CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

An Analysis of Cabir Mobile Phone Virus

By

Jayanta Parial

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Issue Date: May 11, 2005

TABLE OF CONTENTS

1.0 Introduction:

A significant development in 2004 was the arrival of the mobile phone virus. It was talked about for a long time but the first virus that spreads from mobile to mobile phone was detected in June 2004.The first virus to come out was the SymbOS/Cabir. Fortunately the virus spreads with mobile phones running only on Symbian-60 series Operating Systems enabled with Bluetooth technology.

2.0 Bluetooth:

Cabir which first appeared as a proof of concept virus spreads using the Bluetooth wireless networking technology. The Bluetooth wireless technology provides short range, wireless connectivity between common devices. The current Bluetooth System specification defines security at the link level. Application level security is not specified, allowing application developers the flexibility to select the most appropriate security mechanisms for their particular application. The range of blue tooth is very limited with class 1 blue tooth devices having a range of around 100 m.

3.0 Symbian Operating System:

In 1998 leading companies dealing with wireless and wireless products established Symbian to create a standardized operating system for mobile phone application. Symbian operating is specifically designed for data enabled mobile devices. Symbian OS has its own application installation system and a special software management engine is included in the OS. This gives the user the possibility to view and uninstall already installed components. Installation packages (.sis files) are used for application delivery. Software developer kits include tools for application developers to create the installation package files consisting of the application components and data. There are several ways to install a SIS package on a device.

3.1 Installing from PC

Applications can be installed on a device from a PC using a serial cable, infrared or Bluetooth connection. This requires special installation software on the PC which is usually provided by the device manufacturer and delivered with the device.

3.2 Installing over the air

Applications can also be installed over–the air (OTA) using a mobile network . There are a couple of ways to implement OTA installation. The installation package can be linked for example to a WAP page that can be viewed with the device's browser. The user can then use the link to start the download. Downloading can be done protocol independently, but in most cases either the WAP or HTTP protocol is used. After the download has been completed, the device's software management engine completes the installation. WAP push can also be used for transferring the installation package to the device. It can be activated for example by an SMS message or from a web page.

4.0 Origin of CABIR:

The worm is supposed to have been written by a member of a grey-hat virus research group.

4.1 Nature of the virus:

This malware has been classified as a worm. Once active it will send a copy of itself to the first Bluetooth device it finds. But in order for the virus to be installed the user must confirm two software install dialogues- It thus also can be called a Trojan as it requires user intervention for installation. This virus has not been detected in the wild.

4.2 Risks from the Virus:

Only Symbian OS phones that use the Series 60 User Interface platform can be infected. Fujitsu FOMA phones are not enabled with installers hence can not be infected.
Anti virus Vendors have given Cabir a low rating.

4.3 Virus Propagation:

The virus has little chance of widespread propagation. The following are the pointers that prove the above statement.

1. The virus infects only the first Bluetooth device it finds for its onward distribution
2. The target device must be a Symbian series 60 device
3. The user must have Bluetooth switched on and set to be discoverable.
4. Phone must be within 30 meters of the receiving Bluetooth-activated Series 60 phone
5. The worm arrives on the phone as a Bluetooth message which has to be explicitly accepted by the user

5.0 Mobile Phones using Symbian Operating System

Following is a list of manufacturers using Symbian Operating System as their base operating system

1. Arima
2. BenQ
3. Fujitsu
4. Lenovo
5. LG
6. Mitsubishi
7. Motorola
8. Nokia
9. Panasonic
10. Sanyo
11. Sendo
12. Siemens
13. Sony Erricson
14. NTT DoCoMo

6.0 Countermeasures

The Trojan cannot spread in the wild and requires user intervention for its spread. The following are the recommendations for defense against the virus.

1. If Bluetooth is not required, it should be turned off.
2. While using Bluetooth enabled devices try to remain in the hidden mode.

3. Never install unknown packages
4. Avoid use of device pairing. If it must be used, ensure that all paired devices are set to "Unauthorized". This requires each connection request to be authorized by the user.
5. If infected use a proper anti virus product for cleaning the mobile phone.

7 Evolution of CABIR

The first version of Cabir was detected on 15th June 2004. Since then there has been a continuous detection of various version of the virus. The virus has also evolved into more complex mutants like the “Skull” and “MetalGear”. A chronological analysis of the various versions of the virus is given below.

7.1 CABIR.A

This virus was detected on the 15th of June 2004.

- Virus Installation The virus arrives as a SIS file. When the CABIR .SIS file is executed the installation manager extracts and installs the worm files in the directory ‘\SYSTEM\APPS\CARIBE’. The Installation Manager also creates a file named ‘\SYSTEM\INSTALL\CARIBE.SIS’, which contains only information about how to remove the installed application. 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.

- Virus Symptoms When the ‘CARIBE.APP’ file is executed, it displays a message announcing its presence. The message is ‘Caribe-VZ/29a’

- Virus propagation After copying the necessary file the worm creates a new .SIS file and tries to propagate using a three stage approach. The first stage searches for Bluetooth enabled devices and attempts to connect to the first one that it has found regardless of the type of device. The second stage sends the SIS file and the third stage disconnects from the target device. Immediately after disconnecting it searches for new Bluetooth enabled devices.

7.1 CABIR.B

This virus was detected on 16th June 2004. This virus was similar in all respect to the earlier version of the virus except that it displayed a different message “Carbie “upon infection.

7.2 SKULLS.A

The variant of Cabir was first detected on 19th Nov 2004. Skulls.A is a malicious SIS file Trojan that will replace the system applications with non-functional versions, so that all but the phone functionality will be disabled. The virus propagates like any other cabir virus

- Virus Installation: The virus comes as a .SIS package. The file name is Extendedtheme.SIS. The application files installed by Skulls are normal Symbian OS files extracted from the phone ROM. The malicious part is in the AIF (Application Info and icon) file which comes with the applications. Instead of correct AIF file the

Skulls SIS will install AIF file that has Skulls and crossbones as icon and instead of real application it will point to nowhere.
- Virus Symptoms: Once installed all the icons of the phone will be changed to skull and only receiving and answering phone call will be the functionality of the phone.

7.3 SKULLS.B

This variant of Cabir was detected on 29th Nov 2004.It has similar functionality to Skulls.A but it used different files. It is a malicious .SIS file Trojan which upon installation will replace the system application with non functional versions and drop the SymbOS/Cabir.B virus.
- Virus Installation: The virus does not install automatically. The user has to go to the Cabir icon on the phone to run it and once executed it tries to infect other Bluetooth enabled devices in the vicinity. The file name of the virus installation package is “Icons.SIS” and does not show any pop up message other than the security message when being installed.
- Virus Symptoms: The Skulls.B replaces standard application icons with generic application icon instead of skull and cross bones like Skulls.A did. Only simple phone calling and receiving functionality is available after infection.

7.4 Cabir.C

This variant of Cabir was first detected on 9th December 2004. Cabir.C is a minor variant of Cabir.B the only significant differences are that the Cabir.C displays different text on the start dialog when worm starts and that the Cabir.C spreads as Ni&Ai-.SIS instead of Cabir.SIS. Cabir.C displays text "Ni&Ai-" while Cabir.B displays text that contains just "Caribe"

7.5 Cabir.D

This Trojan was detected on 9th December 2004.Cabir.D is a minor variant of Cabir.B the only significant differences are that the Cabir.D displays different text on the start dialog when worm starts and that the Cabir.D spreads as MYTITI.SIS instead of Cabir.SIS. Cabir.D displays text "Mytiti" while Cabir.B displays text that contains just "Caribe". The battery life of the mobile is drastically reduced.
- Virus Installation: The file name of the virus package is MYTITI.SIS.

7.6 Cabir.E

This Trojan was detected on 9th December 2004.Cabir.E is a minor variant of Cabir.B the only significant differences are that the Cabir.E displays different text on

the start dialog when worm starts and that the Cabir.E spreads as [YUAN].SIS instead of Cabir.SIS. Cabir.E displays text "[YUAN]" while Cabir.B displays text that contains just "Caribe".
- Virus Installation: The file name of the virus package is [YUAN].SIS.

7.7 Cabir.F

This Trojan was detected on 21st December 2004. Cabir.F is a minor variant of Cabir.B the only significant differences are that the Cabir.F displays different text on the start dialog when worm starts and that the Cabir.F spreads as Skulls.SIS instead of Cabir.SIS. Cabir.F displays text "Skulls" while Cabir.B displays text that contains just "Caribe".
- Virus Installation: The file name of the virus package is Skulls.SIS.

7.8 Cabir.G

This Trojan was detected on 21st December 2004. Cabir.G is a minor variant of Cabir.B the only significant differences are that the Cabir.G displays different text on the start dialog when worm starts and that the Cabir.G spreads as Tee222.SIS instead of Cabir.SIS. Cabir.G displays text "Tee222" while Cabir.B displays text that contains just "Caribe".
- Virus Installation: The file name of the virus package is Tee222.SIS.

7.9 Metal Gear A

This Trojan was detected on 22nd December 2004. The virus looks for and disables anti virus software. This Trojan uses the same icon disabling technique as variants of Skull ans works in the same way as a Skull variant.
- Virus Installation: The file name of the virus package is SEXXXY.sis

7.10 Cabir.H.

This Trojan was detected on 27th December 2004. This is a recompiled version of the original Cabir virus. The main difference is that Cabir.H has a fixed replication routine and is capable of spreading faster. Unlike earlier variants of Cabir, the Cabir.H is capable of finding a new target, after the first one has gone out of range. - -
- Virus Installation: The file name of the virus package is velasco.sis

7.11 Cabir.I

This Trojan was detected on 27th December 2004. Cabir.I is a minor variant of Cabir.H being functionally identical to Cabir.H variant, with the exception that the I variant is recompiled and uses different binary.

7.12 Cabir.J

This Trojan was detected on 28th December 2004. Cabir.J is a minor variant of Cabir.H being functionally identical to Cabir.H variant, with the exception that the I variant is recompiled and uses different binary.

7.13 Cabir.K

This Trojan was detected on 30th December 2004. Cabir.K is a minor variant of Cabir.H being functionally identical to Cabir.H variant, with the exception that the K variant is recompiled and uses different binary.

7.14 Cabir.L

This Trojan was detected on 30th December 2004. Cabir.L is a minor variant of Cabir.H being functionally identical to Cabir.H variant, with the exception that the I variant is recompiled and uses different binary.

7.15 Cabir.M

This Trojan was detected on 3rd Jan 2005. This is a minor variant of the Cabir.B virus, the only significant differences are that the Cabir.M displays different text on the start dialog when worm starts and that the Cabir.M spreads as free$8.SIS instead of Cabir.SIS. Cabir.M displays text "free$8" while Cabir.B displays text that contains just "Caribe".

- Virus Installation: The file name of the virus package is free$8.SIS

7.16 Cabir.N

This Trojan was discovered on Cabir.N is a minor variant of Cabir.B the only significant difference is that Cabir.N Spreads in -SEXY-.SIS while Cabir.B uses Caribe.sis

7.17 Cabir.O

This Trojan was detected on 19th January 2005. It is a minor hexedit variant of cabir.B and with the exception of a few file names it behave identically as Cabir.B

7.18 Cabir.P

This Trojan was detected on 19th January 2005. Cabir.P is a minor variant of Cabir.B the only significant difference is that Cabir.P Spreads in 22207-.SIS while Cabir.B uses Caribe.sis

- Virus Installation: The file name of the virus package is 22207-.SIS

7.19 Cabir.R

Cabir.R is a minor variant of Cabir.B the only significant difference is that Cabir.R Spreads in fuyuan.SIS while Cabir.B uses Caribe.sis

- Virus Installation: The file name of the virus package is fuyuan.SIS

7.20 Cabir.S

Cabir.S is a minor variant of Cabir.B the only significant difference is that Cabir.S Spreads in guan4u.SIS while Cabir.B uses Caribe.sis

- Virus Installation: The file name of the virus package is fuyuan.SIS

7.21 Cabir.T

Cabir.T is a minor variant of Cabir.B the only significant difference is that Cabir.T Spreads in iLoveU.SIS while Cabir.B uses Caribe.sis

- Virus Installation: The file name of the virus package is iLoveU.SIS

7.22 Cabir.U

Cabir.U is a minor variant of Cabir.B the only significant difference is that Cabir.U Spreads in SEXXXY.SIS while Cabir.B uses Caribe.sis

- Virus Installation: The file name of the virus package is SEXXXY.SIS

7.23 Cabir.V

Cabir.V is minor hexedit variant of Cabir.B, with the exception of new filename Cabir.V behaves identically Cabir.B

7.24 Commwarrior

This worm is capable of spreading both over Bluetooth and MMS messages. The infected phone will start searching other phones that in can reach over Bluetooth and send infected SIS files to the phones it finds. The SIS files that Comwarrior sends are named with random file names, so that users cannot be warned to avoid files with any given name. In addition of spreading over bluetooth the Comwarrior will also read the users local address book for phone numbers, and start sending MMS messages containing the commwarrior SIS file.

The MMS messages are multimedia messages that can be sent between Symbian phones and other phones that support MMS messaging. As the name says the MMS messages are intended to contain only media content, such as pictures, audio or video, but they can contain anything, including infected Symbian installation files.

The Comwarrior contains following texts:

CommWarrior v1.0 (c) 2005 by e10d0r

ATMOS03KAMA HEAT!

The text "OTMOP03KAM HET!" is Russian and means roughly "No to braindeads".

8.0 Conclusion

It may be noted that the virus affects upper end mobile phones with Symbian OS and Series 60 UI. In Symbian Operation System that runs most of the High end mobile phones, the packages are developed are called SIS packages as they have a .SIS extension. Malicious packages are transmitted using Bluetooth and if the user installs or runs them the viruses infect the mobile phone users.To date, Trojan horses and proto-viruses aimed at smart phones have mostly failed to spread wildly. CABIR has managed to infect other phone in the vicinity using Bluetooth. However, Cabir's spread -- and the spread of all phone viruses -- is severely curtailed by the need for users to accept and install the programs.

9.0 References

1. F-Secure
2. Symentac
3. Virus Bulletin
4. **WildList**