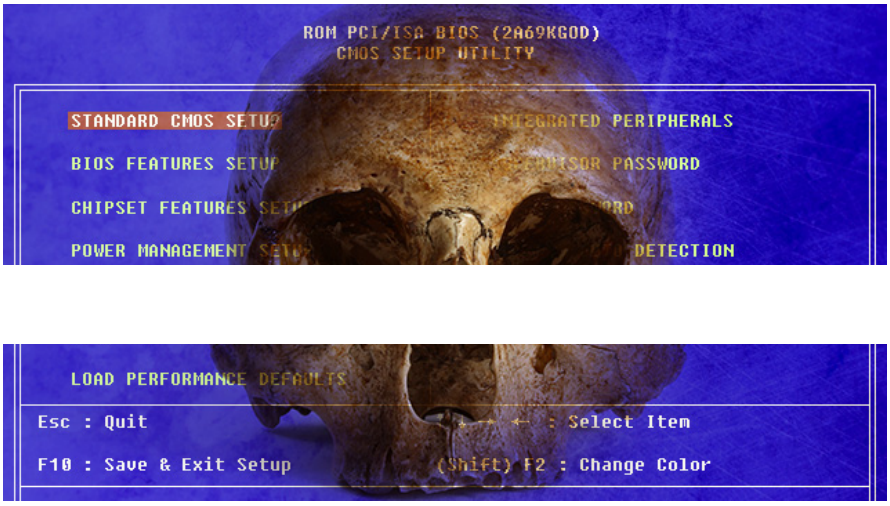
BIZ & IT

Meet “badBIOS,” the mysterious Mac and PC malware that jumps airgaps

Like a super strain of bacteria, the rootkit plaguing Dragos Ruiu is omnipotent.

DAN GOODIN – OCT 31, 2013 7:07 AM | 646



Credit: Aurich Lawson / Thinkstock

TEXT SETTINGS

Three years ago, security consultant Dragos Ruiu was in his lab when he noticed something highly unusual: his MacBook Air, on which he had just installed a fresh copy of OS X, spontaneously updated the firmware that helps it boot. Stranger still, when Ruiu then tried to boot the machine off a CD ROM, it refused. He also found that the machine could delete data and undo configuration changes with no prompting. He didn't know it then, but that odd firmware update would become a high-stakes malware mystery that would consume most of his waking hours.

In the following months, Ruiu observed more odd phenomena that seemed straight out of a science-fiction thriller. A computer running the Open BSD operating system also began to modify its settings and delete its data without explanation or prompting. His network transmitted data specific to the Internet's next-generation IPv6 networking protocol, even from computers that were supposed to have IPv6 completely disabled. Strangest of all was the ability of infected machines to transmit small amounts of network data with other infected machines even when their power cords and Ethernet cables were unplugged and their Wi-Fi and Bluetooth cards were removed. Further investigation soon showed that the list of affected operating systems also included multiple variants of Windows and Linux.

"We were like, 'Okay, we're totally owned,'" Ruiu told Ars. "'We have to erase all our systems and start from scratch,' which we did. It was a very painful exercise. I've been suspicious of stuff around here ever since."

In the intervening three years, Ruiu said, the infections have persisted, almost like a strain of bacteria that's able to survive extreme antibiotic therapies. Within hours or weeks of wiping an infected computer clean, the odd behavior would return. The most visible sign of contamination is a machine's inability to boot off a CD, but other, more subtle behaviors can be observed when using tools such as Process Monitor, which is designed for troubleshooting and forensic investigations.

Another intriguing characteristic: in addition to jumping "airgaps" designed to isolate infected or sensitive machines from all other networked computers, the malware seems to have self-healing capabilities.

"We had an air-gapped computer that just had its [firmware] BIOS reflashed, a fresh disk drive installed, and zero data on it, installed from a Windows system CD," Ruiu said. "At one point, we were editing some of the components and our registry editor got disabled. It was like: wait a minute, how can that happen? How can the machine react and attack the software that we're using to attack it? This is an air-gapped machine and all of a sudden the search function in the registry editor stopped working when we were using it to search for their keys."

Over the past two weeks, Ruiu has taken to Twitter, Facebook, and Google Plus to document his investigative odyssey and share a theory that has captured the attention of some of the world's foremost security experts. The malware, Ruiu believes, is transmitted though USB drives to infect the lowest levels of computer hardware. With the ability to target a computer's Basic Input/Output System (BIOS), Unified Extensible Firmware Interface (UEFI), and possibly other firmware standards, the malware can attack a wide variety of platforms, escape common forms of detection, and survive most attempts to eradicate it.

But the story gets stranger still. In posts here, here, and here, Ruiu posited another theory that sounds like something from the screenplay of a post-apocalyptic movie: "badBIOS," as Ruiu dubbed the malware, has the ability to use high-frequency transmissions passed between computer speakers and microphones to bridge airgaps.

Bigfoot in the age of the advanced persistent threat

At times as I've reported this story, its outline has struck me as the stuff of urban legend, the advanced persistent threat equivalent of a Bigfoot sighting. Indeed, Ruiu has conceded that while several fellow security experts have assisted his investigation, none has peer reviewed his process or the tentative findings that he's beginning to draw. (A compilation of Ruiu's observations is here.)

Also unexplained is why Ruiu would be on the receiving end of such an advanced and exotic attack. As a security professional, the organizer of the internationally renowned CanSecWest and PacSec conferences, and the founder of the Pwn2Own hacking competition, he is no doubt an attractive target to state-sponsored spies and financially motivated hackers. But he's no more attractive a target than hundreds or thousands of his peers, who have so far not reported the kind of odd phenomena that has afflicted Ruiu's computers and networks.

In contrast to the skepticism that's common in the security and hacking cultures, Ruiu's peers have mostly responded with deep-seated concern and even fascination to his dispatches about badBIOS.

"Everybody in security needs to follow @dragosr and watch his analysis of #badBIOS," Alex Stamos, one of the more trusted and sober security researchers, wrote in a tweet last week. Jeff Moss—the founder of the Defcon and Blackhat security conferences who in 2009 began advising Department of Homeland Security Secretary Janet Napolitano on matters of computer security—retweeted the statement and added: "No joke it's really serious." Plenty of others agree.

"Dragos is definitely one of the good reliable guys, and I have never ever even remotely thought him dishonest," security researcher Arrigo Triulzi told Ars. "Nothing of what he describes is science fiction taken individually, but we have not seen it in the wild ever."

Been there, done that

Triulzi said he's seen plenty of firmware-targeting malware in the laboratory. A client of his once infected the UEFI-based BIOS of his Mac laptop as part of an experiment. Five years ago, Triulzi himself developed proof-of-concept malware that stealthily infected the network interface controllers that sit on a computer motherboard and provide the Ethernet jack that connects the machine to a network. His research built off of work by John Heasman that demonstrated how to plant hard-to-detect malware known as a rootkit in a computer's peripheral component interconnect, the Intel-developed connection that attaches hardware devices to a CPU.

It's also possible to use high-frequency sounds broadcast over speakers to send network packets. Early networking standards used the technique, said security expert Rob Graham. Ultrasonic-based networking is also the subject of a great deal of research, including this project by scientists at MIT.

Of course, it's one thing for researchers in the lab to demonstrate viable firmware-infecting rootkits and ultra high-frequency networking techniques. But as Triulzi suggested, it's another thing entirely to seamlessly fuse the two together and use the weapon in the real world against a seasoned security consultant. What's more, use of a USB stick to infect an array of computer platforms at the BIOS level rivals the payload delivery system found in the state-sponsored Stuxnet worm unleashed to disrupt Iran's nuclear program. And the reported ability of badBIOS to bridge airgaps also has parallels to Flame, another state-sponsored piece of malware that used Bluetooth radio signals to communicate with devices not connected to the Internet.

"Really, everything Dragos reports is something that's easily within the capabilities of a lot of people," said Graham, who is CEO of penetration testing firm Errata Security. "I could, if I spent a year, write a BIOS that does everything Dragos said badBIOS is doing. To communicate over ultrahigh frequency sound waves between computers is really, really easy."

Coincidentally, Italian newspapers this week reported that Russian spies attempted to monitor attendees of last month's G20 economic summit by giving them memory sticks and recharging cables programmed to intercept their communications.

Eureka

For most of the three years that Ruiu has been wrestling with badBIOS, its infection mechanism remained a mystery. A month or two ago, after buying a new computer, he noticed that it was almost immediately infected as soon as he plugged one of his USB drives into it. He soon theorized that infected computers have the ability to contaminate USB devices and vice versa.

"The suspicion right now is there's some kind of buffer overflow in the way the BIOS is reading the drive itself, and they're reprogramming the flash controller to overflow the BIOS and then adding a section to the BIOS table," he explained.

He still doesn't know if a USB stick was the initial infection trigger for his MacBook Air three years ago, or if the USB devices were infected only after they came into contact with his compromised machines, which he said now number between one and two dozen. He said he has been able to identify a variety of USB sticks that infect any computer they are plugged into. At next month's PacSec conference, Ruiu said he plans to get access to expensive USB analysis hardware that he hopes will provide new clues behind the infection mechanism.

He said he suspects badBIOS is only the initial module of a multi-staged payload that has the ability to infect the Windows, Mac OS X, BSD, and Linux operating systems.

Dragos Ruiu. Credit: Julia Wolf

"It's going out over the network to get something or it's going out to the USB key that it was infected from," he theorized. "That's also the conjecture of why it's not booting CDs. It's trying to keep its claws, as it were, on the machine. It doesn't want you to boot another OS it might not have code for."

To put it another way, he said, badBIOS "is the tip of the warhead, as it were."

“Things kept getting fixed”

Ruiu said he arrived at the theory about badBIOS's high-frequency networking capability after observing encrypted data packets being sent to and from an infected laptop that had no obvious network connection with—but was in close proximity to—another badBIOS-infected computer. The packets were transmitted even when the laptop had its Wi-Fi and Bluetooth cards removed. Ruiu also disconnected the machine's power cord so it ran only on battery to rule out the possibility that it was receiving signals over the electrical connection. Even then, forensic tools showed the packets continued to flow over the airgapped machine. Then, when Ruiu removed the internal speaker and microphone connected to the airgapped machine, the packets suddenly stopped.

With the speakers and mic intact, Ruiu said, the isolated computer seemed to be using the high-frequency connection to maintain the integrity of the badBIOS infection as he worked to dismantle software components the malware relied on.

"The airgapped machine is acting like it's connected to the Internet," he said. "Most of the problems we were having is we were slightly disabling bits of the components of the system. It would not let us disable some things. Things kept getting fixed automatically as soon as we tried to break them. It was weird."

It's too early to say with confidence that what Ruiu has been observing is a USB-transmitted rootkit that can burrow into a computer's lowest levels and use it as a jumping off point to infect a variety of operating systems with malware that can't be detected. It's even harder to know for sure that infected systems are using high-frequency sounds to communicate with isolated machines. But after almost two weeks of online discussion, no one has been able to rule out these troubling scenarios, either.

"It looks like the state of the art in intrusion stuff is a lot more advanced than we assumed it was," Ruiu concluded in an interview. "The take-away from this is a lot of our forensic procedures are weak when faced with challenges like this. A lot of companies have to take a lot more care when they use forensic data if they're faced with sophisticated attackers."

Listing image: Aurich Lawson / Thinkstock

DAN GOODIN
SENIOR SECURITY EDITOR

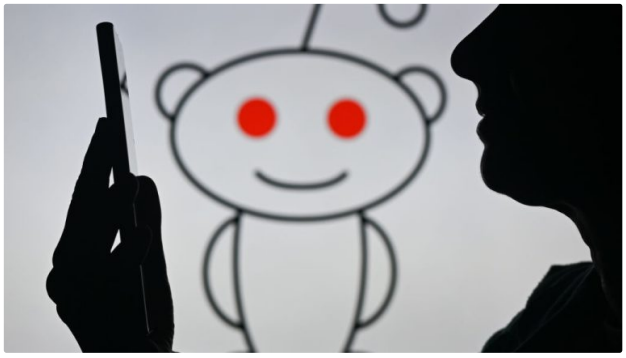
Dan Goodin is Senior Security Editor at Ars Technica, where he oversees coverage of malware, computer espionage, botnets, hardware hacking, encryption, and passwords. In his spare time, he enjoys gardening, cooking, and following the independent music scene. Dan is based in San Francisco. Follow him at here on Mastodon and here on Bluesky. Contact him on Signal at DanArs.82.

646 COMMENTS

PREV STORY

NEXT STORY

MOST READ



1. Reddit will lock some content behind a paywall this year, CEO says

2. DOGE's .gov site lampooned as coders quickly realize it can be edited by anyone