QUICK HEAL
ANNUAL THREAT REPORT | 2018

www.quickheal.com

Executive Summary

The Quick Heal Annual Threat Report 2018 puts together information that concerns individuals and business owners alike. The report brings forth insights and intelligence from Quick Heal Security Labs about all that unfolded in the realm of cybersecurity in 2017 - divided into two sections viz. Windows and Android.

The threat report begins with the Windows malware detection highlights of 2017 – a breakup of detection per day, per hour, per minute, and the entire year, and a graph showing which quarter clocked the highest detection. This is followed by the detection statistics of various malware categories and the top 10 Windows malware of 2017. The report also cites some notable cybersecurity incidents that occurred in 2017. Other important topics discussed in this report are Ransomware, top 10 Windows exploits, Targeted Attacks, top 10 PUAs and Adware, and the Internet of Things.

The threat report's section on Android begins with the malware detection highlights of 2017 followed by the yearly and quarterly detection statistics of the categories of Android malware. Then comes the top 10 Android malware list and a few stories revolving around mobile ransomware, phishing and banking Trojan, and the rise of fake apps in app stores. The report shares some important observations made by Quick Heal Security Labs about Cryptocurrency Mining in 2017. A section on how Android vulnerabilities have grown throughout the year has also been included in this report.

And towards the end, the report presents an outlook on how 2018 will play out for cybersecurity in a section called Top Cybersecurity Predictions for 2018.

Contributors

- Quick Heal Security Labs
- Quick Heal Marketing Team

Table of contents

Windows

Android

Introduction

In 2017, Quick Heal Security Labs detected over 930 million Windows malware with Q1 (Jan – March) clocking the highest figure of over 295 million. On a daily basis, the Labs detected over 2.5 million malware, 30,000 ransomware, 23,000 exploits, and 2,41,000 PUA & Adware. In 2017, ransomware targeting Windows users grew 300% in comparison with 2016. The Trojan horse family retained its position as the most dominant malware in all the quarters of 2017. The exploded value of cryptocurrency triggered the rise of cryptocurrency mining and malware involved in this process. The top malware of the year is a polymorphic file infector and Quick Heal detected 13 ransomware variants with improved encryption and anti-detection techniques. April and October recorded the highest detection for ransomware thanks to the occurrence of the WannaCry and BadRabbit ransomware. In June 2017, Quick Heal detected an Advanced Persistent Attack targeted at a Government embassy and in December, a new, sophisticated banking Trojan called Icedid came to our notice.

Quick Heal Security Labs detected over 1 million Android malware in 2017. This figure comes to over 3,000/day, 128/hour, and 2/minute. The PUA (Potentially Unwanted Application) family comprised 46% of the total detection of the year. Quarter-wise, Q1 was dominated by Android malware with 48% of the total detection. Adware clocked the highest detection in Q2 with 51%. PUA was heavy in Q3 with 61% while in Q4, Android malware started regaining its dominance. The proliferation of fake apps has been one of the biggest mobile security concerns in 2017 & so has downloading apps from third-party app stores. New trends were observed in the working of mobile ransomware in 2017 and also in the way how attackers combined phishing attacks and banking Trojan to steal financial data. In the same year, Quick Heal Security Labs detected many fake Android apps that tried masquerading genuine apps on the Play Store. Towards the end of 2017, cryptocurrency mining was observed to have spread from PC to smartphones where malware authors targeted gaming, antivirus, adult entertainment, and mobile browsing apps. And these apps were compromised for mining cryptocurrency on infected devices.

The cybersecurity predictions for 2018 put forth some interesting insights into the near future of ransomware, cryptojacking, mobile security, artificial intelligence, Internet of Things, DDoS attacks, security for small and medium-sized businesses, brute-force attack techniques, and biometric authentication.

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

Follow us on:

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.

WINDOWS

Windows Malware Detection Highlights of 2017

Malware

Per Day: **2,548,240**
Per Hour: **1,06,176**
Per Minute: **1,769**
2017: **930,107,913**

Ransomware

Per Day: **30,283**
Per Hour: **1,261**
Per Minute: **21**
2017: **11,053,636**

Exploit

Per Day: **23,771**
Per Hour: **990**
Per Minute: **16**
2017: **8,676,549**

PUA and Adware

Per Day: **241,494**
Per Hour: **10,062**
Per Minute: **167**
2017: **88,145,423**

Source: Quick Heal Security Labs

Windows Malware Detection in 2017

2017 was dominated by ransomware and cryptocurrency miners and some prominent zero-day exploits. The below graph represents the statistics of the total count of malware detected by Quick Heal.

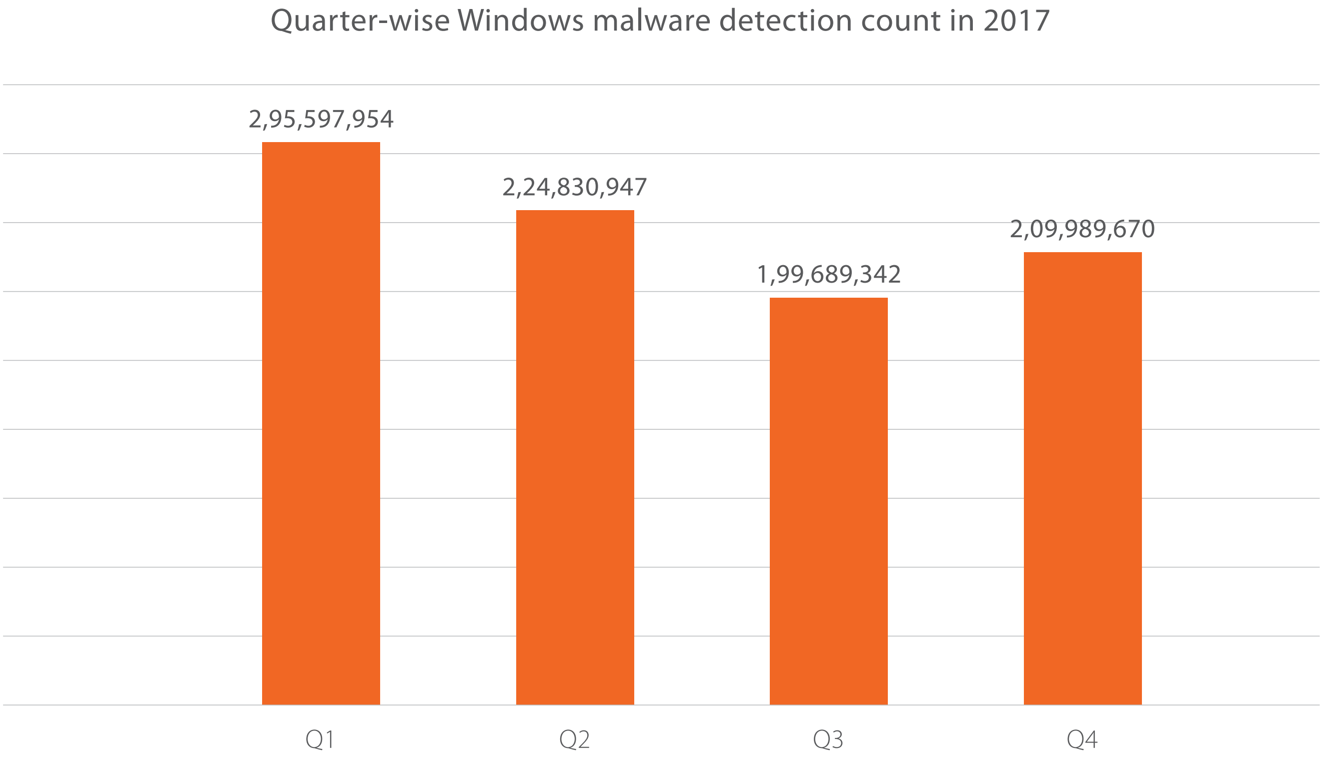


Fig 1

Observations

Q1 received the highest malware detection count with the Trojan horse malware family clocking the highest detection rate. In the same quarter, a notable observation was made against a ransomware that used NSIS installers (Nullsoft Scriptable Install System, a professional open source system to create Windows installers) to evade antivirus software.

Category-wise Windows Malware Detection

The below graphs (fig 2 & 3) represent the statistics of the categories of Windows malware detected by Quick Heal in 2017.

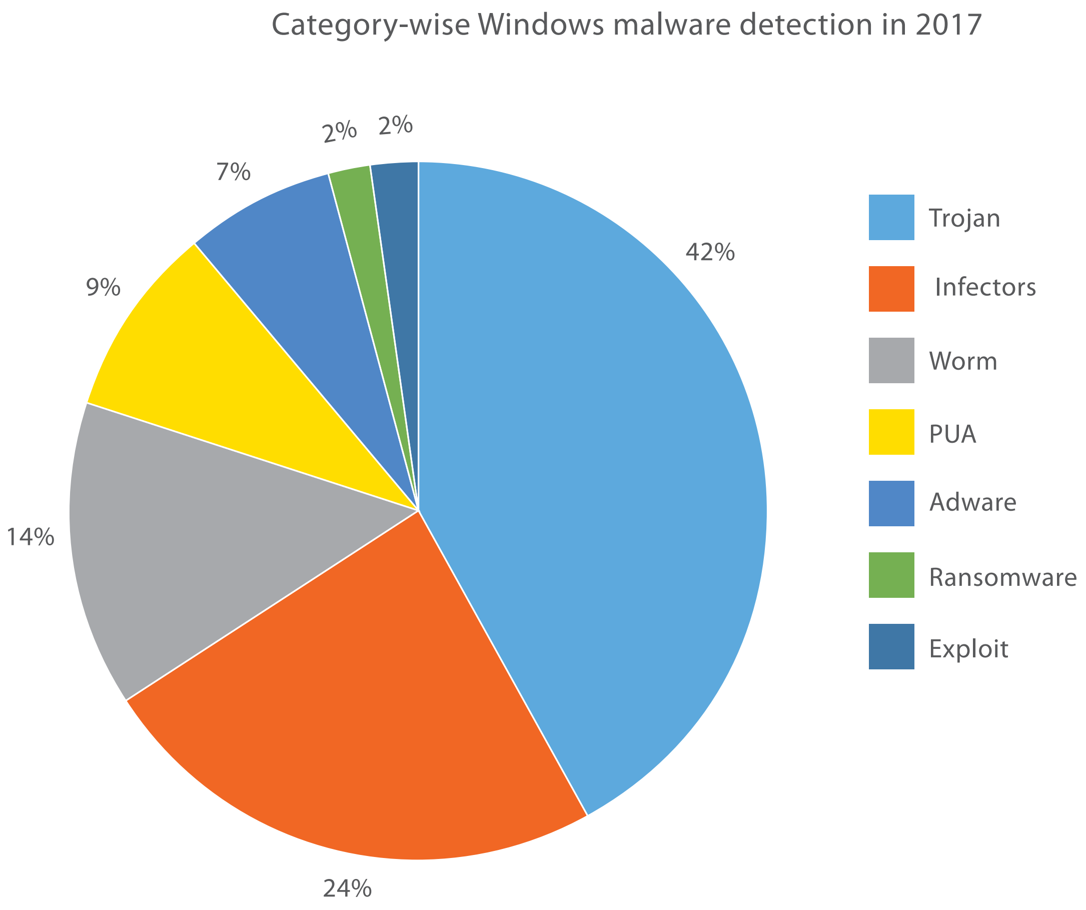


Fig 2

Observations

- Ransomware grew 300% in 2017 in comparison with 2016.
- Trojan led the pack with 42%, followed by Infector with 24% and Worm with 14%. Adware and PUA comprised 16% of the total detection.

Category-wise Windows malware detection in 2017 | (Q1 - Q4)

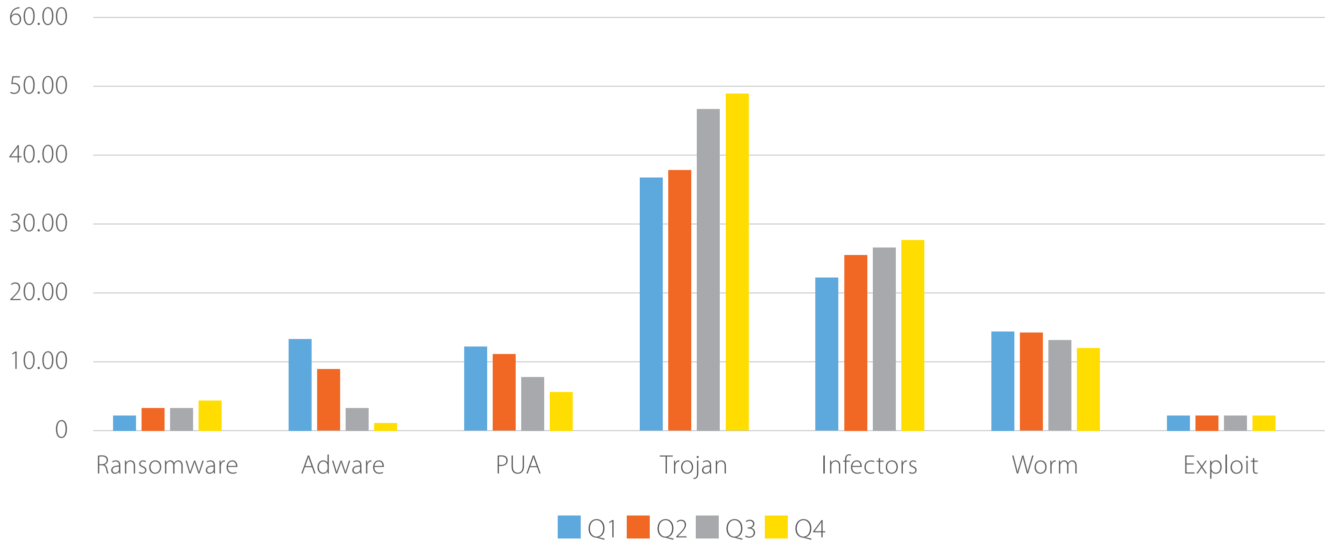


Fig 3

Observations

The Trojan horse family retained its dominance in all the quarters of 2017, followed by the Infector and Worm family.

A year dominated by Shadow Brokers NSA leaked exploits

In April 2017, Shadow Brokers leaked several exploits claimed to have been illegally obtained from the private repository of Equation Group of NSA. The leaked data contained a Metasploit alike exploitation framework called Fuzzbunch which included several zero-day exploits and their supporting post-exploitation payloads. Some critical SMB related zero-day exploits such as Eternalblue, EternalChampion, EternalRomance, and EternalScholar were also included in the leaked data. These were soon adopted in many widespread ransomware campaigns such as WannaCry, NotPetya, EternalRocks, and BadRabbit.

The WannaCry ransomware attack gained worldwide attention as it managed to infect more than 230,000 computers within a day in more than 150 countries. High profile organizations including clinics and hospitals, telecom, gas, electricity, and other utility providers in the UK and worldwide were the main casualties of this attack. WannaCry, which was launched almost a month after the leak, was also among the very first ransomware to integrate the EternalBlue exploit for its lateral propagation.

A new version of Petya a.k.a. NotPetya ransomware, which originated in June from an update of MeDoc software, also used the EternalBlue exploit. This new version of Petya was different from the old one as it functioned as a wiper and used a random key to encrypt data making it impossible to decrypt.

Along with ransomware, a few cryptocurrency miner campaigns such as Adylkuzz, Zealot, XMR (RIG), and Monero also leveraged the Shadow Brokers exploits for spreading to other machines.

The below graph shows the adoption of the EternalBlue exploit after its inception in May, in various campaigns.

MS17-010 - EternalBlue Detection Monthwise Statistics

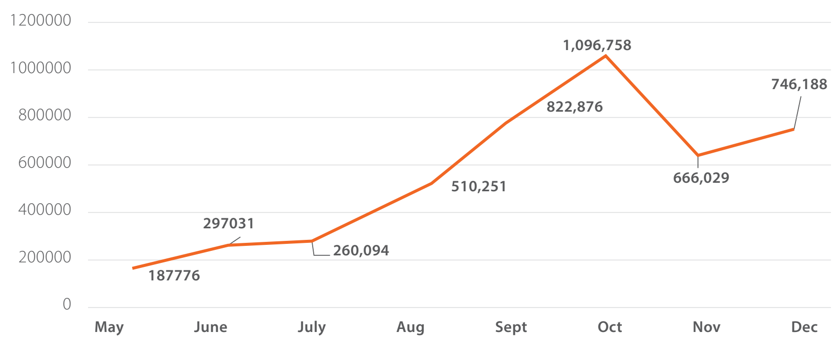


Fig 4

References:
http://blogs.quickheal.com/wannacrys-never-say-die-attitude-keeps-going/
http://blogs.quickheal.com/ms17-010-windows-smb-server-exploitation-leads- ransomware-outbreak/
http://blogs.quickheal.com/technical-analysis-recent-petya-ransomware-attack/
http://blogs.quickheal.com/bad-rabbit-ransomware-outbreak-analysis- quick-heal-security-labs/
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

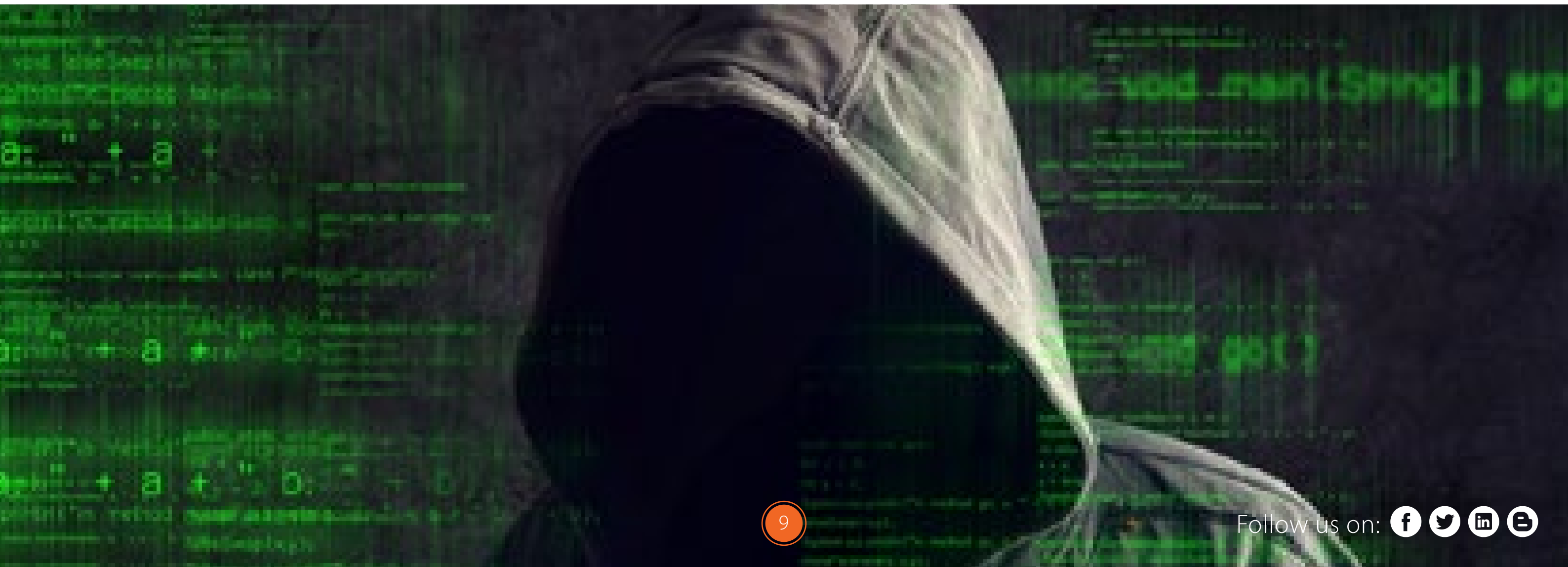
Cryptocurrency mining - A hot trend

With the sudden inflation in Bitcoin's valuation, cryptocurrency miner malware became a hot attack vector for cybercriminals. Quick Heal observed multiple distributed mining campaigns which performed mining for Monero (XMR). Cybercriminals misuse the processing power of infected machines for mining. Below are some campaigns and highlights we observed for cryptocurrency mining in 2017.

- Attackers leveraged compromised WordPress sites to spread Monero miners. When a user visits these compromised sites, mining starts in the background on the user's machine. The capability of Monero of being mined using JavaScript APIs makes it a favorite cryptocurrency for hackers.
- Overall, we received over 14 million hits of cryptocurrency miners on our users' machines. Among these, PE executable miners contributed about 3 million and more than 10 million of script miners were detected. The major script formats were NSIS and JavaScript. These statistics clearly signify the heavy prevalence of cryptocurrency malware in 2017.
- We saw mining malware making use of PowerShell and WMI database. It embeds several executables along with it. It makes use of mimikatz to extract and steal passwords. The malware requests for a job ID from its C&C server and upon its response, it starts mining. It loads the CPU with many simultaneous mining conhosts which slows down the execution of other applications. The malware also spreads in the network by making use of SMB exploits.

As long as miners are undetected in the victim's system, they will keep working to generate revenue. In the near future, we can see more obfuscated and crafty techniques being used by mining malware to evade security software. These miners would try to bypass the monitoring tools and would try to use newer techniques even after removal.

References:
http://blogs.quickheal.com/massive-campaign-delivering-monero-miner-via-compromised-websites-analysis-quick-heal-security-labs/



Top 10 Windows Malware

Fig 5 represents the top 10 Windows malware of 2017. These malware have made it to this list based upon their rate of detection throughout the 4 quarters of the year.

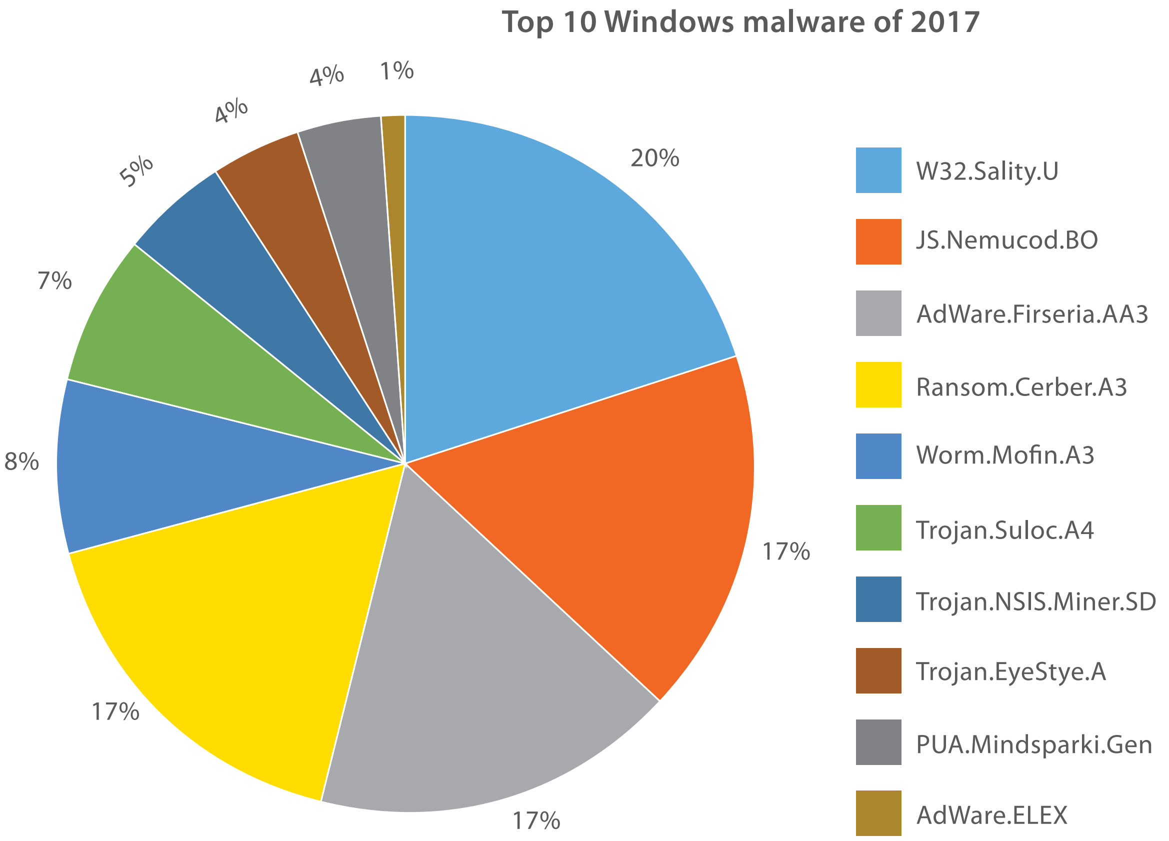


Fig 5

Observations

Infector W32.Sality.U maintained its dominance as the top malware throughout 2017. And thanks to the exploded popularity of the cryptocurrency Bitcoin, the miner malware Trojan.NSIS.Miner.SD also made it to the list of the top 10 Windows malware of 2017.

1. 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.

2. JS.Nemucod.BO

Threat Level: High

Category: Trojan

Method of Propagation: Spam emails

Behavior:

- Connects to a remote host for downloading malicious payloads or for receiving updated configurations.
- Delivers end payloads including ransomware, credentials stealing Trojans and ad-clicking backdoors.

3. AdWare.Firseria.AA3

Threat Level: Medium

Category: Adware

Method of Propagation: Dropped by other malware or as a file downloaded unknowingly by users while visiting malicious sites

Behavior:

- Make changes in the browser's settings of Internet Explorer, Mozilla Firefox, Google Chrome, and Safari.
- Adds extensions, add-ons, or plug-ins.
- Drops and executes the malicious files with random names.

4. Ransom.Cerber.A3

Threat Level: High

Category: Ransomware

Method of Propagation: Phishing emails

Behavior:

- Uses the VSSADMIN utility to delete shadow copies of volume so that victims are unable to recover data.
- Encrypts files with extensions such as .doc, .docx, .pdf, .xls, .xlsx, .py, .c, .cpp, .txt, etc., and renames them to [10 RANDOM CHARACTERS].cerber.

- Uses RSA algorithm to encrypt files and sends information of the infected computer to C&C server.
- Drops the ransom notes into each folder with names such as DECRYPT MY FILES.html, DECRYPT MY FILES.txt, and DECRYPT MY FILES.vbs.

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 the system.
- 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.NSIS.Miner.SD

Threat Level: High
Category: Bitcoin mining Trojan
Method of Propagation: Dropped or downloaded by other malware from malicious sites
Behavior:

- Runs on the infected system and uses GPU and CPU power to mine bitcoins.
- Joins the mining pool created by the malware author and uses CPU computation power of the user's system required for mining.
- Changes system settings to persist in the system. For example, it modifies the registry and adds its entry to the startup.
- Degrades system performance significantly.

8. Trojan.EyeStye.A

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

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

9. PUA.Mindsparki.Gen

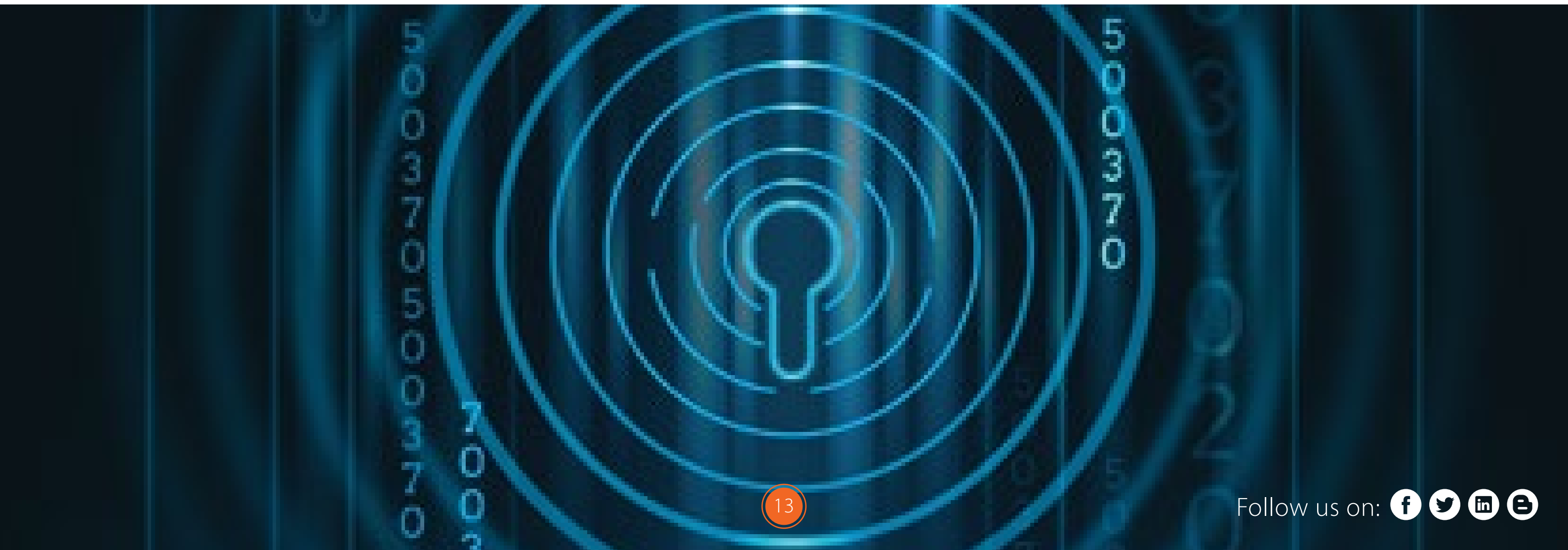
Threat Level: Medium
Category: Potentially Unwanted Application
Method of Propagation: Bundled software and malicious websites
Behavior:

- 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. Adware.ELEX

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

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



Ransomware in 2017

Ransomware is a malware that hijacks a user's system or encrypts its files and demands a ransom to unlock the system or release the encrypted files. In 2017, many ransomware variants were discovered with improved encryption and anti-detection techniques. These variants included:

- WannaCry
- BadRabbit
- Sage 2.0
- FireCrypt
- Zyka
- Spora
- Mole
- Xdata
- Widia
- GlobeImposter
- Karo
- Philadelphia
- SyncCrypt

Fig 6 represents the statistics of ransomware detected by Quick Heal on its users' machines.

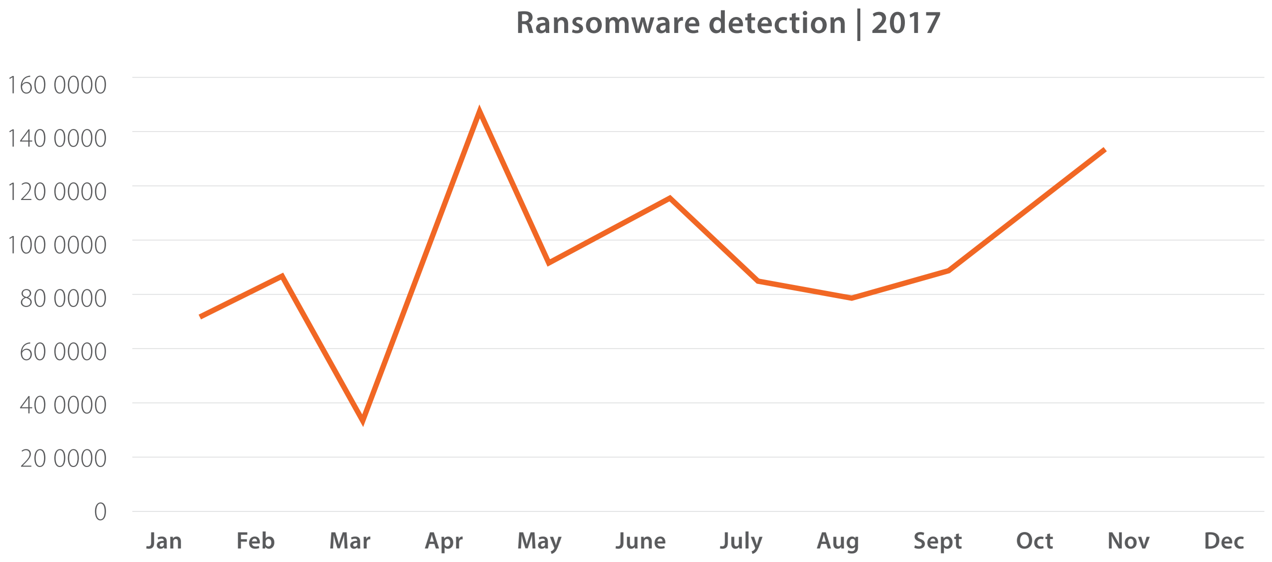


Fig 6

Observations

- When ransomware such as WannaCry and BadRabbit surfaced in April and Oct 2017 respectively, we observed a sharp increase in the overall detection.
- The distribution channels for ransomware largely include malicious spam email campaigns and exploit kits. The network spreading behavior of a ransomware is a new and destructive attack vector.

References:

http://blogs.quickheal.com/wannacry-ransomware-creating-havoc-worldwide-exploiting- patched-windows-exploit/

http://blogs.quickheal.com/bad-rabbit-ransomware-outbreak-analysis-quick-heal-security-labs/

IcedID - A new sophisticated banking Trojan

In Dec 2017, Quick Heal Security Labs observed many sophisticated versions of the banking Trojan malware. One notable detection was of that of a new player called IcedID. It has a modular architecture and is capable of stealing banking credentials of the targeted user by performing a man-in-the-middle attack (MITM). IcedID tunnels the victim's web traffic by setting up a local proxy and redirects all Internet traffic through it. Targeting businesses could be the main intention of IcedID's operators as they had added a network propagation module to it. This type of propagation is rarely observed in other banking Trojans.

References:
http://blogs.quickheal.com/technical-analysis-icedid-new-sophisticated-banking-trojan-analysis-quick-heal-security-labs/

File infectors - Dormant yet prevalent in 2017

- Although no new prominent families of file infectors were seen in 2017, we saw a few old families still making editions in the old code. This kept the file infector family in action and made it a prevalent threat in 2017. With families such as Sality, Virut, Slugin, VirRansom, Neshta, and Ramnit gaining a slot in the top 100 malware families, file infectors comprised 24% of the malware detection by Quick Heal.
- We saw the mother file of the Pioneer family keeping its complete malicious code in a reloc table. At runtime, the OS applies the relocation items specified in the table, decrypting the code and restoring the original malware. This avoids the use of a plain de-obfuscation procedure inside the virus, transferring the de-obfuscation duty to the OS instead, and making the malware highly stealthy and hard to catch by signature analysis. However, this executable was successful in executing on Windows XP and older versions but failed in Windows Vista and higher versions.
- Neshta was seen in action using existing and the latest packers and protectors for changing its mother file of infection, thus evading the static detection signatures. It also used different file types such as DotNet and VB.
- File infectors mostly attack PE files, but we observed malware families like Zombie, Sulpex and Anomaly also modifying non-PE files. Zombie and Sulpex modify non-PE files by encrypting them with a specific key. Anomaly, on the other hand, makes changes by overwriting bytes of non-PE file and making it into a corrupt file.

References:
http://blogs.quickheal.com/virus-infectors-perpetual-attack-vector-report-quick-heal-security-labs/
https://blogs.seqrite.com/virus-infectors-a-perpetual-attack-vector/

Top 10 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. Fig 7 and 8 represent the top 10 Windows exploits (host-based and network-based) of 2017.

In Fig 7, the detection for the top exploit 'Exp.RTF.CVE-2017-0199' was prominent in 2017. The vulnerability CVE-2017-0199 was found in April 2017. Considering the ease of building exploit for this vulnerability, it was picked up by many ongoing and new campaigns thus gaining more popularity. Also, the same exploit was widely used in many APT (Advanced Persistent Threat) attacks.

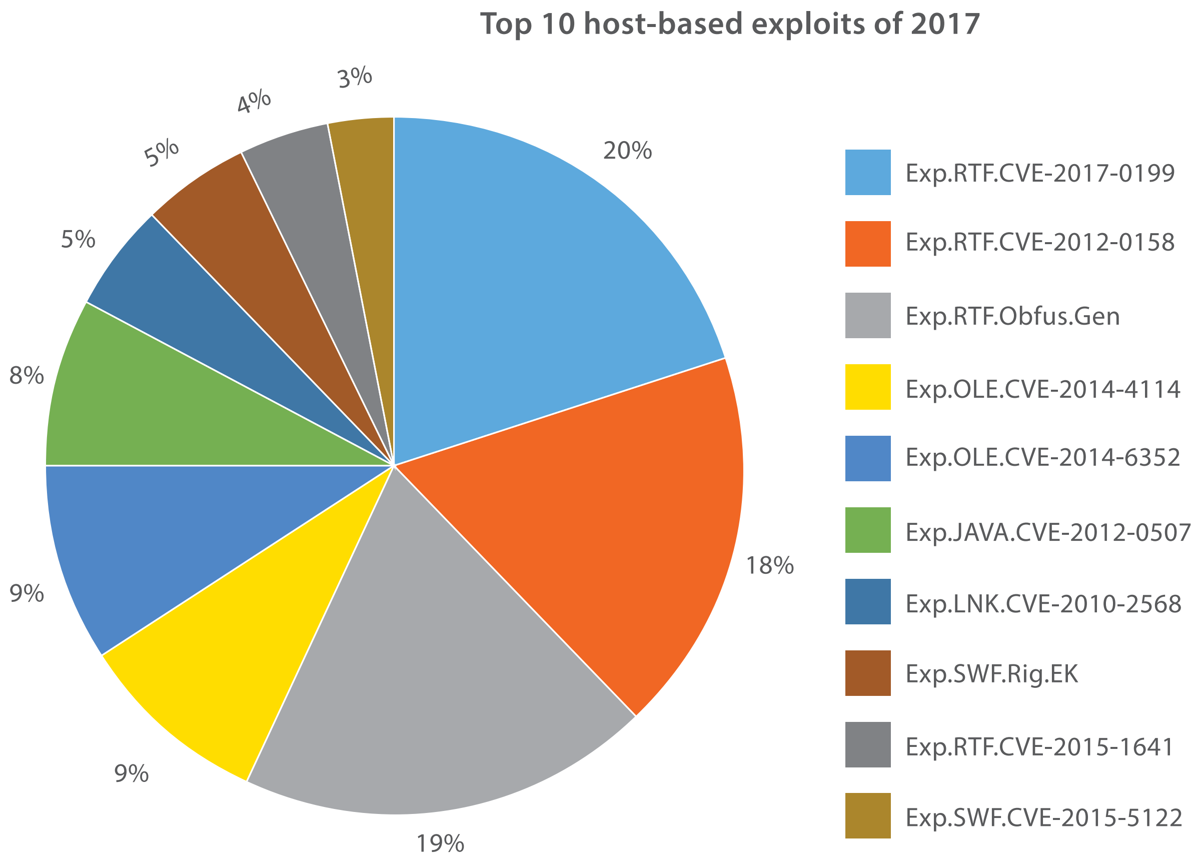


Fig 7

What are host-based exploits?

Host-based exploits are those that target security vulnerabilities found in host-based applications (host is a computer or other device connected to a computer network). These exploits are detected by endpoint detection modules such as Virus Protection, Email Protection, and Scanner.

The infamous 'Conficker' worm was observed to use the exploit of CVE-2008-4250 in order to spread across a targeted network.

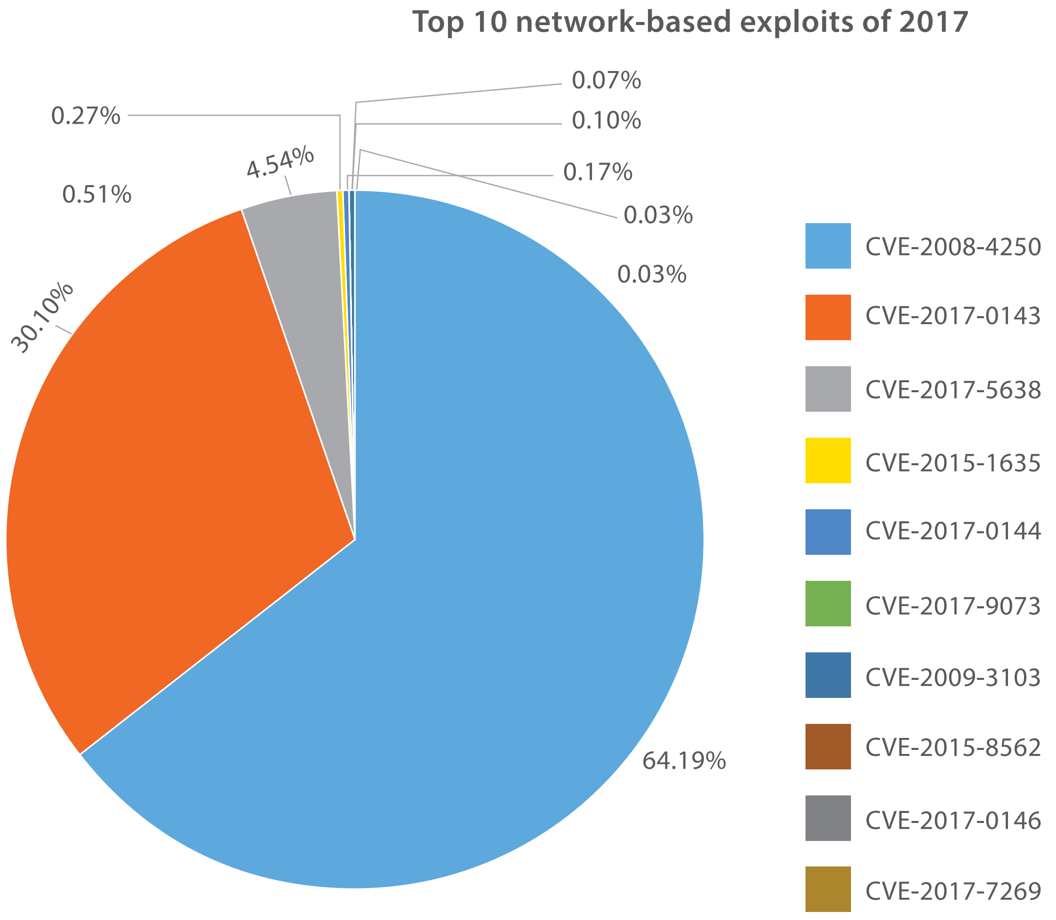


Fig 8

What are network-based exploits?

Network-based exploits are those that target security vulnerabilities found in network-based applications. Such exploits are detected by IDS/IPS (Intrusion Detection and Prevention System).

Sophisticated and powerful exploits of MS Office spotted in the wild

In 2017, we came across several zero-day exploits related to Microsoft Office which were being used in many cyberattacks. Since DOC and RTF files are the most preferred mode of infection by attackers these days, the demand for finding exploits in MS Office has gone up.

- The vulnerability CVE-2017-0199 was found in April 2017. It was being used in various campaigns to target prominent private industries in India. The vulnerability was triggered due to improper handling of HTA files while parsing a crafted RTF file having an embedded OLE2 link object. Remotely hosted malicious HTA files embedded an obfuscated VBScript which further downloaded the stage 2 payload.
- CVE-2017-8759 was another zero-day exploit that was triggered using a malicious RTF file as an initial attack vector. The remote code execution bug was present in a SOAP WSDL parser module present in System.Runtime.Remoting.ni.dll of .NET framework. The malicious samples have been seen distributing FINSPY payloads.
- Another attack vector being used by attackers is an authorized MS Office feature called Dynamic Data Exchange (DDE). The DDE feature enables data transfer between different applications like Word, Excel, RTF, and Outlook. The malicious word file asks the user for permissions to fetch data from other files and execute a Powershell script through cmd.exe. If the user selects 'Yes' in both the cases, the malware silently downloads a malicious payload from a remote location and infects the user's computer.
- The latest MS Office zero-day exploit found in the wild is CVE-2017-11882. It exploits a stack buffer overflow vulnerability in the equation editor component of MS Office. This 17 year old bug delivered a full-fledged exploit because the vulnerable binary eqnedt32.exe was not compiled using ASLR and DEP flags. After triggering the exploit, a remotely hosted malicious payload gets downloaded and executed.

References:

http://blogs.quickheal.com/cve-2017-0199-microsoft-officewordpad-remote-code-execution-vulnerability-wwindows-api/

http://blogs.quickheal.com/malspam-campaign-using-cve-2017-0199-targets-manufacturing-pharmaceutical-important-industries/

http://blogs_admin.quickheal.com/wp-content/uploads/2017/08/An-analysis-of-the-CVE-2017-0199-MalSpam-Campaign-by-Quick-Heal-Security....pdf

http://blogs.quickheal.com/recent-net-framework-zero-day-vulnerability-cve-2017-8759-dropping-infostealer-malware/

http://blogs.quickheal.com/cve-2017-8759-net-framework-remote-code-execution-vulnerability-analysis-quick-heal-security-labs/

http://blogs.quickheal.com/emerging-trend-dde-based-office-malware-analysis-quick-heal-security-labs/

Spike in Java jRAT/Adwind Infection

- Although the jRAT malware is not new, we observed an exponential increase in its activity. Every day, Quick Heal Security Labs identifies many spam emails carrying malicious JAR as attachments.
- The initial vector for this malware is generally a legitimate looking spam email tempting the user to download and open the attachment. jRAT, which is also a variant of Adwind malware, is difficult to detect in static analysis because it is highly obfuscated and uses three layers of packing on the actual source code. Malware authors have also been consistently changing the obfuscators to evade static signature-based detections and integrating anti-debugging and anti-VM techniques to bypass behavior-based detections.
- The jRAT malware on execution receives various bot commands and malicious payloads from its C&C server through a TLS encrypted SSL tunnel and executes it on the victim's machine. It also has the ability to spy on the victim by silently activating the computer's microphone and camera.

References:

http://blogs.quickheal.com/technical-analysis-java-rat-remote-access-trojan-malware-2/

http://blogs.quickheal.com/evolution-jrat-java-malware-analysis-quick-heal-security-labs/

Top 10 PUA (Potentially Unwanted Application) and Adware

Potentially Unwanted Applications (PUAs) are programs that are not necessarily harmful but using them might lead to security risks.

Adware are software used to display ads to users; some are legitimate while some are used to drop spyware that steals user information.

Fig 9 represents the top 10 PUAs and Adware detected by Quick Heal in 2017.

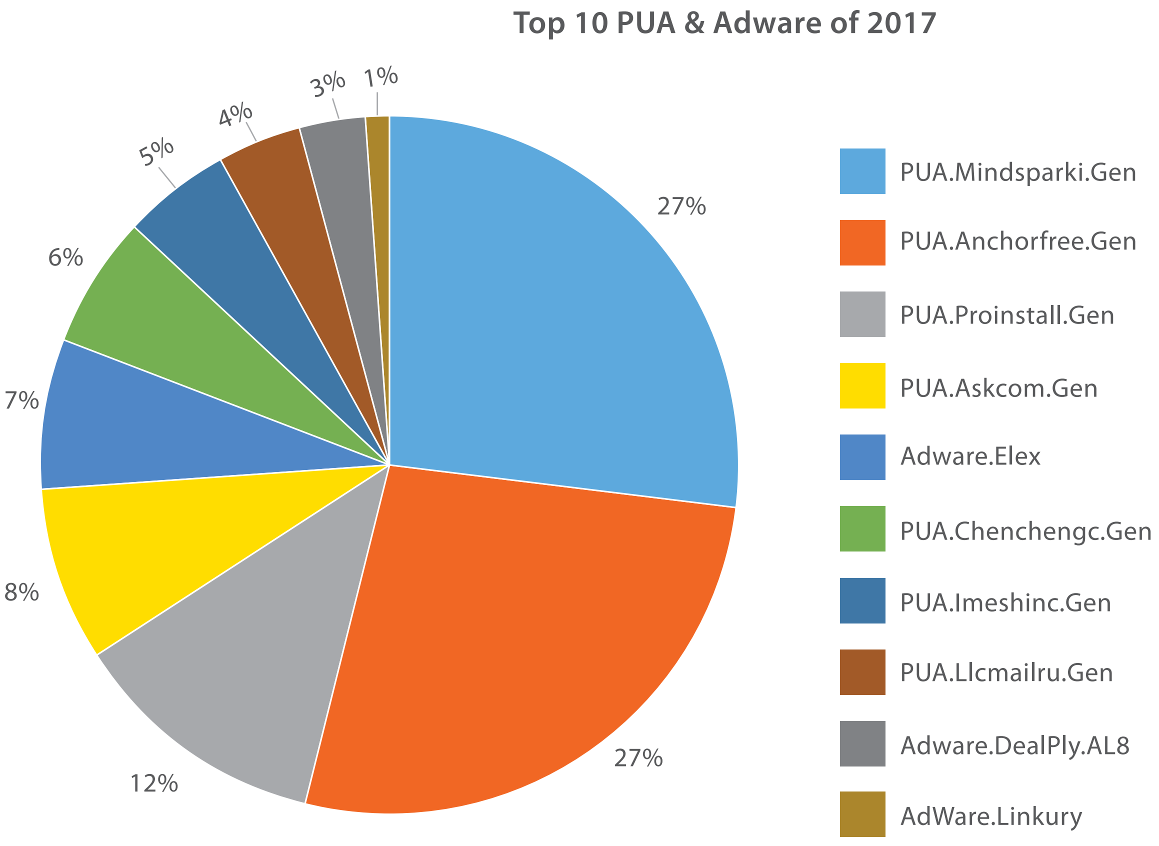


Fig 9

Observations

Quick Heal Security Labs received detections for 'PUA.Mindsparki.Gen' throughout 2017 making it the top PUA detection of the year.

References:
http://blogs.quickheal.com/potentially-unwanted-application-pua-a-digital-nuisance/

The following describes the top 10 PUA and Adware of 2017 in brief.

1. PUA.Mindsparki.Gen

- Comes from third-party bundled installer applications and downloader software.
- Sets the browser's homepage and search engine to ask.com or yahoo.com.

2. PUA.Anchorfree.Gen

- It's a browser hijacker and often comes bundled with free software.
- Changes browser's settings like homepage and search engine and adds unwanted toolbars.

3. PUA.Proinstall.Gen

- After installation, it shows ads and pop-ups on the web browser.
- Frequently redirects the user to unwanted sites.

4. PUA.Askcom.Gen

- Modifies Internet browser's settings such as default search engine and home page.
- 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.

5. Adware.Elex

- Comes with third-party bundled installer applications.
- After installation, it changes the browser homepage and shortcut path.
- Drops files that run at startup.

6. PUA.Chenchengc.Gen

- Enters a targeted computer without user's knowledge.
- Gets installed with names such as 'WinZipper', 'QKSee', or both.

7. PUA.Imeshinc.Gen

- Comes with third-party bundled installer applications and software downloaders.
- Changes browser homepage and other settings.
- Injects unwanted ads and pop-ups on the web browser.

8. PUA.Llcmailru.Gen

- Changes browser's settings such as homepage and search engine.
- Adds unwanted toolbars.

9. Adware.DealPly.AL8

- Comes with third-party bundled installer applications and software downloaders.
- Injects advertising banners on web pages that users visit.

10. Adware.Linkury

- Gets installed along with freeware bundled with installers for browser hijacker.
- Triggers pop-up ads on every site the user visits.

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 (or Advanced Persistent Threat) 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 June 2017, Quick Heal Security Labs discovered an APT targeted at a Government embassy. The attack began with a spear-phishing email having a malicious Microsoft Office document (RTF) as an attachment. The RTF file exploited the vulnerability CVE-2017-0199. This exploit downloaded a malicious HTA file which in turn downloaded a malware. The malware was being delivered from Russia.

Internet of Things (IoT) on malware authors' radar

The Internet of things (IoT) is a network of physical devices (everyday things) embedded with electronics, software, sensors, actuators, and network connectivity which enable them to connect with other devices and exchange data. It is estimated that IoT will comprise about 30 billion objects by 2020 – all the more reasons for attackers to go behind its IoT consumers.

In 2016, we saw how IoT was used by attackers take down several popular websites. The Mirai botnet used the lack of password security in smart devices for exploitation. It continuously scanned for IoT devices that were accessible over the Internet and protected by factory default or hardcoded usernames and passwords. Mirai infected devices with malware that forced them to report to a central control server, turning them into a bot that was used for DDoS attacks.

In 2017, IoT_Reaper started exploiting the vulnerabilities in various IoT devices rather than depending on cracking weak passwords unlike what Mirai did. IoT_Reaper currently includes exploits for nine previously disclosed vulnerabilities in IoT devices from manufacturers such as Dlink, Netgear, and Linksys.

ANDROID

Android Malware Detection Highlights of 2017

Malware

Per Day: **3,065**
Per Hour: **128**
Per Minute: **2**
2017: **1,119,036**

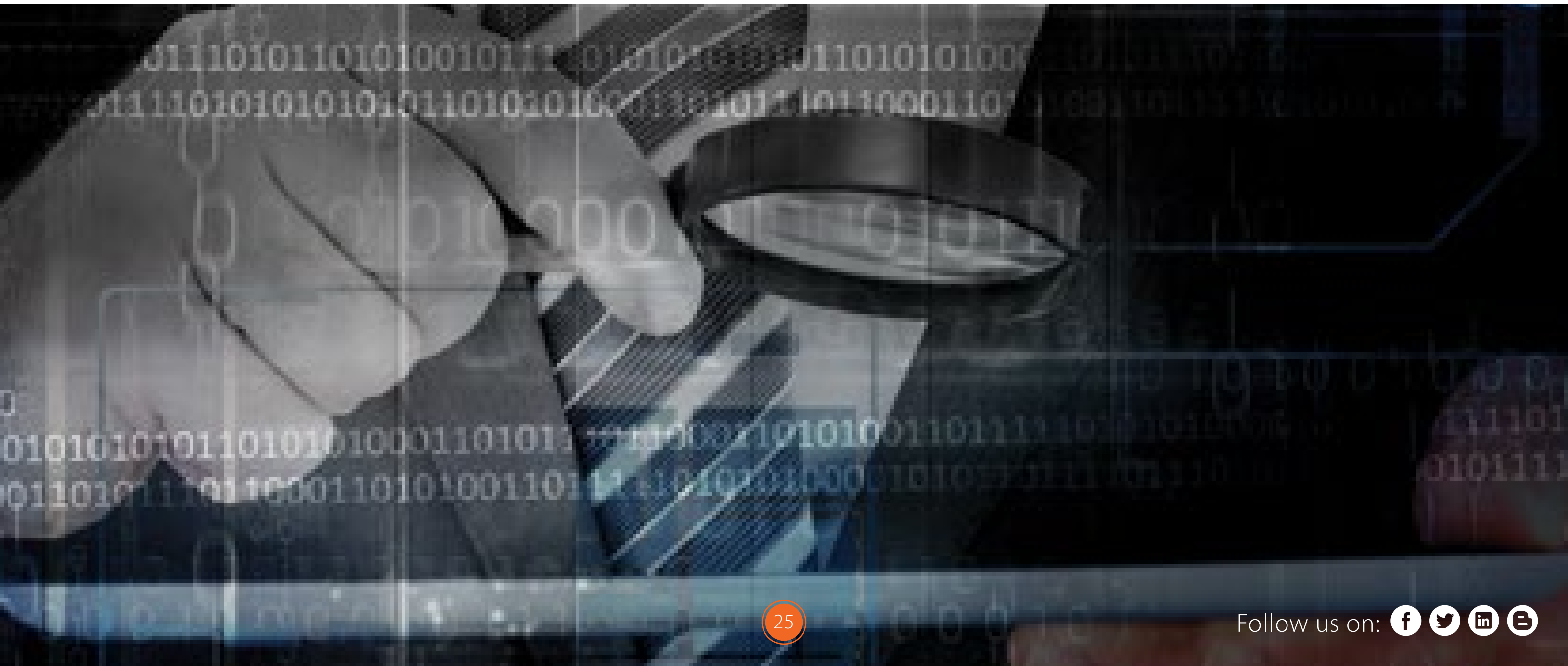
Adware

Per Day: **1,850**
Per Hour: **77**
Per Minute: **1**
2017: **6,75,514**

Potentially Unwanted Application (PUA)

Per Day: **4,247**
Per Hour: **177**
Per Minute: **3**
2017: **1,550,360**

Source: Quick Heal Security Labs



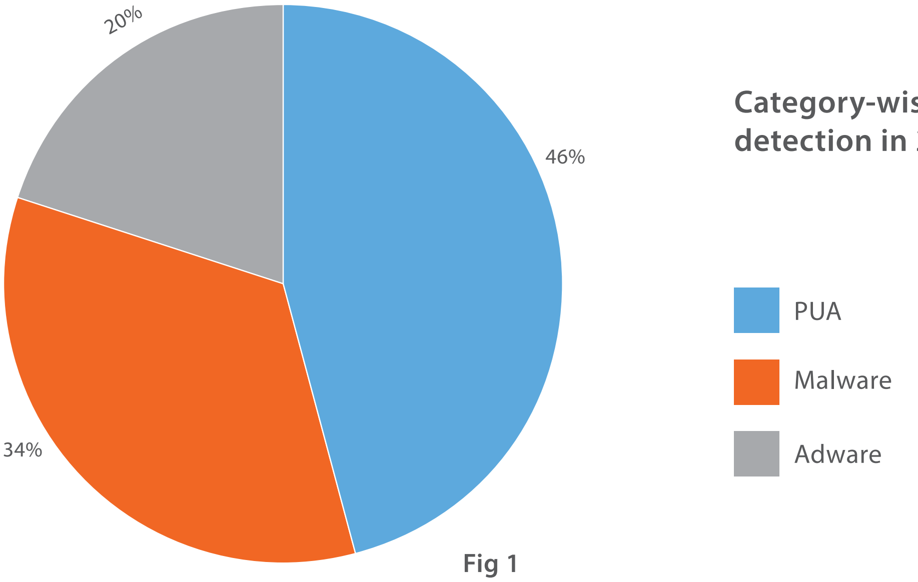


Fig 1

Observations

The PUA family clocked the highest detection in 2017 with 46% followed by malware and adware.

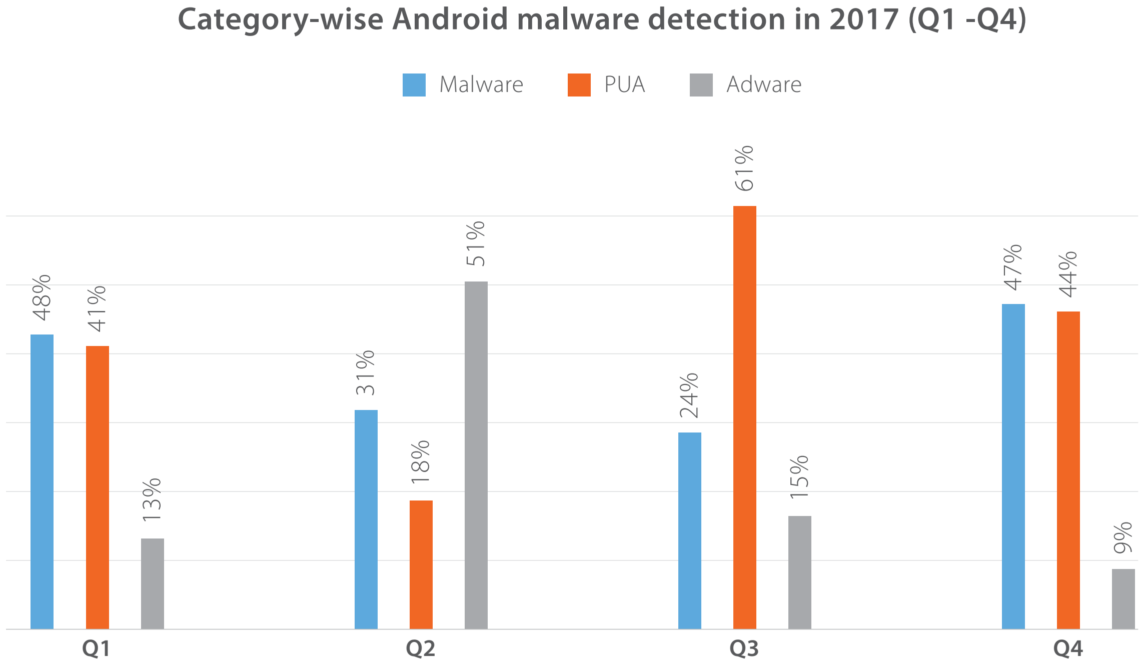


Fig 2

Observations

Q1 was dominated by Android malware comprising 48% of the total detection. Adware clocked the highest detection in Q2 with 51%. PUA was heavy in Q3 with 61% while in Q4, Android malware regained its dominance (fig 2).

Top 10 Android Malware of 2017

Fig 3 represents the top 10 Android malware of 2017. These malware have made it to this list based upon their rate of detection throughout the 4 quarters of the year.

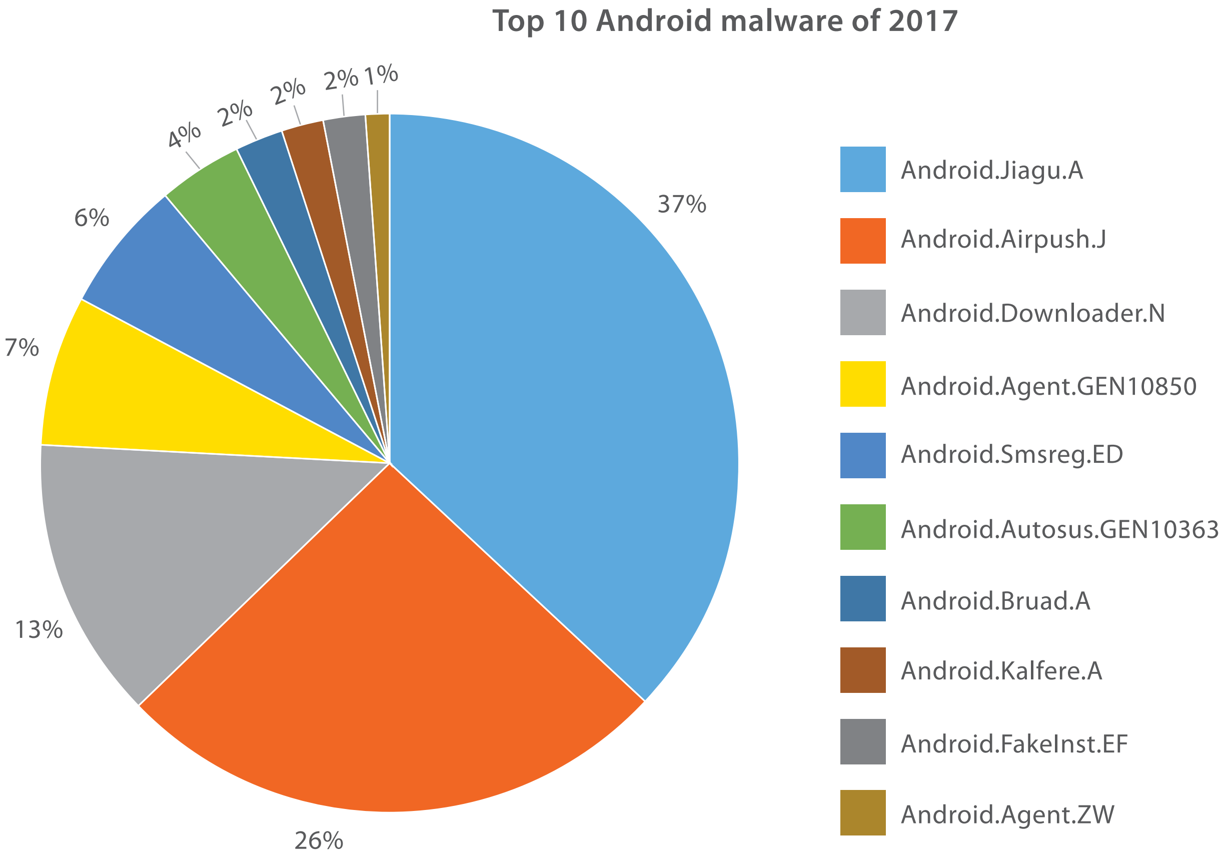


Fig 3

Observations

The proliferation of fake apps has been one of the biggest mobile security concerns in 2017 & so has downloading apps from third-party stores risking theft of personal data. Given this, the fake app malware Android.FakeInst.EF made it to the list of top 10 Android malware of 2017.

1. Android.Jiagu.A

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores and protector plug-ins

Behavior:

- Uses the 'Jiagu' Android app protector. This protector is commonly used by developers to prevent their apps from being tampered or decompiled.
- This technique makes it difficult to run reverse engineering on the malicious app because it encrypts the dex file and saves it in native files.
- It releases the data into memory and decrypts it while runtime.
- Decrypted DEX file may be a malicious or a clean file.

2. Android.Airpush.J

Threat Level: Low

Category: Adware

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

Behavior:

- Displays multiple ads while it is running.
- When the user clicks on one of these ads, they get redirected it to a third-party server where they are prompted to download and install other apps.
- Shares information about the user's device location with a third-party server.

3. Android.Downloader.N

Threat Level: High

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

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

4. Android.Agent.GEN10850

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- Uses icons of famous apps (Hike, Facebook, etc.).

- Places a shortcut of a game icon on the screen.
- In the background, it visits multiple URLs without user knowledge.

5. Android.Smsreg.ED

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

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

6. Android.Autosus.GEN10363

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- If clicked on, the app asks the user to activate 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 and runs silently in the background.
- It redirects to different URLs at different times and collects device information including device ID and incoming messages and sends the data to a remote server.

7. Android.Bruad.A

Threat Level: Medium

Category: Potentially Unwanted Application (PUA)

Method of Propagation: Third-party app stores

Behavior:

- Hide its icon after installation.
- Connects to advertisement URLs and sends the infected device's information such as IMEI, IMSI, model number, and location to a remote server.

8. Android.Kalfere.A

Threat Level: Low

Category: Adware

Method of Propagation: Third-party app stores

Behavior:

- Displays multiple ads to install other apps.
- If the user clicks on one of these ads, it gives a pop-up to install apps from untrusted sources.
- These untrusted source apps could be malicious or clean.

9. Android.FakeInst.EF

Threat Level: Medium

Category: Malware

Method of Propagation: Third-party app stores

Behavior:

- Looks like a genuine app but when launched, it connects to a server from where it receives a link to download an APK.
- It downloads the APK file – this file could be malicious.
- In the background, it also creates the icon on the home screen with the name 'Game HD Free'. If this icon is clicked, it redirects the user to a malicious web page.

10. Android.Agent.ZW

Threat Level: High

Category: Trojan

Method of Propagation: Third-party app stores

Behavior:

- Pretends as an antivirus app or adult entertainment app for Android phones.
- If clicked on, it asks the user to activate Device Administrator rights. If the user selects 'Cancel', it displays the same activity repeatedly until the user selects the 'Activate' button.
- Carries another malicious file in an encrypted format, decrypts it at runtime and drops on the infected phone. This file extends its malicious functionalities.

New trends observed in mobile ransomware

- Mobile ransomware are changing their trends. DoubleLocker is an Android ransomware detected in October 2017. It is designed to launch a two-pronged attack - it locks down the infected phone by changing its PIN and at the same time encrypts all files stored on the device. This type of a ransomware was never seen before.
- Another unusual mobile ransomware was one that demanded iTunes gift cards as a ransom instead of money/Bitcoins. The malware generated a ransom note depending on whether the infected device was online or offline. If online, it demanded iTune gift cards as a ransom, and if offline the ransom was demanded in Bitcoins.

References:
http://blogs.quickheal.com/android-ransomware-alert-doublelocker-locks-down-your-phone-and-encrypts-its-data/
http://blogs.quickheal.com/android-ransomware-demands-itunes-gift-card-ransom-analysis-quick-heal-security-labs/

Deadly combination of phishing and banking Trojan to steal financial data

In 2017, we analyzed an Android malware known for targeting banking apps. These apps are designed to collect device information such as installed apps, incoming messages, and banking credentials. Such malware checks whether the victim top most running app is a banking app and if it matches with the targeted app then a similar fake login page is displayed which lies on top of the original login page. And when an unsuspecting victim tries to login using the fake screen, their confidential info such as user ID and password goes to the attacker. Most of these malware are known to target banking apps in Australia, Russia, New Zealand, and South Korea.

References:
http://blogs.quickheal.com/beware-fake-flash-player-apps-google-play/

Rise in fake apps on Play Store

The rampant growth of fake Android apps made headlines in 2017. Quick Heal Security Labs reported many such apps to Google post which they were removed from the Play Store. Fake apps use names of popular apps, their icon/logo and even their description to fool users into downloading them. Some fake apps even have good ratings and high download counts compared with the original app.

In 2017, Quick Heal detected some fake apps that tried masquerading the popular IM app WhatsApp. One of these was downloaded more than 1 million times.

In a similar case, fake apps took advantage of the news of free services provided by Reliance JIO and the recent government's mandate of linking one's phone to Aadhaar. We found a fake JIO app claiming to provide high-speed Internet and extended validity for JIO SIM card. We also found a fake app claiming to help users link their Aadhaar to their phone.

Quick Heal Security Labs detected many such fake apps which masqueraded popular names including Avast and Pandora.

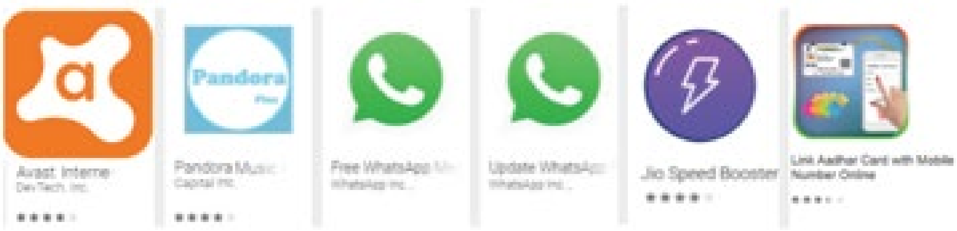


Fig 4. Fake apps that look like their original counterparts

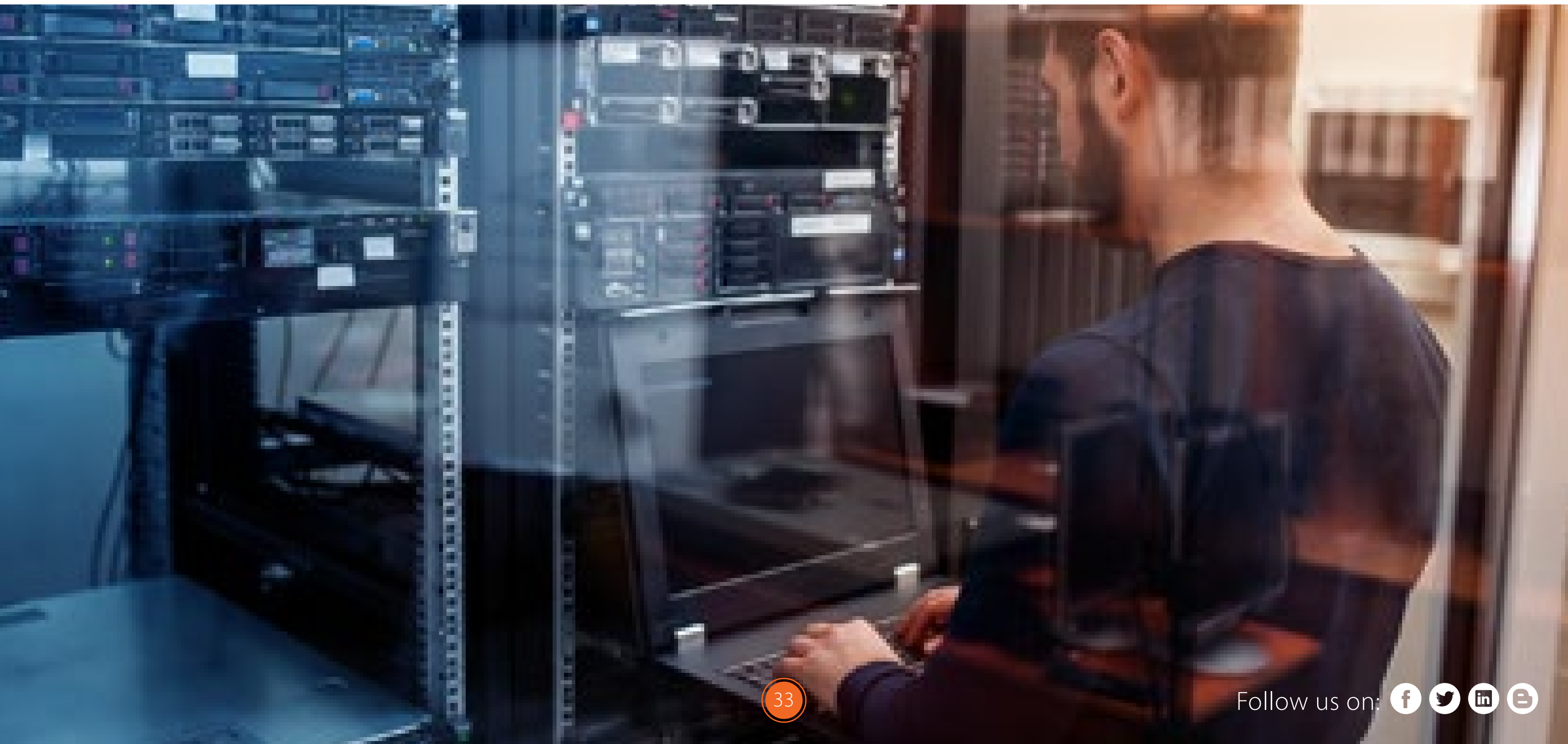
References:
http://blogs.quickheal.com/fake-whatsapp-apps-google-play-analysis-quick-heal-security-labs/
http://blogs.quickheal.com/beware-fake-apps-uses-jiojeo-names/
http://blogs.quickheal.com/beware-fake-apps-claim-link-mobile-number-aadhaar/
http://blogs.quickheal.com/fake-apps-new-emerging-trend/

Cryptocurrency Mining: from PC to Smartphones

Given the recent boom in cryptocurrency, it is not surprising that cybercriminals are trying various ways to milk it dry. And as smartphones become the new computer for many, attackers are targeting mobile devices more than ever. Towards the end of 2017, malware authors targeted gaming, antivirus, porn, and mobile browsing apps. These apps were injected with a mining JavaScript code so that once installed they would start mining cryptocurrency on the infected mobile device by using its resources. This further leads to overheating, faster battery discharge, and reduced lifespan of the device.

Below are the Quick Heal detections of cryptocurrency miners in 2017:

- Android.BitCoinMiner.GEN8416
- Android.Bitcoinminer.B42aa (PUP)
- Android.Bitcoinminer.Ab410 (PUP)
- Exploit.bitcoinminer.A97d (PUP)
- Android.Bitcoinminer.B953b (PUP)
- Android.Bitcoinminer.B646a (PUP)
- Android.Bitcoinminer.B6461 (PUP)



Security 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. The following graphs (fig 5 and 6) show the growth of Android security in 2017 and also a comparative analysis between 2016 and 2017.

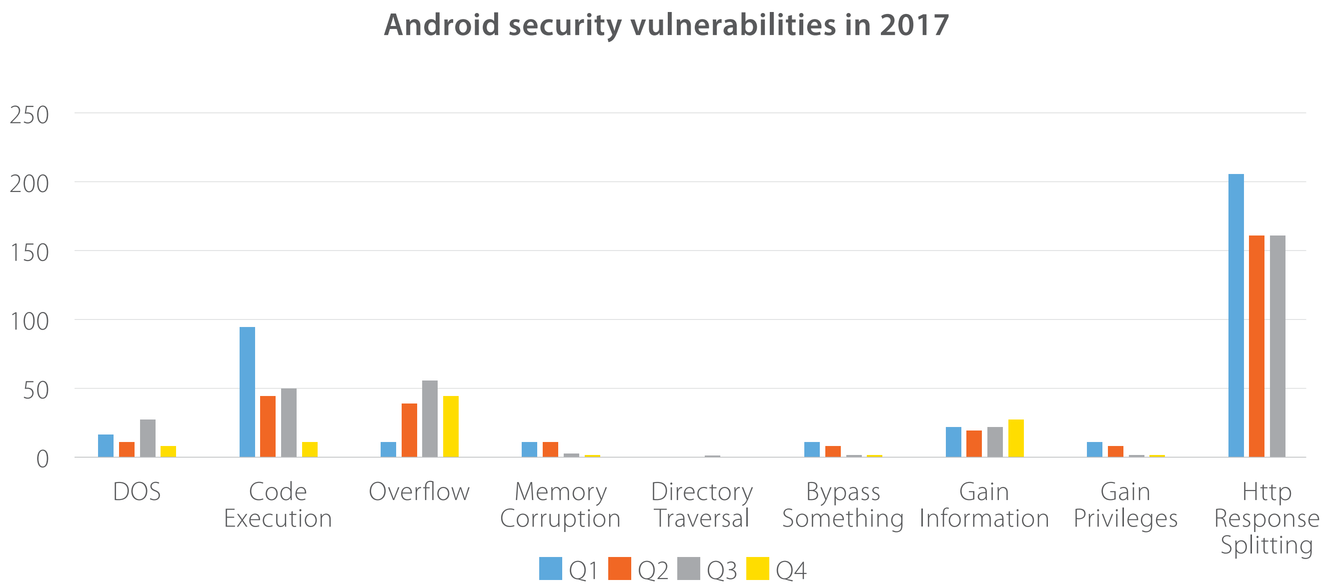


Fig 5

Source: cvedetails.com

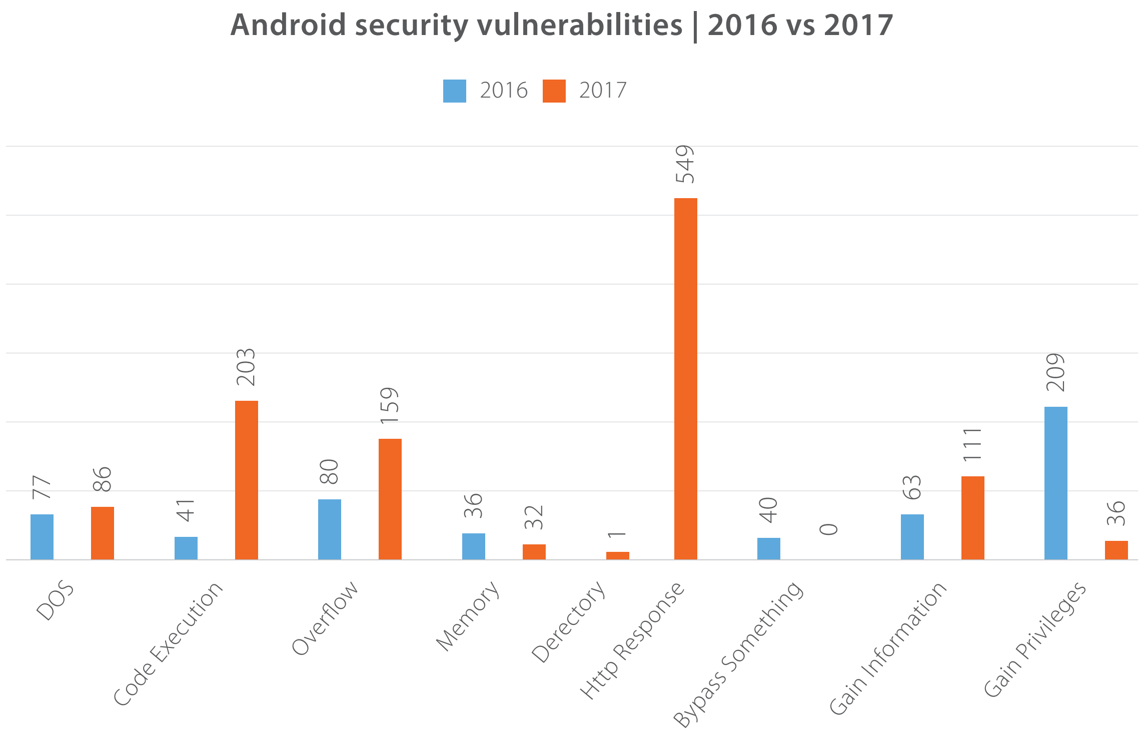


Fig 6

Source: cvedetails.com

Top Cybersecurity Predictions for 2018

1. Ransomware will become more vicious

This is a fairly obvious and logical cybersecurity prediction for 2018 – deductible from the success rate of ransomware and their growth in 2017. Ransomware is no more just a malware category but it has evolved into a fully functional business thanks to Ransomware-as-a-Service: seasoned coders create ransomware and sell them to beginners or novice criminals on the online black market – that's right, as a service. Ransomware hits businesses and individuals where it hurts the most – their data. And because these attacks pay off well, attackers will strengthen their encryption techniques and work on advanced methods to beat antivirus software. In addition to that, most ransomware creators ask ransom in cryptocurrency like Bitcoins whose value have recently started going through the roof – a sort of encouragement for cyber crooks to work harder on their ransomware business.

2017's highlight was the WannaCry Ransomware that blew away the entire cybersecurity world. Due to its integration of the EnternalBlue exploit, its network spreading ability was a menacing threat. WannaCry was followed by other ransomware campaigns carrying a similar attack pattern.

2. Crpytojacking - a new menace to deal with

If you haven't been paying attention, cryptocurrencies (digital or virtual currency like Bitcoin) have skyrocketed in the recent few months. During the time when this article was written, 1 Bitcoin was worth $15,400. That's a lot of money in there; which brings us to 'cryptojacking'. Cryptojacking refers to secretly mining cryptocurrency (generating digital cash) by a website using the resources of your computer usually without your knowledge. How is this harmful? It is estimated that a single Bitcoin transaction (which happens in cryptojacking) consumes 215 kilowatt-hours (KWh) of energy causing significant system slowdown and spiked electricity bills. Now, cryptojacking might be used by legitimate sites as a revenue stream instead of serving their visitors with pesky advertisements – which makes sense in a way. But, the fact that, this entire thing goes on without the user's consent still makes it malicious. Looking at cryptojacking from an angle of cybercrime – there is another side to it. Hackers might inject mining codes into legitimate websites (without the website owner's nor its visitor's knowledge) to generate cryptocurrency and fill their wallet.

Now, all this might not look as harmful as a phishing or traditional malware attack, but at the end of it all you are being robbed of your money indirectly without your knowledge or will.

3. Increase in threats to mobile devices

The biggest elephant in the room of cybersecurity is mobile device security – we all see it but no one wants to discuss it. Let's agree that most of us are more worried about our smartphone getting scratched than having it infected by a virus. Threats to mobile devices will increase in 2018 and the years to come because of two simple reasons (at least):

1) Mobile transactions (banking, shopping, paying bills, etc.) are growing exponentially. If we talk about only India, Prime Minister Narendra Modi's website stated a startling fact that over 72 crore transactions were done using mobile banking in 2016-17. This is a mammoth jump from 9.47 crore in 2013-14.

2) Netizens are replacing computers with mobile phones to stay online. According to a data published by StatCounter GlobalStats, users in India accessed the Internet through their mobiles nearly 80% of the time in 2017. And as accessing the Internet and buying smartphones become more affordable, it is only a matter of time before laptops and desktops suffer the same fate as that of the floppy disk. As of now, India leads the world in accessing the Internet by mobile phones.

So, with mobile phones becoming an inseparable part of our daily lives, it should be pretty easy for us to sense the magnitude of the threat that looms over all of us – well, particularly those who believe mobile phones are less attractive targets for cybercriminals.

4. Artificial Intelligence – its use and misuse

The same technology that we use to improve our lives is used by cybercriminals against us. It's a double-edged sword, and AI is just one example. In a bid to counter advanced cyberattacks that most traditional antivirus software fail to do so, security software are now being bolstered with AI and machine learning. AI will fasten up the process of detecting security weaknesses and patching them, and analyze the history of attacks to prevent future attacks. Involvement of AI will prove to be more helpful in detecting Advanced Persistent Threats that usually go undetected until a time where the damage becomes irreversible. And these are just a handful of examples of how AI can bring about a revolution in cybersecurity. Now, the AI prospect becomes scarier when we start decoding the possibilities of how it can be used by folks on the other side of the wall – cybercriminals. They will use AI to speed up the process of detecting vulnerabilities and exploiting them, for staying hidden and launching their attacks in more intelligent and full-proof ways. In short, it will be AI-powered security vs AI-laden malware.

5. Internet of Things (IoT) will still remain an easy picking for attackers

When convenience triumphs security, we get the Internet of Things (IoT). Your smartphone-controlled coffee mug can make your mornings bright but if misused by a cyber crook, the results might just be the opposite. One of the biggest challenges that have remained with IoT is their slow adoption of security. They are like the newborns in a heard of animals who are relatively weak, slow, juicy, and fresh but with no security – easy pickings! Having said all of that, the IoT security ecosystem seems to have been put on high priority in 2018 according to experts. So, we can hope to see some major improvements there.

6. DDoS attacks will get more menacing

While the growing menace of ransomware might have been the spotlight of the cybersecurity battlefield in 2016 and 2017, the havoc created by DDoS attacks wasn't any lesser. Case in point: the Mirai botnet attack in August 2016 was responsible for one of the largest DDoS attacks in history. It is projected that the attack cost affected companies roughly $110 million (as of October 2016). And this was followed by a massive wave of DDoS attacks by the Persirai botnet in 2017. In these attacks, more than 1000 different models of Internet-connected cameras were targeted by the botnet.

The primary damage that a DDoS attack causes is immediate loss of traffic and revenue for the affected websites. And this is further worsened by unhappy customers who simply take their business elsewhere – that's a long-term impact. It is only simple math to deduce that the growth of IoT-targeting botnets will be directly proportional to the rise in DDoS attacks in the near future. And as these botnets grow and become more powerful, they will lead to new and stronger waves of DDoS attacks which will be more difficult to tackle.

7. Small and medium-sized businesses will remain in the kill zone for cybercriminals in 2018

This is more of a logical deduction than a prediction. Small and medium-sized businesses operate with a false sense of security – 'they are too small to attract predators'. And if there is anything worse than living without any security is living with a false sense of it. According to the Verizon Data Breach Investigation Report of 2017, 61% of all cyberattacks target small businesses. Still, wonder why that happens? Primarily for two reasons:

1) Small businesses hold information (although less) but valuable

2) And even if they do not hold any data worth stealing, they can be used as pawns by attackers to hack into bigger clients who hold more valuable data.

So, if you own a small food joint where you collect basic information about your customers such as phone numbers, email addresses, names, etc., or if you are dealing with a bigger organization as their partner, you have all reasons to worry about the security of the network you are on and the computers you use.

8. Brute-force attack traditional but still effective

Some attacks just won't die despite being old and traditional – one glaring example of this is the brute-force attack. 2017 witnessed massive brute-force attacks on RDP which led to many ransomware attacks. Along with this, MSSQL, MySQL, MongoDB, SSH, and SMB were victims of this brute-force attack. This only indicates that this technique will become more effective and nefarious in 2018.

9. Biometric authentication data at risk

Biometric authentication technology such as fingerprint and face recognition are being adopted increasingly for unlocking smartphones. Many countries are using it to authenticate their banking security as well. If you forget your password or if it gets stolen, you can change it but biometric identification can't be lost, misplaced or changed. Biometric matching happens on the server side and if successful, the server provides the decryption key to the client. And this very process harbors the risk of a server getting hacked ultimately leading to a leak of biometric data.

Conclusion

Roughly 82 years back, the first electro-mechanical binary programmable computer was invented. And roughly 54 years after that, the World Wide Web came into being. That's a story that spans across almost 8 decades witnessing a change too colossal to fathom. Mankind has come a long way in discovering, inventing, and marveling the wonders of technology and trying to make life easier by the day. We are clinging to technology, increasing our dependencies on it, and sharing our data with almost every digital object we use. It's a click-and-done world we live in! But, when it comes to securing our digital selves, we are as primitive as the first computer. Case in point: the worst password used by most people in 2017 is '123456'. Our complacent attitude towards cybersecurity is one of the major reasons why cybercriminals get the better of most of us and sadly we still do not see them coming. And this has been a story for long. Will we ever realize that our digital security is no more a choice but a responsibility we cannot afford to shy away from? Until we get a resounding 'yes' to this question, we are not an inch away from the kill zone of cybercriminals. Having said that, we are not completely defenseless. In a battle, knowing what you are up against and predicting your enemy's next blow may fill your heart with dread and ominousness. But, this is what being prepared for a brewing storm is all about. It is about surviving an attack, learning from it, and fighting the next wave and keeping up the fight. An attacker might send you 10 infected emails – all they need is one click on your end. What if you avoid this? There might be 10 malicious apps in the app store just waiting to get inside your smartphone and ruin your life. What if your mobile is secured with an antivirus app? You might get 10 pop-up ads infected with malware on a random website you visit. What if you know better than to click on them? Our one cautious step can foil 10 malicious attempts of an attacker to trick us. All we need to do is find an answer to the question, "Will investing my time and money in securing my digital devices cost me more than what I'll suffer from a cyberattack?" If we choose the answer wisely, well, 2018 might turn out to be a good year after all!