2010

Yet Another Symbian Vulnerability Update

Nizam Uddin Bhuiyan
Edith Cowan University

DOI: 10.4225/75/57b523eccd8ae
Originally published in the Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Yet Another Symbian Vulnerability Update

Nizam Uddin Bhuiyan
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
nizamb@our.ecu.edu.au

Abstract

The more the mobile devices are approaching to advance their security, the numbers of vulnerabilities are also becoming more astonishing. The number of mobile phones including smart phones is rising vertically, and so has the amount of malware activity. This report documents the latest threats in Symbian mobile industry and analyses the consequence. In addition, it will suggest the possible solution that may help individuals to protect their device & ultimately maintain the privacy.

Keywords

Symbian, Nokia vulnerability, Nokia threats, Mobile threat, Symbian malware, Symbian virus, Cell security, Consequences and counter measure for mobile threats.

BACKGROUND

The popularity of mobile has reached to sky high regardless whether you receive a blank SMS frequently or your mobile keeps sending a SMS to strangers persistently without your knowledge. According to Goode Intelligence 2009 Mobile Security Survey, "In the last couple of years, the percentage of mobile messaging traffic (SMS/MMS/e-mail) that is defined as spam or malware has risen from approximately 2% to between 20% and 30% of total traffic" (Francis, 2010). We are always worried about computer and network related virus, threats, vulnerabilities and security issues over the years because our workstations are involved with financial, intellectual or confidential transmission. In reality, network communication has emerged with mobile communication such a way that mobile is getting more advanced than ever. For example, Android OS based Google Nexus has the CPU capacity of 1GHz (Google site, 2010). Thus, users and corporations are relying on smart phones for their daily financial or communication related transaction.

Malware developers have found a new environment – 'mobile platform' to release their malicious code since they realised that the world's business is going to be heavily dependent on compact device like smart phone, PDA, and iPad. Furthermore, their choice is smartly determined as they realise that the mobile security barrier is still immature (Panda Labs Blog, 2010). As a result, we have been encountering mobile related virus, malwares and hidden attacks. In a nutshell, mobile threats have been escalating (Brenner, 2006).

Consequently, new types of threats are being added to the current list and affecting our confidential information. Despite the fact of imminent threats of mobile environment, we rely on these devices and have to upgrade to more complex ones repeatedly. Therefore, network security industry has expended its research and development to mitigate the situation as they become conscious that mobile threat is inevitable.

INTRODUCTION

Security Researchers and Communication Managers Marcus wrote, we would notice more mobile malware attack in coming years while users are feeling comfortable to store their personal details for example, financial or identification data (Westervelt, 2007). In addition, senior news editor of *Information Security Magazine* quoted on one of his articles "Hypponen claimed that he had seen over 370 different types of malware running on Symbian based mobile because it runs on over half of the smart phone in the world" (Brenner, 2007).

According to *CIO* News (Sacco, 2008), mobile related security threats are on the rise and such threat are not limited to user operating error but also unauthorized used, phishing attack and misuse of device. Higgins, 2010 explains that a survey was conducted by *Goode Intelligence* and found that 54% of organisation plan to implement mobile antivirus solution by the end of this year.

As the mobile phone is having powerful operating system nowadays, they are capable of holding large amount of information and unsecured access to Wi-Fi. Constantin, 2009 wrote that many users misjudged mobile network threats and they were not aware that the mobile was also prone to security risk.

This report examines the history of Symbian threats, current update of threats and consequences. In addition, possible solutions will be documented to advise the audience.

HISTORY OF MOBILE MALWARE

According to MediaBuzz, 2009 mobile virus are in market since 2004 and number of virus is swelling. SYMBOS_CABIR - was the first malware identified and it was expected to spread widely (Shevchenko, 2005). She also explained that this was dominating from June 2004 to January 2005 and the following six months were ruled by primitive Trojans for Symbian.

In the year 2006, malware developer came out with the idea of spreading virus through PC to mobile connection and vice versa. One of the malware was SMiShing that was basically utilizing the phishing technique to port the email to SMS (Rediff news, 2006). Additionally, another nasty virus was SymOS/Felsispy.B that was able to activate the microphone of the victim's mobile remotely. McAfee predicted that the spread of commercial spyware targeting mobile devices to grow in 2007. Neel, 2006 said that F-Secure antivirus company counted over 300 viruses by the year 2006.

Nokia has been very popular because of its friendly graphical interface until two years ago. However, iPhone and Android based phones are climbing the share ladder sharply. Therefore, it is difficult to conclude which platform based mobile will be major target by hackers at this moment since they like to code more for most popular platform (Gostev, 2009).

The facts about the total number of threats to date varies, however, all references indicate that there is dramatic increase of mobile virus over the last few years. For instance, Kaspersky Lab, 2009 report shows that there are approximately 253 malwares for Symbian itself and the number of mobile families have increased by 235%. Another latest report claims that there are 200 viruses targeted to mobile phone to date (2010). Some relevant statistic can be found form Figure 1 and Figure 2.

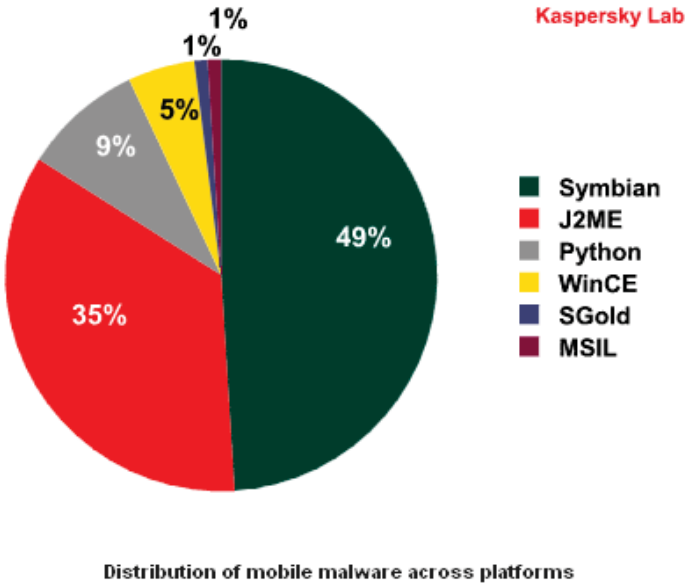

Figure 12: Distribution of Mobile Malware Across Platforms

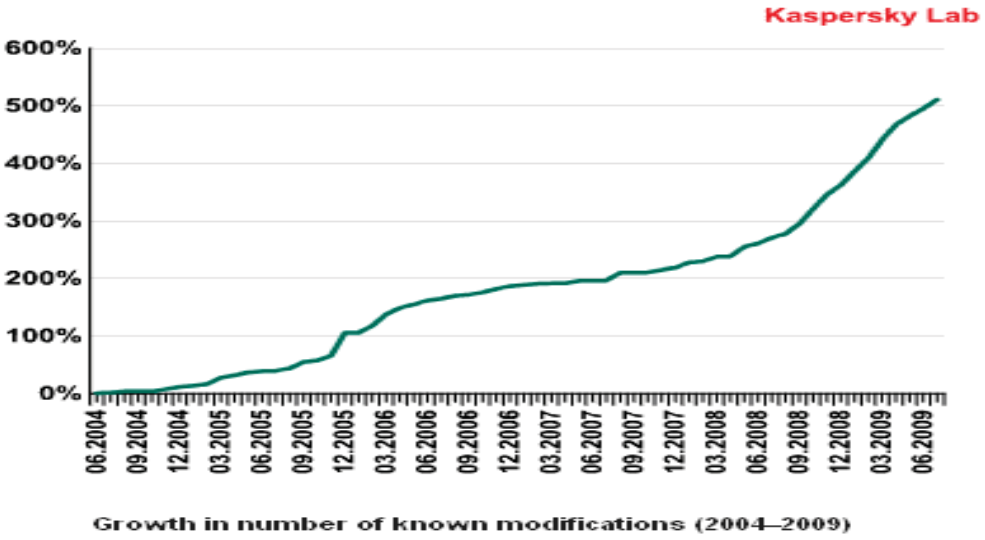

Figure 13: Symbian Malware Growth in Number of Known Modifications

By analyzing the record of Panda Security, we understood that mobile malware developed very rapidly during the years of 2004 to 2006. These malware programs were very similar to computer malware program for instance, viruses, worms, Trojans, spyware, backdoors and adware as reported by Gostev, 2009.

TYPES OF MALWARE

There are a few types of mobile malware families in the market, for example Brador, Cabir, CardBlock, CardTrap, Commwarrior, Cxover, Dampig, Doomed, Duts, Fontal, Locknut, MMS Bomber, Skulls, Velasco and Qdial 'Mobile Antivirus Store', 2010. However, according to analysis common Symbian virus families are Cabir, Skulls and Commwarrior.

HISTORY OF MALWARE SPREAD

The activity of mobile malware has been very active since 2004. According to Kaspersky Lab, 2006 the number of Symbian malware was 150 in early 2006 and it had increased to almost 300 by the summer of that year. However, Figure 3 shows that incidents of new variants declined significantly during the same period. Additionally, it explained that there was new type of virus released that was developed with mixture of multiple types of existing virus and the number was increasing as usual (Figure 4).

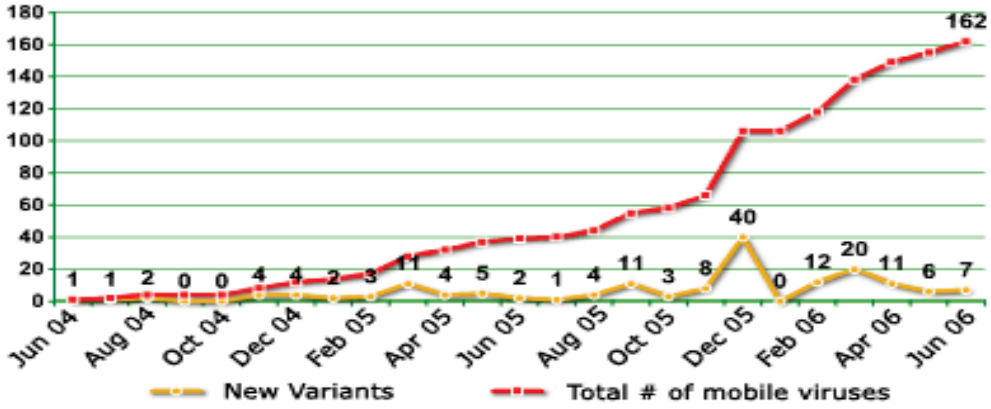

Figure 14: New Variants vs. Total Number of Mobile Viruses

Figure 15: Increases in Known Malware Families

Kaspersky Lab, 2010 released a report that indicates that there were 39 (257 variants) new mobile malware families in 2009 compared to 30 (143 variants) identified families in 2008 (Figure 5). This also explained that remote server related virus became very common because of the capability of Wi-Fi networks. Therefore, we realise that the existing viruses are getting smarter with better capability of causing many types of damages.

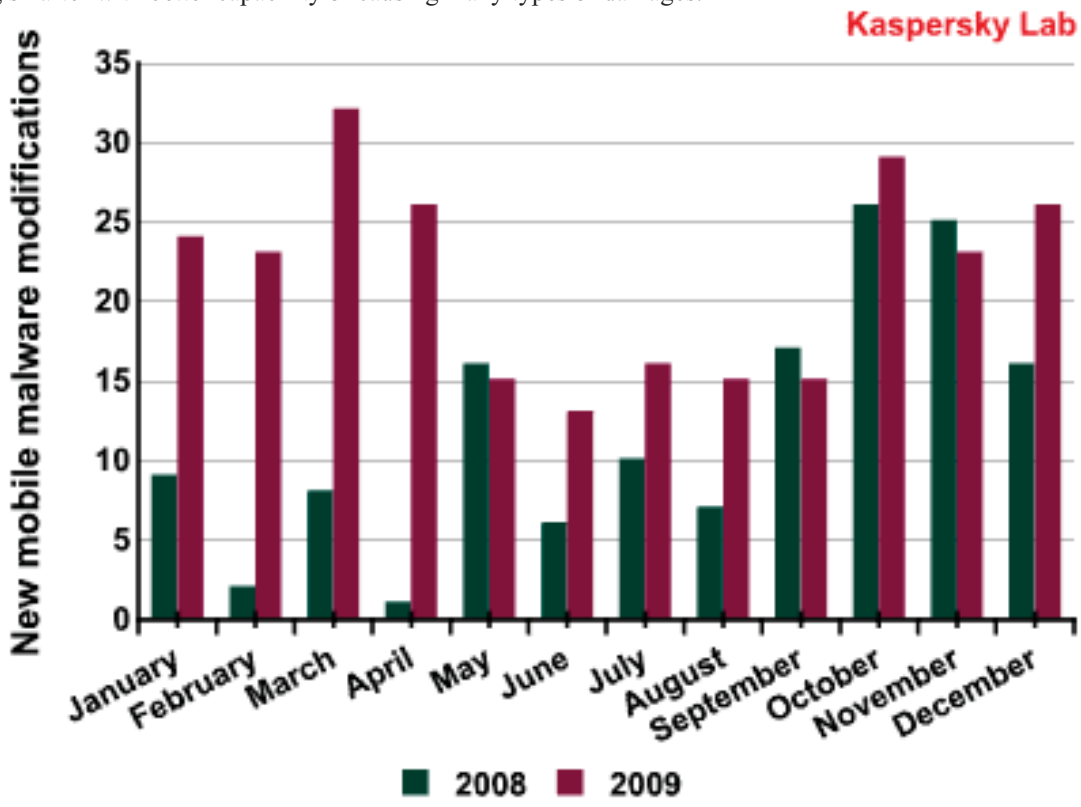

Figure 16: New Mobile Malware Modifications

CONSEQUENCES OF MOBILE MALWARE

All malware or threats are not necessarily harmful. Yet, there are significant numbers of mobile malware families, which cause various degrees of damage. Some of the major types of consequences are highlighted in next section.

DATA THEFT

Gostev, 2007 understood that the first complete spyware was Flexispy that was sold for $50 through website. It had the potential of taking complete control of Smart phone and transfers of information such as SMS and calls details, which could potentially be cybercrime related.

The second one was Acallno, which was able to forward all sorts of SMS to a designated number once installed.

FINANCIAL THEFT

Hackers wrote malicious codes to steal financial information and the first successful virus was RedBrowser Torjan – it was described as utility that could be used to access internet via SMS. In fact, it actually sends the SMS to premium rate number that cost a user up-to $5 per SMS. Another similar virus was Wesber that was released in September 2006.
In addition to data and financial theft, there were other types of damages, which were published by Media Buzz, 2009.

- Malicious code multiplies itself via Bluetooth and MMS as Bluetooth does not have proper security mechanism
- Send out MMS and SMS without user's knowledge
- Contaminate files; then by synchronizing with PC and other mobile device it spreads even quicker
- Send out contaminated files via email, Wi-Fi, Bluetooth to people under owner's name
- Erase personal details for instance contact details, bookmarks, files and steal private information
- Disable mobile functionality partially or completely
- Enable remote access to smart phones
- Exchange files icons and system application
- Modify fonts and install suspicious applications
- Work against antivirus application
- Lock memory cards and steal information
- Use up the on board battery much quicker

SYMBIAN THREATS UPDATE

Regional director of McAfee – Hayati said that the problem of spam attack on mobile phone is escalating very quickly and the world is not completely aware of the damage that could take place.

Cabir.A is one of the most widely used threat families since 2005 and there are 120 different types of malware under this family itself. Shevechenko, 2005 said that most notorious types of malware would be self-replicating virus so called worm. Due to the nature of self-replicating, it is able to infect large number of devices within short period of time causing device functionality problem as well as transforming a mobile network into widely distributed network controlled by a malicious user. Major Symbian threats which were common in recent years are documented below.

THREATS IN 2010

Merogo SMS worm

According to Mikko, 2010 from F-secure, one of the latest (22nd March, 2010) worms called Merogo SMS worm was found in China that is categorized as Trojan family23. This is specifically created for Symbian Series 60 3rd Edition mobiles.

It spreads through Chinese SMS that contains a link of website. When a user clicks on the link, then user is prompted to install an application, which results in infecting the phone and starts spreading SMS. To make it even worse, it has the capability to send message to premium numbers.

We know that it is impossible to install any unsigned application in Symbian platform (series 60 3rd edition). However, F-secure statement says that this latest worm has gone through Symbian signed mechanism. This signed installation file in fact contains many different SISX files; as a result, the host installer will deploy such files in the device. This newer technique makes the certification process harder, which causes difficulties to get a full view of what the program actually does.

However, nothing more is reported about this malware except the incidents in China and Symbian has canceled the publisher ID that was used in the package.

Another weblog by Sean from F-Secure claims that, even though Symbian revoked the publisher ID from certification, the problem is not solved yet because of the fact that, Series 60 phones are not necessarily configured by default to check certification revocation instance. Therefore, they have posted a guideline as to how to bypass this warm activity when

browsing. We can have a look on the animated flash file by visiting http://www.f-secure.com/weblog/archives/00001918.html.
Alternatively, the following process can be used to demonstrate this.

- Go to 'Control Panel' then click on 'Application Manager' then "Download Application' and click on 'Download Settings'.
- Click on 'Software Installation' and choose 'Signed Only' Option.
- Then click on 'Online Certification Check' and check on' radio button.

SymbOS/Yxe worm

According to FortiGuard Center another new Symbian threat is known as SymbOS/Yxe that was released on 1st March, 2010. F-Secure database classifies this as malware category of worm type alternatively SMS-Worm – Trojan type. It could have one of the few various names - SymbOS.Worm.Yxe.A, Worm.SymbOS.Yxe, Worm:SymbOS/Yxe, and Worm:SymbOS/Yxe.gen.

The characteristic of this worm is to send SMS, killing some applications and gathering information from the device. Therefore the user may face unusually high bill and quick battery loss. It could be present as the following files:

- c:\sys\bin\LanPackage.exe
- c:\sys\bin\Installer_SV.exe

In addition, FortiGuide Center explains that it creates or builds the following files when installed:

- C:\sys\bin\Installer_SV.exe: program that installs the malware
- C:\sys\bin\LanPackage.exe: main malicious server
- C:\system\data\SisInfo.cfg: configuration file used by the installer.
- C:\system\data\Source.ini: written by the installer.
- C:\System\Data\NotPure.txt
- C:\system\data\Remote_Para.txt
- C:\system\data\Local_Para.txt
- C:\private\20028B98\SisInfo.cfg: copy of system data SisInfo.cfg
- C:\private\20028B98\Source.ini: copy of system data Source.ini

The removal mechanism is provided by FortiGuide Center and antivirus definition version is 11.643.

THREATS IN 2009

SymbOS/Beselo

This was released early January as a 'SymbOS/Beselo.A!Worm.DAM' worm. According to FortiGuard Center, there is no visible symptom however it is typically capable of damaging SIS archives file. There is a virus removal definition provided, the file is called 11.643.

There were 8 families of mobile virus released in March 2009 itself. The following table represents all of those families along with different types of worm or Trojans. This information is extracted from the encyclopedia of FortiGuard Center.

Virus Family	Virus Variants	Released Date
SymbOS/PbBlister	PbBlister.A!tr	March 09, 2009
SymbOS/FwdSMS	Fwdsms.A!tr.spy; Fwdsms.B!tr.spy; Fwdsms.D!tr.spy;	March 19, 2009
SymbOS/Pbstealer	Pbstealer.F!tr;	March 24, 2009
SymbOS/Feak	Feak.A!worm;	March 25, 2009
SymbOS/TrapSMS	Trapsms.A!tr.spy;	March 25, 2009
SymbOS/Yakki	Yakki.A!tr;	March 30, 2009
SymbOS/Cabir	Cabir.E465!Worm	March 30, 2009
SymbOS/Romride	Romride.B!TR	March 31, 2009

SymbOS/PbBlister

If any device is infected by this Trojan virus (PbBlister.A!tr), then the device will be unable to receive calls, SMS & MMS; and responds to the caller that device is always busy. We typically can find the file as %SystemDir%\apps\osanimator\osanimator.app.

Deeper analysis shows that it deletes quite a few files while auto starting (details could be found from http://www.fortiguard.com/encyclopedia/virus/symbos_pbblister.a!tr.html) and the malware file appears as a SIS file (AnitatedScorpion.SIS) without any certificate. It starts installing as soon as user presses on 'Yes' button. This malware is created with the combination of two legal applications, bundled with an additional configuration file. Definition of this virus removal could be found in FortiGuard Center.

SymbOS/FwdSMS

This usually forwards the SMS to another phone and requires user interaction to be installed. It is considered as Trojan because the server runs silently, it does not consist of any application icon, SMS messages containing commands are automatically deleted once process is executed and installs as legal application. A removal method is provided by FortiGuard Center under the definition no 11.643. The group of variant of this family is "Fwdsms.A!tr.spy; Fwdsms.B!tr.spy and Fwdsms.D!tr.spy".

SymbOS/Feak

Feak.A!worm is capable of sending existing SMS to all contacts once a device is contaminated. Thus, we understand that it spreads through SMS which is crafted with a link leading to a copy of the worm. The virus fixing tools are developed by FortiGuard Center, the definition number is 11.643.

SymbOS/Pbstealer

This is another sort of Trojan (Pbstealer.F!tr), which is able to spy and steal contacts. Infected devices show that it is just compacting the contacts database however it is not. This is similar type of Trojan known as PBSENDER that was released in 24th January, 2006.

SymbOS/TrapSMS

It is categorized as malware and installed by an attacker on the victim's mobile with the typical name 'Backuper'. It remains hidden since it does not have any icon. Once the spyware software is installed on the victim's mobile, all the SMS messages will be forwarded to the website of the spyware. The next step for the attacker is to log in to the spyware website that allows read access to the entire text.

When it is installed on Symbian OS 8 version, it generally deletes some files and creates some files as well. Yet, it is little different when it is configured on Symbian OS version 9; it deletes quite a few different files even though resulting damage remains almost identical. By installing the virus definition from 11.643 at FortiGuard Center, the problem could be mitigated.

SymbOS/Yakki

This is determined as Trojan by experts that are able to completely lock the phone by splash screen display. Indeed, it disables all call functionality and SMS/MSM messages. The splash display screen is impossible to be removed. Typically Symbian OS 7 and 8 is friendly enough to support this Trojan, which does not show any icon and makes it harder for victim to have control over the device. After reboot, the phone locks itself up entirely. In addition, it copies itself to on board memory card and makes the memory card incurable because it is impossible to reset the hardware or software of memory card. If infected memory card is used on different phone that will be contaminated too. A virus removal database is available at FortiGuard Center.

SymbOS/Romride

This is considered as a Trojan and identifies itself as an application updater by MSF. It could be found as "%System%\Shareddata\10005943.ini''.

It deletes the following files even though these are nearly zero bytes.

- %System%\bootdata\LocaleData.D01
- %System%\Shareddata\10005943.ini
- %System%\Shareddata\10005a40.ini
- %System%\Shareddata\1005984.ini

Security experts were also busy during April, 2009 because few new viruses were kicking off the mobile markets and those are SymbOS/Rommwar.C!Tr, SymbOS/Booton.C!TR, SymbOS/ACALLNO.A!TR.SPY and SymbOS/ALACCNO.B!TR.SPY. Details are discussed below.

SymbOS/Rommwar.C!Tr

It was released early April, 2009 and the purpose of this Trojan is to install application with the name 'DSISHARK_69' and force the user to reboot that makes the device unusable. The continuous reboot process is achieved by setting the 'application to be launched at startup' to a system executable that restarts the device.

SymbOS/Booton.C!TR

It struck the mobile world on the 3rd week of April, 2009 that is capable of restarting the mobile with partial changes of settings. Once installed, some files would be missing.

SymbOS/ACALLNO.A!TR.SPY

This also came out just two days after the last one. Due to the damage caused by this malware, a user often faces unexpectedly high bill as this is responsible for forwarding incoming and outgoing SMS messages to a pre-arranged number. However, this application also needs user's approval to be installed on the phone. Once the installation is completed, some files will be dropped.

SymbOS/ALACCNO.B!TR.SPY

This deadly Trojan was the last malware released for the month of April, 2009. Experts from FortiGuard Center said that this Trojan horse allows a nearly complete compromise of the targeted mobile device. It causes the following actions however, the list is not exhaustive.

- Track location of device
- List missed/incoming/outgoing phone calls
- Intercept/spy/record incoming phone calls
- Retrieve IMSI and phone number of spied device each time the SIM is replaced
- Query IMEI
- Capture screenshot
- Turn on/turn off/dim/increase the background light of the phone

THREATS IN 2008

SymbOS/Beselo.A!Worm

The year 2008 started with the toxic outbreak of this virus and ensuring regular malware entrance in the mobile world. Like many other worms, this also expands its rivalry through MMS and Bluetooth. It sends to devices with the same operator and existing contact address. Surprisingly, it does inform the user not to install if someone does not trust the provider. However, if a user decides to trust the providers and allows the installation, then three different files are installed. The virus fixing method was provided by FortiGuard Center.

SymbOS/Comwar.V30.Var!Worm

This was released in early February, 2008 that was capable of forcing the battery to lose the power very quickly because of the continuous action of trying to infect other mobiles via Bluetooth. Solution was suggested by FortiGuard Center.

SymbOS/SpyPhone.A.Tr

This Trojan came out on 12th February, 2008 that was able to perform the following as reported by FortiGuard Center.

- It loads the other components, namely, NVG.exe, NVG1.exe, and setting.app
- It monitors incoming calls and stores the call information in the setting.ini file
- It accepts a call from an external number without notifying the user. This external number is hardcoded in the malware
- It saves/logs the entire screen to a bitmap (snapshot)

It arrives as a SIS file and once the user installs it, the malware is capable of installing its components automatically. Interestingly one of the installed files does not have any name and this makes it harder to identify the process running on the system. Additionally, the components of the malware do not show up in the program menu. Therefore, it is believed that it was crafted smartly to keep it hidden from user while a device is infected. However, the process could be killed by most process viewer applications.

Secondly, this malware is designed to contain additional 4 SIS files (autostart.sis, NVG.sis, NVG1.sis & Settings.sis) along with the original SIS file. Once these are installed successfully, then the malware penetrates the "c:\system\install\'' path and automatically deletes all related files to cover any hint of being installed. The remaining files spy on backlight features, records key strokes and reloads the main component if necessary.

The mitigation technique is provided by FortiGuard Center and anyone can update the virus definition version 11.643 to stabilize the system.

SymbOS/Comwar

This family was released in March, 2008 with few different variants for instance,

- ComwarV10.VAR!WORM.DAM and ComwarV10B.VAR!WORM.DAM in 4th March,
- ComwarV10.NOSTR!WORM.DAM in 5th March, and
- ComwarV10B! WORM.DAM in 12th March.

According to the documentation of FortiGuard Center, the deleted file is no longer infectious and it is a damaged version of SymbOS/Comwar variant. Furthermore, damaged files have no major sign of truncation. It expands its existence through MMS and Bluetooth messages. Fixable virus definition was released by FortiGuard Center.

SymbOS/HatiHati.A!Worm

Another malware was released on 13th March, 2008 that was capable of stealing client's credit. It spreads basically via memory card exchange between mobiles. When the application identifies a SIM card different from the current one, it starts to secretly discharge "SIM changed'' SMS messages to a predefined phone number. This problem could be solved by the virus definition provided by FortiGuard Center.

SymbOS/Flerprox.B!Tr

This is considered as a Trojan that was released late March. Once the installation is complete a long string is displayed and user is requested to press any key. If a key is pressed then the device becomes very slow. A fix is available from FortiGurad Center.

SymbOS/Beselo.C!Worm

Another worm was released on 16th June, 2008 that was responsible for rapid battery power loss. Once the device is infected, the application turns the Bluetooth on continuously to seek for nearby devices in order to transfer the infected files, with the ultimate goal of rapid replication.

This malware comes up as a SIS file and does not have a Symbian certificate and the installers are informed while attempting to install. It deletes few files once the installation is done successfully. Once it is able to locate a Bluetooth enables device, it tries to send one of the three files – beauty.jpg, love.rm and sex.mp3.

A fix is distributed by FortiGuard Center.

Some of the hostile programs for Symbian are documented here; however all of those still require the input of the user to run.

Drever.A

It is a malicious SIS file Trojan that attempts to disable the automatic startup from Simworks and Kaspersky Symbian Anti-Virus applications.

Locknut.B

It is a malicious SIS file Trojan that pretends to be a patch for Symbian S60 mobile phones. When installed, it deletes a binary that will crash a critical system service component. This will prevent any application from being launched in the phone.

Fontal.A

It is a SIS file Trojan that installs a corrupted file which causes the phone to fail at reboot. If the user tries to reboot the infected phone, it will be permanently stuck on the reboot, and cannot be used without disinfection – that is, the use of the reformat key combination which causes the phone to lose all data. Being a Trojan, Frontal cannot spread by itself – the most likely way for the user to get infected would be to acquire the file from unreliable sources, and then install it to the phone, inadvertently.

Symbian cabir

It (the predecessor of 15 variants) was released in June 2004. This worm infects Symbian Series 60 smart phones by sending itself over Bluetooth connections. It requires the victim to open a messaging file and click ‘yes’ when prompted by the installer. Cabir then tries to spread by searching for nearby Bluetooth devices in discoverable mode. Although Cabir infections have been reported in more than 20 countries, most antivirus companies consider it low risk. Cabir targeted a very popular device but propagated far too slowly, infecting just one phone per reboot. For most victims, Cabir's only adverse impact was battery drain.

CommWarrior

In early 2005, Commwarrior (the predecessor of seven variants) improved on these techniques by searching both for nearby Bluetooth devices and sending itself via MMS to phone numbers in the victim's local address book. Commwarrior also sends randomly named files to avoid immediate user recognition and tries to cover its tracks afterwards. As a result, even though it still required user acceptance to install, Commwarrior was far more successful in propagating. More importantly, it caused financial damage by racking up MMS transmission fees. One operator reported that malware was responsible for 5% of its MMS traffic.

Pbstealer

Symbian Pbstealer is a Trojan that builds upon Cabir's Bluetooth propagation mechanism. To trick users into installing it, Pbstealer poses as a shareware address book compaction utility. In reality, Pbstealer sends a copy of the victim's local address book to the first nearby Bluetooth device that it can find.

RedBrowser

In February 2006, the first J2ME Trojan emerged as Redbrowser, a Java applet that masqueraded as a shareware WAP browser that could retrieve Web pages for free. In reality, Redbrowser sent SMS messages to premium numbers in Russia at a cost of $5 a piece.

Beselo

In December 2007, the Symbian Beselo worm started to spread itself via Bluetooth and MMS. Beselo is similar to Commwarrior, except that installation files are not identified by the usual .SIS extension. Instead, Beselo files are named with .MP3, .JPG, or .RM extensions, fooling users into opening these phony multimedia files, thereby installing Beselo.

MultipleDropper

In March 2008, Symbian Series 60 second edition devices were targeted by MultipleDropper, a malicious program that arrives via Bluetooth or MMS then installs Commwarrior, Beselo, and a new Trojan, Kiazha. After sending an SMS to the malware's author, Kiazha attempts to extort $7 (RMB 50) as ransom, to be sent by the user through the Chinese IM network QQ.

EVALUATION OF THREATS

After the above analysis, we realised that mobile malware was spreading very quickly at the beginning and these programs were quite similar to traditional computer malwares. These new sort of modified malwares were mainly targeted smart mobile phones and successfully entered into the market for a short while. It was easier to spread because mobile phone does not have as efficient security features as traditional computers do. During that time, most of the viruses were developed for Symbian OS only as over half of the phones were built by Nokia. We see correlation with the computer industry; we see that the attackers are releasing malwares for the most popular OS like windows compared to Linux or UNIX. Nonetheless, the types of mobiles are so numerous that it is quite difficult to write such program to cover most types of phones. Therefore, they are interested to utilize polymorphism technique or hidden code with fake signed application now that is much harder to isolate or determine. Moreover, other newer techniques are infecting memory sticks, user data, paralyzing OS security features, downloading files via internet, and making fake call to premium numbers or pornographic sites. It is not limited to spreading virus through Bluetooth, SMS, MMS, modify icon, locking memory cards and deactivating antivirus, it also causes financial losses to unsuspecting victims.

POSSIBLE SOLUTIONS

Mobile has security vulnerabilities like computer and network. There is no particular locking system or guarding system that is able to ensure 100 percent security. Conversely, there are various types of security locks or guards that are suitable for different situations. We can make use of the combination of available and up to date technologies to fight the serious attacks. Yet there is no guaranty that this option will provide 100 percent security, nevertheless, this methodology certainly maximizes the mobile security and it is often possible to stop a threat. Few techniques are documented here which are also suggested by Wi-Fi Planet, 2007; TechRepublic, 2008; and TechGuru, 2010.

- Enable SIM, device and access lock from mobile settings. Enable the periodic lockdown feature. Enable the memory access code.
- Think before accessing any internet site and installing any application.
- Spend little bit time to check the application through Google or any search engine before downloading or installing unknown files.
- Disable WLAN and Bluetooth when you are out door and when you are not using it.
- Find a phone with the service option to remotely kill it when it is irretrievably lost.
- Never let others to access your phone. Be careful while accepting calls or messages from unknown numbers.
- Enable WPA 2 encryption for WLAN connection and pass code request feature for Bluetooth connection.
- If you noticed that your phone has connected to GPRS, UMTS, and HSDPA, disable those instantly.
- Keep regular backup.
- Install antivirus software.
- Do not simply save sensitive information on the phone unless absolutely essential.

FORECAST

The best feature of Smartphone is the ability to decide whether to install an application or not. Additionally, it allows a user to remove the OS and reinstall specific OS from scratch. Users love to have variety of applications for different features. We realise that iTune based application has gained the popularity. At the same time applications for Android and Symbian are also becoming popular. Applications continue to be incompatible under various OS.

Attackers are coming out with even new sorts of ideas and trying to utilize the hacking techniques of Wi-Fi like a sniffer which can intercept two way traffic, as the new Smart phones have Wi-Fi capability without having strong authentication. According to Red Orbit news, 2010 cyber criminals are making use the facility of email and browsing functionality while security experts are developing antivirus and anti theft features for mobile.

2010 is the dawn of new era when the applications are being developed which will be hugely popular; however, it is not likely that the mobile malware will target Smartphone extensively. Users will experience that Smart phones will have more similar features like netbook or laptop. If the above mentioned OS based mobile becomes more popular which perform confidential and financial transactions then the mobile malware will spread much faster than it has been to date.

CONCLUSION

The mobile threats will not stop as in the case of computer virus since the popularity of Smartphone will increase every day and will have more sophisticated functions. The propagation techniques will certainly reach to a new level and it will be more challenging to stop the attacks. Malwares are getting smarter with the advancement of technology.

The popularity of Nokia is decreasing slowly due to the fact that few new companies are releasing very promising Smartphone with all sorts of features including better user interface. Therefore, it is difficult to identify which platform based mobile will be major target by hackers at this moment since they like to code more for most popular platform (Gostev, *2009*).

The confidentiality will be compromised due to stealing of data and financial theft will be more sophisticated. The security techniques will not be adequate to guarantee all of user activities. Therefore, the users need to be educated and be aware of what they can possibly lose if they ignore security threats. Furthermore, users should follow all available security features to maximize security.

Finally, users should be wary of any unknown senders before accepting any request. They can also learn to manage the remote access security so that they can kill the phone or make the phone unusable remotely if they misplace it or someone steals it.

REFERENCES

"A Brief History on the Types of Mobile Viruses" (2009) retrieved on 10th April, 2010 from http://www.mediabuzz.com.sg/asian-emarketing/september-october-2009/617-a-brief-history-on-the-types-of-mobile-viruses

Brenner, B. (2006) "How to Survive Mobile Phone Attacks" retrieved on 20th April, 2010, from http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gci1232051,00.html

Brenner, B. (2007) "Apple iPhone to Provoke Complex Mobile Attacks, Expert warns" retrieved on 10th April, 2010 from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1267620,00.html

Constantin, L. (2009) "Many Users Underestimate Mobile Malware Threats" retrieved on 10th April, 2010 from http://news.softpedia.com/news/Many-Users-Underestimate-Mobile-Malware-Threats-120491.shtml

"Common Types of Mobile Malware" (2010) retrieved on 03rd April, 2010 from http://www.mobileantivirusstore.com/mobile-malware

Francis, L. "Mobile Threats on the Rise" (2010) retrieved on 20th April, 2010 from http://www.itweb.co.za/index.php?option=com_content&view=article&id=29162:mobile-threats-on-the-rise&catid=147:internet&Itemid=68

F-Secure "News From the Lab: Merogo SMS Worm" (2010) retrieved on 4th April, 2010 from http://www.f-secure.com/weblog/archives/00001912.html

FortiGuard Center "Encyclopedia" (2010) retrieved on 10th April, 2010 from http://www.fortiguard.com/encyclopedia/virus/symbos_yxes.h!worm.html

F-Secure "Security Lab: Latest Threat" n.d. retrieved on 4th April, 2010 from http://www.f-secure.com/v-descs/worm_symbos_yxe.shtml

Gostev, A. "Kaspersky Security Bulletin 2006: Mobile Malware" (2007) retrieved on 3rd April, 2010 from http://www.securelist.com/en/analysis?pubid=204791922

Gostev, A. "Mobile Malware Evolution: An Overview, Part3" (2009) retrieved on 08th April, 2010 from http://www.securelist.com/en/analysis?pubid=204792080

Higgins, K. J. "Survey: 54 Percent of Organisations Plan to Add Smartphone Antivirus This Year" (2010) retrieved on 10th April, 2010 from http://www.darkreading.com/securityservices/security/antivirus/showArticle.jhtml?articleID=222200724

"How to Protect Your Mobile Device from Loss, Theft & Malware" (2007) retrieved on 05th April, 2010 from http://www.wi-fiplanet.com/tutorials/article.php/3662386/How-to-Protect-Your-Mobile-Device-from-Loss-Theft--Malware.htm

"Insight on Mobile Phone Viruses & Other Malware" (2010) retrieved on 02nd May, 2010 from http://www.techquark.com/2010/04/insight-on-mobile-phone-viruses-other.html

"Kaspersky Security Bulletin 2009: Malware Evolution 2009" (2010) retrieved on 2nd April, 2010 from http://www.securelist.com/en/analysis/204792100/Kaspersky_Security_Bulletin_2009_Malware_Evolution_2009#2

"Kaspersky Security Bulletin. January – June 2006: Malicious Programs for Mobile Device" (2006) retrieved on 2nd April, 2010 from http://www.securelist.com/en/analysis/198981193/Kaspersky_Security_Bulletin_January_June_2006_Malicious_programs_for_mobile_devices

MediaBuzz "A Brief History on the Types of Mobile Viruses" (2009) retrieved on 3rd April, 2010 from http://www.mediabuzz.com.sg/asian-emarketing/september-october-2009/617-a-brief-history-on-the-types-of-mobile-viruses

"Mobile Threats" (2010) written by lecturer of Alluri Institute of Management Sciences, Warangal' retrieved on 08Th May, 2010 from http://tricks9.info/2010/mobile-threats/

"Nexus One" (2010) retrieved on 20th April, 2010 from http://www.google.com/phone/static/en_US-nexusone_tech_specs.html

Neel, D. "CA and F-Secure Tangle over Mobile Malware Threat" (2006) retrieved on 2nd April, 2010 from http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=191101187

Olzak, T. "Five Steps to Protect Mobile Devices Anywhere, Anytime" (2008) retrieved on 05th April, 2010 from http://blogs.techrepublic.com.com/security/?p=529

Raywood, D. "Mobile Messaging Attacks to Rise in 2010" (2010) retrieved on 10th April, 2010 from http://www.securecomputing.net.au/News/165500,mobile-messaging-attacks-to-rise-in-2010.aspx

Sacco, A. "Mobile Related Security Threats on the Rise" (2008) retrieved on 10th April, 2010, from http://cio.co.nz/cio.nsf/news/B564CF4034D0E4F9CC257451000AC691

Shevchenko, A. "An Overview of Mobile Device Security" (2005) retrieved on 02nd April, 2010 from http://www.securelist.com/en/analysis/170773606/An_overview_of_mobile_device_security

"Smartphones: Target for Hackers?" (2010) retrieved on 01st May, 2010 from http://pandalabs.pandasecurity.com/smartphones-target-for-hackers/

Tang, C. "Summary of Mobile Threats for Year 2005" (2006) retrieved on 3rd April, 2010 from http://www.symbian-freak.com/downloads/pdf/summary_of_mobile_threats_for_year_2005.pdf

"Top 10 Computer Virus Threats in 2007" (2006) retrieved on 02nd April, 2010 from http://inhome.rediff.com/money/2006/nov/30spec.htm

Westervelt, R. "Future Mobile Attacks Inevitable, Researchers say" (2007) retrieved on 20th April, 2010 from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1271668,00.html