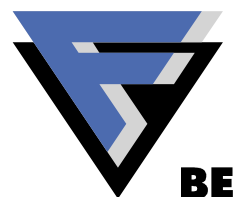




# AusCERT Asia Pacific 2008

Information Security Conference

**F-SECURE®**



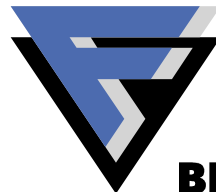
**BE SURE.**

# Evolution of Kernel-Mode Malware

May 19, 2008

Kimmo Kasslin

**F-SECURE®**



**BE SURE.**

# Agenda



- Definition of kernel-mode malware
- History
- Trend and present situation
- Evolution
  - The average Joe
  - Haxdoor, Apropos, Rustock, Srizbi, Mebroot
- Conclusions

# Definition



“Kernel malware is malicious software that runs fully or partially at the most privileged execution level, ring 0, having full access to memory, all CPU instructions, and all hardware.”

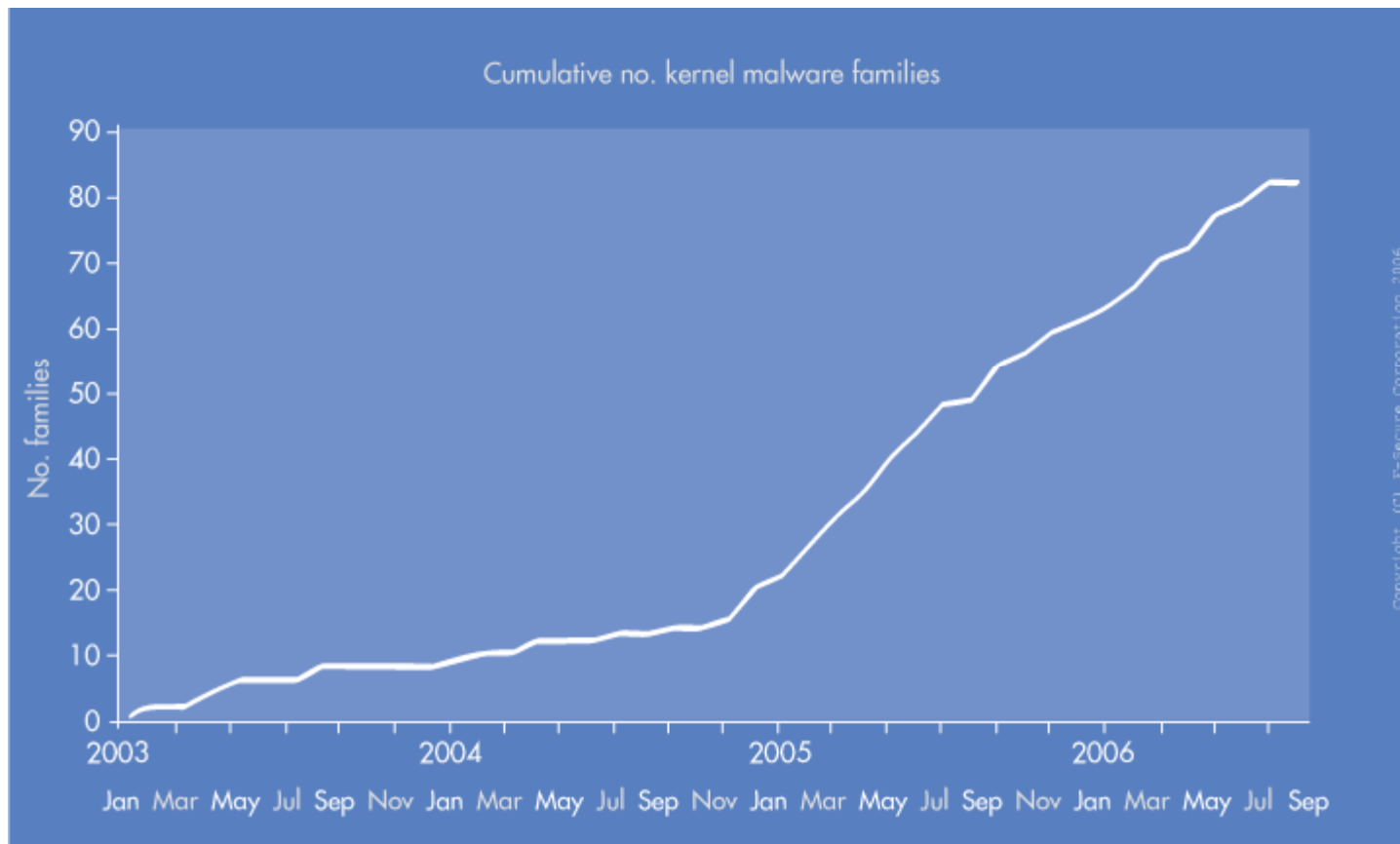
- Can be divided into two subcategories
  - Full-Kernel malware
  - Semi-Kernel malware

# History



- Kernel malware is not new – it has just been rare
- WinNT/Infis
  - Discovered in November 1999
  - Full-Kernel malware
  - Payload – PE EXE file infector
- Virus.Win32.Chatter
  - Discovered in January 2003
  - Semi-Kernel malware
  - Payload – PE SYS file infector
- Mostly proof of concepts

# Increase of Kernel-Mode Malware



# Situation Today



- Growth of kernel malware has been steady
- More main stream malware is utilizing kernel-mode techniques
  - Storm, Srizbi, Pandex, various banking trojans and password stealers
- Over half of the biggest spam botnets are kernel malware! [1]
  - Number 1 – Srizbi, 315.000 bots
  - Number 3 – Rustock, 150.000 bots
  - Number 4 – Pandex, 125.000 bots
  - Number 5 – Storm/Peacomm, 85.000 bots
- Malware is moving to kernel to protect themselves against security products and against other malware

1. Steward, Joe. (2008). Top Spam Botnets Exposed. <http://www.secureworks.com/research/threats/topbotnets/>

# Evolution – The Average Joe



- A simple piece of code whose purpose is to perform a specific task on behalf of the main malware component
- No code obfuscation or packing
- Usually a rootkit that hides
  - Files/Directories
  - Registry keys/values
  - Network connections
- Uses System Service Table and IRP handler hooks
- Easy to find and remove by modern AV solutions



# Evolution – Haxdoor



- Backdoor with rootkit and spying capabilities
  - First variant found in August 2003
- Has three components – EXE (installer), DLL (payload), SYS (rootkit)
- Uses the driver to make its detection and removal more difficult
  - Hides its process and files
  - Protects its own threads and processes against termination
  - Protects its own files against any access
  - Injects the main payload into newly created processes
- First widely utilized kernel-mode malware

# Evolution – Apropos



- Adware/Spyware with rootkit capabilities
  - Emerged in October 2005
- Has multiple components – EXEs (installer), DLLs (payload), SYS (rootkit)
- Uses the driver to make its removal more difficult and to bypass personal firewalls
  - Hides its directory, files, registry entries and processes
  - Driver is obfuscated
  - Uses inline patching with Interrupt handler hooking to hook kernel functions
  - Hooks ndis.sys and tcpip.sys modules to bypass firewalls
- First kernel-mode malware to utilize code obfuscation and NDIS hooking

# Evolution – Rustock



- Spambot and backdoor with rootkit capabilities
  - First variant found in December 2005
  - Rustock.A was found in 27<sup>th</sup> May 2006
  - Rustock.B was found in 3<sup>rd</sup> July 2006
- Consists of a single kernel-mode driver
  - EXE file loads the driver and deletes itself
  - SYS file carries the main payload inside an encrypted user-mode DLL
- The driver loads the main payload and acts as a rootkit to complicate its detection/removal and to bypass personal firewalls
- The most powerful and stealthiest rootkit seen by that time

# Evolution – Rustock – Details



- Rustock introduced new techniques to the stealth malware scene
  - Consists of a single driver which starts early during the boot process
  - Obvious traces of the loaded driver are removed from the memory
  - Driver is stored in a “hidden” and protected NTFS Alternate Data Stream
  - Driver uses obfuscation and a polymorphic packer
  - Hooks INT 0x2E and SYSENTER handler functions to control system calls
  - System Service Table hooks are present only when needed
  - Has an advanced rootkit anti-detection engine
  - Bypasses filter drivers by communicating directly to the lowest level device
  - Bypasses NDIS hooks by getting original pointers from ndis.sys file
  - Uses Asynchronous Procedure Call mechanism to execute the DLL in user mode
  - Tunnels network traffic from the DLL directly to the NDIS layer

# Evolution – Srizbi



- Spambot and backdoor with rootkit capabilities
  - Emerged in April 2007
- Consists of a single kernel-mode driver
  - EXE file loads the driver and deletes itself
- First complex full-kernel malware!
  - Implements a fully blown spam client with a HTTP based C&C infrastructure
  - Uses low-level NDIS hooks and private TCP/IP stack to send/receive packets
  - Has complex code to bypass memory hooks
- The first malware to bypass virtually every personal firewall!
- Basic rootkit – easy to detect and remove by modern AV software

# Evolution – Mebroot



- Downloader and backdoor with rootkit capabilities
  - First variant found in November 2007
- Consists of a custom MBR (loader) and a custom kernel-mode driver
  - EXE file replaces the MBR and writes the driver to raw disk sectors located in unpartitioned slack space at the end of the disk
- The most advanced and stealthiest malware seen so far!
  - Uses MBR as its launch point
  - All non-volatile data is stored in physical sectors outside of the file system
  - Driver uses polymorphic packer and advanced code obfuscation
  - Uses advanced NDIS hooks and private TCP/IP stack to send/receive packets
  - Utilizes “code pullout” technique to bypass memory hooks

## Srizbi – Spam from the kernel!

# Conclusions



- Kernel malware is a threat that has to be taken seriously
  - Wide distribution – Srizbi and Pandex spam runs, Mebroot drive-by-downloads from high volume web sites in Italy
- Today's kernel-mode malware is robust and effective
  - Biggest spam botnets are kernel-mode malware
  - Rustock, Srizbi and Mebroot are written by professional developers
- Detection and removal is becoming very challenging
  - How do you fight against someone who cheats?
- Prevention is a solution but how about false positives?
  - Please digitally sign your drivers



# Additional Information

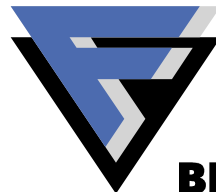


- Kasslin, K. (2006). Kernel malware: The attack from within.
  - [http://www.f-secure.com/weblog/archives/kasslin\\_AVAR2006\\_KernelMalware\\_paper.pdf](http://www.f-secure.com/weblog/archives/kasslin_AVAR2006_KernelMalware_paper.pdf)
- Florio, E.; Pathak P. (2006). Raising the bar: Rustock and advances in rootkits
  - <http://www.virusbtn.com/virusbulletin/archive/2006/09/vb200609-rustock>
- Kasslin, K.; Florio E. (2007). Spam from the kernel.
  - <http://www.virusbtn.com/virusbulletin/archive/2007/11/vb200711-srizbi>
- Kasslin, K.; Florio E. (2008). Your computer is now stoned (...again!).
  - <http://www.virusbtn.com/virusbulletin/archive/2008/04/vb200804-MBR-rootkit>

**THANK YOU... QUESTIONS?**

[kimmo.kasslin@f-secure.com](mailto:kimmo.kasslin@f-secure.com)

**F-SECURE®**



**BE SURE.**

**BE  
SURE.**

**F-SECURE®**

