Quick Heal
Security Simplified

SEQRITE
Enterprise Security Solutions by Quick Heal

QUARTERLY THREAT REPORT Q3 2016

www.quickheal.com

TABLE OF CONTENTS

INTRODUCTION

This report aims to highlight some of the major malware detected on the Windows and Android platform by the Quick Heal Threat Research Labs in Q3 2016. The detections were analyzed for the malware threat level, their mode of propagation, behavior post infection, and their growth Q3 2016.

In Q3 2016, the threat analysis recorded a 14% jump in the overall detection count of Windows malware. Ransomware detections have increased by 22% when compared with Q2. The report lists out 11 new ransomware families that were observed in this quarter and also presents a case study on a particular strain of ransomware. Further, a genuine website was observed to have been spreading ransomware through its software.

Speaking of Android devices, the malware detection has increased by 34% and mobile ransomware has gone up by 33% in comparison with the previous quarter. The mobile banking Trojan family has also made the headlines, clocking a massive 76% increase in 2016 when compared with 2015. Security vulnerabilities found on the Android platform in Q3 2016 alone have increased by 158% when compared with the statistics recorded in all the three quarters of 2015.

The report concludes with information on some noteworthy Windows and Android malware, followed by trends and predictions about what we can expect in the upcoming months.

WINDOWS MALWARE DETECTION STATISTICS

Compared with Q2, Q3 recorded a 14% increase in the detection count of malware on Windows computers. Given below is the statistics of malware detected by Quick Heal Labs.

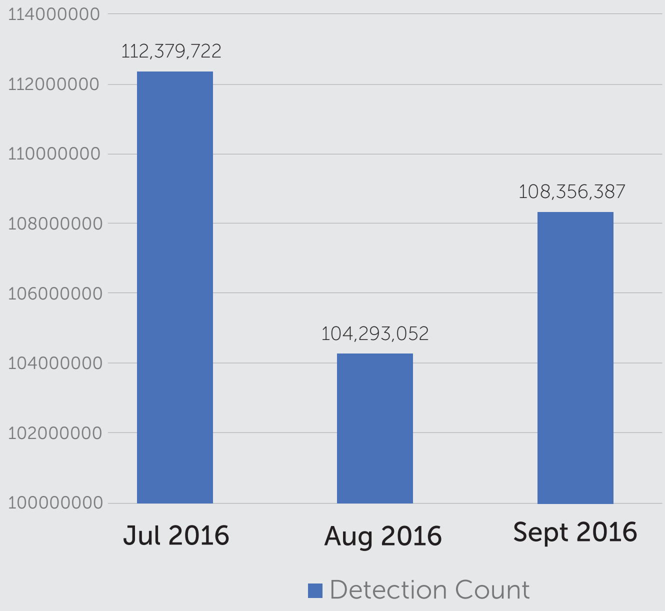


Fig 1

MONTH	DETECTION COUNT
July	112,379,722
Aug	104,293,052
Sept	108,356,387
TOTAL	**325,029,161**

TOP 10 WINDOWS MALWARE

The top 10 malware detected by Quick Heal in Q3 2016 are as follows:

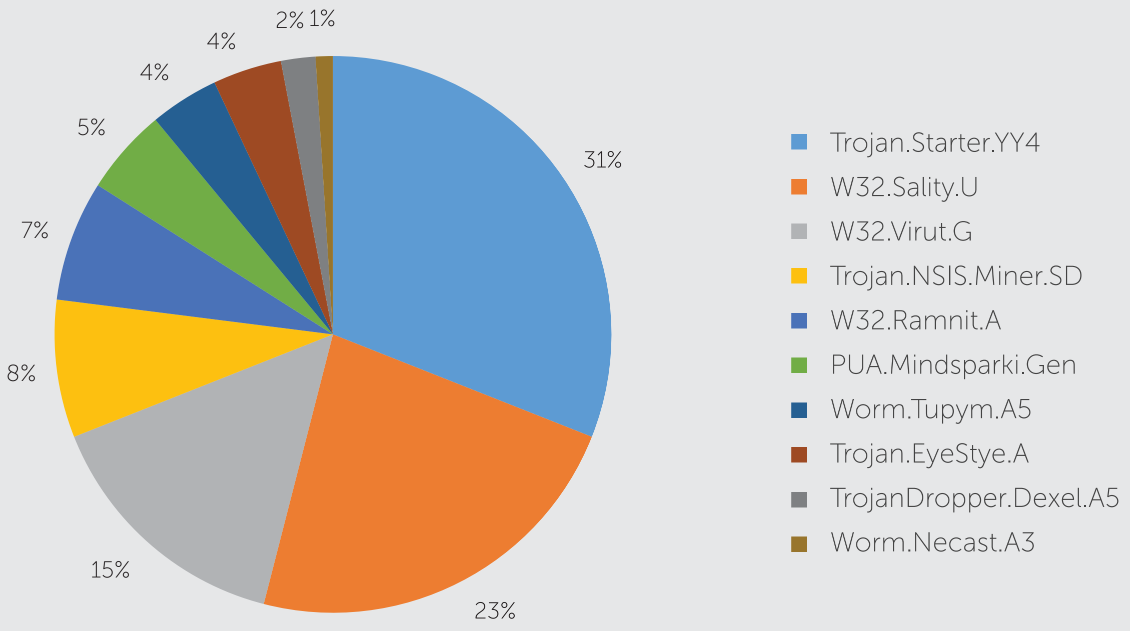
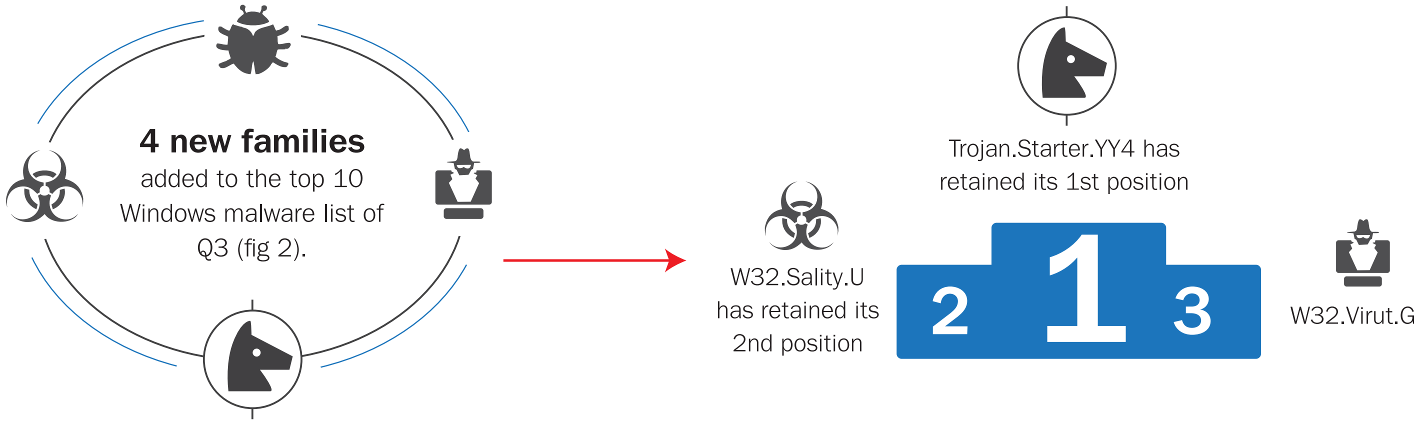


Fig 2

Observations in Q3 vs Q2:



4 new families

added to the top 10 Windows malware list of Q3 (fig 2).

Trojan.Starter.YY4 has retained its 1st position

W32.Sality.U has retained its 2nd position

W32.Virut.G

1. 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.

Behavior Post Infection:

- Creates a process to run the dropped executable file.
- Modifies computer registry settings which may cause a 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.

2. W32.Sality.U

Damage Level: MEDIUM

Method of Propagation: Bundled software and freeware

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.

Behavior Post Infection:

- 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.

3. W32.Virut.G

Damage Level: MEDIUM

Method of Propagation: Bundled software and freeware

Summary: W32.Virut.G is 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 enter the infected system.

Behavior Post Infection:

- 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.

4. Trojan.NSIS.Miner.SD

Damage Level: HIGH

Method of Propagation: Bundled software and freeware

Summary: Trojan.NSIS.Miner.SD is a Trojan that comes with freeware and shareware programs. Once installed on the infected computer, it redirects the victim to malicious websites.

Behavior Post Infection:

- Downloads or installs free software from malicious websites.
- 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.
- Opens a backdoor for other malware to enter the infected system.

5. W32.Ramnit.A

Damage Level: HIGH

Method of Propagation: Removable and remote shared drives

Summary: W32.Ramnit.A is a file infector designed to infect .EXE, .DLL, .HTML files for malicious purposes.

Behavior Post Infection:

- Creates a backdoor by connecting to a remote server.
- Using this backdoor, a remote hacker can download other malware or run harmful files on the infected system.
- Creates a default web browser process and injects a malicious code into it.
- Steals information from the infected system.

6. PUA.Mindsparki.Gen

Damage Level: MEDIUM

Method of Propagation: Bundled software and malicious websites

Summary: PUA.Mindsparki.Gen is a Potentially Unwanted

Application (PUA) that comes with third-party bundled installer applications and software downloaders.

Behavior Post Infection:

- 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.

7. Worm.Tupym.A5

Damage Level: LOW

Method of Propagation: Removable and remote shared drives

Summary: Worm.Tupym.A5 is a worm that changes browser settings like homepage and search engine.

Behavior Post Infection:

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

8. Trojan.EyeStye.A

Damage Level: HIGH

Method of Propagation: Removable and remote shared drives

Summary: Trojan.EyeStye.A is a Trojan designed to steal confidential data for destructive purposes.

Behavior Post Infection:

- Copies itself to the targeted drive and modifies registry entry to execute itself automatically.
- Copies and uses autorun.inf files for automatic execution.
- Rapidly spreads from one infected system to another.
- Steals important data from the victim's computer and shares it with a remote server.
- Slows down system performance by consuming more resources.

9. TrojanDropper.Dexel.A5

Damage Level: HIGH

Method of Propagation: Email attachments and malicious websites

Summary: TrojanDropper.Dexel.A5 is a Trojan that can break the infected system's security.

Behavior Post Infection:

- 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.

10. 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. The worm also uses the latest programming language and technology and has the ability to change its characteristics in order to evade detection and removal by antivirus software.

Behavior Post Infection:

- Utilizes advanced Java, Active X and VB Script techniques to propagate its components onto HTML pages.
- 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.

MALWARE CATEGORY-WISE DETECTION STATISTICS

The below graph presents the statistics of every category of Windows malware that were detected by Quick Heal in Q3 2016.

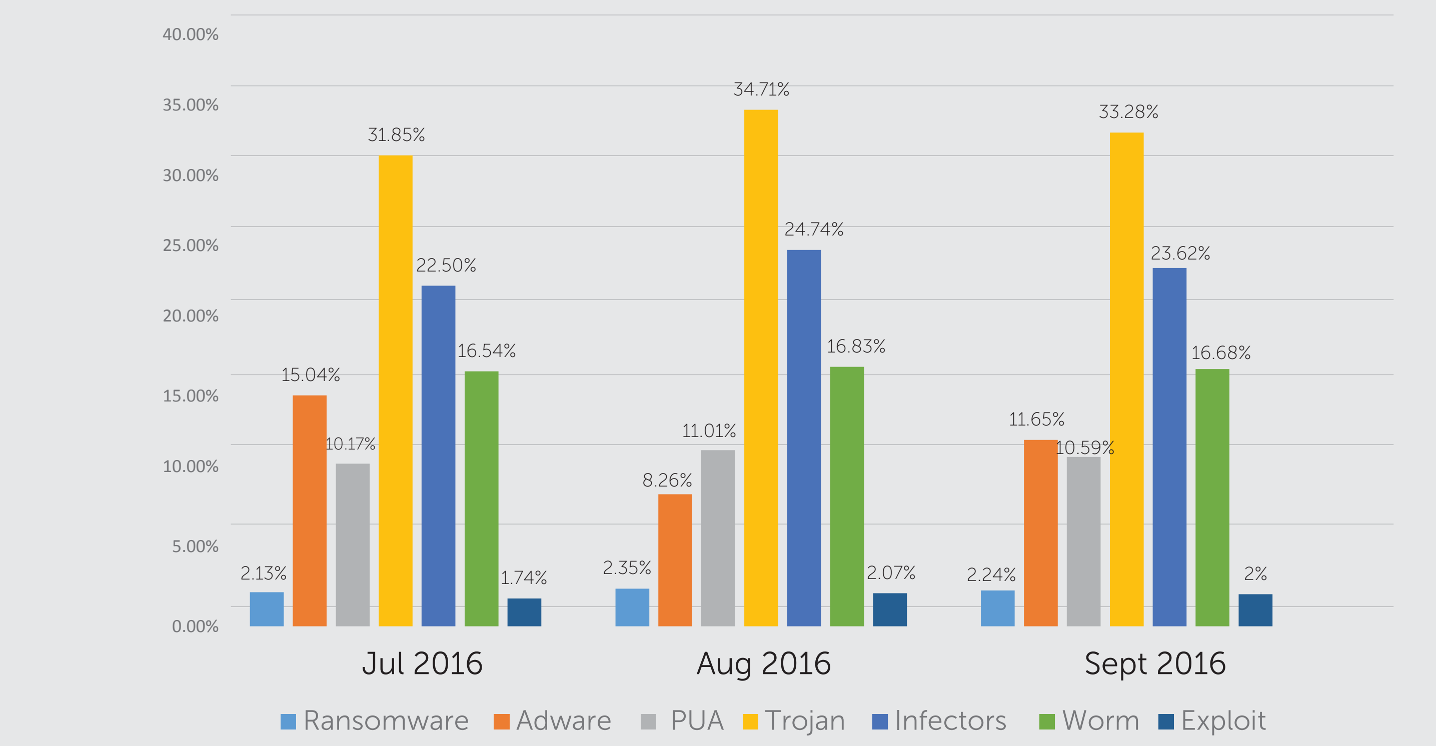


Fig 3

Observations in Q3 vs Q2:

1

Trojan leads the pack with **(~33%)** (fig 3)

Infector follows with a detection of **(~23%)** (fig 3)

Worm accounts for **(~16%)** of the detection count (fig 3)

2

RANSOMWARE GROWTH

1.8% (Q2 2016)

↑ **22%**

2.2% (Q3 2016)

3

Adware and **PUA** account for **23%** of the detections on an average.

TOP 10 PUAs AND ADWARE

Here are the top 10 PUAs and adware samples detected by Quick Heal in Q3 2016.

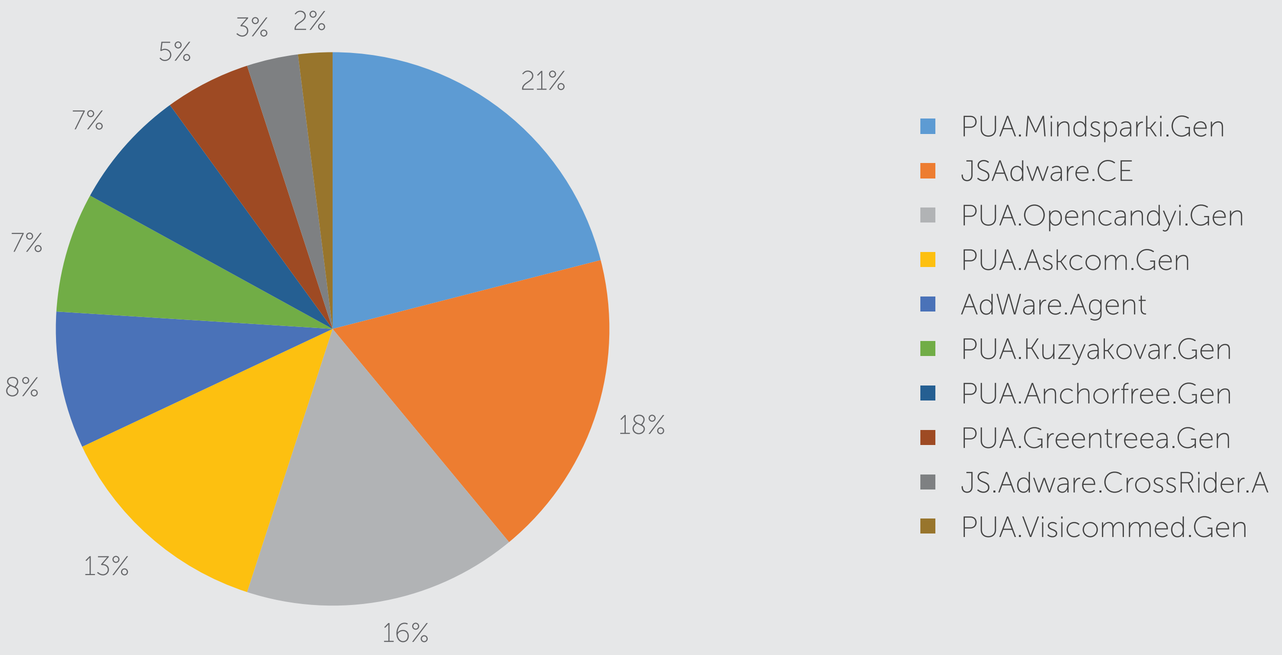


Fig 4

Observations in Q3 vs Q2:

1. In Q3 2016, the top PUAs reported are Mindsparki, Opencandy and Askcom.
2. Anchorfree has reported a high count than that of the previous quarter. It is a browser hijacker and often comes bundled with free software. It changes browser settings like homepage and search engine, and also adds unwanted toolbars.
3. Visicom Media behaves like a browser hijacker. It can add yahoo, goodsearch or similar other toolbars to the infected system's browsers and change the default homepage, search engine, etc. It is designed to alert the user about free coupons, discounts or special deals available on the merchant's site.
4. Adware CrossRider may install BHO/Plugins/extensions and change some of the browser settings without user consent. It also shows pop-up ads on web pages while the user is surfing the internet. The adware can also inject advertising banners into web pages.

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.

The top 10 Windows exploits of Q3 2016 are as follows:

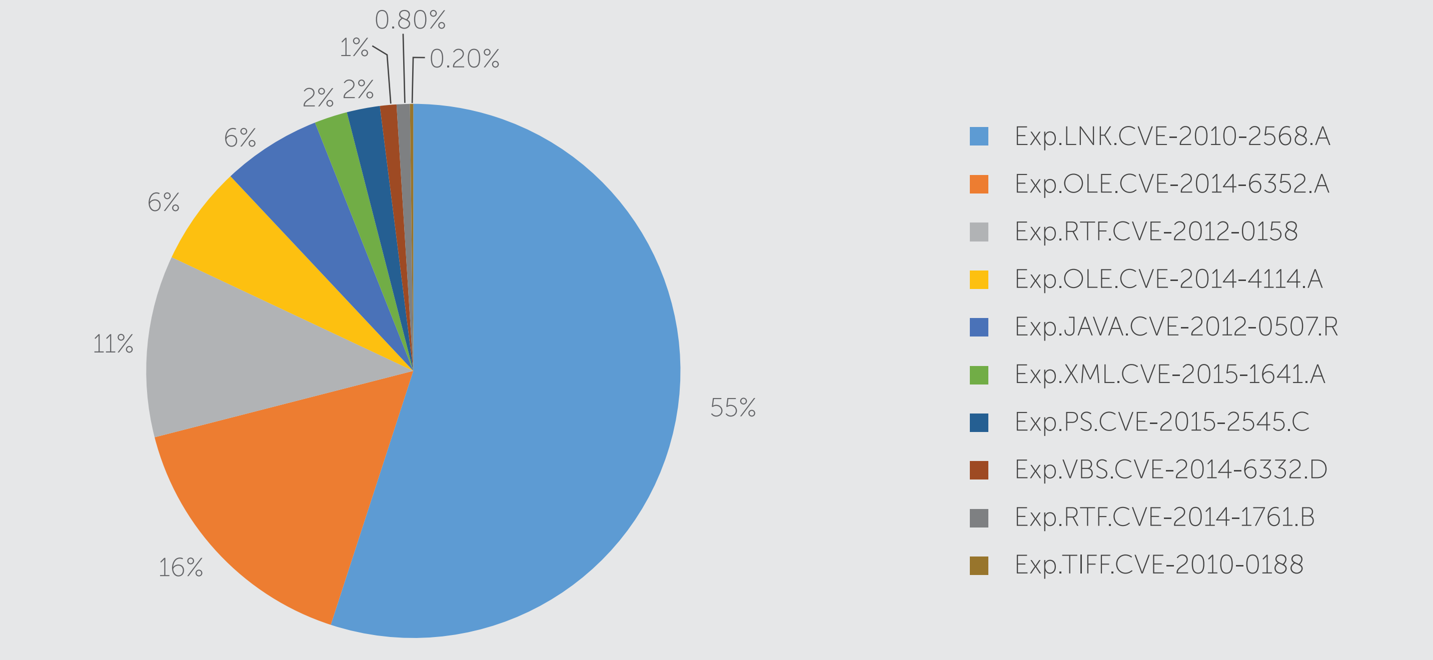


Fig 5

5.1 Most observed Common Vulnerabilities and Exposures (CVE) in spam campaigns

CVE-2012-0158 is a security vulnerability which was widely used in various spam campaigns in Q2. However, its usage has died down as hackers seem to be using another vulnerability called CVE-2015-2545.

Read the detailed analysis of CVE-2015-2545 here > http://bit.ly/2eJ3Vkh

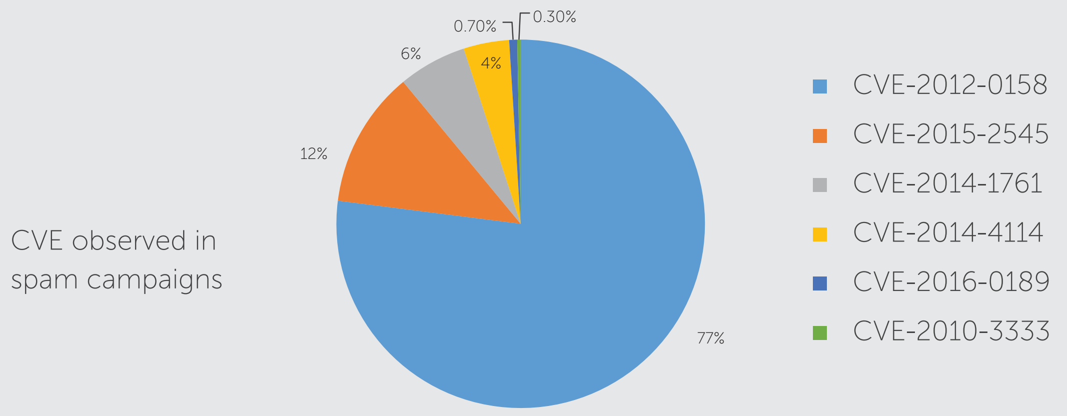


Fig 6

5.2 Most observed CVE in Advanced Persistent Threat (APT) attacks

For the last few years, CVE-2012-0158 has been widely used in many targeted attacks. But, this vulnerability is being replaced by another vulnerability called CVE-2015-1641.

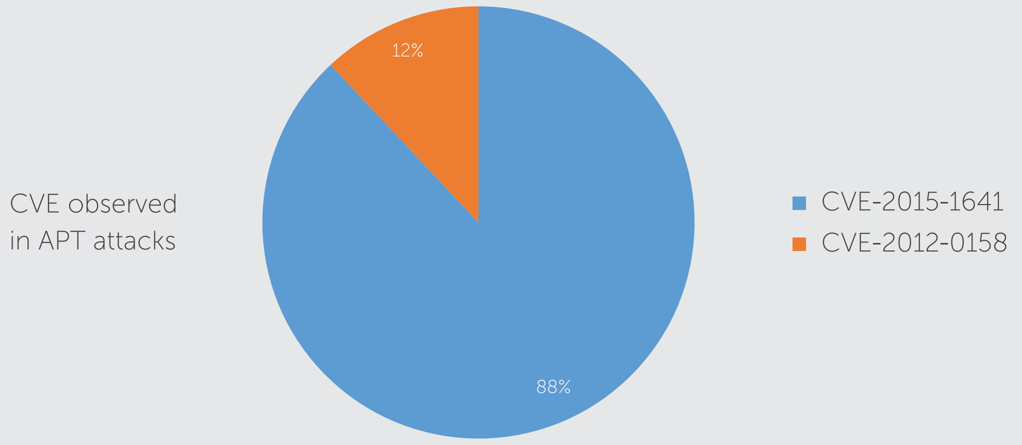


Fig 7

5.3 Most observed exploit kits

An exploit kit is like a box that contains several malicious codes. It is designed to identify software vulnerabilities on the system it is placed and targeting these vulnerabilities with the right code that it has in store.

After the shutdown of the Angler exploit kit, Neutrino became the most widely used exploit kit in Q3.

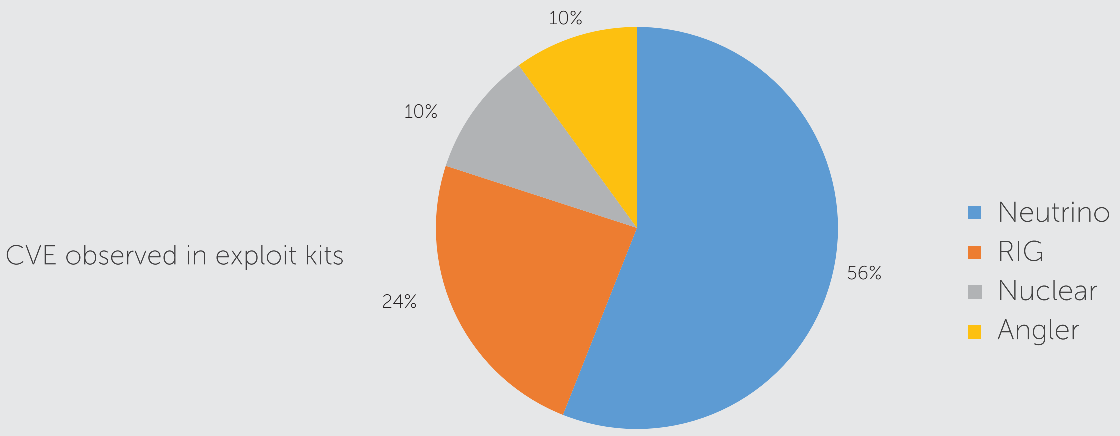


Fig 8

MAJOR WINDOWS MALWARE

Ransomware

Q3 has clocked a high success rate for ransomware attacks coupled with new variants. In this quarter, a new variant of the Locky ransomware known as the Zepto ransomware has been on the rise. It is spreading rampantly through malspam (malicious spam) and exploit kits. The most apparent change observed in Zepto is in the appended extension of the encrypted files, i.e., from '.locky' to '.zepto'. In most cases, the victim receives an email containing an attachment that seems to be from a legitimate source. The archived attachment (which can contain a JS, WSF, HTA or DOCM) file is actually a Trojan Downloader responsible for downloading the payload on the targeted computer. The downloaded payload is initially an encoded extension-less file which is then decoded by the Trojan downloading into an executable file (.EXE) which then forms into an encryptor ransomware. In later variants, we observed that the payload changed from an executable (.EXE) to a Dynamic link library (.DLL). The use of DLL files was previously seen in CryptXXX ransomware variants, which were spread through the Angler exploit kit, and then the Neutrino exploit kit later on.

Incidents of ransomware spreading through non-pe (portable executable) files have increased in Q3. Below are the top 10 detections for non-pe files acting as a downloader.

Top 10 non-pe ransomware received

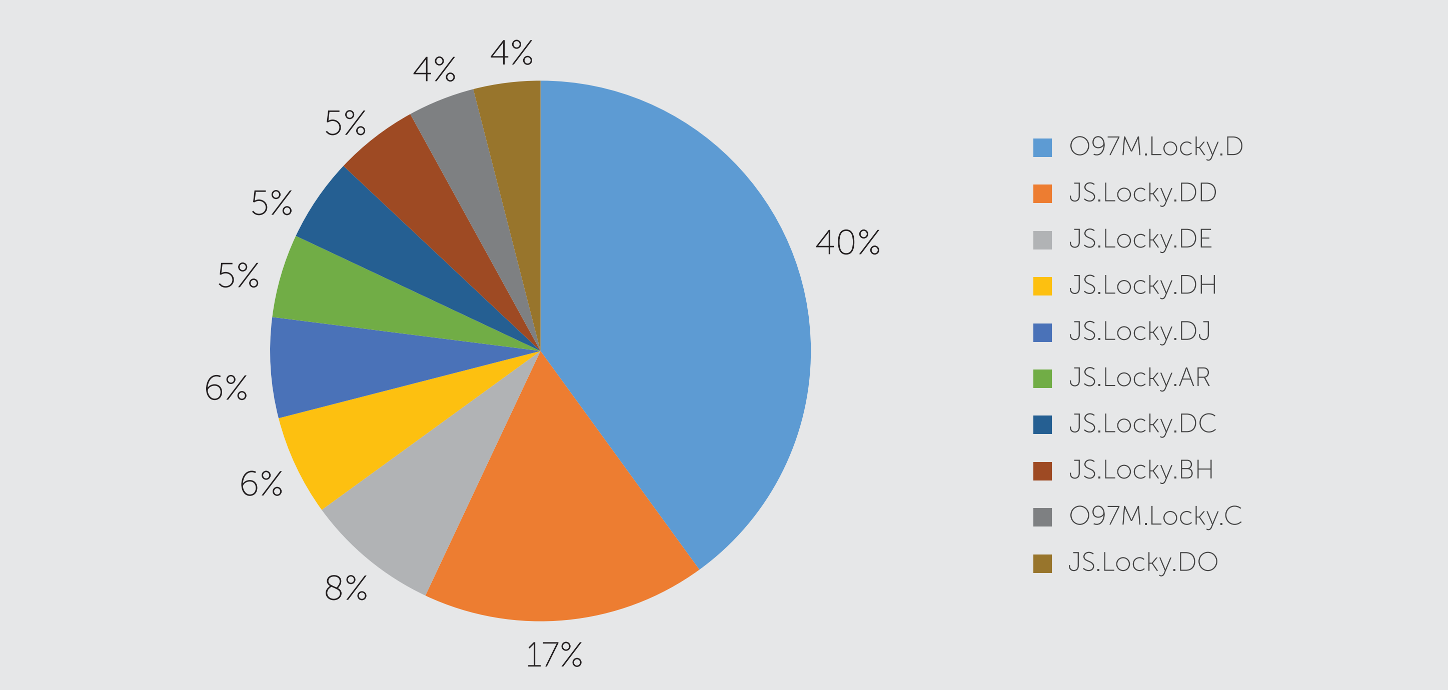


Fig 9

Further reading

The Troldesh Ransomware

As observed recently, criminals are using a new carrier to deliver the ransomware known as Troldesh (also known as XTBL). Cybercriminals are suspected of spreading and executing this malware by directly gaining access to the victim's computer through Remote Desktop. By default, Windows Remote Desktop will work only on a local network unless configured otherwise on a router or H/W Firewall. This is usually seen in organizations where systems (usually servers) are accessed from multiple branches for various tasks. This explains why most of the affected systems are Windows Server OS. Remote access to the victim's computer is gained by using brute force techniques which can effectively crack weak passwords.

Typically, a brute force attack scans IP ranges and TCP ports (3389 in the case of RDP) which are open for connection. Once an attacker finds a port, they launch the attack. The brute force technique uses a trial and error password guessing attack with a list of commonly used credentials, dictionary words, and other combinations. Once the access is gained, criminals simply disable the system's antivirus and run the payload directly. This means, even if the antivirus is updated and has a detection against the malware, turning off its protection renders the system defenseless.

Read more about Troldesh here > http://bit.ly/2eUIOIi

The Cerber3 Ransomware

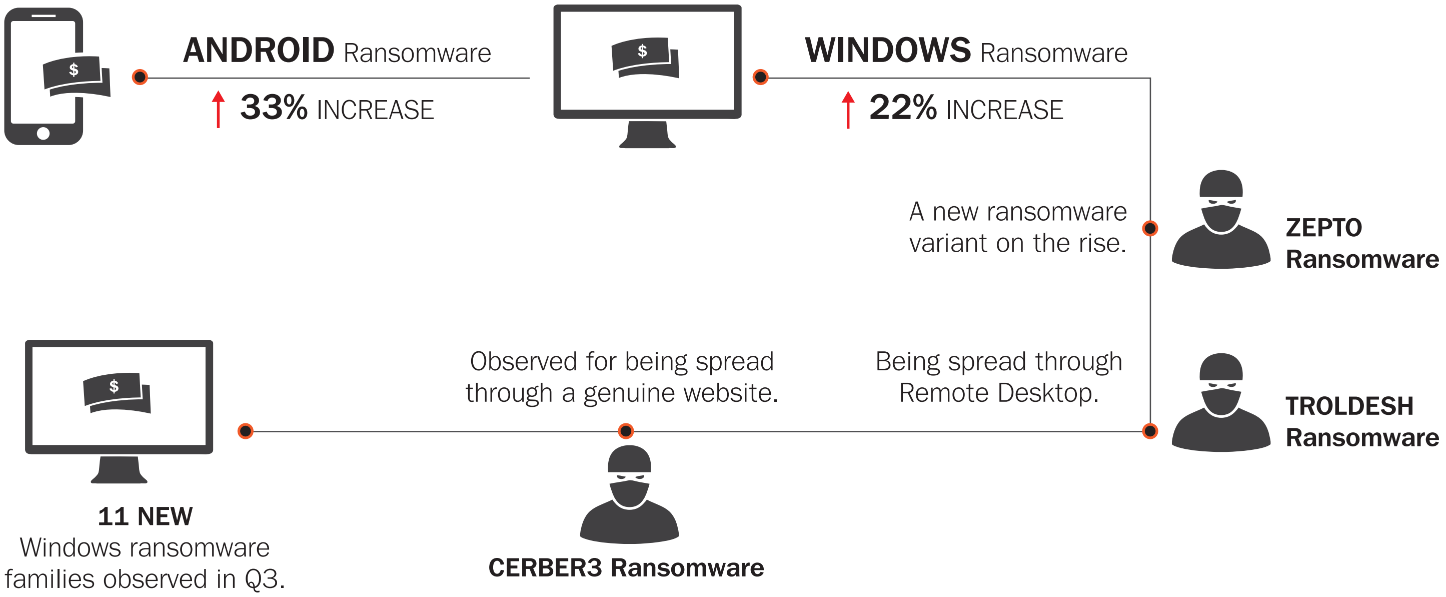
We have observed that a new variant of the Cerber3 Ransomware is being spread through the Ammyy Admin software on the official Ammyy Admin website. This news, however, is not surprising as this website has been found to host malware on several instances. In a previous case, the website was found to spread the notorious Cryptowall 4.0 Ransomware. We have also observed increased cases of Cerber ransomware infections wherein the victims had downloaded and run the Ammyy Admin software from the original website.

Read more about the Cerber3 Ransomware here > http://bit.ly/2cijZqV

New ransomware observed in Q3 2016:

- Crypmic
- VenusLocker
- PokemonGo
- Hitler
- Shark
- DetoxCrypto
- CryptoBit
- Domino
- CryptoFinance
- Cry
- HDDCrypt

The Ransomware Situation in Q3 vs Q2 (2016)



ANDROID Ransomware

↑ **33%** INCREASE

WINDOWS Ransomware

↑ **22%** INCREASE

A new ransomware variant on the rise.

ZEPTO Ransomware

Being spread through Remote Desktop.

TROLDESH Ransomware

Observed for being spread through a genuine website.

CERBER3 Ransomware

11 NEW Windows ransomware families observed in Q3.

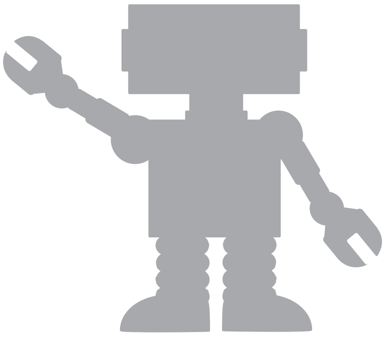
Targeted Attacks

A targeted attack is launched to steal confidential and critical data from targeted systems. This kind of an attack is designed to steal intellectual property or extract confidential information over a period of time, instead of carrying out a short-term but deadlier attack or denial of service. The NetTraveler APT campaign has been running since 2004 and targeting different companies. In this campaign, attacks were carried out by shooting spear-phishing emails that contained compromised URLs hosting malicious Microsoft Word documents designed to exploit the CVE-2012-0158 vulnerability.

Adware

Adware is a program that enters the user's computer with freeware bundled software. Adware displays unwanted ads and pop-ups when a user is online. It can also redirect the user to the targeted advertisement. Additionally, adware can be used to hijack web browsers where it changes the browser's default settings, homepage, etc. In Q3 2016, we saw an interesting piece of Adware known as Dotdo Audio which employs a different method for advertising and browser hijacking. Advertisements are presented in the form of an audio instead of images, banners, etc. For browser hijacking, Dotdo Audio replaces executables of installed web browsers like chrome.exe, firefox.exe, etc., with their own executables while the original executables are renamed and kept as chrome334.exe and firefox334.exe, etc. After these replacements are done, opening any browser shortcut will trigger a fake browser with audio advertisements in the background. With this technique, the hijacker doesn't have to make any modifications in the browser's shortcut target path.

TRENDS AND PREDICTIONS



1

Ransomware

Ransomware variants will continue to evolve, and advanced variants of families such as Locky/Zepto will be a challenge for security products. We can expect Locky/Zepto ransomware getting embedded in PDFs and other formats.

Ransomware-as-a-service (RaaS) type attacks may increase due to its user friendliness and its availability.

Crypmic is another ransomware family which is expected to hit its target with new variants and sophisticated propagation techniques.

In the coming days, new ransomware attacks are expected to rise because this malware family has proven to be the most profitable type of attack.

2

Adware

Attackers have broadened their scope of attacks with the help of adware. Strategies are changing from showing only ads to stealing information and developing destructive capabilities such as ransomware infections. Adware or Potential Unwanted Programs (PUPs) may hook themselves into running genuine processes making it difficult for installed security software to trace their presence in the infected system.

CASE STUDY - EXPLOIT OF CRYPMIC RANSOMWARE

Ransomware like CrypMIC, CryptXXX, and Zepto are now spreading rampantly through exploit kits like Angler, Neutrino, and Rig. We had recently come across one such incident of CrypMIC ransomware wherein based on the evidence collected and analysis conducted, we were able to trace some of the steps that led to the infection.

The traced scenario:

- On the day of the encryption, it was observed that the user was browsing some websites on Internet Explorer.
- Among the several websites visited, the user had also visited a compromised website that was responsible for triggering the infection chain.
- The compromised website redirected the user to a suspected landing page that hosted the Neutrino exploit kit. The site, in this case, 'bxxxxxxxtion.maxxxxxxers.com'.
- From this landing page, the exploit was delivered onto the system via a flash file (bwzmexzlza.swf).
- As soon as the above exploit file was downloaded, within a few seconds, we observed a series of activities which were related to the download of the ransomware payload (%temp%\rad43d29.tmp.dll).
- Windows system file regsvr32.exe was then called to load the above ‘rad43d29.tmp.dll’ file which was found out to be the main encryptor ransomware.
- Before the ransomware begins encrypting the files, it runs the command ‘vssadmin.exe delete shadows /all /quiet’ to prevent the chances of any recovery through volume shadow copies.
- And as expected, after the encryption was completed, the ransomware opened up its ransom note informing the victim about the encryption and how the ransom is to be paid.

Quick Heal Browser Sandbox feature restricts the ransomware’s encryption activity.

ANDROID SAMPLES AND THEIR DETECTION STATISTICS

Given below are the statistics of Android samples received by Quick Heal in Q3 2016.

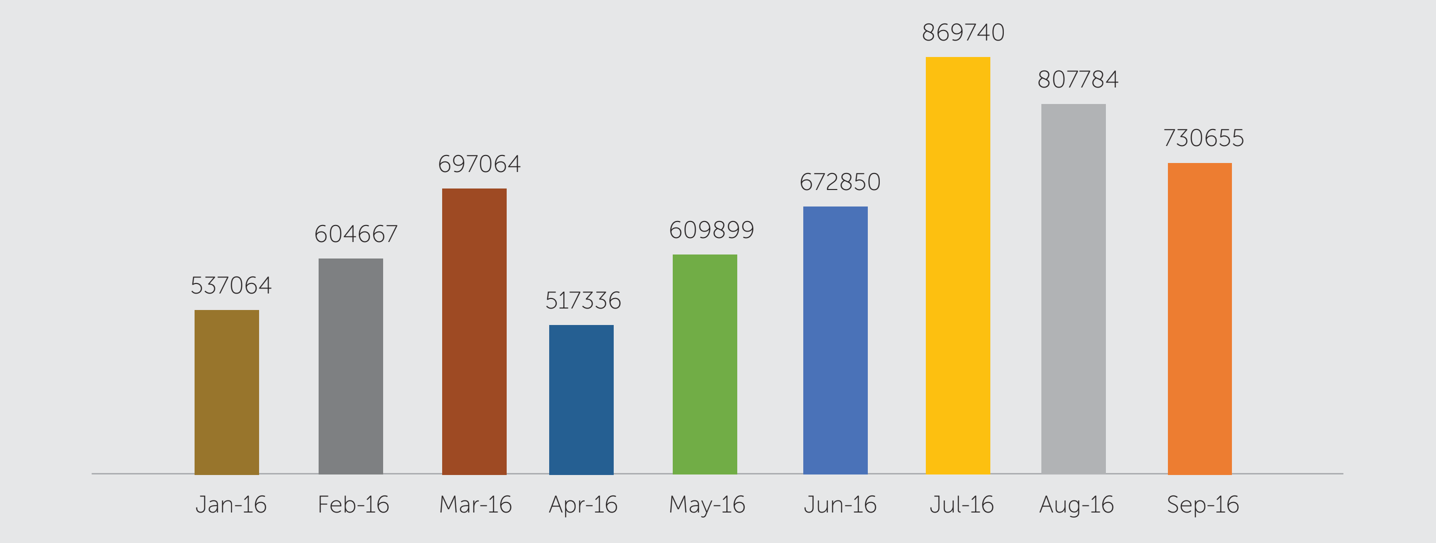


Fig 1

Detection category flow (Q1, Q2, & Q3 2016)

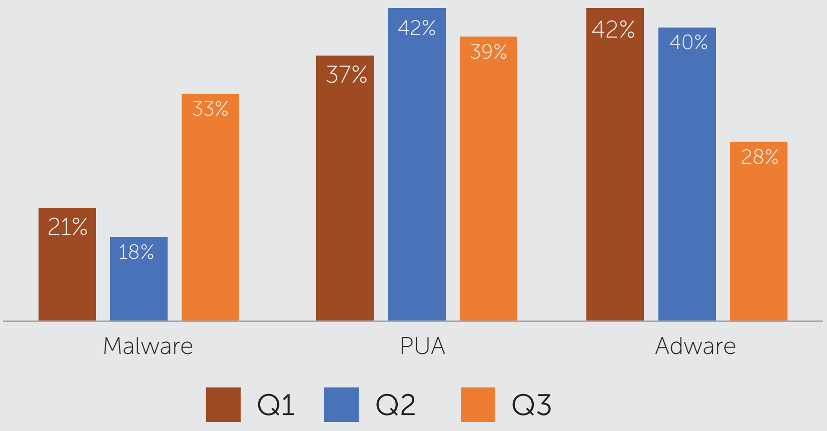


Fig 2

Observations in Q3 vs Q2:

The Android samples count has increased by about **34%** (fig 1).

The detection count of Potential Unwanted Applications (PUA) has dropped by **3%** (fig 2).

Mobile adware detection has dropped by **12%** (fig 2).

TOP 10 ANDROID MALWARE

The top 10 Android malware detected by Quick Heal in Q3 2016.

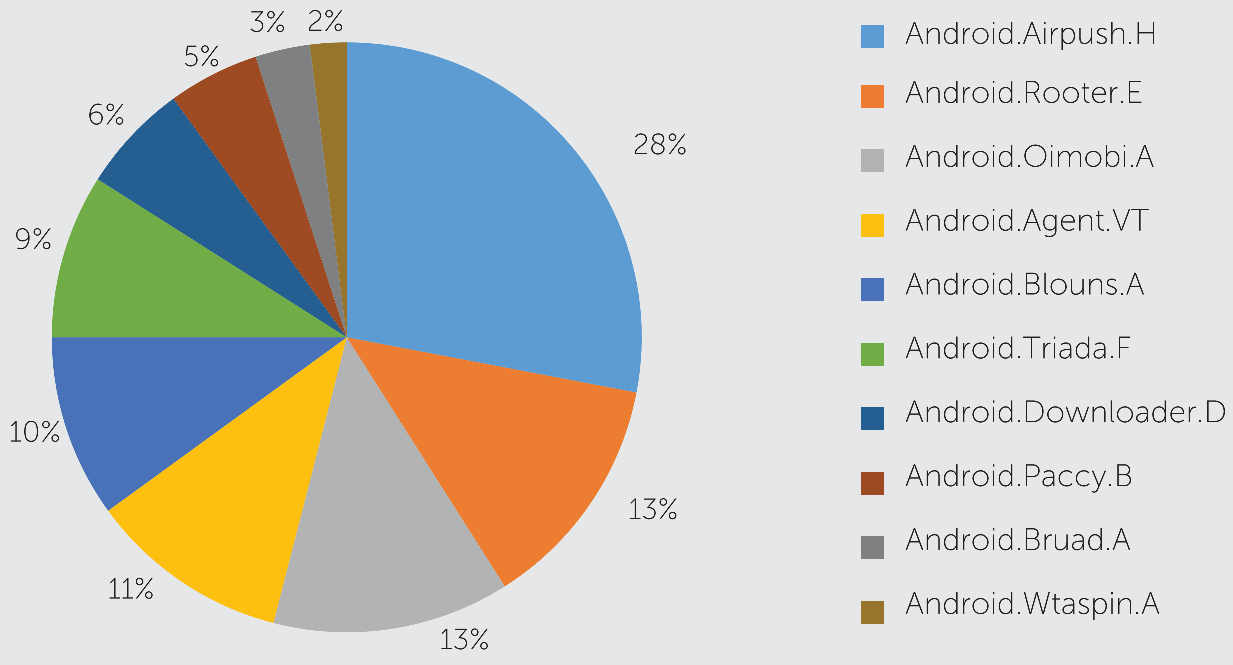


Fig 3

1. Android.Airpush.H

Damage Level: MEDIUM

Category: Adware

Method of Propagation: Google Play Store

Behavior:

- Shows ads while using the infected 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.

2. Android.Rooter.E

Damage Level: HIGH

Category: Potential Unwanted Application

Method of Propagation: Google Play Store, Kingroot.net, forum.xda-developers.com, etc.

Behavior:

- Displays unwanted ads.
- Checks if super user privileges are activated or not on the device. If not, it prompts the user for granting these privileges.
- Roots the infected phone with one click.
- Gathers device information such as IMEI, IMSI, etc.

3. Android.Oimobi.A

Damage Level: LOW

Category: Adware

Method of Propagation: Third-party app stores

Behavior:

- Repackages genuine applications injected with ads-related code.
- Connects to a server which can display ads or download malicious software on the infected device.
- Contains an encrypted file and after execution, it creates a malicious file in '\data\data\' folder of the device.
- Loads malicious files dynamically from assets which contain an adware SDK.

4. Android.Agent.VT

Damage Level: HIGH

Category: Trojan

Method of Propagation: Third-party app stores

Behavior:

- Most of the apps infected with this Trojan are adult apps. Once installed, the malware downloads and installs multiple malicious apps in the background without the user's knowledge.
- Displays a pop-up that prompts the user to install other apps; this pop-up cannot be dismissed.
- Collects information about all the Internet browsers installed on the infected device.

5. Android.Blouns.A

Damage Level: HIGH

Category: Trojan

Method of Propagation: Third-party app stores

Behavior:

- Makes use of an icon of any genuine application to fool the user.
- On execution, it shows the message "To complete the installation, please find <app name> in accessibility screen, click it and enable it". The message doesn't have a cancel button and forces the user to enable the accessibility in order to use the app.
- Spies on the device data such as IMEI, IMSI, package install, version number, etc., and uploads the information to a remote server.

6. Android.Triada.F

Damage Level: HIGH

Category: Trojan

Method of Propagation: Third-party app stores

Behavior:

- Hides its icon, and runs silently in the background.
- On execution, it asks the user to grant device admin permissions.
- Starts displaying a pop-up that prompts the user to download other apps. The prompt cannot be dismissed and it shows up continuously on the mobile screen.
- In the background, it downloads and installs several other malicious apps.
- Records device information and sends it to a remote server.

7. Android.Downloader.D

Damage Level: MEDIUM

Category: Potential Unwanted Application

Method of Propagation: Google Play Store and third-party app stores

Behavior:

- It masks itself as a gaming app.
- Sends information about the infected device to a remote server.
- Automatically or on-click downloads other PUAs or adware.
- Installs additional malicious apps.

8. Android.Paccy.B

Damage Level: MEDIUM

Category: Potentially Unwanted Application

Method of Propagation: Third-party app stores

Behavior:

- APKs from this category use protector, which is commonly used by Android application developers to prevent their apps from being tampered or decompiled.

- This technique makes it difficult to run reverse engineering on this malicious app as malware authors use this to stay undetected. Hence, Quick Heal detects Android apps that use this packer under the Potentially Unwanted Application category as a precautionary measure.
- Once installed, the app unpacks itself and then loads a decrypted DEX file.
- The decrypted DEX file may behave maliciously like a Trojan Dropper, Trojan SMS, etc.

9. Android.Bruad.A

Damage Level: MEDIUM

Category: Potentially Unwanted Application

Method of Propagation: Third-party app stores

Behavior:

- Tries to gather information regarding system level application packages.
- Keeps a watch on device activities like changing of Wi-Fi status or battery level notifications.
- Sends system-related information to a remote server.

10. Android.Wtaspin.A

Damage Level: HIGH

Category: Trojan

Method of Propagation: Third-party app stores

Behavior:

- Targets popular instant messaging apps such as WhatsApp.
- If installed, it seems to work just like WhatsApp; asks for a phone number for verification and sends a one-time password (OTP) to the device.
- Once the verification is complete, it displays a message which says that the version has expired on a date which is prior to the device date. (E.g. if the device date is 27-9-2016, the expiry date will be displayed as 26-09-2016).
- It then asks the user to click on a link ‘http://ab&^*sad*m.net/4plus’ which downloads the infected app.
- It also installs the app in the background from the link http://giovan&*^%rlingen.nl named as WhatsApp+V(pink,beta,d,test).apk.
- The downloaded app will simply infect the device or may steal user data.

MOBILE RANSOMWARE AND BANKING TROJANS

Below are the detection statistics of mobile ransomware and mobile banking Trojan in Q3 2016.

Mobile ransomware growth (Q3 2016)

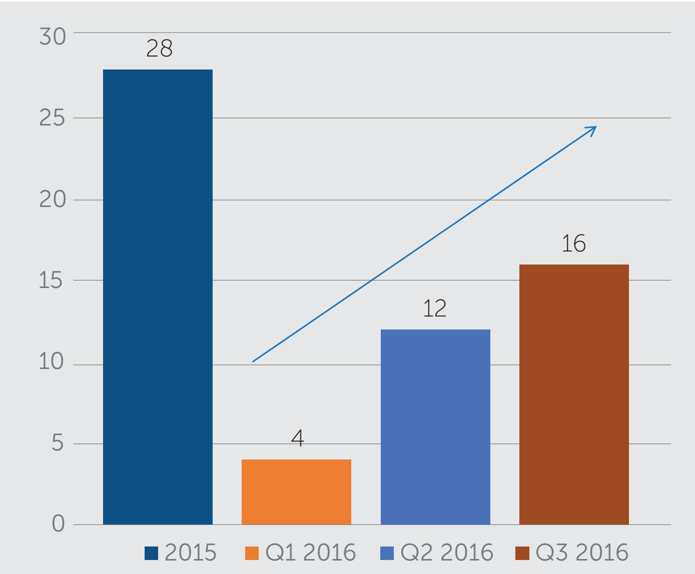


Fig 4

Mobile banking Trojan growth (Q3 2016)

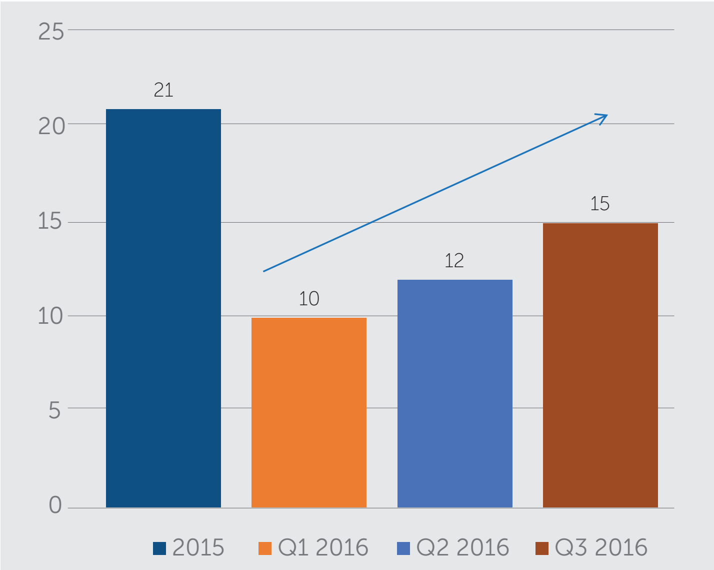
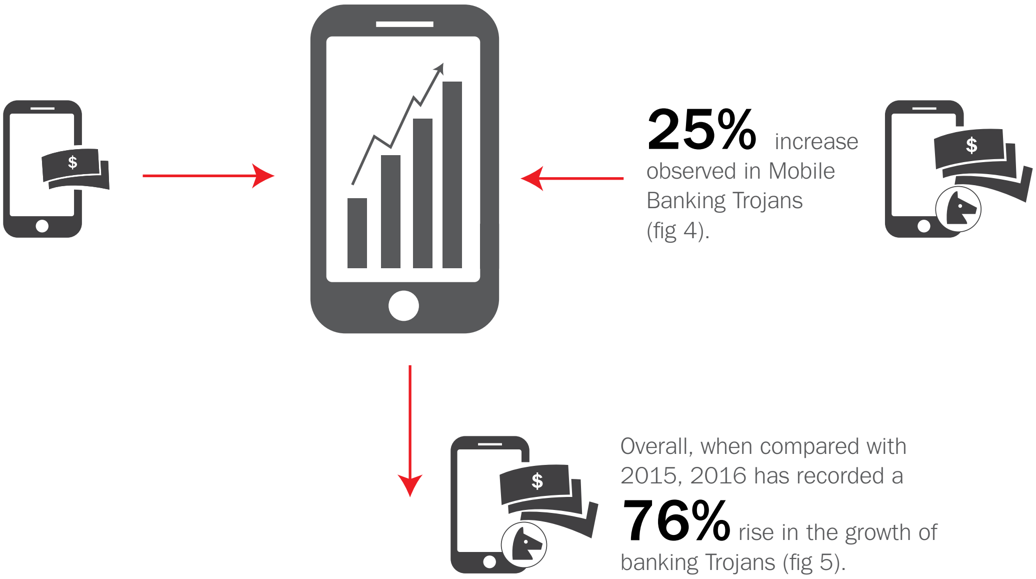


Fig 5

Observations in Q3 vs Q2:



Mobile Ransomware is up by **33%** (fig 4).

25% increase observed in Mobile Banking Trojans (fig 4).

Overall, when compared with 2015, 2016 has recorded a **76%** rise in the growth of banking Trojans (fig 5).

MALWARE USING UNIQUE TECHNIQUES

Android.Agent.VX

Damage Level: HIGH

Category: Trojan

Method of Propagation: Downloaded automatically via the Google AdSense advertising network.

How is this malware unique?

1. The Trojan is downloaded via the Google AdSense advertising network. Many genuine sites use this network to display ads.
2. It is downloaded when a webpage with the targeted ad is visited by the user.
3. Steals credit/debit card details.
4. Intercepts as well as modifies text messages which can be used to compromise secondary authentication via SMS.
5. Checks if an antivirus app is already installed on the infected device and tries to stop it.

Android.Rittew.A

Damage Level: HIGH

Category: Trojan

Method of Propagation: Third-party app stores or download links in SMSs

Behavior: Downloaded automatically via the Google AdSense advertising network.

How is this malware unique?

1. It is linked to a Twitter account that acts as an Android botnet.
2. Once launched, it hides its icon and starts running in the background as a service.
3. It contacts a particular Twitter account after regular intervals to receive commands. Based on these commands, it can download other malicious apps.
4. To prevent detection, the Android botnet uses encrypted messaging communication.
5. The malware can also change the Twitter account dynamically so that it starts receiving commands from a new account.

Android.Spynote.A

Damage Level: HIGH

Category: Trojan

Method of Propagation: Third-party app stores or download links in SMSs

How is this malware unique?

1. It's a new Android RAT (Remote Administration Tool) with a wide range of spying capabilities.
2. It can allow the attacker to gain complete control over the infected device.
3. Some of the capabilities of this RAT include:
   - » Copies files from the infected device to a computer.
   - » Accesses all SMSs, contacts, call logs, etc.
   - » Makes calls, records calls, records live audio from mic, and clicks pictures or shoots videos using the device's camera.
   - » Gets GPS location of the device.
   - » Checks installed apps on the device and uninstalls any chosen app.
   - » Accesses all files stored on the device.

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 shows how security vulnerabilities in the Android platform have been growing at a significant rate.

Security vulnerabilities discovered in 2016 (Q1, Q2, Q3) vs 2015

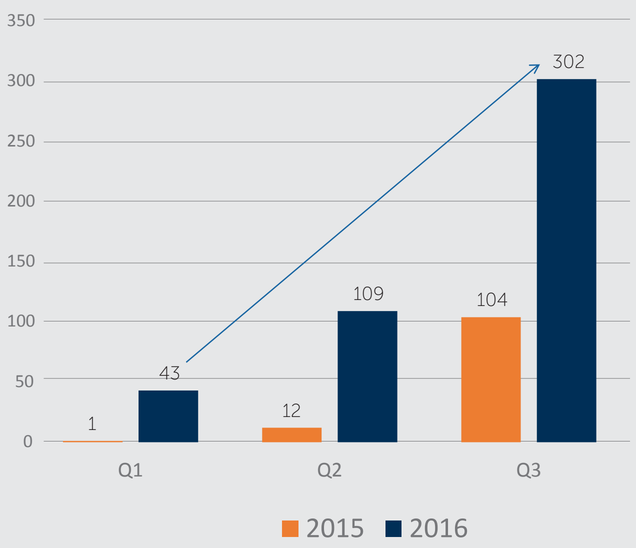


Fig 6

Source: https://www.cvedetails.com

Vulnerabilities categorization as per type in Q3 2016

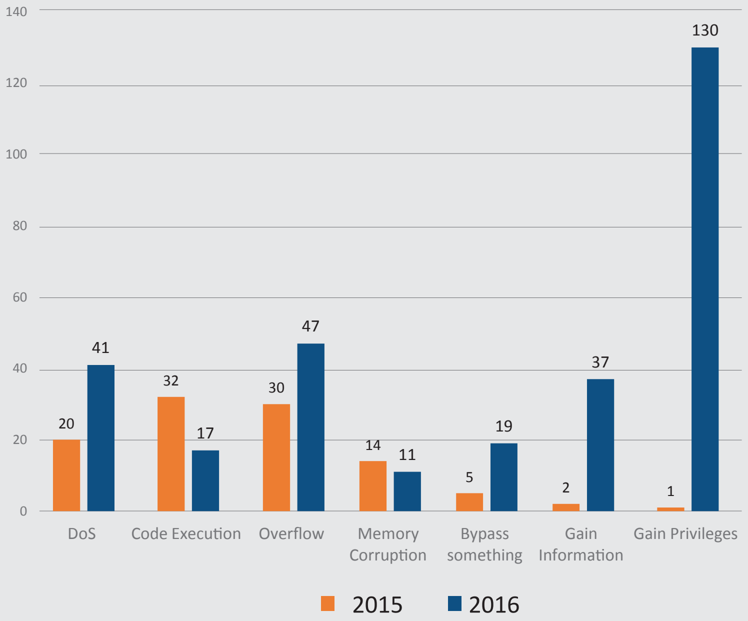
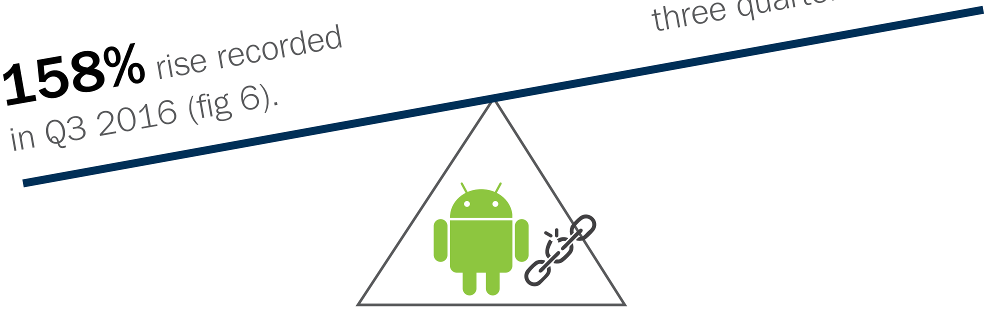


Fig 7

Source: https://www.cvedetails.com

Observations in Q3 vs Q2:

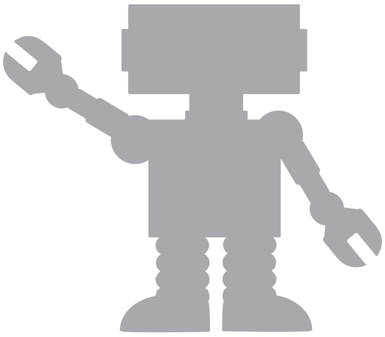


158% rise recorded in Q3 2016 (fig 6).

Compared with all the three quarters of 2015 (fig 6).

SECURITY VULNERABILITIES on ANDROID OS

TRENDS AND PREDICTIONS



1

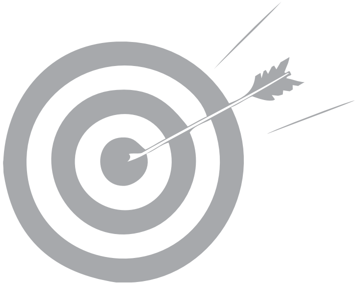
Rise in Android vulnerabilities heralds more attacks

Given the explosive rate at which security vulnerabilities are being detected on Android devices, attackers are going to ramp up their attacks on Android users. Moreover, as smartphones have started replacing desktops and laptops as portable data banks, hackers have all the more reasons to go behind them as easy targets.

2

Payment system & banking malware threats are going to rise

The Q1 threat report predicted a rise in the detection of banking malware and so it has, as seen in the statistics shown previously. While banks embrace the mobile domain to simplify banking for their customers, this is paving a risky track where cybercriminals will lie in wait to ambush those who are not careful enough about their digital security.



CONCLUSION

As long as we are connected to the Internet, we will be surrounded by attackers. But, one particular threat which constantly has us in its cross hairs is clearly the ransomware. As observed from the Q3 2016 report, this data hijacking malware has become the most dreaded nuisance for individual users and businesses alike. Reportedly, 93% of phishing emails now deliver ransomware and this only cements the fact that attackers are aggressively hunting for user data and the money it generates. While digital security is a pressing matter for all of us, we are not completely helpless; we do have a silver lining. Being aware of how and where our data is being used and how it is being protected, coupled with following a few basic security measures can make a significant difference. A few examples include being prudent about what information you share on the Internet, being careful about what software you download and what websites you visit, and most importantly, what security tools you invest in to keep your computer, mobile devices, and data safe against unknown or unexpected cyberattacks.