International Journal of Advanced Research in Engineering Technology & Sciences
ISSN: 2394-2819
December-2015 Volume 2, Issue-12
Email: editor@ijarets.org www.ijarets.org

Mobile Phone Attacks, Security Precautions and Packages

Pawan Ahuja
Research Scholar
Department of Computer Science & Engg.
Sunrise University
Alwar

Sudhir Dawra
Associate Professor
Department of Computer Science & Engg.
Ideal Institute of Technology
Ghaziabad

ABSTRACT:
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.

INTRODUCTION:
The virus was created by a group from the Czech Republic and Slovakia called 29a, which 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.[1] 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.
The Cabir worm affects Symbian OS-based mobile phones running Nokia's Series 60 user interface. Once triggered, Cabir uses Bluetooth to send itself from one phone to another as a SIS package.[2,3] The package's filename depends on the Cabir version; examples include cabir.sis, caribe.sis, ni&ai-.sis, skulls.sis and velasco.sis. Cabir can only spread to phones that are in "discoverable" mode and the user must choose to install the SIS package. A flaw in early Cabir variants caused infected phones to only spread the malware to one new device when the worm was initially triggered and on each subsequent reboot. Virus writers have fixed this flaw in later Cabir variants and the worm can now spread to multiple devices each time it is triggered.

INSTALLATION:
When the main SIS package is installed, the following files are installed onto the device:

- c:\system\apps\velasco\marcos.mdl
  (Boot hook)
- c:\system\apps\velasco\velasco.rsc
  (Resource file)
- c:\system\apps\velasco\velasco.app (application)

When the worm runs, the boot hook file is copied to the correct location:

- c:\system\recogs

Interestingly, these variants share a bug with the original Cabir - the boot hook does not work on the 6600 (S60 2.x) platforms.[4]
The application and resource files are also copied when the worm runs, to the following directory:

- c:\system\symbiansecuredata\velasco\

These variants also are intended to remove older variants if they exist on the phone. The following files are deleted if they exist:

- caribe.app
- caribe.rsc
- flo.mdl
- caribe.sis

from the following directories:

- c:\system\apps\caribe\
- c:\system\symbiansecuredata\caribesecuritymanager\
- c:\system\recogs\
- c:\system\installs\
- c:\system\install\
- c:\nokia\installs\

Additionally, these directories are removed entirely if they are present:

- c:\system\apps\caribe\
- c:\system\symbiansecuredata\caribesecuritymanager\

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.[5] 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.

INFECTION:

When the caribe.sis file is installed the installer will copy the worm executables into following locations:

- c:\system\apps\caribe\caribe.rsc
- c:\system\apps\caribe\caribe.app
- c:\system\apps\caribe\flo.mdl

When the caribe.app is executed it copies the following files:
flo.mdl to

- c:\system\recogs

caribe.app to

- c:\system\symbiansecuredata\caribesecuritymanager\

caribe.rsc to

- c:\system\symbiansecuredata\caribesecuritymanager\

This is most likely done in case user installs the application to memory card.[6] Then the worm will recreate the caribe.sis file from worm component files and data blocks that are in caribe.app.
After recreating the caribe.sis file the worm starts to look for all visible bluetooth devices and send the SIS file to them.

SECURITY TIPS:

1. Most of the worms which use e-mail to propagate use Microsoft Outlook or Outlook Express to spread. If you need to use Outlook, download and install the latest Outlook security patch from Microsoft. In general, keep your operating system and applications up-to-date and apply the latest patches when they become available. Be sure to get the updates directly from the vendor.
2. When possible, avoid e-mail attachments both when sending and receiving e-mail.

3. Configure Windows to always show file extensions. In Windows 2000, this is done through Explorer via the Tools menu: Tools/Folder Options/View - and uncheck "Hide file extensions for known file types". This makes it more difficult to for a harmful file (such as an EXE or VBS) to masquerade as a harmless file (such as TXT or JPG).
4. Never open e-mail attachments with the file extensions VBS, SHS or PIF. These extensions are almost never used in normal attachments but they are frequently used by viruses and worms.[7]
5. Never open attachments with double file extensions such as NAME.BMP.EXE or NAME.TXT.VBS
6. Do not share your folders with other users unless necessary. If you do, make sure you do not share your full drive or your Windows directory.
7. Disconnect your network or modem cable when you're not using your computer - or just power it down.
8. If you feel that an e-mail you get from a friend is somehow strange - if it is in a foreign language or if it just says odd things, double-check with the friend before opening any attachments.
9. When you receive e-mail advertisements or other unsolicited e-mail, do not open attachments in them or follow web links quoted in them.
10. Avoid attachments with sexual filenames. E-mail worms often use attachments with names like PORNO.EXE or PAMELA_NUDE.VBS to lure users into executing them.
11. Do not trust the icons of attachment file. Worms often send executable files which have an icon resembling icons of picture, text or archive files - to fool the user.

REPLICATION:

Cabir replicates over Bluetooth in caribe.sis file that contains the worm main executable caribe.app, system recognizer flo.mdl and resource file caribe.rsc.[8] The SIS file contains auto start settings that will automatically execute caribe.app after the SIS file is being installed.

The caribe.sis file will not arrive automatically to the target device, so user needs to answer yes to the transfer question while the infected device is still in range.

When the Cabir worm is activated it will start looking for other Bluetooth devices, and starts sending infected caribe.sis files to the first device it finds. The replication routine in Cabir contains a bug that causes it to lock to first device it finds and it won't look for other devices.

This means that Cabir is capable of sending infected files to only one other device per activation. So Cabir will try to infect one other device when it is activated the first time, and then one more each time when the phone is rebooted.

Also in our tests we found that the newly infected phone will first look for the phone that sent the infected file.[9] So Cabir is capable of spreading widely only in cases where the phone that sent the infected file is out of range before user activates the Cabir in a new phone.

Which means, that while Cabir is capable of spreading in the wild, it would spread quite slowly and would not cause large epidemic

One curious fact is that in series 60 phones the Bluetooth functionality is independent from the GSM side, and if phone is rebooted the cabir will try to spread even if user doesn't enter PIN code.

REMOVAL INSTRUCTIONS:

F-Secure Anti-Virus for Symbian series 60 will detect the Cabir and delete the worm components. After deleting worm files you can delete this directory:

- c:\system\symbiansecuredata\caribesecuritymanager\

Clean up steps require that a third party file manager application capable of reading and writing to the system directories be installed on the phone.

Note that on the Nokia 6600 (and possibly other Series 60 2.x devices); the boot hook does not work. On these devices, the worm can be rendered inert simply by rebooting and uninstalling the application.[10] The infected files will be left on the drive, but they cannot be executed in such a state.

Using a file manager, delete the boot hook:

- c:\system\recogs\marcos.mdl

Reboot

Use the Manager application to uninstall "velasco".

Using a file manager, delete the following directory and all of its contents:

- c:\system\symbiansecuredata\velasco

REFERENCES:

1. Castells, M.1996. The Rise of the Network Society. Massachusetts: Blackwell. ISBN 1557866171
2. Cohen, F. 1984. Experiments with Computer Viruses. http://www.all.net/books/virus/part5.html (accessed 8 September 2004).
3. Computer Virus. 2004. http://www.campusprogram.com/reference/en/wikipedia/c/co/computer_virus.html.
4. Feldmen, T. 1997. An Introduction to Digital Media. London: Routledge. ISBN 0415151082
5. Hansen, E. 2000. New email virus bombards mobile phone users. http://news.com.com/2100-1023-241489.html?legacy=cnet (accessed September 8, 2004).
6. Harding, D. 2004. Hackers unleash mobile phone virus. http://www.thisislondon.com/news/articles/11405102?source=Metro (accessed September 8, 2004).
7. Hartley, J. 2002. Communication, Cultural and Media Studies: The Key Concepts - Third Edition. London: Routledge. ISBN 0415268893
8. History of Viruses. 2004. http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html (accessed 8 September, 2004).
9. Windows-run ATM hit by virus. 2003. http://p2pnet.net/story/354 (accessed September 8, 2004).
10. Zetter, K. 2000. How a computer virus works. http://www.cnn.com/2000/TECH/computing/10/23/virus.works.idg/ (accessed 8 September, 2004).