Virus Attack on Mobile Phone as an Impediment to Network Stability

*JEREMIAH CHUKWU[1], NWODE SUNDAY NNAMDI[1]
[1]Information and Communication Technology/Research Centre, Ebonyi State University, Abakaliki – Nigeria
E-mail:* j3chuks@yahoo.co.uk

ABSTRACT

Viruses that infect cell phones especially Smartphone's are beginning to emerge as a new obverse in the fight against computer viruses. Cell phones viruses have become real as many smartphones and other modern cell phones feature internet capability and contain storage space. Cell phones viruses can be harmful because they can steal personal information entered by the user that is useful in identity theft, make expensive calls using the victim's account or run down the battery quickly. In this paper, we will study mobile phone viruses and how they affect network stability.

Keywords: Virus, Cell Phones, Smartphones, Operating System (OS)

1.0 INTRODUCTION

Computing is turning modern mobile phones and smartphones into high targeted viruses' areas. We are reaching a situation where an increasing number of applications and services are available for mobile users. People today are accustomed to using mobile phones in everyday life and regularly people carry one with them. Mobile phones are no longer measly communication devices, but are used as organizers, data repositories, and containers for users' applications. In addition, mobile phones are utilized in accessing services and information content in the network. Traditionally, mobile phones have been closed platforms without any possibility for application development. However, due to great development in mobile phone industry, mobile phones today provide an open, truly everywhere computing platform for the applications. Considering this development and the role of mobile phones in people's everyday lives, it can be said that mobile phones are becoming fundamental tools in area of human empowerment. The problem of mobile phone viruses are expected to worsen as modern phone and smartphones developer continue to improve on the technology and as virus writers become more proficient in working with mobile phones (TMSMD, 2005).

Mobile phone viruses can compromise personal information, delete data, drain the battery (Racicm, R., 2006), and steal phone services by using expensive features (Dagon, D., 2004). The impact of mobile phone viruses on phone service providers includes increased customer complaints concerning infected phones and extra network congestion due to the virus-related traffic (Viveros, S., 2003). It is vital that the mobile phone manufacturing company anticipate and act now against these looming threats to dependable and secure mobile phone services. Because mobile phones are communications devices with many connectivity options, there exist many possible infection vectors (TMSMD, 2005)..

Previously, mobile viruses differed from computer viruses in using specific ways of propagating - via Bluetooth or to multimedia message service (MMS). However, the functionality of the .NET programming platform which is integrated into WinCE has enabled virus writers to exploit yet another, more traditional infection vector: email. For example, the Letum worm behaves in exactly the same way as thousands of typical PC email worms: once it gets onto a phone, it sends itself to all the email addresses stored in the infected device's contact list. Furthermore, Letum could be classified as a cross-platform virus, as it is capable of running on computers running .NET.

2.1 MOBILE PHONE

A mobile phone (also known as a cellular phone, cell phone and a hand phone) is a device that can make and receive telephone calls over a radio link while moving around a wide geographic area. It does so by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network. By contrast, a cordless telephone is used only within the short range of a single, private base station.

In addition to telephony, modern mobile phones also support a wide variety of other services such as text messaging, MMS, email, Internet access, short-range wireless communications (infrared, Bluetooth), business applications, gaming and photography. Mobile phones that offer these and more general computing capabilities are referred to as smartphones.

The first hand-held mobile phone was demonstrated by John F. Mitchell and Dr Martin Cooper of Motorola in 1973, using a handset weighing around 2.2 pounds (1 kg)(Heeks, R., 2008). In 1983, the DynaTAC 8000x was the first to be commercially available. From 1990 to 2011, worldwide mobile phone subscriptions grew from 12.4 million to over 6 billion, penetrating about 87% of the global population and reaching the bottom of the economic pyramid (Worldmapper, 2010).

2.2 MOBILE PHONE VIRUS

A mobile phone virus is a computer virus specifically adapted for the cellular environment and designed to spread from one vulnerable phone to another. Although mobile phone virus hoaxes have been around for years, the so-called Cabir virus is the first verified example. The virus was created by a group from the Czech Republic and Slovakia called 29a, who sent it to a number of security software companies, including Symantec in the United States and Kapersky Lab in Russia. Cabir is considered a "proof of concept" virus, because it proves that a virus can be written for mobile phones, something that was once doubted.

Cabir was developed for mobile phones running the Symbian and Series 60 software, and using Bluetooth. The virus searches within Bluetooth's range (about 30 meters) for mobile phones running in discoverable mode and sends itself, disguised as a security file, to any vulnerable devices. The virus only becomes active if the recipient accepts the file and then installs it. Once installed, the virus displays the word "Caribe" on the device's display. Each time an infected phone is turned on, the virus launches itself and scans the area for other devices to send itself to. The scanning process is likely to drain the phone's batteries. Cabir can be thought of as a hybrid virus/worm: its mode of distribution qualifies it as a network worm, but it requires user interaction like a traditional virus.

Cabir is not considered very dangerous, because it doesn't cause actual damage, and because users can prevent infection by simply refusing to accept suspicious files. However, the virus's code could be altered to create more harmful malware that might, for example, delete any information stored on phones it infects, or send out fake messages purporting to be from the phone's owner.

Another worm making its appearance in 2005 was CommWarrior. It also sends out copies of itself through Bluetooth®, and it can make automatic replies to texts, thus sending the worm on to other users. Doombot appeared in 2006, a Trojan horse virus that appears to be a downloadable cell phone copy of the game Doom 2. When it is downloaded onto a cellphone, it automatically installs both Cabir and CommWarrior, and then keeps the phone from operating properly.

RedBrowser has been most expensive for people, especially in Russia, and is another example of the Trojan horse virus. It makes text calls to a phone number in Russia, which are then charged to the user. Another mobile phone virus that has many people concerned is Flexispy, a bit of spyware that sends logs of the phone calls you make to an Internet server.

2.3 CROSS PLATFORM VIRUSES

The Cxover virus is the first cross-platform malicious program for mobile phones. When launched, it checks to see which operating system is running, and when launched on a PC, it looks for access to mobile devices via ActiveSync. The virus then copies itself to the mobile device using ActiveSync. Once it is on the mobile device, the virus attempts to perform the procedure in reverse, i.e. to copy itself to the PC. It can also delete user files on the mobile device.

The Mobler worm works a little differently. Once it’s launched on a PC (with a Win32 component), it creates a SIS file on the E: drive. The SIS file contains several empty files which are used to overwrite a number of system applications on the phone. The file also contains the worm itself which then copies itself to the phone's memory card and adds a file called autorun.inf. If a user connects a Mobler-infected phone to a computer and tries to access the phone's memory card, the worm will automatically launch and infect the computer. Mobler is a clear example of a cross-platform virus capable of running on totally different operating systems: Windows and Symbian.

2.4 NEW PLATFORMS

Prior to 2006, the two most frequently attacked mobile platforms were Symbian and WinCE, which are the main smartphone platforms. The appearance of the RedBrowser Trojan in February 2006 was an unpleasant surprise. This was the first time that standard handsets (i.e. not smartphones) were infected. RedBrowser targeted mobiles which use the J2ME platform to run certain applications.

Although until recently it seemed an impossibility, infecting almost every kind of mobile phone is now a reality. The very appearance of Trojans for J2ME is just as worrying as the appearance of the first worm for smartphones in June 2004. It's still difficult to assess all the potential threats. However, it's a fact that the standard handsets still outnumber smartphones and malicious users have now worked out how to infect a standard phone and use it for criminal purposes. This means that antivirus protection for such devices is becoming a relevant issue.

Also in 2006, the first proof of concept backdoor for BlackBerry devices was detected. However, it was written in Java, and according to Kaspersky Labs, therefore can't really be classified as malicious code for a new platform.

Some of the early versions of mobile viruses:

Cabir

Cabir not only developed own variants, which differ just by file names and composition of the installation file (SIS file), but also resulted in independent and at first sight completely dissimilar parasite families such as StealWar, Lasco and Pbstealer.

Lasco

The worm Lasco appeared as the first of these independent families. Apart from usual worm functionalities, it can also infect files, too.

Pbstealer

This harmful program was developed in China and was discovered on a hacked Korean Webpage with the online game "Legend of Mir".This Trojan overtook Cabir in Bluetooth spreading, but the authors also made this time an important change in the source code: The Trojan selects the address database of the mobile phone and stores it in a text file. This is dispatched via Bluetooth to the next found device at hand. This is where the designation Pbstealer -"Phonebook Stealer"- comes from.

Comwar

A further milestone in the development of mobile parasites was the worm Comwar, which was one of the first to also spread through MMS. Considering the enormous propagation of mobile threats, its functionality has to be classified as extremely dangerous - the range of Bluetooth enabled devices is 10 to 15 meters, whereas MMS has really no borders. At present, at least seven modifications of the Comwar worms are well-known. In the variant Comwar.g the author used for the first time the possibility of infecting files. To do this, the worm looks for other SIS files in the mobile phone and registers itself thereby waiting for another opportunity to spread further.

What is remarkable is the fact that Comwar hasn't yet become the "progenitor" of a number of other virus families. The reason for this is most probably traced back to the fact that its source code is unpublished. However Comwar, like Cabir, is used more as a "carrier" for other Trojans. Only the Trojan Stealwar is considered as predecessor of a new family, which is built up on Comwar. Stealwar is a worm, which contains parts of Cabir, Comwar and the Trojan Pbstealer and in this way has the ability for greater proliferation and therefore poses a higher risk.

The principle of MMS dispatch will however outweigh in the future all other kinds of spreading methods. This is especially since a serious weak point in MMS application under Windows Mobile 2003 is already known, which leads to a buffer overflow as well as to the execution of an arbitrary code.

Showing another dastardly side, Comwar.c used for the first time root kit technology. The worm hides itself in the list of processes and is in the task manager under the started applications, by defining its type of process as a SIS file (system file). The good news is that with the assistance of other programs, which list started applications and processes, it can be discovered without a problem. Different harmful programs for Symbian are using similar technologies at present, too.

Mobile viruses have technically grown out of its infancy and only the still relatively small distribution of smart phones is preventing the situation from getting out of hand so far. However, with each passing day that Symbian and Windows Mobile gain ground, it is probably only a question of some months until mobile viruses are as well an everyday topic in Asia, too.

What mobile viruses can do?

- Spread themselves through Bluetooth and MMS
- Dispatch SMS and MMS without your knowledge

- Infect Files
- Send infected files to people in your name (via email, WiFi, Bluetooth, etc.)
- Delete your personal information (e.g. address book, file, etc.) or steal confidential information
- Disable functions on the phone (SMS, games, cameras, etc.) or completely disable the whole device
- Allow external access to smart phones
- Exchange file icons and system applications
- Modify fonts and install other applications
- Fight anti-virus functions
- Install other harmful programs
- Transfer malicious code from the smartphone to a PC upon connection
- Lock memory cards
- Use up the phone battery much faster than usual
- Steal information

3. HOW TO PREVENT MOBILE PHONE VIRUSES

The cell phone industry has evolved in a different fashion than the PC industry. Rather than having one dominant operating system such as Windows, the cell phone industry has two platforms in use—the Symbian OS and the Windows Mobile OS. A virus writer must create a virus for one of these platforms, which prevents it from affecting the other because viruses are OS specific. And then the writer must take into account the myriad handsets available, the different network topologies of the providers, and more. Simply put, the lack of homogeneity found in cell networks when compared to the local LAN makes cell phones an unattractive target for anything but a proof-of-concept.

Secondly, the vector for spreading cell-based viruses limits their impact. With PC-based viruses, malicious code often sends copies of itself to every email address in an infected computer's address book and also starts searching the network—or even the Internet—for other computers to attack. With a cell-phone virus, Bluetooth is the major medium used to spread viruses between phones. Spreading viruses depends on close proximity between an infected cell phone and a potential new host.

The following three steps to reduce your exposure:

1. Limit use of Bluetooth: Bluetooth is a convenient way to pass phone numbers between cell phones or transfer calendar information. Because it is not authenticated, it is also a convenient way to pass viruses. Whenever possible, the use of Bluetooth should be limited or deactivated. One way to discourage its use is to turn it off in the default configuration.
2. Look into antivirus products: A number of antivirus companies have come out with specialized versions of their products for cell phones. Although not a necessity today, in the future you will need the same level of security for cell phones as laptops. It is better to do the research now and understand what is available.
3. Deploy a firewall: As more information is stored in mobile phones, it will be critical to protect them—limiting what connections go into and out of them. By deploying a centrally managed firewall on cell phones, you will take back control over what can happen on these mobile computing platforms.

CONCLUSIONS

Mobile devices have rapidly transformed from limited embedded systems to highly capable computing platforms. While such devices have long enjoyed significant diversity in hardware and operating systems, the rising popularity of modern phones especially smart phones and the ability to sell applications to users is leading to the establishment of standardized mobile software platforms and operating systems, such as Microsoft’s Windows Mobile, Google’s Android and Apple’s Mobile OS X.

Although all of them provide the latest technological services, many of them are unlikely to include security mechanisms including memory protection and separation of privilege, what makes these systems an increasing target for malware. Recent researches showed that as mobile phones included more applications, the risk of being maliciously manipulated raised too. Given that 10% of cellular users downloaded games to their mobile devices once per month and the wide availability of free ringtones, downloadable content and executables make mobile devices susceptible to malware propagated not only through the cellular network itself but also through Bluetooth and Wi-Fi because of the multiple communications interfaces it permits.

The impediment caused by mobile phone viruses on phone service providers includes increased customer complaints concerning infected phones and extra network congestion due to the virus-related traffic. Also these mobile phone viruses can compromise personal information, delete data, drain the battery, and steal phone services by using expensive features.

REFERENCES

Heeks, Richard (2008). "Meet Marty Cooper – the inventor of the mobile phone". *BBC* 41 (6): 26–33. doi:10.1109/MC.2008.192.

"ITU releases latest global technology development figures". *ITU*. 2010-07-09.

"Global mobile statistics 2012 Part A: Mobile subscribers; handset market share; mobile operators". *Mobithinking*. 2012-08-09.

"The world as you've never seen it before". Worldmapper. Retrieved 26 August 2010.

Saylor, Michael (2012). *The Mobile Wave: How Mobile Intelligence Will Change Everything*. Perseus Books/Vanguard Press. p. 5. ISBN 978-1593157203.

Trend Micro. Security for Mobile Devices: Protecting and Preserving Productivity, Dec. 2005.

D. Dagon, T. Martin, and T. Starner (2004). Mobile phones as computing devices: The viruses are coming! Pervasive Computing, IEEE, 3(4):11–15.

R. Racicm, D. Ma, and H. Chen (2006). Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery. SECURECOMM,

S. Viveros (2003). The economic impact of malicious code in wireless mobile networks. 4th Intl. Conf. on 3G Mobile Communication Technologies, pages 1–6.

http://www.eweek.com/c/a/Mobile-and-Wireless/This-Time-Cell-Phone-Virus-Is-for-Real/

http://books.google.com/books?id=YLL7LL6SA5QC&pg=PA24&dq=cell+phone+virus&hl=en&ei=ngK-TMfTB8Sp8AbDw5n8Bg&sa=X&oi=book_result&ct=result&resnum=7&ved=0CE4Q6AEwBg#v=onepage&q=cell%20phone%20virus&f=false