Quick Heal

Security Simplified

Quarterly Threat Report

Q3, 2015

Fitness Trackers and IoT present rising threats to personal data

www.quickheal.com

Threat Report:

3rd Quarter, 2015

Contents

Introduction	1
Android Malware Collection Stats	2
Top 10 Android Malware	4
Most Popular Malware	6
Top Android Blogs	7
Upcoming Trends for Android Malware	8
Windows Malware Collection Stats	9
Top 10 Windows Malware	10
Major Windows Malware Categories	13
Malicious Spam Emails from Q3	15
Digitally Signed File Detection Statistics	17
Top 10 Windows Exploits	18
Notable Malware from Q3	18
Case Study: Dridex Banking Malware	20
Upcoming Trends for Windows Malware	22
Conclusion	23

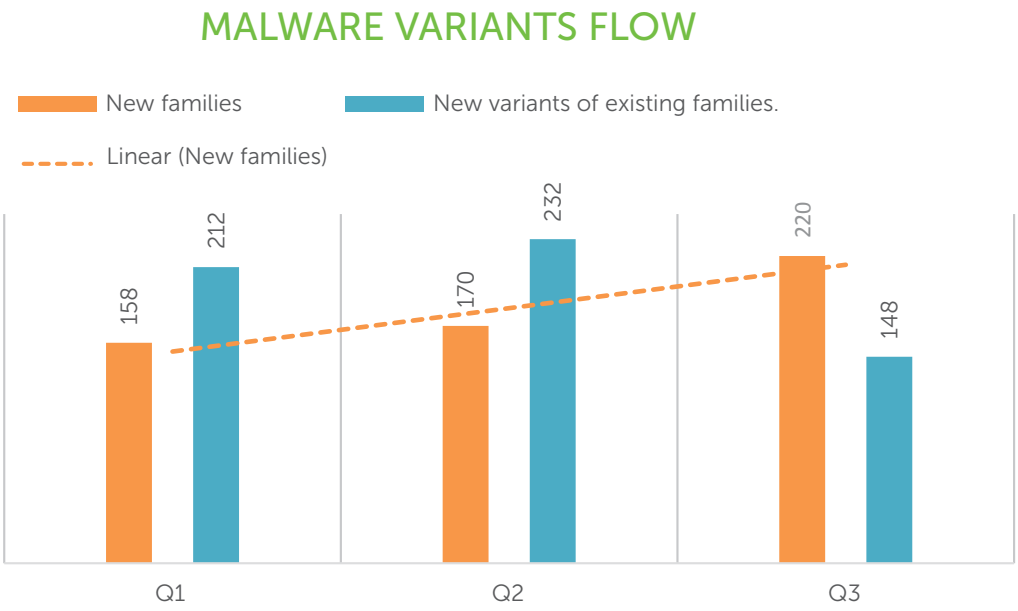
Introduction

In the third quarter of 2015 (July, August & September), the Quick Heal Threat Research Labs have received file samples at the rate of about 420,000 samples a day for the Android and Windows platforms combined. With millions of computers and smartphones connected online around the world, and accessing billions of online websites and cloud-based services, the potential for malicious software, harmful codes or infectious worms entering these systems is now at never seen before levels. Moreover, these devices and machines also hold data silos of their users' sensitive information, personal data, browsing history, shopping history, financial details and much more. Ultimately what makes things even worse is the degree of human error that comes into play when downloading that interesting but suspicious app, or clicking on that inviting but malicious ad.

In this report we analyze the samples received for Windows and Android and share details about how these samples propagate, and what they are actually capable of doing when they enter a vulnerable machine. We also study some notable trends that malware authors are currently using and predict how existing samples can adapt and morph into more dangerous variants in the near future. With technology becoming more and more ubiquitous and people carrying more than one device on them nowadays (smartphone, tablet, laptop, smartwatch, fitness tracker and more), the potential for security breaches is higher than ever. This Quick Heal Threat Report can be used as a guide to gain in-depth information into these trends and threats, and what it means for Internet users all around the world.

Android Malware Collection Stats

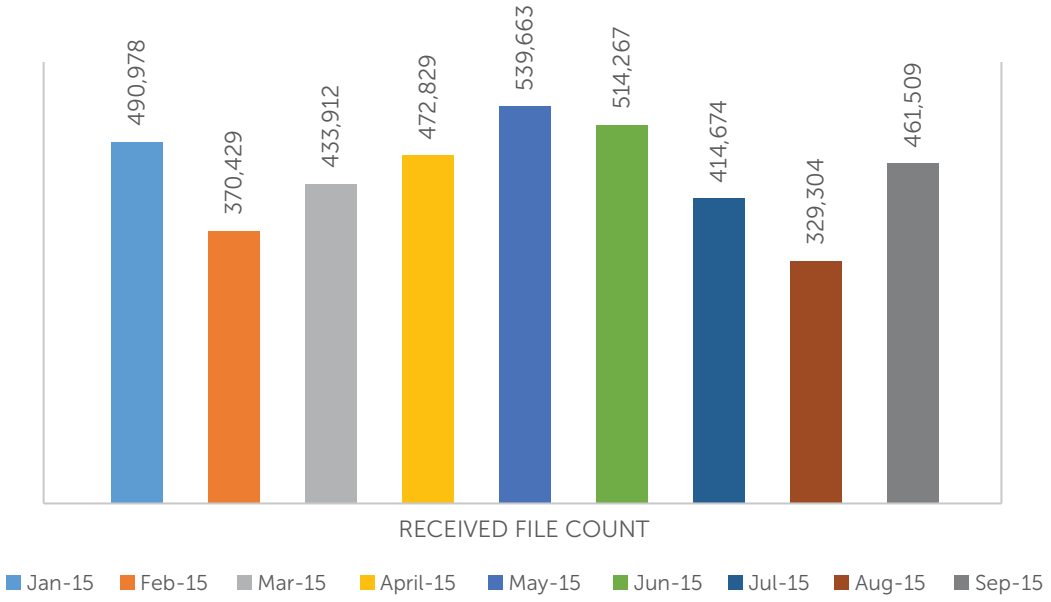
As always, the growth of Android malware samples from the previous quarter has been staggering and this trend has continued in the third quarter of 2015 as well. In the last three months, the Quick Heal Threat Research Labs have found 220 new families of Android malware. These families include several strains of Potentially Unwanted Applications (PUAs) and Adware strains as well. Additionally, the Labs have also discovered 148 new variants of existing Android malware families. As the graphs below show, the number of new Android malware families in 2015 so far has now crossed the 500 mark. Moreover, new variants of existing malware families are also close to 600 variants for 2015. These figures can be viewed in the figure representing 'Malware Variants Flow'.



The total number of samples received by the Quick Heal Threat Research Labs in Q3 2015 has seen a slight decrease when seen in comparison with the figures of Q1 2015 and Q2 2015. This highlights how Android security measures are widely being adopted by more users than before. More people are also now making use of Android antivirus software so this is clearly leading to fewer cases of infection. The figures for the 3 quarters of 2015 are seen below:

Time Period	Files Received
Q1 2015	1,295,319
Q2 2015	1,526,759
Q3 2015	1,205,487

SAMPLES RECEIVED BY QUICK HEAL

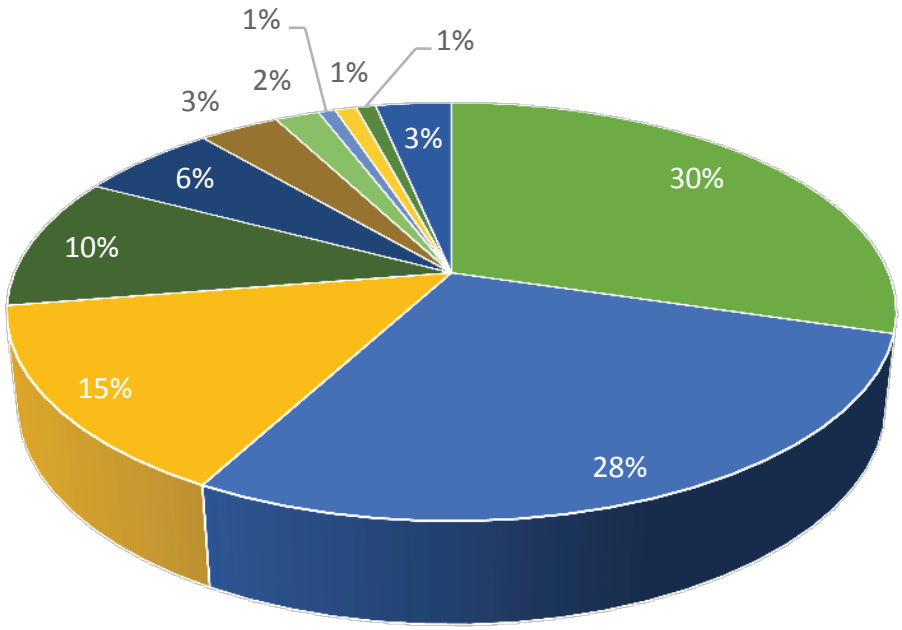


When the Android samples received are further broken down into the primary categories – Adware, PUAs and Other Malware, a few key observations can be made from the same. Adware constitutes about two-thirds of all samples received in Q3 2015, and samples of other malware have increased in this quarter as well. Adware and PUAs together comprise 85% of total samples received in the months of July, August and September 2015. These stats can be further viewed in the graph below:

DETECTION CATEGORY FLOW

Top 10

Android Malware, Q3-2015



Android.Airpush.G

This Adware strain aggressively pushes ads to the notification bar of all infected devices. It also has the capability of adding shortcuts of these ads on the homescreen. In most cases, this Adware enters Android devices through bundled software. The Adware is also capable of modifying browser bookmarks in the device and altering the appearance of the homescreen. It can also steal the following information:

- IMEI number and details
- Device location
- Device name, type and OS version details

Android.Smsreg.DA

This malicious Android app comes under the category of Potentially Unwanted Applications (PUAs) and it asks Android users to make payments through premium-rate SMS's in order to complete their registration. The app also collects the following personal information:

- Phone numbers
- Incoming SMS details
- Device ID and contacts list

Android.Sprovider.A

This is an aggressive Adware strain that does not even have an icon attached with the application installer files.

- It displays ads using "SYSTEM_ALERT_WINDOW" which popup even when the user is using another app
- It adds shortcuts to the homescreen
- It sends device information such as IMEI, IMSI and location information

Android.Ztorg.A

This is a malware family which is primarily targeted towards the Android platform. The common methods of propagation of this family are visiting infected websites and infected memory cards. In the background, it also drops downloaded packages, extracts binaries from them and tries to start them with root privileges on the device. It also performs the following malicious activities:

- Downloads malicious files
- Lowers security settings
- Steals personal information

Android.Wroba.A

This family of Android malware mostly targets Korean online banking applications and their users after installation. This app appears as a fake 'Google Play Store app' or as 'Google Services'. It immediately requests administrator privileges as well. It also performs the following tasks on devices by replacing legitimate banking apps with fake ones:

- Siphons device ID and contacts list
- Steals user data like phone numbers, incoming messages and more
- Monitors installed applications
- Accesses login credentials for bank accounts and banking information and other data

Android.Leech.E

This app comes under the Malware category and it performs the following malicious activities:.

- Connects to a malicious server to download the infected file
- Reads destination files and inputs file names on SD cards
- Creates a folder called "etemp" and replaces downloaded '.jar' file names to '.dex'
- Decrypts infected files and enables further dynamic loading
- Hides some apps and acquires a wake lock and then releases it after the malicious activity

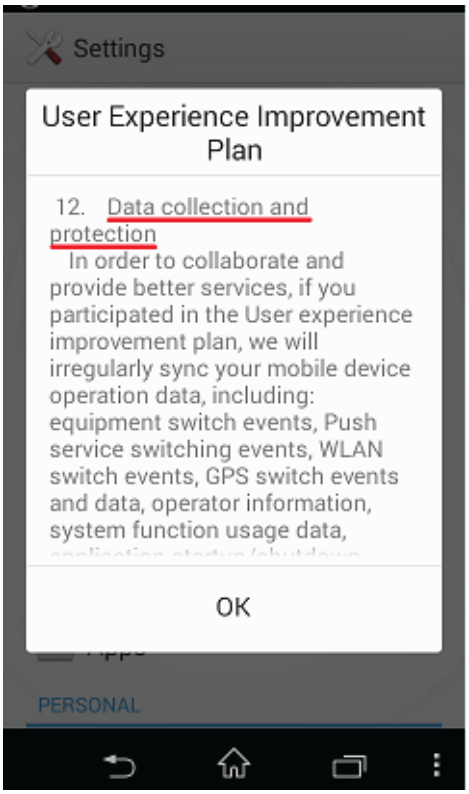
Android.Rootnik.C

This malware comes bundled with genuine apps over third-party app stores and it has the ability to root infected Android devices. It also performs the following malicious activities:

- Mounts system partitions
- Loads native libraries
- Takes admin privileges after rooting and voids device warranty
- Sends device information to a remote server
- Steals IMEI and IMSI numbers
- Accesses the camera application
- Gathers device location data

Android.Reaper.A

This app has the name "User Experience" and does not display any affiliated icons. The app gets started from the 'LenovoUEServiceActivity.java' class which first shows a popup with an agreement that states that it is going to take all user data. The data then gets sent to the URL "h**p://uefsr.le***mm.com/re**er/server/".



Android.CallPay.A

This Android malware redirects calls to third-party sites where the voice of the caller gets altered. This functionality is limited to a few countries only. These calls are then recorded on these third-party sites and some outgoing call numbers are also changed.

Android.Senrec.A

This is a Potentially Unwanted Application (PUA) for Android devices. It carries out the following malicious activities:

- Records phone calls and saves them in device memory
- Steals device information
- Reads contacts information
- Access SD card data

Most Popular Malware

CAPTCHA-bypassing malware from Google Play store

Detection name: Android.Mkero.A

In the third quarter of 2015, a malware that bypasses a CAPTCHA has been found in the Google Play store for the first time. This malware has the capability to bypass CAPTCHA authentication systems by redirecting these requests to an online image-to-text recognition service. It also has advanced concealment capabilities built in so as to operate in silent mode and to make its removal close to impossible.

Fake malicious game clones social network accounts

Detection name: Android.Feabme.A

Two applications have been found on the Google Play store and they steal the Facebook credentials of their victims. These apps are called “Cowboy Adventure” and “Jump Chess” and once installed; they create a fake Facebook login phishing screen where users are asked to key in their phone number or email address, as well as their Facebook password. On doing so, the data gets transferred to a server that belongs to the attackers.

Top Android Blogs

Android Security Tips: Get the most out of your Android apps

Installing apps can be done easily and quickly within a few simple clicks. As a result, most users end up installing apps that they may not actually use or need. On an average, a smartphone user has about 20-30 apps installed on his or her device, but it pays to be aware of the privacy configurations of these apps. Running a check of what permissions these apps use, where these apps are installed and from where these apps are downloaded will make every Android device user secure.

8 security tips to avoid falling prey to SIM swap frauds

With the popularity of online banking surging amongst smartphone users right now, a new type of fraud has been detected. Known as a SIM swap fraud, such attacks are aimed at people who are relatively new to the field of online banking and are not fully versed with the security precautions to take. This blog post highlights the key security measures that can be undertaken to prevent these SIM swap frauds.

Why it is unsafe to use pattern locks to protect smartphones

Many people use the smartphone pattern lock feature and live in the comfort that their device is safe against unwanted parties who get their hands on their devices. However, studies have shown that the actual number of patterns used by people is fairly limited, and a malicious party who is well versed with these patterns can easily guess the correct pattern. It's probably safer to make use of a strong password to lock your smartphone instead.

Android Lollipop users vulnerable to massive password hack attack

A group of researchers have discovered a serious security flaw in the Android Lollipop version running on devices right now. This flaw allows attackers to bypass the lockscreen of an Android smartphone by using a massive password and thereby exposing the homescreen. The attack essentially works by opening the in-built camera application and afflicts people using a password to protect their Android device and lock their screen.

Upcoming Trends for Android Malware

1

High profile targeted attacks on iOS in the coming months

As the number of iPhone owners rises across the world, iOS has become a new potential target for Android malware authors and hackers. It is expected that Android malware will soon be altered to affect iOS users as well, and jailbroken iOS devices will be the first wave of targets for these attacks. Recently, the 'XcodeGhost' malware was found on the Apple App Store and this is just the beginning of such attacks. Quick Heal detected this malware as "Trojan.OSX.XcodeGhost.A".

2

Continued dominance of Adware on Android devices

This prediction has held up for several quarters now and it does not show any signs of receding any time soon. Adware has notoriously been the leading source of malware on Android devices for a long time now and this pattern will continue for the rest of 2015 as well. Existing Adware variants are further expected to evolve and play a leading role in Android malware samples as well.

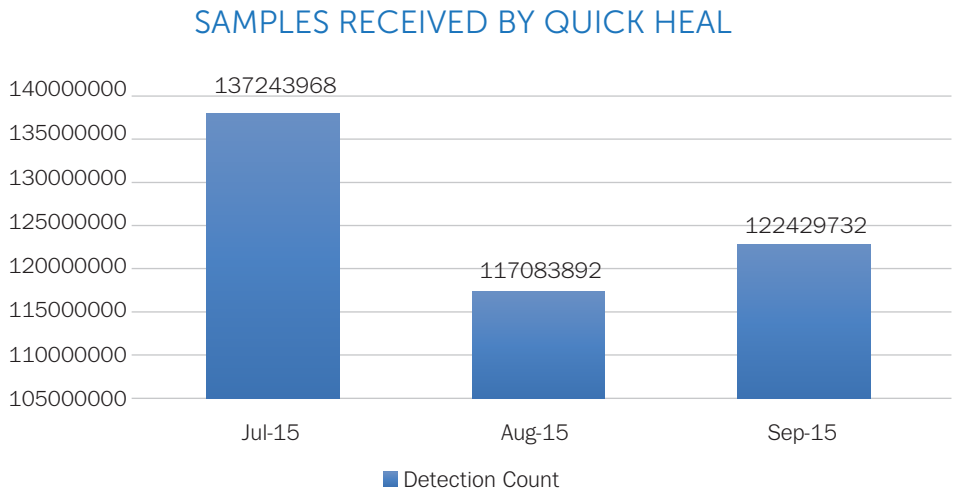
3

Fitness wristbands and smart watches to open new security loopholes

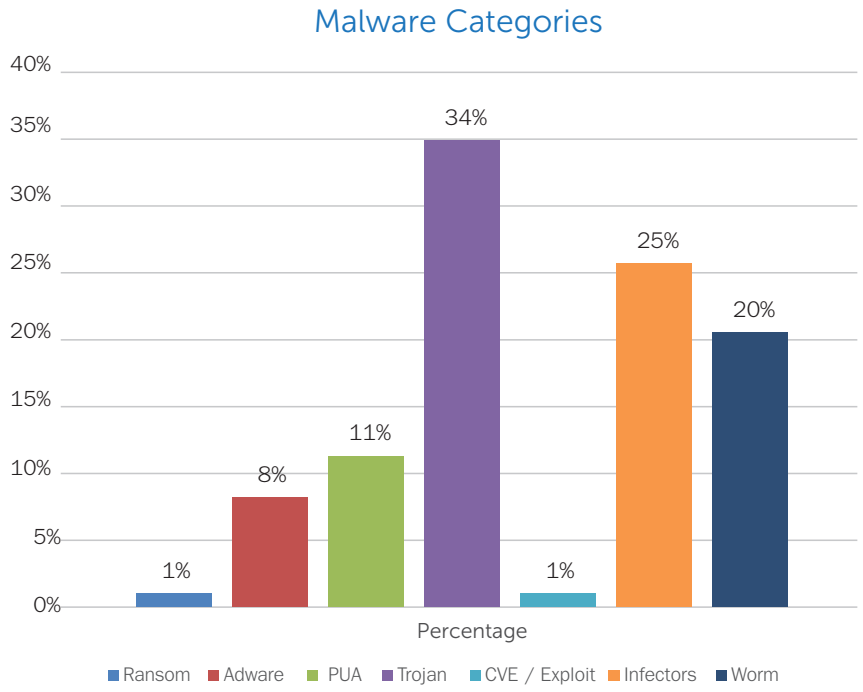
With connected smart watches and fitness wristbands constantly gathering user data, it is only a matter of time before we see security incidents afflicting these devices as well. The data collected by these devices can be used against users in several creative ways, and moreover, hackers can create a greater sense of panic by appearing in channels where unsuspecting users will not be expecting them. This shock value will lead to instant payback for some attackers.

Windows
Malware Collection Stats

The detection count for Windows malware over the last three months of 2015 – July, August and September 2015 (Q3) has undergone a twofold rise. The number of files received by the Quick Heal Threat Research Labs has now reached stratospheric levels and there are several notable attributes that have caused this. Given below are the numbers of the samples received by the Quick Heal Labs in these preceding months. As can be seen, the month of July saw the maximum number of samples detected, followed closely by September. These numbers which range in the millions highlight the dominance and prevalence of Windows malware across the world.

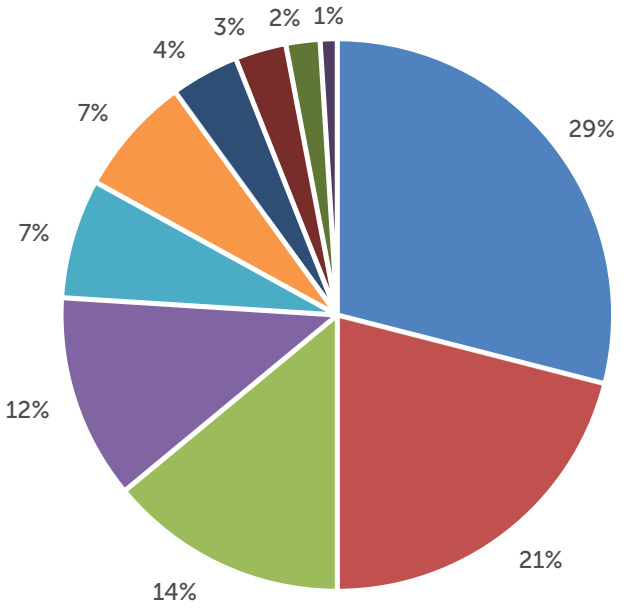


Upon analyzing the samples that have been received by the Quick Heal Labs, it has become apparent that Trojans are the most common types of malware affecting the Windows platform in the third quarter of 2015. Over these 3 months of July, August and September 2015, the following malware categories were discovered.



Top 10

Windows Malware



Worm.Conficker.Gen

Dissemination: Worm.Conficker.Gen replicates itself to the Windows system folder and it also spreads through removable USB drives or file sharing.

Threat Behavior:

- It can infect a system and spread to other computers through the network without any human interaction.
- It allows the remote code execution whenever file sharing is enabled on systems.
- It disables important system services and security products and also downloads arbitrary files.
- Infected systems are blocked from visiting websites of security apps and other services that may assist with the removal of this worm.

Browser.MalExt

Dissemination:

- Browser extensions installed by Potentially Unwanted Programs (PUPs) are the source of this.
- The major issue faced by customers is that of unwanted popups and advertisements.

Threat Behavior:

- Web URLs get altered according to variants.
- Various popups and ads are displayed during web browsing.
- Normal browsing is adversely affected and users are redirected to malicious or unwanted websites.

JS.Adware.CrossRider.A

Dissemination: This advertising software gets unintentionally installed by other software components on a user's computer without his or her permission.

Threat Behavior:

- After infection, the browser displays advertising banners, popups, and in-text ads.
- Other unwanted adware programs also get installed without user permission.
- It can also hijack the default homepage and search engine of browsers.
- It also generates several ads and interferes during browsing sessions.

Trojan.BitMin

Dissemination: Trojan.BitMin is commonly distributed through insecure webpages, social sites, instant messengers or removable USB drives.

Threat Behavior:

- Trojan.BitMin is a risk tool or a Potentially Unwanted Application that uses a victim's computer resources to generate Bitcoin blocks.
- Users with high-end graphics cards and Internet access can generate Bitcoins and sell the virtual currency for real hard currency.
- Malware authors infect computer systems with powerful GPUs for the sake of money.

PUA.Clientconn.Gen

Dissemination:

- These are Adware program publishers which are promoted and downloaded by third-party software.
- They are specifically designed to promote their own search engines – default-search.net, search.ask.com, Trovi search.

Threat Behavior:

- It changes the default search engines to Bing and the browser homepage to Trovisearch.com.
- It adds entries of Bing, Ask.com, AOL and Trovi in the browser settings search engines.
- It excessively displays popup ads.
- It shows ads about software that claim to be highly recommended and then downloads them from malicious websites.

Adware.Linkury.A3

Dissemination: Adware.Linkury.A3 is an Adware program that comes in the form of a browser add-on like CD burning software, for instance.

- It excessively displays popup ads.
- It shows ads about software that claim to be highly recommended and then downloads them from malicious websites.

Threat Behavior:

- It gains access to search results, visited sites and cookies, and based on these it shows ads which appeal to the victim.
- It redirects users to potentially harmful sites.
- Popups and ads utilize system resources which hamper system performance.
- Some users may also experience a slowdown in the speed of web browsers.

Trojan.Quolko.A

Dissemination: Trojan.Quolko.A mostly spreads through various software bundles that are downloaded by users. It also spreads through hacked or malicious websites.

Threat Behavior:

- It drops its file and registry entry into a system and starts the infection when the system reboots.
- Using backdoor techniques, it allows third-party attackers to remotely control infected computers and it then steals

confidential information.

- Gives other malware entry into the system, corrupts computer functions and changes startup system items.

TrojanDownloader.Esaprof.A4

Dissemination: This malware spreads through spam emails that contain infected attachments or links, and even through malicious websites or peer to peer (P2P) connections.

Threat Behavior:

- It changes computer system settings such as registry entries, system files and startup settings.
- Once installed on a PC, it silently downloads other malicious programs as well.
- It is capable of exploiting system loopholes to allow other viruses to get into the targeted computer. These viruses can gather important information and misuse it.
- It also provides access into these infected machines to other intruders.

PUA.Softonicin.Gen

Dissemination: This Potentially Unwanted Application (PUA) downloads software stubs (downloader executables) which then download installer setups from websites along with additional malicious setups.

Threat Behavior:

- While downloading the below listed software it provides some unwanted software downloads and installations such as VOpackage with vuupc, SiteFinder which causes changes in browser settings and default search engine settings.
- Some other examples are "007-password-recovery" and "100-sudoku-puzzles".

TrojanDownloader.Upatre

Dissemination:

- This spreads through spam emails and unsafe links. Attackers send malicious attachments with emails that contain malicious programs and links.
- It is a type of malware which downloads various other malware strains such as 'Dyzap' or 'Zbot'.

Threat Behavior:

- As its name suggests, this Trojan contains malicious or potentially unwanted software which it drops and installs on an affected system.
- It opens a backdoor which may then be used by remote attackers to upload and install further malicious or potentially unwanted software on the system.
- It connects to the Command & Control (C&C) server and downloads various malware.
- Infected PCs become slow and take longer to open processes.

Major Windows Malware Categories

Adware

Adware is a software package that allows ads, banners and promotional content to be displayed in places where a user does not expect them to show up. In addition to displaying unwanted ads, Adware also redirects users to specific websites. They also remain installed on the system without the knowledge or consent of the users, and silently collect data from the machine in order to send it to a remote server. Adware usually reaches the machines of victims through bundled software with freeware and shareware programs. Another source of Adware is malicious websites that are visited by unsuspecting users.

The third quarter of 2015 has seen a noticeable rise in the number of Adware samples that have been detected. Heightened Internet usage across the world has opened many doors for cyber crooks to get Adware on to systems and their advanced techniques have also enabled them to hit their targets with more sophisticated methods.

Today, ads are getting delivered to users based on their browsing habits thanks to cookies that are collected by almost all websites. Malvertising is another technique that allows hackers to penetrate genuine websites by delivering malicious ads there. When a user accesses these pages, malicious codes get downloaded and they can perform further harmful activities on these machines. These activities adversely impact system performance, network bandwidth and also open backdoors for other malware to enter the system.

In Q3 2015, these are the prominent malware samples that were discovered in-the-wild:

- CrossRider
- Linkury
- MultiPlug
- Kranet
- Eorezo

Ransomware

Going into the last few months of 2015, the ransomware malware family remains a key challenge for the IT security world. Ransomware is a malware type that makes an infected system unusable by locking the screen or system, encrypting the data on the system and then demanding a ransom to unlock and decrypt this data. In most cases, the ransomware also displays threatening messages and pretends to be from some law enforcement agency so as to appear genuine. The payment of the ransom is usually demanded in the form of Bitcoins, a

virtual currency that is highly untraceable once dispatched. The key aspect of ransomware is that there are very few new ransomware strains that are discovered from time to time. Attackers simply use existing

samples and morph them to avoid detection and to spread further. One of the most consistently seen ransomware samples has been Cryptowall 3.0.

Use of social engineering

In Q3 2015, social engineering tricks were widely used by attackers in order to spread their ransomware strains further. Cryptowall 3.0, one of the most consistent file encryptors made use of Google Drive in one of its campaigns for delivering malware and encrypting user's files. CTB-Locker also used the much awaited Windows 10 upgrade as a subject line in spam emails to lure unsuspecting users. These emails actually contained a malicious ZIP file as an attachment that invisibly dropped the CTB-Locker malware.

Enhanced techniques to lure security products

Ransomware as a Service (RaaS) encryptor and the .DLL version of Cryptowall 3.0 played significant roles in the propagation of ransomware techniques. "Operation Kofer" has been discovered in Q3 2015 and it automatically generates and delivers new variants for every target in order to avoid signature-based detection. The detected samples have also showcased the ability to evade advanced detection techniques by sandboxes.

Some other major ransomware samples that were detected in Q3 2015 were:

- Variants of Cryptowall 3.0
- Variants of Troldesh malware
- Variants of TeslaCrypt 2.0
- MW_file Encryptor
- Blocker
- Onion

Exploit Kits

An exploit kit is a technique that is used by attackers to deliver malicious payloads to the systems of victims. These exploit kits use known and unknown vulnerabilities of these systems, most of which commonly arise due to unpatched programs, browsers and operating systems. In Q3 2015, Adobe Flash was found to be the most commonly afflicted and exploited program. Some critical vulnerabilities like "CVE-2015-5119" and "CVE-2015-5122" have been identified in Adobe Flash Player 18.0.0.204 and earlier versions for Windows, Mac and Linux. These exploit

kits commonly cause a system crash and potentially allow an attacker to take control of affected systems.

Another exploit kit that was discovered was the Windows Local Privilege Escalation (LPE) exploit kit – CVE-2015-2426. Attackers can make use of this vulnerability to install rootkits or bootkits malware strains under unexpected system privileges without users' knowledge. This vulnerability can allow hackers to easily control affected systems from a remote location.

Lastly, CVE-2015-2590 is a Java zero-day exploit that was used in 'Operation Pawn Storm', a targeted attack campaign or Advanced Persistent Threat (APT). Thanks to this, victims are infected via emails that contain malicious URLs where the Java exploit is hosted. Once successfully exploited, attackers can run arbitrary code on the default Java settings that may lead to high risks for infected machines. Additionally, this exploit spreads a chain of malware infections that further lead to information stealing malware samples.

Banking Malware

Over the last few years, banking malware has become a lasting trend in the cyber security world thanks to the prevalence of banking apps and online banking. With increased use of the Internet and other online services which are provided by financial institutions, banking transactions are now faster and can be completed within a few clicks. Malware authors are commonly taking advantage of this by infecting users' machines with banking malware that digs out personal and sensitive information from systems.

The recently discovered Upatre Trojan downloader used polymorphic techniques to deliver the famous "Dyre" banking malware into systems. Another campaign was discovered related to the banking malware "Dridex" in which malware was digitally signed and certificates issued by COMODO were used.

Banking malware authors have also now turned their attention towards the employees of banking organizations around the world. They have started gathering information about different employees, which employees are vulnerable to hacks and attacks and which employees have greater access to sensitive data infrastructure. Attackers are also devising ways to pinpoint machines that access such data on an everyday basis. With the time-test methods of spear phishing emails, hackers are tricking employees into providing them access into these systems. Additionally, they are also installing Remote Access Tools (RATs) to capture videos and images of these daily transactions with critical data silos.

Malicious Spam Emails from Q3

The Quick Heal Threat Research Labs detected an unusual number of malicious spam emails from all sources in the last 3 months – July, August and September 2015. The detailed statistics about these malicious phishing emails are as below:

Month	Malicious spam Emails
July-15	35%
August-15	32%
September-15	33%

The percentage of Malicious spam emails which have been received in Q3 have been the highest in 2015 so far and here are the corresponding figures for the preceding quarters of 2015.

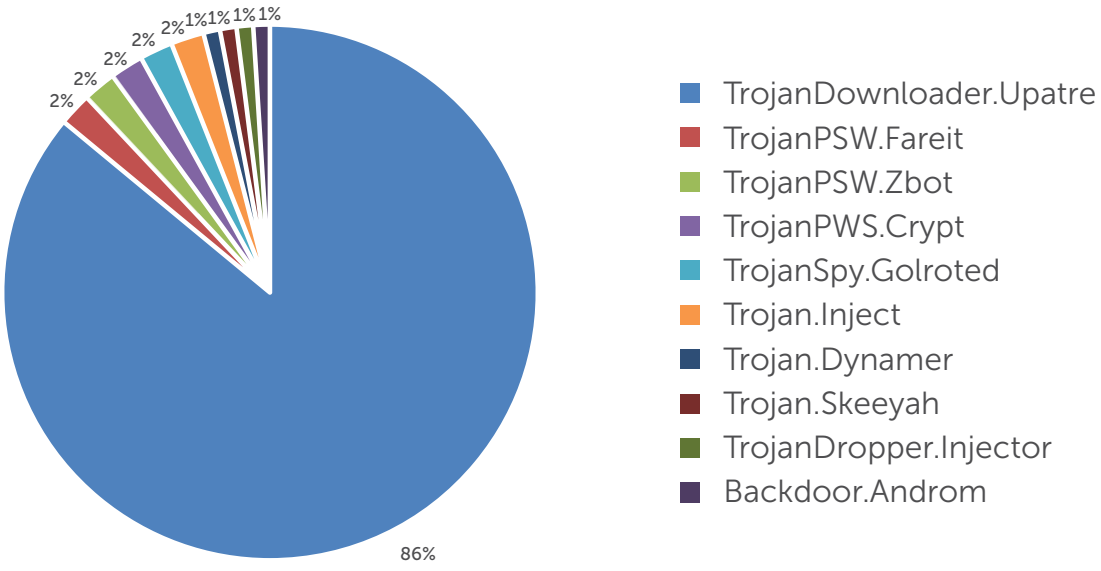
Quarter	Percentage
Q1-15	30%
Q2-15	34%
Q3-15	36%

When these emails are received and opened by unsuspecting users, they contain attachments of various types. Since some of these attachments came with familiar looking extensions, some people ended up downloading them on their systems and this caused complications to arise. The different file types that were discovered as attachments of these malicious emails are as follows:

Type	Percentage
OLE, PDF, XML	9%
ARCHIVE	91%

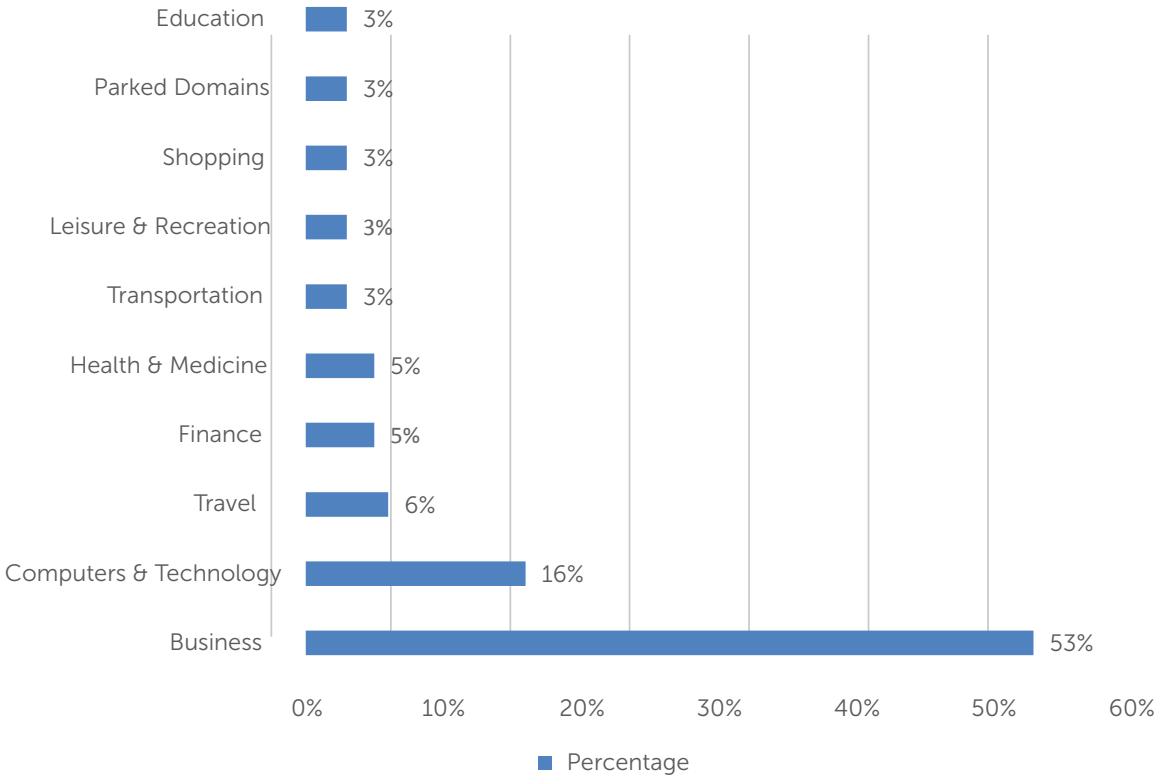
Upon further analysis by the Threat Research team at Quick Heal, the top 10 targeted malware families that were discovered in these malicious emails from Q3 2015 are listed below.

Statistics of Top 10 Malware Families of Email



A lot of spear phishing campaigns and targeted attacks were aimed at several industries of all sizes and here are the top 10 targeted industries from the months of July, August and September 2015.

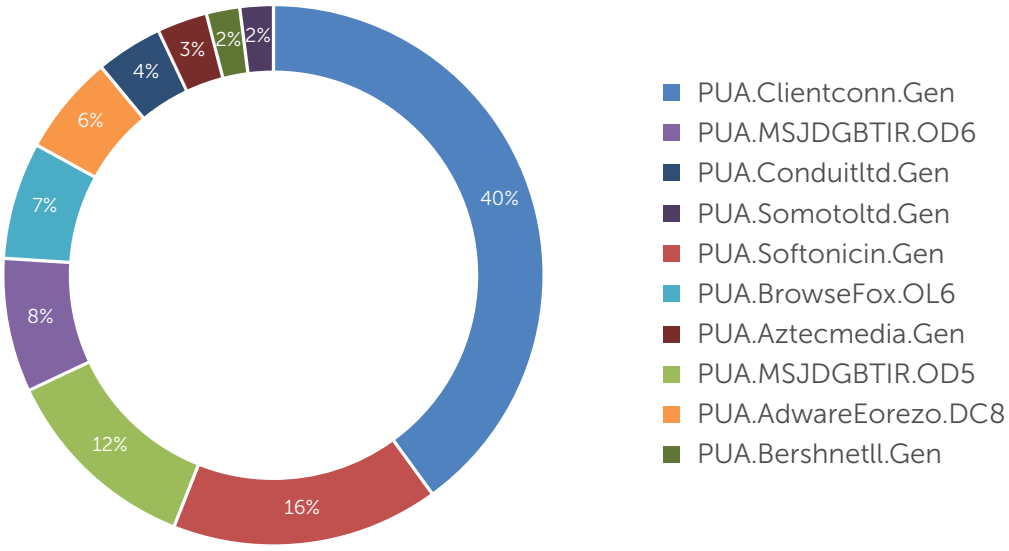
Statistics of Top Targeted Industries



Digitally Signed File

Detection Statistics

Digitally Signed File Detection Statistics Shown below are the detailed statistics for the top 10 digitally signed files that were received in the Quick Heal Labs in Q3 2015.



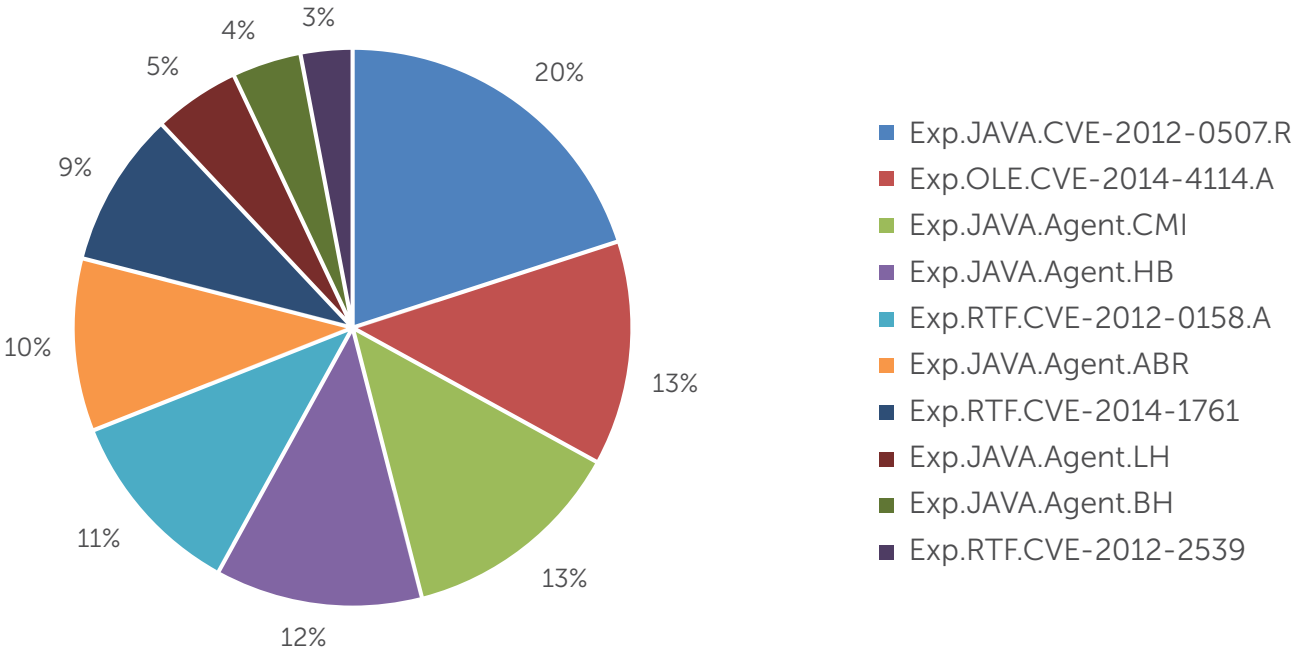
Potentially Unwanted Application (PUA) Activity

- There are several publishers who provide custom toolbars, free apps, software bundles and downloaders from third-party sites. These are the main sources.
- Distributes search protect software and browser hijacker programs.
- Installs browser plugins which lead to commercial advertisements that are disruptive and dangerous.
- Some customized toolbars modify browser search settings, change the browser default homepage and also the default search engine settings.
- Provides such programs for which the user accepts the EULA (End User License Agreement) by default while installing them.

Top 10

Windows Exploits

Given below are the detailed statistics of the top 10 targeted exploits that were received by the Quick Heal Threat Research Labs in Q3 2015.



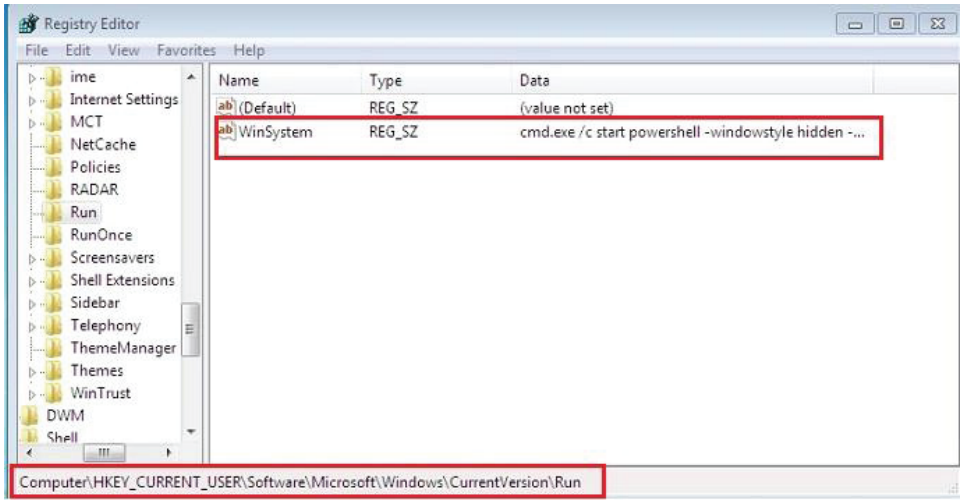
Notable Malware from Q3

Out of the many malware samples that were detected in Q3, there were 2 malware families that stood out the most during the quarter. The techniques for infiltration and evasion used by them were relatively novel in nature and we expect these tricks to be used by more malware samples in the upcoming quarter as well.

'Bedep' malware employed fileless techniques

Running malicious code directly in the memory of a system without being physically present on the disk is an innovative evolution of malware propagation tactics and this trick is referred to as "fileless malware". Poweliks was the first fileless malware to surface, and it was followed by one of its variants and subsequently the PhaseBot malware.

This fileless malware technique was seen to be used by the Bedep malware in Q3 2015. Quick Heal detected this malware as win32/Bedep malware and the variant detected directly added a malicious PoweShell code into the registry entries to remain present in the victim's computer for a long duration. The malicious code was added into systems with the key name "WinSystem".



Persistence of this malware is maintained by registering a malicious Shell Code so that each time the system gets restarted, the code will be executed in a hidden process. This makes it difficult for detection software to trace the malicious activity. Since all this malicious activity is performed directly within system memory, the registry entry is the only traceable point to detect the infection.

'StegoLoader' malware used PNG files to hide itself

Malware authors are constantly at work to evolve their techniques for spreading and propagating malware, and also for evading detection technologies. Another interesting malware from Q3 2015 was StegoLoader, which made use of digital steganography techniques to achieve success. Digital steganography is the advanced technique of hiding or encrypting private messages inside digital image files.

StegoLoader is a malware that was used by attackers to hide malicious codes inside a PNG (Portable Network Graphics) image file. In order to infect the system, an embedded malicious code is extracted and decrypted using the RC4 algorithm and a self-contained key. The extracted malicious code is directly written into the system memory and run from there and

this makes it extremely difficult for security software to detect the presence of the malicious code.

The primary purpose behind this malware was found to be information stealing. Moreover, another infection vector of the malware was bundled software obtained from third-party sources. While such attacks have only just begun, they are expected to rise in number going forward.

Case Study:
Dridex Banking Malware Focusing on New Evasion Techniques

'Dridex' is an infamous banking malware that was first discovered in 2014 and is still active in-the-wild. Recently, this malware variant was found to be focusing more on employing new propagation techniques and evasion methods to avoid security software. Dridex is a direct descendant of the 'Cridex' banking malware and it reaches its victims via spam emails with Macro embedded Microsoft Word documents as attachments. Once Dridex has infiltrated a system, it steals banking credentials and other personal information from the system to gain access to the financial information of the victim.

Infection

The spam emails that enable Dridex to propagate are delivered to vulnerable systems and are composed so as to look like they have been sent by legitimate companies and are related to the user's financial accounts. The attachment is simply a Word document that contains malicious Macro code. When a victim opens the document, a blank document gets opened. At the same time, it tells the user to 'Enable the Macro' in order to view the contents. Once the user does this, the crafted Macro is executed and the Dridex malware is downloaded into the system. Once installed, Dridex keeps monitoring user activities that are related to online banking. A list of banks is maintained in a configuration file. Finally, data theft is conducted either by taking screenshots or by the site injection method.

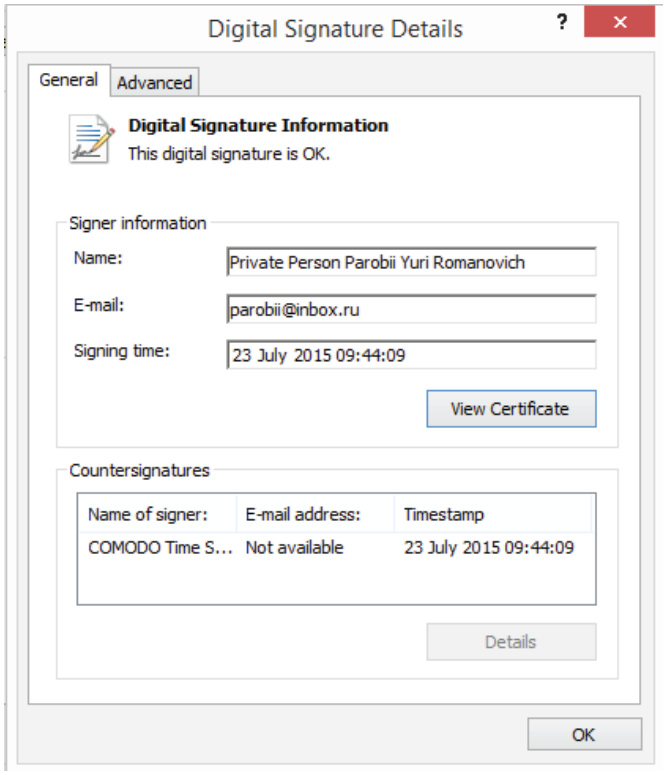
Listens for AutoClose Method

Recently spotted variants of Dridex malware have been found to be delivered via spam emails, but with a slight alteration in their infection technique. These Dridex variants do not execute until the malicious document is actually closed. The malware also have an AutoClose method embedded within, which makes it possible for the malware to go undetected from security software installed on the machine. When the attached document is opened, and the user has enabled the Macro upon prompting by the malicious attachment, then no malicious activity is

performed as long as the document stays open. The malicious Macro code waits for the document to be closed to execute its malicious activity. This method is highly effective against Sandbox detection. However, the technique is not used at the first time of asking and if the Sandbox is waiting for a long time but is closed before the malicious document gets closed, the infection successfully takes place.

Use of Digitally Signed Certificates

Dridex is a famous banking malware that has been found to be digitally signed. This technique is commonly used by malware authors to make the malware look like legitimate software.



The files related to the malware are found to be signed by one of the following names:

- PJSC “BIZNES AVTOMATYKA”
- Private Person Parobii Yuri Romanovich
- AVTOZVIT Scientific Production Private Company

Dridex malware has also been discovered to make constant network contact with several IP addresses. The list of these IP addresses is maintained in one of its configuration files which are embedded in the sample itself. With the help of this technique, Dridex tries to evade detection from security products and convinces them to treat Dridex as a legitimate application.

Dridex authors are constantly changing their approaches in order to target their victims and are thus focusing on tricking users and bypassing security checks. Proactive approaches should thus be employed by security firms to tackle such cases.

Upcoming Trends for Windows Malware

1. Adware: Delivers what the user wants, but does what the attacker wants

Offers, promotions and discounts have become very common over the Internet and these are great crowd pullers and click-baiters. With the boom in online ads and presence of brands, it has become very simple for attackers to display all kinds of ads and make them very appealing for web users to click on. With the holiday season also just around the corner, it is expected that Adware authors will add more sophistication to their tricks. Email inboxes of users could also be bombarded with promotional offers and enticing subject lines, and these mails could potentially contain URLs that redirect users to malicious websites. These advanced and enhanced propagation techniques pose a serious risk to Internet users all around. It is also expected that dangerous 'Malvertising' techniques will also hit systems with advanced data stealing malware and ransomware as well.

2. Ransomware will continue its dominance as a profit maker

Ransomware has already proven itself as one of the most effective malware types and this is expected to continue further. It is anticipated that ransomware will encrypt more data and hold it hostage. Moreover, ransomware can also broaden its business from user systems to webpage database encryption or backed up data encryption, also known as "RansomWeb". This will pose serious risks to the critical data of enterprises and business entities.

The Internet of Things (IoT) has also made it possible to connect electronic devices to a centralized network. Attackers are well aware of this and have long been preparing their strategies for infiltrating these devices that are embedded within the homes of their potential victims.

Old ransomware samples like CryptoWall 3.0, TorrentLocker, TeslaCrypt and more have already showcased their impact and capabilities by replicating themselves with improved propagation, encryption and anti-detection techniques. This is expected to continue in the 4th quarter of 2015 as well.

3. APT attacks: Serious challenge for security products

Advanced Persistent Threats (APTs) are extremely hard to detect since they function very slowly over a period of many years. They are also highly sophisticated in nature and allow the authors of the attacks to gain unauthorized access to a particular network or organization. APTs then remain undetected for long periods and slowly steal critical data from the victims.

The recently discovered "Digitally Signed Dridex Campaign" is one such APT that has come to the fore recently. Dridex is a famous banking malware and the details of this case are mentioned in the previous section of this report.

Some other recently discovered APTs are Operation Liberpy, Hammertoss and SeaDask. More advanced attacks are expected in the upcoming weeks/months and they will pose a more severe challenge for security products.

CONCLUSION

This Quick Heal Threat Report from Q3 2015 highlights plenty of key findings and trends from the preceding three months. It remains to be seen whether some of these threats can be eradicated by adopting effective and proven security strategies. However, the reality is that as one threat dissipates, another one rises up in its place. The security industry is a constantly evolving real-time battleground where all parties are constantly attempting to get one over each other.

The best tool for users here though is awareness. It pays to be in-the-know and to be aware of what threat can enter a system and through which channel. This knowledge helps people stay on top of constantly changing threats, and it also enables them to secure their sensitive data and their privacy. The Quick Heal Threat Research Labs are constantly receiving, compiling and analyzing malware variants, and this information is then shared in order to create efficient, effective and proactive security solutions for our users. However, the need for awareness and effective security measures cannot be overlooked.