Mobile Viruses

Pranav R Shah
Information Technology Department, Mumbai University, Thadomal Shahani Engineering College, Bandra

Yash Shah
Information Technology Department, Mumbai University, Thadomal Shahani Engineering College, Bandra

Saurabh Madan
Information Technology Department, Mumbai University, Thadomal Shahani Engineering College, Bandra

ABSTRACT

It has just been seven years since the time when first virus was introduced in a game 'Mosquito' by a company called as Ojam. Ever since then, malware has been introduced in various ways and affecting MCDs (Mobile Computing Devices) all over the world. It has been an issue of great concern since it invades into the privacy of mobile users. Once installed in the victim's phone it can track the user's location via GPS, call other people, send SMS/MMS, gain unauthorized access to the resources or even use the mobile remotely over the 3G/Wi-Fi Internet connection. It can also cause the user to have a monetary loss without the owner even knowing anything about it. Malware can be categorized into various types-Virus, Worms, Trojan horse, Spyware, etc. They are transferred to the device by emails, messages and downloaded files. One of the characteristics of malware is self-duplication, where it creates replicas inside the device without the user noticing it. Malware can be any type of code, script, executable file or software. The malware writers have not spared any Mobile Operating System, be it Symbian (Nokia), iOS - iPhone OS, Android OS, Blackberry or Windows OS. Some of these viruses are Cabir, CommWarrior (Symbian), Rick Astley virus (iOS-iPhone OS) and SMS.AndroidOS.FakePlayer (Android OS). In this paper, we have analyzed the different types of malware and their effects on Symbian, iOS & Android, Windows, Blackberry devices. We have also suggested ways to detect and remove them.

General Terms

Operating Systems, Antivirus software, Security.

Keywords

Malware, Virus, Trojan horse, iOS-iPhone OS, Android OS.

1. INTRODUCTION

Malware derived its meaning from root word 'mal' which means bad or evil. It is short for "malicious software." The variety in malware has increased significantly (see Figure 1) from 2004 to 2008. As of March 2008, F-secure has discovered 401 different types [1] of malwares and McAfee has discovered 457 types of malware. It has a solitary target to impair the functioning of the system. The system over here could be any computer, server, or a computer network. The malware is designed in such a way that it has an ability to replicate itself without the knowledge and permission of the user. It can propagate with the help of mediums like floppy disk, CD, DVD, or USB Pen drives. Malware could be anything from viruses, worms, Trojan Horses [2], spywares, etc. They can also be transmitted by e-mails, messages, P2P (PEER TO PEER connections) [3], websites, etc. One of the first viruses that had a tremendous impact was the 'Creeper virus '. It was written by Bob Thomas. It affected all computers with TENEX OS(Operating System) after acquiring access via ARPANET-(predecessor to the Internet), got copied to the host machine and displayed a message, "I am a Creeper, catch me if you can." Another program, 'the Reaper' was created to delete the Creeper.

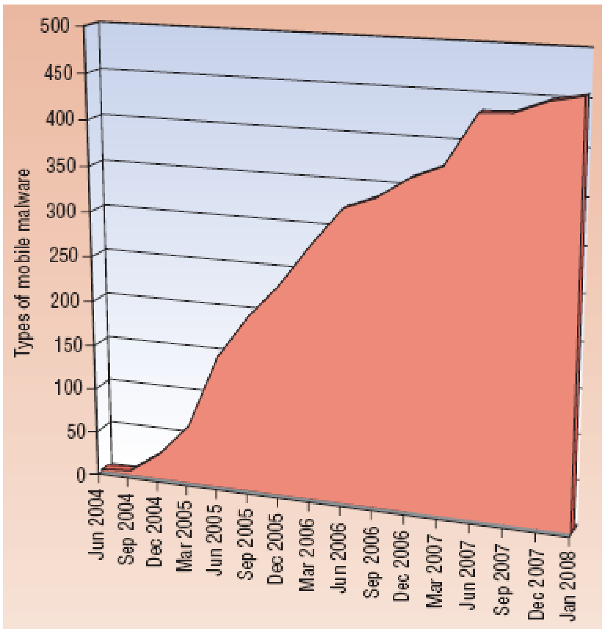


Figure 1: Increase in Malware from June 2004 to Jan 2008

2. TYPES OF MALWARE

Initially, malware was written for computer systems, but with the advent of Smartphones coming up having strikingly akin features to computers, one gradually comprehended that they were no longer immune to malicious attack. The most susceptible operating system (see Figure 2) in the history of mobile phones is Symbian. Later operating systems like iOS and Android were also affected. A list of a few malware for these operating systems is as follows [4,5]:

1. Zeus Trojan (BlackBerry)

2. Cabir (Symbian)

3. Mosquito (Symbian)

4. Skulls (Symbian)

5. CardTrap (Symbian & Windows)

6. CommWarrior (Symbian)
7. LibertyCrack (Palm)
8. Phage (Palm)
9. Vapor (Palm)
10. Rick Astley/Ikee (iPhone)
11. Duh (iPhone)
12. GG Tracker
13. Google++
14. A virus integrated in some versions of Angry Birds.

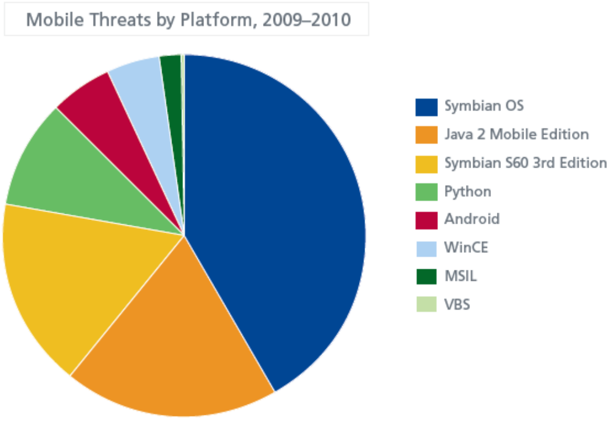
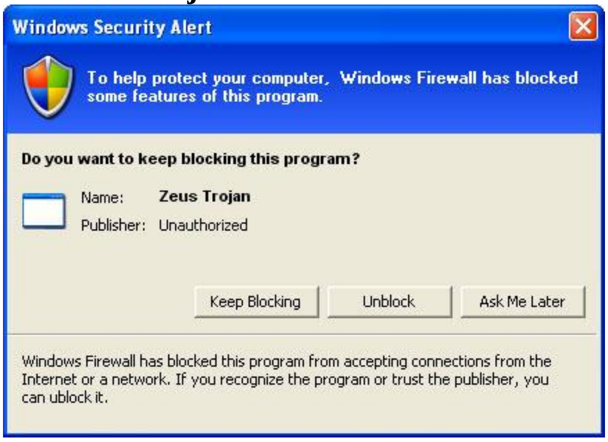


Figure 2: Market Share of various Operating Systems under McAfee

2.1 Zeus Trojan


Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: Zeus Trojan
Publisher: Unauthorized

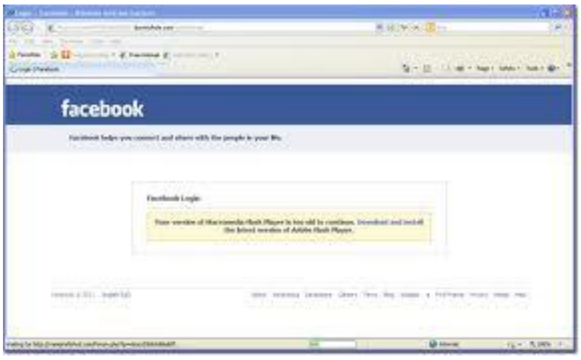
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can ublock it.

Figure 3: Zeus Trojan making way via web based service

A new study [11] has found that this virus specifically targets SMSes sent by BlackBerry's Messenger Service. A 'trojan' virus, dubbed Zeus (see Figure 3) — which appears to perform a desirable function for the user prior to run or install, but steals information or harms the system later. The ZeuS Trojan, however, has been designed specifically to tamper with Blackberry's SMS feature. The aim of the Zeus Trojan is to monitor users' private information, particularly when they conduct mobile online banking transactions. The BBOS_ZITMO.B Zeus Trojan [13] variant is very terrifying because once installed, it will then send a confirmation text message to the hacker notifying him that the infected phone is ready for remote commands.

2.1.1 Installation

There are many entry points for this virus to make inroads into this system. Very first is the email in the mask of which the malicious code is sent. Secondly the growing number of web based services also gives way to these viruses. Sometimes this virus gets installed [6] as a default one with particular software of which the user is unaware. It disables GUI and hides itself from the list of applications making it dearer for antivirus to detect it (see Figure 4). The virus is hidden with the software necessary for internet applications. Here it refers to Adobe Flash Player required for video streaming.



Facebook helps you connect and share with the people in your life.

Facebook Login

Your version of Macromedia Flash Player is too old to continue. Download and install the latest version of Adobe Flash Player.

Figure 4: Zeus Trojan making way via web application

2.1.2 Removal of Zeus Trojan Virus

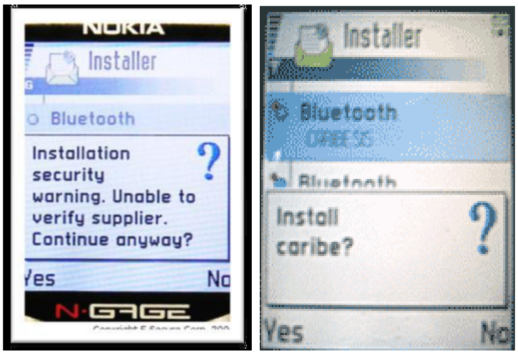
Zeus is very difficult to detect even with up-to-date antivirus software. Symantec Browser Protection can prevent some infection attempts but it remains unclear if antivirus software is effective at preventing all of its variants from taking root. Zeus Trojan Remover detects and removes all known variants of the very dangerous Zeus Trojan, also known as ZBot. When ZBot infection [7] is detected the infected file that resides on hard disk is removed immediately.

2.2 Cabir

Cabir was written by Vallez [8], a member of 29A Group. It is also called by another name Caribe. The main purpose of Cabir virus was to educate the developers that malicious code could be written for non-standard operating systems as well. Cabir (Symbian) and Dust (Windows Mobile) were first few viruses with non-intentional goals. Such malware is known as proof-of-concept viruses. Russian antivirus company KasperSky detected it in an email sent by the group. This worm was designed to infect and be transmitted by Symbian operating phones. It was a first network worm which travelled via mobile networks. The file was sent as .SIS (Symbian Installation file), but then masqueraded itself as a part of Caribe Security Manager Utility [10]. Once the file is installed (see Figure. 5, 6) it displayed the inscription Cabir on the screen of the Symbian phone. The worm was activated each time the phone rebooted. It also scanned for nearby devices using 'Bluetooth' and sent its own copy to the devices found.

2.2.1 Installation

First, the phone would display a warning dialogue. If the user would press YES [19], then the phone would ask for the normal installation.



Installation security warning. Unable to verify supplier. Continue anyway?

Install caribe?

Figure 5, 6: Installation of Cabir Virus

The worm will not be able to reach the user's mobile automatically. Only if the device to be infected is in range and the user accepts by saying 'yes', only then the virus can be installed in the phone. If the user refused to accept it, then the user would be prompted to reply till they answered a 'yes'. The replication was limited to the first user found in the scanned list, i.e. it will stop looking for more devices once a device was found. The noteworthy fact was that, Cabir infected only one device each time it was activated. Due to this reason, it spread slowly.

2.2.2 Removal of Cabir Virus

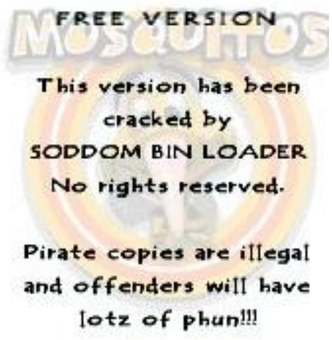
Automatic: New software called as F-Cabir [18] was made available online by f-Secure so that the users could get rid of this worm. F-Cabir could be downloaded from http://www.f-secure.com/tools/f-cabir.sis.

Manual*:* One can disinfect the system manually by installing a file manager application like (Fexplorer for Symbian) and manually delete all files from the folder Caribe →c:\system\apps\caribe\caribe.app

Reset to Factory Settings*:* To format the phone, the user would have to press *#7370# and reset the mobile to factory settings i.e. get back to it's original form when it was manufactured. This will be done, once the user enters his device security code i.e.12345 [17] default for all Nokia phones. However, it is a tedious option since it will delete all the contacts and memory from the user's phone.

2.3 Mosquito Virus

Picking up inklings from Cabir, arose the next malware-Mosquito[5]. It was a Trojan-i.e.designed for financial gain. It was concealed in a game for Symbian users. The company Ojam developed it as a copy-prevention technique. It would send messages or make calls to the company without the user aware, thus resulting in hefty mobile bills for the user. The intent was to notify the company if the game was cracked or if it was run on an unlicensed device. But after some time, it was observed that the plan had backfired[12] on the company, since it affected it's very own legitimate users. The number where the calls or messages were sent was a premium number with rates as high as $5.99 per message. After receiving lots of accusations from it's users, they cancelled the premium service on the number. Ojam claimed that they removed the 'phone home' feature from further versions and the users were safe from this feature of silent dialling. But by that time, the original version started appearing on P2P and other web sharing sites, so the users would be charged as per normal text messaging rates.The original and the cracked versions[20] can be differentiated by the message (see Figure 7).



FREE VERSION

MOSQUITOS

This version has been cracked by SODDOM BIN LOADER No rights reserved.

Pirate copies are illegal and offenders will have lotz of phun!!!

Figure 7: Installation of Mosquito Virus

2.3.1 Removal of Mosquito

One can uninstall the old version manually and download the updated version from the company website, free of this malware. The newer versions cannot function outside UK. If a user is using it in a country other than UK, it is a clear indication that it is a cracked version.

2.4 Skulls

There has been a lot of hullabaloo[20], surrounding the fact, whether Skulls was a virus or a trojan!Since it didn't propagate itself, it was not a virus.And once it was on the mobile, it didn't go anywhere in the phone so it wasn't a trojan either.But it did cause a lot of harm to the user, once it was installed. The name(Extended Theme.SIS) suggests that it was designed for the S60 Nokia phones(Nokia 7610[16],Nokia 6600,etc) since they had a large market share at that time[9].It had the ability to overwrite existing applications by exploiting the loopholes present in Symbian architecture.

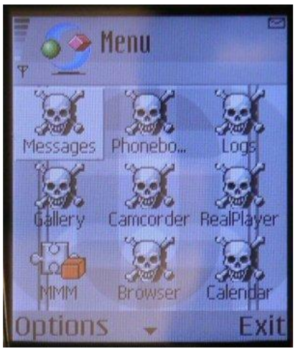


Figure 8: Installation of Skulls Virus

Once installed, the skulls supplanted normal icons[14] in the phone menu, ultimately making the entire mobile functionality disabled, except for dialling and receiving calls.All functions needing some system application such as SMS,MMS,Web browsing and camera no longer functioned.The icons resembled an image of a skull with bones(see Figure 8) similar to that normally shown in a

Danger [11] image.Symbian phones with a UIQ user interface were reported to be unaffected by this malware.The operating system has a feature causing any file in C: drive replaces the file in ROM drive with identical name and location. The application files installed by Skulls are normal Symbian OS files extracted from the phone ROM. However, due to this feature copying them into correct locations in the device C drive, causes critical system applications failure.

2.4.1 *Precaution*

If the software has been installed on the mobile, please don't reboot the phone, instead follow instructions to remove it.

2.4.2 *Removal of Skulls*

Using two phones (S60): Install f-Skulls .sis by f-Secure into memory card of a clean phone. Put MMC into the infected phone. Once started, the phone should work properly. Go to Tools-Application Manager and uninstall the Extended Theme Manager .SIS file from the phone. Now the phone should work properly.

Using the same phone: This method will work only if one has a working File Explorer (FileMan/Fexplorer) on their phone. Go to →c:\System\apps\appinst and delete app file.

2.5 CardTrap

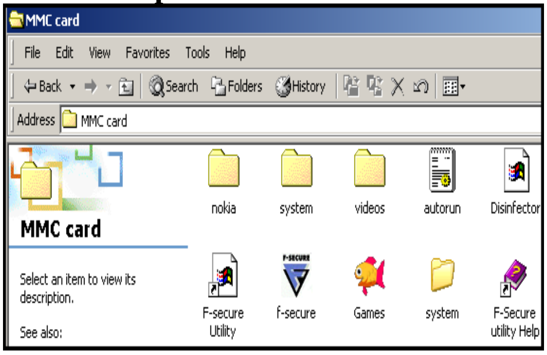
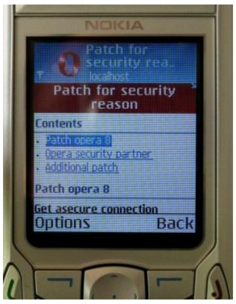


Figure 9: Computer screenshot when memory card was accessed.

CardTrap [11] was the first cross platform malware i.e. it infected two platforms, Windows and Symbian both at the same time. It dropped installers for Symbian malwares such as Cabir, Skulls, CommWarrior, Virus.Win32.Kangen, etc. It was distributed in a .SIS file which when installed disabled most of the functions like Application Manager, Browser, File Manager, Media Gallery, SMS/MMS Inbox, etc. of the mobile phone. Thus, the files in the phone's C and E (MMC) drives. On the next reboot, the overwritten applications will no longer work and the phone will be inoperable. It even tried to damage some antiviruses installed in the device and instead installed Windows viruses, worms and Trojans with the 'autorun.inf' file to the memory card [15]. 'autorun.inf'(see Figure 9) contained a script that would execute the Windows malware files automatically when phone memory card was inserted in the PC, thus transferring the viruses on the computer (Windows). It was named Black_Symbianv0.10 and was spread by e-mail and P2P networks. This virus even misled people by showing references to f-Secure and some files used f-Secure (an antivirus company) icons, so that people feel that this is a new antivirus program developed and circulated by f-Secure. But f-Secure was in no way responsible for this. The malware also contained modified Opera Browsers home page which had links to more additional malware SIS files. Most of the S60 phones were affected by this (Nokia N-Gage QD, 7610, 6600, 3650, etc.)The updated version of this malware affected users tremendously, since it bricked the mobile when rebooted.



Patch for security reason

Contents

- Patch opera 8
- Opera security partner
- Additional patch

Patch opera 8

Get asecure connection

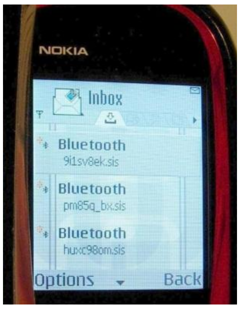
Figure 10: Screenshot of Opera Browser

2.5.1 *Removal of CardTrap*

All overwritten applications should be reinstalled. Performing a software format is also an option, but with the risk of losing all data in the C drive (see Figure 10) on the phone. The memory card of the phone should be scanned before connecting it to a remote PC.

2.6 CommWarrior

CommWarrior was the first of its kind to replicate via MMS services. MMS (Multimedia Messaging Service) is used to send an image/audio/video to any other supporting mobile. It was one of the most popular viruses ever made. The speed at which it was propagating, it was confirmed that at least 7 out of 10 people using the Symbian phones were affected by this virus. It used network resources like Bluetooth to make multiple copies of itself. When running in a device, CommWarrior searches for phones nearby, once a target is located, it will send an arbitrarily named SIS (see Figure 11) file to the device. If the device found has gone out of reach or rejects file transfer then a new device would be found. Via MMS, it would send different messages to contacts located in the phonebook claiming to have attachments [14] of antivirus, internet, happy birthday, free content, etc. The selection of the user to be sent a MMS [21] could also be on the grounds of the last phone call or message sent. On opening the message, the receiver is infected. Sending randomly named files was a characteristic of this malware since there could be no predetermined warning to reject SIS files with a particular name. Once sent, the file stays in the inbox of the receiver's device. The virus is installed at every reboot and when the message is opened. Phone owners were mainly tricked, since they felt that the message had come from someone the victim knew.



Bluetooth
9i1sv8ek.sis

Bluetooth
pm85q_bx.sis

Bluetooth
huxc98om.sis

Figure 11: CommWarrior installed in Nokia 7610

2.6.1 Disinfecting the phone

A new software called as AntiCommWarrior was designed to clean the malware off every infected device. Once installed, it would scan the phone for similar files and delete them permanently to free the device.

2.7 LibertyCrack

It is one of the four main viruses that target the Palm OS. It is the simple Trojan which targets the handheld devices to a great extent. Being a Trojan it does not replicate itself and attempts to delete all the application files on the device. It disguises itself as a crack. It is specially written for 3COM Palm platform and is the first known PDA virus to spread wirelessly in real world.

2.7.1 Installation

Liberty being a shareware has a crack that can convert the shareware into a full registered version. This virus comes in the form of a disguise. Behind this crack lies the malicious code which infects the device. It spreads through desktops and wireless emails.

2.7.2 Removal of LibertyCrack

F-Secure Anti-Virus can detect and remove the Trojan. And it thus prevents from adding it to the users handheld during a HotSync. The Symantec Anti-Virus for Palm OS is a beta application that runs on the users Palm OS handheld making it easier for scanning and removal of viruses.

2.8 Phage

It works by overwriting the beginning of Palm executable. The host files are destroyed in the process. Once one infected PRC file is transferred to Palm, the virus keeps spreading to other Palm programs until they are all infected. One can spot the infection from the fact (see Figure 12) that when one starts an infected file, the screen goes blank for a second and the program exits without doing anything visible. During this time the virus locates and infects all other programs in the system. Phage can spread from one Palm to another if infected files are shared via beaming or installed via a docking station. When activated Phage infects and destroys all application files in the device but does not harm database files.

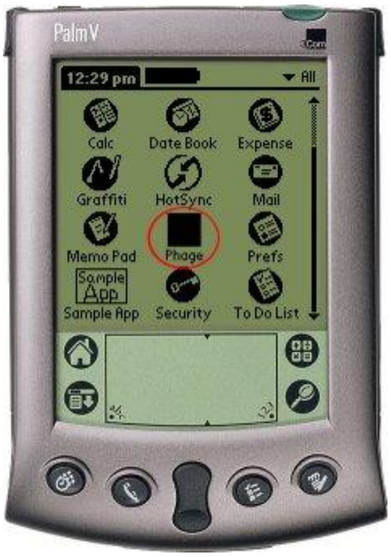


Figure 12: Original infector application of Phage virus

2.8.1 Removal of Phage

The Phage virus can be removed by deleting any file that is infected. In addition any occurrence of the file phage.prc should also be deleted from the backup folder. It is then possible to reboot the palm and resynchronize with the desktop.

2.9 Vapor

When infected with vapor all the files on the PDA disappear. When the infected file is executed, all application icons vanish as if deleted. But the files do not get deleted. They all still exist. In reality the virus simply removes the icons from the display.

2.9.1 Removal of Vapor

F-Secure Anti-Virus can detect and remove the Trojan. And it thus prevents from adding it to the users handheld during a HotSync. The Symantec Anti-Virus for Palm OS is a beta application that runs on the users Palm OS handheld making it easier for scanning and removal of viruses.

2.10 Rick Astley Virus (iOS- iPhone OS)

Rick Astley virus is also called Ikee virus. It has it's origins from Australia. It was a proof-of-concept virus (see Figure 13) developed to illustrate the world that if proper measures weren't taken even the most secure mobile operating system iOS could be infected. iOS is an operating system developed at Apple and by far very secure. The main reasons behind this are that Apple strictly reviews all applications sent by developers and if any loopholes have been found, then Apple quickly issues an update with a patch[22] for the same. This important feature of security is unavailable to most jailbroken users, thus making jailbroken devices most susceptible to malware. An iDevice is jailbroken to give the users the rights that were blocked by Apple. Once infected the display of the iPhone, iPad or iPod showed a new wallpaper of a person Rick Astley.

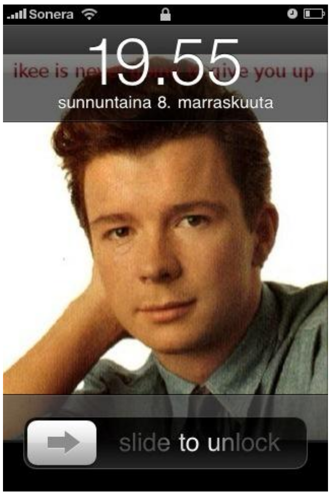


Figure 13: Rick Astley Virus in iPhone

2.10.1 Removal of Ikee(Rick Astley) Virus

Update the iOS software online periodically by using iTunes. This could lead to a software reset.

2.11 Duh Virus

After the Rick Astley virus, malware writers dropped in with a higher level malware creating havoc for a few. The virus entered the iDevice without asking any permission from the user. It first originated in Netherlands. It added the phone to a botnet, thus making the iDevice a slave of who managed the botnet. Besides, the virus not only does this but also changes the root password of the device. The virus without taking care what text lingered over the old password puts a new password hash over the old one. Once this is done, there was no way that the users could get a hang of the original password. It was only known to the attackers and not the victim. With the help of a few softwares like John the Ripper one could get the new password[23] 'Ohshit'. So users could easily check whether they had been infected with the virus if they weren't given access to the phone by the default password 'alpine.'

2.11.1 Precaution

Change the root password from 'alpine', once you have jailbroken your iDevice. One can remove the virus if the iDevice has been infected, by installing and running an application Terminal via Cydia. Now reinstall the SSH package. Applications run in an isolated compartment that Apple calls a "sandbox." Each application looks like an application machine to the user and hides the operating system, file system, and network from the user.

2.12 GGTracker

It was a malware which implemented Malvertising.They displayed a page similar to the Android Market.It signed the victim on apremium messaging service thus resulted intohuge bills for the users.The developers posted the legitimate application without any malware in the baseline version.However, once they had a huge and popular database they started releasing updated versions with harmful codes thus affecting theusers indirectly.

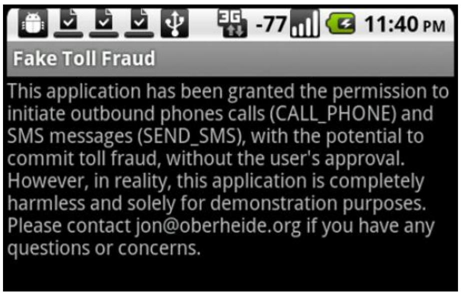
2.13 Google++

Recently an application disguised itself as it wasdistributed by Google.The application recorded phone calls, accessed GPS locations , text messagesand call logs.All this information was recorded and sent to remote server.It even violatedcopyrights by using an image of Google+ as it's name.It is not listed in the Android Market and is downloaded by visiting a malicious web site.Theapplication also had an auto answer feature thus putting it ahead of all other mobile malware.

2.14 Angry Birds

Google recently deleted 10 addons to Angry Birds(see Figure 14), since when installed they stole the devices information and connected it to a remote server.The name of the Trojan is Plankton and some of the details it uploaded are phone information like the IMEI[24] number,contacts(see Figure 15), browser bookmarks and browsing history.

Figure 14: Angry Birds Virus



Fake Toll Fraud

This application has been granted the permission to initiate outbound phones calls (CALL_PHONE) and SMS messages (SEND_SMS), with the potential to commit toll fraud, without the user's approval. However, in reality, this application is completely harmless and solely for demonstration purposes. Please contact jon@oberheide.org if you have any questions or concerns.

Figure 15: Permissions granted to Angry Birds Trojan

2.14.1 Disinfecting the phone

Click Settings—Applications-Manage Applications-Select Clear Data-Press Uninstall-Select OK when asked for confirmation and wait. (Common method for removal of GGTracker, Google++, Angry Birds- Android malware).

3. CONCLUSIONS

Malware has been consistently targeting MCDs (Mobile Computing Devices), the first OS that was targeted is Symbian. Refer [Table 1] for comparison of the mobile malware and their effects.

Table 1. Comparison of Mobile Viruses

No.	Name	OS	Removal
1	Cabir	Symbian	f-Cabir.sis
2	Mosquito	Symbian	Uninstall from Manager
3	Skulls	Symbian	f-Skulls.sis
4	CardTrap	Symbian & Windows	Software Format(*#7370#)
5	CommWarrior	Symbian	AntiCommWarrior .sis
6	Rick Astley/Ikee	iOS-iPhone	Update iOS periodically using iTunes.
7	Duh	iOS-iPhone	Update iOS periodically using iTunes
8	GG Tracker	Android OS	Uninstall from Applications.
9	Google ++	Android OS	Uninstall from Applications.
10	Angry Birds Trojan	Android OS	Uninstall from Applications.
11	Zeus Trojan	BlackBerry OS	Zeus Trojan Remover
12	LibertyCrack	Palm OS	F-Secure & Symantec Anti-Virus
13	Phage	Palm OS	F-Secure
14	Vapor	Palm OS	F-Secure & Symantec Anti-Virus

Each type of malware affects the system in some or the other way. The aim of the Zeus Trojan is to monitor users' private information, particularly when they conduct mobile online banking transactions. Once installed, the virus sends a confirmation message to the administrator to start receiving commands. Cabir was activated each time, the phone rebooted and scanned for nearby devices using 'Bluetooth' and sent its own copy to the devices found. Mosquito is concealed in a game for Symbian users.Skulls virus once installed, it supplanted normal icons with skull like structure in the phone menu, ultimately making the entire mobile functionality disabled, except for dialling and receiving calls.

CardTrap is the first cross platform malware i.e. it infected two platforms, Windows and Symbian both at the same time. CommWarrior was transmitted via MMS, it would send different messages to contacts located in the phonebook claiming to have attachments of antivirus, internet, happy birthday, free content, etc. The selection of the user to be sent a MMS could also be on the grounds of the last phone call or message sent. On opening the message, the receiver is infected. LibertyCrack acts as a Trojan by coming in a disguise. And it spreads through desktops and wireless emails. Phage can spread from one Palm to another if infected files are shared via beaming or installed via a docking station. Vapor virus performs the magic by vanishing all the icons as if they were deleted. Rick Astley Virus (iPhone) affects jailbroken phones, didn't have any consequences. Duh virus makes the iDevice a slave of who managed the botnet. Besides, the virus not only does this but also changes the root password of the device. GGTracker implements Malvertising, thus by arbitarily displaying any advertisement victims are fooled and huge amount of money is collected.Google++ violated copyrights by using an image of Google+ as it's name.It is not listed in the Android Market and is downloaded by visiting a malicious web site.The application also had an auto answer feature thus putting it ahead of all other mobile malware.

4. ACKNOWLEDGMENT

It is indeed a matter of great pleasure to present this paper titled 'Mobile Viruses'. We have tried our efforts in the right direction towards the completion of the paper. We express our profound gratitude to Prof. Anjali Malviya and Prof. Kumkum Saxena and our friends Aanchal Bhambhani & Shruti Apraj who have helped us in accomplishing this endeavor.

5. REFERENCES

[1] Ontology-based Mobile Malware Behavioral Analysis Hsiu-Sen Chiang, Woei-Jiunn Tsaur, Department of Information Management, Da-Yeh University, Changhua, Taiwan, R.O.C.

[2] D. Dagon, T.Martin, and T.Starner, "Mobile phones as computing devices: The viruses are coming!" IEEE Pervasive Computing, vol. 3, no. 4, pp. 11-15, 2004.

[3] M. Piercy, "Embedded devices next on the virus target list," IEE Electronics Systems and Software, vol. 2, pp. 42-43, Dec.-Jan. 2004.

[4] The zdnet website [Online] Available: http://www.zdnet.com/blog/btl/mcafee-malware-going-mobile/44549.

[5] The net security website [Online] Available: http://www.net-security.org/malware_news.php?id=1748

[6] A. Bose, X. Hu,, K. G. Shin, and T. Park, "Behavioral Detection of malware on mobile handsets, " in Proceeding of the 6th international conference on Mobile Systems, applications and services. Brecken-ridge, CO, USA: ACM, 2008, pp. 225-238.

[7] Dagon, D.; Martin, T.; Starner, T.; Georgia Inst. of Technol., Atlanta, GA, USA,"Mobile phones as computing devices: the viruses are coming", Pervasive Computing, IEEE, Oct.-Dec. 2004, pp. 11-15.

[8] The panda security website [Online] Available: http://press.pandasecurity.com/usa/wp-content/uploads/2011/06/CNCCS-Smartphone-Malware-Full-Report-Translated-06-7-11-FINAL.pdf

[9] The pda street website [Online] Available: http://www.pdastreet.com/articles/2005/1/2005-1-13-Mobile-Malware-The.html

[10] The smartphonetoday website [Online] Available: http://www.smartphonetoday.com/articles/2004/6/2004-6-15-Worm-Hooks-Symbian.html

[11] M. Becher, F. Freiling, J. Homann, T. Holz, S. Uellenbeck, and C. Wolf. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In IEEE Symposium on Security and Privacy, 2011.

[12] The securelist website [Online] Available: http://www.securelist.com/en/analysis/200119916/Mobile_Malware_Evolution_An_Overview_Part_1#beg

[13] The week website [Online] Available: http://www.eweek.com/c/a/Security/Symbian-Says-Skulls-May-Not-Be-Malware/

[14] The geek zone website [Online] Available: http://www.geekzone.co.nz/content.asp?contentid=3713

[15] The f-Secure website [Online] Available: http://www.f-secure.com/v-descs/trojan_symbos_cardtrap_m.shtml

[16] The f-Secure website [Online] Available: http://www.f-secure.com/v-descs/trojan_symbos_cardtrap_a.shtml

[17] A.-D. Schimdt, F. Peters, F. Lamour, and S. Albayrak, "Monitoring Smartphones for anomaly detection, " in MOBILEWARE 2008, International Conference on MOBILE Wireless MiddleWARE, Operating Systems, and Applications, Innsbruck, Austria, 2008.

[18] The f-Secure website [Online] Available: http://www.f-secure.com/v-descs/skulls.shtml

[19] The f-Secure website [Online] Available: http://www.f-secure.com/v-descs/cabir.shtml

[20] The f-Secure website [Online] Available: http://www.f-secure.com/v-descs/mquito.shtml

[21] The f-Secure website [Online] Available: http://www.f-secure.com/v-descs/commwarrior.shtml

[22] The f-Secure website [Online] Available: http://www.f-secure.com/v-descs/worm_iphoneos_ikee.shtml

[23] G. Lawton. Is it finally time to worry about mobile malware? Computer, May 2008.

[24] M.Fossi (Editor). Symantec Report on the Underground Economy. Symantec Corporation, 2008.