GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

A Virus in the Palm of my Hand

Computer viruses and trojan horses have become commonplace in the PC desktop environment. Almost everyone familiar with a computer has heard stories of lost data, crashed hard drives, and funny, but potentially dangerous, pop-up screen messages. The Melissa virus helped break the virus problem into mainstream media, with television news show coverage and even jokes on the David Letterman show. Everyone with a PC is now more aware of viruses, and how to take precautions against them.

However, another emerging market is also gearing for an influx of malicious code. The PDA (Personal Digital Assistant) market consists of the Palm, Microsoft CE and Symbian EPOC operating systems. Generally, these operating systems are inherently more vulnerable, because they have memory that is readable and writeable. The processors used in these devices typically have no security features, and place few constraints on the operating system. Seeing that these devices are normally synchronized to a PC allows an even greater risk of infection.

The Palm does not employ any access control to databases and records. System application databases are easily modified as regular user applications. This allows malicious code to not only modify system files, but also to destroy systems files. With a single click, one could wipe out all the applications and data on the device. (EC)

The security status of these devices is far behind that of PC's, which is not very heartwarming. With the movement to wireless connectivity, we will be seeing more of these devices connected to the internet, and more uses for these operating systems in other devices. Concept automobiles have been developed that use the Windows CE operating system to control the vehicle's functions. What do you do when a virus attacks a system while you are doing 55 mph down the highway?

Ryan McGee, product marketing manager at Sunnyvale, CA based McAfee, said he would not be surprised to see the first full-fledged virus directed towards PDAs within a year. The more advanced memory capabilities of these devices make them an immediate target, McGee noted, adding cell phones may also face a similar test in the near future. "Any time a device has the capability to access a network or another device, it is dangerous". (AV)

"The challenge was taking the existing concepts of our engine technology and fitting it inside the device so it would be fast enough and require a small amount of memory to be functional," said Carey Nachenberg, chief researcher at the Symantec Antivirus Research Center in Cupertino, Calif. (JN)

Recently a virus, (or more accurately, a trojan horse), was released for the

© SANS Institute 2000 - 2005 Author retains full rights.

Palm Pilot operating system. We will not review whether this was a legitimate mistake or a planned malicious release by the author; the damage has been done. This trojan program, named "Palm.Liberty.A", is being distributed under the name "Crack 1.1" through the IRC (Internet Relay Chat). When run, it deletes all the programs on the user's Palm device.

"It will definitely get attention," said Vincent Weafer, director of Symantec Corp.'s Anti-Virus Research Center. "I believe we've opened a Pandora's Box on some handheld devices". (AP)

A virus or trojan can be installed to a PDA device in a number of ways.

1. Downloaded from a PC during a HotSync operation. This provides the easiest means of introducing malicious code.
2. It can also be beamed from one PDA device to another via infrared during file-sharing sessions. Using IR, malicious programs could potentially speak to other infected devices, exchanging information without the owner's knowledge.
3. It is also possible for OmniSky wireless internet users to receive this trojan via email as an attachment. This is a means of introducing the virus or trojan directly into the PDA.
4. Using standard TCP/IP protocols, a PDA connected to a network can establish a connection with any other machine on the network. The malicious code can then utilize open listening ports allowing remote access.

The potential for in-the-wild viruses, trojans, and worms for PDA's is certainly possible; however, the spread of such viruses would not be nearly as fast a PC-based virus. The number of PDA users is extremely lower than the number of PC users. PDA users still download applications and data from a few sources, rather than exchanging information with other PDA users. Once PDA to PDA, or PDA networking, is commonplace we will most likely see a significant rise in the spread of viruses.

How do we prevent this from happening to us, and/or getting worse in the near future? (RH)

1. Obtain your software legitimately. Register your shareware and use only registration codes/registered versions received directly from the developer.
2. Software distribution sites generally test applications before they distribute them to the public.
3. Test applications on a Palm Emulator (POSE) before installing and

© SANS Institute 2000 - 2005 Author retains full rights.

running them on your Palm.
4. Backup your Palm before installing new applications.

The internet is a great place to download information, but we must be careful as to the source of that information. Unfamiliar web sites, email from unknown sources, and freely distributed CD programs are all places that viruses can hide. By following some simple guidelines we can help reduce the risk of infecting our equipment.

(EC) Chien, Eric. "Palm Breach." July 2000 Virus Bulletin, The Pentagon, Abington, Oxfordshire, OX14 3YP, England. http://www.symantec.com/avcenter/reference/palm.breach.pdf

(AV) Vance, Ashlee. "Palm gets first Trojan Horse." http://www.infoworld.com/articles/hn/xml/00/08/29/000829hntrojan.xml

(RH) Hopkins, Rick. "Trojans, Virii, and Rumors 101." Aug 29, 2000. http://news.pdalive.com/pdalive070720029.html

(JN) Niccolai, James. "Palm Anti-Virus Product Previewed." September 9, 2000. http://www.infoworld.com/articles/hn/xml/00/09/07/000907hnpalmvirus.xml

AP) Associated Press. "Palm Virus Unleashed." August 29, 2000. http://www.abcnews.go.com/local/wpvi/News/42107_8292000.html

Allan J. Hollowell
allan.j.hollowell@lmco.com
856 722-6950

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event