virustotal
INSIDE VIRUSTOTAL'S PANTS

WEDNESDAY, 27 JANUARY 2016

Putting the spotlight on firmware malware

Firmware malware has been a hot topic ever since Snowden's leaks revealed NSA's efforts to infect BIOS firmware. However, BIOS malware is no longer something exclusive to the NSA, Lenovo's Service Engine or Hacking Team's UEFI rootkit are examples of why the security industry should put some focus on this strain of badness.

To all effects BIOS is a firmware which loads into memory at the beginning of the boot process, its code is on a flash memory chip soldered onto the mainboard. Since the BIOS boots a computer and helps load the operating system, by infecting it attackers can deploy malware that survives reboots, system wiping and reinstallations, and since antiviruses are not scanning this layer, the compromise can fly under the radar.

As of today VirusTotal is characterizing in detail firmware images, legit or malicious. These are a couple of examples of the kind of information that is now generated, please refer to the *File Detail* tab:
https://www.virustotal.com/en/file/3afb102f0a61f5a71be4658c3d8d3624e4773e36f64fd68a173f931bc38f651e/analysis/ [1]
https://www.virustotal.com/en/file/4db9177af43a958686b9367f19df90023acf3189c388497a8a7d1d8cb3f7f0e0/analysis/ [2]
https://www.virustotal.com/en/file/57a0c38bf7cf516ee0e870311828dba5069dc6f1b6ad13d1fdff268ed674f823/analysis/
Pay attention to the *Additional information* tab in this other case, you will see a new *Source Details* field which gives attribution information for the given file:
https://www.virustotal.com/en/file/8b1ec36a50683db137d3bd815052dd6034697af8ef2afd6c81c912b6d0f0f2e0/analysis/
100% PE resource match is not required in order to provide some attribution context, e.g.
https://www.virustotal.com/en/file/a90f803e10530e8f941d7054a12a37aa7b22c89bac89b6d2b8e40878bffccf11/analysis/

SEARCH

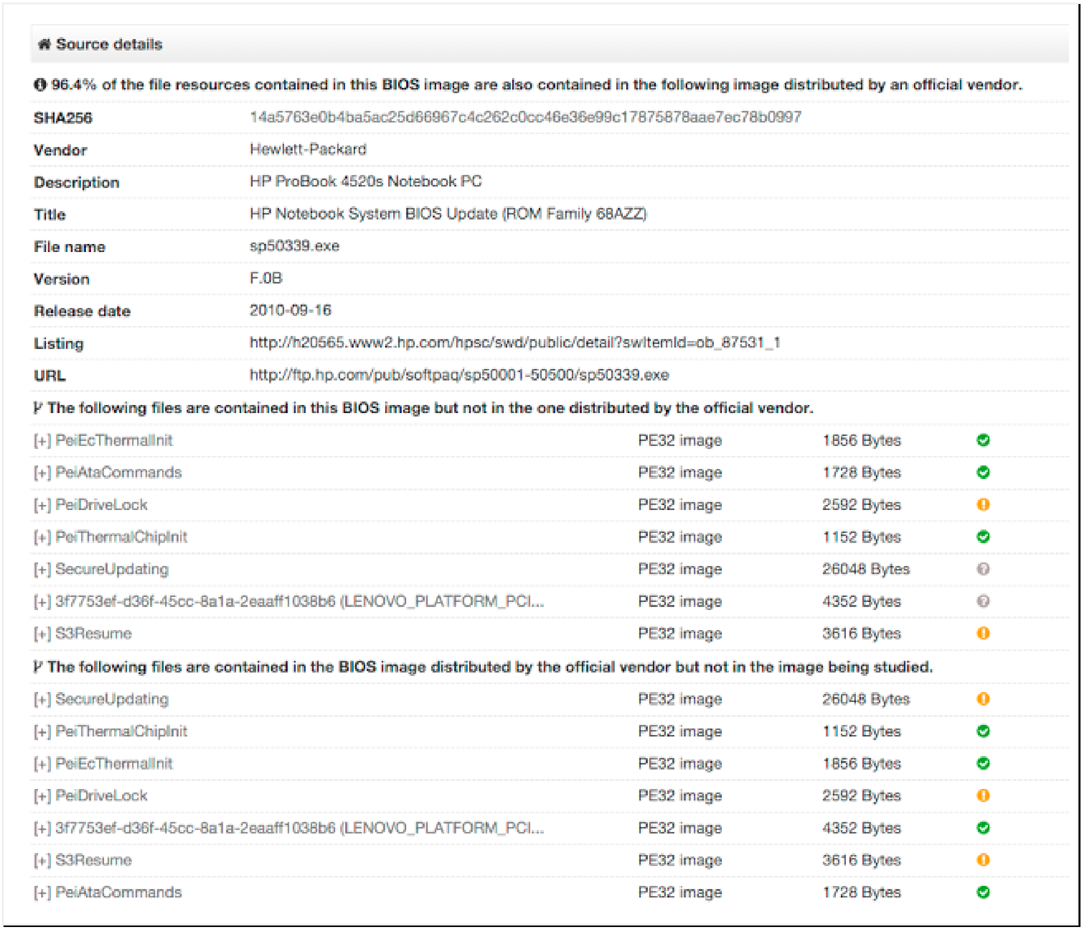
Search

BLOG ARCHIVE

- ▼ 2016 (1)
  - ▼ January (1)
    - Putting the spotlight on firmware malware
- ► 2015 (8)
- ► 2014 (24)
- ► 2013 (26)
- ► 2012 (26)
- ► 2011 (1)

CONTRIBUTORS

- Víctor Manuel Álvarez
- Julio Canto
- Julio Canto
- Bernardo Quintero
- Karl Hiramoto
- Francisco Santos
- Emiliano Martinez
- VirusTotal Team



Source details

96.4% of the file resources contained in this BIOS image are also contained in the following image distributed by an official vendor.

SHA256	14a5763e0b4ba5ac25d66967c4c262c0cc46e36e99c17875878aae7ec78b0997
Vendor	Hewlett-Packard
Description	HP ProBook 4520s Notebook PC
Title	HP Notebook System BIOS Update (ROM Family 68AZZ)
File name	sp50339.exe
Version	F.0B
Release date	2010-09-16
Listing	http://h20565.www2.hp.com/hpsc/swd/public/detail?swItemId=ob_87531_1
URL	http://ftp.hp.com/pub/softpaq/sp50001-50500/sp50339.exe

The following files are contained in this BIOS image but not in the one distributed by the official vendor.

[+] PeiEcThermalInit	PE32 image	1856 Bytes	✓
[+] PeiAtaCommands	PE32 image	1728 Bytes	✓
[+] PeiDriveLock	PE32 image	2592 Bytes	!
[+] PeiThermalChipInit	PE32 image	1152 Bytes	✓
[+] SecureUpdating	PE32 image	26048 Bytes	?
[+] 3f7753ef-d36f-45cc-8a1a-2eaaff1038b6 (LENOVO_PLATFORM_PCI...	PE32 image	4352 Bytes	?
[+] S3Resume	PE32 image	3616 Bytes	!

The following files are contained in the BIOS image distributed by the official vendor but not in the image being studied.

[+] SecureUpdating	PE32 image	26048 Bytes	!
[+] PeiThermalChipInit	PE32 image	1152 Bytes	✓
[+] PeiEcThermalInit	PE32 image	1856 Bytes	✓
[+] PeiDriveLock	PE32 image	2592 Bytes	!
[+] 3f7753ef-d36f-45cc-8a1a-2eaaff1038b6 (LENOVO_PLATFORM_PCI...	PE32 image	4352 Bytes	✓
[+] S3Resume	PE32 image	3616 Bytes	!
[+] PeiAtaCommands	PE32 image	1728 Bytes	✓

The new tool performs the following basic tasks:

- Apple Mac BIOS detection and reporting.
- Strings-based brand heuristic detection, to identify target systems.
- Extraction of certificates both from the firmware image and from executable files contained in it.
- PCI class code enumeration, allowing device class identification.
- ACPI tables tags extraction.
- NVAR variable names enumeration.
- Option ROM extraction, entry point decompilation and PCI feature listing.
- Extraction of BIOS Portable Executables and identification of potential Windows Executables contained within the image.
- SMBIOS characteristics reporting.

What's probably most interesting is the extraction of the UEFI Portable Executables that make up the image, since it is precisely executable code that could potentially be a source of badness. These executables are extracted and submitted individually to VirusTotal, such that the user can eventually see a report for each one of them and perhaps get a notion of whether there is something fishy in their BIOS image. Additionally, the tool will highlight which of these extracted PEs are Windows targeted, i.e. they will run on the Windows OS itself rather than on the UEFI pseudo-OS. Usually you would not see Windows executables in this layer, though there are some exceptions like the following case: https://www.virustotal.com/en/file/b3387bca327350038ef455d80ca22833e5d7a5173f0b52300b50fcce78ba0d22/analysis/

As you can see, the report distinguishes between any kind of PE and PEs that will run on the Windows OS itself, the first one of which happens to be detected by a noticeable amount of antivirus vendors. This executable is actually an antitheft product called

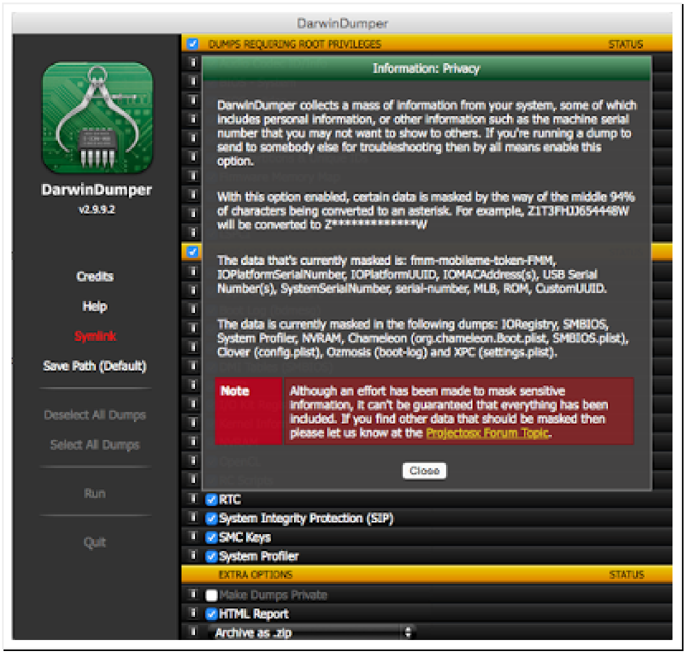
Computrace, embedded in many BIOS in order to be able to track a system after theft, even if the system is wiped and reinstalled. Totally legit when used for this purpose.

This exemplifies one way in which the new characterization can help in hunting badness, for instance, if you take a closer look at the very first two examples:
https://www.virustotal.com/en/file/3afb102f0a61f5a71be4658c3d8d3624e4773e36f64fd68a173f931bc38f651e/analysis/
https://www.virustotal.com/en/file/4db9177af43a958686b9367f19df90023acf3189c388497a8a7d1d8cb3f7f0e0/analysis/
You will notice that this is precisely the Lenovo rootkit case. They are two different BIOS updates for Lenovo S21e laptop systems, the second one removes what was identified as factory-installed malware, taking a closer look at both reports you will notice that the first image contains a NovoSecEngine2 Windows executable in charge of deploying further artifacts onto the target system.

Knowing that this new tool is available, the next interesting step would be to be able to dump your own BIOS in order to further study it by submitting it to VirusTotal, the following tools might come in handy:
https://bitbucket.org/blackosx/darwindumper/downloads
https://github.com/chipsec/chipsec
https://www.blackhat.com/docs/us-13/US-13-Butterworth-BIOS-Security-Code.zip
https://flashrom.org/Flashrom

Obviously, this has its limitations, the system could be compromised in such a manner that the dumpers are deceived, you should understand that the ultimate ground truth is physically attaching to the chip and electronically dumping the flash memory.

When performing BIOS dumps and uploading to VirusTotal make sure you remove private information, certain vendors may store secrets such as WiFi passwords in BIOS variables in order to remember certain settings across system reinstalls. If you are on a Mac, DarwinDumper will allow you to easily strip sensitive information by checking the "Make dumps private" option.



Information: Privacy

DarwinDumper collects a mass of information from your system, some of which includes personal information, or other information such as the machine serial number that you may not want to show to others. If you're running a dump to send to somebody else for troubleshooting then by all means enable this option.

With this option enabled, certain data is masked by the way of the middle 94% of characters being converted to an asterisk. For example, Z1T3FHJJ654448W will be converted to Z**************W

The data that's currently masked is: fmm-mobileme-token-FMM, IOPlatformSerialNumber, IOPlatformUUID, IOMACAddress(s), USB Serial Number(s), SystemSerialNumber, serial-number, MLB, ROM, CustomUUID.

The data is currently masked in the following dumps: IORegistry, SMBIOS, System Profiler, NVRAM, Chameleon (org.chameleon.Boot.plist, SMBIOS.plist), Clover (config.plist), Ozmosis (boot-log) and XPC (settings.plist).

Note: Although an effort has been made to mask sensitive information, it can't be guaranteed that everything has been included. If you find other data that should be masked then please let us know at the Projectosx Forum Topic.

Close

☑ RTC
☑ System Integrity Protection (SIP)
☑ SMC Keys
☑ System Profiler

EXTRA OPTIONS STATUS
□ Make Dumps Private
☑ HTML Report
Archive as .zip

Premium users of VirusTotal Intelligence and VirusTotal Private Mass API will soon be able to read a follow-up article in Intelligence's blog in order to understand how all of this information is now indexed and searchable, allowing you to track down advanced actors making use of BIOS badness in order to persist in their targets' systems.

We would like to specially thank Teddy Reed, developer of the UEFI firmware python parser, he has been instrumental in helping us overcome our ignorance about BIOS, UEFI, and its ecosystem.

Published by Francisco Santos

G+1 +5 Recommend this on Google

Tags: bios, efi, firmware, flash, malware, uefi

No comments:

Post a Comment

Enter your comment...

Comment as: ggyy (Google)

Sign out

Publish Preview ☐ Notify me

Home Older Post

Subscribe to: Post Comments (Atom)