WORMS AND TROJANS GO MOBILE

Shaharudin Ismail and Zahri Hj Yunos
National ICT Security and Emergency Response Centre (NISER)

(This article was published in The STAR InTech on 24 March 2005)

Nowadays, mobile phones are installed with advanced operating systems such as the Symbian OS, Microsoft Mobile OS and Palm OS. Such mobile phones are also known as smartphones.

They have many great features such as built-in cameras for taking still and moving pictures, high-resolution colour screens, wireless data access, MP3 players, e-mail clients and even calendars and address books which can be synched wirelessly with the PC.[1]

Some smartphones are also equipped with Bluetooth and other wireless technologies, making them in effect tiny computers.

Symbian OS is the advanced operating system licensed by the world's leading mobile phone manufacturers such as Nokia, Motorola and Sony Ericsson. Designed for the specific requirements of advanced 2G, 2.5G and 3G (third-generation) mobile phones, Symbian combines the power of an integrated applications environment with mobile, bringing advanced data services to the public.[2]

Some of the smartphones that run on the Symbian platform are Nokia 6600 and 7610, Sony Ericsson P900 and P910, and Motorola A925 and 1000.

Bundled with an OS and multiple apps, these phones – just like PCs – are vulnerable to security threats like worms and Trojan horses.

Security experts and antivirus companies have identified the worms and trojan horses that have emerged on smartphones. Listed below are some of the identified malware:

Cabir

Cabir was the first to be identified. This worm uses Bluetooth to infect the phones and also to transfer itself to the new host as a file.[3] F-Secure (**www.f-secure.com**) researchers believe the author of the Cabir worm released the source code of the worm on the Internet as they have discovered two new versions of Cabir worm - Cabir.H and Cabir.I.

These new versions are able to search for and find new targets. They spread faster between mobile phones using a specially-formatted Symbian Installation System (SIS) file.

When infected, the mobile phone's screen displays the word "Caribe". The worms also modify the Symbian OS on the phone so that Cabir is launched each time the phone is switched on.[4]

The infected mobile phones also scans for vulnerable phones using Bluetooth. Finding a target, the phone then sends the velasco.sis file contains the Cabir worm.

Cabir.H and Cabir.I do not destroy data on the phones they infect. Instead, they block legitimate Bluetooth wireless connections and rapidly consume the phone's battery.

MetalGear

SimWorks Anti-Virus (**www.simworks.biz/sav/AntiVirus.php?id=home**) reported that this trojan horse combines several malicious mobile phone programs that work to spread over Symbian-based phones. The Trojan, a fake version of the *Metal Gear Solid* game, disable antivirus programs as well as other programs. It then installs the Cabir worms.[5]

If you see the program installer file, MetalGear.sis, on your phone, do not click on it.

If you run the program, it will install Cabir and another installer file called SEXXXY.sis.[6] This installer adds code that disables the handset's Menu button. ***Figure 1*** shows MetalGear in the smartphone's menu.

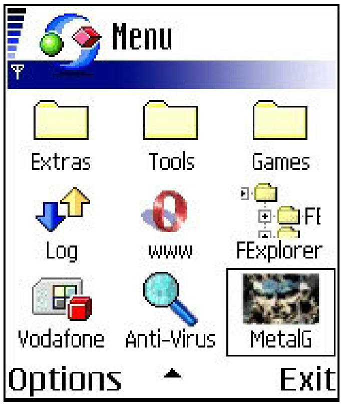

Figure 1

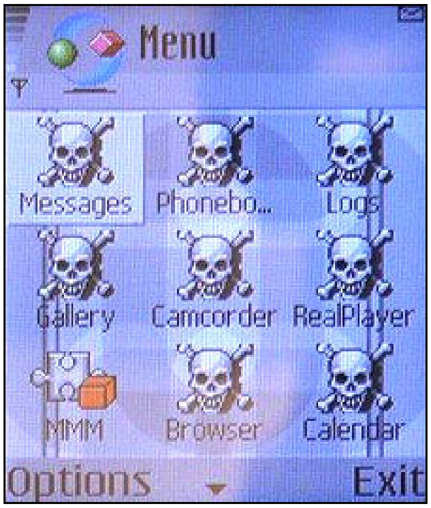

Figure 2

Skull.D

Skulls.D is another trojan horse. It disables applications, installs the Cabir worm and informs the user that his phone has been infected by displaying flashing skulls on the screen (*see **Figure 2***).[7] The latest Skulls trojan horse comes disguised as a new version of the *Macromedia Flash* player. Once the "program" is downloaded and installed, Cabir will be activated and it will overwrite all existing applications. [8]

Gavno.a and Gavno.b

Gavno.a and Gavno.b trojan horses masquerade as patches to trick users into downloading them. Gavno is the first Trojan aimed at disrupting telephony, a core function of mobile phones. This trojan disrupts text messaging and e-mail.

Gavno.a, which is around 2KB, comes disguised in a SIS (Symbian Installation System) file, called patch.sis.

Gavno.b, on the other hand, is tucked inside the patch_v2.sis.[9]

These trojans are believed to be from Russia. Antivirus experts believe the Gavno trojans can cause a lot of damage even though they are not sophisticated by design. [9]

How to mitigate these threats

Now that we know how to identify these threats, what can we do to protect our phones from them?

To date, most of the smartphone worms and trojan horses have failed to spread. In a few cases, Cabir.a managed to spread from one phone to another using Bluetooth. However, the spread of Cabir's viruses is severely curtailed by the need to accept and install the programs.[6]

Users can prevent attacks by disabling Bluetooth and declining to accept and install any new software from the networks, especially pirated software.

According to industry experts, users most likely to be hit by trojan horse programs such as Skulls and MetalGear are typically who like to download new software from Symbian freeware sites or peer-to-peer networks.[7]

The only way to get rid of trojans is to reset the infected phone to its default factory setting.[8] However, this means all the data and configuration will also be lost.

Conclusion

It is expected that this new mobile threat will become more serious in the near future. Bluetooth is a fine example of how technology can be abused to distribute mobile viruses.

In the future, not only will worms pose a security threat to smartphones, but also to other types of equipment that install and use the Bluetooth and other wireless technologies.

References

[1] *Versi terbaru OS telefon pintar Symbian*. 11 Feb 2005. Berita Harian – Komputer.

[2] http://www.symbian.com/technology/symbos-ds.html

[3] Lemos, R. *Worm ready to wriggle into smart phones*. http://news.zdnet.com/2100-1009_22-5233517.html

[4] Roberts, P. *New, virulent Cabir mobile phone worms spotted*. 28 Dec 2004. http://www.infoworld.com/article/04/12/28/HNcabir_1.html

[5] *'Metal Gear' Trojan targets symbian phones*. 22 Dec 2004. http://www.theregister.co.uk/2004/12/22/metal_gear_virus/print.html.

[6] Lemos, R. *Hybrid Trojan horse aims at Symbian phones*. http://news.zdnet.com/2100-1099_22-5500229.html

[7] Blau, J. *Trojan disguised as Flash player targets cell phones*. 07 Jan 2005. http://www.infoworld.com/article/05/01/07/HNflashtrojan_1.html

[8] Lemos, R. *Skulls program kills cell phone apps*. http://news.zdnet.com/2102-1009_22-5460194.html

[9] Blau, J. *Mobile malware kills Symbian service*. 24 January 2005. http://www.infoworld.com/article/05/01/24/HNmalwarekillssymbian_1.html

ABOUT NISER

NISER (National ICT Security and Emergency Response Centre) is a technical agency formed by the National Information Technology Council (NITC) and started its operation in November 2000. NISER has been specifically tasked to support the nation's Information and Communications Technology (ICT) security and cyber defence initiatives to avert potential intrusions and unlawful cyber-actions that could threaten the nation's critical infrastructure. NISER current services and efforts include of Incident Response (MyCERT), Computer Forensic Services, Security Assurance and Security Management & Implementation.

For further details, please contact NISER at:

National ICT Security and
Emergency Response Centre (NISER)
MIMOS Berhad
Technology Park Malaysia
57000 Kuala Lumpur
Telephone: +60 3 8996 5000 (General) | +60 3 8996 1901 (Direct Line)
Facsimile: +60 3 8996 0827
Email : info@niser.org.my | Website : http://www.niser.org.my