Global Information Assurance Certification Paper

The Palm OS and Malicious Code

Hugh R. Taylor

Recent announcements have brought to light the fact that devices using the Palm OS are susceptible to attacks by viruses and trojans. The first Palm Trojan, LibertyCrack (Palm.Liberty.A), has been receiving a lot of press recently. Fortunately, the Trojan does not seem to have affected many users and is not widespread. This paper will discuss the LibertyCrack Trojan and will attempt to shed some light on the significance, if any, on the information system community.

First, let's define a Trojan, the SANS GIAC LevelOne Security Essentials course, Malicious Software defines a Trojan as "[a program] with an intended action that is not documented or revealed. Typically, Trojan horses masquerade as some other harmless of trusted program."

This definition fits the LibertyCrack program. The LibertyCrack program was circulated as a free version of the Liberty 1.1 Game Boy emulator. Instead the program, when installed on a Palm OS device and run deletes all files from the device and attempts a reboot, definitely not what the user expected! Fortunately, because of the nature of the Palm OS, recovering from this attack is as simple as re-syncing the device to the desktop.

According to its creator, Aaron Ardiri, LibertyCrack was not intended to be released to the public. Ardiri was writing a new program for Palm devices and used LibertyCrack to setup a new Palm environment. Ardiri claims that one of the few people he gave the program to must have released it.

Removing LibertyCrack from a Palm device is as simple as deleting the program from the device and also deleting it from the desktop the device synchronizes with. No reports of widespread "attacks" of this Trojan have been made.

So, what is the significance of the LibertyCrack Trojan? McAfee and Symantec have updated their desktop virus scanners to look for the LibertyCrack Trojan signature and remove it from the Mac or PC before it is transferred during hotsync. Symantec has announced a virus scanner for the Palm OS and McAfee has produced a version of Guard Dog for the Palm OS.

The question remains, is there a "real" threat to the Palm OS community specifically, and the desktop/network community generally? Most security analysts view the emergence of the LibertyCrack Trojan as a milestone, now that malicious code has been written for the Palm OS, more damaging versions are sure to follow. Will this really happen? Let's examine what we know about the people who write malicious code.

Security experts agree that most writers of malicious code want some kind of recognition and to get it they attack the most popular operating systems. The popularity of the Palm OS, though not nearly as ubiquitous as the different versions of Windows, is steadily growing. As the installed base of Palm devices grows the lure of writing malicious code for the device will increase.

Malicious code is also written for effect, and for the challenge of "breaking into" the system for purposes of stealing data or using those systems to mount further attacks. The effect of deleting all the data on the Palm device is inconvenient at best, as synchronizing the Palm device with its desktop will restore practically all the data. Using Palm devices to stage attacks is highly unlikely as most are not connected to the internet on a permanent basis. As for stealing data, it would be easier to get the data from the desktop that synchronizes with the Palm device.

During my research for this paper, I came across a document titled "Is a Palm OS virus/worm possible?" by Al Leitch (no date). In the aforementioned paper, the author presents what he considers the obstacles presented by the Palm OS for viruses, worms and how they spread. The paper concentrates on the Palm Pilot and I believe some of the

"obstacles" Mr. Leitch mentions are no longer valid on the newer Palm devices. Leitch's first obstacle for viruses is the way data and binaries are stored. While he is correct in stating that most data is stored in RAM, there are now utilities and Palm devices that allow data and programs to reside in the Flash ROM or on removable storage (i.e., CompactFlash). In addition, Palm has released a program that allows users to upgrade the operating system. A virus or Trojan that exploits this capability could conceivably overwrite the OS rendering the device inoperable.

Leitch's second obstacle to viruses is the transmission of the virus. Palm Inc. provides a network synchronization that allows multiple Palm devices to be synchronized using one cradle. A program that transfers itself from an infected Palm device to the network has the opportunity to install itself onto other Palm devices. In addition, some email applications for Palm devices have the capability of automatically installing any attached prc (the file extension for Palm OS programs) files.

Leitch's first obstacle for a worm is visibility. Leitch states that any worm that hijacked the Hotsync process would be noticed in while the Palm device was synchronizing with the desktop. I feel this is not the case. My own experience is that I start the synchronizing process then go do something else. Leitch also states that all applications installed on the Palm show up in the applications list. Again, this is not always the case. The various "hacks" for the Hackmaster program are examples of "hidden" programs.

Palm, Inc. has admitted that there is little provision for security built in to the operating system, which seems to make Palm devices an attractive target for malicious code. Because of the above mentioned points and the increasing popularity of Palm devices, and as more companies deploy Palm devices that are synchronized via a network to a single server or workstation the opportunity for mass infections will increase. Thereby increasing the likelihood of an enterprising programmer attempting to gain recognition by creating malicious code to attack these devices.

How, as security managers, do we respond to this threat? First, instituting a strong policy on which Palm devices (and what software is installed on them) are allowed to synchronize to our central servers must be written. Second, virus scanning software that identifies and removes (or quarantines) malicious code for Palm devices should be installed on all desktops and servers that synchronize with Palm devices. Third, and most importantly, Palm device users must be educated on the risks associated with the Palm OS. The opportunity exists to create a strong, proactive environment for the prevention of Palm malicious code now, before we are forced into a reactive environment.

References:

Anti-Virus Center, "LibertyCrack Trojan (Palm.Liberty.A)", http://www.zdnet.com/downloads/antivirus/liberty.html, no date.

Bob Brewin, "Developer Unleashes Palm Trojan Horse Program", Computerworld p20, Vol. 34, No. 36, Sept. 4, 2000.

Alan Hoyle, "Liberty crack Trojan news mutating!", http://www.techweb.com/wire/story/TWB20000828S0025, Aug. 31, 2000.

Brian Fonseca, "Palm Trojan Horse Emerges", Infoworld p24, Vol. 22, Issue 36, Sept. 4, 2000.

Al Leitch, "Is a Palm OS virus/worm possible?", http://ppilot.homepage.com/Papers/PalmVirus.html, no date.

Robert Lemos, "Trojan Horse Kicks the Palm", ZDNet News, http://www.zdnet.com/zdnn/, Aug. 28, 2000.

Robert Lemos, "The new virus war zone: Your PDA", http://www.zdnet.com/zdnn/stories/news/, Aug. 30, 2000.

McAfee.com, "McAfee.com Protects Against First Known Trojan Targeting Wireless/PDA operating System", http://www.mcafee.com/aboutus/press_room/press_releases/pr08290001.asp, Aug. 29, 2000.

McAfee.com., "McAfee.com Announces Increased Protection for Wireless Users in Wake of Recent PDA Trojan Discovery",

http://www.mcafee.com/aboutus/press_room/press_releases/pr09050001.asp, Sept. 5, 2000.

Stephanie Miles, "Trojan horse rears its head on Palms", CNET.com, http://technews.netscape.com/news/0-1006-200-2635223.html, Aug. 28, 2000.

Carmen Nobel, "PDA Virus: More on the Way", eweek p19, Vol. 17, No. 36, Sept. 4, 2000.

Bob Sullivan, "A new era for computer viruses?", http://www.msnbc.com/news.

SANS GAIC LevelOne Course, "Malicious Software (Malware)", DC Seminar, July 2000.

Symantec Corp., "Symantec Offers Early Look at World's First AntiVirus Technology Residing Directly on the Palm OS Platform", http://www.symantec.com/press/2000/n000907.html, Sept. 7, 2000.

Robert Vamosi, "Trojan Horse Targets Palm Users", http://www.zdnet.com/zdhelp/stories/main/, Aug. 29, 2000.

Last Updated: July 28th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event