(U) BIOS Threats

Jump to: navigation, search

(U) I would like feedback on this page. Please edit or leave a comment on the Talk page!

(U) BIOS implants are firmware written which reside in a computer's BIOS and perform some function. Though not necessarily malicious, implants can be used to conduct CNA and CNE.[1]

(U) BIOS attacks and implants have been used and are known by both state and non nation-state actors. There have been presentations on them in previous Black Hat and DEF CON conventions.[2] LOJACK for laptops is an optionally manufacturer-installed BIOS implant for Dell laptops.[3] BIOS attacks can even be traced back at least to the Chernobyl virus in 1998.[4]

Contents

[hide]

[edit] (U) Key Findings

- (U) Using a BIOS implant for CNE is more difficult than for CNA. Without specific information about the targeted system(s), the implant is much more likely to prevent proper system booting (CNA).[5]
- (U) When using a BIOS implant for either CNE or CNA by remote means, there must be an initial infection by traditional malware. The intruder still needs to obtain administrator or root access. Supply chain and insider threat are both still possible.[5]
- (TS//SI//REL TO USA, FVEY) There are currently no ways in use to detect a BIOS infection outright on NIPRNet. The only way we would see a BIOS infection using current methods would be indirectly, through network traffic generated when the implant phones home.[5]
- (U//FOUO) The main reason for introducing malware into an expansion card (or BIOS) is to maintain a persisting presence through typical methods of system rebuilds. In addition to being immune to hard disk reformatting and OS reinstallations, some BIOS implants can survive a flashing of the BIOS by hiding in the BIOS's free space. Graphic, sound, and network card firmware could provide further hiding places. "Graphic cards have been subverted to support distributed brute-force password breaking. Network cards could be used to create covert channels. Security researchers have shown that sound cards can be controlled by malware to emit frequencies beyond normal hearing range designed to exfiltrate data."[6]

[edit] (U) Key Judgments

- (TS//SI//NF) PLA and MAKERSMARK versions do not appear to have a common link beyond the interest in developing more persistent and stealthy CNE.[7][8][9]
- (TS//SI//NF) Among currently compromised are AMI and Award based BIOS versions. The threat that BIOS implants pose increases significantly for systems running on compromised versions.[10]

[edit] (U) Recent News and Reporting

click column headers to sort

Agency	Feed
Open Source	Failed to load RSS feed from [redacted]
CIA	Failed to load RSS feed from [redacted]
DIA	Failed to load RSS feed from [redacted]
NSA	Failed to load RSS feed from [redacted]
State Department	Failed to load RSS feed from [redacted]

[edit] (U) Virus attacks

(U) There are at least three known BIOS attack viruses.

[edit] (U) CIH

(U) The first was a virus which was able to erase Flash ROM BIOS content, rendering computer systems unstable. CIH, also known as "Chernobyl Virus", appeared for the first time in mid-1998 and became active in April 1999. It affected systems' BIOS and often could not be fixed on their own since they were no longer able to boot at all. To repair this, Flash ROM IC had to be ejected from the motherboard to be reprogrammed somewhere else. Damage from CIH was possible since the Virus was specifically targeted at the then widespread Intel i430TX motherboard chipset, and the most common operating systems of the time were based on the Windows 9x family allowing direct hardware access to all programs.

(U) Modern systems are not vulnerable to CIH because of a variety of chipsets being used which are incompatible with the Intel i430TX chipset, and also other Flash ROM IC types. There is also extra protection from accidental BIOS rewrites in the form of boot blocks which are protected from accidental overwrite or dual and quad BIOS equipped systems which may, in the event of a crash, use a backup BIOS. Also, all modern operating systems like Linux, Mac OS X, Windows NT-based Windows OS like Windows 2000, Windows XP and newer, do not allow user mode programs to have direct hardware access. As a result, as of 2008, CIH has become essentially harmless, at worst causing annoyance by infecting executable files and triggering alerts from antivirus software. Other BIOS viruses remain possible, however:[11] since most Windows users run all applications with administrative privileges, a modern CIH-like virus could, in

principle, still gain access to hardware.

[edit] (U) Black Hat 2006

(U) The second one was a technique presented by John Heasman, principal security consultant for UK based Next-Generation Security Software at the Black Hat Security Conference (2006), where he showed how to elevate privileges and read physical memory, using malicious procedures that replaced normal ACPI functions stored in flash memory.

[edit] (U) Persistent BIOS Infection

(U) The third one, known as "Persistent BIOS infection", was a method presented in CanSecWest Security Conference (Vancouver, 2009) and SyScan Security Conference (Singapore, 2009) where researchers Anibal Sacco[12] and Alfredo Ortega, from Core Security Technologies, demonstrated insertion of malicious code into the decompression routines in the BIOS, allowing for nearly full control of the PC at every start-up, even before the operating system is booted.

(U) The proof-of-concept does not exploit a flaw in the BIOS implementation, but only involves the normal BIOS flashing procedures. Thus, it requires physical access to the machine or for the user on the operating system to be root. Despite this, however, researchers underline the profound implications of their discovery: “We can patch a driver to drop a fully working rootkit. We even have a little code that can remove or disable antivirus.”[13]

[edit] (U) References

1. ↑ BIOS Threat Mitigation Info
2. ↑ (U) www.coresecurity.com/content/Deactivate-the-Rootkit
3. ↑ (U) www.absolute.com/en/lojackforlaptops/home.aspx
4. ↑ (U) www.Symantec.com/security_response/writeup.jsp?docid=2000-122010-2655-99
5. ↑ 5.0 5.1 5.2 (TS//SI//REL TO USA, FVEY) Basic Input-Output System (BIOS) based Malware by [redacted]
6. ↑ (S//NF) USCYBERCOM; J2 Bulletin 10-03; Hardware-Based Malware Demonstrates Resistance to Standard Security Practices; 30 June 2010
7. ↑ (TS//SI//REL TO USA, FVEY) NTOC; V22-ITN-087-10; Analysis of a BIOS Rootkit; 24 MAY 2010
8. ↑ (U//FOUO) TDX-315/072060-10 240000Z SEP 10, source marked (TS//HCS//NF)
9. ↑ IOC CTW 2010-02-4C 28 Feb 2010
10. ↑ (TS//SI//REL TO USA, FVEY) DIRNSA, 3/OO/521733-10 READDRESSAL Probable Contractor to PRC People's Liberation Army Conducts Computer Network Exploitation Against Taiwan Critical Infrastructure Networks; Develops Network Attack Capabilities, R 011521Z SEP 10
11. ↑ New BIOS Virus Withstands HDD Wipes, March 27, 2009 by Marcus Yam – Tom's Hardware US
12. ↑ Sacco, Anibal; Alfredo Ortéga. Persistent BIOS Infection. *Exploiting Stuff*. Retrieved on 2010-02-06.
13. ↑ Fisher, Dennis. Researchers unveil persistent BIOS attack methods. *Threat Post*. Retrieved on 2010-02-06.

[edit] (U) Additional Reading

- (S) DIA; Defense Intelligence Digest: BIOS: China's Covert Cyber Capability; 14 Oct 2010 (A-Space required)
- (U) TOUCHWOLF – NSANet Wikiinfo page
- (U) STROMTIME BIOS Action Plan Status – NSANet Wikiinfo page

Retrieved from "http://[redacted]
Categories: Cyber Threat Assessments | BIOS

TOP SECRET//SI//NOFORN

Search Search

- Main Page
- Recent changes
- Help
- Random Article
- Sandbox
- Guidelines
- Recent files
- Top categories

interaction

- Featured articles
- Announcements
- Collaboration requests
- Tutorial
- Bulletin Board
- Metrics
- Acronyms
- People Finder

social software tools

Toolbox

- Privacy policy
- About Intellipedia
- Disclaimers
-

[redacted]

This page contains dynamic content -- Highest Possible Classification isTOP SECRET//SI/TKSecurity BannerTerms of Use