MALWARE THREATS TO UEFI AND HOW TO MITIGATE THEM

Introduction to UEFI

The Unified Extensible Firmware Interface (UEFI) is a software interface which serves as the intermediary between the firmware and the operating system on modern PCs. Established in 2005 by an alliance of the leading software and hardware developers, most notably Intel, it is now quickly superseding the legacy BIOS standard. This is achieved thanks to a number of advanced features which BIOS lacks: for example, the ability of install and run executables, network and Internet capability, cryptography, CPU-independent architecture and drivers, etc.

UEFI Vulnerabilities

The very advanced capabilities that make UEFI such an attractive platform also open way to new vulnerabilities that didn't exist in the age of the more rigid BIOS. For example, the ability to run custom executable modules makes it possible to create malware that would be launched by UEFI before any anti-malware solution – or, indeed, the OS itself – had a chance to start.

Secure Boot is not a panacea

Secure Boot is a technology described by recent revisions of the UEFI specification; it enables a hardware-verified operating system bootup process that is supposedly malware-free by design, thus ensuring the security of system deployment.

While this is definitely a step in the right direction, we believe it cannot guarantee a 100% malware-free system startup due to the following reasons:

- Not all hardware manufacturers support Secure Boot, as it significantly limits the UEFI functionality.
- As this protective measure can be turned on/off by the user, some of them will definitely choose to deactivate it.
- Secure Boot itself might contain vulnerabilities that the cybercriminals will take advantage of.

The complex architecture of UEFI inevitably contains vulnerabilities which can potentially enable cybercriminals to introduce malware that would persist on the system even after complete OS reinstallation. For example, a trio of vulnerabilities which can allow the attacker with local access to bypass firmware write protections and reflash the firmware came to light early this year[1] [2]. This makes it possible to initiate the attacks along the following vectors:

- Compromise OS and EFI loaders (add new or infect the existing ones)
- Compromise UEFI drivers
- Get direct access to the motherboard's flash memory from the OS
- and many others.

By exploiting these vulnerabilities, the perpetrators will become able to launch both indiscriminate and targeted attacks, allowing them to:

- Intercept data input and output; safely exfiltrate stolen data
- Create reliably hidden areas in the computer's flash memory
- Compromise electronic signatures
- Establish hidden channels of communications with remote command&control servers
- Load external OSs using UEFI's networking interfaces

And the genie is now out of the bottle – even if these vulnerabilities are patched in future versions of UEFI, others are likely to be found by highly dedicated attackers. Whereas in 2014 only a couple of papers on malware affecting firmware were published as well as a couple of viable proofs of concept demonstrated, now, just over the 3 months of 2015, these figures have grown by several times. A new generation of tailored malware specifically targeting firmware (not UEFI, but HDD or SSD controllers... for now) was even detected in the wild – of course, we are referring to the infamous Equation Group[3]. It's probably a safe bet that malware targeted at UEFI exploits is even now being developed and tested by the same cybercriminal groups that stand behind the most insidious APTs of the recent years.

Legacy OS vulnerabilities

Another class of malware that could be eradicated overnight by making UEFI more secure is rootkits and bootkits – some of the most advanced technologies used by cybercriminals to launch the malicious code before the operating system starts.

(over, please)

After gaining access to OS bootup process, the bootkit malware begins to deploy advanced anti-detection countermeasures, compromise system drivers, create its own processes and services that the OS considers as legitimate.

This technology is used in many implementations of malware, such as Careto[4], to name a recent example. For instance, it very effectively conceals targeted attacks.

Even now, hunderds of thousands of systems are infected by rootkits. This figure might appear to be insignificant when compared to the millions of 'traditional' viral and Trojan infections, but unlike the latter, rootkits and bootkits are some of the most dangerous malicious technologies in use today. This makes the creation of a reliable and versatile anti-rootkit/anti-bootkit 'magic bullet' one of the most desirable goals in the entire information security industry.

UEFI Needs to Be Secured – Now!

Right now UEFI, an incredibly important part of any PC, remains virtually unprotected from the new generation of malware threats. No such malware was ever detected in the wild, but the theory behind it is sound, and we are expecting to see the emergence of such threats very shortly.

The good news is that, among other features, the UEFI specification has provisions to embed a security solution 'on the chip'. Ideally, such a solution must perform UEFI self-integrity checks, making sure it is not infected, as well as scan the OS files on the local machine, detecting and eliminating any malware, such as rootkits and bootkits.

Kaspersky Anti-Virus for UEFI

Kaspersky Lab took hold of this opportunity to develop the world's first UEFI-compliant anti-malware product designed to scan selected system files and memory addresses before the operating system even starts loading. The advantages of such an approach cannot be overstated:

- Previously, rootkits and bootkits could embed themselves deeply into the system and load ahead of any conventional anti-malware solution, thus obfuscating their activity from the anti-virus, or even preventing it from loading altogether. Even though market-leading solutions are able to detect and eliminate them, this requires extra steps (booting from secure media, etc.), and even then, the result is not 100% guaranteed for the newest breeds of malware.
- The EFI threats that we expect to see in the nearest months remain completely invisible and, thus, invulnerable to 'classic' desktop solutions. This means that, an overwhelming majority of the newest computer systems (using UEFI instead of the legacy BIOS) remains at mercy of tomorrow's malware.

But now, by loading from a ROM chip on motherboard that is guaranteed to be clear of bugs, Kaspersky Anti-Virus for UEFI (KUEFI) will be able to scan system critical area (EFI System Partition, GUID Partition Table, OS loader and core, key OS files, registry, etc.) before loading the OS. It relies upon the Kaspersky Anti-Virus Engine to ensure protection from rootkits, bootkits and other malware. Based on Kaspersky Lab's cutting-edge technologies and the award-winning Kaspersky Anti-Virus core, the solution allows for flexible scan settings to reach the desired 'performance vs. detection rate' tradeoff and achieve the exact performance level the user needs.

1. https://threatpost.com/cert-warns-of-uefi-hardware-vulnerabilities/110213
2. http://www.securityweek.com/researchers-find-several-uefi-vulnerabilities
3. https://threatpost.com/inside-nls_933w-dll-the-equation-apt-persistence-module/111128
4. http://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/