“I can’t go back to yesterday, because I was a different person then”
“I can’t go back to yesterday because I was a different person then” - Lewis Carroll (English Author, mathematician)

Life is like a game, unfortunately, you can’t save and reload it - Chun Feng (Virus Researcher)

You still need to continue your life! 😊
Topics

- Hard Disk Recovery Card
  - What is a Hard Disk Recovery Card
  - How does it work

- Malware that targets Hard Disk Recovery Cards - Dogrobot
  - How does Dogrobot penetrate the protection offered by Hard Disk Recovery Cards
  - Why does it target Hard Disk Recovery Cards
  - What is its final goal
A system restore facility that can protect/restore hard disk data (MBR, partition table, files etc)

- preserves checkpoints on a hard disk
- reverts back to checkpoints (manual/auto)
Hard Disk Recovery Cards

Widely used by computers with public access (e.g., in Computer Labs, Internet Cafés, etc.)

- Prevents ongoing tampering with system configuration
- Restores system after infection
How Hard Disk Recovery Cards Work? (Copy-on-Write)
How Hard Disk Recovery Cards Work? (revert operation)
How Hard Disk Recovery Cards Work? (commit operation)
The implementation of Hard Disk Recovery Cards (Windows File System Overview)

File system Driver
- Ntfs.sys

Volume Driver
- Volsnap.sys
- ft_disk.sys

Disk Driver
- partmgr.sys
- disk.sys
- atapi.sys
The implementation of Hard Disk Recovery Card Windows File System Overview (Continued)

CreateFile( )

User Mode

D:\test.txt

Kernel Mode

NtCreateFile( )

\Global??\D:\test.txt

Object Manager

\Device\HarddiskVolume2\test.txt

VPB

File System Driver

Volume IO

Volume Driver

Disk IO

Disk
The implementation of Hard Disk Recovery Cards (disk filter driver)

\Device\Recovery is attached onto \Device\Harddisk0\DR0

\Device\Recovery

\Device\Harddisk0\DR0
I can’t go back to yesterday (emergence of Dogrobot)

- 1st Sample observed in September 2007
- Penetrates the protection offered by Hard Disk Recovery Cards and overwrites system file (e.g., userinit.exe, conime.exe)
- Caused 8 Billion RMB (1.2 Billion USD) loss to Internet Cafés in China
Penetrating the protection offered by Hard Disk Recovery Cards

Defeating “Copy-on-write”
Penetrating Hard Disk Recovery Cards (method 1)

- Detach DEVICE_OBJECT -> AttachedDevice of disk device object; then write to the file

- Raw disk access \\\PhycialDrive0
Penetrate Hard Disk Recovery Card (method 2)

Unusual Disk read/write via disk.sys:

IRP_MJ_READ/IRP_MJ_WRITE
IRP_MJ_INTERNAL_DEVICE_CONTROL

construct SCSI_REQUEST_BLOCK structure to perform disk read/write
Penetrate Hard Disk Recovery Card (method 3)

Another Unusual Read/Write via disk.sys

IRP_MJ_READ/IRP_MJ_WRITE

IRP_MJ_INTERNAL_DEVICE_CONTROL

IRP_MJ_DEVICE_CONTROL with I/O Control Code:

• IOCTL_SCSI_PASS_THROUGH
• IOCTL_ATA_PASS_THROUGH
• IOCTL_IDE_PASS_THROUGH
Raw Disk Sectors Access Limits

- Built-in file system parsing code 😞
- Does not function on compressed drive 😞
- Can only overwrite existing file, not add new files 😞
Penetrate Hard Disk Recovery Card (Virtual Disk technique)

Virtual Disk \\.\yyy2

C:\

D:\

Physical Disk

Permanent Storage

Scratch Space
Penetrating Hard Disk Recovery Cards (Virtual Disk technique)

- Disk read/write in virtual disk will be mapped to physical disk (permanent storage) (via unusual read/write)

Dogrobot can manipulate the files like
- Copy("C:\\dogrobot.exe", "\\\\\yyy2\\windows\\system32\\userinit.exe", ...)

The file system of \\\yyy2 will be mounted the same as c: volume
Penetrating Hard Disk Recovery Cards (Virtual Disk technique)

- Create new files ☺
- Compressed drive support ☺
- 3rd party file system support ☺

Code is based on open source Filedisk
http://www.acc.umu.se/~bosse/
Who let the dog out? (Distributing Dogrobot)

- Via exploits (0 day exploits, e.g. MS09-032)

- Via removable drives (using autorun.inf)

- Via ARP cache poisoning
Man In the Middle attack

Gateway

Victim

Attacker

IP-G/ARP-G

IP-V/ARP-V

IP-A/ARP-A

Insert iframe with link to exploit script into HTTP(port 80) traffic
What is the final target?

- Designed to target Internet Cafés in China
  - Hard Disk Recovery Cards are widely used in Internet Café
  - ARP cache poisoning is effective in Internet Café
- Sold as “black product in the black market”
- Downloads password stealing trojans (1:20)
  - Frethog
  - Lolyda
  - Zuten
  - Tilcun
The operation of the black market

1. Exploit Scripts
2. Dogrobot
3. PWS trojans
4. Money
Black Market History

2006-2007
Viking

2007-2008
Dogrobot
The real face of Dogrobot

- Downloads and protects PWS trojans
- Why does it target Internet Cafés?
  Ideal place to steal online game passwords
  70% of password theft occurs in Internet Cafés (unofficial statistic)
- From the black market, for the black market
Conclusion

- The 1st sample targeting Hard Disk Recovery Cards in the wild
- Designed specifically to target Internet Cafés in China
- From the black market, and for the black market
- I can’t go back to yesterday, but I will still enjoy today- because I still have tomorrow