SETIT 2007
4th International Conference: Sciences Of Electronic, Technologies Of Information And Telecommunications
March 25-29, 2007 – TUNISIA

Dawn of the mobile malware: reviewing mobile worms

Usman Sarwar, Sureswaran Ramadass and Rahmat Budiarto

Network Research Group, School of Computer Sciences, University Science Malaysia

usman@nrg.cs.usm.my,

sures@cs.usm.my,

rahmat@cs.usm.my

Abstract: There is a new era of worm attack on mobile devices. In the past, worms on cell phones and PDA were more like science fiction but recently it is more than a reality. The objective of this paper is to brief the new threats on mobile devices and review the current hazards on it. We did taxonomy of current malware on mobile devices specifically worms and state their technical details.
Key words: Worm, Bluetooth worms, MMS worms, Cabir, Commwarrior, Lasco,

INTRODUCTION

A worm is a self replicating program which does not need to be part of the other program to propagate and are designed to exploit the vulnerabilities of the computers and policy flaws. In addition to replicate itself, the worms may be designed to do various tasks like deleting files on the host system, send document or itself for spreading by emails and more recent worms have multi-headed and carry other executables as their payloads. Worms can slow down the network traffic because of its reproduction.

Recently the mobile devices like cell phones and PDA are the new targeted platform for worms; using Bluetooth and MMS as their medium of propagation and distribution. Although few years back worms and viruses for these types of devices seems more like science fiction but now it is a hard fact. People are not aware that viruses and worms do exists on mobile devices and they use multiple ways like Bluetooth and MMS as a medium of proliferation. Mobile users may use Bluetooth for multiple purposes like transferring of data like Pictures and play network gaming; in doing so the worms from the infected device can infect the mobile device with worms like cabir.

As evolution from current generation to next generation phones are undergone there is a good possibility of powerful worms and higher epidemic in the future. Study released by McAfee Avert labs "The number of malicious software programs created for mobile devices is expected to reach 726 by the end of 2006, up from an estimated 226 at the end of 2005"[6]. Another survey conducted by Finnish company F-Secure stated in 2005 "Symbian malware is the vast majority in all mobile malware, but in our opinion this is not because Symbian would be any more insecure compared to other mobile platforms. The large number just shows how popular Symbian devices are, and thus they are the most interesting target for malware authors" [NVSR 03].

Following are the objectives of this paper:

1- To review the mobile worms capabilities and hazards.

2- To foresees the threats possibilities

3- To educate the mobile users about malware hazards

1- Discussion

1.1. Differences between mobile and pc worm

Worms on the mobile devices have somehow the similar characteristics of the computer worm but with the exception of limited processing power and specifically utilizing the features and functionality of these devices. Mobile worms use features like Bluetooth and MMS for its propagation. Although with limited resources these malicious codes are still destructive and will be communal sooner or later. Until now these worms shows different behaviors and give deficit to the device user for instance crashing the phone, high phone bills, stealing personal information.

In this paper we study two pioneers of worms on mobile devices specifically SymbOS/Cabir and Commwarrier

1.2. Symbian Cabir worm

Cabir worm is the dawn of new era to have malicious code on the limited computation power devices like phones and pda. Cabir is considered to be the first worm infection on mobile devices and targeted at Symbian OS. The worm was first discovered by Symantec on 14 June 2004.

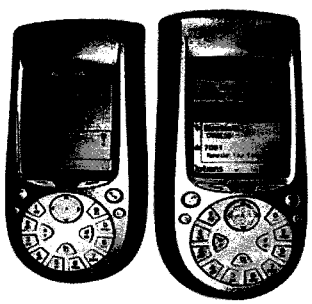

Figure 1

"The worm's code is compatible with mobile phones using ARM series processors with Symbian operating system such as Nokia 60 series. Normally the Bluetooth connection is off on these devices but as the users exchange data such as images and some little programs between their devices, and in doing so they open up the Bluetooth communication channel to Cabir-like worms as well" [PR 01].

Until now these worms risk rating by most of the anti virus companies is low to medium. But security experts are expecting to see high rating worms in near future as the devices are getting more powerful and common as well as tools written on these devices are also getting more complex and there will be vulnerabilities to be exposed by the worm writers.

Cabir worm uses three phases to spread itself. In the first phase, it searches for Bluetooth enabled devices and connect to the first device found even if it is a printer or mouse. In the second phase it sends the caribe.sis file to the device. And third stage disconnect from the device. The worm will restart first stage again and repeat all the phases on the same device until it is allowed to do so. Phase one dramatically reduces the battery power of the device but if Bluetooth is disabled worm will not turn it on and hence will not be spread.

Cabir worm arrives at the device as an installation package (.sis file) which encloses files or scripts and processed by Symbian operating system installation manager. After installation package is executed and the files are copied to their respective directories; package installation is destroyed. The installation package contains the three files which are illustrated in Table1.

File name	Size [bytes]	Description
caribe.app	11944	Application file
Caibe.rsc	44	Resource and necessary files
flo.mdl	11498	Mime recognizer file

Table 1. *Installation package*

In each replication cycle, Cabir copies itself to appropriate pseudo hidden directories. It also performs necessary configuration for auto restarting itself when phone is restarted. The mime recognizer file "flo.mdl" are used for auto restarting the application i.e. worm will be loaded again when phone restarts due to user or application intervention. Installation package also creates a Caribe.sis file which contains information of application removal. "The .SIS file is configured so that the Installation Manager will then run the extracted 'CARIBE.APP' file. This application runs on the ARM series of processors." [D 05]

After this procedure, Cabir start searching for phones with Bluetooth activation. After finding the target it sends itself to the other device as message. Target device will receive message with the same interface of mms. When the user

opens the message, it will start the installation manager and prompt the user to install it. As most of the users are not aware of phone malware they will press ok. Hence mobile device will be infected with the Cabir worm. Cabir worm can reach only mobile phones that support bluetooth, and are in discoverable mode. Setting your phone into non-discoverable (hidden) Bluetooth mode will protect your phone from Cabir worm.

Variants	Size [bytes]	Discovered Date	Infected File
cabir.a	11,944	16June04	cabir.sis
cabir.b	11,932	16June04	cabir.sis
cabir.c		09Dec04	Ni&Ai-.sis or MYTITI.sis
cabir.d		09Dec04	YUAN.SIS
cabir.e		14Dec04	Ni&Ai.SIS
cabir.f		21Dec04	Skulls.SIS
cabir.g		21Dec04	Tee222.SIS
cabir.h		27Dec04	velasco.sis
cabir.o	15,092	19Jan05	Mobile.sis
cabir.p		19Jan05	22207-SIS
cabir.r		19Jan05	Fuyuan.SIS
cabir.s	15,092	19Jan05	Guan4u.SIS
cabir.t		19Jan05	iLoveU.SIS
cabir.u		19Jan05	SEXXXY.SIS
cabir.v		02May05	GAVNOR.SIS
cabir.y		02May05	symTEE.SIS
cabir.z		31Aug05	QEXOOR.SIS
cabir.aa		24Oct05	INBOX.SIS
F-Secure are the first one to discover all the variants of Cabir worm. [J 04]			

Table 2. *Variants of Cabir worm*

Table 2 illustrates the different variants of cabir worm. One of the major released variant of cabir worm was cabir.h which has fixed replication routines and capable of spreading faster than other variants.

Execution of 'CARIBE.APP' displays a message, to show its presence on the device. These Messages varies from different Cabir variants like Cabir.A shows this 'Caribe-VZ/29a' and Cabir.B show this 'Caribe'. Once 'OK' is pressed by the user it takes 10 seconds to proceed. These are the variants of Cabir.

The Cabir worm did not create major havoc as may expected by the worm writer. It used Nokia 60 series specific user interface component which restricted it to those mobile phones only. It must have spread broader if the worm writer states this specific limitation. Another limitation is that it can only spread by using Bluetooth in discoverable mode. Hence if the phone is configured as non-discoverable (hidden) Bluetooth mode it will not get infected.

There are worm which are based on Cabir. For instance SymbianOS.Lasco . There are also Trojan horses which infiltrates the mobile devices and spread cabir worm. Following are the Trojan horses:

1- Cadomesk.A
2- Cardtrp variants
3- Dampig.A
4- Doomboot.B
5- Doomboot.F
6- Locknut
7- MGDropper
8- Skulls variants

1.3. Symbian Commwarrior

Commwarrier is another mobile worm which propagates using Bluetooth and MMS. It was first discovered in March 2005. It shows the capabilities of mass mailing itself by using MMS. It was designed to accomplish faster mobile propagation using MMS by spamming but it was depleted in epidemic. It was targeted for Symbian Series 60 smart phones and it propagates randomly named .sis file.

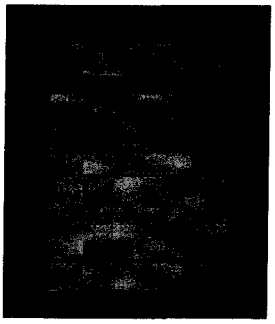

Figure 2. *Arrival of worm by Bluetooth*

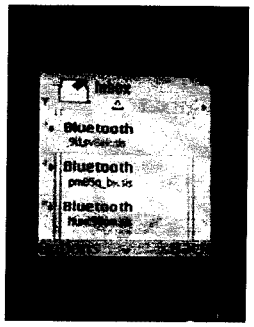

Figure 3. *After infection*

Worm starts working on the device by counting the number of processes that are running. If it founds another instance of itself then it exits or kills that process. Figure 1 and 2 illustrates the worm arrival on the phone [MJ 05].

Subsequently the worm retrieves the machine identification number, and calculates an additive

sum of the characters, to produce a unique value. This value might have been used by the worm's author during testing to avoid the infection of his own device, but now the result is simply discarded [FPE 05].

The replication approach of this worm is very interesting as it uses the different time frames for the infection. During the normal user working hours from 8am to 11:59pm it uses Bluetooth to spread itself as there will be good possibility of other Bluetooth devices within its range. During the normal user sleeping hours which are normally 12:00am to 6:59 am; it uses phonebook and sends itself by attaching with MMS. It sends MMS after every 10 seconds. The selection of phone number is done by enumerating every contact and looking for mobile number which means that land numbers are ignored. The purpose of this procedure is to maximize the propagation of infection to compatible mobile devices. From 7:00am to 7:59am it cleans up sent MMS carefully as well as message log afterwards. On 14th day of every month, worm's payloads activate and reboot the phone in silent mode.

"In addition worm sets a lower priority to replication threads, to make their activity less noticeable. The overall scheduling of the worm's replication is accomplished by a single timer, which is set to trigger after every ten seconds. Within the main timer callback, the worm ensure the payload condition, time of the day and the Bluetooth state, in order to pick a replication method."[PF 05]

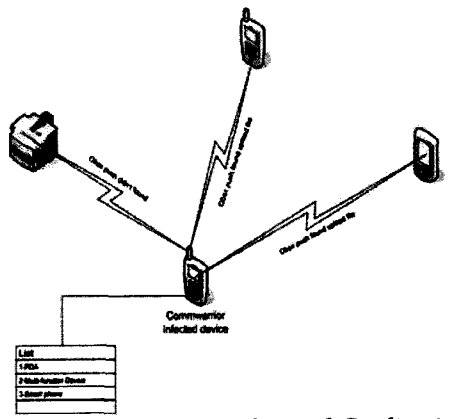

Figure 4. *Commwarrior Bluetooth Replication*

The replication method by using Bluetooth is different from SymbianOS.Cabir. Commwarrior enumerates the devices within its range and make a list of it. Then it inquires each device for Obex Push service which is required for uploading files. The devices which fulfill the requirements are sent SIS worm file with randomly generated lower case strings with eight character length. Figure 4, illustrates the Bluetooth replication. After accomplished the replication of worm to all the devices in the list it cleared up the connections and starts the new phase after 50 seconds.

Commwarrior is an advent of its kind and there will be more possibility in the future to have worms with this functionality. On 28 September 2005, F-secure reported that commwarrior was spread to twenty countries [F 05]

These are the variants of Commwarrior.

Variants	Size [Bytes]	Discovered date
Commwarrior.A		07Mar05
Commwarrior.B		08Mar05
Commwarrior.D	27,162	09Mar06
Commwarrior.J	27,162	06Jun06
Commwarrior.K	27,222	06Jun06
Commwarrior.L	27,018	06Jun06
Commwarrior.M		23Jun06
Commwarrior.N		23Jun06
Commwarrior.Q		01Aug06

Table 2. *Variants of Commwarrior worm*

These are the Trojans which infiltrates the mobile devices and spread commwarrior worm.

1- Fontal.D
2- Doomboot.A
3- Skudoo.A
4- Cardtrp.C
5- Doomboot.G

2 - Securing the device

Security experts advice the user to use Bluetooth carefully. Moreover they also suggest to open MMS with cautious. There are also antivirus softwares available from different security companies like Symantec and F-Secure to secure mobile devices.

3 - Conclusion

We have done comprehensive study on Cabir and Commwarrior. These types of worms will be more common in the near future as the next generation of phones will be more powerful and will be loaded with more complicated

applications as well as powerful hardware. Complicated and not well written applications can give opportunities to worm writers to exploit the vulnerability of the devices. There can be major epidemic if the attacker manages to utilize the functionality of the mobile devices which can make havoc in the mobile phone usage. Moreover mobile users need to be educated to reduce the chances of getting device infected as well as to have precautions for reducing the epidemic. Cabir and Commwarrior are the dawn for mobile malware we should expect more powerful worms later.

We can also expect the possibility of rapid global epidemic of mobile worms through MMS and moreover as the device users are not aware of the possibility of destruction by these worms, there can be major panic in using the cellular network and utilization of mobile devices. As we have seen the Commwarrior shows the low global epidemic in many countries [F 05].

REFERENCES

[AA 06] Kaspersky Security Bulletin, January - June 2006: Malicious programs for mobile devices. Alexander Gostev, Alisa Shevchenko

[B 04] Specification of the Bluetooth system.

[D 05] Mobile malware to triple in 2006, Dawn Kawamoto, CNET http://news.zdnet.co.uk/internet/0,39020369,39242892,00.htm

[F 05] Number of mobile malware close to 100. F-Secure https://europe.f-secure.com/wireless/news/items/news_2005092800.shtml.

[FPE 05] Symantec security response. Symbian OS Commwarrior, Frederic Perriot, Peter Ferrie and Eric Chien

[J 04] F-Secure Virus Descriptions : Cabir. Jarno Niemela F-secure http://www.f-secure.com/v-descs/cabir.shtml

[K 06] Kaspersky Lab,http://www.kaspersky.com

[M 06] Mcfee, http://www.mcafee.com

[MJ 05] F-Secure Virus Descriptions: Commwarrior.A. Mikko Hypponen, Jarno Niemela. http://www.f-secure.com/v-descs/commwarrior.shtml

[NVSR 03] A *taxonomy of computer worms*. Nicholas Weaver (UC Berkeley), Vern Paxson ICSI), Stuart Staniford (Silicon defense), Robert Cunnigham (MIT Lincoln Laboratory)

[P 05] *The Art of Computer Virus Research and Defense* by Peter Szor published by Addison Wesley Professional

[PF 05] Symantec security response, Virus analysis 'Commwarrior' paradise lost by Peter Ferrie and Frédéric Perriot

[PR 01] *Bluetooth: Technology for short range wireless apps* by Pravin Bhagwat, Reefedge Inc.

[RDH 06] Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery by Radmilo Racic, Denys Ma, and Hao Chen in *15th USENIX Security symposium, Vancouver, B.C, Canada.*