


Quick Heal

Security Simplified

SECURITE



Quick Heal Quarterly Threat Report | Q3 2017

www.quickheal.com

Contents

Contributors:

Anand Singh
Gajanan Khond
Pramod Shinde
Rohit Bhange
Rupali Parate
Sandip Borse
Sanket Temgire
Varsha Thangan

Anita Ladkat
Dipali Zure
Pawan Chaudhari
Pradeep Kulkarni
Pranali More
Prashant Tilekar
Prashil Moon

Introduction	01
About Quick Heal	01
About Quick Heal Security Labs	01
Quick Heal Detection	02
Windows Malware Detection Statistics	03
Top 10 Windows Malware	03
Malware Category-wise Detection Statistics	07
Top 10 Potentially Unwanted Applications and Adware	07
Top 10 Windows Exploits	08
Major Windows Malware of the Quarter	10
Trends and Predictions	14
Android Samples and their Detection Statistics	15
Top 10 Android Malware	16
Android Ransomware and Android Banking Trojans	20
Android Malware Using Unique Techniques	21
Most Popular Android Malware in Q3 2017	22
Vulnerabilities and Android OS	23
Usage of APK Packers or Protectors	24
Mobile Payments are on the Rise but are they Safe?	24
Trends and Predictions	25
Blue Whale Challenge: Should Parents be Worried About this Game?	26
Conclusion	28

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

About Quick Heal Security Labs

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

Introduction

In Q3 2017, over 199 million malware samples were detected on the systems of Quick Heal users – the highest of these surfaced in July. Compared with Q2 2017, Q3's malware detection dropped 11%. This, however, should not be taken as a respite; ransomware have been incessantly targeting users across the world. Quick Heal Security Labs detected 9 new ransomware families in this quarter. The top malware of the quarter is the same browser modifier Trojan that topped the list from the last quarter. Methods of propagation used by these malware mostly include free software, removable and network drives, spam emails, and malicious websites. The Trojan family is still leading with the highest detection count followed by infectors, worms, and adware. Supply chain attacks were the notable targeted attacks in Q3 2017 – one of these involved a popular free system optimizer tool called CCleaner. Quick Heal Security Labs also shared its findings of Advanced Volatile Threats – a type of APT (Advanced Persistent Threat). Given the growth in digital payments, an important mention in the report was about the TrickBot Banking Malware that steals banking details.

The detection of Android samples in Q3 rose 40% in comparison with that in Q2. Third-party app stores continue to be the top source of malicious apps. Potentially Unwanted Applications (PUA) grew 238%. In Q3, Quick Heal Security Labs also observed a rise in the usage of APK packers or protectors by attackers to evade security analysis and detections. The report also includes two special mentions - the rising popularity of mobile payments and the Blue Whale Challenge.



Quick Heal Detection | Q3 2017

Malware

Per Day	Per Minute	Every 1 second
2,218,770	1,541	26

Ransomware

Per Day	Per Minute	Every 3 seconds
25,750	18	1

Exploit

Per Day	Per Minute	Every 4 seconds
21,268	15	1

PUA and Adware

Per Day	Per Minute	Every 2 seconds
1,31,094	91	3



Windows Malware

Windows Malware Detection Statistics

In Q3 2017, we detected over 199 million malware samples on our users' machines.

Windows malware detection

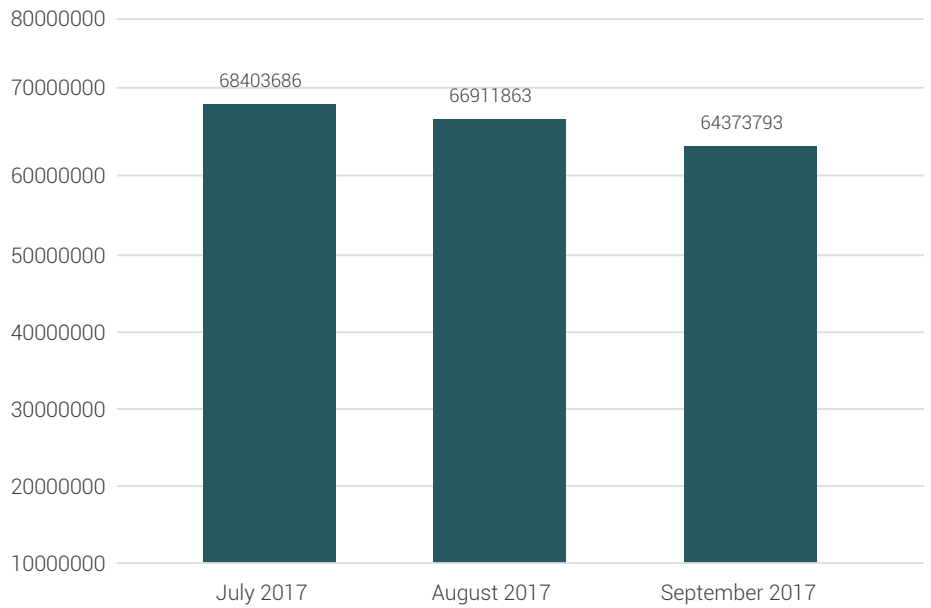


Fig 1

Compared with Q2 2017, Q3 2017 registered a drop of 11% in the detection count of Windows malware samples.

Top 10 Windows Malware

These are the top 10 Windows malware detected by Quick Heal in Q3 2017.

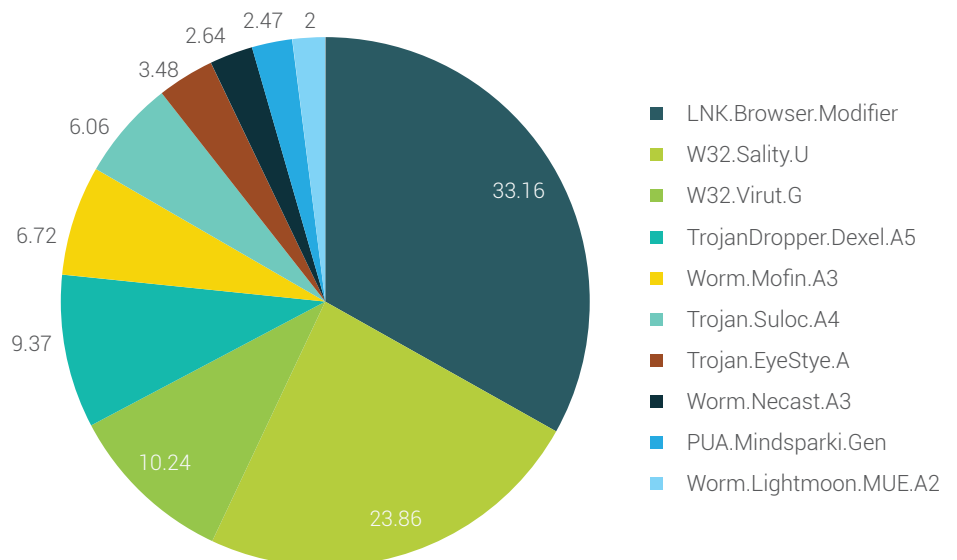


Fig 2

Top 10 Windows Malware

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.Sality. U

Threat Level: Medium

Category: Polymorphic file infector

Method of Propagation: Removable or network drives

Behavior:

- Injects its code into all running system processes. It then spreads further by infecting the executable files on local, removable, and remote shared drives.
- Tries to terminate security applications and deletes all files related to any security software installed on the system.
- Steals confidential information from the infected system.

3. 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.

4. TrojanDropper.Dexel.A5

Threat Level: High

Category: Trojan

Method of Propagation: Email attachments and malicious websites

**Behavior:**

- Allows entry of other malware into the infected system.
- Changes registry and browser settings. Automatically redirects the user to malicious websites where more Trojan malware are dropped on the system.
- Steals confidential data from the infected system.
- Slows down system performance by consuming more resources.

5. 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.

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. 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.

8. Worm.Necast.A3

Threat Level: Medium

Category: Worm

Method of Propagation: Spam emails and malicious websites

Behavior:

- Infects a computer via spam emails or when a user visits a website that is loaded with exploits.
- 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.
- 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 attackers misuse the infected system's vulnerabilities to access the compromised machine without the user's knowledge and consent.

9. PUA.Mindsparki.Gen

Threat Level: Medium

Category: Potentially Unwanted Application

Method of Propagation: Bundled software and malicious websites

Behavior:

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

10. Worm.Lightmoon.MUE.A2

Threat Level: Low

Category: Worm

Method of Propagation: Spam emails and P2P (Peer to Peer) sharing applications.

Behavior:

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

Hoaxes use weaknesses in human behavior to ensure they are replicated and distributed. In other words, hoaxes prey on the Human Operating System.

– Stewart Kirkpatrick

Malware Category-wise Detection Statistics

The below graph represents the statistics of the categories of Windows malware that were detected by Quick Heal in Q3 2017.

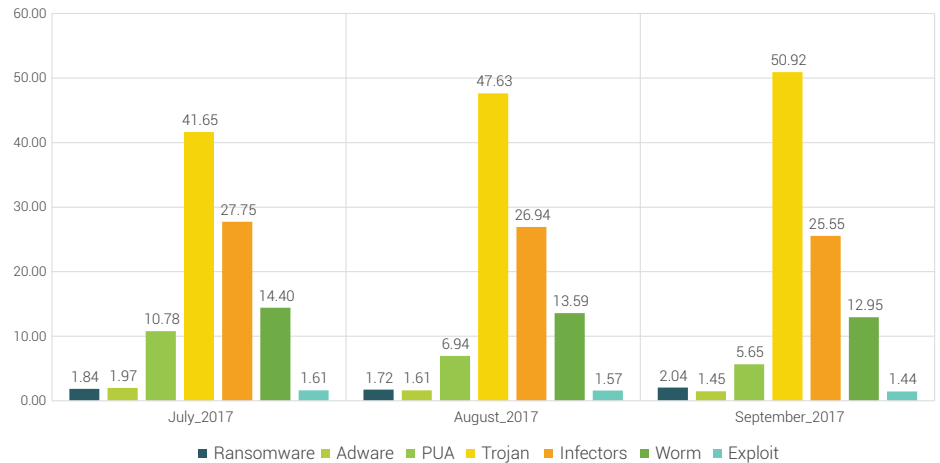


Fig 3

Top 10 Potentially Unwanted Applications (PUA) and Adware

These are the top 10 PUAs and Adware samples detected by Quick Heal in Q3 2017.

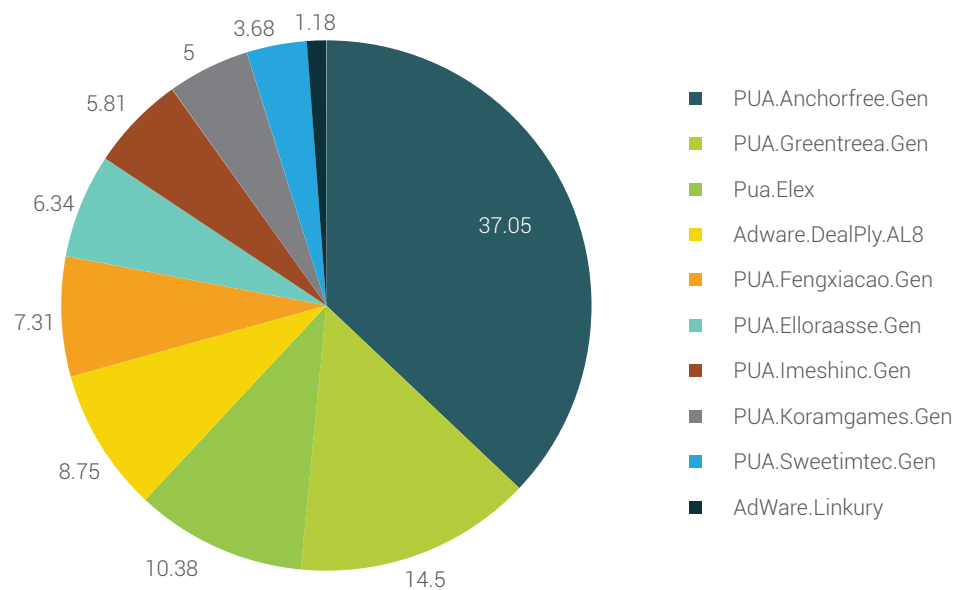
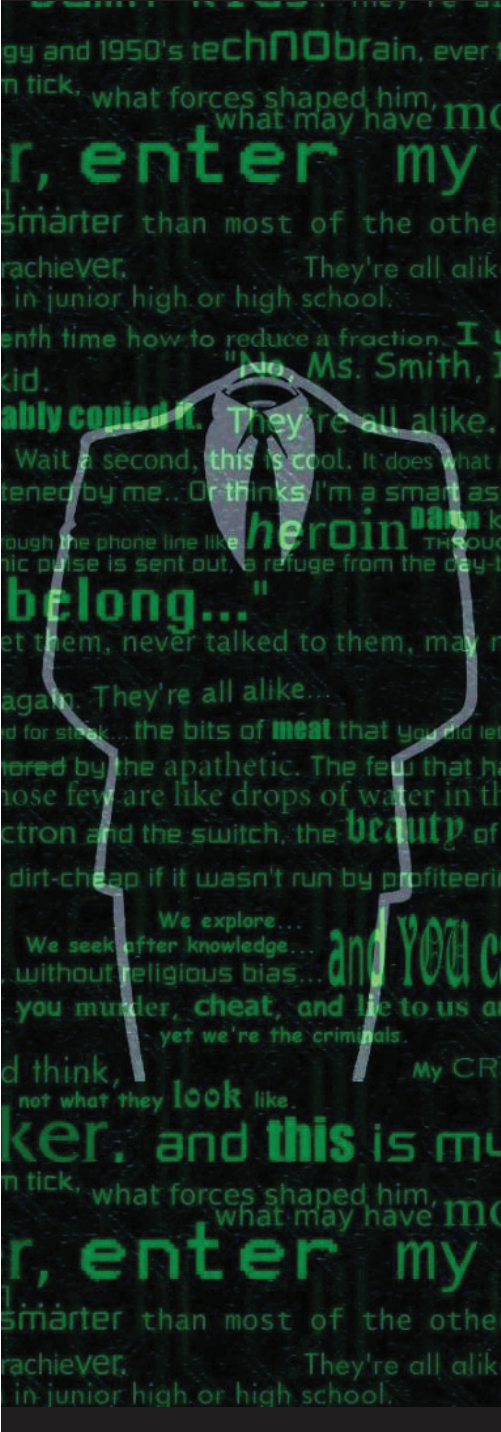


Fig 4

Detections in descending order (average):
Trojan: 46.73% | Infector: 26.74%
Worm: 13.64% | Adware & PUA: 9.46%

- 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.



Host-based exploits are those that target security vulnerabilities found in hosts (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.

Newly observed Adware and PUAs in Q3 2017

Adware.DealPly.AL8

This family of adware was observed installing add-ons for web browsers, creating browser extensions, and displaying advertisements in the affected browser.

Adware.Linkury

This family of adware gets installed along with free software bundled with installers for browser hijackers. As a result, the user observes pop-up advertisements on every site they visit.

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 Q3 2017.

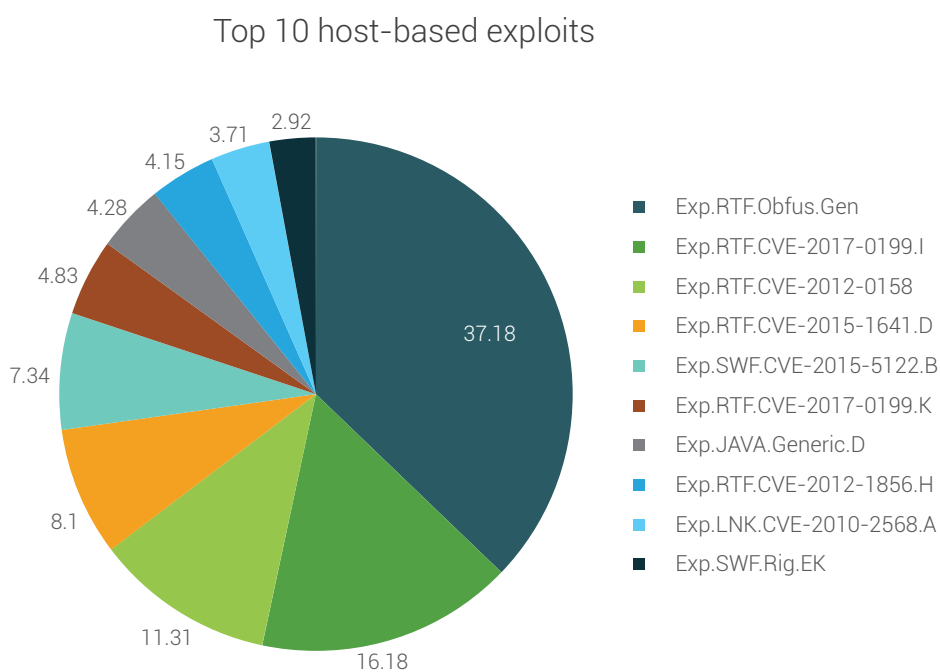


Fig 5

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

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

Top 10 network-based exploits

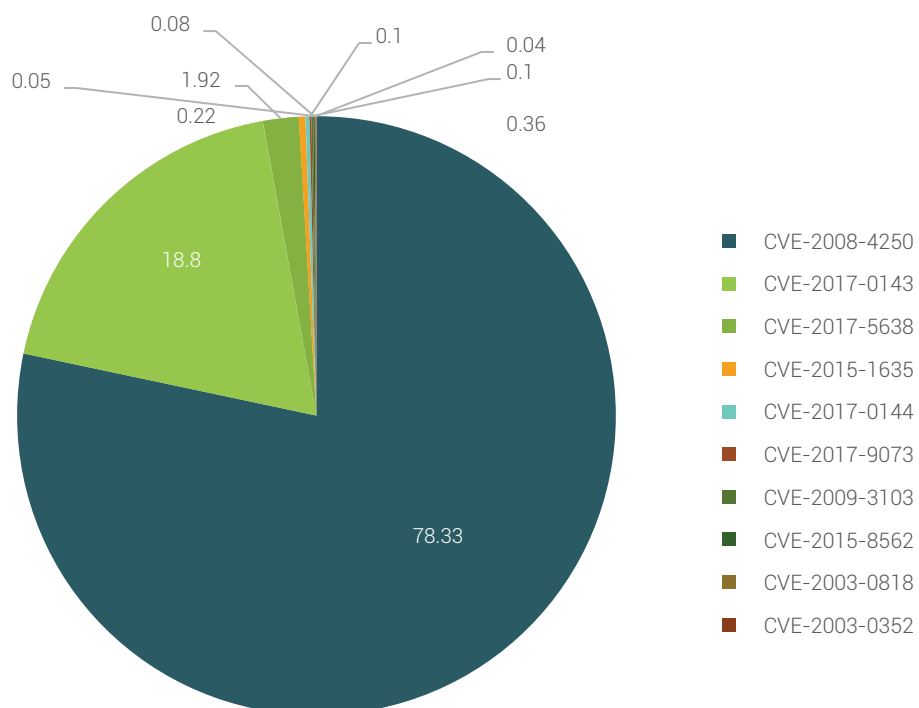
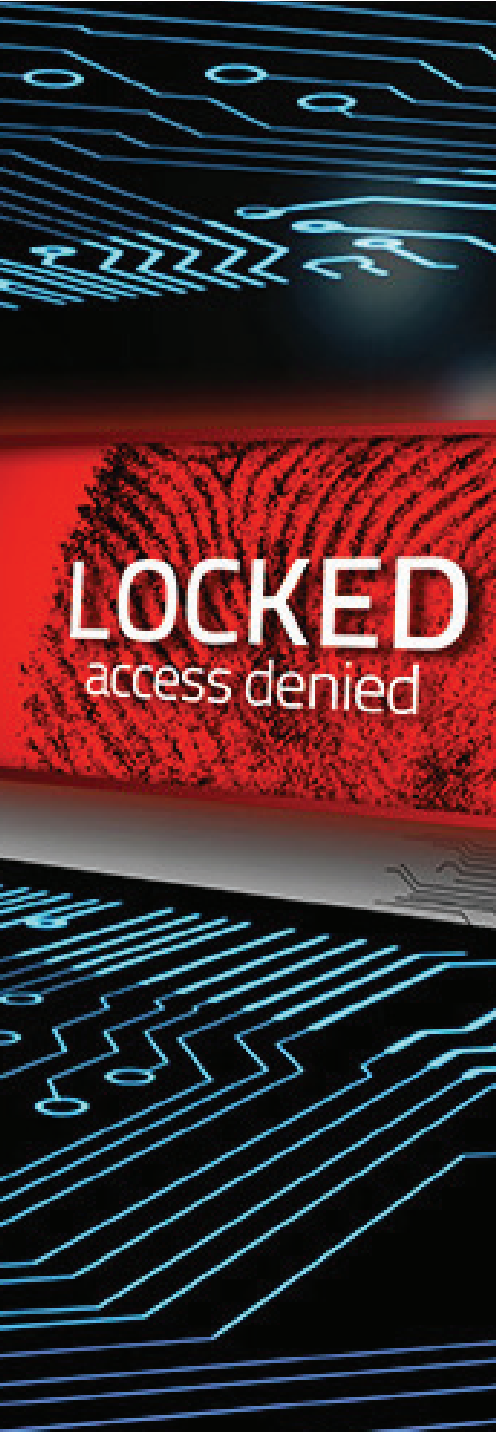


Fig 6



Major Windows Malware of the Quarter

Ransomware

- In the Q3 2017, new variants of Cryptomix ransomware were on the rise. They spread rampantly through malicious spam (malspam) emails and exploit kits. Over the past three months, we have been observing an increase in the Globeimposter ransomware variants appending different suffixes to files it encrypts. Previously this ransomware was spreading through RDP (Remote Desktop) connection only, but now it has started using malspam campaigns as well.
- A new variant of Petya ransomware was observed which created havoc all over Europe as well as major parts of Asia including India. The major target for Petya was Ukraine – its major banks and power services. This new version of Petya not only encrypts data files but it also encrypts master file table (MFT) & overwrites the Master boot record (MBR) because of which the infected system fails to boot. This is a wiper kind of a ransomware in which once a system's MBR is infected, data recovery is not possible.
- Arena and Aleta are the new BTCWare ransomware variants observed in Q3 2017. These variants use RDP brute-force attacks to gain access to the infected system.
- The new variants of Locky ransomware has been recently observed that appends ".Lukitus", ".diablo6" and ".ykcol" suffixes to the files it encrypts.

Other ransomware observed in Q3 2017:

- | | |
|---------------|----------------|
| • Karo | • Philadelphia |
| • NemucodAES | • Gryphon |
| • Reypson | • SyncCrypt |
| • Viro | • Princess |
| • Oops Locker | |

Targeted Attacks

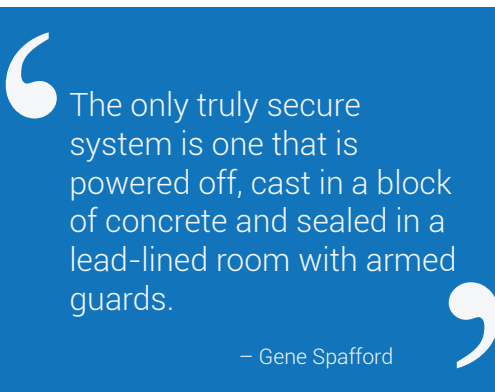
These are well-planned, systematic campaigns where attackers work with a motive to keep their presence hidden while stealing as much data as possible from the victim. A targeted attack usually goes undetected for months and sometimes even for years. Malicious emails, compromised websites, and exploits are some common channels used to carry out these attacks. In Q3 2017, attacks by compromising supply chain infrastructure were observed as a new trend in attacking specific users.

- A legitimate MEDoc updater process was compromised to spread destructive Petya (exPetya) MBR modifier ransomware. M.E.Doc is a Ukraine-based tax accounting software firm that develops software related to accounting, taxes, etc. Hackers breached and compromised the company's update server systems.
- Another supply chain incident was discovered in which a popular free system optimizer tool called CCleaner (version 5.33.6162) was compromised and malware was injected into it. This attack targeted many technology and telecommunication organizations. It has affected over 2.27 M users worldwide.
- One hospital chain in Israel was targeted by attackers with the Retadup malware. This malware is known for its stealthy behavior - it collects system related information. Its worm-like characteristic makes it more powerful. Downloading malicious files, key-logging activity, and C&C communication with its servers are some of the routine activities carried out by Retadup. The malware was also found to be targeting certain South American agencies.

Advanced Volatile Threats (AVT)

Advance Volatile Threats are advanced persistent threats that do not need to reside in an infected system's hard disk and are designed to work in memory. Fileless malware, also identified as memory-resident and RAM-based malware, are part of one such malware family that resides only in the system's memory. As there is no file-based existence of AVTs, these malware can evade security products for as long as possible. Apart from being resident in RAM, these threats use Window's built-in tools such as Power Shell to run malicious scripts without the user's knowledge.

One such malware attack was widely observed during Q3 2017 that led to a click-fraud campaign. The malware was found to be residing in the system's registry having a shell code to run a malicious script using Power Shell command. The existence of the malware came into notice when a malicious link was visited continuously by the infected system. For more details, please refer to <http://blogs.quickheal.com/analysis-fileless-malware-quick-heal-security-labs/>





Spam Emails - primary malware distribution method

Malspam email (malicious spam email) campaigns grew rapidly in Q3 2017. Attackers used different techniques to spread ransomware and banking malware. This is the most preferred method used by attackers to launch malware campaign in order to target a large number of victims. Malspam emails having archive files as attachments contain malicious script files or word document files which are responsible for delivering the actual malicious payload.

TrickBot Banking Malware

The TrickBot Banking malware spreads through malspam with polymorphic propagation methods. TrickBot is involved in stealing banking details (personal sensitive information and authentication codes).

TrickBot comes through VBS, WSF, PDF, and OLE file types in attachment and has a functionality to download the next stage payload from compromise websites.

Below are some of subject lines and names of attachments used in these campaigns:

File type	Email subject line	Attachment name
VBS	blank subject line	doc<10_digits>.zip
WSF	Voice Message Attached from <11_digits> – name unavailable	<11_digits>_<07_digits>_<06_digits>.zip
PDF	Emailing: <8_digits>	<8_digits>.PDF
OLE	Account secure documents	PaymentAdvice.doc

Globelmposter Ransomware

In the Globelmposter ransomware malspam campaign, the email attachments used script files which are heavily obfuscated containing multiple URLs to download payload through Windows Script Host (WSH) or Power Shell to evade detection

Blank Slate Malspam Campaign

In this campaign, attackers used emails leaving with a blank email body and a subject line which is blank or which is unclear. Also, the sender's email ID is spoofed. Because of the blank message, victims are tricked into opening the malicious attachments out of curiosity.

NemucodAES Ransomware

This is a new malicious spam variant that is spreading via an email claiming to be from the United Parcel Services (UPS) carriages. The email carries a zip attachment that contains NemucodAES Ransomware and the file-less Kovter Trojan. Attached zip archives contain a JavaScript file that will first download a DOC file and then download the actual ransomware component PHP script and DLL file. Kovter is a file-less malware which is different from other Trojan families. It hides in the registry which is difficult to scan or detect. It uses a conventional malware file to add the entries with its malicious code in the registry and ensures it is loaded into memory when the infected computer boots. It makes use of Windows' genuine utility PowerShell for its malicious operations. Kovter gathers user data and sends it to its Command & Control server (CnC). This is used for click-fraud campaigns where a computer or a person is maliciously used to click on ads to generate revenue.

Below are some subject lines and names of attachments used by one of these campaigns.

Email subject Line	Attachment name
Problems with item delivery n.004640147	UPS-Package-004640147.zip
Problems with item delivery n.001656569	UPS-Label-001656569.zip
Parcel ID004692898 delivery problems please review	UPS-Receipt-004692898.zip
We could not deliver your parcel #004522553	UPS-Delivery-004522553.zip
Our UPS courier cannot contact you (parcel #008284689)	UPS-Parcel-ID-008284689.zip
Notification status of your delivery (UPS 5952930)	UPS-Delivery-Details-5952930.zip
Notification status of your delivery (UPS 001387092)	UPS-Package-001387092.zip

“If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.”

– Richard Clarke



Trends and Predictions

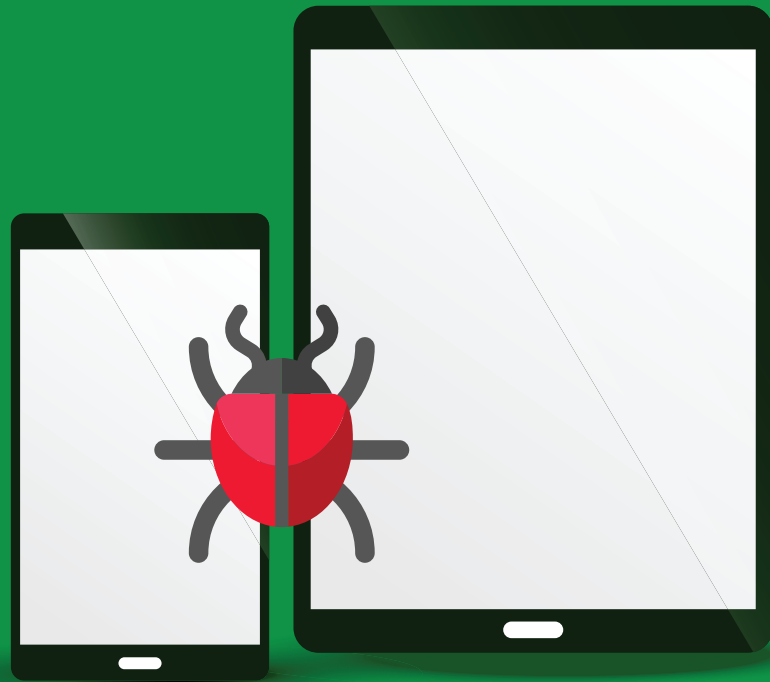
Ransomware

- » Newer and advanced variants of the Locky ransomware family are expected to rise.
- » Ransomware-as-a-Service type attacks may increase due to its user-friendliness and high return on investment (ROI).
- » Cryptomix and Cerber ransomware are expected to hit its targets with new variants and sophisticated propagation techniques.

Targeted Attacks

- » Email attachments will be used largely to deliver malware to targeted users. These emails might use new file types for their attachments to avoid detections by security software.
- » We are observing more malware to be using Advanced Volatile Threats (AVTs) techniques for resilience. File-less malware are expected to add sophistication in their upcoming attacks.





Android Malware

Android Samples and their Detection Statistics

In Q3 2017, we received over 2 million Android samples.

Android samples are APK files (exhibiting malicious or suspicious behavior) received by Quick Heal Security Labs from multiple sources.

Compared with Q2 2017, Q3 2017 registered an increase of 40% in Android samples (fig 2).

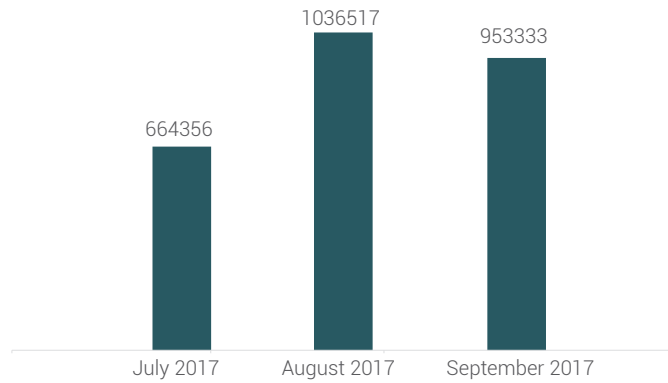


Fig 1

Android samples received at Quick Heal
(Q2 2017 vs Q3 2017)

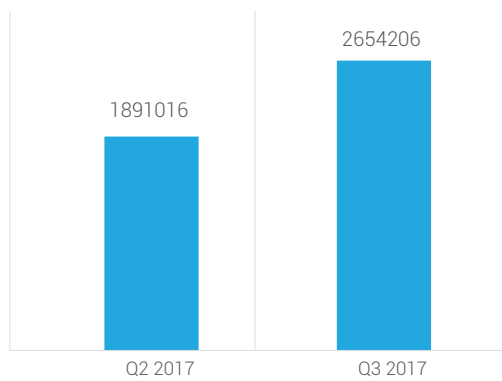


Fig 2

Category detection
(Q2 2017 vs Q3 2017)

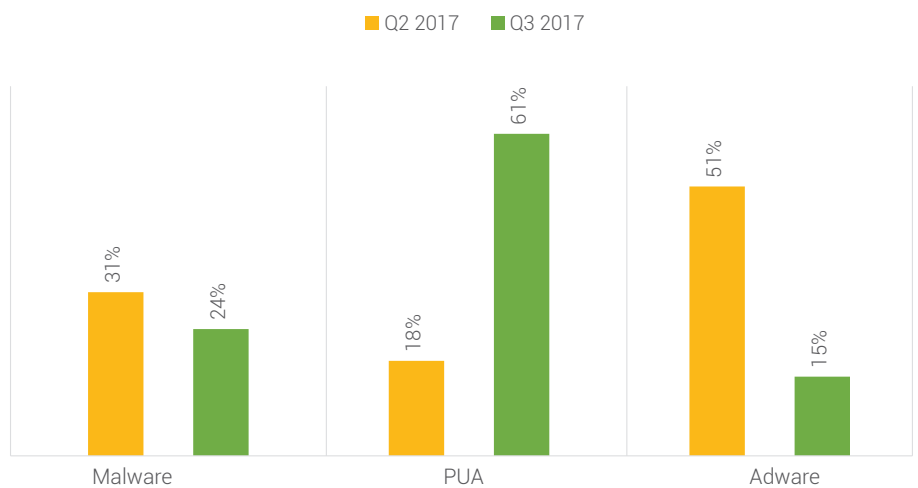


Fig 3

An increase of 238% noticed in the growth of the PUA family (Potential Unwanted Programs) (fig 3).



Top 10 Android Malware

These are the top 10 Android malware detected by Quick Heal in Q3 2017.

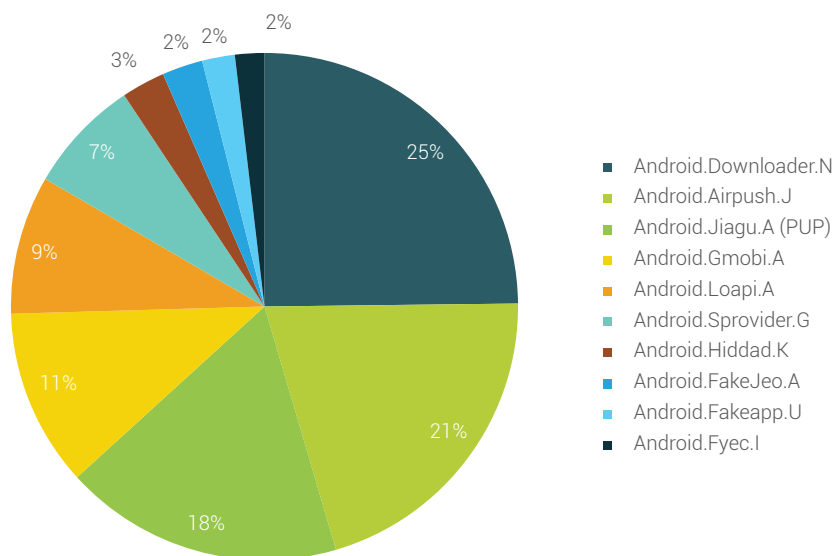


Fig 4

1. 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.

2. Android.Airpush.J

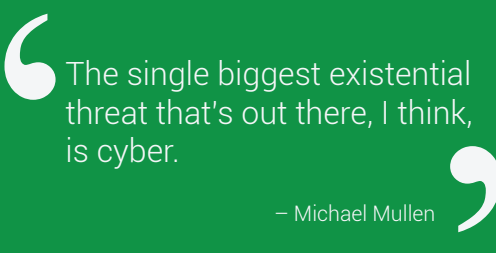
Threat Level: Low

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.



“The single biggest existential threat that’s out there, I think, is cyber.”

– Michael Mullen

3. 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.
- Releases the data into memory and decrypts it while runtime.
- Decrypted DEX file may be a malicious or a clean file.

4. 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.

5. Android.Loapi.A

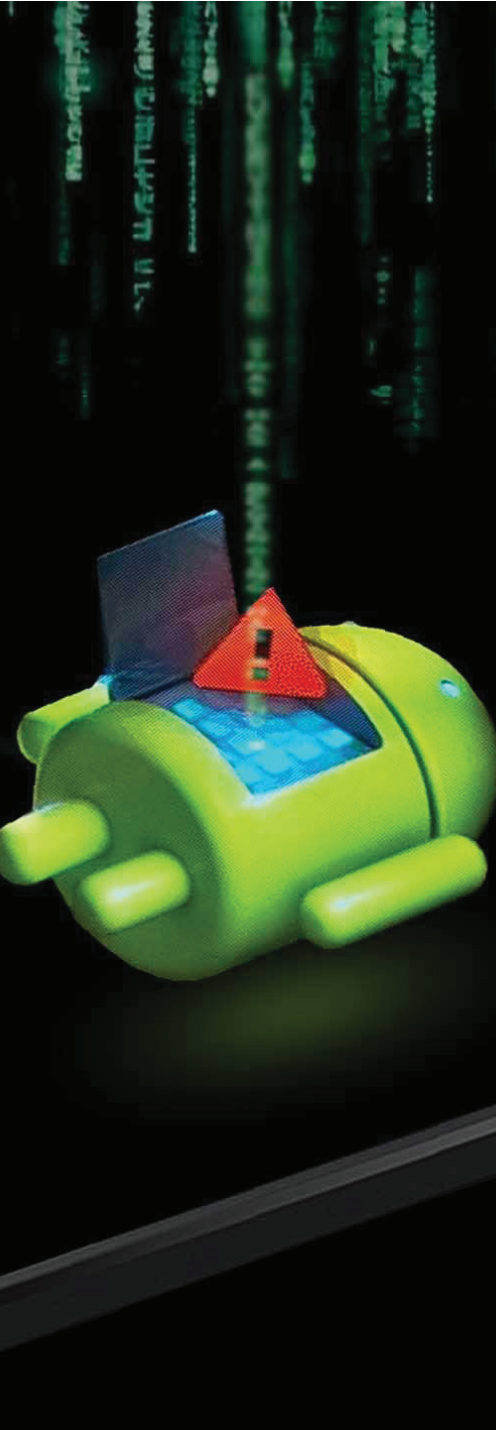
Threat Level: High

Category: Malware

Method of Propagation: Third-party stores

Behavior:

- It's a fake antivirus for Android.
- Carries another malicious file in an encrypted format, decrypts it at runtime and drops it on the infected phone.
- Gains device admin rights which makes it difficult for novice users to uninstall the app.
- In the background, it checks if any antivirus app is installed on the infected device by checking it against its saved list of antivirus app names; it then changes its behavior accordingly.



6. Android.Sprovider.G

Threat Level: Medium

Category: Adware

Method of Propagation: Third-party app stores

Behavior:

- It downloads the apk files from malicious URLs when the user opens the app.
- Once downloaded, the user is prompted to install the app.
- Once installed, it hides the app icon after first-run.
- Displays unnecessary ads quite frequently.

7. Android.Hiddad.K

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- The app has a transparent icon and has no name to it.
- After clicking on the app, it asks for activation of Device Administrator rights. If the user selects 'cancel', it displays the same activity repeatedly until the user selects the 'activate' button.
- After Device Administrator activation, the app hides itself and runs silently in the background.
- Connects to a URL and download unwanted adware apps which may cause battery drainage, unnecessary data usage or steal personal data.

8. Android.FakeJeo.A

Threat Level: Low

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- Malware authors created this fake Jeo app to generate revenue from Ads.
- Tricks user into sharing its download link to 10 contacts on WhatsApp to access actual offer which is never there in the first place.

9. Android.Fakeapp.U

Threat Level: Low

Category: Potentially Unwanted Application (PUA).

Method of Propagation: Third-party app stores

Quick Heal Mobile Security Apps were the first to detect fake Jeo apps under the Android.FakeJeo family and report them to Google, post which these apps were removed from the Play Store. For more information, click [here](http://blogs.quickheal.com/beware-fake-apps-uses-jiojeo-names/) - <http://blogs.quickheal.com/beware-fake-apps-uses-jiojeo-names/>

Behavior:

- This app is created using a genuine tool. It might look genuine but when opened, may redirect the user to some malicious URLs.
- Its only task is to load the malicious URL & increase the website's visit.

10. Android.Fyec.I

Threat Level: Low

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- Uses icons of genuine apps after installation on a user's device.
- Collects & sends device information such as IMEI, IMSI, model, OS, etc.
- Intercepts SMS, shows overlay screen, shows ads, decrypts additional executables, downloads & runs payload which can be malicious.



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 release the data or the phone.

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 Q3 2017.

Android Ransomware
(Q1, Q2 & Q3 2017)

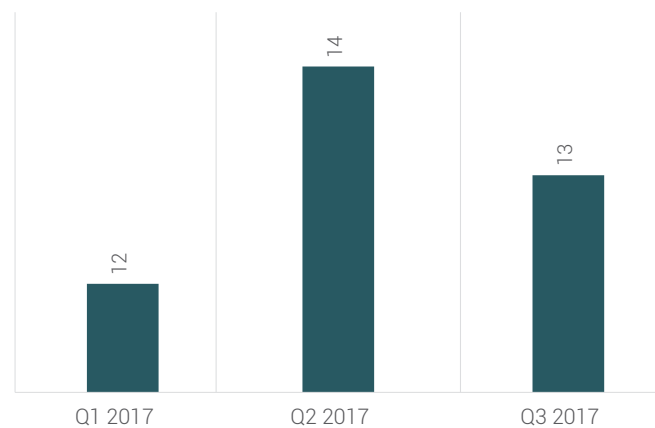


Fig 5

Android Banking Trojan
(Q1, Q2 & Q3 2017)

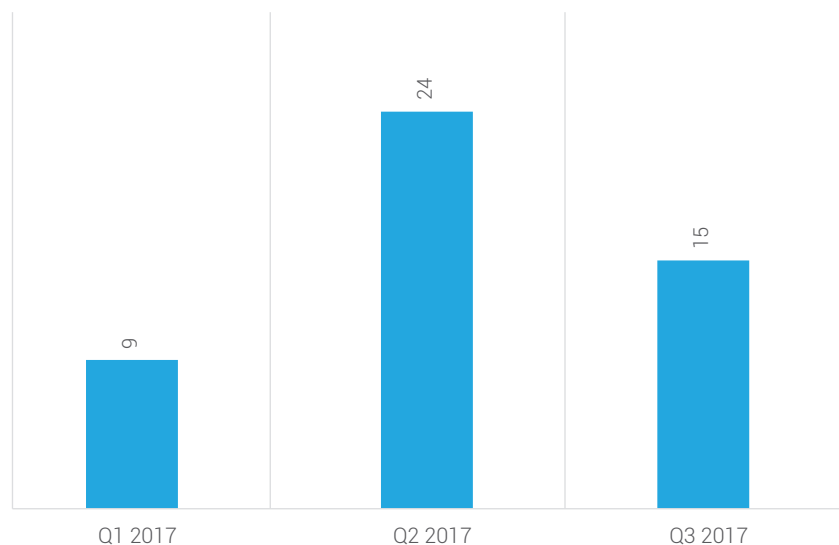


Fig 6

Android Malware Using Unique Techniques

1. **Android.Xafekopy.B**

- This application acts as a battery optimizer but after installation it loads a malicious library.
- This library decrypts and loads a malicious JS file present in Assets, and disable the user's Wi-Fi so that it can start mobile network for WAP billing.
- It checks for the user's MCCMNC code (Mobile Country Code and Mobile Network Code). Using this, the attacker can identify the country and mobile operator of the infected user. The JS file starts the WAP billing activity after bypassing captcha and steals money from the user's mobile accounts.

“We won't sit idly by when a crime is committed in the real world. So why should we when it happens in cyber space?”

— Max Baucus



Most Popular Android Malware in Q3 2017

1. **Android.Kasandra.B**

- Targets social networking apps.
- After installation, if user clicks on its icon it hides itself.
- Mainly targets rooted devices.
- After getting super-user privileges, it tries to get all data related to social networking apps like Instagram, WhatsApp, etc.

2. **Android.Locker.A**

- Was found on Google Play Store.
- Looks harmless but once started, it executes its malicious activity and locks the home screen.
- Loads a malicious file from a remote server and steals the victim's private data such as emails, Chrome history, contacts, call logs and messages.
- The stolen data is randomly displayed to the victim on a web page.

3. **Android.FakeApp.GEN18393**

- Was found on Google Play Store.
- Once installed, it hides its icon and sends user information to its C&C server.
- Silently records audio, takes photos with the camera, makes outbound calls, sends text messages to specified numbers, and accesses call logs, contacts, etc.
- Can respond to over 73 different remote commands so that attackers can manipulate a victim's device through a 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 from Q1 2017 to Q3 2017.

Security vulnerabilities
Q3 2017 vs Q1 & Q2 2017

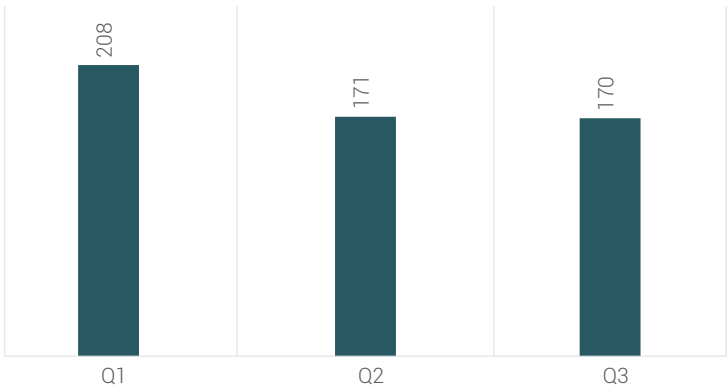


Fig 7

Security vulnerabilities discovered
(Q3 2017 vs Q1 & Q2 2017)

■ Q1 2017 ■ Q2 2017 ■ Q3 2017

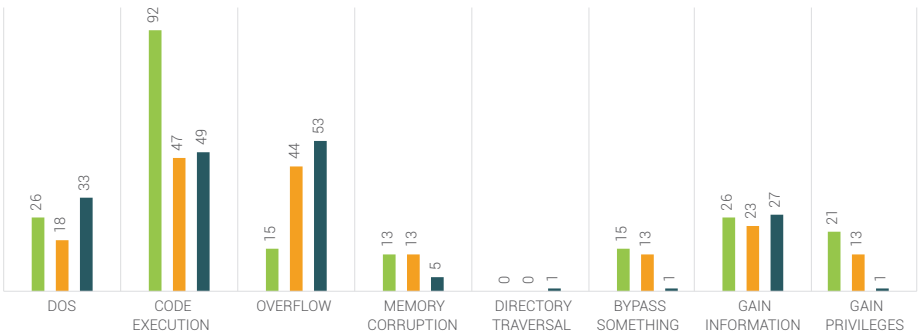


Fig 8

Source: cvedetails.com



Usage of APK Packers or Protectors

Quick Heal Security Labs is observing a rise in the usage of APK packers or protectors to evade analysis and detections. Below is the list of prominent Android malware families using such packers or protector in Q3 2017

- Android.Jiagu.A [detected as one of the Top 10 detected PUA in Q2 and Q3 2017]
- Android.Congur.Z
- Android.Dowgin.BL
- Android.KyView.D
- Android.Wapron.Q
- Android.Dropac.A

Mobile Payments are on the Rise but are they Safe?

Several non-banking institutions have entered the market offering payment services and this has only boosted the consumer's readiness to adopt digital payments. The following statistics easily paint the picture of the exponential growth of digital transactions in the country:

1. Cashless payments in October 2016 increased 22% when compared to October 2015.
2. Money transfers using mobile banking and IMPS (immediate payment system – money is transferred instantly using text messaging or online banking) showed the highest increase in over 12 months ending October 2016.
3. Mobile banking transactions grew 175%, while money transacted using mobile banking grew 369% from October to October, according to an IndiaSpend analysis of Reserve Bank of India (RBI) data.
4. IMPS transactions grew 116% while IMPS transfers grew 150% over 12 months ending October 2016.
5. According to a new study by Google and BCG (Boston Consulting Group), digital payments industry in India will grow 10 times to touch \$500 billion by 2020.
6. The Google-BCG report also identified that top three services for which Indian consumers prefer online payments to offline payments include online shopping, utility bill payments, and movie ticket purchases.



7. Indian consumers are 90% as likely to use digital payments for both online and offline transactions.
8. According to the Reserve Bank of India (RBI), the volume of mobile wallet transactions doubled during April 2015-February 2016 period to cross Rs.55 crore.

If the above statistics were to be summed up in one sentence, it would easily be "Digital Payment Industry is booming." The proliferation of mobile devices, mobile apps and operating system, has boosted innovation in the mobile ecosystem. And while innovation raises the bar for convenience, it brings along with it new risks, threats, and vulnerabilities - which, if not addressed, widen the mobile attack landscape. The wealth of information that is stored on and transmitted via mobile devices create unmeasured opportunities for attackers to target user data (personal, confidential, and sensitive information) regardless of the motive.

Sources:

<http://www.livemint.com/Industry/M6SPyd4vUcC7QlQRnjBqaO/Digital-payments-in-India-seen-touching-500-billion-by-2020.html>

http://www.business-standard.com/article/economy-policy/post-demonetisation-digital-payments-are-down-15-116122700098_1.html

<http://www.livemint.com/Politics/637uTLKanriP4PbFhhCznJ/Can-India-meet-the-target-of-2500-crore-digital-transaction.html>

<http://economictimes.indiatimes.com/industry/banking/finance/banking/digital-payments-indias-new-currency-debit-card-transactions-surge-to-over-1-billion/articleshow/58863652.cms>

Trends and Predictions

1. Android vulnerabilities

Malware authors can access a user's device to gain almost anything they want by misusing critical vulnerabilities that are unpatched. Hence, Android vulnerability becomes a major concern in the coming days.

Blueborm & DirtyCow are the best examples.

2. PUA on the rise

In earlier threat reports of Quick Heal in 2017, PUA has growing rampantly. It consistently rose from Q1 (41%) to Q2 (51%) to Q3 (61%)

We are expecting more malware threats will use PUA to target the Android community.



Blue Whale Challenge: Should Parents be Worried About this Game?

This is a special addition to the Quick Heal Quarterly Threat Report that aims to help our readers (especially parents) understand why they should be worried about the Blue Whale Challenge.

What is the Blue Whale Challenge?

It is supposedly an Internet game where players (mostly teenagers) are assigned 50 different tasks by the game admin (also known as a curator). A player has to complete all these tasks (comprise self-harm activities) within 50 days and can only win the game by committing suicide.

Read more about this in Quick Heal blog:

<http://blogs.quickheal.com/parents-5-things-must-know-blue-whale-challenge/>

Spread In India

According to Google Trends, India ranks no. 1 for the highest Blue Whale related searches worldwide. The below statistics are based on different keywords searched by users on Google.

- Kolkata is the top city in the world to search for 'blue whale challenge'
- The top 5 states searching for the keyword 'blue whale challenge' are Manipur, Nagaland, Meghalaya, Mizoram, and Arunachal Pradesh
- Jammu and Kashmir, Assam, and Tamil Nadu are the top three states to search for 'blue whale challenge game download'

Source: <https://trends.google.com/trends/explore?geo=IN&q=blue%20whale%20challenge>

The Blue Whale game is allegedly linked to over 100 suicides all over the country. As of Oct 2017, hearings have been held in India's Supreme Court to take a decision on a blanket ban on this game.

Should parents be worried about this game?

Although several cases of teen suicides in India have been linked to the Blue Whale Challenge, they have not been officially confirmed. These incidences are based on anecdotes from the deceased or affected person's family, friends, and acquaintances. But, officially proven or not, every parent must be definitely worried about this game and all those things that can nudge their kids into taking a step as drastic as committing suicide.

We must first understand that the Blue Whale Challenge is not a mobile app nor a website or a social media group until proven otherwise; it's a phenomenon. Which means, you cannot prevent the game from getting installed on your kid's phone nor can you block any specific websites. Theories suggest that the admins of this game find their potential targets (troubled teens) through the comment sections of shady websites, public forums, and so on.



What can parents do?

Getting more involved with your kids and understanding their daily challenges and inhibitions should be the first step towards defeating sinister elements such as the Blue Whale game. From the point of view of online security, here are a few things that parents can do:

- Teach your kids (right from a young age) not to share their personal information on the Internet. Follow this rule yourself.
- Let them know that they can talk to you about anything wrong they see or come across online.
- Help them understand that strangers in real life are no different from strangers on the Internet.
- Caution them against joining any groups that ask them to perform strange or undesirable tasks.
- Consider giving your children phones that they can use for just calling and texting. This way, you can limit their impressionable minds to the Internet. Dr. Harsh Shetty, child psychiatrist at LH Hiranandani Hospital, Mumbai, says "never give gadgets as gifts, and do not use gadgets as a means to calm a child or keep them busy".
- As an added measure of security, parents can consider installing a Parental Control software on their computers and the smartphones used by their kids. This software can help parents block access to websites that contain adult, violent, and anti-social content. Parents can also use the software to assign a fixed timetable to their kids to access the Internet. You may learn about how Quick Heal Parental Control tool works to keep children safe online; click here - <http://www.quickheal.com/parental-control>





Conclusion

Digital security is still an afterthought for many - getting a new mobile phone scratched is more worrisome than the risk of having it infected by a virus. While desktops and laptops do get the attention they need for their security, mobile phones still have a long way to go in this aspect. It's time we realized that viruses, malware, and Internet threats do not only prey on computers. We don't use our smartphones just for making calls anymore, do we? It's our online wallet for shopping, banking and paying bills on the Internet. It's our data bank storing important contacts, personal information, photos, music, videos, and what not. Giving such a device unrestricted access to our personal and financial information and at the same time leaving it exposed to infected websites, fake or malicious apps can only spell disaster that could be beyond recovery. Investing in a reliable mobile security solution won't cost us more than a situation where we are left recovering our lost or stolen data. Cybercriminals have a job to do – trick us, get inside our computers and phones, steal our data, and make money. Our job is to realize that security of our devices is not an option anymore – it's a necessity. And the sooner we come to terms with this realization, the more jobless cybercriminals will become. Stay aware. Stay safe.