPad zero-day vulnerability

The vulnerability (CVE-2017-0199) was a zero-day exploit that was disclosed on April 7, 2017. It was patched by Microsoft on April 11, 2017. It is a remote code execution vulnerability that exists in Microsoft Office and Wordpad. It is a bug that, while parsing RTF files, can trigger the download and execution of a malicious HTA (HTML Application) file from a remote server.

We have observed active exploitation of this vulnerability in various malicious spam campaigns. Below are some subject lines and names of attachments used by one of these campaigns.

Subject	Attachment's name
ATTEN:DEPARTMENT OF HOMELAND SECURITY. IMPORT AND EXPORT VIOLATION REPORT.	DHS international report.doc
DHL DOCUMENTS	DHL DOCUMENT.doc
payment advise 10,000USD	payment advise 10,000USD.doc
RFQ & Specifications on Large Order	PI-20170614.rtf
PO FOR JUNE SHIPMENT	PO FOR JUNE SHIPMENT.doc
Swift copy of payment	Swift copy of payment.doc
Emailing: Swift Payment	SWIFT 0748576643.doc
RFQ for Vessel: M/V SOUTHERN WISDOM / RFQ REF.: R09002983	SOUTHERNWISDOM09002983-0001 .doc
ESTIMATE ORDER LIST	PO# 94716.doc
INVOICE REF_#014893	Bill Of Reconcilliation.doc

CVE-2017-0199 detection statistics

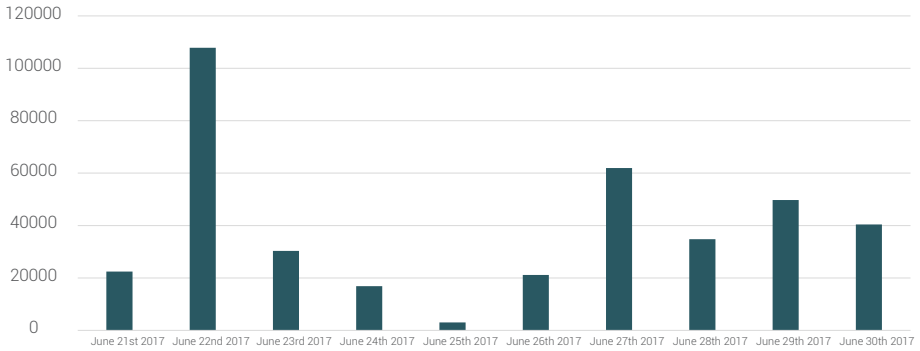


Fig 9

Threat Names:

- Exp.RTF.CVE-2017-0199
- Exp.RTF.CVE-2017-0199.A
- Exp.RTF.CVE-2017-0199.B
- Exp.RTF.CVE-2017-0199.C

Trends and Predictions

Ransomware

- With more users adopting the cloud to store their data, ransomware attacks on cloud server are expected to show up in the near future.
- There is an increased likelihood of massive attacks like WannaCry due to individual users and businesses failing to keep their systems patched and up-to-date.
- Ransomware attacks might increase on health care organizations.
- Newer, destructive and more advanced variants of the Wannacry and Petya/NotPetya are expected to surface.

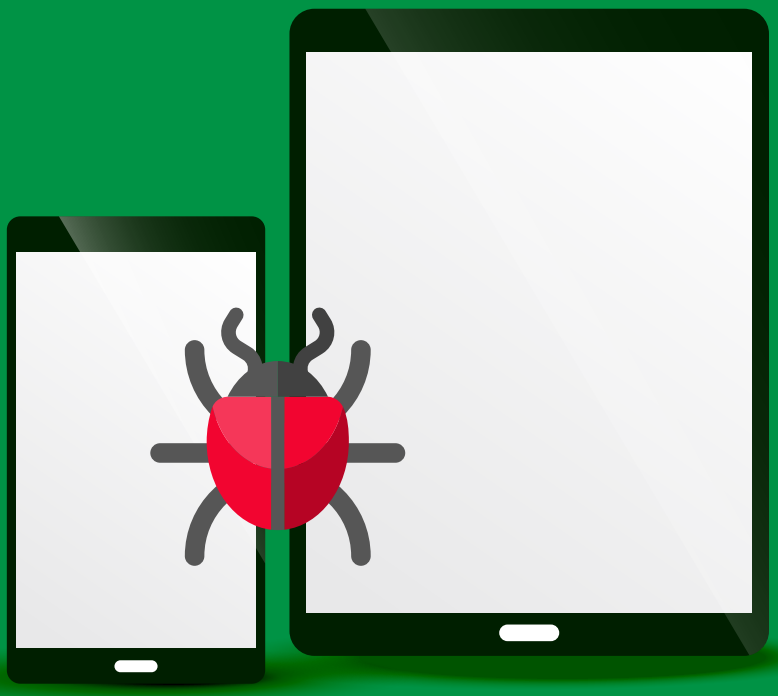
Adware

Like fireball, we are expecting more and high-impact adware campaigns in the future. In these campaigns, adware might be used to spread ransomware.

Targeted Attacks

Targeted attacks by using fileless and memory-based malware are expected to increase in the coming days. IoT devices are expected to be targeted at a higher scale as it was evident in the case of Mirai and Persirai botnet attacks.

As digital payment gets increasingly mainstream, businesses running on digital wallet programs can become hot targets for attackers in 2017.



Android Malware

Android Samples and their Detection Statistics

In Q2 2017, we received over 1 million Android samples.

Compared with Q1 2017, Q2 2017 registered a drop of 21% in the total number of Android samples (fig 2).

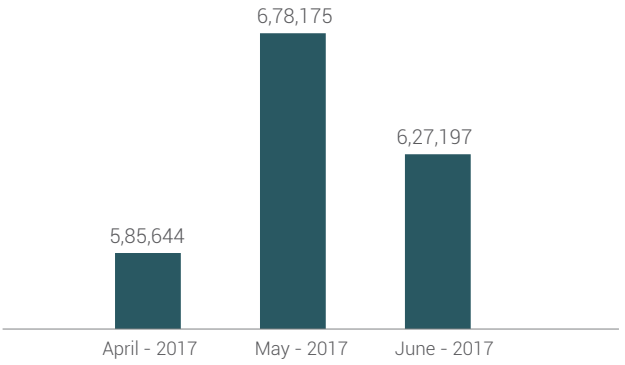


Fig 1

Android samples received at Quick Heal
(Q1 2017 vs Q2 2017)

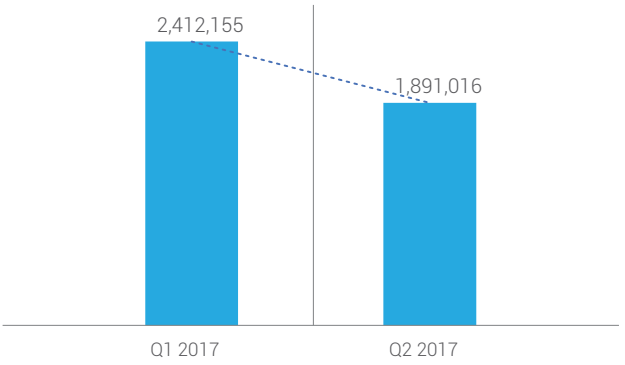


Fig 2

An increase of 38% noticed in Adware growth, while the PUA family (Potential Unwanted Programs) has grown by 24% (fig 3).

Category detection
(Q1 2017 vs Q2 2017)

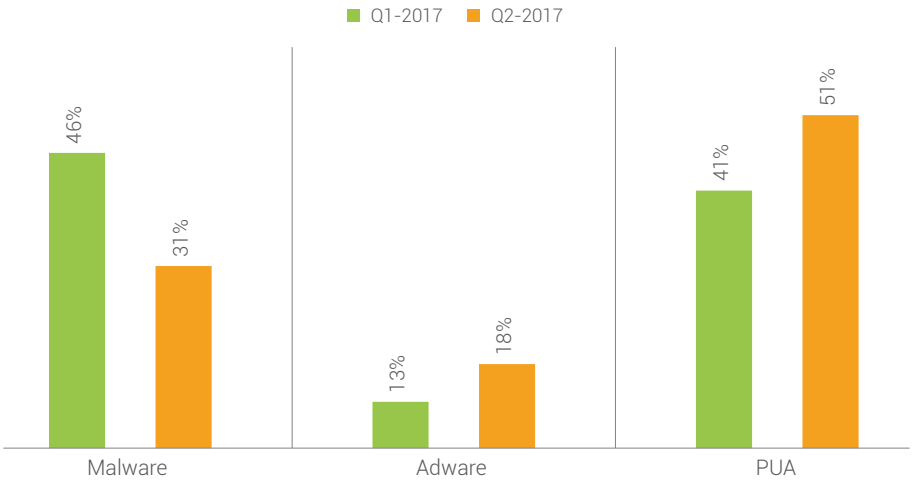


Fig 3

Top 10 Android Malware

These are the top 10 Android malware detected by Quick Heal in Q2 2017.

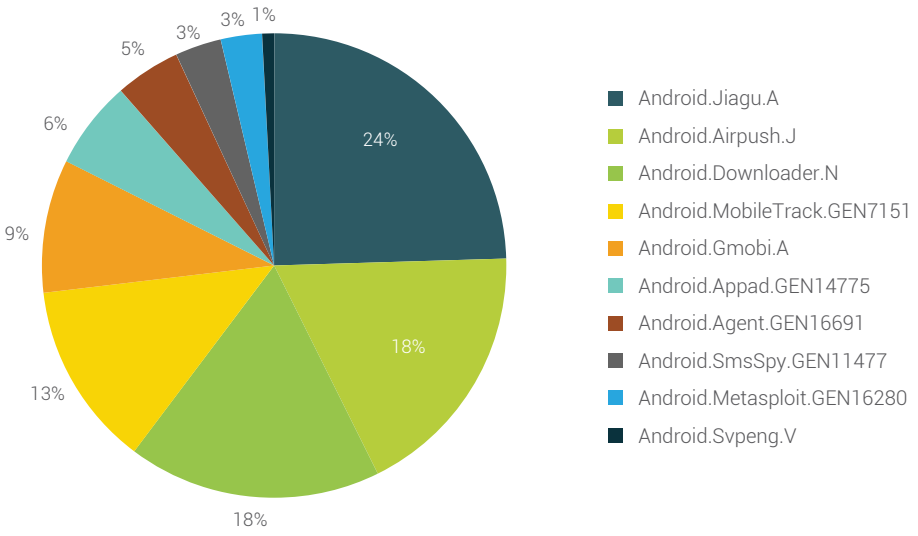


Fig 4

1. Android.Jiagu.A

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

- 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 file 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.

2. 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 it 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.

> Most people do not believe in ghosts but when they encounter one, we can guess what happens. Ransomware is one such ghost.
>
> – Anonymous

3. 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 some a specific time interval.
- The downloaded malicious apps can infect the device further or may steal the user's information before sending it to the external 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 an SMS after SIM change or phone reboot with specific keywords in the body.
- Collects device information such as IMEI and IMSI numbers.

5. 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.

6. Android.Appad.GEN14775

Threat Level: Medium
Category: Adware
Method of Propagation: Third-party app stores
Behavior:

- Displays ads which cover half of the screen; these ads cannot be closed by the user.
- If any of these ads are clicked on, respective ad app is downloaded.
- Once downloaded, the user is prompted to install the app.

7. Android.Agent.GEN16691

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

- Masks itself as a fake antivirus for Android.
- Carries another malicious file in an encrypted format, decrypts it at runtime and drops it at a later time on the infected phone. This file adds to the malicious activity.
- Forces the user allow admin privileges.
- Once it completes its operation, it hides its icon.

8. Android.SmsSpy.GEN11477

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

- Intercepts and forwards incoming SMSs to premium numbers.
- Collects the device's current location and sends it to a remote server.
- Wipes all contacts and messages stored on the device, the SIM card and even internal and external SD cards after receiving commands from the C&C server.

9. Android.Metasploit.GEN16280

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

- It's a repackaged app that resembles the popular Facebook lite app on Google Play store.
- Has an additional code to generate an executable file, which is created by decryption at runtime.
- To clear its activity track, the app deletes another executable file created at runtime.

A ransomware has made its entry into the top 10 Android malware with a detection rate of 1%. Although less, this figure has a high likelihood to increase in the coming days.

10. Android.Svpeng.V

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

- Once launched, it displays a white screen for a few seconds and takes the user back to the launcher screen.
- Within a few moments, an FBI lock screen appears which states that the device has been locked due because adult content has been found on the user's phone and presents a predefined photo as a proof of evidence.
- A ransom note is displayed on this fake screen that demands a ransom as a penalty for the user's offense.
- The user is asked to provide their details of an inactivated 'One Villa' card to make the payment.

Android Ransomware and Android Banking Trojans

Android ransomware works in the same fashion like Windows ransomware do. The malware can lock your device or encrypt the stored data and demand a ransom to put things back to normal.

Banking Trojans (also known as Banker Trojan-horse) are programs used to obtain sensitive information about customers who use online banking and payment systems.

Below are the statistics of Android ransomware and Android Banking Trojans detected by Quick Heal in Q2 2017.

Android Ransomware grew by 16% from Q1 2017 through Q2 2017.

Android Ransomware
(Q1 2017 vs Q2 2017)

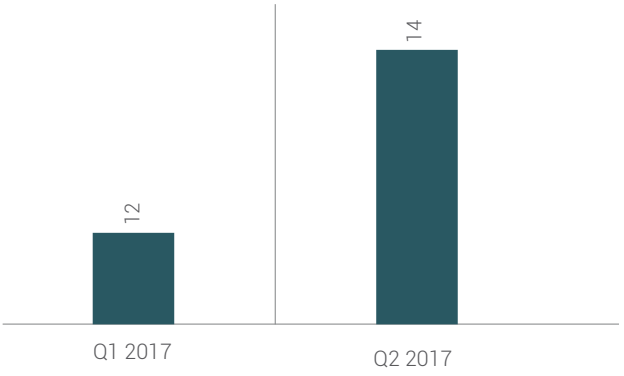


Fig 5

Android Banking Trojans has had a massive growth of over 166% in Q2 2017. This could be due to the increase in digital payments.

Android Banking Trojan
(Q1 2017 vs Q2 2017)

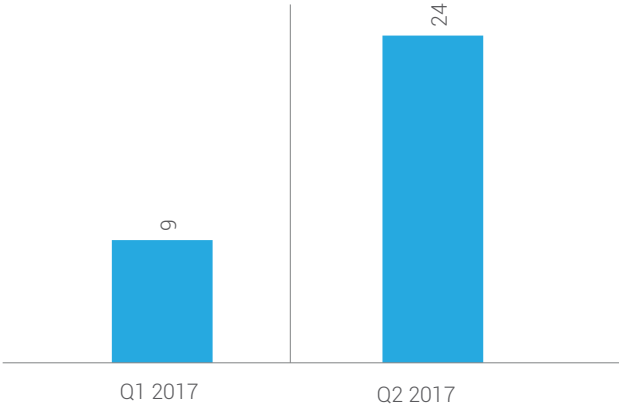


Fig 6

Android Malware Using Unique Techniques

1. **Android.Asacub.F**

- It's a mobile banking malware that looks like a legitimate app that allows users to watch funny videos
- In the background, it checks if the user has opened any banking app and checks this app against its saved list of 425 banking app names.
- If found, the malware displays an overlay (a fake page) on the top of banking app.
- This overlay is to trick the user into entering their banking login ID and password.
- If the user falls for this trick, the details are sent to the attacker.

2. **Android.Agent.YD**

- After installation, the malware connects to an external command & control (C&C) server.
- It downloads an SDK as a zip file, which further carries on with the malicious activities.
- This ad library is capable of installing other android applications silently in the background without user knowledge.
- It collects the infected device's information such as country and mobile operator.
- It looks for an emulated environment and if found, it terminates its activity banking app.

3. **Android.Agent.ZS**

- Uses a technique that allows it to execute other apps without installing them.
- This kind of activity has never been seen before as app installation was compulsorily needed.
- Performs the activity to create fake Twitter apps.

> True cybersecurity is preparing for what's next not what was last.
>
> – Neil Rerup.

Most Popular Android Malware in Q2 2017

1. **Android.Ewind.AU**

- It's an Adware that presents itself as a gaming app. Its package name contains the word 'Judy' and hence it is famous by the name JUDY malware.
- After it infects a device, it opens up web pages where it generates large amounts of fraudulent clicks on advertisements to make money for the malware's creator.
- It also asks the user to collect gaming stars to be able to proceed to higher levels, while installing multiple apps at the same time.
- While on the mobile screen, it shows as if it is redirecting the user to another app, but in the background it opens multiple ad URLs and increases its clicks before downloading the actual app.
- These clicks are generated in extensive amounts – more clicks means more money.

2. **Android.FakeAV.D**

- The app claims to protect phones from WannaCry ransomware. Note: WannaCry only affects Windows OS and not Android.
- This is a scare tactic the app uses to frighten users into downloading fake apps that could be dangerous too.
- Also uses icons that portray protection against the WannaCry ransomware.

3. **Android.Chrysaor.A**

- The malware targets rooted Android devices. If the device is not rooted, it tries to get root access.
- It steals user information and shares it with a remote server.
- Remote controlling is done via SMS.
- The malware also targets iOS devices.
- It can self-destruct if it finds itself at any risk, by receiving commands from its C&C server.

Vulnerabilities and Android OS

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 6 represents the growth of security vulnerabilities in Q1 2017 vs Q2 2017.

Compared with Q1 2017, Q2 2017 registered a mild decrease of 17% in the security vulnerabilities targeting the Android platform.

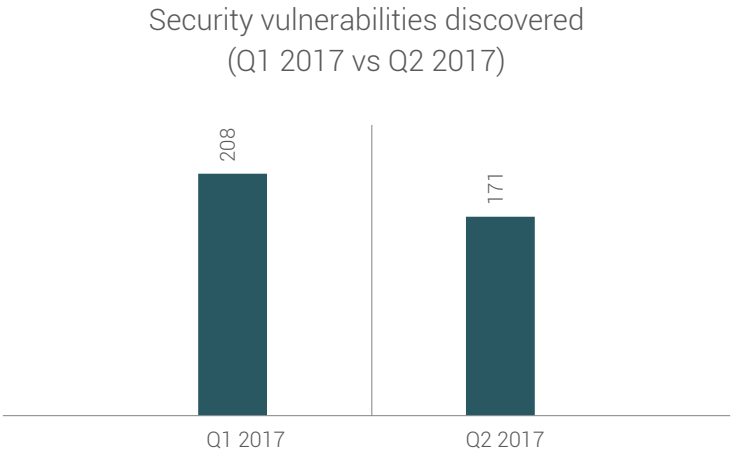


Fig 7

Source: cvedetails.com

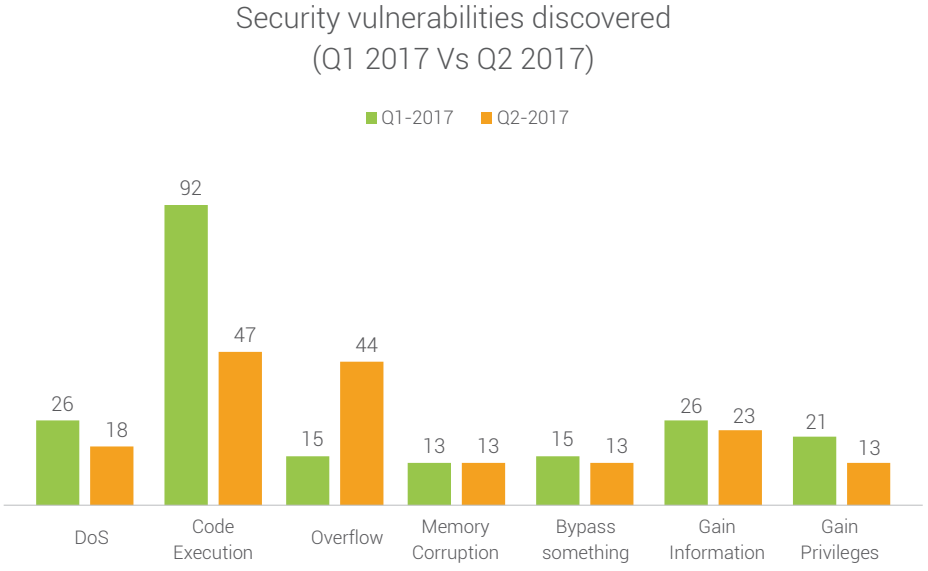


Fig 8

Source: cvedetails.com

Trends and Predictions

1. Fake applications are a growing concern

Scammers are distributing fake apps, labeling them with popular keywords to trick users into downloading them. These apps are mostly developed by novices and are not coded properly which leaves security vulnerabilities in them. These 'weak' apps are then used by seasoned attackers to target mobile users. Fake applications are expected to increase in volume not only in third-party app stores but Google Play as well.

2. Growth of Ransomware

As observed in the earlier sections, the top 10 Android malware list has included an Android ransomware and Q2 has registered a 16% spike in the malware compared to Q1. This only adds to the prediction that ransomware is going to get worse in the coming days.

Conclusion

With the number of ransomware attacks we have witnessed so far, 2017 may well be dubbed as "The Year of the Ransomware". As discussed in our 'key observations' at the beginning of this report, cybercriminals are trying to make their lives easier by working on attacks that require fewer resources but at the same time, give higher returns. And this is why ransomware is becoming a dreaded nightmare to individuals and businesses across the world. With increased digitization, people are sharing their personal data more than ever. And data is seen as a gold mine by attackers and ransomware is their tool of choice to extract this gold. What makes this scarier is the ease of pulling it off. Thanks to outsourcing crimes such as Ransomware-as-a-Service, even novice cybercriminals who may not create a ransomware, can purchase one at a meager price, drop the malware on their profiled targets and make easy money. WannaCry couldn't have been the biggest attack in history if people were prudent enough to keep their Operating Systems up-to-date with the security patches which Microsoft had released way before the attack happened. This was a disaster which could have been easily avoided – again a screaming reminder that humans still are the weakest link in computer security. It's about time we paid heed to warnings, understand the types of digital threats that surround us, be wary of sharing our personal details and treat our digital lives in the same manner as we treat our real lives – with a sense of security.