Malware burrows deep into computer BIOS to escape AV

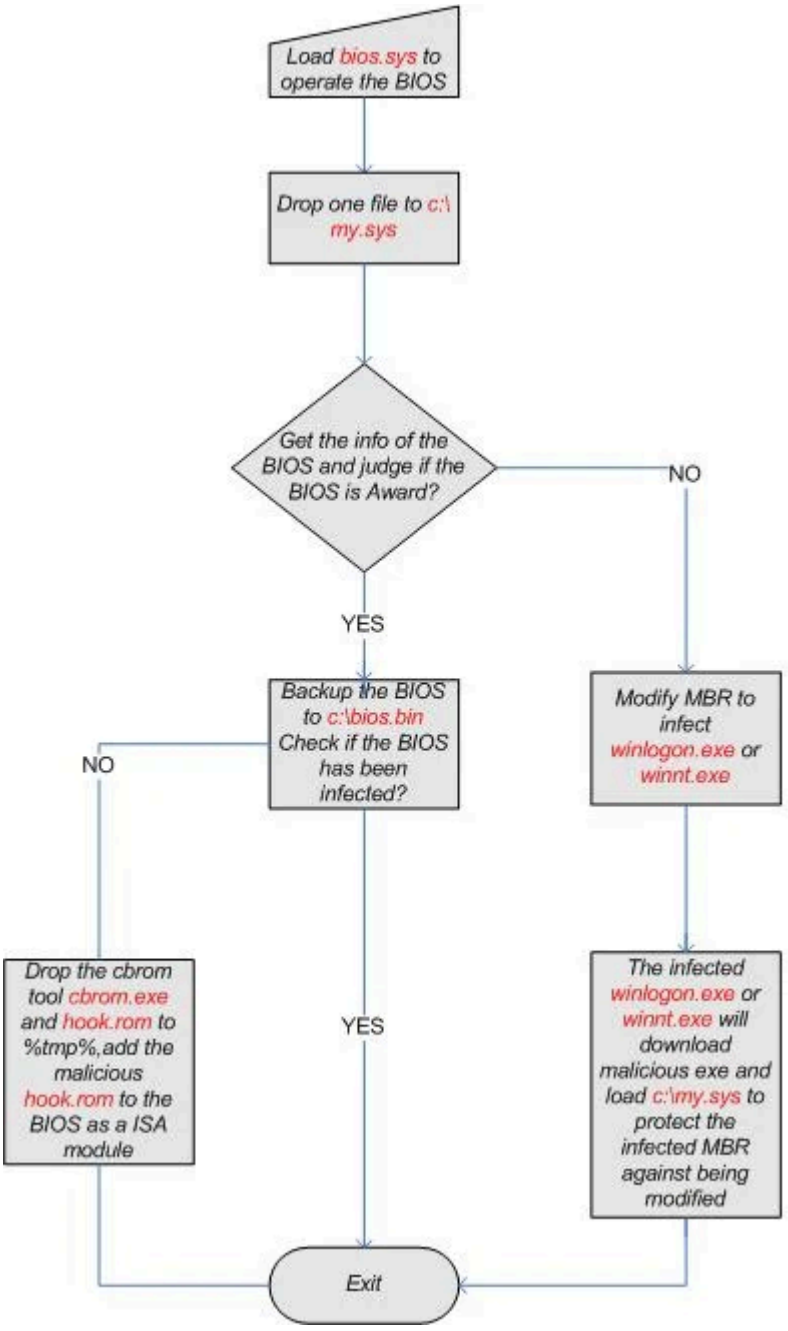
By Dan Goodin

Published: 2011-09-14 · Archived: 2026-04-10 02:41:08 UTC

Researchers have discovered one of the first pieces of malware ever used in the wild that modifies the software on the motherboard of infected computers to ensure the infection can't be easily eradicated.

Known as Trojan.Mebromi, the rootkit reflashes the BIOS of computers it attacks to add malicious instructions that are executed early in a computer's boot-up sequence. The instructions, in turn, alter a computer's MBR, or master boot record, another system component that gets executed prior to the loading of the operating system of an infected machine. By corrupting the processes that run immediately after a PC starts, the malware stands a better chance of surviving attempts by antivirus programs to remove it.

In addition to posing a threat to end users, Mebroot could create serious obstacles to antivirus developers in producing products that scrub computers clean of detected threats without harming the underlying system.



A flowchart from Symantec detailing Mebromi's BIOS tampering process.

"Storing the malicious code inside the BIOS ROM could actually become more than just a problem for security software, giv[en] the fact that even if antivirus detect[s] and clean[s] the MBR infection, it will be restored at the next system startup when the malicious BIOS payload would overwrite the MBR code again," Webroot researcher Marco Giuliani wrote in a blog post published Tuesday. "Developing an antivirus utility able to clean the BIOS code is a challenge, because it needs to be totally error-proof, to avoid rendering the system unbootable at all."

He went on to say the job of ridding malicious instructions added to the BIOS ultimately should be left to the makers of the motherboards that store the startup code. Because the BIOS is stored on an EEPROM, or electronically erasable programmable read-only-memory chip, modifications have the potential to render a computer largely inoperable with no easy way to fix it.

The discovery represents one of the few times researchers have documented malware used in the wild that modifies the BIOS. In the late 1990s, malware known as CIH/Chernobyl did much the same thing on machines running Windows 9x by exploiting a privilege escalation bug in the Microsoft operating systems. In 2007, proof-of-concept software known as IceLord also reportedly made changes to the BIOS of infected machines, but there are no reports it has ever been used in actual attacks.

Mebromi is able to attack only BIOS ROMs made by Award, a manufacturer that was purchased by Phoenix in the late 1990s. The malware checks the BIOS ROM each time the PC boots up. If it's made by Award and the malicious instructions aren't found, Mebromi adds the code by reflashing the chip on the motherboard. According to Giuliani, it was first documented by the Chinese security company Qihoo 360, and primarily infects computers in that country.

Symantec researchers have more about Mebromi here. ®

This article was updated to clarify the type of chip stores the BIOS.
