CEIC® 2014

Why is removing malware so difficult?

A look at malware persistence—registry, service, DLL hijacking and bootkit

www.encase.com/ceic

Why is removing malware so difficult? CEIC 2014

KEYW
Keywcorp.com

Hexis CYBER SOLUTIONS a KEYW company
Hexiscyber.com

Parrot Labs™
KEYW Corporation
Training.keywcorp.com

Why is removing malware so difficult? CEIC 2014

Purpose

This presentation seeks to:

- Discuss the concepts of malware persistence
- Put them into practice
- Educate beginner to intermediate network defense practitioners

Assumptions

- All necessary privileges are gained
- Stealth is not in play

Page 3

Why is removing malware so difficult? CEIC 2014

Lab environment

Virtual Machine

- Win 7 SP 1 32bit
- Code for running the techniques
- Tools
  - Sysinternals
  - Depends
  - Autopsy
  - Windows CLI foo

Page 4

Why is removing malware so difficult?

CEIC 2014

Presentation does not contain original research

Page 5

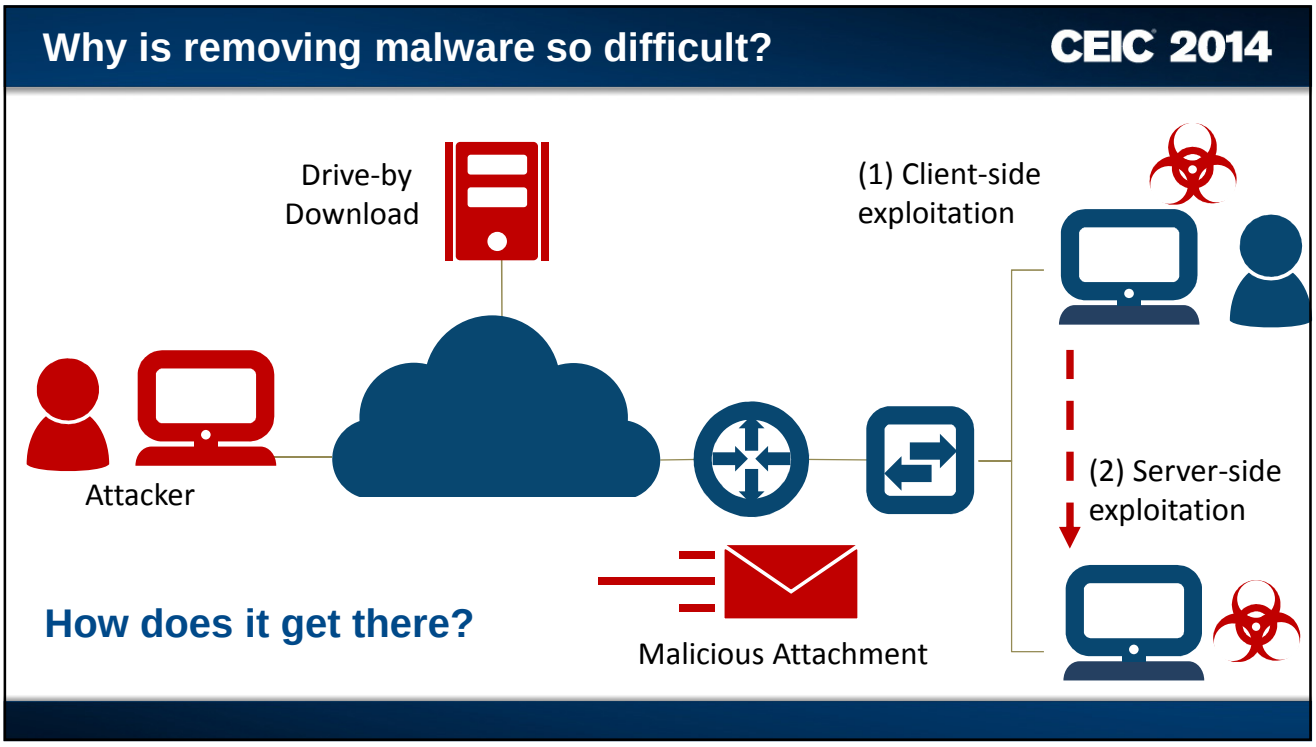
Why is removing malware so difficult?

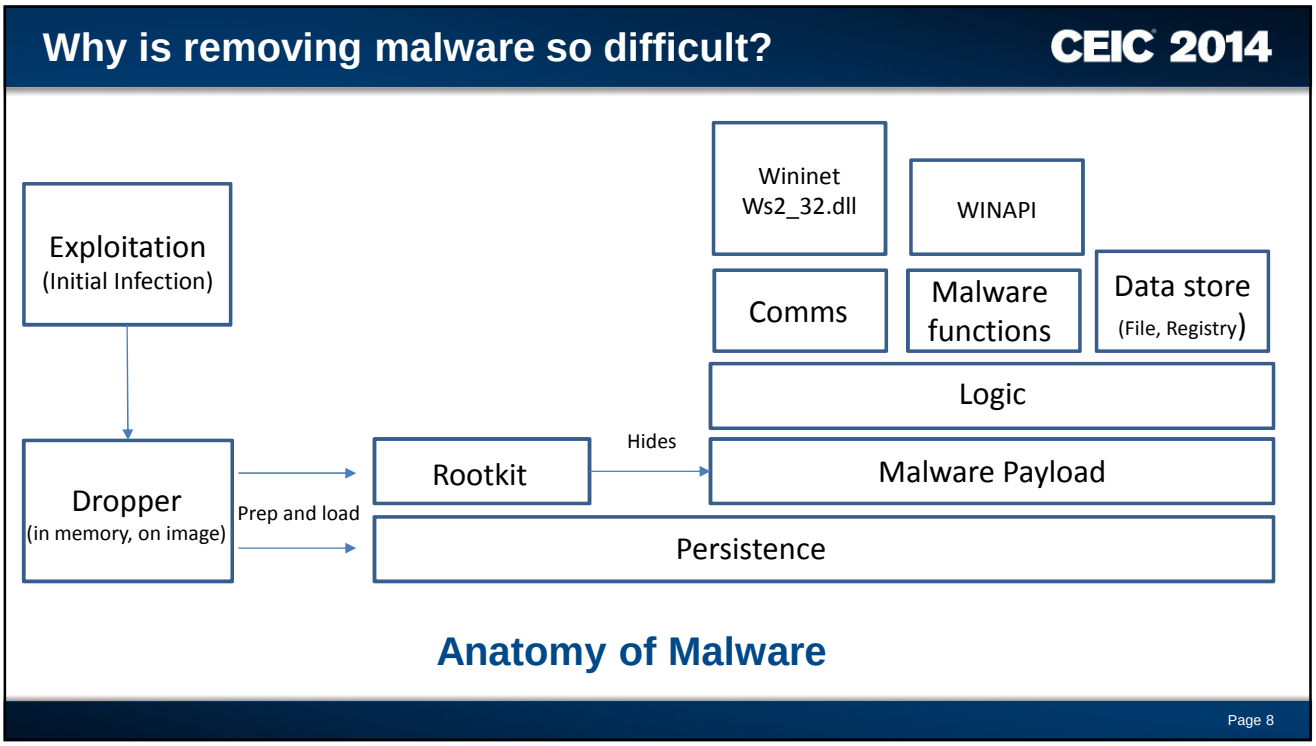
CEIC 2014

What is persistence

- Provides malware the ability to run after reboot
- Provide resiliency, i.e. re-write (download) malware to image after partial removal
- Designed to maintain a foothold on hosts of importance

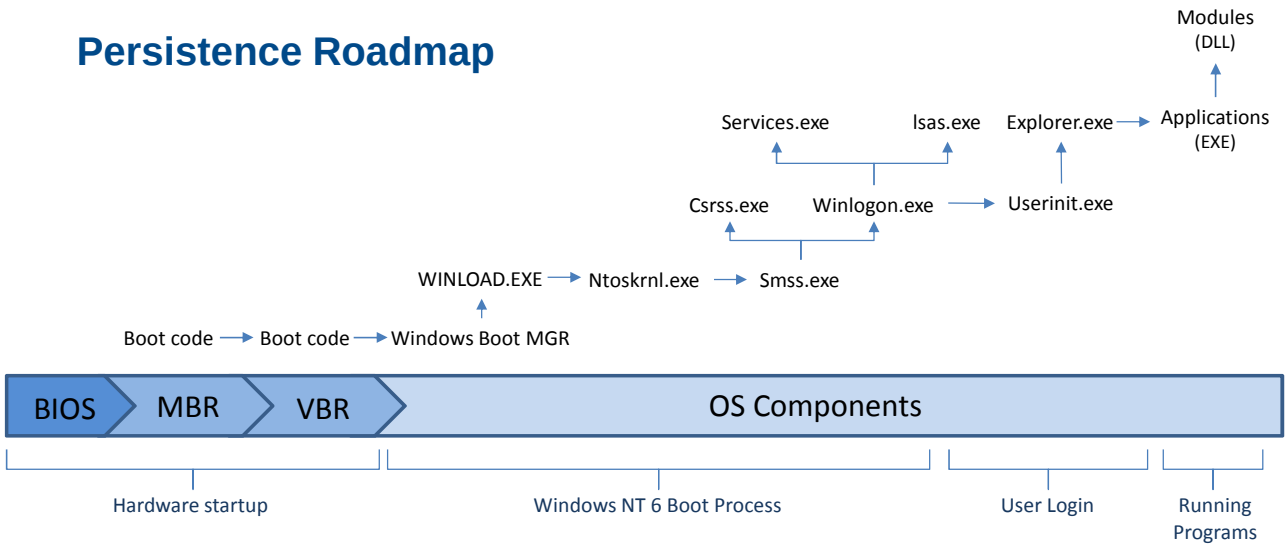
Page 6


Why is removing malware so difficult?
CEIC 2014
Drive-by Download
(1) Client-side exploitation
Attacker
(2) Server-side exploitation
How does it get there?
Malicious Attachment


Why is removing malware so difficult?
CEIC 2014
Exploitation (Initial Infection)
Dropper (in memory, on image)
Prep and load
Rootkit
Hides
Wininet Ws2_32.dll
WINAPI
Comms
Malware functions
Data store (File, Registry)
Logic
Malware Payload
Persistence
Anatomy of Malware
Page 8

Why is removing malware so difficult? CEIC 2014

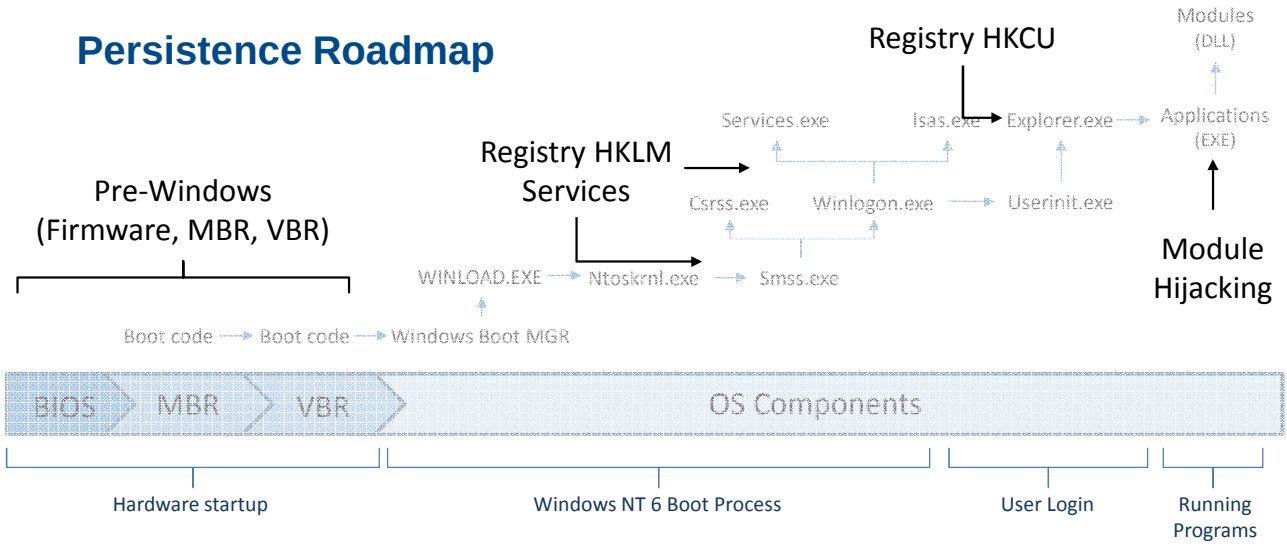
Persistence Roadmap



Page 9

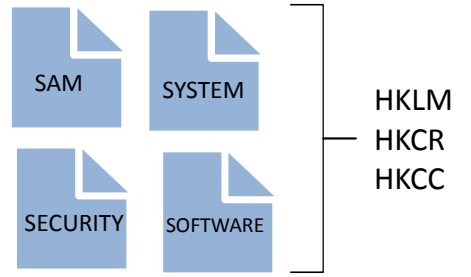
Why is removing malware so difficult? CEIC 2014

Persistence Roadmap



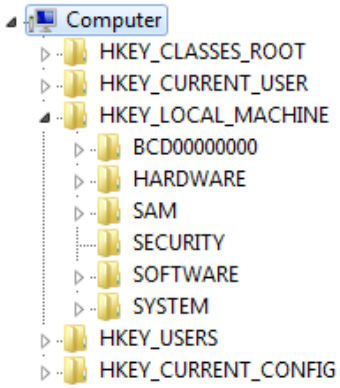
Page 10

Why is removing malware so difficult? CEIC 2014



<SYSTEM_ROOT>\System32\config

C:\Users\<user_name>



- Autorun keys
- Easy to hide data (most users have no idea!)
- Gain execution on system start or user login
- Fairly standard but effective!

Page 11

Why is removing malware so difficult? CEIC 2014

Persistence with the Registry

- Load malware on Startup
  - HKLM (services)
- Load malware on User login
  - HKLM
  - HKCU

Page 12

Why is removing malware so difficult? CEIC 2014

On start up (Services)

Can be accomplished via Service Control Manager

HKLM\SYSTEM\CurrentControlset\services\<service_name>

HKLM\SYSTEM\CurrentControlset\services\<service_name>\Parameters\ServiceDll

Start and Type DWORD values matter

http://support.microsoft.com/kb/103000

Page 13

Why is removing malware so difficult? CEIC 2014

On user login

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
- HKCU\software\Microsoft\windows NT\CurrentVersion\winlogon\Shell
- HKCU\software\Microsoft\windows NT\CurrentVersion\winlogon\Userinit

Page 14

Why is removing malware so difficult?

CEIC 2014

Persistence with the Registry in action

Why is removing malware so difficult?

CEIC 2014

DLL Search Order Hijacking

- DLL (dynamic-link library)
- DLL = shared object which contains resources
  - (code, data, etc.)
- Programs (.exe) use DLLs for modularity
- DLL's are loaded into memory space and functions are imported (import table)
- DLL's export functions (export table)

Why is removing malware so difficult? CEIC 2014

DLL Search Order

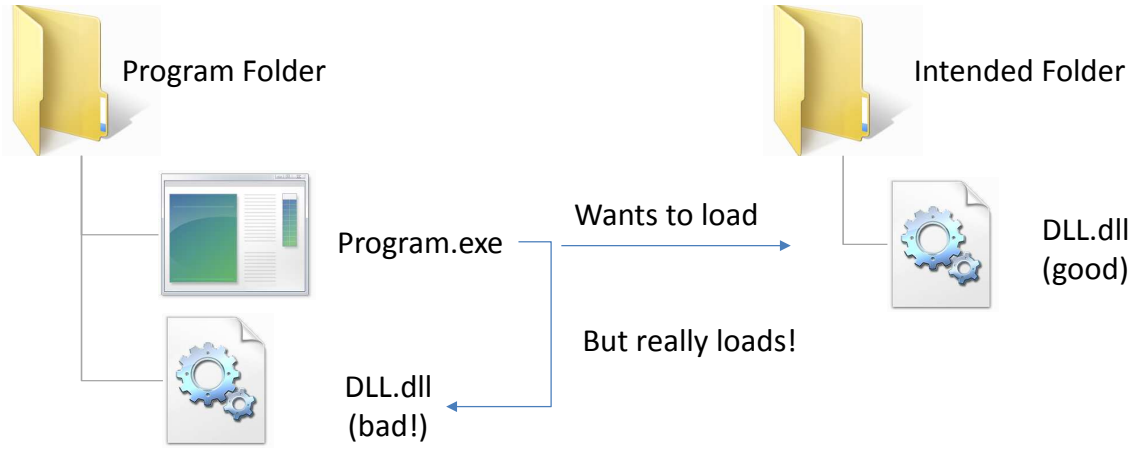
1. Directory from which the application is loaded
2. The system directory (C:\Windows\system32)
3. The 16-bit system directory (C:\Windows\system)
4. The Windows directory (C:\Windows)
5. The current directory (User context)
6. Directories that are listed in the PATH environment variable

http://msdn.microsoft.com/en-us/library/windows/desktop/ms682586(v=vs.85).aspx

Page 17

Why is removing malware so difficult? CEIC 2014

The Hijack



Page 18

Why is removing malware so difficult? CEIC 2014

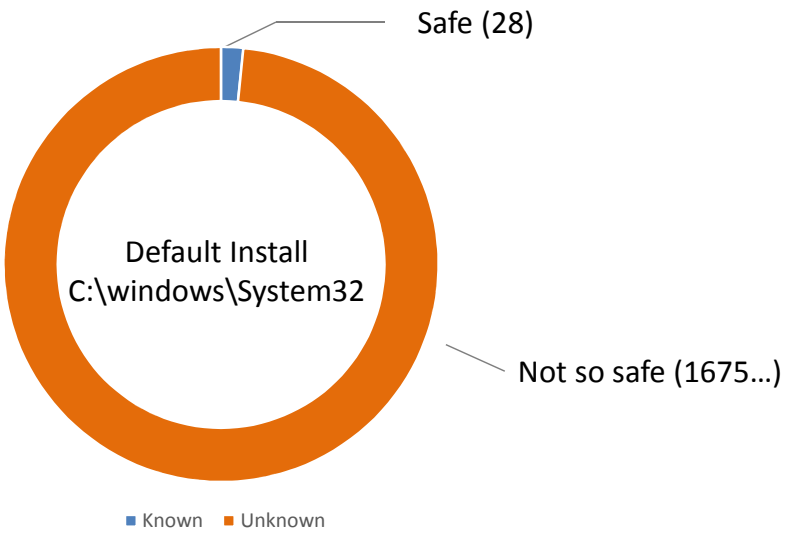
Are all DLLs hijackable?

- The system has certain DLLs cached
- HKLM\system\currentcontrolset\control\session manager\knowndlls

Clbcatq.dll	LPK.dll	Setupapi.dll	Difxapi.dll
Ole32.dll	MSCTF.dll	SHELL32.dll	
Advapi32.dll	MSVCRT.dll	SHLWAPI.dll	
COMDLG32.dll	NORMALIZ.dll	URLMON.dll	
Gdi32.dll	NSI.dll	User32.dll	
IERTUTIL.dll	OLEAUT32.dll	USP10.dll	
IMAGEHLP.dll	PSAPI.DLL	WININET.dll	
IMM32.dll	Rpcrt4.dll	WLDAP32.dll	
Kernel32.dll	Sechost.dll	WS2_32.dll	

Page 19

Why is removing malware so difficult? CEIC 2014



Page 20

Why is removing malware so difficult? CEIC 2014

Going Deeper

- Look for programs that load DLL's and import their functions
- Try to find a common DLL that any system has (max target space)
  - Typically part of the 1675 in system32
- Make sure the DLL is not protected
- Can't overwrite WFP DLLs (so location matters!)

Page 21

Why is removing malware so difficult? CEIC 2014

Finding Hijack-able DLLs

- Identifying DLL dependencies, depends.exe
  - http://www.dependencywalker.com/
- Automated identification, finddllhijack.exe
  - http://blog.mandiant.com/wp-content/ammo/finddllhijack1.zip
- Our role your own with Python pefile module
  - https://code.google.com/p/pefile/

Page 22

Why is removing malware so difficult? CEIC 2014

The Tables

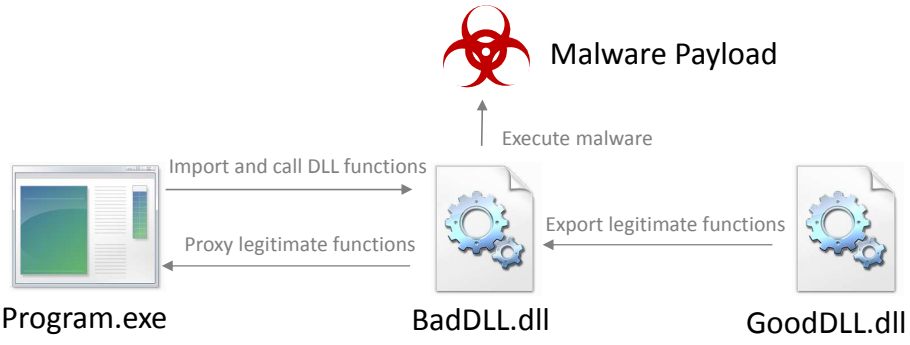
- Export Address Table
  - Functions the DLL will export
  - Method is referenced by ordinal or ASCII name (usually method name)
- Import Address Table
  - The functions that the process imports from a given DLL

	PI	Ordinal ^	Hint	Function	Entry Point
SOLITAIRE.EXE					
KERNEL32.DLL		N/A	82 (0x0052)	CloseHandle	0x77E305B7
USER32.DLL		N/A	129 (0x0081)	CreateDirectoryW	0x77E2EC9A

Why is removing malware so difficult? CEIC 2014

DLL Proxy

- To take advantage of Window's behavior, we need a DLL proxy (the persistence vector)
- Purpose is to gain execution while still exporting legitimate functions for the parent program



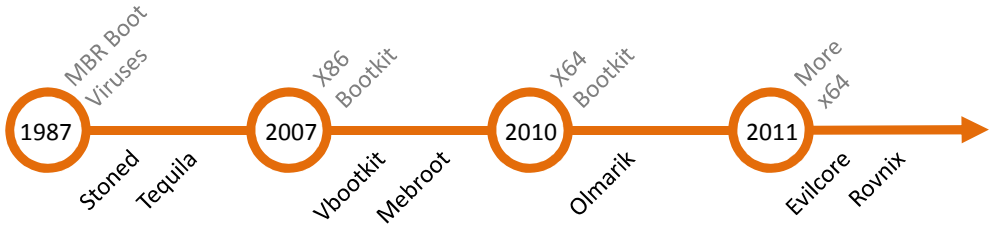
Why is removing malware so difficult? CEIC 2014

DLL Hijacking in Action

Why is removing malware so difficult? CEIC 2014

Bootkit

- Malware hooks prior to the OS loading
- Enables malware to load in a privilege mode upon reboot
- Concept of Bootkits have been around for a while (technique has changed)

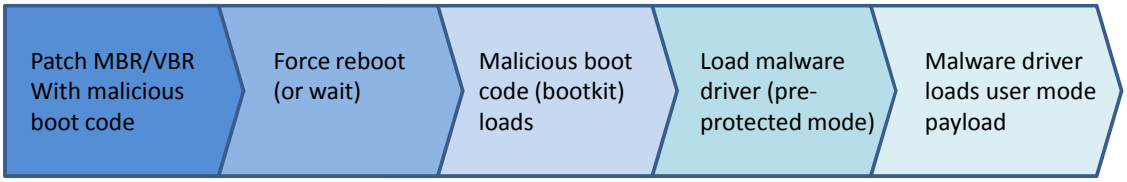


http://go.eset.com/us/resources/white-papers/Rodionov-Matrosov.pdf

Why is removing malware so difficult?

CEIC 2014

How it works



Page 27

Why is removing malware so difficult?

CEIC 2014

Bootkit in Action

Page 28

Why is removing malware so difficult? CEIC 2014

Other Persistence Mechanisms of Interest

- Firmware
  - Write into the Firmware from the OS
- Browser Helper Objects
  - Browser loads DLL to provide pluggable functionality
  - Can be used to execute malware payload

Page 29

Why is removing malware so difficult? CEIC 2014

Remediation Strategy

- Do you really trust what the system tells you?
- Assume compromise
- When in doubt, wipe the host…sometimes that may not save you!

Page 30

Why is removing malware so difficult?

CEIC 2014

Q & A