VIRUS ANALYSIS 1

CABIRN FEVER

Peter Ferrie and Péter Ször
Symantec Security Response, USA

It has been a long time coming, but in June 2004 the first worm arrived that spreads from mobile phone to mobile phone: SymbOS/Cabir. Fortunately, due to the fact that the worm uses a specific user-interface component, it is restricted to *Series 60*-based mobile phones.

BLUETOOTH

Cabir spreads using the Bluetooth wireless networking technology. The name of the technology comes from a translation of the name of the tenth century Danish king Harald Blåtand, or Bluetooth. Some say that it was Blåtand who united Denmark and Norway, and Bluetooth which unites the rest of the world. That would be for large values of 'unite' or small values of 'world', though, given the very limited range of Bluetooth.

ALL SIS-TEMS GO!

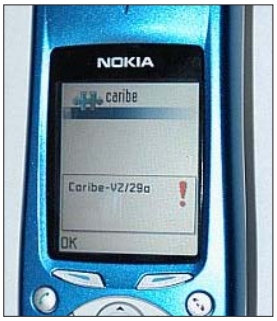
Cabir arrives as a .SIS file. A .SIS file is an installation package that contains files and/or scripts, and is processed by the Installation Manager that is part of the *Symbian* operating system.

When the Cabir .SIS file is executed, the Installation Manager will extract and place the worm files (CARIBE.APP, FLO.MDL and CARIBE.RSC) into the '\SYSTEM\APPS\CARIBE' directory.

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.

HELLO WORLD

When the 'CARIBE.APP' file is executed, it displays a message announcing its presence. The message is 'Caribe-VZ/29a' in the .A variant, and 'Caribe' in the .B variant. Once the user clicks 'OK', the worm waits 10 seconds before proceeding.



Cabir begins by checking the filename of the currently running file. If the filename is not 'CARIBE.APP', running from the directory C:\SYSTEM\SYMBIANSECUREDATA\CARIBESECURITYMANAGER' (note the hard-coded 'C:', which is the default drive but is not always used), the worm will create that directory, and copy itself there as a file named 'CARIBE.APP'.

The worm also copies the .rsc file to the same directory, as a file named 'CARIBE.RSC'. If there is a failure during the copying of the .rsc file, the worm deletes the 'CARIBE.APP' file that has just been created. Such a failure will prevent the worm from running by default, if the device is restarted.

Finally, the worm creates a directory named 'C:\SYSTEM\RECOGS', and copies to this directory the file named 'FLO.MDL'.

MIMETIC BEHAVIOUR

The 'FLO.MDL' file is a MIME recogniser. MIME recognisers that are present in the 'RECOGS' directory are called whenever applications are launched, and are used to prepare the environment for an application to run.

The 'FLO.MDL' file simply runs the 'CARIBE.APP' file from the 'CARIBESECURITYMANAGER' directory, rather than from the 'APPS' directory. This means that even if a user uninstalls the CARIBE application, the worm will continue to run. Additionally, files under the 'SYMBIANSECUREDATA' directory are not visible by default to users unless File Manager is installed, which is able to show these files.

The more recent models of *Series 60* devices do not allow MIME recognisers to run files in directories other than the 'APPS' directory.

After copying the necessary files, the worm creates a new .SIS file, using the .SIS file header that it carries, and the files that it has copied. This step is necessary because a .SIS file is usually deleted by the Installation Manager after an installation has completed.

FIRST CONTACT

Cabir attempts to spread using a three-stage approach. The first stage searches for Bluetooth-enabled devices, and attempts to connect to the first one that is found, regardless of the type of device (i.e. even a printer or a mouse will be attacked if they are in range).

The second stage sends the 'CARIBE.SIS' file, and the third stage disconnects from the target device. Immediately after disconnecting from the target device, the worm runs the first stage again. The worm will connect to the same device

again and again, for as long as it is in range. The cycle continues for as long as the worm application is allowed to run.

The first-stage search for Bluetooth-enabled devices causes a significant drain on the battery of the mobile phone – however, Bluetooth support can be switched off by the user, since the worm does not switch it on (though, by default, Bluetooth support is not enabled).

CLICK ON EVERYTHING

Cabir requires several interactive steps on the part of the recipient in order to execute. The first step is to accept the incoming connection request from another user (this would soon become a great many requests while the two devices remain in range of each other).

Having accepted the request, the recipient is presented with a warning that the supplier cannot be verified. However, this warning message is displayed by any application that originates from anywhere other than *Symbian*, even if that application is signed.

If the recipient elects to continue anyway, a final prompt is displayed that asks whether the recipient wants to install the application. Only if this prompt is accepted will the worm be installed and executed.

FLYING CIRCUS

Cabir introduces new problems to natural infection testing. Normally, it is sufficient to walk into a secure zone and work on an isolated network. In an attempt to test Cabir, one analyst tried to find the closest emergency evacuation bunker; another suggested running out into the middle of a deserted park with no one nearby. Although sending files through well built walls does not seem to work reliably, the wireless security of the virus labs needs to be prepared for wireless devices that use stronger signals.

What will be next? A mass mailer using MMS? A downloader using SMS? Ring, ring your virus is calling!

SymbOS/Cabir	
Size:	11,944 bytes (.A), 11,932 bytes (.B).
Type:	Mobile phone worm.
Payload:	Phone battery drained by search method.
Removal:	Delete the referenced files.