Quick Heal
Security Simplified

SEQRITE
Enterprise Security Solutions by Quick Heal

Quarterly Threat Report Q2 2016

www.quickheal.com

TABLE OF CONTENTS

INTRODUCTION

The second quarter of 2016 (April, May, and June) has noticed a feeble decline in the detection count of both Android and Windows malware. This, however, should not be mistaken as a sign of weakness in cyber criminals. The Quick Heal Threat Research Labs has recorded a good increase in the detection of Potential Unwanted Programs (PUA). A more concerning matter is a 200% increase in the detection of mobile Ransomware in this quarter alone. In fact, this detection is almost close to 50% of the detection of all the four quarters of 2015 combined. In other news, newer variants of Windows malware have joined the pack of the top 10 malware of Q2 and security vulnerabilities have swelled to scary proportions.

The Q2 Threat Report outlines the top malware afflicting Windows and Android users, with a brief low-down on each of the malware families. Additionally, the report lays out the difference between the malware detection stats of this quarter and that of the previous. This is accompanied by some important observations about certain malware that have caught our attention due to their unique behavior. Towards the concluding section, some important trends and predictions have been put together to give our readers an insight into what they may expect in the coming months of 2016.

Windows malware detection statistics

Compared with the previous quarter (Q1 2016), this quarter has seen a decline of 16% in the detection count of malware on Windows computers. Given below is the statistics of malware detected by Quick Heal Labs.

Malware detection statistics by Quick Heal

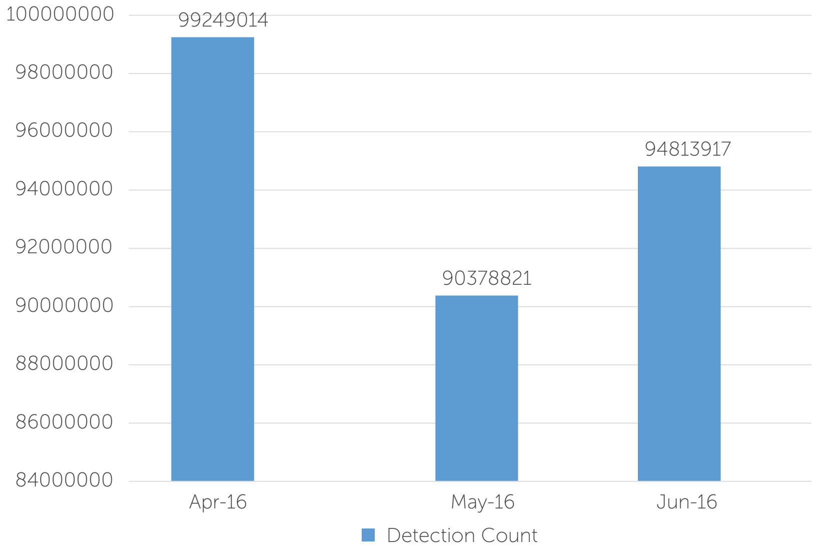


Fig 1

MONTH	DETECTION COUNT
APRIL	9,92,49,014
MAY	9,03,78,821
JUNE	9,48,13,917
TOTAL	**284,441,752**

TOP 10
WINDOWS MALWARE

The top 10 malware detected by Quick Heal in the last three months are as follows:

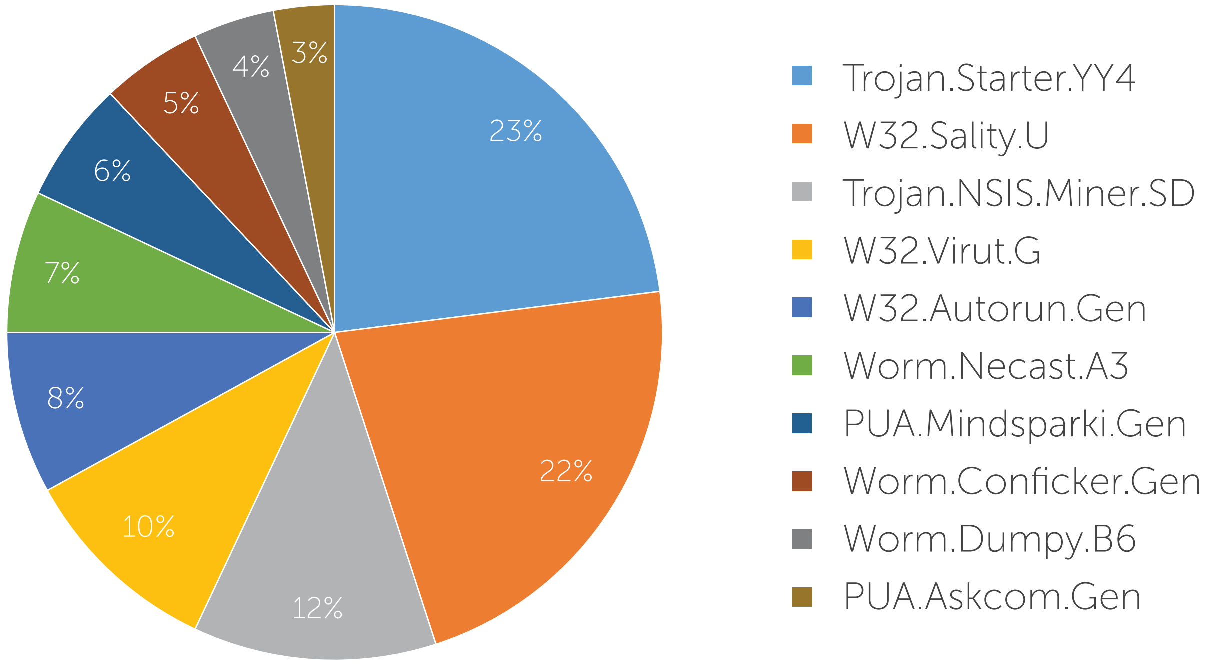


Fig 2

Observations when compared with Q1's Top 10 Malware list

- The malware 'W32.Sality.U' hasn't moved from its 2nd position.
- The malware 'Trojan.NSIS.Miner.SD' has moved up from 4th to the 3rd position.
- 'PUA.Mindsparki.Gen' has moved down from the 3rd to 7th position.

The above observations tell us that malware artists do not follow a routine. They keep changing their gameplay in an effort to trick more users.

Trojan.Starter.YY4

Damage Level: HIGH

Method of Propagation: Email attachments and malicious websites.

Summary: Trojan.Starter.YY4 is a Trojan that works by connecting to a remote server and installing other malware on the computer that it infects. In other words, it is used as an entry point by other malware. This malware is linked to various banking Trojans and worms designed to spread over networks.

Post-infection Behavior:

Trojan.Starter.YY4

- Creates a process to run the dropped executable file.
- Modifies computer registry settings which may cause system crash.
- Downloads other malware like keyloggers.
- Slows down the booting and shutting down process of the infected computer.
- Allows hackers to steal confidential data like credit card details and personal information from the infected system.

Top 10 Windows malware

W32.Sality.U

Damage Level: MEDIUM

Method of Propagation: Removable or network drives.

Summary: W32.Sality.U is a polymorphic file infector. After execution, it starts computing and infecting all the executable files present on local drives, removable drives, and remote shared drives.

Post-infection Behavior:

W32.Sality.U

- 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.

Trojan.NSIS.Miner.SD

Damage Level: HIGH

Method of Propagation: Bundled software and freeware.

Summary: Trojan.NSIS.Miner.SD is a Trojan that infects systems via compromised websites or malicious links. Once installed on the infected computer, it redirects the victim to malicious websites. It also lets other malware gain entry into the infected system.

Post-infection Behavior:

Trojan.NSIS.Miner.SD

- Downloads and installs free, unwanted software on the infected system via malicious websites without the user's knowledge or consent.
- Automatically executes when the system starts.
- Modifies important system files and Windows registry settings.
- Makes excessive use of system resources for bitcoin mining which further degrades the infected system's performance.

W32.Virut.G

Damage Level: MEDIUM

Method of Propagation: Removable or network drives.

Summary: W32.Virut.G a family of viruses associated with various botnets. It injects its code within running system processes and starts infecting the executable files present on local drives and removable drives. It also lets other malware gain entry into the infected system.

Post-infection Behavior:

W32.Virut.G

- 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 affected system.

W32.Autorun.Gen

Damage Level: HIGH

Method of Propagation: Removable or network drives.

Summary: W32.Autorun.Gen is a worm. Once inside a computer, it looks for similar drives and repeats the process on any other drives that are discovered.

Post-infection Behavior:

W32.Autorun.Gen

- Copies itself to the root of the drive, then creates or modifies the Autorun.inf file (*text file used by the AutoRun and AutoPlay components of Microsoft Windows*), instructing it to run the dropped worm each time the drive is accessed.
- Changes system settings, files and registry.
- Utilizes system resources and degrades its performance.
- Keeps track of the user's browser history and steals confidential information.

Worm.Necast.A3

Damage Level: MEDIUM

Method of Propagation: Spam emails and malicious websites.

Summary: Worm.Necast.A3 is a type of malware and a worm that runs as a self-contained program. It infects a computer via spam emails or when a user visits a website that is loaded with exploits. The worm also comes attached with freeware. It does not need to attach itself to the host program in order to perform its operation. It simply takes advantage of network connections in order to reproduce copies of itself and propagate parts of itself onto other systems.

Post-infection Behavior:

Worm.Necast.A3

- Exploits the infected system's vulnerabilities so that it can drop and install additional threats such as Trojans, keyloggers, fake antivirus programs, and even ransomware.

- Helps remote hackers misuse the infected system's vulnerabilities to access the compromised machine without the user's knowledge and consent.

PUA.Mindsparki.Gen

Damage Level: MEDIUM

Method of Propagation: Bundled software and malicious websites.

Summary: PUA.Mindsparki.Gen is a Potential Unwanted Application (PUA) that comes from third-party bundled installer applications and software downloaders.

Post-infection Behavior:

PUA.Mindsparki.Gen

- 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.

Worm.Conficker.Gen

Damage Level: HIGH

Method of Propagation: Removable or network drives.

Summary: Worm.Conficker.Gen is a worm that can infect systems and can spread to other systems in the network automatically, without any human interaction.

Post-infection Behavior:

Worm.Conficker.Gen

- Allows remote code execution when file-sharing is enabled on the infected system.
- Disables several important system services including security software.
- Downloads and executes other malware on the infected system.
- Stops victims from visiting websites related to security software and services that can assist in its removal.

Worm.Dumpy.B6

Damage Level: HIGH

Method of Propagation: Removable or network drives.

Summary: Worm.Dumpy.B6 is a worm that relies on security vulnerabilities to infect computers.

Post-infection Behavior:

Worm.Dumpy.B6

- Connects to a remote server in order to install corrupt files on the infected computer.
- Acts as a backdoor and lets other malware enter the infected computer.
- Uses a computer network to spread itself.
- Attempts to connect to other computers in the network by using preconfigured user names and passwords in the background.
- Constantly redirects the victim to randomly chosen or unsafe websites.

PUA.Askcom.gen

Damage Level: LOW

Method of Propagation: Bundled software and freeware.

Summary: PUA.Askcom.gen is a PUA that modifies Internet browser settings like default search engine and home page.

Post-infection Behavior:

PUA.Askcom.gen

- Adds extensions to Internet browsers which modifies the browser settings, redirecting the user to malicious websites.
- Tracks the user's activities on the Internet without their knowledge.
- Sends the collected data to a remote server for delivering targeted advertising.
- Triggers unwanted pop-up ads.

Malware category-wise detection statistics

The below graph presents the statistics of every category of malware that were detected by Quick Heal in the last three months.

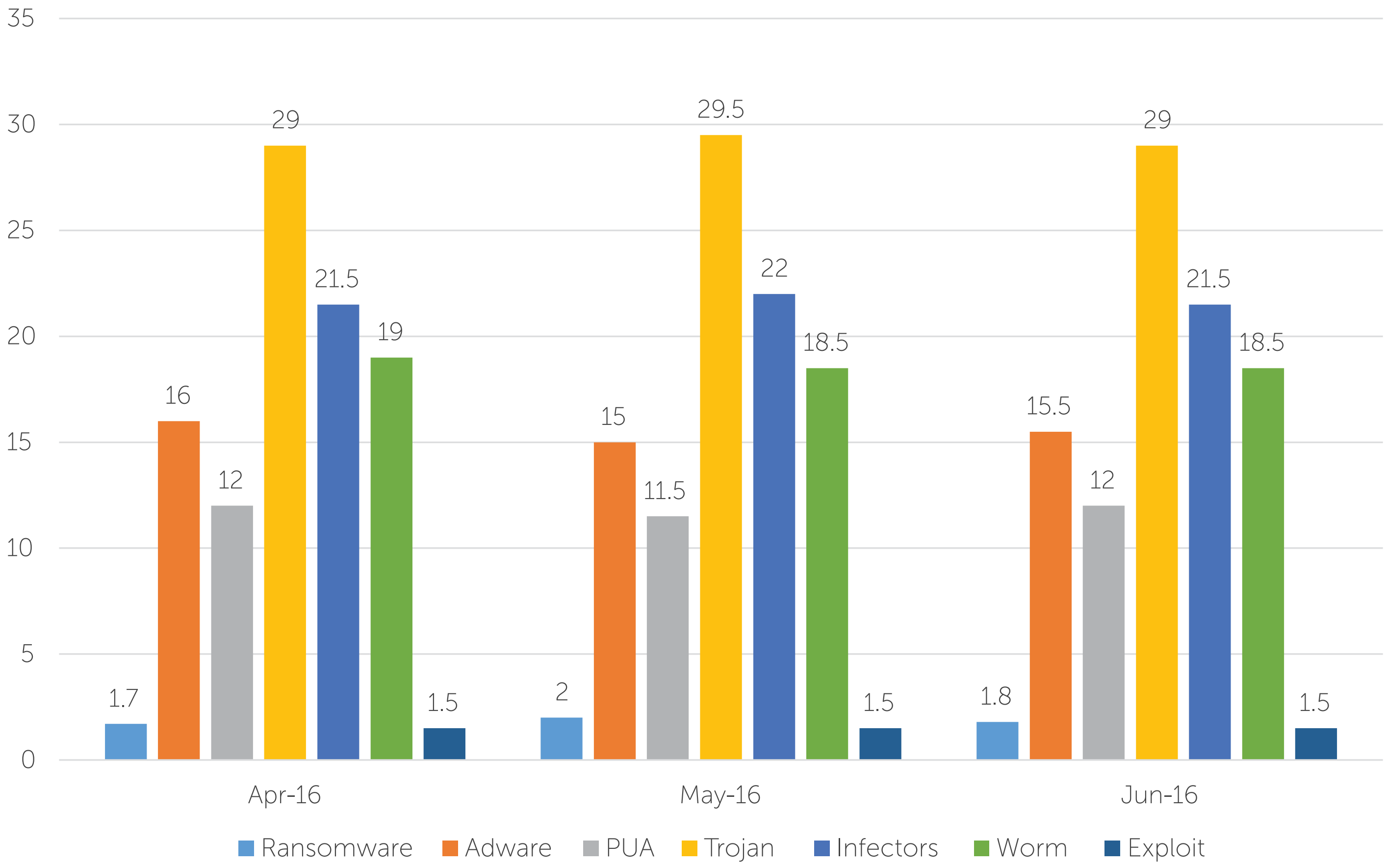


Fig 3

Observations:

1. Trojan (~29%), Worm (~19%), Infector (~21%) and Exploits (1.5%) show near constant detection rates for every month in Q2.
2. The combined figure of Adware and PUA category detection is 28% on an average.
3. Ransomware detection seems to have declined by a tiny margin in June when compared with May.

TOP 10

PUAs and adware

Here are the top 10 PUAs and adware samples detected by Quick Heal in Q2 2016.

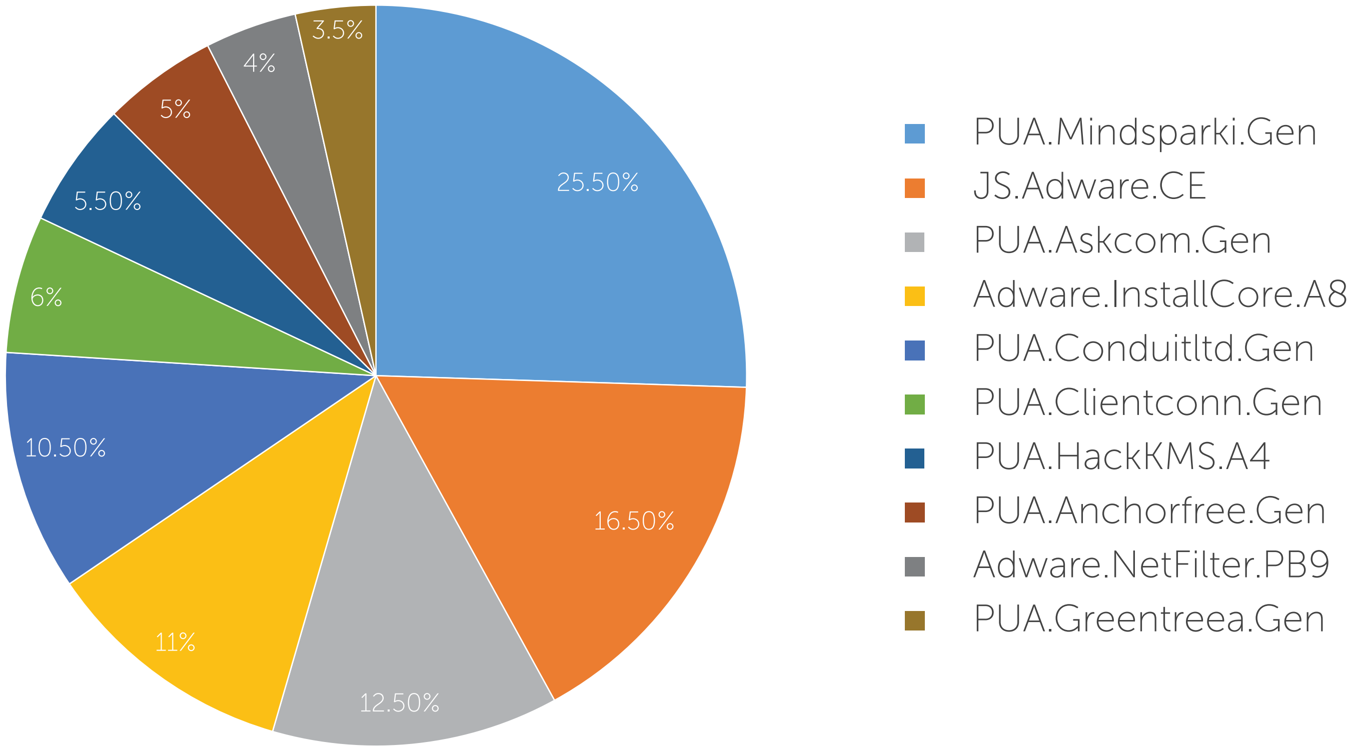


Fig 4

As observed in Q1, Mindsparki, BrowseFox and Clientconnect were the top PUA families with the highest detection rate. In Q2, however, we saw new families coming up which include Askcom, InstallCore, and Greentree. Generally, these are marked as low risk threats. InstallCore and Askcom, however, are difficult to remove once they have infected a computer, making them a bit stubborn.

Users need to exercise caution while clicking on the **Accept** button while installing any software, particularly the free ones. We strongly recommended users to read the **Privacy Policy** and **End User License Agreement** so that they understand what all applica-tions are going to get installed besides the primary software.

TOP 10

Exploits

The top 10 exploits of Q2 2016 are as follows:

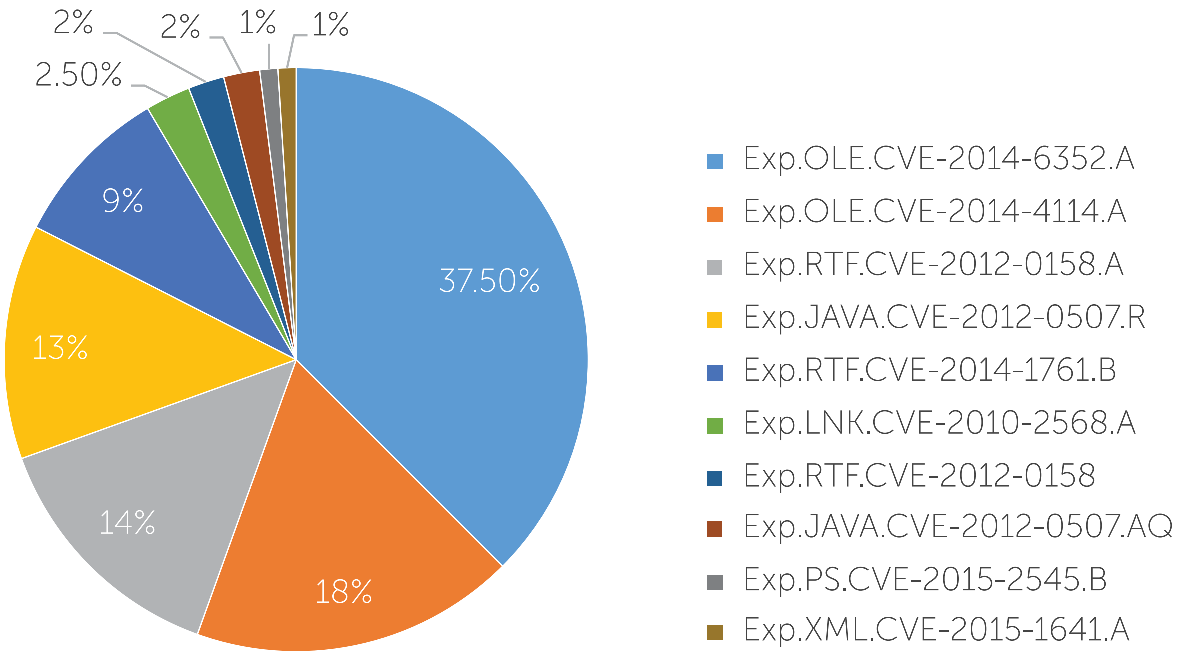


Fig 5

Observations:

- OLE (Object Linking and Embedding) and RTF (Rich Text File) format related vulnerabilities have contributed to 80.5% of the detections.
- Java vulnerabilities have contributed 15%.

MAJOR WINDOWS MALWARE

PUAs and Adware

Adware is a program that displays unwanted ads when a user is online. It arrives with free software and gets installed on the system without the user's knowledge or consent. Additionally, adware can redirect users to targeted or malicious advertisements. Adware are also capable of hijacking Internet browsers by changing browser's default settings and homepage.

As observed in the detection statistics of Q2 2016, adware remains one of the major malware categories. Stealing information and siphoning money are the primary objectives of criminals behind creating and distributing adware.

Adware incidents

A. Web anonymizers such as Unstopp.me/Unblockservice.com that use Web Proxy Auto-Discovery Protocol (WPAD) configuration techniques, were reported to cause adware activities. The WPAD protocol was basically introduced to allow automatic discovery of web proxy configuration without having to rely on manual changes. This works in large network environments where clients connect with the outside world through a proxy. However, Potentially Unwanted Applications (PUAs) that get installed on the system configure WPAD proxies in the user's registry that redirects traffic through external servers. This file-less technique is being exploited to display pop-up ads, modify browser homepage, and trigger redirections to unwanted advertisements. This can cause Man-in-the-Middle attacks (MitM) by mimicking the servers on the other end during secure transactions. If that isn't troublesome enough, they can also record the user's browsing history and web traffic without their knowledge.

B. Faster Internet Adware is an adware designed to steal information related to system resources such as CPU, network adapters, hard drives, among other information about the infected computer. This information is then uploaded to one of the attacker's server. Delivering more advertisements or malware payload to the victims based on their system configuration could be the purpose behind this stealing.

C. 'Tech Support Scam' was observed in early April 2016. The culprit was an adware designed to lock the infected computer's screen; it forced the victim to contact a fake tech support call center. Once contacted, the support center demanded money for unlocking the screen.

D. Hohosearch and YesSearches are browser hijacking programs that were observed to arrive with freeware. They change Internet browser settings and set a customized homepage. They also redirect victims to targeted advertisement pages and trigger pop-up ads.

Ransomware

The dominance of the ransomware family showed no respite even in this quarter. Interestingly, the cybercriminals behind the notorious Teslacrypt Ransomware revealed the master key to the public, which can be used to decrypt files that were previously encrypted by the malware.

Ransomware incidents

A. Newer ransomware families and their variants are being discovered with improved encryption and anti-detection techniques. Cryptxxx ransomware is one such ransomware which was observed in the mid of April 2016; it seemed to have different versions. One of its variants was found to be dropped by the Bedep malware and the Angler exploit kit. The malware encrypted the infected system's files and added the ".crypt" extension to the encrypted files. Decryption of these encrypted files was possible and to overcome this, authors of Cryptxxx released a new version which was dubbed as Cryptxxx 2.0; this made the decryption process ineffective. Cryptxxx 2.0 then advanced to Cryptxxx 3 and higher versions, having ".cryp1" and ".crypz" extensions.

B. Locky Ransomware also maintained its dominance. The ransomware was being spread through spam emails carrying attachments of malicious Java Script (JS) or MS Office files (Doc/docx/docm/xls). Locky encrypts files on the infected system and adds the ".locky" extension to them. Because the authors used several email campaigns to spread the malware and due to a lack of decryption possibility, Locky was considered as one of the most dangerous ransomware in this quarter.

List of some new ransomware observed in Q2 2016

- JigsawLocker
- Zcrypt
- CryptoHost
- DMA Locker 4.0
- AlphaLocker
- TrueCrypter
- Mahasaraswati
- CryptoMix
- BadBlock
- Troldesh (XTBL)
- Xorist
- Rokku

Targeted Attacks

Targeted attacks are known for their hidden and persistent approach of stealing sensitive information for monetary or political gain. Attacks can be customized, modified or improved depending on the intention behind the attack.

In Q2 2016, targeted attacks were found to be making use of security vulnerabilities. Reuse of leaked code infrastructure and social engineering tactics still remains a useful tool for attackers.

Targeted Attack Incidents

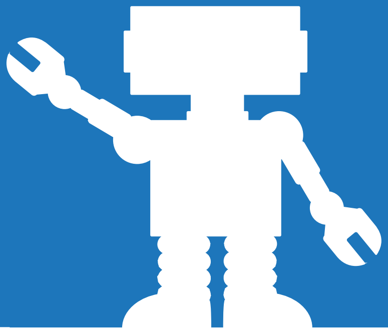
A. Microsoft Office Malformed EPS (Encapsulated Post Script) file vulnerability (CVE-2015-2545) was exploited in many targeted campaigns. Hacking groups such as the Platinum Group targeted government agencies in Malaysia, Indonesia, China, and India; the EvilPost group targeted Japanese defense sector; and the Danti group targeted Indian Government. These groups are mostly found to target Asia.

B. Indian Government officials were targeted by a Pakistan-based APT group via a spear phishing email designed to exploit the CVE-2012-0158 vulnerability. The attack was carried out by a spam email containing a fake attachment related to the "7th Pay Commission". When this attachment was opened, a backdoor payload (Breach Remote Administration Tool) was downloaded and installed which furthered communicated with a remote Command and Control (C&C) server.

C. Attackers benefited from the leaked source code of the notorious Carberp and Zeus banking Trojan. Authors of the Bolek malware reused the Carberp and Zeus code which recently targeted customers of Russian banks for stealing their confidential information. Bolek is weaponized with the ability to steal login credentials from online banking applications by injecting itself into Internet browser's processes, taking screenshots of the user's screen, and keylogging. Bolek is also designed to replicate itself on the other files of the system or USB drives.

D. An attack was observed where cybercriminals targeted travelers applying for US Visa in Switzerland. Attackers sent a *.JAR file to the victims via a fake Skype account. This file was infected with a new Remote Excess Trojan (RAT) named Qarallax RAT that is used by attackers to gain access to the victim's computer.

E. The Lurk Trojan is another banking malware that was observed in this quarter. It was designed to steal money from online banking systems of some large banks in Russia. Lurk was also found to feature strong anti-detection techniques.



Trends and Predictions

1

PUA and Adware

Given the free and widespread reach of the Internet, adware is a cash generating machine for hackers. Adware will be seen to offer more interesting product services to communicate with victims and trick them into the attacker's trap.

Adware or PUAs are suspected to be laced with destructive functionalities including damaging or crashing boot sector records of infected computers. Additionally, adware is most likely to be used for delivering ransomware into the targeted systems.

2

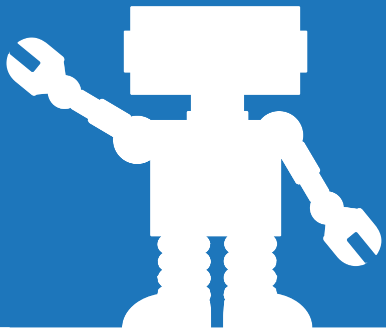
Ransomware

Ransomware variants will keep rising in the coming quarter as well. The cryptxxx ransomware is suspected of hitting its targets with new and more advanced variants.

Locky ransomware will also be a challenge for security products because of its continuously changing internal coding and obfuscation techniques.

DGAs (Domain Generation Algorithm) could become a menace as these domains are generated based on current date or time which leads to a vast variety of domains at hand. DGAs help malware evade security detections by not having hard coded domains. The recent Locky ransomware was one such malware using DGA. We may see some more ransomware families using this technique in the future.

Ransomware-as-a-service (RaaS) is another trend that we have observed taking momentum. In RaaS, malware authors sell ransomware along with a customizable kit through the online black market. Interested people can register and download them for free or a nominal fee. Once the ransomware file is customized as per the requirement, it is then spread through the desired infection vectors.



Trends and Predictions

Targeted Attacks

The upcoming United States Presidential Election 2016 could be piggybacked by attackers to spread malware with destructive capabilities. The upcoming Rio Olympic Games 2016 in Brazil could be yet another opportunity for spammers. So, we can expect highly potential spam attacks in the coming days.

Mobile wallets and new payment technologies have simplified online shopping. But, at the same time, they have opened themselves to hackers. Credit card data theft and fraud may rise in the future.

After incidents of the SWIFT (Society for Worldwide Interbank Financial Telecommunication) interbank messaging system hack and failed attempt on Vietnam's "Tien Phong Commercial Joint Stock Bank", we can expect similar attacks on other banking institutions in the coming days.

3

Internet of Things (IoT) devices are making personal and business operations more convenient than ever. But, their serious lack of security is beginning to open gaping holes that attackers can benefit from.

Malvertising

4

Malvertising, which makes use of online advertisements to spread malware, is becoming a prominent infection vector. The attack involves injecting malicious ads into genuine sites that redirect users to malicious sites that can exploit security holes in the user's web browser and other software like Adobe Flash and PDF Reader, Java, SQL, etc. Once the vulnerability is exploited, it then downloads and runs the malware on the system. Thus, by merely visiting a compromised website a user's computer may get infected.

Android malware detection statistics

Given below are the detection statistics of Android malware & samples received by Quick Heal in Q2 2016.

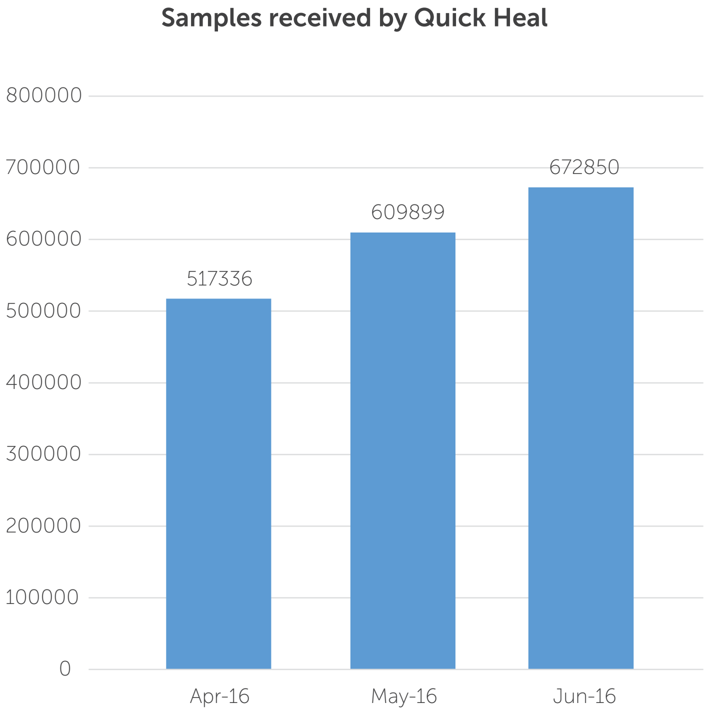


Fig 1

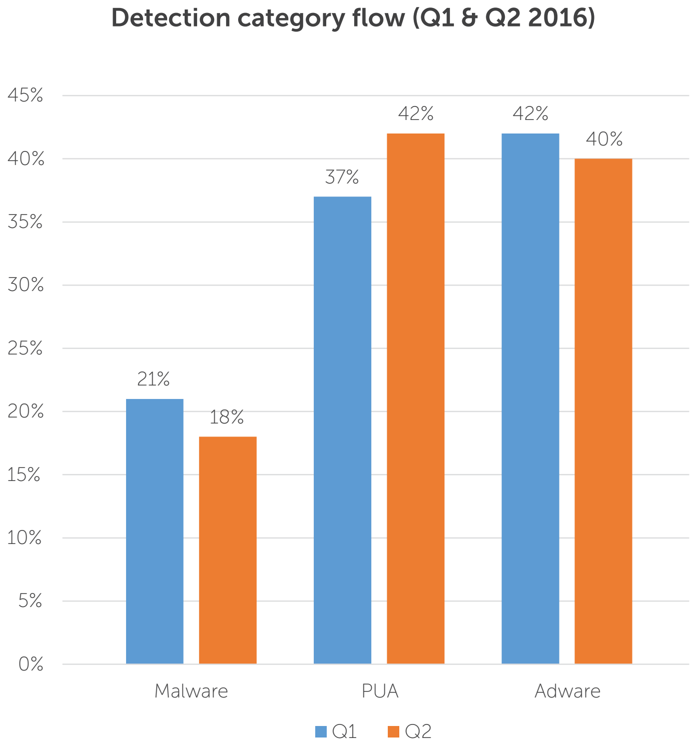


Fig 2

Observations:

- When compared with Q1, Q2's Android malware detection has dropped by 2.1%.
- The malware and adware family has shown a little respite in their detections; each falling by 3% and 2% respectively.
- Detection of Potentially Unwanted Programs (PUAs) has shown an increase of 5% in Q2, when compared with Q1.

Top 10 Android malware

The top 10 Android malware detected by Quick Heal in Q2 2016 are as follows:

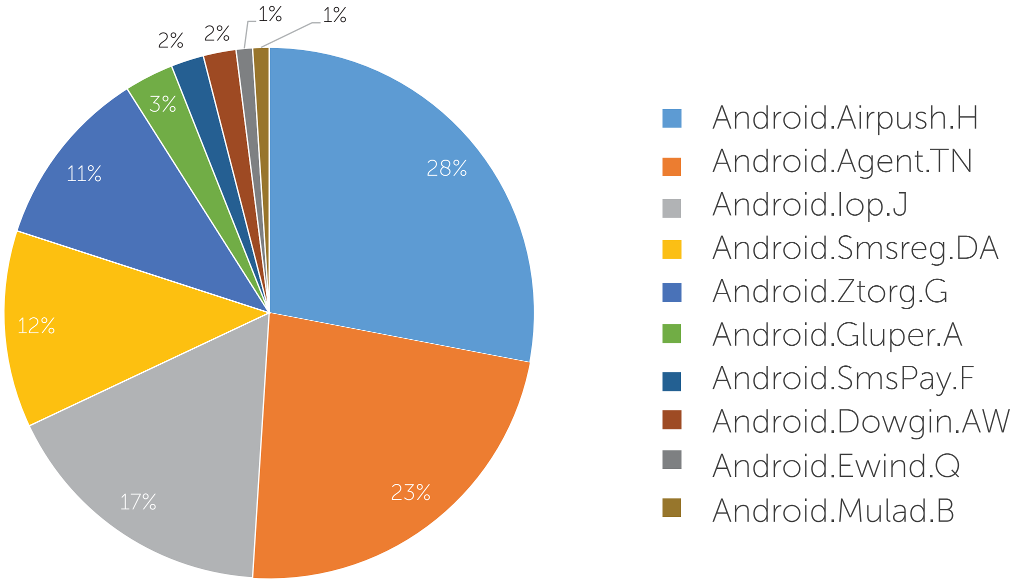


Fig 3

Android.Airpush.H

Damage Level: MEDIUM

Category: Adware

Method of Propagation: Google Play Store.

Behavior:

- Shows ads while the affected app is in use.
- Downloads unwanted apps by visiting their URLs.
- Steals user and device information and sends it to the attacker.
- Fetches user's location for pushing ads.

Android.Agent.TN

Damage Level: HIGH

Category: Malware

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

Behavior:

- Shows itself as an adult entertainment app; performs malicious activity in the background.
- Attempts to gain the affected device's admin rights.
- Sends device information to an external server.
- Requests for action from the adware component of other ads.
- On receiving certain information about how the user is interacting with the app (such as 'user present' and 'connectivity change') the app stops itself.

Note: Android.Agent.TN is popularly known as the 'Hummer malware'.

Android.Iop.J

Damage Level: HIGH

Category: Malware

Method of Propagation: Fake apps in third-party app stores.

Behavior:

- Looks like a normal application but carries a hidden encrypted file inside it.
- Decrypts and loads the encrypted file which in turn drops the malicious file.
- Installs additional malicious applications and sends all installed packages as well as device information to an external server.

Android.Smsreg.DA

Damage Level: MEDIUM

Category: Potentially Unwanted Application (PUA)

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

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, contact list, etc., and sends it to a remote server.

Top 10 Android malware

Android.Ztorg.G

Damage Level: HIGH

Category: Malware

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

Behavior:

- Drops downloaded packages, extracts binaries from them and tries to start them with admin privileges on the infected device.
- Downloads malicious files on the device and lowers security settings.
- Steals user's personal information.

Android.Gluper.A

Damage Level: HIGH

Category: Malware

Method of Propagation: Third-party app stores.

Behavior:

- Hides its icon after it gets executed for the first time.
- Tries to connect to a malicious URL, without the user's knowledge.
- Sends device details such as IMEI, IMSI, Model, Brand, and OS details via the connected URL.
- Decrypts files which are nothing but exploits (malicious codes that take advantage of security vulnerabilities in software).
- Attempts to gain admin privileges to take complete control of the infected device.
- Looks for any security application installed on the infected phone.

Android.SmsPay.F

Damage Level: MEDIUM

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores.

Behavior:

- Asks for device administrator permission to gain full control of the infected device.
- Displays a user agreement asking for the user's permission to send SMSs; the agreement only has an OK button without any option to reject the notice. If the OK button is opted, the app starts sending SMSs whose cost is incurred by the user.

Android.Dowgin.AW

Damage Level: LOW

Category: Adware

Method of Propagation: Third-party app stores.

Behavior:

- Displays unwanted ads on the infected device.
- Decrypts the malicious file from the asset having any random name.
- Loads the decrypted file and after loading it, deletes the original file from storage.
- Collects device info such as IMEI, IMSI, device version, and location.

Android.Ewind.Q

Damage Level: LOW

Category: Adware

Method of Propagation: Third-party app stores.

Behavior:

- Displays ads on the infected device while the app is in use.
- Shows ads on the device's home screen even if the application is idle and not running in the background.
- Repackages genuine applications with malicious codes to push ads.
- Downloads potentially malicious files if these ads are clicked.

Android.Mulad.B

Damage Level: MEDIUM

Category: Adware

Method of Propagation: Third-party app stores.

Behavior:

- Collects and sends sending data such as IMEI, device location, device model number, time zone, SIM operator name, user account info (email ID), and MAC address to the ad server, so that it can display targeted ads on the infected device.
- Requests ads stored in HTML format and serves these ads to the user.
- Redirects the user to third-party app stores tricking them into install app themes, which are designed to show more ads.

Mobile Ransomware and Banking Trojans

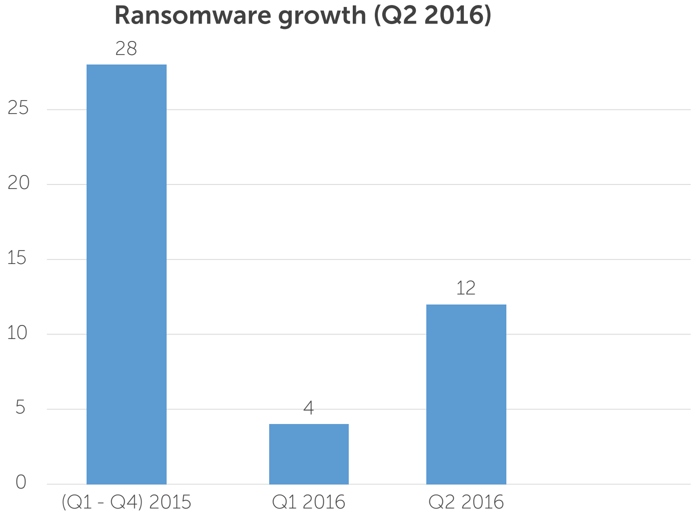


Fig 4

One family that has created much noise in the mobile threat landscape is the Android ransomware. As aptly predicted in 2015, ransomware is set to become one of the greatest banes of Windows and Android users alike. This family has been spreading and evolving since the time it began its journey. In Q2 2016, Quick Heal detected new ransomware variants that target Android devices, including old and new families.

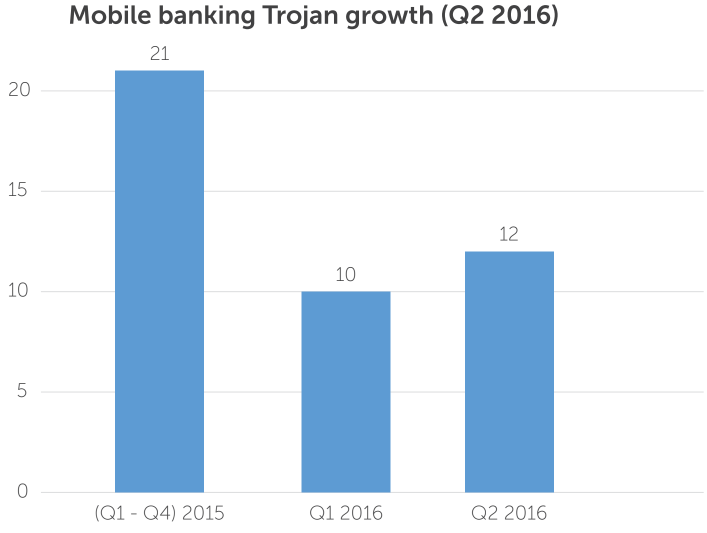


Fig 5

Adding to the woes of ransomware are banking Trojans which have showed no respite in their consistent growth. Under the category of mobile banking Trojans, 10 new families were detected. These included completely new families and new variants of existing families as well.

Observations:

1. Q2 recorded a 200% rise in the detection of Ransomware, compared with the previous quarter.
2. Q2's detection of Ransomware is almost close to 50% of the detection of the entire year of 2015.
3. Newer variants of mobile banking Trojans are using obfuscation techniques to bypass and avoid security detection.

Malware Using Unique Techniques

1). **Android.Fusob.F - Mobile Ransomware**

The first variant of this ransomware surfaced in May 2015. Many new variants of this malware were observed in mid-April 2016. These variants are armed with advanced obfuscation techniques to avoid detection from antivirus software. The latest variant of “Android.Fusob.F” is a police Trojan that pretends to be US Cyber Police or another law enforcement agency. Once the malware has successfully infected a system, it takes photos of the user and displays a ransom note; first, accusing the victim of crimes they haven’t commit. This warning is followed by a demand (ransom) of iTunes gift cards worth 200 USD. Reportedly, if the infected device’s location belongs to some of the Eastern European countries, the malware deactivates itself.

2). **Android.Viking.A - Viking Horde: Botnet campaign on Google Play**

At least five instances of the Viking Horde malware were observed in the Google Play store. Viking Horde creates a botnet that uses proxies IP addresses to disguise ad clicks, generating revenue for the attacker. The malware conducts ad fraud, and can also be used for attacks such as DDoS attacks, and spam messages. The C&C sends a "create proxy" command with two IP addresses and ports as parameters. These IP addresses are used to open two sockets - one for a remote server (which is a client of the botnet exploiting the anonymous proxy) and the other for the remote target. In this way, the malware hijacks the device to simulate clicks on advertisements to gain profit. On rooted devices, it installs additional components which makes malware removal more challenging.

3). **Android.Triada.K - Android malware embeds into browsers**

This Android Trojan is capable of embedding itself into mobile browsers, intercepting URL requests, and modifying those URLs so that users get redirected with other web pages. It gains root access of the infected device, then modifies zygot process of the kernel to achieve persistence. It injects itself into the following processes of different browsers:

- com.android.browser (the standard Android browser)
- com.qihoo.browser (360 Secure Browser)
- com.ijinshan.browser_fast (Cheetah browser)
- com.oupeng.browser (Oupeng browser)

The malware can monitor and modify the URLs the user is trying to view in a browser.

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 attacks by hackers and malware. While this has been an age-old security concern for Windows, it has gradually started to affect the Android platform at a scarily rapid rate. Compared to two quarters of 2015, Quick Heal Labs has observed significant growth in security vulnerabilities affecting Android smartphones in this quarter. Below are some statistics in support of this finding.

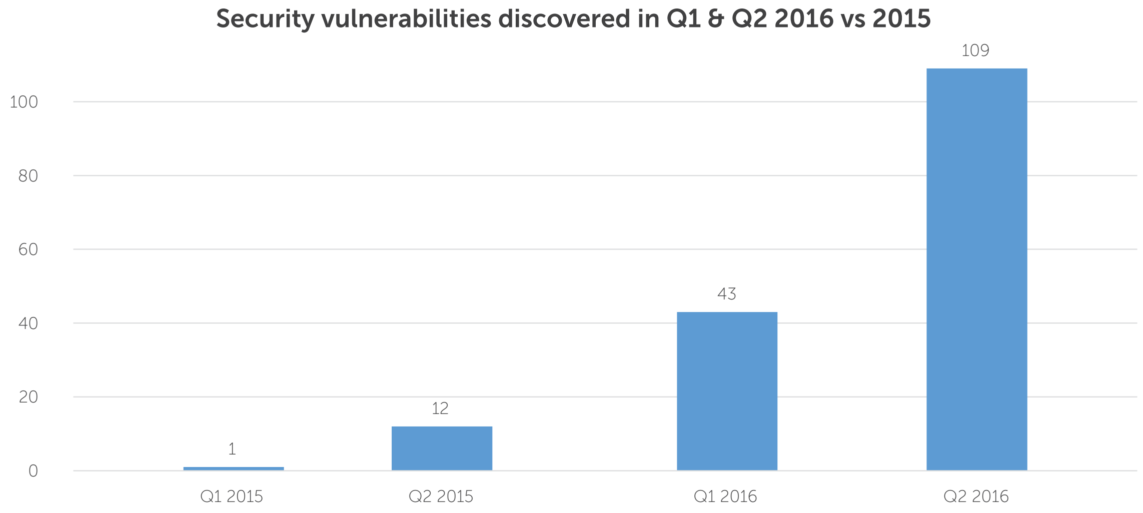


Fig 6

Source: https://www.cvedetails.com

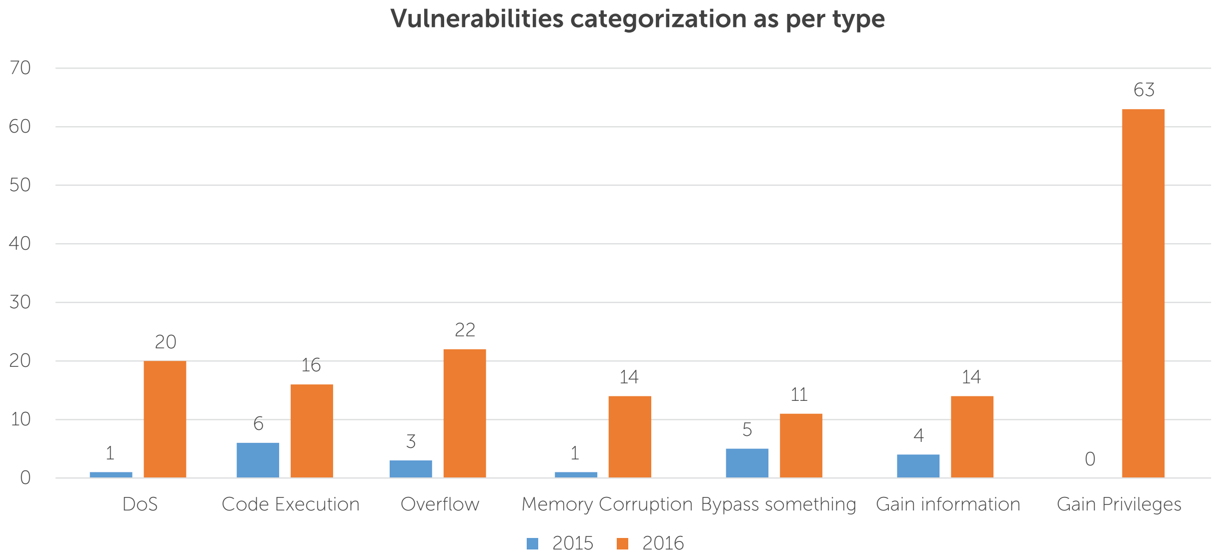


Fig 7

Source: https://www.cvedetails.com

Observations:

- The detection statistics of security vulnerabilities from Q2 2016 has easily overshadowed those from Q1, Q2 2015 and Q1 2016 combined.
- In 2016, 152 types of security vulnerabilities have been found on the Android platform. Most of these go unnoticed and unpatched because either OS updates are not available from vendors or users don't apply the received updates.
- Security updates for Android devices generally take long to reach users. Devices older than 18 months are unlikely to receive any updates at all. A fix for this issue could be an over-the-air (OTA) firmware update for all affected devices.

A case in point of Android vulnerabilities - the Godless Malware

Godless is a newly detected Android malware that takes advantage of security vulnerabilities found in Android devices. Quick Heal Labs detects it as Android.Godless.A and Android.Godless.B.

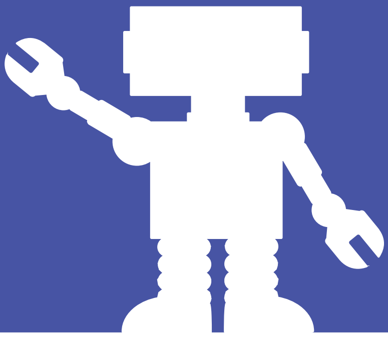
What does it do?

Godless is known to target devices running Android 5.1 Lollipop or earlier. It mainly targets two widely used vulnerabilities viz. CVE-2015-3636 (used by the PingPongRoot exploit) and CVE-2014-3153 (used by the Towelroot exploit).

Once installed on the targeted device, Godless:

- Gains root privilege and can then receive remote instructions by its creator.
- Can silently install unwanted apps on the infected device. These can be used to serve unwanted apps, spy on the user, or for allowing other malware to get into the device.

Read more about the Godless malware from our security blog.
http://blogs.quickheal.com/beware-of-the-godless-malware/



Trends and Predictions

1

Attacks on social networking sites are expected to increase

Malware attacks on social networking sites are likely to increase in the near future. By 2018, it is estimated that there will be about 2.55 billion users on social network. With such a sheer volume of user interaction, such sites are only easy targets for online scammers and cyber criminals. A case in point is the recent 'Facebook Comment Tagging Malware' incident which affected Chrome users. Here, users would receive an app or email notification about their friends tagging them in a comment. Clicking the link in the notification would download a malware on the targeted device. So, incidents such as these are likely to increase and become worse with time.

2

Banking malware threats are going to rise

Banking malware is going to be a concern in the coming days for security experts and more importantly users of mobile Internet banking. With almost all banks developing dedicated apps for banking, hackers are going to leverage this as a lucrative opportunity to trick users and generate illegitimate cash to further fuel their nefarious intentions.

CONCLUSION

There is no debate about the fact that cyber criminals are nefarious. But what's more concerning is that they are a busy lot. They too adapt to the ever-changing technology but for reasons which bring nothing but bad news for the rest of us. With social networking engulfing the lives of almost everyone who is connected to the Internet and mobile banking becoming a habit, users are but sitting ducks. One wrong move, informed or otherwise, can get them in the hairline of the attackers' crossbow. Carefully planned and targeted attacks on government organizations, and other private sectors are increasing, and so are cases of ransomware incidents. At the present time, a user simply needs to load a web page to get their computer infected by a malware, without having to click on anything. Criminals are tirelessly working to attack their preys with the least amount of human interaction. It would not be impractical to predict that we may get our device infected merely by switching it ON; yes, just like that. But all hope is not lost. Keeping ourselves updated with the latest security incidents, following a good security hygiene, and using the right defense for our protection, should be good enough to keep us in the green zone.