iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

A Study on Emerging Smartphone Malware with Special Emphasis p on the Biggest Security Events of 2016

Ritvika Singh[1]
[1]*Second year, Electronics and Communication EngineeringPunjab Engineering College(Deemed to be University)Chandigarh*

Abstract: ***Increasing demand of smartphones has led to an upsurge in its sales worldwide with more and more people embracing and relying on it to the extent of having their most confidential and sensitive data stored in it. Naturally, as the demand and production of anything shoots high, so do the problems and complexities associated with it. Cyber security experts suggest that the rampant multiplication of mobile malware being injected into the various devices and operating systems is a result of cyber criminals continuously shifting their attention to pry into our personal information.***
This paper makes an attempt to study the number and increase of mobile malware over the previous years. An attempt has been made to understand the various reasons for different number of malware reported by different operating systems viz Android, IOS, Microsoft etc. We also analyse why smartphones are more targeted than laptops and PCs. Later, we cast a glance at the major security-interfering events of 2016 namely the Mirai Botnet, Pegasus etc and the associated impacts of the same.
Keywords: Smartphone, malware, Android, Mirai Botnet, iOS

I. INTRODUCTION

The smartphone industry has been steadily developing and growing, both in market size, as well as in models and suppliers. Smartphone shipments worldwide are projected to add up to 1.71 billion in 2020. By 2018, over a third of the world's population is projected to own a smartphone, an estimated total of almost 2.53 billion smartphone users in the world and which further increase to a whopping 2.87 billion by 2020 (Statista).As the usage of smartphones per person is extraordinarily increasing across the globe at a great rate, we are depending all the more on it. According to cyber security experts, cyber criminals are increasingly focussing their attention to this most personal computer we own, the one on which we trust and rely the most for storing the most sensitive and important of our data.

"Over the last two years or so, we have seen a huge influx" in the number of hackers targeting smartphones, says Roel Schouwenberg, principal security researcher for Kaspersky Labs, a well-known anti-virus firm. Since these devices carry much of our private, personal and financial information, hackers and criminals are constantly on the lookout to gain unauthorised access to our data. The major reason for this breach of privacy stems from the fact that most of our mobile devices are not well equipped with security and anti-malware protection, thus providing an easy pathway to malware creators to pounce on email and contacts lists, monitor highly personal communications and capture vital data such as the password we type into our mobile banking app.

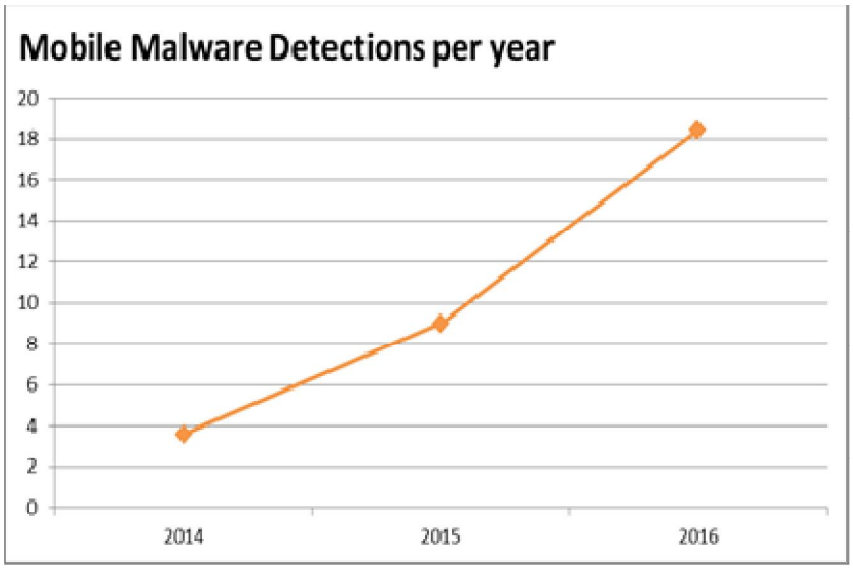
II. METHODOLOGY

Research is based mainly on secondary data which has been taken from various reliable reports. The study is basically exploratory research which is based on the analysis of the different parameters of the past year. Primarily chronological annual reports on mobile malware have been analyzed to achieve the objectives of the paper. The data for the period 2014-16 have been compiled to deduce the findings. Internet Security Theft Report, 2017 published by Symantec proved to be very instrumental.

A. Number of Mobile malware detections per year

According to Internet Security Theft Report, 2017 published by Symantec,Overall threat detections on mobile devices, including data from Symantec cloud technologies, doubled in 2016, resulting in 18.4 million mobile malware detections in 2016. However, the increase of 105 percent in 2016 was significantly smaller than the 152 percent increase in the previous year, despite the growth in smartphone adoption. This suggests that attackers are consolidating their activities, facing the consequences of the measures introduced for Android security. The following chart represents the data.

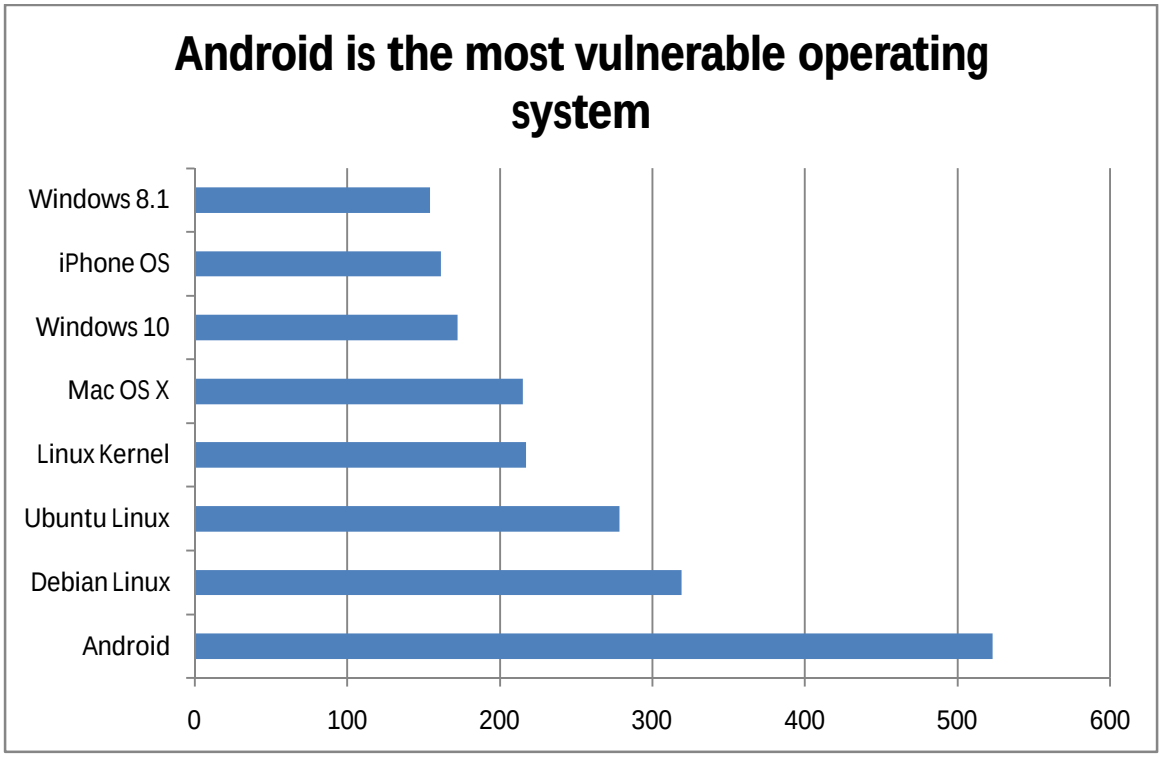
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com



The number of mobile malwares detected grew significantly in 2016. Personal Computers and laptops also comprise a major target for cybercriminals but their number is still very less as compared to malware on mobile phones.The major reason for this being isthe constant hype in the use of smartphones and our relying on our mobile phone to the extent of trusting it with our most confidentialata.

B. Android is the most vulnerable operating system

The Android operating system remains the main focus for mobile threat actors, it being the most vulnerable among all operating softwares. Attacks on the iOS operating system are still relatively rare. The given chart provided by Statista, based on CVE Details, shows the number of vulnerabilities reported by different operating systems in 2016.In this case, vulnerabilities are defined as a mistake in the software that can be directly used by a hacker to gain access to a system or network



There are many reasons for android being the most prone to cyber crime influence.

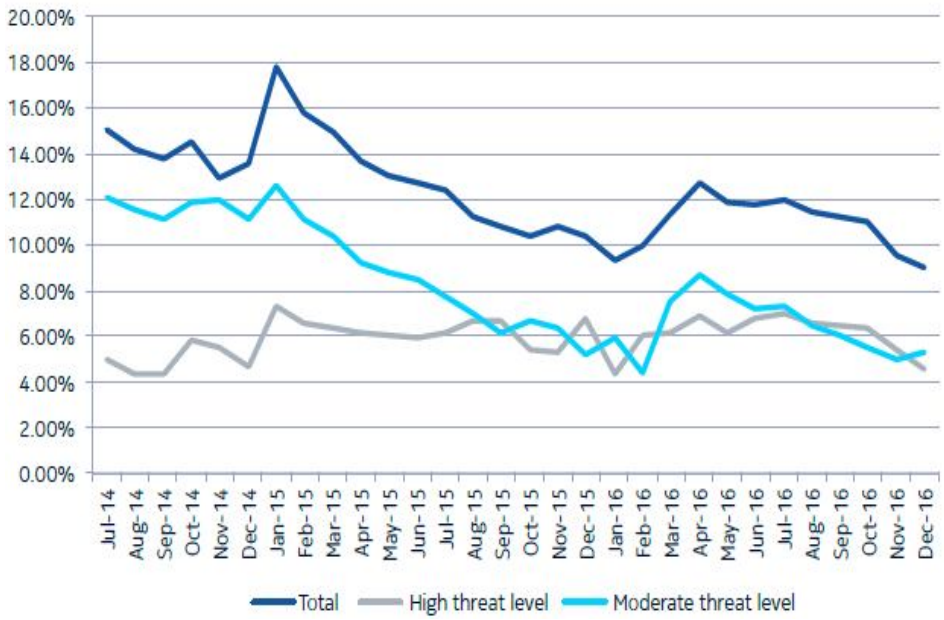
1) Android continues to be the most popular operating system and its dominance is guaranteed in the future also, thus making it the biggest target of cyber attacks.
2) One main reason for the Android's vulnerability toward threats is its openness with distributing apps and ease of enlisting as a developer. It's easy for cybercriminals to register as a developer, download apps , insert malicious code, and re-upload it to the Android Market.
3) Although Google is constantly on a lookout for developing and updating the Android Operating System, but the Android's security syestem has been created in different manner. The Android Market relies mainly on its community of developers and users to review and report any possible malicious or Trojanized versions of an app.

C. A Word about iOS

While it is a quite obvious fact that Android malware as of now, contributes to the major chunk of malicious, mobile malware,the iOS operating systemis not completely unaffected by cyber crimes. It has been reported for inspite of possible ways and methods available to create malware for iOS devices, there are a multitude of reasons why themalware developer community refrains from utilising its potential and resources against the platform.iOS and Android have very different security meausures when it comes to their application stores.Android has an open ecosystem, supervised by the Android community while Apple's App Store is tightly controlled with an upfront review process and strict terms of service that make it difficult but not impossible for malware developers to infect the App Store. Thus malware developers have lately focussed their attention on the Android platform because it reaches the largest majority of smartphone users and has breachable security barriers.

D. Malware in Fixed Residential Networks

By Residential Networks,we mean the network connections installed in the form of broadband or WiFi Routers.The given figure shows the Monthly residential infection rate recorded by networks where Nokia's NetGuard Endpoint Security solution is deployed. This is based on an analysis of traffic from more than 100 million devices deployed on both fixed, broadband and mobile networks, according to Nokia.



Residential rates continued to decline throughout 2015. Due to an upturn in moderate threat level adware activity, there was an upward trend in the first half of 2016 This, however, dropped off in the second half of 2016 and the downward trend in moderate threat level adware activity continued.The overall residential infection rate dropped to nine percent in December 2016. The infection rate for high threat level malware such as bots, ransomware, and banking Trojans has remained fairly stable at around six percent for some time, and closed out the year at 4.56 percent in December. It is very mandatory to note here that because households can have both moderate and high threat level infections at the same time, the total is not the sum of the two.

The given table shows the most prominent residential network malware

Name	Threat
Win32.Adware.MarketScoreModerate	
Android.Adware.PornClk.ATModerate	
Win32.Adware.BrowseFox.AF	Moderate
Win32.RansomWare.CryptoWall4High	
Win32.Adware.PullUpdateModerate	
Android.Adware.Ewind.DModerate	
Win32.Hijacker.DiplugemModerate	
Android.MobileSpyware.Kasandra.B	High
Win32.Adware.BrowseFox.GModerate	
Win32.Adware.InstallCoreModerate	

The decreasing trend of fixed residential network affected by malware and the continously increasing trend of mobile malware clearly suggests that though residential networks come into the ambit of malware infection, they still are not as prone as mobile devices (smartphones, primarily). Smartphones account for about 85% of the net mobile infections. Mobile devices are rapidly overtaking home devices in the number of users. These devices are replacing personal computers at home and in the workplace for everything from web surfing to ecommerce transactions to online banking.The threat vector has increased exponentially as mobile devices are used more and more to make payments. Digital wallets and other technology allowing businesses to accept mobile payments have acted as a magnet for cybercriminals.

E. A look at the biggest security threat events of 2016

1) The Mirai Botnet

The first reported attack was a 600Gbit/sec attack on Brian Krebs' security blog in late September and the French internet service and hosting provider OVH. In October,2016, a series of distributed denial-of-service (DDoS) attacks against Dyn DNS impacted the availability of a number of sites concentrated in the northeastern United States and, later, other areas of the country.The targeting of these DNS servers had localized impacts on users within these regions attempting to resolve DNS queries sent to Dyn servers. The attacks continued throughout the day in two subsequent waves: one occurring around 1:00 PM ET, and another later that evening. The two subsequent attacks were successfully mitigated by Dyn DNS and resulted in no outages, although some customers may have experienced slight delays.

2) Impacted sites include but are not limited to:

a) PayPal
b) Twitter
c) Reddit
d) GitHub
e) Amazon
f) Netflix
g) Spotify
h) RuneScape
i) CNN
j) AirBnB
k) Vox

'Mirai' is a well-planned and executed way of infecting Internet-of-Things devices, feeding them with artificial commands and causing them to shut down under a DDoS (distributed denial of service) attack — which means that the devices simply go out of order, denying performing their functions because of server overload.

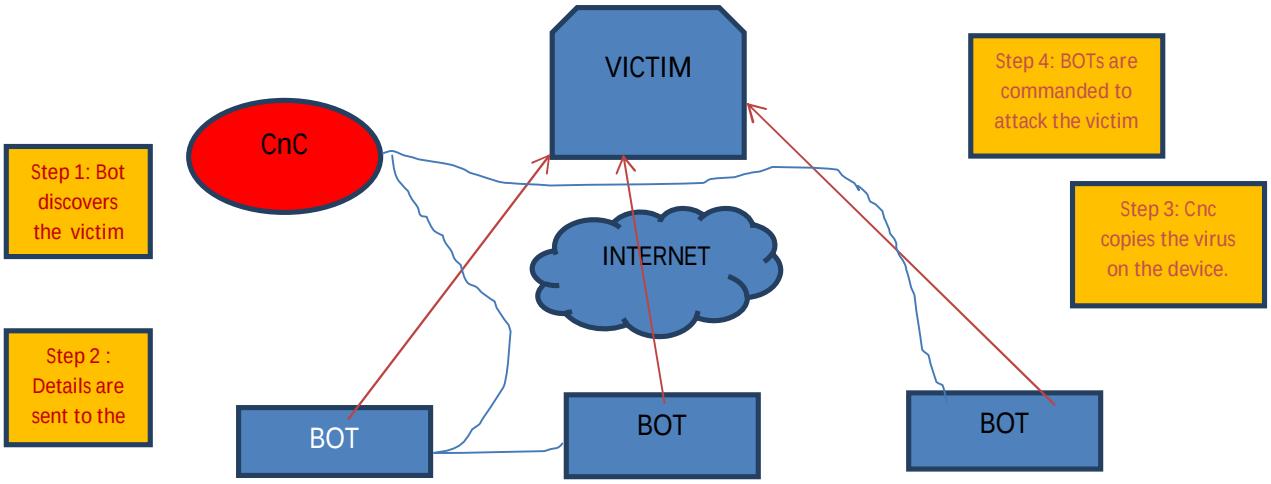
The launch of DDoS attacks by at a huge scale by the hacking community has gained momentum through the development of Internet of Things (IoT) botnets over the years. These developments have culminated in the Mirai botnets used in these attacks. Mirai targets IoT devices like routers, DVRs, and web-enabled security cameras, enslaving vast numbers of these devices into a botnet, which is then used to conduct DDoS attacks. Mirai malware has strategically targeted the right IoT devices that allow for botnets of immense size that maximize disruption potential.

F. How Mirai Targets its victim

There are two main components to Mirai, the virus itself and the command and control center (CnC). The virus contains the attack vectors, Mirai has ten vectors that it can launch, and a scanner process that actively seeks other devices to compromise. The CnC is a separate image that controls the compromised devices (BOT) sending them instructions to launch one of the attacks against one or more victims.

The scanner process runs continuously on each BOT using the telnet protocol to try and login to IP addresses at random. The login tries up to 60 different factory default username and password pairs when login succeeds the identity of the new BOT and its credentials are sent back to the CnC.

The CnC supports a simple command line interface that allows the attacker to specify an attack vector, a victim(s) IP address and an attack duration. The CnC also waits for its existing BOTs to return newly discovered device addresses and credentials which it uses to copy over the virus code and in turn create new BOTs.



This Mirai incident illustrates how vulnerable the Internet of Things can be anddemonstrates that additional security requirements are necessary to protectit from attacks and exploitation. Measures must be put in place to ensure itis securely managed, has secure communications and is monitored for future
breaches.

G. Pegasus-iPhone

In August 2016, Lookout alongwith Citizen Lab, found out"Pegasus," a kind of mobile spyware used by nation state actors to watch over high-value targets.The spyware employs a combination of phishing and three iPhone vulnerabilities (hence the name Trident) to exploit the phone remotely, compromise the device and launch a cyber-espionage attack against high profile individuals. The malware uses an immensely destructive way of taking into control communication apps such as Gmail, Facetime, Facebook, Skype and WhatsApp and monitors phone calls, SMS messages, call logs and allows remote audio and video recording.

Pegasus has been accredited to the NSO Group, an Israeli company whose only means to procure money is developing spyware. That means the malware is commercial — it's sold to whoever is willing to pay for it. Pegasus relied on a whopping three zero-day (previously unknown) vulnerabilities in iOS that allowed it to silently jailbreak the device and install surveillance software. Another cybersecurity firm, Zerodium, once offered $1 million for an iOS zero-day, so you can imagine that it cost quite a bit of money to create Pegasus.

Pegasus is modular malware. After scanning the target's device, it installs the necessary modules to read the user's messages and mail and obtain screenshots, listen to calls, log pressed keys, secede browser history, contacts, and so on. Basically, it makes an attempt to keep an eye on every activity of the its target.

Pegasus has got a wonderful ability to even listen to encrypted audio streams and read encrypted messages — thanks to its keylogging and audio recording capabilities, it was stealing messages before they were encrypted (and, for incoming messages, after decryption).

Another interesting fact about Pegasus is that it tries to hide itself really diligently. The malware self-destructs if it is not able to communicate with its command-and-control (C&C) server for more than 60 days, or if it detects that it was installed on the wrong device with the wrong SIM card.
What we can conclude from this is that inspite of the measures taken to secure the
Apple iPhone app ecosystem, the iPhone is still prone to exploits and
once jailbroken, is wide open to attack.

H. Pokemon Go and DroidJack

A big security threat event in 2016 was the release of the Pokémon Go augmented reality game has quickly proven to be a cultural phenomenon since July. At its advent,the game was available in certain countries only. Thousands of enthusiasts in other countries were desperate to get an advanced bootleg copy of the game, leading some players to install the game from third-party sources.
Now, a malicious version of the software is poised to infect Android phones with code that provides hackers a backdoor to their phones. Most Android malware comes in the form of trojanized applications that people download and install from third party app stores or websites. It is trivial, using standard Android developer tools, to take an existing application file, inject malware into it and repackage it for re-distribution to unsuspecting users.
Pokémon Go is infected with a Remote Access Trojan (RAT) called “DroidJack” that allows the attacker “full control over a victim’s phone” allowing him to track the phone’s location, record calls, take pictures and steal information and files from the phone. To the user, it is identical to the Pokémon Go game.
For the consumer, the following rules will keep them safe:
Don’t download games or any apps from untrusted third-party sites.
Install anti-virus software on your phone.
Don’t give games or apps permissions that they obviously don’t need.

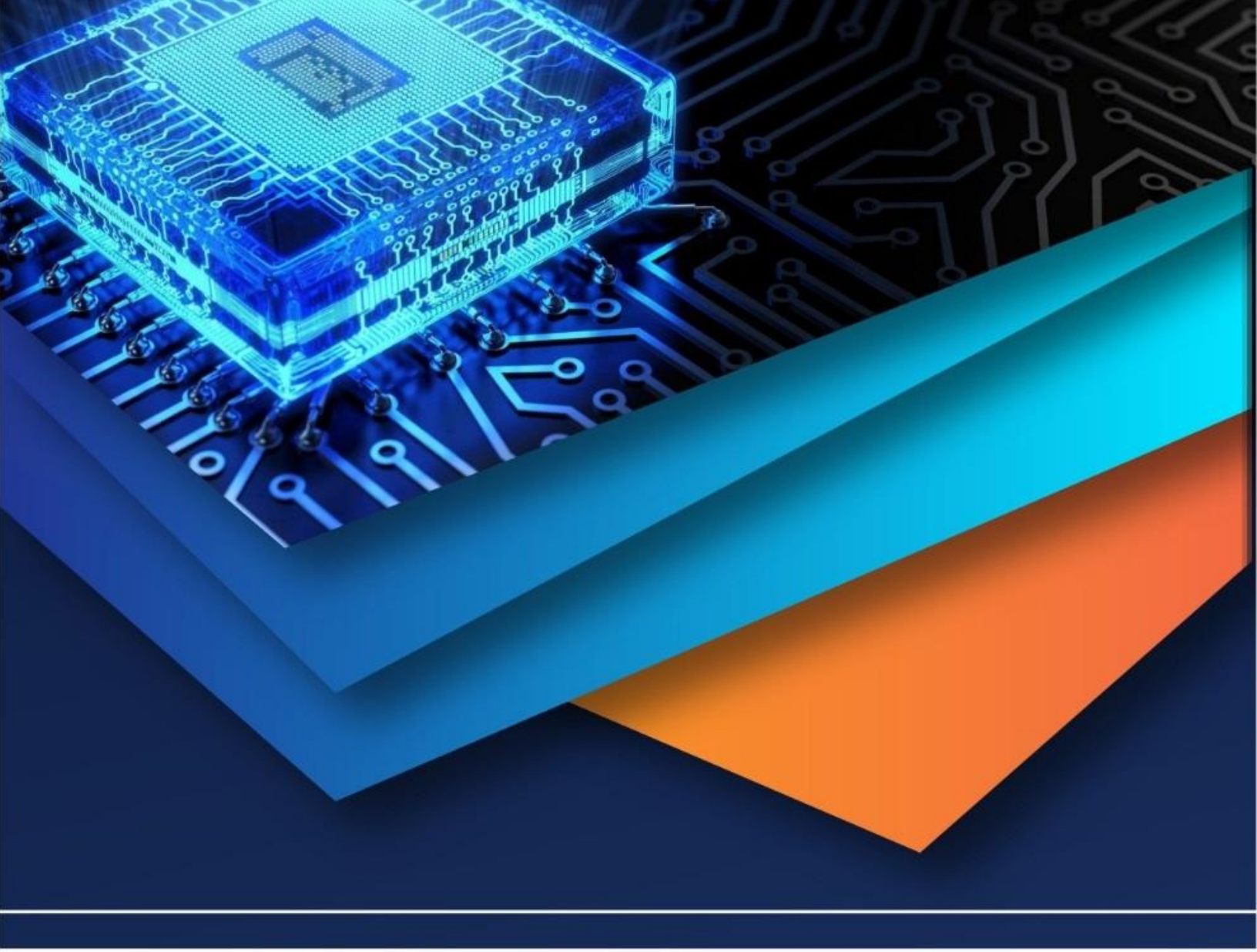
III. CONCLUSION

The number of security breaches in Android operating system has continously exceeded that in ios.As a result of this, Android has been taking serious steps to improve it’s security architecture. This creates obstructions for the malware community to inject malware into the phones.Even if they successfully infect the phone, they are not able to derive monetary benefits out of the same. As obtained from the Internet Security Theft Report, Symantec, 2017, attackers use SMS as a major source to mint money from mobile malware.However, all the versions of Android are coming up with some features or the other to improve the security system. Android 4.2 (Jelly Bean) introduced an update in 2012 that sabotaged the operation of premium SMS Trojans, which were rampant at the time. The update meant the phone would display an alert if there was an attempt to send a message to a premium phone number, greatly reducing the effectiveness of these scams.
Elsewhere, updates introduced in Android 5.0 (Lollipop) and Android 6.0 (Marshmallow) made the creation of mobile banking malware a tedious task for the attackers. Mobile banking malware works by creating overlay injections to phish the current running application, but these updates thwarted malware’s ability to find the current running task by deprecating the getRunningTasks() API. Since then, attackers have been engaged in finding workarounds to overcome these additional security measures.
Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key(trendmicro.com). Steps have been taken in Marshmallow to curb the same.
Android updates – unlike those of its rival iOS – never roll out on time, something which has been most Android users’ biggest complaint(thequint.com).Manufacturers also fail to feed the latest versions of Android on their smart phones. So, to change this once and for all, Google has decided it’s time to speed things up and deliver new Android versions much faster than before.

REFERENCES

[1] Statista.com: Android is the most vulnerable operating system.
[2] CBC News(Technology): Smartphones becoming prime target for criminal hackers.
[3] Businessinsider.in Report: Android had a tough year compared to iOS in one crucial area.
[4] Nokia Threat Intelligence Report,2016.
[5] Internet Security Theft Report, Symantec, 2016 & 2017.
[6] https://www.scmagazineuk.com/updated-97-of-malicious-mobile-malware-targets-android/article/535410/

[7] Pulse Secure, Mobile Threat Report, A Word about Apple, 2016.
[8] Mobile Threat Report: What's on the Horizon for 2016, Intel Security 2016.
[9] Anti-Virus Comparative, Mobile Security Review 2016.
[10] Toward new possibilities in threat management, How businesses are embracing a modern approach to threat management and information sharing, PWC 2017.
[11] Safeandsavvy.f-secure.com Article:Reasons-97-of-all-new-mobile-malware-is-targeting-android
[12] The security ledger: Android Malware Doubled in 2016, Adding to Mobile Malware Problem, March 2017.
[13] Sophos-Security News Trend-When Malware Goes Mobile, 2017.
[14] Flashpoint-Intel, An After-Action Analysis of the Mirai Botnet Attacks on Dyn, October 2016.
[15] How botnets are breaking into smart homes, Article16078750, Science and Technology, The Hindu website, October 2016.
[16] Heightened DDoS Threat Posed by Mirai and Other Botnets - United States Computer Emergency Readiness Team, October 2016.
[17] KrebsOnSecurity: KrebsOnSecurity Hit With Record DDoS.
[18] Sophos: Mirai "internet of things" malware from Krebs DDoS attack goes open source.
[19] ICS-CERT: Sierra Wireless Mitigations Against Mirai Malware
[20] Federal Bureau of Investigation Public Service Announcement: Internet of Things Poses Opportunities for Cyber Crime.
[21] Corero, Mirai Botnet DDoS Attack Type.
[22] Lookout Blog, Trident vulnerabilities: All the technical details in one place, November 2016.
[23] Kaspersky Lab daily, Pegasus: The ultimate spyware for iOS and Android.
[24] Fortune.com: Hackers Are Spreading Malware Through Pokémon GO, David Z Morris, July 2016.
[25] The Hacker Way: Downloading Pokémon GO Game for Android? Beware! It Could be Malicious, July 2016.
[26] IndianExpress: Pokémon GO download: Android APK file might has malware, July 2016.
[27] https://www.thequint.com/tech-and-auto/tech-news/google-new-android-version-faster-updates
[28] https://www.trendmicro.com/vinfo/us/security/definition/ransomware



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY