AMERICAN MARKETER

Business at its best

COLUMNS

A brief history of mobile malware

May 7, 2013

By AN AMERICAN MARKETER COLUMNIST

By Richard Clooke

Given the growth in popularity of smartphones over the last decade, the rise of mobile malware seems inevitable.

Malware always rises where there is a popular platform, a range of attack vectors and some means of monetization, and mobile devices offer all three. Yet, it was not always so.

Virus takes flight with bite
If we date the emergence of the smartphone back to 2000, with the launch of the Ericsson R380 and the Nokia 9210, it took over three years for the first examples of mobile malware to arrive.

We will look at how mobile phones have increasingly become the target of malware authors.

In June 2004, security researchers were sent copies of the first mobile virus, Cabir, a worm that infected the Symbian 60 OS.

Written by members of an international group of virus writers, 29A, it was a proof-of-concept virus written in C++ using Symbian and Nokia's own SDK.

Ingeniously, it used an attack vector common to nearly all Symbian smartphones, Bluetooth, appearing as a .SIS file installed in the phone's apps directory.

The virus itself was harmless, doing little more than displaying the message Caribe' on the phone's display every time it was turned on. It was not even released into the wild.

Unfortunately, it was not long before less scrupulous hackers found Cabir, and began to engineer their own variations.

By mid-2005 Cabir was the foundation for whole families of Symbian viruses, including Pbstealer, a Trojan that searched the phone's address book, then transmitted data obtained via Bluetooth to the first device in range.

Cabir might have been the first mobile virus, but it was not alone for long.

In August 2004 a Trojan was found in illicit versions of the Symbian mobile game, Mosquito.

Each time the game was played, the Trojan would send a premium SMS message to a certain number, making it the first mobile virus to take money from its victims.

By autumn 2004, Cabir and Mosquito had been joined by Skuller, another Symbian Trojan.

Skuller exploited a vulnerability in Symbian, replacing system icons with skull and crossbones alternatives, then delete application files.

It was a simple vandal Trojan, distributed through Web sites and forums as a theme file offering new icons and new wallpapers.

However, it was surprisingly successful, particularly when enhanced with the incorporation of code from Cabir to spread through Bluetooth.

Cabir, Mosquito and Skuller began a stream of viruses attacking the Symbian OS, replacing system apps, installing corrupt or malignant apps, or infecting user files.

The viruses spread via malignant apps, Bluetooth and MMS multimedia messages.

The latter vector allowed the malware to spread rapidly by replicating itself and sending copies to other phones listed in the owner's address book, as in the case of the CommWarrior virus.

This phase also saw the first examples of the cross-platform virus, with SymbOS Cardtrap not just deleting files and replacing system apps on the phone, but installing Windows malware on memory cards. Connect your phone, and you infected your PC.

New decade, new platforms, new threats

By early 2006, mobile malware was spreading to other platforms.

Viruses for Windows CE and Windows Mobile became more prevalent, with MMS vulnerabilities in Windows Mobile 2003 making it a particularly attractive option.

While the popularity of Nokia phones made Symbian the lead platform for virus writers until 2010, canny hackers had noticed an even more exciting opportunity: the Java platform for embedded systems, J2ME.

J2ME viruses had an advantage in that they did not just attack Symbian smartphones, but every mobile platform that supported the Java implementation.

The first J2ME virus, RedBrowser.A, used vulnerabilities in Java and SMS to send premium-rate SMS messages to a fraudulent contact, setting the dominant pattern for J2ME malware.

Between 2009 and 2010 there was an explosion in mobile malware, with numbers doubling, and as the fastest-growing platform, a large percentage of viruses focused on SMS fraud.

By 2009, the attacks were also growing increasingly sophisticated, with examples such as the Chinese SexySpace Symbian S60 virus kicking off by sending SMS messages with links to every phone number in the address book, prompting them to download pornographic content.

This is a trend that we have seen continue onto the Android platform.

Rise of Android malware

Launched in 2008, Google's Android operating system did not boast a big enough user-base to attract virus-writers in its first two years. But, by 2010, its potential as a platform for malware was clear.

Android simply was not as secure as Apple's iOS operating system. Google's open model made it possible for a range of app stores, some illicit, to operate, and made it easy for malware to use social engineering methods to propagate.

It was even possible to smuggle malware onto Google's own Android Marketplace store; difficult in Apple's more carefully controlled ecosystem.

The first Android Trojan, AndroidOS.DroidSMS.A, was a classic SMS fraud app, emerging in August 2010.

In the same month, another Trojan was discovered in the game TapSnake, with this one transmitting the GPS location of infected phones.

Meanwhile, the notorious FakePlayer app was allowed to spread under the guide of a Movie Player app. It was not the most effective video player, but it did a marvelous job of sending SMS messages to premium numbers.

By the end of 2011, Android had overtaken Symbian and J2ME to become the lead platform for mobile malware.

While iPhone users had not been entirely protected, the most serious threats only affected Jailbroken iPhones.

Android threats, however, were only becoming smarter.

Backdoor malware was allowing hackers to take control of infected devices, while Android spyware was stealing user-date and information that would make devices even more vulnerable.

The NickSpy Trojan even went so far as to record the owner's phone conversations and upload them to a remote server, while variants added text messages, call data, GPS coordinates and photos to the package.

The year 2011 also saw the first mobile Man in the Middle attacks hit the Android, BlackBerry and Windows Mobile platforms.

Working in conjunction with the successful Zeus PC Trojan, ZitMo (Zeus-in-the Mobile) worked to gather information, such as mobile authorization codes, from smartphones that could then be used with data gathered from the user's PC to access bank accounts.

WHILE GOOGLE has done much to beef-up Android security, Android's huge market-share 70 percent of smartphone sales in fourth-quarter 2012, according to Gartner guarantees that it will be the leading malware platform for the foreseeable future, particularly as its share of the tablet market develops to match.

The question is, what threats are coming, and what will the world's security experts do to repel them?

Richard Clooke is Norton mobile security expert and editor of mobilesecurity.com at Norton by Symantec, London. Reach him at richard_clooke@symantec.com.

American Marketer is published each business day. Thank you for reading us. Your feedback is welcome.