Hacking BIOS Chips Isn't Just the NSA's Domain Anymore

Kim Zetter ⋮ 6-7 minutes ⋮ 3/20/2015

The ability to hack the BIOS chip at the heart of every computer is no longer reserved for the NSA and other three-letter agencies. *Millions* of machines contain basic BIOS vulnerabilities that let anyone with moderately sophisticated hacking skills compromise and control a system surreptitiously, according to two researchers.

The revelation comes two years after a catalogue of NSA spy tools leaked to journalists in Germany surprised everyone with its talk about the NSA's efforts to infect BIOS firmware with malicious implants.

The BIOS boots a computer and helps load the operating system. By infecting this core software, which operates below antivirus and other security products and therefore is not usually scanned by them, spies can plant malware that remains live and undetected even if the computer's operating system were wiped and re-installed.

BIOS-hacking until now has been largely the domain of advanced hackers like those of the NSA. But researchers Xeno Kovah and Corey Kallenberg presented a proof-of-concept attack today at the CanSecWest conference in Vancouver, showing how they could remotely infect the BIOS of multiple systems using a host of new vulnerabilities that took them just hours to uncover. They also found a way to gain high-level system privileges for their BIOS malware to undermine the security of specialized operating systems like Tails---used by journalists and activists for stealth communications and handling sensitive data.

Although most BIOS have protections to prevent unauthorized modifications, the researchers were able to bypass these to reflash the BIOS and implant their malicious code.

Kovah and Kallenberg recently left MITRE, a government contractor that conducts research for the Defense Department and other federal agencies, to launch LegbaCore, a firmware security consultancy. They note that the recent discovery of a firmware-hacking tool by Kaspersky Lab researchers makes it clear that firmware hacking like their BIOS demo is something the security community should be focusing on.

Because many BIOS share some of the same code, they were able to uncover vulnerabilities in 80 percent of the PCs they examined, including ones from Dell, Lenovo and HP. The vulnerabilities, which they're calling incursion vulnerabilities, were so easy to find that they wrote a script to automate the process and eventually stopped counting the vulns it uncovered because there were too many.

"There's one type of vulnerability, which there's literally dozens of instances of it in every given BIOS," says Kovah. They disclosed the vulnerabilities to the vendors and patches are in the works but have not yet been released. Kovah says, however, that even when vendors have produced BIOS patches in the past, few people have applied them.

"Because people haven't been patching their BIOSes, all of the vulnerabilities that have been disclosed over the last couple of years are all open and available to an attacker," he notes. "We spent the last couple of years at MITRE running around to companies trying to get them to do patches. They think BIOS is out of sight out of mind [because] they don't hear a lot about it being attacked in the wild."

An attacker could compromise the BIOS in two ways---through remote exploitation by delivering the attack code via a phishing email or some other method, or through physical interdiction of a system. In that case, the researchers found that if they had physical access to a system they could infect the BIOS on some machines in just two minutes. This highlights just how quickly and easy it would be, for example, for a government agent or law enforcement officer with a moment's access to a system to compromise it.

Their malware, dubbed LightEater, uses the incursion vulnerabilities to break into and hijack the system management mode to gain escalated privileges on the system. System management mode, or SMM, is an operations mode in Intel processors that firmware uses to do certain functions with high-level system privileges that exceed even administrative and root-level privileges, Kovah notes. Using this mode, they can rewrite the contents of the BIOS chip to install an implant that gives them a persistent and stealth foothold. From there, they can install root kits and steal passwords and other data from the system.

But more significantly, SMM gives their malware the ability to read all data and code that appears in a machine's memory. This would allow their malware, Kovah points out, to subvert any computer using the Tails operating system---the security and privacy-oriented operating system Edward Snowden and journalist Glenn Greenwald used to handle NSA documents Snowden leaked. By reading data in memory, they could steal the encryption key of a Tails user to unlock encrypted data or swipe files and other content as it appears in memory. Tails is meant to be run from a secure USB flash drive or other removable media---so that conceivably it won't be affected by viruses or other malware that may have

infected the computer. It operates in the computer's memory and once the operating system is shut down, Tails scrubs the RAM to erase any traces of its activity. But because the LightEater malware uses the system management mode to read the contents of memory, it can grab the data while in memory before it gets scrubbed and store it in a safe place from which it can later be exfiltrated. And it can do this while all the while remaining stealth.

"Our SMM attacker lives in a place nobody checks today to see if there's an attacker," Kovah says. "System management mode can read everyone's RAM, but nobody can read System Management Mode's RAM."

Such an attack shows, he says, that the operating system Snowden chose to protect himself can't actually protect him from the NSA or anyone else who can design an attack like LightEater.