Deactivate the Rootkit

Anibal Sacco
Alfredo A. Ortega
History:

2004: The BIOS size of 60% of all notebooks suffered an increase of 25Kb

- Fast forward 5 years, 2009:
  - We were trying to install our own BIOS rootkit (Persistent BIOS Infection Talk, CanSecWest / Syscan)
  - We found that there was something already there!
What is the rootkit?

- Absolute Corp. Computrace, Anti-theft agent
- Option ROM Embedded in Phoenix BIOS
- Agreements with law enforcement agencies.
- Inside notebooks from HP, Dell, Lenovo, Toshiba, Gateway, Asus, Panasonic, and more.

Option ROM header:

```
00000000 55 aa 2a eb 15 43 6f 6d 70 75 54 72 61 63 65 20 |U.*..CompuTrace |
00000010 56 38 30 2e 38 36 78 1d 00 e9 5c 01 50 43 49 |V80.866x...\PCI|
00000020 52 17 19 34 12 00 00 18 00 00 06 00 00 2a 00 00 |R..4.........*..|
```
Basic Inner workings:

See patent application US 2006/0272020 A1

- BIOS
  - Activation via secret SMBIOS API or DMI Strings
  - Direct filesystem modification from BIOS while booting
  - FAT / FAT32 / NTFS / bitlocker driver

- Boot
- Windows 98/2000/XP/Vista 32/64
  - Injests into IE
  - And calls Home
  - RPC-like over plain HTTP

- Agent
  - Home: search.namequery.com
Basic Inner workings:

PCI Option ROM

- Computrace Loader Module - 6kb
- Agent Installation Module - 6kb
- Agent - 10kb
- Configuration Block

PCI Header
- Reserves memory (PMM)
- Loads Agent Inst. Module
- Resize (Unload)

Installs Agent in supported OSes
- Supports NT/2000/XP and 9x/Me
- Supports FAT/FAT32 and NTFS

Agent self-installs instance
- As service in OS
The Agent service once Installed, initiates all server Sessions (RPC over HTTP-like)
Problems found:

- Huge privacy risk (bad/no authentication)
- Anyone could activate it with enough privileges
- Anyone can change the configuration
- Anyone can de-activate it (at least in certain known cases)
- Whitelisted by AV (potentially indetectable)
More problems found:

- Use of URL instead of IP (hosts redirection)
- Configuration block modification:
  Demo if there is time...

```
Configuration block XOR 0xB5:
00000000 b1 b7 b5 b5 35 ab b1 b4 b5 f5 b4 aa b1 b5 b5 b5 |....5............|
00000010 b5 a5 bf 41 41 30 49 4e 30 30 30 30 95 b1 1f |...AA0IN00000...|
00000020 ee 30 86 a0 b1 8b b5 35 b5 ac ae 4a 4a 4a 4a 4a |0.....5...JJJJJJ|
00000030 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a |JJJJJJJJJJJJJJJJ|
00000040 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a 4a |JJJJJJJJ...5....|
00000050 b5 a8 b7 b5 b5 f3 b3 b5 b5 b5 b5 b5 b5 b5 f2 b3 b5 |........................|
00000060 b5 b5 b5 b5 b5 fd af 00 50 d1 35 71 17 73 65 61 |........P.5g.sea|
00000070 72 63 68 2e 6e 61 6d 65 71 75 65 72 79 2e 63 6f |rch.namequery.co|
00000080 6d bf b7 b2 a5 b3 b3 ac 35 b4 b4 b5 b5 b2 b3 b5 |m........5.......|
00000090 b5 b5 b5 b5 b5 4a 98 b4 0d 98 b4 0d 9e b1 41 54 44 |....J.........ATD|
000000a0 54 81 b7 38 2c 80 b7 39 2c 82 b2 39 2c 39 31 38 |T..8,..9,..9,918|
```

Stub agent: Unauthenticated BIOS code execution
Detecting the Rootkit Agent

- A single file to look for:
  - `system32\rpcnet.exe` (Normal Agent)
  - `system32\rpcnetp.exe` (BIOS Persistent Agent)

- A service called "Remote Procedure Call (RPC) Net" with no description

- Outgoing connections to search.namequery.com (209.53.113.223)

- Our Computrace Option Rom Dumper tool
Deactivating:

- Easiest way: hosts file redirection
- Modifying BIOS (only **unsigned BIOS**)!
- Modifying configuration block (Registry, hard-disk, etc.)
- Modifying nvram, then full HD Wipe.
The Past:

- US 6,300,863 B1 Pat. Figure 8A
- Filed Mar 24 1998, Absolute Corporation
- Agent inside modem Option ROM
- Support for DOS Backdooring

See “Implementing and Detecting a PCI Rootkit”, Heasman, BlackHat 2007
The Future:

- Phoenix Failsafe:
  - Inside SMM, sounds familiar?
  - Always-on OS-independent, Wifi and GPS tracking
  - It has “safe” in the name instead of “trace”

- Intel Anti-theft technology:
  - vPro technology
  - Using AMT secondary processor
  - Works even with the notebook turned off!

- Other security applications residing in BIOS

Strong authentication: “Trust us, is for your own protection”.
This is only the beginning

- More research is needed in this area!
- CoreBoot (LinuxBIOS) project, is computrace-free
- Questions?
- Thanks! Now if you'll just look into the light: