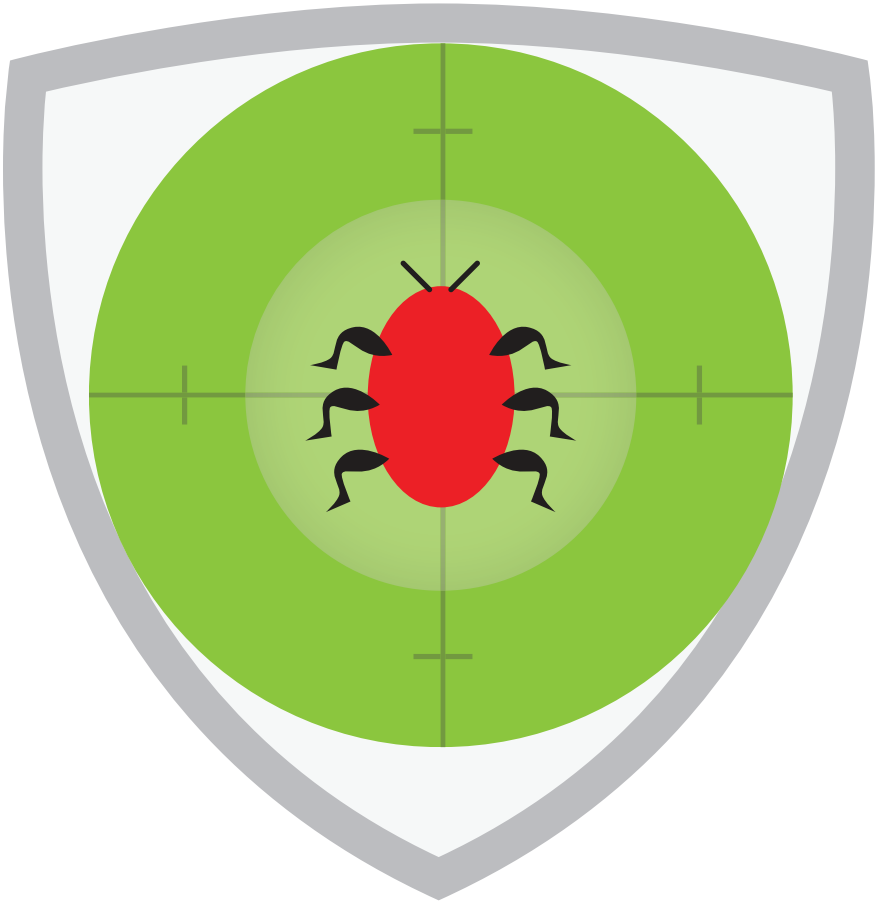
Quick Heal
Security Simplified

SEQRITE
Enterprise Security Solutions by Quick Heal



Quick Heal Quarterly Threat Report | Q1 2017

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:

Introduction

In Q1 2017, about 295 million malware samples were detected on the systems of Quick Heal users - February clocked the highest number of detection. Compared with Q1 2016, however, this quarter saw a drop of 13.61% in the detection count. Trojan horse malware family continues the tradition of having the highest detection of all, followed by infectors, worms, and adware. Quick Heal Labs detected 10 new ransomware families in this quarter. A notable observation was made against a ransomware that uses NSIS installers (Nullsoft Scriptable Install System, a professional open source system to create Windows installers) to evade antivirus software. In targeted attacks observed in Q1 2017, malware that made news included 'EyePyramid', a Dridex banking malware variant, and the Windows version of the infamous botnet Mirai. Speaking of the Android platform, Quick Heal Labs received over 2 million samples - an increase of 31% in comparison with Q1 2016. Third-party app stores were found to be the most common source of malware in the top 10 Android malware list. Compared with Q1 2016, Q1 2017 registered a massive growth of 200% of Android ransomware. The growth of Android Banking Trojans has been 10% less than the growth observed in Q1 last year. Important trends and predictions to watch out for include evolution of ransomware, targeted attacks on IoT devices, Cloud services, and rising security vulnerabilities on Android devices.

Contents

Contributors:

Anita Ladkat
Dipali Zure
Lishoy Mathew
Pranali More
Prashil Moon
Priyanka Dhasade
Sagar Kadam
Shraddha Khedkar
Tejas Girme
Leena Chaudhari
Prachi Sudame
Sanket Temgire
Sandip Borse
Swati Pharate

Windows Malware Detection Statistics

In Q1 2017, we detected over 295 million malware samples on our users' machines.

Compared with Q1 2016, Q1 2017 registered a drop of 13.61% in the detection count of Windows malware samples.

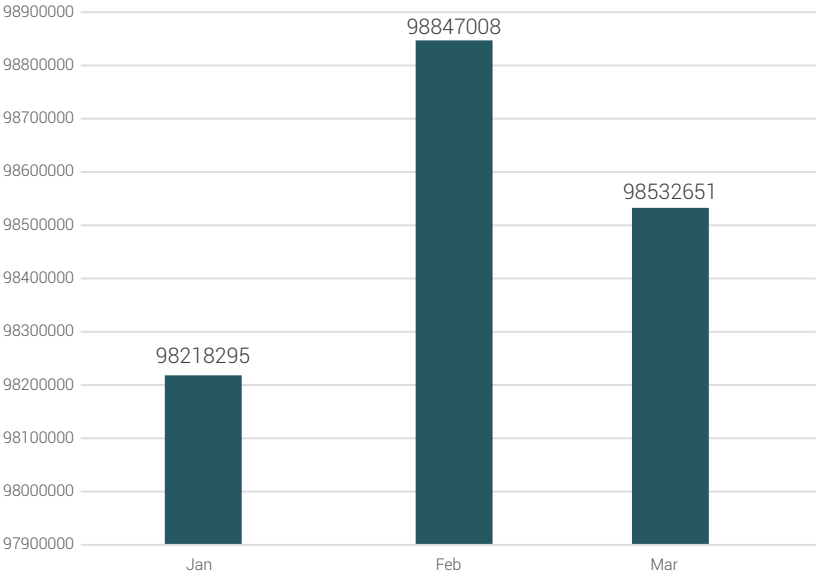


Fig 1

Top 10 Windows Malware

These are the top 10 Windows malware detected by Quick Heal in Q1 2017.

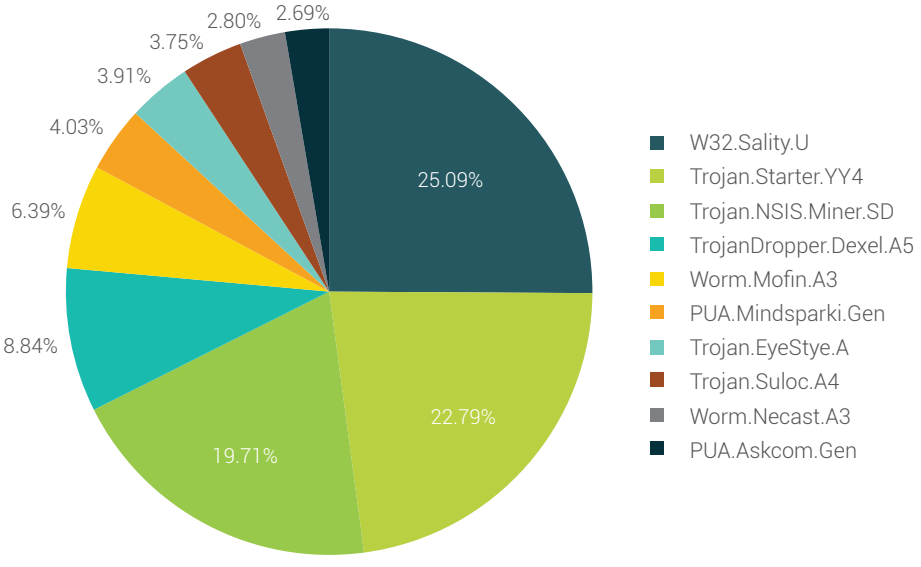


Fig 2

Share this Report

Top 10 Windows Malware

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. Trojan.Starter.YY4

Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites
Behavior:

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

3. Trojan.NSIS.Miner.SD

Threat Level: High
Category: Trojan
Method of Propagation: Bundled software and freeware
Behavior:

- Enters a targeted system through hacked websites or unverified links.
- Downloads or installs free software from malicious websites.
- Automatically executes when the system starts.
- Modifies important system files and Windows registry settings.
- Makes excessive use of system resources for bitcoin mining which further degrades the infected system's performance.
- Opens a backdoor for other malware to enter the infected system.

4. TrojanDropper.Dexel.A5

Threat Level: High
Category: Trojan
Method of Propagation: Email attachments and malicious websites
Behavior:

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

> We're in the stone age of cyber security. Real learning will only come after the 1st major incident.
>
> – Dr Christopher Frei, Secretary General of World Energy Council

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 in infected drives which contain 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.
- Copies the files it finds and sends them via an SMTP to the attacker.

6. 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.

7. Trojan.EyeStye.A

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

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

> Only after users have been fake-phished will they really pay attention to the training.
>
> – Todd Fitzgerald, Grant Thornton International global director of Information Security

8. Trojan.Suloc.A4

Threat Level: High
Category: Trojan
Method of Propagation: Bundled software and freeware
Behavior:

- Modifies system settings.
- Consumes more system resources leading to poor system performance.
- Invites other malware into the infected system like spyware, keyloggers, and other harmful infections.
- While browsing, it redirects the user to malicious websites which trigger the download of malicious content.
- Spreads through the network and infects other connected computers.
- Can cause a computer to crash or shut down abruptly.

9. Worm.Necast.A3

Threat Level: Medium
Category: Worm
Method of Propagation: Spam emails and malicious websites
Behavior:

- Infects a computer via spam emails or when a user visits a website that is loaded with exploits.

- Comes attached with freeware. It does not need to attach itself to the host program in order to perform its operation. It simply takes advantage of network connections in order to reproduce copies of itself and propagate parts of itself onto other systems.
- Exploits the infected system's vulnerabilities so that it can drop and install additional threats such as Trojans, keyloggers, fake antivirus programs, and even ransomware.
- Helps remote attackers misuse the infected system's vulnerabilities to access the compromised machine without the user's knowledge and consent.

W32.Sality.U was the top 2 Windows malware detected in Q1 2016 (23%) and it has moved to the top position in Q1 2017 (25.09%).

10. PUA.Askcom.Gen

Threat Level: Low
Category: Potentially Unwanted Application
Method of Propagation: Bundled software and freeware
Behavior:

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

Malware Category-wise Detection Statistics

The below graph represents the statistics of the categories of Windows malware that were detected by Quick Heal in Q1 2017.

Detections in descending order (average):
Trojan: 37% | Adware & PUA: 24% | Infector: 21%
Worm: 14%

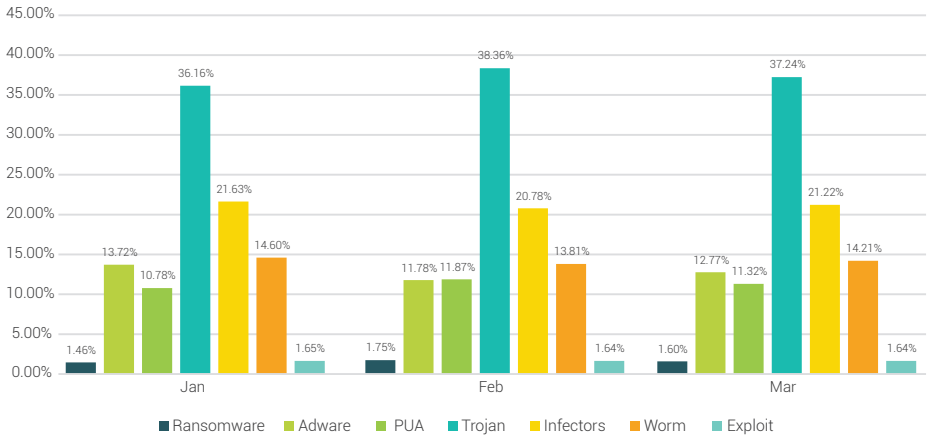


Fig 3

Top 10 Potentially Unwanted Applications and Adware

Potentially Unwanted Applications (PUAs) are not necessarily harmful but might lead to security concerns when used. Adware are software used to display ads to users - some are legitimate while some are used to drop spyware that steals user information.

These are the top 10 PUAs and Adware samples detected by Quick Heal in Q1 2017.

PUA.Mindsparki.Gen topped the PUAs and Adware list in Q1 2016 (36%) and it has retained its place in Q1 2017 with a slightly reduced detection rate of 25.58%.

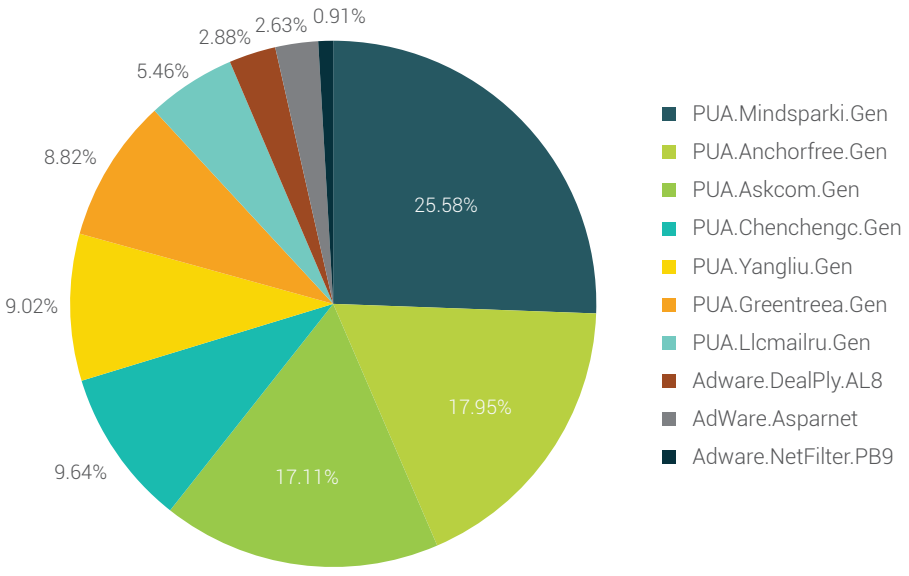


Fig 4

Share this Report

Newly observed Adware and PUAs in Q1 2017

Adware.DealPly

Comes with third-party bundled installer applications and software downloaders. It injects advertising banners on web pages visited by users.

PUA.Chenchengc.Gen

Enters into a user's computer without their knowledge. It gets installed with the name 'WinZipper' or 'QKSee' or both.

PUA.Yangliu.Gen

Comes with third-party bundled software. It shows ads and pop-ups on web browsers, may change browser homepage and redirect the user to advertisement websites.

PUA.Llcmailru.Gen

Changes browser settings like homepage and search engine; also adds unwanted toolbars.

Top 10 Windows Exploits

A computer exploit is defined as an attack designed by a hacker to take advantage of a particular security vulnerability the targeted system has.

These are the top 10 Windows exploits of Q1 2017.

Exp.OLE.CVE-2014-6352.A was at the top of the list in Q1 2016 (31%) and it has retained its position in Q1 2017 with a reduced detection rate of 27.41%.

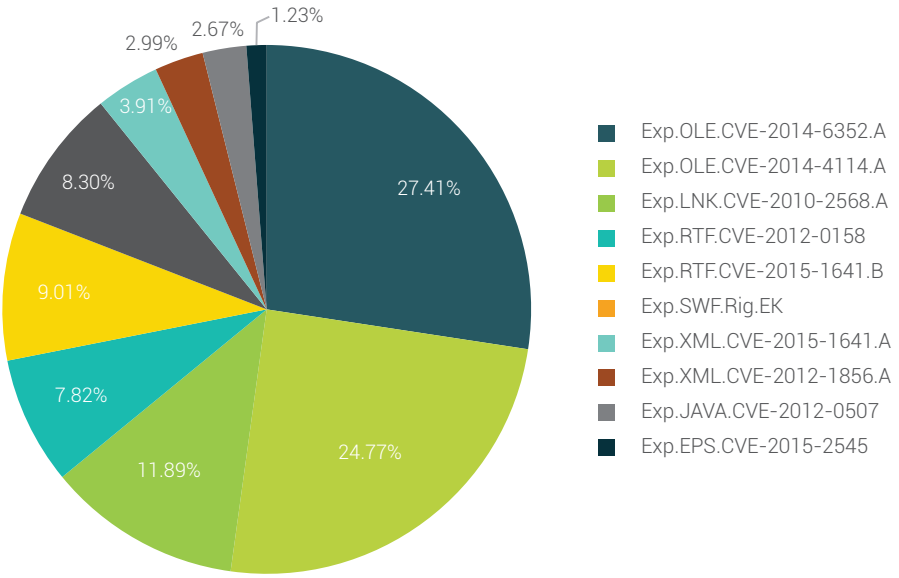


Fig 5

Major Windows Malware

Ransomware

Ransomware is a malware that locks an infected system's desktop screen or encrypts the data stored on it. It then demands a ransom for letting go of the system or the data.

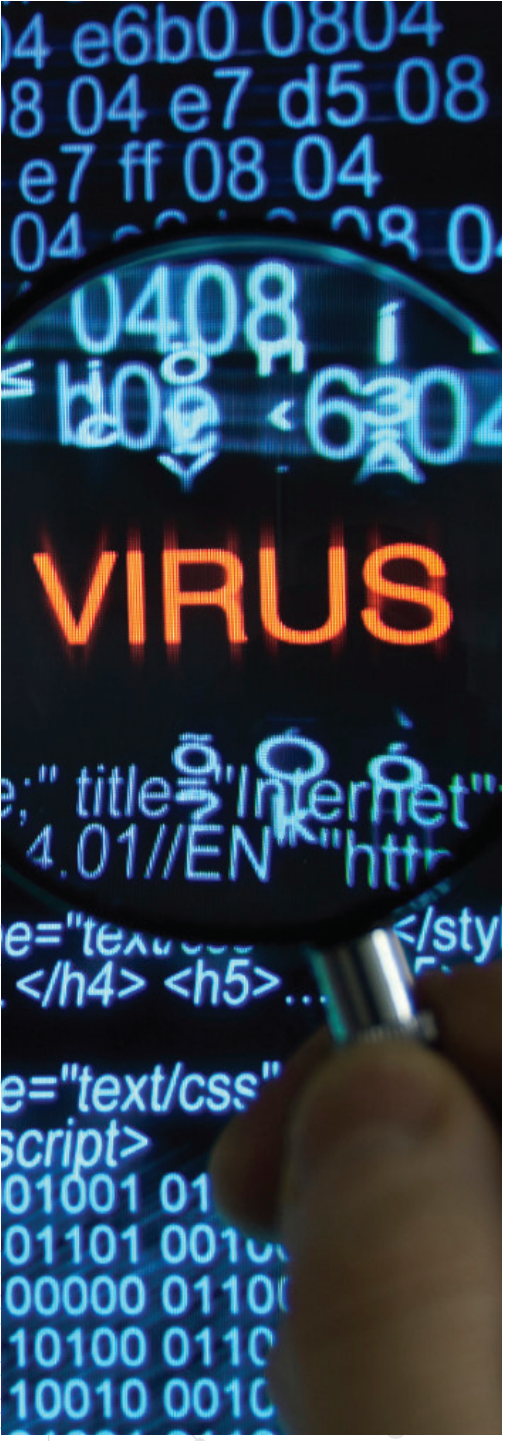
- One of the widespread ransomware observed in Q1 2017 is the Dharma Ransomware, a decedent of the Crysis Ransomware. Files encrypted by this malware have the '.dharma' extension. As observed by Quick Heal Threat Research Labs, the master key of this ransomware has been leaked. We have used the key to develop a Decryption Tool to help affected users. The tool can now be downloaded for free by clicking on the link given below:
  http://www.quickheal.co.in/free-ransomware-decryption-tool/

- Globe Ransomware is another malware that was found to be hacking into the victim's system with Remote Desktop services. As of now, three versions of this ransomware have been observed. Each one uses its own set of extensions to append the files they encrypt. Quick Heal Labs was able to develop a tool which can decrypt files having some of these extensions. The tool can be downloaded from the link given below:
  http://bit.ly/2mQFrKp

- New ransomware strains observed in Q1 2017
  - Sage 2.0
  - Satan
  - MerryChristmas
  - Opentoyou
  - FireCrypt
  - CryptoShield 1.0
  - Cancer
  - JobCrypt
  - Zyka
  - Spora

- Ransomware encrypted in NSIS installers

  It has been observed in the last few months that ransomware creators are extensively using NSIS installers (Nullsoft Scriptable Install System - a professional open source system to create Windows installers) with embedded components for encryption to evade antivirus detections. The embedded component in the NSIS installer is a custom DLL which is accompanied by an encrypted component having file sizes varying from 20 KB to 800 KB. The DLL component is used to decrypt the encrypted component which is the actual ransomware payload. This payload remains in the process memory and is never dropped onto the disk. From the analyzed ransomware samples and embedded NSIS components, the following two encryption mechanisms have been observed which are evolving with time.



1. **Usage of custom decryption algorithm**
   The encrypted component itself follows a specific file structure which contains initial garbage bytes. It is followed by a hard-coded key which is of a fixed size. Furthermore, it has a list of Windows Functions a.k.a. APIs which are used for process code injection. The actual ransomware payload is stored in an encrypted form in the file. The decryption is performed by using specific keys and custom decryption algorithm and APIs.

2. **Usage of Windows Crypto APIs**
   The encrypted component from NSIS contains an encrypted ransomware payload which can be decrypted using Windows Crypto APIs. The symmetric algorithm like AES-256, RC2 and 3DES are used for decrypting where the key for decryption is the NSIS extracted component file name. The content obtained after decryption is an RtlCompressed executable file.

This technique was found to be effective in evading detection by security products. Ransomware families like Cerber and Locky were also using this encrypting mechanism in its initial phase to evade the detection. It has gotten more evolved with customization and is being used extensively in developing other ransomware families such as Genasom, Firecrypt, Teerac, and Troldesh.

Targeted Attacks

These attacks target a specific entity's financial and private data. These are carried out as a long-term attack running silently in breached systems and staying undetected by installed security software.

1. The EyePyramid malware was used by attackers to target many high profile Italian personnel with an attempt to steal data. Spear phishing emails were used as an infection vector to deliver malware to the victims. When installed, it can give an attacker the access to the infected system resources.

2. A variant of the infamous Dridex banking malware was observed in the beginning of Q1 2017 having UAC (User Access Control) bypass capability. With this, the malware was able to execute without alerting the user to unknown files. It drastically increased the chances of the victim getting infected with this malware and performing its stealing operations by making modifications in the infected system.

3. In 2016, we had found the Linux version of the Mirai botnet carrying out DDoS attacks on IoT devices. In Q1 2017, we came across its Windows version. This new version scans the IP addresses of the targeted devices and tries to log in to them. If logged successfully, it finds the installed Operating System and drops bots accordingly. These bots further look for other targets.

Potentially Unwanted Applications and Adware

PUAs and Adware display pop-up ads on users' computer. There are many publishers who provide custom toolbars, free applications, software bundlers or downloaders from websites other than the product publisher's website.

Attackers make use of these services to reach the user's system by bundling unwanted or harmful software without the user's knowledge. This triggers ad banners on the user's computer screen or redirection to websites hosting ads. Adware can steal information about the user's computer configuration so that they can display ads based on the user's computer configuration.

If the user falls for the bait and clicks on the displayed ads, an adware can track the ads clicked by the user or opened for a long time, displaying more ads based on this information. Some types of adware are also designed to trigger audio ads in the background.

In Q1 2017, we observed Adware that installs fake or unwanted PC optimization program. Upon installation, these programs start scanning the user's computer, show fake alerts and detections, and ask the user to fix the issues. When the user clicks on the 'fix issues' notification, they are prompted to 'buy a product'. Although this product looks like a genuine scanner, it is a fake.

> As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace.
>
> – Newton Lee, Counterterrorism and Cybersecurity

Trends and Predictions

Ransomware

- In Q2 2017, ransomware variants may continue to evolve.
- Locky Ransomware is expected to hit its targets with new and advanced variants.
- We can expect to see a drastic increase in the number of Locky samples being distributed via spam emails or exploits.
- Ransomware-as-a-Service (RaaS) type attacks may increase due to its user friendliness.
- Old ransomwares like CryptXXX, Teslacrypt, etc., have already shown their impact by replicating themselves with improved propagating capability, encryption, and anti-detection techniques; this trend is likely to continue in Q2 2017.
- Given their profitability, ransomware attacks are predicted to increase in the coming quarter.

> Newer ransomware families are more advanced and persistent. Looking at the progress of last couple of years in ransomware category it looks like this threat is going to stay for long and become more and more sophisticated and complex in years to come.
>
> – Sanjay Katkar,
> MD & CTO, Quick Heal Technologies Ltd.

Targeted Attacks

- IoT (Internet of Things) devices are expected to be hit with new botnet families. After Linux, the Windows variant of the Mirai botnet has already been discovered with new capabilities. We can expect Mirai to evolve further and target IoT devices.
- Attackers can target PoS (Point of Sale) terminals and online payment systems due to the increased use of many cashless payment options.

Adware

- Increase in theft of bank related information leading to loss of money.
- More adware may begin using audio ads.

Android Samples and their Detection Statistics

In Q1 2017, we received over 2 million Android samples.

Android samples received at Quick Heal
(Q1 2016 vs Q1 2017)

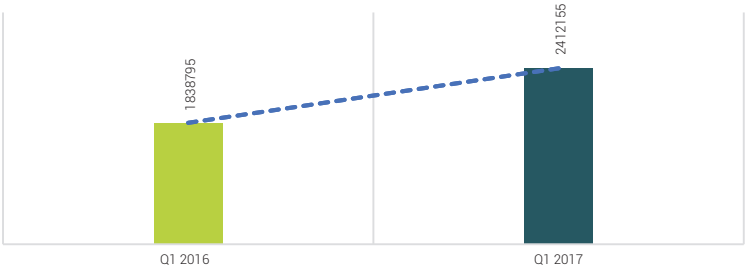


Fig 1

Android samples received at Quick Heal
(Q1 2016 vs Q1 2017) | Monthly breakdown

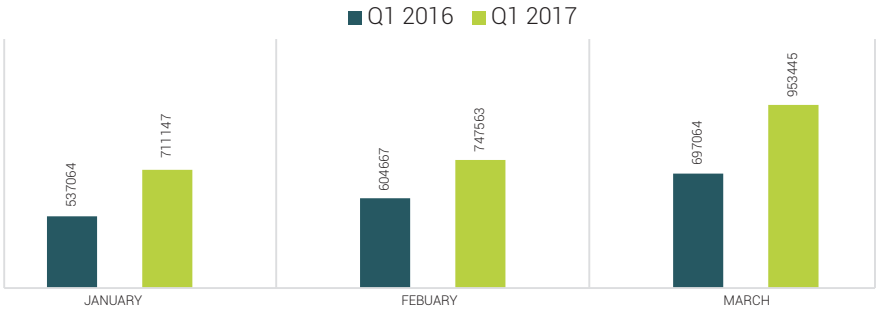


Fig 2

Compared with Q1 2016, Q1 2017 registered a rise of 31.1% in the total number of Android samples received at Quick Heal Labs (fig 2).

Category detection
(Q1 2016 vs Q1 2017)

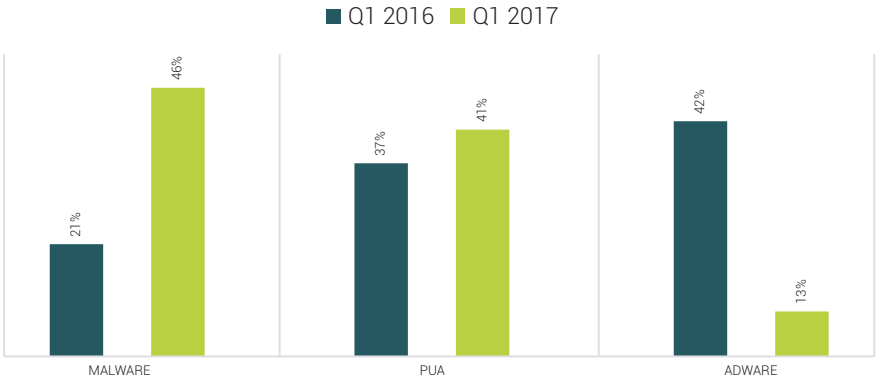
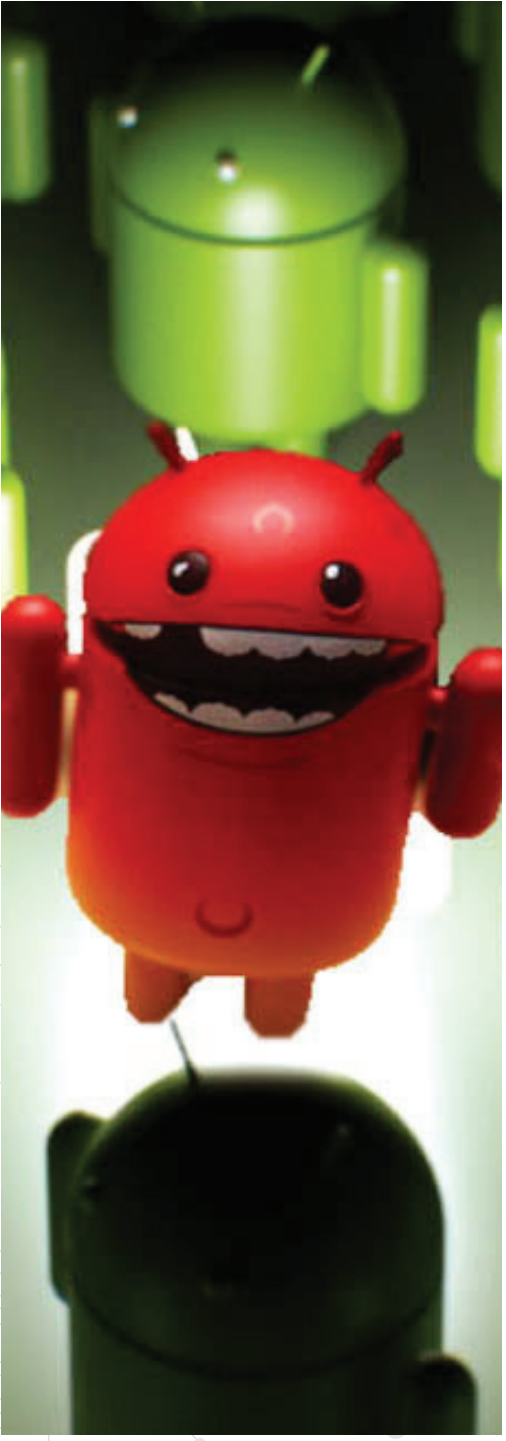


Fig 3

Malware growth has increased from 21% (Q1 2016) to 46% (Q1 2017) and so has the growth of Potentially Unwanted Applications (PUAs).

Share this Report



Top 10 Android Malware

These are the top 10 Android malware detected by Quick Heal in Q1 2017.

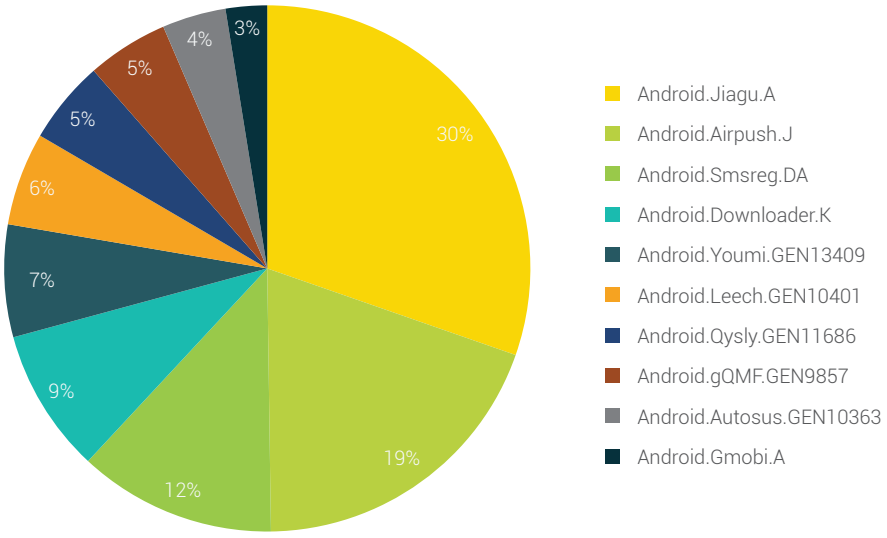


Fig 4

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 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.Smsreg.DA

Threat Level: Medium
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores
Behavior:

- Asks targeted Android users to make payments through Premium Rate SMSs in order to complete their registration.
- Collects personal information such as phone numbers, incoming SMS details, device ID, contacts list, etc., and sends it to a remote server.

> Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication.
>
> – James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology

4. Android.Downloader.K

Threat Level: High
Category: Trojan
Method of Propagation: Third-party app stores
Behavior:

- Looks like a genuine app and when opened, it redirects the user to a Google's settings web page.
- In the background, the app connects to a third-party server.
- The server responds to the app with a waiting time before it can perform further activities on the infected device.
- Once the waiting time lapses, it downloads other malicious apps on the device.

5. Android.Youmi.GEN13409

Threat Level: Low
Category: Potentially Unwanted Application (PUA)
Method of Propagation: Third-party app stores

Behavior:

- Displays 10 apps and asks the user to download them to get certain rewards.
- There is a condition not to uninstall the app for a minimum of 10 days. Even if the user abides by this condition, they receive no rewards.
- The app further recommends the user to share and earn more rewards.
- Causes unnecessary usage of mobile data.

As observed in the 'Behavior' section, most these malware are designed to collect and share device information with a third-party source.

6. Android.Leech.GEN10401

Threat Level: Medium
Category: Trojan-dropper
Method of Propagation: Third-party app stores
Behavior:

- When opened for the first time, the app hides.
- If the app is opened again, it drops other malicious apps on the device.
- Dropped files further connect to harmful URLs.
- Shares information of the infected device with a remote server.

7. Android.Qysly.GEN11686

Threat Level: High
Category: Trojan-dropper
Method of Propagation: Third-party app stores
Behavior:

- When opened for the first time, the app hides and runs in the background without the user knowing about it.
- Displays continuous ads and prompts the user to download other apps.
- Carries a file within itself which it decrypts and then executes it. This file is usually an adware.
- Creates an ad's URL shortcut on the home screen and opens the link in the browser.
- Shares information about the infected device with a remote server.

8. Android.gQMF.GEN9857

Threat Level: Medium
Category: Potential Unwanted Application (PUA)
Method of Propagation: Third-party app stores

Behavior:

- Starts displaying ads after it is opened by the user.
- If the user clicks on one of these ads, other apps are downloaded and installed on the device. These installed apps could be clean or suspicious.
- Creates a shortcut on the home screen, clicking on which automatically downloads that particular app.
- Collects and shares information about the device and installed apps with a remote server.

As always, most malicious apps are spread through third-party app stores.

9. Android.Autosus.GEN10363

Threat Level: High
Category: Trojan
Method of Propagation: Third-party app stores
Behavior:

- When opened, it prompts the user to grant 'Device Admin' privileges. Even if the user clicks on 'cancel' it keeps asking them to enable the Device Admin privileges.
- If the Device Admin privileges are granted, the app hides its icon but keeps running in the background.
- Collects all incoming SMSs and sends them to a remote server. It can also update and delete all SMSs stored on the device.
- If the user removes its Device Admin privileges, the app again starts prompting the user to enable the same.
- Shares information such as IMEI, model number, manufacture details, email ID, and Android Version with a remote server.

PUAs and Trojans comprise 80% of this list.

10. Android.Gmobi.A

Threat Level: High
Category: Adware
Method of Propagation: Third-party app stores and repacked apps
Behavior:

- Makes use of SDK to easily recompile other genuine apps.
- Downloads other apps on the device causing unnecessary memory usage.
- Shares device information such as location and email account with a remote server.
- Displays unnecessary advertisements.

Android Ransomware and Android Banking Trojans

Android ransomware works in the same fashion like Windows ransomware do. The malware can lock your device or encrypt the stored data and demand a ransom to put things back to normal.

Banking Trojans (also known as Banker Trojan-horse) are programs used to obtain sensitive information about customers who use online banking and payment systems.

Below is the statistics of Android ransomware and Android Banking Trojans detected by Quick Heal in Q1 2017.

Compared with Q1 2016, Q1 2017 registered a massive growth of 200% in the growth of Android ransomware (fig 5).

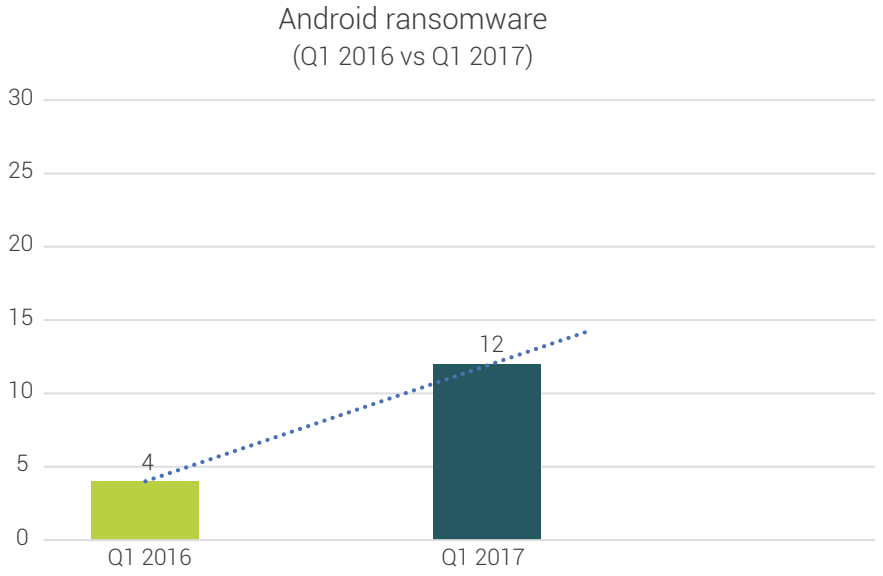


Fig 5

The growth of Android Banking Trojans, however, seemed to have mellowed down by 10% (fig 6).

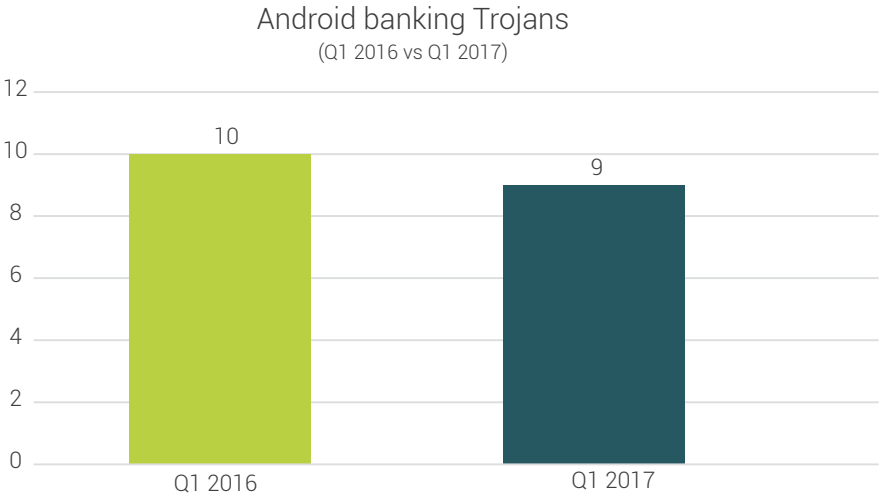
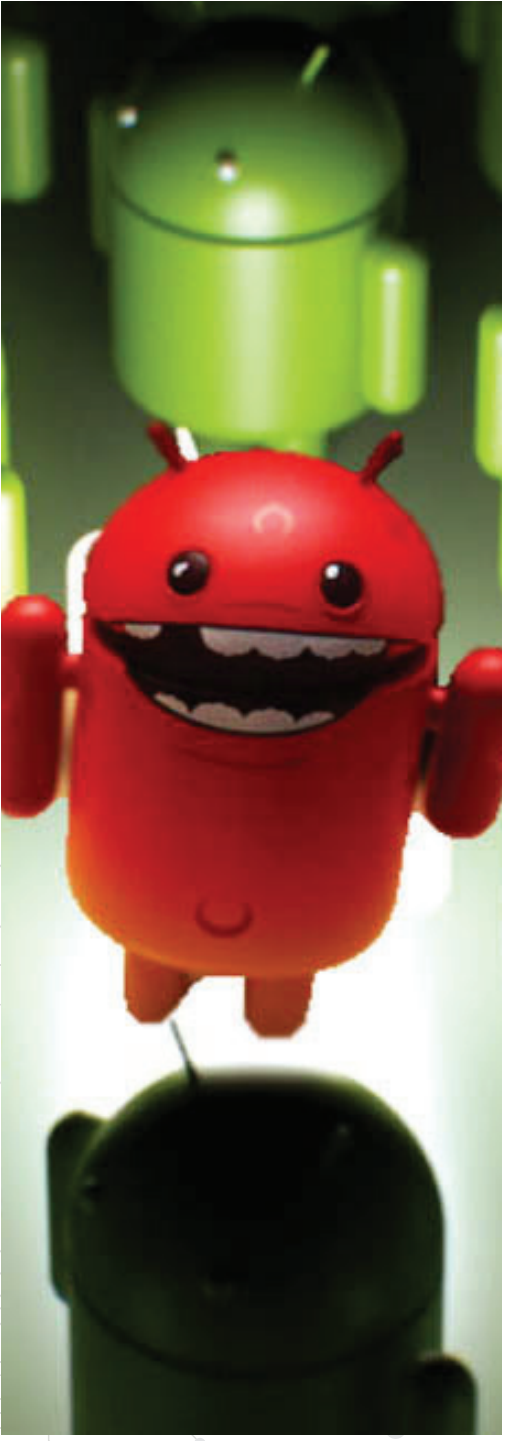


Fig 6

Share this Report



Android Malware Using Unique Techniques

I. DroidPlugin - being used by malware authors

- DroidPlugin is a framework originally developed for the purpose of hot patching.
- The popular use of DroidPlugin is to launch multiple instances of apps on the same device.
- It can directly load and launch an app from its APK file without installation.
- All plugin apps share the same UID with the host app.
- The host app has pre-defined components and permissions for plugin apps.
- Examples of malware using DroidPLugin -
  - Android.Dnotua.A (Adware)
  - Android.Iop.Z

II. Android.Boogr.A

- Has a similar icon like that of Google Play.
- Asks for administrative privileges and deletes its icon from the home screen.
- Receives commands from a C&C server.
- Checks the infected device for any banking or payment apps.
- Receives a list of attacked banking apps from its C&C server.
- Collects the list of phone numbers from the contact list and sends SMSs.
- To hide any banking transaction related messages, it forwards received messages and then deletes the original.
- Whenever the user opens apps like Whatsapp, Facebook, Viber, etc., the malware displays a 'purchase window' which seems like it is from Google Play. If the user provides any personal or banking information, it goes to the attacker.
- Also checks if any antivirus app is installed on the device.
- Collects information about the device's location.

III. Android.Spynote.A

- Uses a fake icon of Netflix App (subscription service for watching TV episodes and movies on phone).
- If clicked on, it hides and runs in the background.

- Activates the device's microphone and listens to live conversations without user knowledge.
- Records screen captures and reads SMSs and contact list.
- Shares all collected data with its C&C server.
- Can be used remotely by the attacker to root the user's device using vulnerabilities.

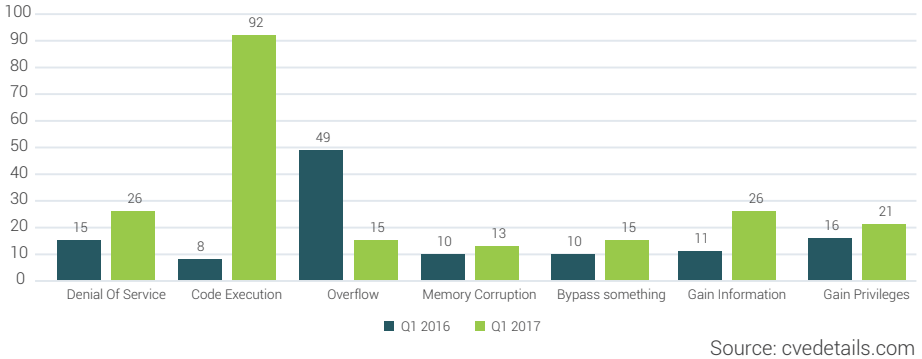
Vulnerabilities and Android OS

Compared with Q1 2016, Q1 2017 registered a giant increase of 1200% (approx.) in the security vulnerabilities used for 'Code Execution' (fig 7).

The detections of almost all vulnerabilities are higher in this quarter when compared with Q1 2016.

A security vulnerability (also known as a security hole) is a security flaw detected in a product that may leave it open to hackers and malware. Fig 7 represents the growth of security vulnerabilities in Q1 2016 vs Q1 2017.

Security vulnerabilities discovered
(Q1 2016 vs Q1 2017)



Source: cvedetails.com

Fig 7

Share this Report

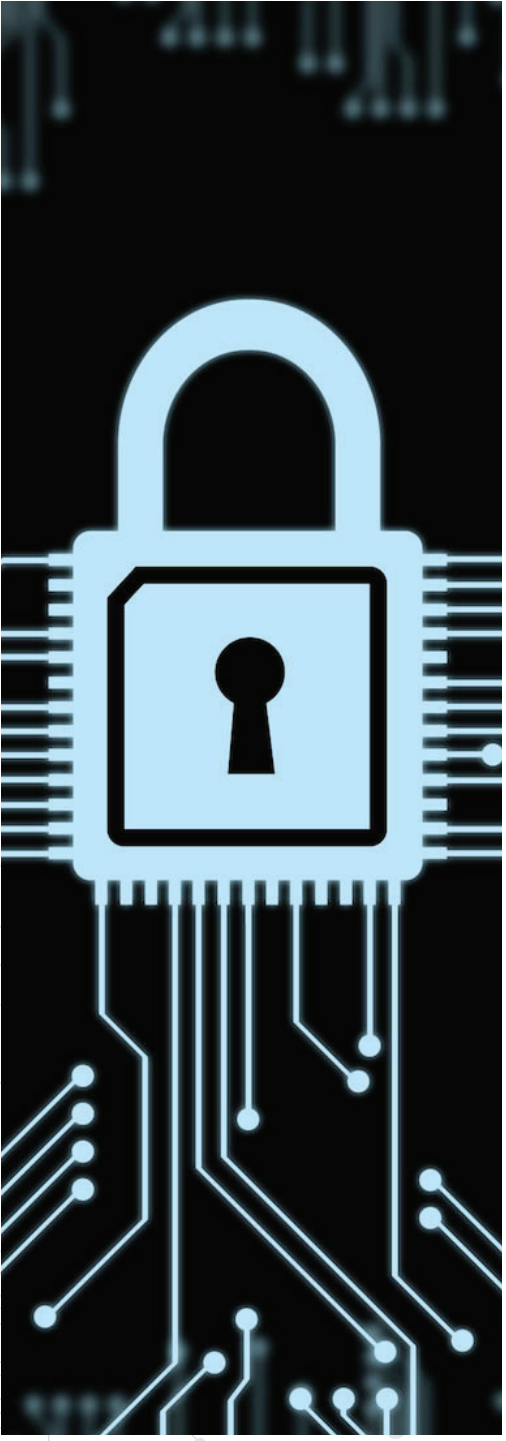
Trends and Predictions

Cloud security is a growing concern

Many organizations are making a rapid shift to Cloud due to its popularity and its scores of benefits. This means more sensitive data is being stored on Cloud every day. This trend is bound to attract the attention of attackers making way for more targeted attacks on such organizations resulting in data breaches and operational loss.

Vulnerability

Android vulnerabilities are only increasing giving attackers more reasons to target vulnerable devices and ultimately their users. And because Android malware are getting more complex with time, users cannot rely on app stores to keep a track of all vulnerabilities on their apps.



Conclusion

It's an exciting age to be alive. We are rapidly advancing towards greater heights of technology paying witness to inventions like the Internet of Things (IoT), Artificial Intelligence, Flying Cars, and the prospect of traveling to space as an excursion! The word 'exciting' fails to define these milestones mankind is achieving on its way to glory. And while the world gets drowned in the frenzy of the technology awesomeness, one particular lot keeps themselves busy, working their minds on all the things we do on the Internet - surf, chat, shop, bank, share, and so on. We're referring to the enemies of the World Wide Web and we know them as cybercriminals - always a step ahead of us and always on the lookout for their preys - individual users, businesses, government bodies; anyone and everyone who is connected to the Internet. In all our threat reports published till date, one fact which is as bright as day is that digital threats are increasing in strength and they are surely not showing any major signs of decline. Technological advancements and digital threats are directly proportional to each other. As one increases, the other grows. So, do we stop using the Internet or embracing technology for the fear of being hacked someday? We must agree, that is not an option we all have at our disposal. But what we do have is our discretion of using these tools wisely. Doing things as simple as exercising caution with unknown or unexpected emails, pop-up ads, fake news or hoaxes on social media or while sharing your personal data online, keeping your computer updated and patched, etc., can help you put yourself out of the radar of attackers. And when you couple your cybersecurity hygiene and knowledge with a reliable antivirus software, it is less likely that viruses, malware, and all other threats will find their way to you.