Bad news for attackers: VirusTotal can scan for malicious code in firmware

January 31 2016, by Nancy Owano

What can you do if the reason for your computer infection is so deep that malicious code cannot be detected even with the best antivirus scans? Firmware has become a notoriously great place for mischief, with malware planted at the firmware level.

What is firmware? It is described as the low-level code that bridges the hardware and operating system at startup.

Jan Willem Aldershoff in *Myce.com* wrote "Firmware is often the first piece of code loaded on a system and resides in a flash memory soldered to the mainboard. By infecting firmware an attacker can add malicious code that remains on the computer even after a clean install."

You have probably seen numerous headlines warning about router firmware as vulnerable to attack.

Abner Li in *9to5Google* also talked about the security headache, in that "malicious software that targets firmware can remain on a computer even after reboots, OS wipes, and installations. As most antiviruses do not scan computer firmware, it leaves a gaping security hole."

Findings about routers in December are just one case in point: Two researchers from Edith Cowan University said in *The Conversation* that they extracted the firmware from 37 currently available broadband routers. "We then reverse engineered the firmware to analyze components such as the operating system, system libraries and executable files. This allowed us to construct a comprehensive database of devices, software versions and known vulnerabilities. We found that 90 percent of the components analyzed were more than six years old. In every firmware we found obsolete software with known security issues, regardless of the manufacturer or release date."

A sign if not sigh of relief: Google, reported IDG News Service on Thursday, has added a new tool that analyzes firmware. VirusTotal, a subsidiary of Google, has released a new tool which may help prevent malware from reaching a computer's firmware.

Francisco Santos of VirusTotal announced this step in a blog on Wednesday.

VirusTotal is a free online service that analyzes files and URLs. The service can help enable users to identify malicious content and now has added a tool for analyzing firmware. Since antivirus programs "are not scanning this layer, the compromise can fly under the radar," wrote Santos, a security engineer.

The service aims to characterize in detail firmware images, whether legit or malicious. The firmware scanning tool performs tasks such as Apple Mac BIOS detection and reporting; extraction of BIOS Portable

Executables and identification of potential Windows Executables contained within the image; and PCI class code enumeration, allowing device class

Li in *9to5Google* said, "VirusTotal now allows people to upload a firmware image to have it scanned for any extra files that were not officially shipped by a computer maker. They employ various techniques, including heuristic detection and certification extraction, to perform a thorough scan of your system. Their blog post recommends several utilities for Mac and PC to grab a firmware image and also advise users to remove any private information before uploading to their tool."

Santos expressed thanks to Teddy Reed, developer of the UEFI firmware python parser, who was "instrumental in helping us overcome our ignorance about BIOS, UEFI, and its ecosystem."

What does all this mean to you? VirusTotal is now able to scan firmware and BIOS files for malicious code. The tool can use several methods to determine if a firmware is safe. Catalin Cimpanu of *Softpedia* presented a helpful rundown on what you can do with VirusTotal's new feature and may be worth checking out.

Cimpanu commented: "VirusTotal, the best thing for security aficionados since sliced bread, has announced initial support for detecting and then properly analyzing firmware images. The new feature should come in handy to users who suspect they might be infected with rootkit malware."

More information: www.virustotal.com/en/

blog.virustotal.com/2016/01/pu … ware-malware_27.html