Global Information Assurance Certification Paper

Threat of the New Computer Virus – The Palm/OS Phage Virus

Susan Todd
October 15, 2000

As we begin the 21st century the significant growth rate of Wireless personal data assistant (PDAs), mobile phones, and palmtops devices are on the rise. A new frightening era of computer viruses has begun where they spread like biological viruses. Wires are no longer needed to have a problem. Wireless intruders certainly seem to have kept pace with the growth of wireless devices. Wired information-technology networks (ITNs) have been around for a hundred years; the wired Internet for about 30 years. An identical genealogy exists for the wired intruder starting with plain old telephone system (POTS) taps and leading up to whatever the exploit flavor of the nanosecond is. Wireless ITNs at "popular prices" are just arriving, but with a "vengeance." Industry projections indicate that sales of wireless devices will double this year and exceed sales of all wired ITN devices put together. Will history be repeated? This, of course, is just the very beginning. Will what happens this decade in the wireless ITN domain be a rerun of the said series of events that occurred (and continue to occur) in the wired domain? Below is an overview of some recent wireless ITN exploits.

Starting with eavesdropping on analog cordless and cellular phones (and baby-room monitors) using inexpensive scanners, wireless intruders now appear poised to deliver a quantum jump in the growth of exploitation technologies. Wireless IT security folks are playing catch up (or have yet to wake up). The challenge is warning consumers that handheld wireless electronic devices may face some of the same virus threats that have plagued personal computers in recent years. The big picture is a world of hostile code with attacks increasing day by day. The first documented Palm Pilot virus, was the "Liberty Crack" but it wasn't the first malicious code targeting handheld devices. Mobile Phones, which are used more globally than PDAs, are also at risk. There has been several virus programs targeting the EPOC operating system designed for mobile ROM-based computing devices that is used in the palm-like devices and cell phones in Europe. A Norwegian company found that sending certain text messages would cause the Nokia Mobile phones to freeze up. The only way to start up the phone again is by taking the batteries out of the handset and connects it again. Virus attacks will be more prone to handheld devices than mobile phones because of their connection to PCs. They can be linked to the Internet and by infrared ports beam information between the devices. This threat was reinforced when the first real virus hit, infecting a hand-held organizer called "Phage." This is not a common virus and was reported in the form of a tiny file that rummages through the Palm Pilot. "It's the first real virus for any palm pilot ever, meaning that it actually is a virus with the capability to spread further," quoted by Mikko Hermanni Hypponen, the manager of anti-virus research at Finland-based F-Secure Corporation. Hypponen said, "Viruses such as Phage are often disguised as computer games or pornographic images on Internet newsgroups and chatrooms."

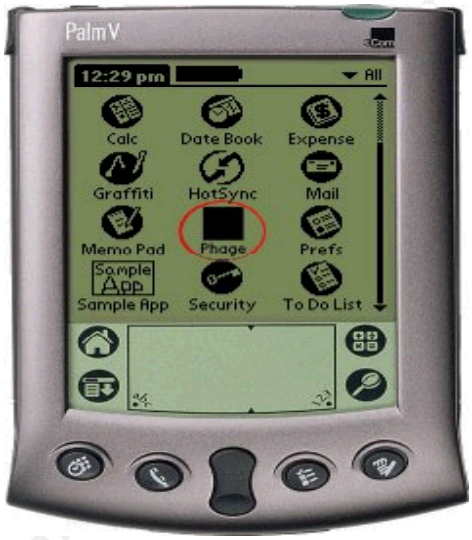
Let's define the word "computer virus." It is a program code that self-replicates and attaches itself into other programs and hides itself in the host programs. A virus is not an independent program and only infects programs already in existence by inserting new code. The virus' primary function is to reproduce. It may also have a secondary function such as destroying data. When the target program is executed, the virus infects another program. Characteristics of a virus include replication, requires a host program as a carrier, activated by external action, and replication limited to (virtual) system. A computer virus is the most prominent of the malicious

agents and is very destructive and might destroy or compromise data.

Description:

Palm Pilots are handheld computing devices that fit into the palm of your hand and provide desktop functions without the magnitude of a laptop. The device connects to your computer that allows information to be transferred from your computer to your Palm Pilot. It also allows for other programs to be downloaded from the Internet and placed on the Palm. PalmOS/Phage works by overwriting the beginning of Palm executables. The host files are destroyed in the process and would infect any Program files or Palm OS Runnable Code (PRC) files that is transferred to the Palm. The virus keeps spreading to other Palm programs until they are all infected and destroyed.

The screen picture below is the Palm infected with the Phage virus.



This virus does nothing else than replicate itself. It contains following texts:

FindVictim
PhageMain

If you are infected most applications in your Palm Pilot do not work. First, your screen goes blank for a second then the program exits and the virus locates and infects all other programs in the system. Phage infects and destroys all application files in the device but does not harm database files. These data files include address book, phone numbers, and calendar entries are by default backed up.

he following graphic shows a blank screen after your Palm pilot has been infected.

In order for a virus to spread from one machine to another executables have to be exchanged. Here are a few ways the ideal virus can spread.

(1) Beam – which allows a Palm Pilot to send information via infrared or a docking station.
(2) Internet – the application is downloaded from the Internet.
(3) PC – the application is hotsynced to the Pilot. Network synchronization that allows multiple Palm devices to be synchronized.

An application that is transferred from an infected Palm device to the network has the opportunity to embed in other Palm devices.

Obstacles:

(1) Palm Pilots store all their data and binaries in Random Access Memory (RAM). There are utilities and Palm devices that allow data and applications to be stored in the Flash Read Only Memory (ROM) or on removable storage. If the batteries go bad then you will lose all your contents in RAM. You must replace those batteries no later than one minute. This is why it is crucial to backup your data to your PC.

(2) Palm OS has a security feature that enables a user to set password protection on various applications. The Palm device allows a user to connect a machine on the network through the HotSync process. This process involves the device to send the encoded password to the HotSync Manager or the HotSync Network Server on the network. The purpose is to verify password protection is still enabled when applications are being accessed from the network. The encoded password block is stored in the 'Unsaved Preferences' database on the Palm device. This is also configurable and allows users to set passwords. The security issues are weak encryption scheme and it is possible to decrypt the password block into the actual ASCII format with the use of an exploit tool.

(3) The virus might be incompatible with future palm upgrades.

What is the biggest threat of Palm OS/Phage?

The biggest threat at this time is the lack of security. All PDAs are insecure and their processors do not support security features. This will become more of a problem as PDAs become more and more connected and the risk of infecting your Palm and compromising data is very high. This makes it a prime target for malicious code. The wireless connection is creating unknown and uncontrolled backdoors into the network. As the new PDA technology increases so is the threat. The ease-of-use over security has the potential for viruses to damage hundreds of systems before detection.

I believe that people are really underestimating the new computer virus "Phage." Although, the threat is low the potential damages are severe and can spread very quickly in a network or computing system. Viral attacks can leave very little traces and require minimal expertise to implement. People should evaluate their vulnerability for this new threat and take action. Phage is very similar virus to "Love Bug" that spreads through email, sending a copy to itself and to anyone in a user's address book shutting down email systems. It has been demonstrated that a virus has the potential to spread through any general-purpose system that allows sharing. Palm Inc's handhelds are the most widely sold PDA and as more and more devices are connected, there will be an extreme amount of possibilities for spreading the virus. These devices are generally unprotected because few people are using security and antiviral software. If the Palm Pilot has lax security, the virus could spread and may even shut down the entire network until the virus is removed. The possibilities are endless and are unclear just how much damage virus writers might be able to do.

What can we do as to remove and prevent the virus?

There are no patches or fixes yet established for this type of virus. The only way to restore your palm pilot capabilities is by deleting all applications or restoring the programs from a backup, .prc files from application packages, or to download and re-install all applications. You need to locate all infected Palm applications, delete them, reinstall, or restore from backups.

First, To protect yourself from the virus, "Phage" users should run anti-virus software. Responding anti-virus vendors were F-Secure which uses a Palm program available designed to help victims of the "Phage" virus by locating and deleting all files. McAfee AVERT anti-virus software program will check for updated information on new viruses and download cures to protect customers or e-businesses from attacks. Also, Enable the Turn off and Lock Device features or implement a third party encryption application. Integrity and security must be maintained in a system in order to prevent virus attacks.

As we begin the 21st century and beyond, a good well-written policy is a must. It should clearly define protection requirements, threats, roles, and responsibilities. It should address issues like how long protection software is kept current and used? What software will be installed on Palm devices? Multi-layer security is needed for handling a number of different security levels. Safeguards including backups are crucial in order to recover from virus attacks. Anti-virus software should prevent, detect, and eradicate viruses and must be used on all Palm devices. This includes desktops, servers, which are used to sync Palms. Mandatory access controls should be enforced to determine who can access what information on your system. People need to be trained and educated in the skills needed to operate Palm devices securely. Palm Pilots should

have a built-in security where you can't overwrite the data and updates can be done using an algorithm or encryption method. We cannot stop all viruses from happening but we can protect ourselves by putting measures in place to help lower the risks.

References:

1. Hoffman, Lance J. "Rogue Programs: Viruses, Worms and Trojan Horses." 1990.

2. Leitch, AL, "Is a Palm OS virus/worm possible?", http://pp.pilot.homepage.com/Papers/PalmVirus.html.

3. Sullivan, Bob, "A new era for computer viruses", http://www.msnbc.com/news August 30, 2000.

4. Bendern, Paul de, "Messages reportedly can Freeze Nokia Phones", http://dailynews.yahoo.com/h/m/200000830/tc/nokia_virus, August 30, 2000.

5. Berndern, Paul de, "Palm, Other Hand-Held Devices to Face Virus Threats", http://dailynews.yahoo.com/h/nm/20000831/tc/handhelds_virus_dc_2.html, August 31, 2000.

6. Hopper, D. Ian, "Experts warn of Palm Pilot virus", http://cnews.tribune.com.html.

7. SANS GAIC Level One Course, "Malicious Software (Malware)", Virginia Seminar, September 2000.

8. Lemos, Robert, "Trojan Horse Kicks the Palm", MSNBC News, http://www.msnbc.com/news/452708.as.

9. Symantec Corp., "Symantec Antivirus for Palm OS Beta Version Now Available", http://www.sarc.com/avcenter/palmsscanner.html.

10. McAfee Avert., "PalmOS/Phage First Wireless to Infect Palm Applications", http://www.nai.com/asp_set/about_pres…e.asp?PR=/PressMedia/09212000.asp&Sel_833

11. F-Secure Corp., "Global Palm Information Center", http://www.datafellows.com/palm

12. Sorid, Daniel,"First Palm Virus Spread, Killing Programs", http://dailynews.yahoo.com/h/mm/20000923/tc/palm_virus/dc_3.html, September 24, 2000.

13. Krause, Micki and Harold F. Tipton, "Information Security Management", 1999.

14. Alexander, Michael, "The Underground Guide to Computer Security", 1996.

Last Updated: July 28th, 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
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
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
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 Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
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