WIRELESS VIRUSES: COMING SOON TO A PDA NEAR YOU?

Kyle D. Lutes, Purdue University, kdlutes@tech.purdue.edu
Charles N. Thurwachter, Purdue University, cnthurwachter@tech.purdue.edu

ABSTRACT

Industry analysts predict that by 2003, more people will be accessing the Web from wireless and handheld devices than from conventional PCs. As mobile computer vendors attempt to build market share by rushing to deliver new products, it is no doubt security features will be of low priority. Although only a few software viruses for mobile computers have been reported to date, they have not received the same degree of media attention as the viruses that target personal computers (PCs). However, as mobile devices gain in popularity, we should expect to see a rise in viruses that target these devices. In this paper, we examine the current state of affairs concerning viruses that affect mobile computers. Topics include the viruses reported so far, probable reasons why few exist, technology changes that will enable new viruses to be developed and proliferate, and how anti-virus software companies are reacting.

Keywords: Security, virus, wireless, mobile computer, PDA, cellular phone

INTRODUCTION

Industry analysts predict the number of mobile computing devices in use will skyrocket in the next several years. For example:

- In March 2001, Gartner Group Inc. projected sales of 700 million cellular phones, 30 million PDAs and 10 million pagers per year by 2004, with individuals commonly carrying three computing and communications devices beginning as soon as 2002 (7).
- In May 2001, UK market research company Canalys reported sales of Compaq's iPaq handheld computer had increased by 1,018% in Western Europe for the first three months of 2001 when compared with the same period last year. The Canalys data also reported that Palm's shipments of PDAs increased by 60%, Casio's by 172% and Hewlett-Packard's by 107% (2).
- An October 2000 Computerworld article predicted that by 2003, more people will be accessing the Web from wireless and handheld devices than from conventional PCs. For example, International Data Corp. (IDC) in Framingham, Mass. predicts there will be 720 million mobile Internet subscribers, compared with 525 million wired users by that time (5).

With these large numbers of devices in use, one might also expect there to be a large number of computer software viruses that target these platforms. In fact, only a few viruses for handheld computers have been reported to date, and they have not received the same degree of media attention as the viruses that target PCs. For simplicity's sake, in this paper we use the general term "virus" to mean any code developed with malicious intent (e.g. viruses, worms, and Trojan horses).

We believe there are three key reasons why virus writers likely have not created viruses for these kinds of devices:

1. There is a lack of a defacto standard software platform, which decreases the ability for a virus to rapidly spread.
2. Programming for their operating systems is a skill limited to a minority of software developers.
3. Transferring data into a handheld device is typically done by "synchronizing" it with a PC, which allows software running on the PC to protect the mobile device from virus infected files.

For the following reasons, we also believe these barriers will fall in the very near future:

1. The Palm OS and the Windows CE OS, are quickly becoming the defacto standard OS for handheld devices.
2. New software development tools have recently been released that greatly simplify the task of developing software for both the Palm operating system (OS) and the Windows CE OS.
3. And finally, the expected rise in wireless networks will create new and uncontrolled backdoors into mobile devices.

As mobile devices continue to gain in popularity and as it becomes easier to infect a mobile device with a virus, we expect to see an increase in the reports of damage caused by viruses.
Viruses will be developed that attack the mobile device itself, or they may use the mobile device as a carrier for a virus that attacks PCs.

REPORTED VIRUS ATTACKS

The Phage virus that hit many Palm OS devices in September 2000 is the first documented PDA virus. This virus has the capability to affect devices manufactured not only by Palm, but others running the Palm OS. This includes devices manufactured by Handspring, IBM and Symbol Technologies. It has the potential to destroy all programs and files on the mobile device. It travels on the optical link that many Palm OS devices use to link to PCs through a docking station. Hence it is classified as a wireless virus.

The Phage virus infects files by overwriting the beginning of executable files found in the Palm OS device. When the virus is transferred to a Palm device and executed, any application running is immediately terminated, the screen goes blank or gray for a moment and the program executes during that time, thus not doing anything visible. It infects all other programs found in the system, thus all other applications in the system will repeat this same behavior when executed.

"Liberty Crack" was discovered about a month before the Phage virus. Because it does not have the ability to travel from one device to another, it was not classified as a true virus. But that doesn't mean it is not damaging. Liberty Crack arrives masquerading as a "crack" for the Liberty application, which allows a Palm OS device to run Nintendo GameBoy games. When run, it attempts to delete all add-on applications from the handheld device (13).

The first documented virus to target mobile phones was reported in June 2000. This virus, called Timofnica, targeted mobile phones in a region of Spain, and was very similar to an Internet worm virus

in structure. It was written in Visual Basic Script (VBScript) and used the Microsoft Outlook address book to mail itself to all addresses found. The virus sent messages to mobile phones using the Short Message Service (SMS) email service to randomly generate telephone numbers for Spain's Global System for Mobile Communications-based Movistar mobile phone service. The SMS messages spammed mobile phone subscribers with statements critical of Telefonica. Its impact to the mobile phone subscriber was relatively harmless, as there is little modifiable data in the mobile phones. However, it was damaging to the wireless service provider (6, 9).

A more recent mobile phone virus that targets Internet-enabled phones was reported in Japan. Japanese cellular giant NTT DoCoMo is uncontested as the world's largest wireless Internet service with over 20 million subscribers (3). DoCoMo's i-mode service, is an always-on Internet service that gives users access to email, web sites, and other Internet-based services via special wireless phones.

In June 2001, DoCoMo issued a statement acknowledging that over 13,000,000 i-mode phones, including 12 different models produced by five different manufacturers, are susceptible to the virus in the form of an email. Features built into DoCoMo's phone software allow email to contain embedded dialing instructions. The malicious email involved in this attack instructs the phone to automatically dial "110" (Japan's equivalent of the US "911" emergency number), and to mass dial randomly generated phone numbers. Variants of the virus can lock up the phone's functions, which require the user to "reboot" the phone by removing and reinserting the unit's battery (4, 12).

PLATFORM STANDARDIZATION

One barrier for virus writers has been the lack of a defacto standard mobile computing platform. Without a standard platform, a virus has a difficult time spreading to other devices. Microsoft Outlook is a virtually universal email client for desktop PCs and when Microsoft added scripting capabilities, Outlook became a target for virus writers. The most famous is the so-called Love Letter virus, which hit in May 2000. This virus sent itself to everyone in the user's Outlook address book and then destroyed local files. It has the distinction of being the fastest spreading virus in history. Within six hours of the first infected email being sent, it affected more than a million computers and caused in excess of $100 million in damage (8).

While we don't predict a single mobile computing platform to achieve the dominance Outlook has as an email client, we do expect PDA standardization to occur primarily on two platforms – Palm OS and Pocket PC (a version of Windows CE). Palm has long been the market share leader, currently with about 74%, but demand is surging for devices based on Microsoft's Pocket PC platform. So much so that in April 2001 Gartner Group Inc. predicted Palm to command only 50% of the market in 2003. Similarly, November 2000 research company IDC predicted that by 2004 Microsoft will have almost 40 percent of the market, compared with 51 percent for Palm (1, 14).

As further evidence, in a July 2001 announcement, Psion stated they were abandoning development of new PDA devices and would instead focus on providing digital networks for businesses. In the announcement, The UK tech company cited heavy competition from Palm, Compaq and Microsoft. Psion has sold between five and six million PDA units since it entered the business in the 1980s (15).

In addition to PDAs, another type of mobile computing device is the so-called smartphone. Currently, most smartphones run Symbian's EPOC OS. But just as Symbian adds PDA-like features to EPOC, they are beginning to face competition from Palm and Microsoft as they add phone technologies to their OSs. Eagerly awaited are phones based on Microsoft's "Stinger" technology, which reportedly will be available fourth quarter 2001.

Stinger devices are fundamentally phones, but also run a version of Windows CE. They combine data and voice functions, and will run the types of applications commonly found on PDAs. Stinger has a very functional web browser, and users will be able to download and install applications over the web. A unique feature for these phones is that wireless service providers will be able to use SMS to automatically push user settings, email, and other data to the phone when it is activated. Given Microsoft's history of offering features over safety, expect to see early Stinger devices as an easy target for virus writers.

SOFTWARE DEVELOPMENT TOOLS

Software development for PDAs and smartphones has historically been the domain of a small number of C++ programmers. However, new tools are being released that allow software to be developed for both the Palm OS and Windows CE using the relatively simple Visual Basic programming language.

Microsoft's eMbedded Visual Tools 3.0 package includes both eMbedded Visual Basic and eMbedded Visual C++. Though not as powerful as Visual Basic or Visual C++, eMbedded Visual Tools nonetheless contains everything a developer needs to write applications for Windows CE. eMbedded Visual Tools is available for free from Microsoft.

Virus writers that target Microsoft Outlook are able to create viruses that email themselves to others because Outlook and its components (contacts, calendar, email, etc.) are available to external code via a COM interface. Although currently not well known, the Pocket Outlook Object Model (POOM) SDK offers the same potential for misuse for viruses targeting Pocket Outlook running on Pocket PC devices. The POOM SDK is also available for free from Microsoft.

Developers familiar with Visual Basic can also use the AppForge software development tool to develop applications for the Palm OS. AppForge is not a stand-alone product, but rather it works with the Visual Basic 6.0 environment to allow developers to code and test their PDA applications under Windows. AppForge announced version 1.2.1, which includes wireless Internet support. Version 2.0 of AppForge is expected to be released August 2001 and will include support for the Pocket PC platform in addition to Palm OS. Theoretically, a virus writer using AppForge will be able to use a single set of source code to write a virus that attacks both Palm OS and Pocket PC devices.

WIRELESS NETWORKS

The expected rise in wireless networks will create new and uncontrolled access to mobile computing devices. One drawback with the transfer of data over a wireless link is that since there is no physical security to the path the data travels, it is fundamentally less secure. For example, in July 2001, Tim Newsham, a researcher for security firm @Stake, presented the details of weaknesses in the password system of wireless networks that could lead to a break in security in less than 30 seconds. Specifically, wireless systems that rely on a 64-bit key – used in many homes and earlier hardware – can be broken in less than a minute (10).

The big question is who will assume responsibility for security and prevention of the spread of viruses. If we look at the history of the wired world, depending on the devices and users for protection is far from optimal. Instead, users should rely on the wireless service providers for email content inspection, filtering, blocking, and neutralization. This should be a basic feature of all wireless data services, but so far, mobile computing device manufacturers have paid little attention to the threat of wireless viruses and unwanted spam.

COUNTERMEASURES

The anti-virus software vendors are offering new products to combat the emerging problem of viruses that target mobile computers. As of this writing, most are developed for the Palm OS and Windows CE. Most are approaching the problem from the perspective that the real danger is the handheld device acting as a virus carrier. The handheld is typically infected while reading email with a wireless modem. This class of product is at least an effective line of defense for the traditional PC being attacked. But it does not protect handheld users from downloading viruses, from the web, email or even the infrared links that are targeted at the handheld. Products that target viruses intended for the handheld are still in their infancy.

One of the core problems with developing a product for the handheld is that traditionally these virus scanners work by using a database of known virus signatures. That approach is still possible today, with the number of viruses so small, but it looms as a real problem for the future. To get an idea of the scale of the problem, today there are about 50,000 known desktop viruses. If a similar number emerge for the handheld class of device, the database will become too large to be stored on many of these devices. There are other approaches, one being looking for patterns of behavior. If a program starts to delete a file, for example, the virus protection software would halt the process and alert the user.

McAfee has issued a Liberty fix that runs on PCs, but both McAfee and Palm acknowledge that they do not expect to offer virus checking software that runs on the handheld soon. The core reason is that virus checking is a processor intensive procedure, and PDAs running on battery power, with limited memory and storage space, are not up to the task. In other words, the traditional approach of client based anti-virus protection is a nonstarter. As suggested above, wireless clients will have to depend on their wireless service providers to provide protection.

More recently, McAfee has released VirusScan Wireless 2.0, ananti-virus program designed to protect devices running Palm and Pocket PC operating systems from viruses. In March, 2001, Symantec

shipped Symantec AntiVirus 2001 for the Palm operating system. Both of these programs are designed to protect PDAs from viruses delivered over infrared wireless connections or during synchronization with the desktop PC.

However, these programs run on the desktop PC and as of June 2001, have only three virus definitions in their database. To address this limited database, they include an auto update feature that retrieves updated definitions from the anti-virus vendors as they become available.

These work in a somewhat different way than the products they offer for the desktop PC. For example the McAfee product places a small amount of code in the client PDA (3 KB), and a much larger piece of code in the desktop PC (250 KB). The small code block enables communication with the larger code element in the PC. The larger code element searches for Windows viruses while the PDA is synced with the PC, rather than searching for Palm based viruses. The theory is that since most viruses are still written for PCs, any new PDA virus will probably be sourced from a Windows environment and hence is most susceptible to being captured during the optical link transfer to the PDA.

This underlies the current thinking by anti-virus vendors. While it is true that viruses could erase PDA files, the real danger is those viruses erasing files in the desktop environment. The concern is that the PDAs will become carriers for moving viruses between PCs, in a similar way to how one child with a cold can infect an entire classroom. Ryan McGee, a product manager for the McAfee anti-virus software company, said “Handheld devices are almost as dangerous to a corporate network as the floppy disk (11).”

CONCLUSION

Industry analysts predict the number of mobile computing devices in use will skyrocket in the next several years. As mobile computer vendors attempt to build market share by rushing to deliver new products, there is little doubt that security features will be of low priority. Only a few software viruses for mobile computers have been reported, but we predict that will change in near future. Analysts also predict that by 2004, the Palm OS and Pocket PC platforms will command over 90% of the PDA market share. New software development tools based on the popular Visual Basic programming language are being released that relatively easily allow software to be written for these platforms. And finally, the expected rise in wireless networks will create new and uncontrolled access into mobile devices.

Even as the threat of software viruses looms, we believe users will take an apathetic approach to virus prevention. Only after a highly publicized virus infects a mobile device network will consumers react and demand that technology vendors offer some sort of protection. But by that time, millions of dollars in damage will likely have already occurred.

REFERENCES

1. Brewin, B. (2001, April 24). Analysts: Pocket PC emerging as Palm challenger. Computerworld. Retrieved July 13, 2001, from http://www.cnn.com/2001/TECH/ptech/04/24/pocket.pc.palm.idg/index.html
2. Compaq iPaq creeping up on Palm. (2001, May 16). Computerweek. Retrieved July 13, 2001, from http://www.computerweek.co.za/pebble.asp?relid=9302
3. Creed, A. (2001, March 4). DoCoMo I-Mode Subscribers Top 20m Mark. Newsbytes. Retrieved July 13, 2001, from http://www.newsbytes.com/news/01/162685.html
4. Delio, M. (2001, June 15). Hello 911, I've Got a Virus. Wired News. Retrieved July 13, 2001, from http://www.wired.com/news/wireless/0,1382,44545,00.html
5. Drew, R. (2000, October 9). Bracing For The Boom. Computerworld. Retrieved March 9, 2001, from http://www.computerworld.com/cwi/story/0,1199,NAV47_STO52068,00.html
6. Kobielus, J. (2000, July 5). Handhelds Will Get Hammered. Network World. Retrieved July 13, 2001, from http://www.pcworld.com/news/article/0,aid,17526,00.asp
7. Lawson, S. (2001, March 22). Gartner: users will adopt wide range of handhelds. IDG News Service. Retrieved July 13, 2001, from http://www.idg.net/idgns/2001/03/22/GartnerUsersWillAdoptWideRange.shtml
8. Legard, D. & Lawson, S. (2000, May 5). Love Letter worm rated most damaging ever. IDG News Service. Retrieved July 13, 2001, from http://www.idg.net/idgns/2000/05/05/LoveLetterWormRatedMostDamaging.shtml
9. Lemos, R. (2001, March 19). Handhelds: Here come the bugs? ZDNet News. Retrieved July 13, 2001, from http://www.zdnet.com/zdnn/stories/news/0,4586,5079712,00.html?chkpt=zdhpnews01
10. Lemos, R. (2001, July 12). Wireless networks lure hackers. ZDNet News. Retrieved July 13, 2001, from http://www.zdnet.com/zdnn/stories/news/0,4586,5094057,00.html
11. Niccolai, J. (2000, August 30). McAfee aims to shield networks from PDA viruses. IDG News Service. Retrieved July 13, 2001, from http://www.cnn.com/2000/TECH/computing/08/30/mcafee.pda.shield.idg/
12. NTT DoCoMo to Advise Customers about Malicious E-mails. (2001, June 13). Retrieved July 13, 2001, from http://www.nttdocomo.com/new/contents/01/whatnew0613.html
13. PalmOS/LibertyCrack. The Association of Personal Computer User Groups. Retrieved July 13, 2001, from http://www.apcug.org/news/palmtrojan.htm
14. Pocket PC devices making headway against Palm. (2000, November 28). Bloomberg News. Retrieved July 13, 2001, from http://news.cnet.com/news/0-1006-200-3894179.html
15. Psion pulls out of handheld market. (2001, July 11). BBC News. Retrieved July 13, 2001, from http://news.bbc.co.uk/hi/english/business/newsid_1433000/1433275.stm