Malicious Code Moves to Mobile Devices

Neal Leavitt

The program was called Liberty Crack, and it first popped up on an Internet Relay Chat group. It was a Trojan horse, a program that includes malicious or harmful code in apparently harmless programming or data.

Although it did not cause major problems, Liberty Crack proved significant because it targeted handheld devices.

Such devices, which have communications and Internet-access capabilities, have become popular only recently and thus have not been significant targets of Trojan horses, viruses, and worms.

Now, however, malicious-code writers apparently realize that the relatively new intelligent-mobile technology has security weaknesses. Liberty Crack thus may serve as a wake-up call for the handheld-device and network-security industries.

"It exposed the underlying fact that destructive applications can be built on any platform, and given a lack of security or precautions, harmful results will ensue," said Kenneth Smiley, a senior analyst with Giga Information Group, a market research firm.

He added that the Liberty Crack incident might inspire more Trojan authors to write malicious code for mobile platforms. In fact, a virus and a Trojan horse that affect the PalmOS were recently discovered.

Not only could malicious code wipe out and damage data, applications, and operating systems in the future, it could also infect other handheld devices and spread across networks and the Internet to PCs, workstations, and other machines.

Currently, a relatively low percentage of handheld devices have communications capabilities. However, market research firm IDC estimates that by mid-2001, a majority of cellular and PCS telephones worldwide will be Internet-enabled using the Wireless Application Protocol (WAP).

IDC also predicts that by 2003, vendors will sell more than 19 million PDAs and 13 million smart phones worldwide and that 61.5 million mobile users will have two-way Internet access.

As the figure on the next page shows, mobile-device vendor Ericsson predicts that mobile Internet access will increase much more rapidly than fixed access. According to Ericsson, most Internet access will take place from mobile devices by the second half of 2003.

Therefore, vendors and users of handheld devices, such as smart phones and personal digital assistants (PDAs), are beginning to acknowledge the need for protection against malicious code.

Several antivirus software companies are already developing products for handheld devices.

However, the handheld community is likely to find itself in an arms race with virus writers looking for ways to defeat antivirus systems, as has long been the case with the PC community.

LIBERTY CRACK

Liberty Crack initially appeared on the Internet purporting to be a free hack for Liberty, a commercial software application that lets a PalmOS-based device run Nintendo Game Boy games. Liberty Crack supposedly would convert Liberty's free shareware version into the full commercial version. However, the program was actually a Trojan horse that removes third-party programs from the target device.

Initially, the Trojan crack appeared in Internet Relay Chat groups, then spread to the Web and newsgroups, from which users could download the program.

Potential for damage

Joe Hartmann, an antivirus engineer with antivirus vendor Trend Micro, said his company received no reports of infection from any of its customers. However, he said, unreported infections could have occurred, as users may not have thought about contacting antivirus vendors when they experienced PDA problems.

Users of PalmOS-based devices—including Palm products and such machines as Handspring's Visor and Sony's Clie—who execute Liberty Crack activate the Trojan horse. The Trojan horse then tries to delete third-party applications, as well as the data they contain, and reboots the device. Users would lose applications and data not saved on another machine.

However, Hartmann said, "The PalmOS itself is not destroyed." A user can hard-reset the unit, resynchronize it with a PC, and restore all programs and data saved during the most recent synchronization.

Several antivirus vendors have updated their desktop software to keep Liberty Crack from spreading to PCs, from which it could spread to handheld devices.

MORE MOBILE MALICIOUS CODE

Handheld devices have been hit by malicious code several other times within the past year.

Most early examples of mobile malicious code haven't had particularly harmful payloads.

However, said Trend Micro's Hartmann, "Future malicious code could attempt to mass-mail itself, target an operating system, infect files [in hard-to-detect ways], steal information, change data, and so on."

Phage

When executed, the Phage virus overwrites third-party PalmOS application programs, which will then no longer function as designed.

"The only option open to users is to delete infected applications and reinstall them from clean backup copies," said April Goostree, research manager for Network Associates subsidiary McAfee.com, an antivirus vendor and application service provider.

Like other types of mobile malicious code, Phage could have infected handheld devices from a PC during synchronization, from another device via infrared transmission, from an e-mail attachment, or from another device via the sharing of removable storage cards.

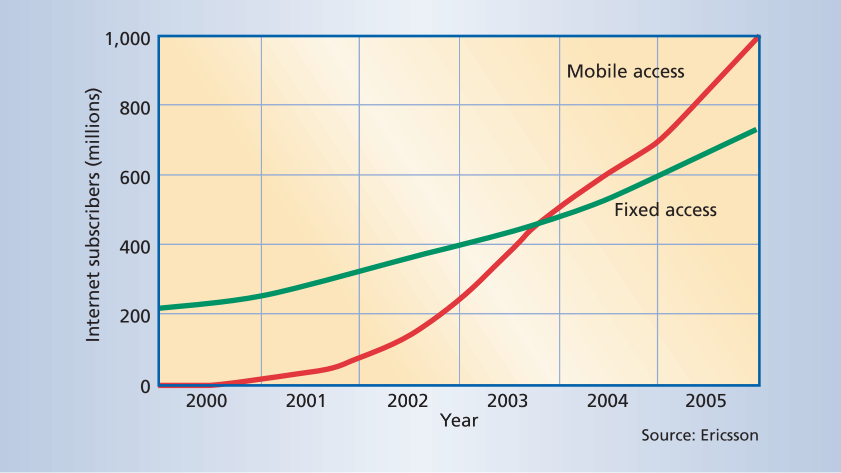
Vapor

Vapor is a Trojan horse disguised as an add-on application for PalmOS-based devices.

"Vapor doesn't delete itself or other applications. It simply causes them to be hidden to the user so that they appear to have been deleted," said Goostree.

NTT DoCoMo phones

Last June, a hacker spammed NTT DoCoMo mobile phones in Japan with an e-mail message containing a malicious script, known as Compact HTML. The message claimed to be a test and asked if users would drink from a girlfriend's half-empty coffee cup, knowing she had a slight cold. Users who clicked on "yes" ran the script, which dialed 110, Japan's equivalent of the US's 911 emergency services number.



Smart-phone vendor Ericsson predicts that mobile Internet access will begin increasing quickly next year and become more popular than fixed access in 2003.

Timofonica

Also in June, a Visual Basic Script worm spammed users of cellular phones and pagers operated by Spain's Telefonica.

Called Timofonica, the worm spread via an attachment to e-mail messages sent to PCs. The worm also sent itself as an e-mail attachment to addresses in a PC user's address book.

From PCs, the worm would send an e-mail message capable of being received by a mobile device via Telefonica's GSM (global system for mobile communication) gateway. The message was sent to random six-digit phone numbers formatted to look like Telefonica mobile numbers. It reached numbers that were valid.

When victims opened the attachment, the worm modified their device's registry so that the next time they booted the phone or pager, the worm would erase system information and leave the machine unable to boot again.

MISERY LOVES COMPANY

Referring to Timofonica, Susan Orbuch, Trend Micro's senior director of communications, said, "This worm showed how, as we connect [mobile] devices to the network, they, too, become susceptible to malicious code attacks."

As handheld devices develop new communications functions and connect to the Internet and corporate networks in greater numbers, the risk increases that the machines could spread malicious code to other handhelds and to PCs.

PCs are not susceptible to such attacks now. For example, PalmOS machines use PRC (Palm resource database) files that don't run on PCs. However, as PDAs become more powerful, they may begin using PC-compatible file formats.

"With an external modem, some of the newer handheld devices can transmit and receive file attachments," Orbuch said, "However, we have not yet seen any malicious code capable of spreading [widely] via this transmission method."

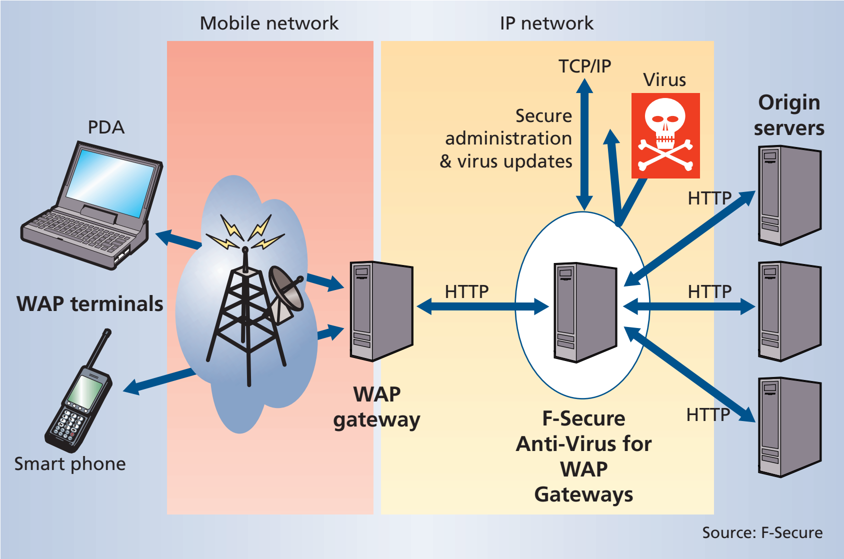
This problem may begin occurring, though, as handheld units become more powerful and their software becomes more functional. For example, handhelds may soon be able to execute embedded scripts, which have been used to infect PCs with viruses.

Meanwhile, PDAs usually contain an infrared transmission port allowing communications with IR-enabled PCs and laptops, said Eric Chien, a senior researcher for antivirus-software vendor Symantec.

"With IR capabilities, devices are able to receive and send applications and thus, potentially, malicious code," Chien said.

Even Bluetooth, a relatively new specification that wirelessly links various types of machines over distances up to 100 meters via radio transmitters, may be vulnerable.

"Bluetooth is another communication path, and wherever information travels,



Source: F-Secure

F-Secure's Antivirus for WAP Gateways product protects smart phones and PDAs from malicious code by checking transmissions to the devices as they arrive at the gateway between the IP network and the WAP mobile network. The product uses multiple scanning engines, each relying on a malicious-code signature database, to find Trojan horses, viruses, and worms. The code is then isolated so that it can't reach the handheld device.

so, too, can malicious code," Trend Micro's Hartmann said.

HANDHELD SECURITY: AN OXYMORON?

Handheld applications like Microsoft's Pocket Word and Pocket Excel don't currently support macros or executables. This eliminates two potential infection methods that have been used in some malicious e-mail attachments to infect PCs.

However, handheld devices are vulnerable to malicious code in many of the other ways that PCs are also susceptible. For example, the major mobile operating systems, including the PalmOS and Windows CE, provide reading, writing, and other standard file-operation functions.

"Such functionality is all that's needed for a viral threat to spread," said Symantec's Chien. And unlike some desktop platforms, he said, mobile operating systems don't limit the ability of code to modify system files.

Immature mobile security

Because handheld devices with communications capabilities are relatively new, vendors are still discovering and trying to solve security problems.

In addition, when vendors rolled out the first wave of intelligent handheld devices, security wasn't a top issue. Even now, said Giga analyst Jan Lundgren, "most vendors are focused more on functionality than security."

"Until the appearance of the PalmOS Liberty Crack Trojan horse program, security on handheld devices was not an area that had garnered widespread attention," said McAfee.com's Goostree. "But this is clearly no longer the case."

Megan Matthews, mobile technology vendor Nokia's director of media relations, said her company focuses on security and is also part of a manufacturers group working on a secure MeT (mobile e-commerce transaction) platform for building wireless e-commerce products.

Group members plan to provide such security services as encryption and authentication with a platform that includes wireless transport security layer (WTLS), wireless identification module (WIM), and public key infrastructure (PKI) technologies.

Currently, though, there is not much security against malicious code. For example, said Symantec's Chien, smart phones and other intelligent mobile devices use processors that aren't powerful enough to support the necessary security features. He said the devices' low storage and battery power also limit the capacity of security they can provide.

Emerging security technologies

Most current desktop-based antivirus products aren't designed to work with handheld devices. For example, PC antivirus products are too big to work within mobile machines' limitations.

However, because authors don't design PC viruses to run on handhelds, vendors can ignore such threats and develop more streamlined antivirus software to deal with mobile malicious code, said Trend Micro's Orbuch.

Thus, several antivirus companies have begun to release products for handhelds. For example, F-Secure recently introduced its F-Secure Antivirus for WAP Gateways product. As the figure on this page shows, the product checks for malicious code at the gateway between the IP network and the WAP mobile network, then keeps it from reaching a handheld device.

McAfee's VirusScan for Handheld Devices product prevents the transmission of known PDA viruses and catches any that may already reside on the PDA. The product, which supports a number of mobile platforms, scans for known virus signatures.

A MALICIOUS FUTURE

Malicious mobile code may take several new forms during the next few years.

As handheld devices develop more functionality, so will mobile malicious code. For example, as smart phones and PDAs develop new capabilities, such as the capacity to work with scripting languages, they will become more susceptible to Trojan horses, viruses, and worms.

"Future phones might be able to process scripts that can contain malicious code [that] could change address books or user data and potentially transfer them to other users," said Trend Micro's Hartmann

Also, handhelds may begin to face attack from malicious programs like 1999's Melissa and this year's LoveLetter, which sent themselves as e-mail attachments to people in victims' address books.

Many mobile applications are programmable, and other programs could interact with them via a standard application-programming interface, according to Symantec's Chien. Thus, a malicious program could send a launch code commanding the e-mail application to send messages with the program as an attachment to addresses in a victim's address book.

During the next few years, antivirus and other security software will become as common for handheld devices as they are for PCs, said McAfee.com's Goostree.

In addition, as handheld technology improves, permitting more memory and processor power, mobile antivirus software will provide more features, such as a virus information database, as well as more protection.

However, handheld vendors and users may find themselves in an arms race with virus writers.

"Malicious code in the wireless world has the potential to broaden its impact beyond the traditional computer network to other networks, such as the telephone network, that affect a much broader segment of society in a more tangible way," said Trend Micro's Orbuch.

"We'll find malicious code that will steal data and will cause denial of service on either the unit itself or another device," Hartmann said. "Wireless technology has the potential of enabling malicious code to jump off our computer networks and into our everyday lives in a way it never has before." ✷

__Neal Leavitt__ is president of Leavitt Communications, a Fallbrook, California, international marketing communications company with affiliate offices in Paris, France, and Hamburg, Germany. He writes frequently on Internet and technology topics and can be reached at neal@leavcom.com.

Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org