ELEC 377 – Operating Systems

Week 11 – Class 3

Last Class

- Security

◊ Passwords and Program Threats

Today

- Security

  ◊ Sony Rootkit and Copy Protection

  - try and relate to the concepts we have covered during the course.

What is a Root Kit?

- Root Kit is software to hide the evidence of system modification
- Originally used by intruders in Unix systems to hide changes to systems
  - ◊ add a back door process such as a chat daemon or ftp server running on non-standard port
  - ◊ changes to ps, netstat, w, passwd and other system commands to hide the back door
- Now applies to any operating system
  - ◊ Changes are now usually made to kernel and system libraries rather than to system commands
    - – Although some combine both system libraries and system commands

What is a Root Kit?

- Not the initial vulnerability
  - ◊ initial vulnerability is used to gain access, root kit is used to maintain access to compromised system
  - ◊ Sometimes the intruder patched vulnerability to keep ‘exclusive’ access to the system
  - ◊ root kit may attempt to maintain ownership of the system
    - - one part of root kit notices when another part has been removed and reinstalls that component
- Often used by viruses and worms to disguise activities.
  - ◊ Thus rootkit detection is a concern for Security Vendors.

Root Kit Research

- Commercial and Personal Systems
  - ◊ when you get malware, you want to remove it
  - ◊ limit its damage
- Sensitive Systems.
  - ◊ You don’t want to eradicate the malware
  - ◊ You need to observe it
    - -- who is it reporting to?
    - -- what kind of information is it interested in
    - -- limit access to sensitive information
  - ◊ Problem: it is checking to see if anyone is watching
    - -- may self destruct/or may attempt to destroy system.
    - -- may change its behaviour.

Root Kit Research

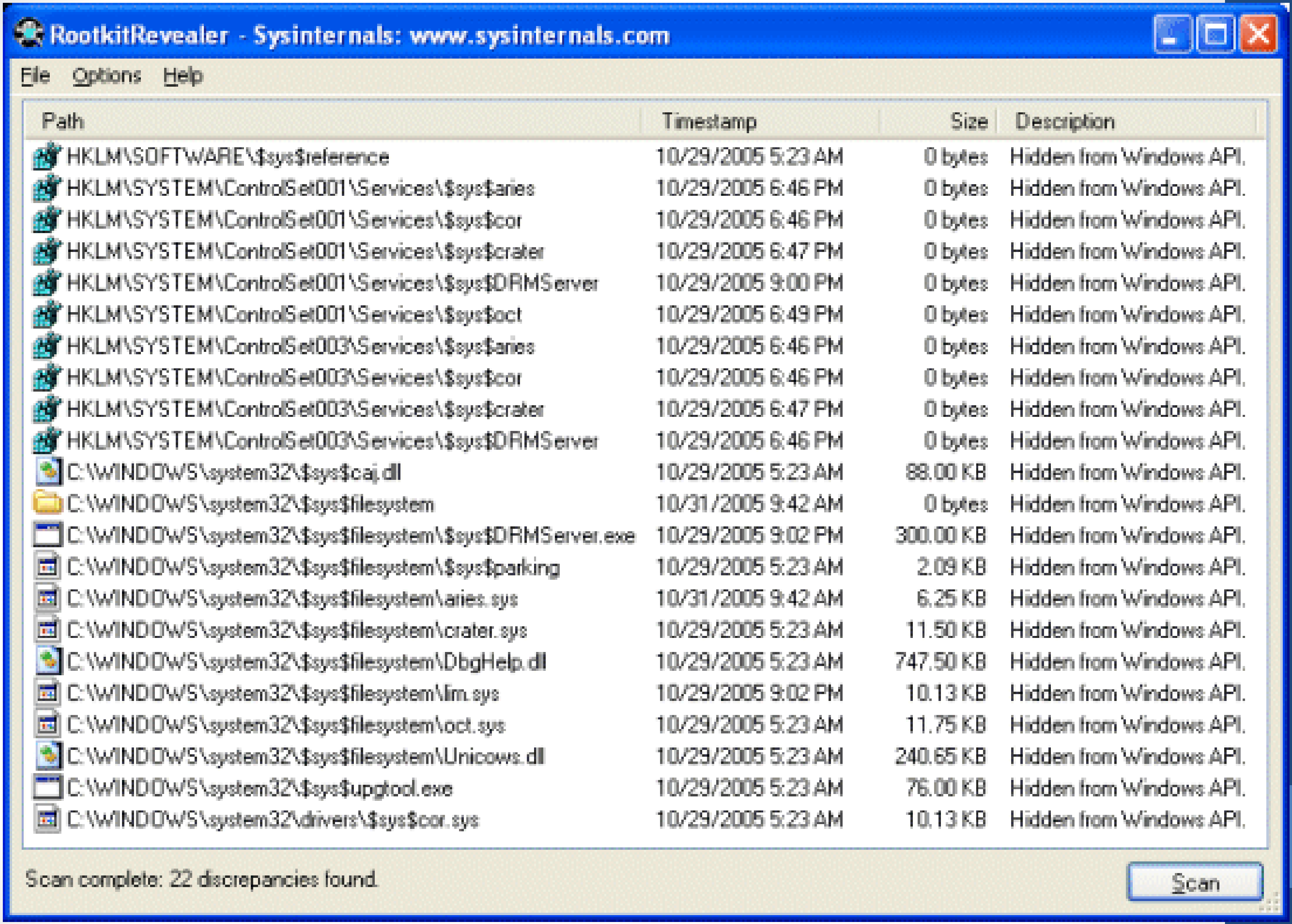
- Kernel Level Asynchronous Procedure Calls(APC)
  - ◊ register a call back routine for a process inside the kernel
  - ◊ call back executes with knowledge of the processes virtual memory tables, and other process info
  - ◊ Our anti-malware executes entirely as APC callbacks.
  - ◊ copy to different memory location
  - ◊ register callbacks on different threads
  - ◊ Can inject into malware's thread and look at malware in malware's context
  - ◊ jump onto thread to exfiltrate information

Sensitive Systems

- Counter-Intelligence Operations
  - ◊ after detecting malware, you provide a simulated environment (including new operator)
  - ◊ replace systems it has access to, with fake systems with fake information
- Observe the malware
  - ◊ CASCON paper
  - ◊ Use root kit techniques to hide the anti malware software from the malware
  - ◊ Installed at time OS is installed -- we are in first!!

Initial Detection of Sony Rootkit

- Mark Russinovich testing Rootkit detection tool
  ◊ RootkitRevealer - utility by Sysinternals LLC
  ◊ discovers rootkit on his own system



Path	Timestamp	Size	Description
HKLM\SOFTWARE\$sys$reference	10/29/2005 5:23 AM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\$sys$aries	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\$sys$cor	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\$sys$crater	10/29/2005 6:47 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\$sys$DRMServer	10/29/2005 9:00 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\$sys$oct	10/29/2005 6:49 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\$sys$aries	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\$sys$cor	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\$sys$crater	10/29/2005 6:47 PM	0 bytes	Hidden from Windows API.
HKLM\SYSTEM\ControlSet003\Services\$sys$DRMServer	10/29/2005 6:46 PM	0 bytes	Hidden from Windows API.
C:\WINDOWS\system32\$sys$caj.dll	10/29/2005 5:23 AM	88.00 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem	10/31/2005 9:42 AM	0 bytes	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\$sys$DRMServer.exe	10/29/2005 9:02 PM	300.00 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\$sys$parking	10/29/2005 5:23 AM	2.09 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\aries.sys	10/31/2005 9:42 AM	6.25 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\crater.sys	10/29/2005 5:23 AM	11.50 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\DbgHelp.dll	10/29/2005 5:23 AM	747.50 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\lim.sys	10/29/2005 9:02 PM	10.13 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\oct.sys	10/29/2005 5:23 AM	11.75 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$filesystem\Unicows.dll	10/29/2005 5:23 AM	240.65 KB	Hidden from Windows API.
C:\WINDOWS\system32\$sys$upgtool.exe	10/29/2005 5:23 AM	76.00 KB	Hidden from Windows API.
C:\WINDOWS\system32\drivers\$sys$cor.sys	10/29/2005 5:23 AM	10.13 KB	Hidden from Windows API.

Scan complete: 22 discrepancies found.

Tracking down the source

- Mr. Russinovich uses other tools to look for the processes and auto startup information and discovers nothing
- Uses *LiveKd** on his running kernel to look at the system service table (Window’s system call table)

  ◊ looks for entries that point outside of the windows kernel main body

  - entries inside main kernel are original entries
  - entries outside of the kernel are third party drivers
  - not all will be for the rootkit (third party graphics drivers for example)

  ◊ discovers several entries that have been modified

* liveKd - utility available from Sysinternals LLC.

Tracking down the source

- Disassembles one of the functions
  - ◊ part of Aries.sys driver.
  - ◊ one of the entries cloaked in the $sys$filesystem

Tracking down the source

- Other entries of $sys$filesystem: Unicows.dll, crater.sys, lim.sys, oct.sys , DbgHelp.sys
- Uses IDAPro to look at disassembly of Aries.sys

IDAPro product of DataRescue™

Tracking down the source

- Aries.sys patches the table
  - ◊ CreateFile, QueryDirectoryFile, QuerySystemInformation …
  - ◊ replaced functions cloak all entries starting with $sys$
- renames notepad.exe, $sys$notepad.exe
  => disappears!!
- Not safe to unload driver that patches the table
  - race condition
  - but aries.sys supports unloading????
- Also system call hooks this way do not work with AMD64

Tracking down the source

- Dbghelp.dll and Unicows.dll are MS libraries
- Who owns Aries.sys and others?
  - ◊ most root kits do not include author information this one does!!
  - ◊ owned by First4Internet
- Visits internet site, notices press release of contract with Sony/BMG, XCP product
- Looks at recent purchase of music, finds *Get Right with the Man* by the Van Zant brothers
  - – no CD trademark logo
  - – contains references to XCP on label

Investigating the Music

- Running the player on the CD causes an increase in CPU usage by $sys$DRMServer
  - ◊ claims to be part of Plug and Play Device Manager
    - - deception, not part of Windows.
- Closing player does not reduce usage of the DRM Server??
  - ◊ scans process list every two seconds
  - ◊ scans executables for each process *8* times each scan
  - --- looking for cd ripping programs
- Communicates with the player through named pipes.

Removing the Software

- No uninstall utility on the CD, no uninstall entry in the Remove Programs Control panel
  - ◊ Minimal reference to software on EULA, no description or notice that it could not be removed
- Deleted drivers and registry keys, and reboot
  - ◊ Reg keys are not only in normal registries, but also in safe boot registries so booting into safe mode includes the DRM server
  - ◊ CD drive is gone!!
- Windows low level interface
  - ◊ Allows drivers to add low level interface
  - ◊ If a driver is registered but not there, windows does not show the device.

Removing the Software

- Sony makes an uninstaller available.
  - ◊ On web site
  - ◊ Difficult to find (not reachable from home page)
- Uninstaller was an ordeal
  - ◊ find web page
  - ◊ must give country, artist name name, email address, CD title and name of store where the CD was purchased

    - privacy policy attached to page gives Sony permission to use for direct marketing.

    - Sony later claims publicly will not use email

Removing the Software

- Uninstaller was an ordeal (cont'd)
  - ◊ get email with case ID and link to another page
  - ◊ 3.5 MB patch that decloaks software
    - – race condition
    - – patch contains updated drivers
  - ◊ also another form if you really want to uninstall the software (default to only decloak)
  - ◊ directs to a page which requires downloading an ActiveX controller CodeSupport.ocx, signed by First 4 Internet
    - - enter case id and reason for request!!
    - - must be done on machine with software
    - - sends system information back to Sony

Removing the Software

- Uninstaller was an ordeal (cont'd)
  - ◊ get another email with case ID and link to a personalized uninstall page, link expires in one week
  - ◊ can only be used on computer with software, not on any other computer. Cannot use the same link to uninstall software from more than one computer.

More Security Implications

- Sony player calls home each time you play the CD
  - ◊ player is checking for updated art/lyrics
  - ◊ web site logs??
- Aries.sys does not check parameters
  - ◊ bad data in parameters crashes system
  - ◊ can be exploited by malicious code

- End of Mark Russinovich’s Story

More Security Implications

- Sony Uninstaller
  ◊ ActiveX component
  ◊ Must be installed with system admin privileges
  ◊ is scriptable and does not check that it is invoked from the Sony Page (*any* web page can script)

GenerateRequestPacket
Uninstall
GetProgress
InitializeDiscScan
IsDRMServerValid
GetAlbumName
GetCurrentBurnCount
IsContentOwnerValid
GetInstalledSoftwareVersion
InstallUpdate
GetCompletionStatus
IsAdministrator

ExecuteCode
RebootMachine
OnLoaded
GetNumberOfDiscs
GetAlbumArtist
GetMaxBurnCount
GenerateIncrementPacket
DoIncrement
IsXCPDiscPresent
GetInstallProgress
IsXCPDiscPresentAsLong

Sony Information

- Claims:
  - ◊ can only be played with their player
  - ◊ of played with any other player, sound will be ‘distorted’
  - ◊ copy using the sony player generates a secure WMA file
  - ◊ can only make a limited number of copies
  - ◊ cannot generate generic MP3’s and Sony does not have a license for Fairplay, will not work on iPod
  - ◊ works normally on CD players and Macintosh
  - ◊ NPR interview Nov 4, “Most people, I think, do not even know what a Rootkit is, so why should they care about it?”

Fallout

- Stewart Baker, Department of Homeland Security's Assistant Secretary for Policy
  - ◊ “It's very important to remember that it's your intellectual property -- it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days”

Fallout

- EFF Lawsuit in California (www.eff.org)
  - ◊ both XCP and Suncomm MediaMax software
  - ◊ anti-spyware laws
  - ◊ Computer Legal Remedies Act
  - ◊ warranty of merchantability
  - ◊ The CDs also condition use of the music on unconscionable licensing terms.
  - ◊ end up with settlement, covenant, coupons
- Texas AG Lawsuit - anti-spyware laws
- Canadian settlement, no covenant, coupons
- Product Recall (Nov 15, 2005), Made regular Audio CDs available for trade
- New York- $7.50 + new copy/3 other albums

Legal Implications

- DMCA - circumvention of copy protection

◊ Sony claims that it will not prosecute any "legitimate security researchers".

- ◊ did Mr. Russinovich's research violate DMCA?
- ◊ who is legitimate security researcher
- ◊ professor at university
- ◊ security group at consulting/auditing firm (Deloitte)
- ◊ security software company (Symatec, F-Secure)
- ◊ undergraduate student?
- ◊ computer professional, with an interest?

Legal Implications

- Every 3 years, the librarian of congress can authorize circumventions to the DMCA act.
  - ◊ In 2006, 6 new exceptions were added
  - ◊ Announced yesterday, go into effect Nov 27th.
  - ◊ 5 = Unlocking Cell Phones
  - ◊ 6 = Sound Recordings ... protected by technological protection measures that .... explote security flaws or vulnerabilities that compromise the security of personal computers... purpose of good faith testing, investigating or correcting of such security flaws or vulnerabilities

Legal Implications

- Sony rootkit was used to defeat Wow Warden protection
  - ◊ did Sony violate DMCA?
    - - rename ripper using $sys$ and player can’t see it!!
  - ◊ did users violate DMCA?
- At least one worm has been discovered using Sony rootkit to mask activities
  - ◊ is Sony liable?
- What is appropriate balance between copyright owners and consumers???

Legal Implications C-32

- Outlaws circumvention of TPM or distribution of circumvention techniques (similar to DMCA)
  - ◊ Some exceptions :
- Other issues with legislation
  - ◊ no fair-dealing rights for anything protected by TPM

Rootkits in Linux

- How would one accomplish this in Linux?
- system calls use int 0x80
  - ◊ system call number in eax
  - ◊ sys_call_table points to system call handler
  - ◊ modules can modify sys_call_table entries to point to them
- create new read directory, open file routines
- lsmod uses /dev/kmem to scan a list
  – remove module from list
- Modify /proc drivers not to show the processes belonging to the back door the root kit is hiding
- put processes in /etc/rc/init.d to ensure they start up each time - (ls hides the files...)

References

- Mark Russinovich’s Blog

http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

◊ Images from the blog are Copyright Sysinternals LLC. The web site contains the following licence: (http://www.sysinternals.com/Licensing.html) Permission for editorial use and in publications distributed without cost in ordinary course of business

- Other Info

http://www.boingboing.net/2005/11/14/sony_anticustomer_te.html

http://en.wikipedia.org/wiki/2005_Sony_CD_copy_protection_controversy

http://cp.sonybmg.com/xcp/english/faq.html

http://www.security.ithub.com/article/Sonys+Uninstaller+Is+Worse+than+Its+DRM/165408_1.aspx

http://www.freedom-to-tinker.com/

- Root Kits

http://en.wikipedia.org/wiki/Root_kit

http://www.infosecwriters.com/hhworld/hh9/lvtes.txt