Stoned déjà vu – again

Peter Kleissner,
Michael Eisendle

Agenda

- Introduction to bootkits
- The new features
- Remote Surveillance Software
- Live Demo
- TPMkit

Who we are

Peter Kleissner:
- Independent Operating System Developer
- 1 year at Ikarus Security Software GmbH (Software Eng. / Malware An.)
- startup "Insecurity Systems" together with Michael Eisendle
- programmer of the Stoned Bootkit
- hoster of AV Tracker

Michael Eisendle:
- programmer of the Remote Software Tool

Vipin Kumar
- developer of the Linux bootkit part

Black Hat USA 2009: Stoned Bootkit
Hacking at Random 2009: The Rise of MBR Rootkits & Bootkits in the Wild
University of Vienna: Stoned Bootkit (private presentation)
DeepSec IDSC 2009 Europe: Stoned déjà vu – again

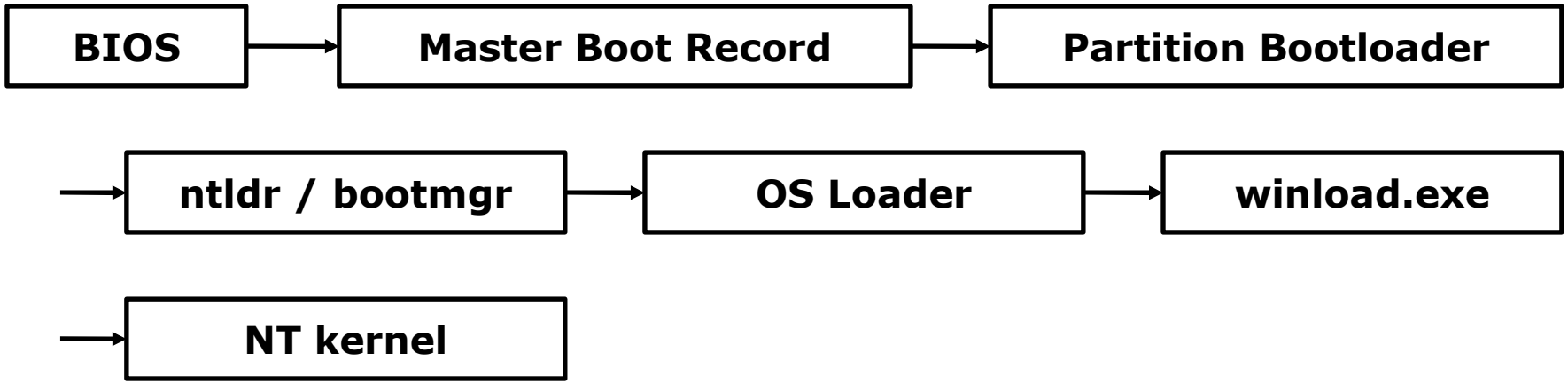
Why we are not finished

Stoned Bootkit 2

"A bootkit is a rootkit that is able to load from a master boot record and persist in memory all the way through the transition to protected mode and the startup of the OS. It's a very interesting type of rootkit."

Robert Hensing about bootkits

Execution flow of a bootkit



Storage on hard disk

Microsoft patched bootloader (injected instructions are loading Stoned)		C:	\ Master Boot Record.bak \Bootkit \Plugins\ …
1 sector	62 sectors		~ 10 MB
Bootloader		Partition	RawFS

7C00h	1024	Loader	Loader.sys
8000h	2048	System Loader	System Loader.sys
8800h	1024	Textmode User Interface	Textmode User Interface.sys
8C00h	9216	Disk System	Disk System.sys
B600h	8192	Preserved Space	[Embedded Boot Application]
D600h	1536	Crypto Module	Crypto Module.sys
DC00h	2048	Boot Module	Boot Module.sys
E400h	4096	Pwn Windows	Windows.sys

RawFS

Used for storing files on unpartitioned space

(especially for encrypted drives)

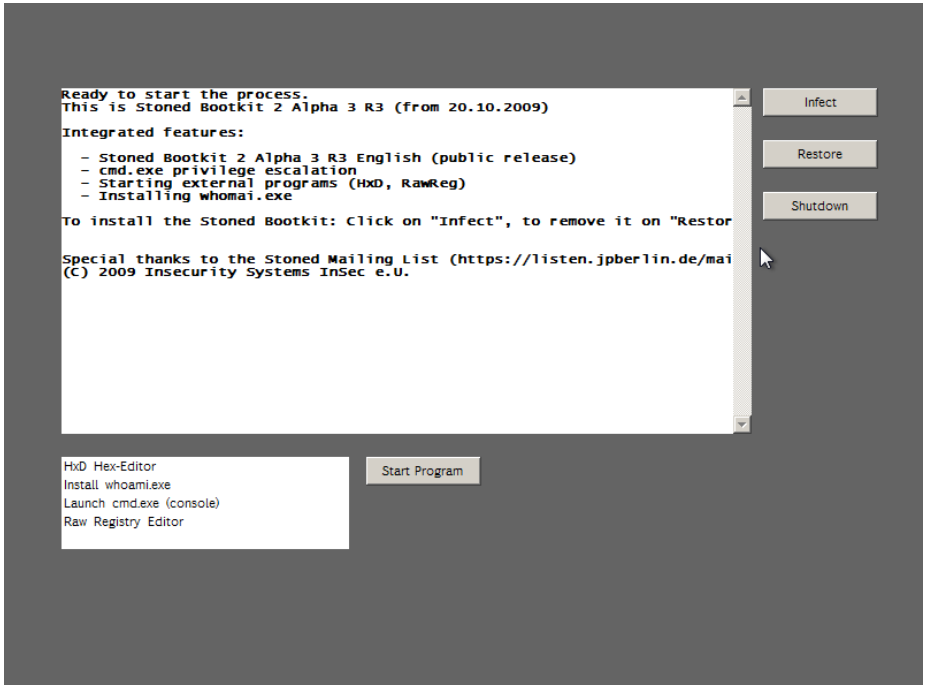
File Table	File 1	File 2	…	File Table	File 4
File 1 at sector X with size X File 2 at sector X with size X File Table at sector	\Bootkit			...	

File Table tells size, location and names (MD5) of files

```
B05B32A085DEFC9F4299C35AC8F358CD  \File Table                Next block of File Table
8F58EADD7BFFF0C557D4B5E9656957A5  \Bootkit                   Bootkit binary
0F13C73AAB0D4E000028038C99D3125A  \Master Boot Record.bak    Original MBR
…                                 \…                        All other files
```

Live CD

Based on Windows PE (created using the Windows AIK)



Native CD – infection only in memory

Boot record directly loaded by BIOS

‚El Torito' Bootable CD-ROM Format Specification

For testing purposes

Sector 16	Primary Volume Descriptor
Sector 17	Boot Record Volume Descriptor
Sector 18	Volume Descriptor Set Terminator
Sector 19	Path Table
Sector 24	Root Directory
Sector 25	\Stoned\
Sector 26	\Stoned\Applications\
Sector 27	\Stoned\Drivers\
Sector 28	\Stoned\Plugins\
Sector 29	Validation Entry, Initial entry (Boot Catalog)
Sector 30 +	Stoned Bootkit Boot Record and data of files

Remote Surveillance Tool – Michael Eisendle

- What this is about…
- Concept
- Features
- Plugins

About the RST

- The RST is a tool for monitoring and manipulating Computers (let's call it a trojan)

- Exactly: The RST is a toolkit utilizing various thechnologies and Web 2.0 services to control vast amounts of PCs for the use of administration, surveillance, information gathering and other uses...

Features

- Different ways of communication
- Encryption
- Authentication (RSA, DSA)
- Scriptable
- Updating (stub or plugins)
- „Code in the wire“
- „Droppers“

Concept

- Completely based on plugins
- Utilizes the concept of code in the wire for executing code from the cloud
- Hehe, another „Cloud Service“
- I think I was Stoned (hehe) while coding this...
- Developed and tested with/for the Stoned Bootkit

Plugins

Plugins for:

- Communication
  - normal TCP/IP, P2P networks, Web 2.0 Services (Twitter and co.)
- Authentication
  - RSA, DSA or whatever suits you
- Encryption
  - Currently only CipherSaber-2
- Commands
- Other uses

Communication Plugins

Give the possibility of using nearly any way of communication:

- TCP, UDP
- Raw IP packets
  - through SYN, ACK requests
- Twitter and co.
- Pastebin (or like these)
- One click hoster
- P2P (DHTs, Overnet, Gnutella...)

Cmd Plugins and Code in the Wire

- An RST Server can do everything, with plugins
- Examples

- Code in the wire
- The code is never ever stored on disk, just for execution in memory → only exists „in the wires“

Scripting and „Droppers“

- RST is scriptable → utilizes „droppers“ to submit information to „Dropzones“

- meh. :-)

- Droppers for
  - HTTP
  - SMTP
  - ...

Future support

- Support for more platforms
- Linux, Mac OS X, ...
- Platform independent plugins
- Poly/Metamorphic stubs

Stoned in 1987

- First „bootkit“
- Operating system independent!
- Only a virus (spreading over boot sector)

```
Your PC is now Stoned!          (1987)
Your PC is now Stoned!  ..again      (2010)
```

Trusted Platform Module

Defeating Trusted Platform Module with TPMkit

- Using hardware breakpoints DR0 – DR7 to catch calls:
  - 1. When overwriting the memory on startup (asm instructions)
  - 2. When reading the boot sector (int 13h)
- Computer will be restarted so TPM-BIOS will re-send hashes (the spoofed ones) to TPM chip
- No fix, all TPM systems affected, TPM becomes useless

References

[1] **Stoned Bootkit 1**

http://www.stoned-vienna.com/

[2] **Schlussbericht zur Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung")**

http://www.justiz.gv.at/_cms_upload/_docs/AG_OnlineDurchsuchung_Endbericht.pdf

[3] **Starting a Process from KernelMode**

http://www.codeproject.com/KB/system/KernelExec.aspx

[4] **"El Torito" Bootable CD-ROM Format Specification**

http://www.phoenix.com/NR/rdonlyres/98D3219C-9CC9-4DF5-B496-A286D893E36A/0/specscdrom.pdf

[5] **Windows Automated Installation Kit for Windows 7**

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34

[7] **OpenNIC TLD Governing Policy and Operated Namespaces**

http://wiki.opennic.glue/TLDPolicy

http://wiki.opennic.glue/OpenNICNamespaces

[3AM]Eminem

http://www.vimeo.com/5758619

Thanks for your attention! ..again

http://www.stoned-bootkit.info/

Presentation materials are published on the above website.

Contact Peter@Kleissner.at for any information.

Questions?

Comments?