Technical Analysis

LoJax UEFI Rootkit Overview

A technical analysis of the malware and how HP Sure Start protects the PC BIOS/UEFI

UEFI Rootkit attacks have long been a concern because they are near impossible to detect, extremely difficult to remove, and can allow hackers to have persistent control over the infected PC, creating a risk for corporate networks.

HP SURE START
HP Sure Start will detect & repair unauthorized modification of the BIOS/UEFI against attacks, including more sophisticated variants of LoJax

The malware of the future is here

After years of research demonstrating that UEFI (a.k.a., BIOS) rootkit attacks are a growing threat, in Oct 2018, the world saw a UEFI rootkit used in a real-world attack. **Researchers from ESET presented their analysis** of this new malware at the 2018 Microsoft BlueHat conference.

This malware includes a UEFI rootkit, called LoJax. Several high-profile targets in Central and Eastern Europe were impacted. This malware infects UEFI firmware, giving it extensive control of the PC. It is designed to exploit vulnerabilities in UEFI implementations that allow a bad actor to modify the UEFI firmware in an unauthorized manner. While ESET originally found that this rootkit was designed to take advantage of vulnerabilities prevalent in older systems, our analysis shows that even modern systems could be exposed. This means that the PCs that are at risk include current shipping systems from vendors across the industry who do not sufficiently protect the UEFI firmware against unauthorized modification, and also older systems that were unpatched against a previously known vulnerability (**https://www.kb.cert.org/vuls/id/766164**).

UEFI Rootkit attacks have long been a concern because they can be difficult to detect, extremely difficult to remove, and can grant hackers near-total control of the infected PC, including access to corporate networks. Any future vulnerability that could be used to modify UEFI firmware (or critical UEFI configuration settings such as but not limited to Secure Boot enablement) will now be a potential target for a new LoJax variant. In anticipation of this threat, HP introduced HP Sure Start technology in 2014, and has continued to advance its protections against UEFI-rootkits, reaching the 4th generation of HP Sure Start this year. HP Sure Start protects against not only LoJax but also advanced variants of LoJax and other sophisticated UEFI attacks that are likely to emerge. HP Sure Start uses HP's Endpoint Security Controller (ESC), a unique hardware component, to detect and automatically recover from any such attacks. HP's ESC also enables advanced HP device security solutions like **HP Sure Run** and **HP Sure Recover**.

HP Sure Start technology is the result of years of collaboration between HP's Commercial PC business group and senior security researchers in HP Labs in Bristol, UK. The primary vision and motivation for the creation of HP Sure Start was to design a modern PC for cyber resiliency from its core hardware and firmware. HP PCs that ship with HP Sure Start meet and exceed recently published resiliency principles described in the NIST SP 800-193 "Platform Firmware Resiliency Guidelines" publication (**https://csrc.nist.gov/publications/detail/sp/800-193/final**). HP Sure Start uses a Defense in Depth[1] approach. In addition to including industry standard protections for UEFI, which are designed to prevent modifications of UEFI code and critical configurations by malicious software, HP also adds a hardware-based Root of Trust mechanism. In the event an attacker manages to bypass the industry standard protections to land a malicious payload in the UEFI flash (via a zero day or even some type of physical attack), this Root of Trust will cryptographically detect the unauthorized modification of UEFI firmware and policies. (Note: cryptographic protection of UEFI policies is also unique to HP Sure Start.) HP Sure Start is also unique in the industry in its ability to repair UEFI using a cryptographically-validated copy that is stored in a tamper-detectable private flash memory. HP adds double the amount of flash memory found on a standard PC to every HP Sure Start system to ensure this hardened firmware resilience. This secondary flash memory is electrically-isolated from access by the host CPU, where potentially malicious software maybe running.

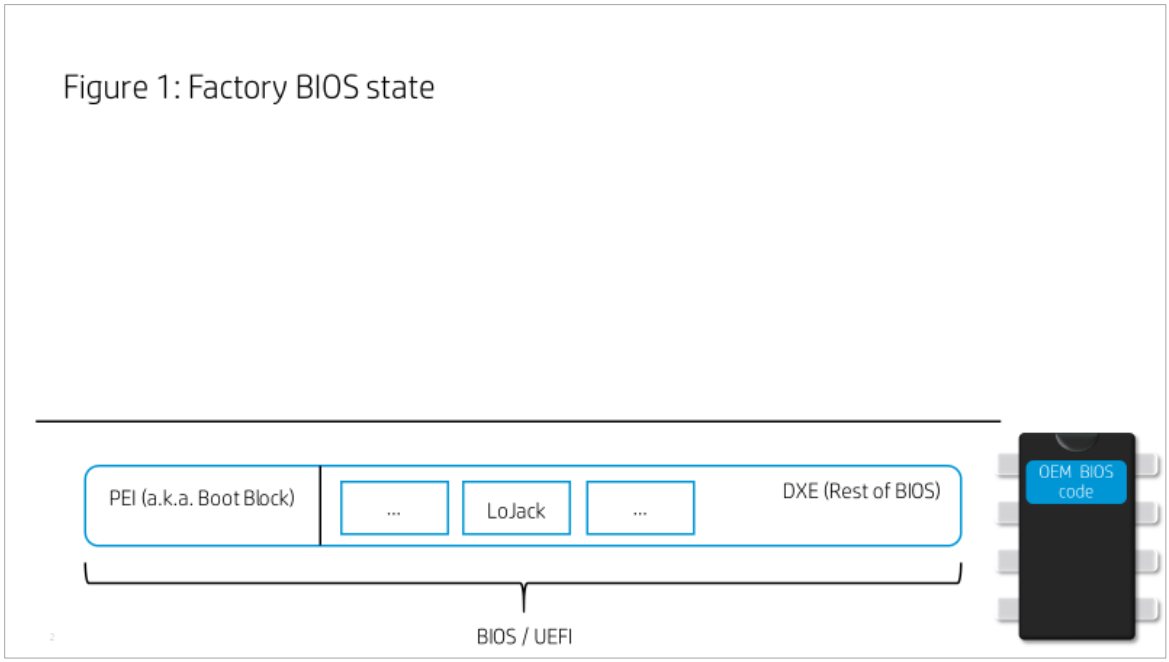
[1] Defense in Depth is a cybersecurity strategy that layers defensive mechanisms for protection of device, identity, and data. If one protection mechanism fails, there are redundancies that can still help provide protection. A layered approach provides a strong security posture for the system against varied attack vectors.

LoJax UEFI Rootkit Overview

Technology overview of the LoJax attack

HP researchers studied the binary code of the exploit described in the ESET report. There are two logical set of components that make up this attack:

1. The set of binaries that are implanted in the UEFI for persistence and to compromise the system at a later stage (this is the "payload").
2. The actual malware that runs in Microsoft Windows to deliver the payload, which consists of tools that read the existing UEFI binary in the system, modify it by adding the malicious payload, and inject the "modified" UEFI binary back in the system.

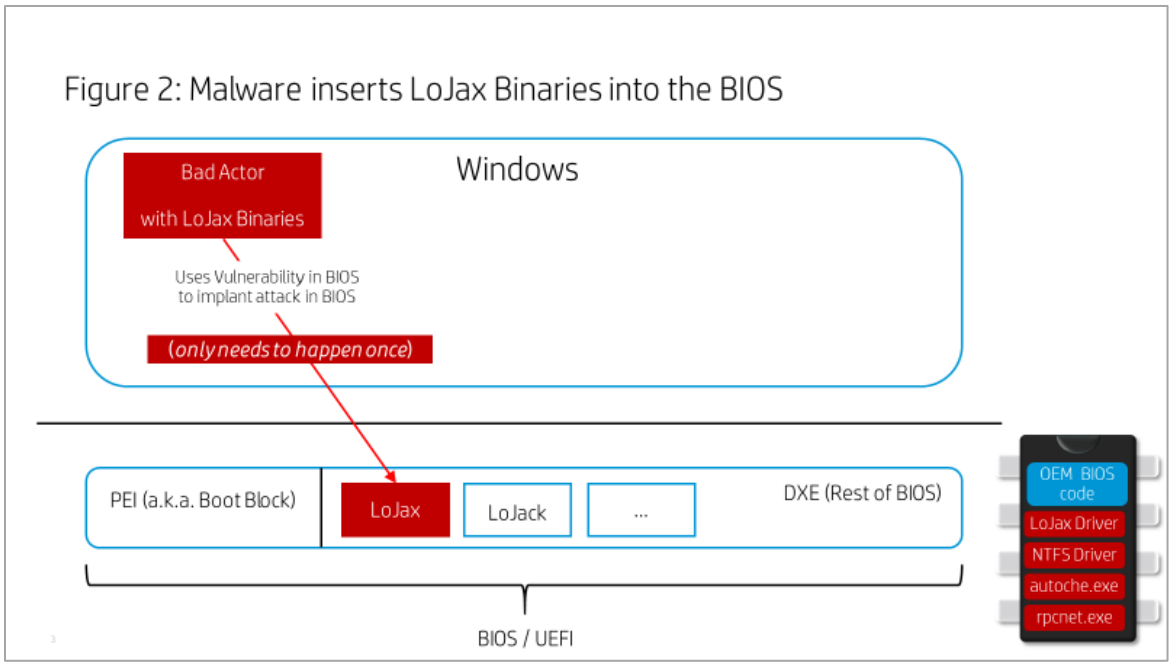


While the exact scheme by which the malware originally gets on the PC is not publicly known, we can hypothesize that usage of common attack vectors, such as phishing or malicious documents, may have led to the original attack.

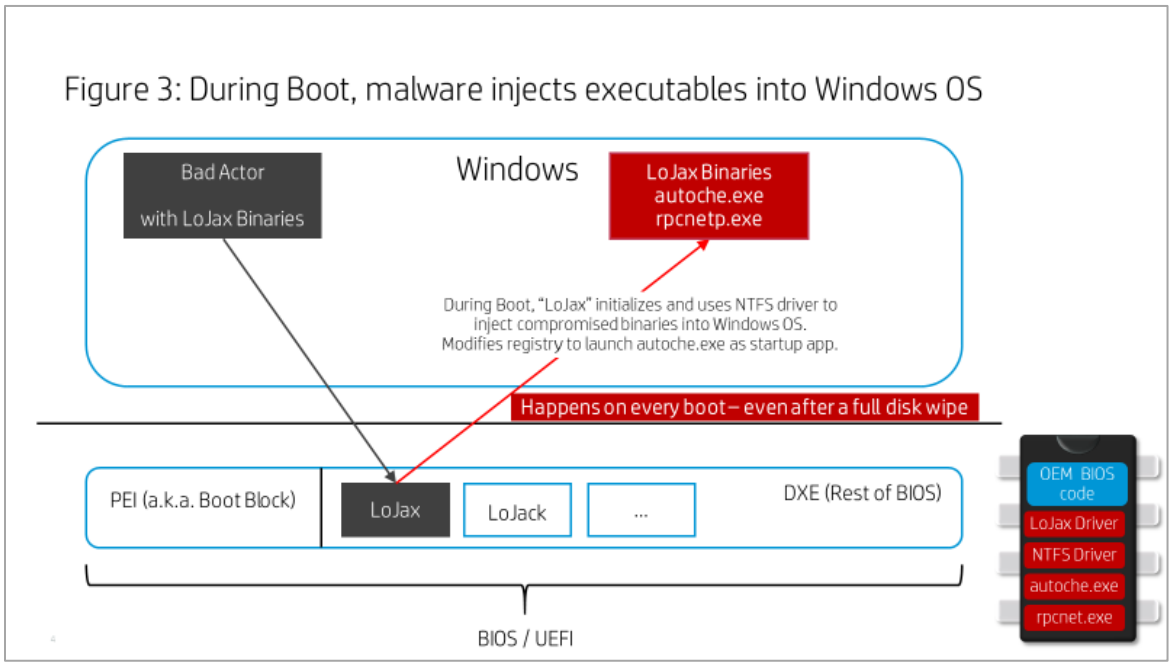
Once this malware lands on a PC, it needs to run with administrative privileges. This is required in order to allow the malware to use a particular kernel mode driver for reading and writing the UEFI image (RwDrv.sys). This driver is part of a free tool available on the internet, called 'Read Write Everything', which is used for legitimate purposes, such as reading and writing low level system settings. Therefore, this driver is properly signed and is not detected as malicious by the operating system. Once it runs, the malware determines if the current system has the UEFI firmware protections properly configured or not. If they are properly configured, the malware will then determine if the system is unpatched against a previously disclosed vulnerability that can be exploited to overwrite UEFI - regardless of whether the firmware protections are properly configured (see: https://www.kb.cert.org/vuls/id/766164). This vulnerability was disclosed in 2015, which means that it is possible that both newer systems and the older pre-2008 systems were both targets of the attack.

If the UEFI image can be overwritten using either of the two mechanisms described above, the malware then extracts the existing UEFI image, modifies it by adding the malicious UEFI binaries, and then writes the modified UEFI image back into the flash memory area used to store the UEFI firmware. More specifically, the payload consists of four components: the LoJax driver to maintain persistence, a modified NTFS driver that provides disk write support, and two additional files which are inserted into the Windows operating system at a later stage.

LoJax UEFI Rootkit Overview



Once the malware binaries are embedded in the UEFI firmware, they are ready to execute the next time the PC boots. During early boot cycles, the malicious LoJax driver is run. It establishes a callback such that when Windows starts to load, the LoJax driver in UEFI is executed again. When that happens, the LoJax driver in-turn uses the newly inserted NTFS driver in UEFI and writes two files into the Windows NTFS partition: (1) autoche.exe and (2) rpcnetp.exe. Autoche.exe is designed to look very similar to autochk.exe, which is part of the Microsoft Windows operating system. Likewise, rpcnetp.exe has the same filename as the genuine Absolute Software LoJack service, except that this specific file has been modified to communicate with the attacker's command and control servers over the internet. This usage of filenames similar to LoJack is the reason why this malware is called LoJax.

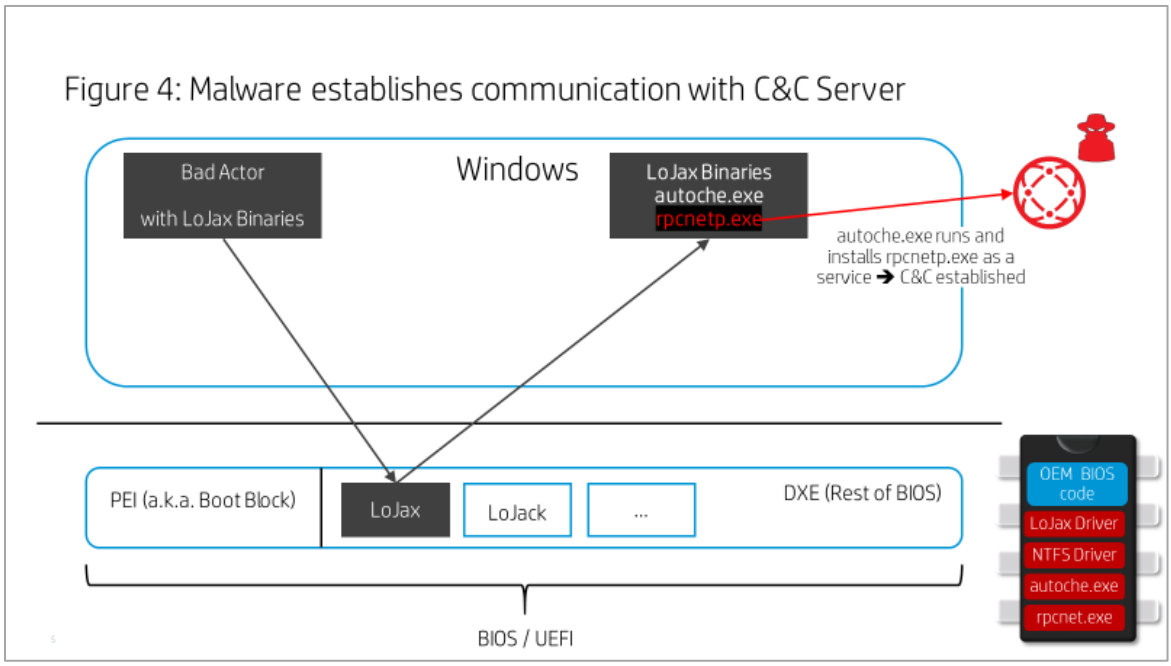


After installing these two files on the disk, the LoJax driver also makes a modification to the registry to automatically run autoche.exe, instead of autochk.exe on every boot. The one letter difference between the two file names (autoch**e**.exe vs. autoch**k**.exe) can be difficult to detect by a person visually inspecting the registry.

LoJax UEFI Rootkit Overview

NOTE: While analyzing this operational flow, as stated in the ESET report, HP engineers concluded that if any full disk encryption utility such as Microsoft Bitlocker had been enabled, the insertion of these files and the modification of the registry would have failed. A later revision of the ESET report confirmed HP's finding in this regard. However, it is important to understand that a future permutation or evolution of this attack could potentially avoid the Bitlocker restriction.

Continuing with the regular boot sequence, Windows will eventually run the autoche.exe binary. This binary then performs two actions: It first installs the malicious rpcnetp.exe as a Windows service, using the same settings as the genuine Absolute Software LoJack agent; next it reverts the registry entry back to point to the original autochk.exe, to hide the presence of the malware during boot. During a later stage of boot, Windows will start the newly inserted but malicious rpcnetp.exe as a Windows service, allowing it to gain elevated system privileges. (Note again that this malicious rpcnetp.exe has been modified to point to the attacker's command and control servers.) This malicious service now acts as a trojan that can be used to download any malicious code, as directed by the bad actors behind the command and control servers.



At this stage, because the UEFI firmware has been compromised, this attack sequence will be repeated during every system boot, giving the malware complete persistence - even if the PC's hard drive is wiped and Microsoft Windows is reinstalled. To remove the malicious code, the UEFI would need to be re-flashed with genuine code from the PC manufacturer, along with a wipe of the disk and reinstallation of Microsoft Windows OS. It is important to note that while the current instance of LoJax malware does not resist firmware update, there is research showing that malware located in UEFI firmware could be engineered to survive or reject firmware updates. This possibility of stealth and persistence makes this type of a rootkit a SIGNIFICANT concern.

While HP Sure Start systems don't have the vulnerability necessary for the LoJax UEFI exploit, HP engineers wanted to test how HP Sure Start would behave if an attacker was able to infect the system flash. To run the experiment, the flash chip had to be physically removed from the system board, infected with LoJax using an external flash programmer, and then reinstalled back on the system board. When power was next applied to the system, as expected, the exploit was automatically detected by HP Sure Start before it was executed, and the UEFI was recovered to its original state. This confirms that HP Sure Start is resilient against the LoJax attack, even if the attacker was able to find a way to somehow deploy the LoJax UEFI rootkit. We also verified that there was a corresponding event added to the HP Sure Start Event Log, leaving behind a record of the attack and subsequent remediation by HP Sure Start. This record of the attack is important to cybersecurity analysts.

LoJax UEFI Rootkit Overview

Myth: LoJax affects older systems, why should I be concerned?

While ESET found this attack to be successful on pre-2008 systems, the same report makes it clear that any system that does not implement proper UEFI firmware protections or that has not been patched against the previously noted vulnerability discovered in early 2015 is also vulnerable to this attack. This could very well mean that some currently shipping systems across the industry may be potentially vulnerable. Furthermore, the updated ESET report also clarifies that security researchers have been demonstrating exploits and proof of concepts of UEFI attacks of this type at industry forums and in academic papers for years, showing that UEFI rootkits were possible. In fact, there was already a previously found BIOS rootkit attack found in the real world. Mebromi (https://www.webroot.com/blog/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/) was a BIOS rootkit that attempted to implant an MBR rootkit, a kernel mode rootkit, a PE file infector and a Trojan downloader. The discovery of another attack in the wild is a very concerning breakthrough for the whole industry and unfortunately a new stage in the evolution of attack sophistication, as attackers may be emboldened by this news and may attempt to create variants of LoJax. Combined with any new UEFI vulnerability that may be discovered, this could lead to persistent UEFI infection of modern PCs. HP has been raising industry awareness on this issue in and advising customers of the dangers of these types of attacks for years. HP continues to invest in research and innovation to provide and improve advanced solutions like HP Sure Start to combat these types of attacks.

Who is protected?

PCs with properly configured firmware protections and with UEFI patched against the previously known vulnerability (**https://www.kb.cert.org/vuls/id/766164**) will prevent this version of LoJax. However, in today's threat landscape, it is prudent to use layers of protection in case attackers find alternative means to get through your defenses. For that very reason, HP Sure Start systems deploy an additional layer (Defense in Depth) that protects your HP systems even in the event that a new zero-day vulnerability is found in UEFI, or if the attacker uses a physical attack to manually implant malware in the firmware flash memory. HP Sure Start will not only detect any such change to the UEFI code, but will also self-heal the UEFI using a cryptographically signed private copy from secure storage isolated and out of the reach of malware running on the host. This ensures that a PC protected by HP Sure Start will always boot with an authentic version of the UEFI. HP Sure Start Gen3 and Gen4 go even further and protect the UEFI copied into and executed from memory (SMM) after the operating system loads, providing critical runtime intrusion detection security. Furthermore, HP Sure Start also extends this hardened level of resiliency to protect and recover critical UEFI settings such as Secure Boot enablement, power on password, BIOS configuration administrative password, and other settings. No other modern PC system can claim this level of resiliency against software or hardware attacks targeted at BIOS/UEFI and critical UEFI configuration settings.

It is important to also note that properly "configured and patched" UEFI implementations could indeed protect systems without HP Sure Start from this specific attack. Using the open source CHIPSEC tool provides a strong assessment of the firmware protections relative to the known vulnerabilities. However, HP Sure Start adds additional layers of protection, advanced detection, and repair techniques that prepare you for more sophisticated attacks and goes further to defend you and your organization.

A legacy of BIOS Security

HP has been pioneering firmware security for over a decade. HP recognized the need for firmware security early and worked with HP Labs toward solving the problem. As far back as 2005, HP introduced the first cryptographically secure UEFI updates for PCs. HP then continued to add support for protecting the BIOS from being overwritten by malicious software over the next several years.

In 2011, recognizing the increasing risks of unauthorized modification of BIOS by malicious software, NIST published **Special Publication 800-147** - a specification that formally documents guidelines for protecting and securely updating PC BIOS. This eventually became **ISO standard 19678** in 2015.

As HP continued to study the evolution of the threat landscape, we realized the need to continue to raise the bar in PC security with a new design for firmware cyber-resilience, anchored into the hardware. This is when HP's PC group and HP Labs invented and developed HP Sure Start, introduced in 2014. HP Sure Start is now in its 4th generation on HP Elite series PCs, with HP Pro 600 series PCs being added in 2018. HP Sure Start Gen4 and prior generations, along with HP BIOSphere Gen4 (and its prior generations), meet and exceed requirements stated in NIST SP 800-147. HP Sure Start has also been adapted to HP Enterprise printer architectures since 2015 and is available in HP Enterprise Laser Jet Products (http://h20195.www2.hp.com/v2/getpdf.aspx/4AA6-4194ENW.pdf).

In 2014, NIST also released a draft specification called **Special Publication 800-155**. This draft includes guidelines to establish a secure BIOS integrity measurement and reporting chain. HP Sure Start Gen4 and prior generations of HP Sure Start, along with HP BIOSphere Gen4 and prior generations of HP BIOSphere, all support NIST SP 800-155.

NIST Special Publication 800-193: Platform Firmware Resiliency Guidelines

Moving beyond the "protection only" approach of NIST SP 800-147, NIST released the **SP 800-193 Platform Firmware Resiliency Guidelines** in May of 2018 which guides designers to build mechanisms to detect and repair tampering with both code and critical data in the event the mechanism protecting those elements are bypassed. HP Sure Start meets and exceeds the NIST SP 800-193 requirement for the HP UEFI since HP Sure Start Gen3 was released in 2017 products.

These guidelines outline three different levels:

1. Protected: meets all Protection and Secure Update requirements
2. Recoverable: meets all Detection and Recovery requirements
3. Resilient: meets all Protection, Detection, and Recovery requirements

Of these three levels, "Resilient" is the strongest level, providing the most benefit to HP Customers. As stated earlier:
HP Sure Start Gen3 and Gen4 meets and exceeds all Resilient guidelines in NIST SP 800-193 for host processor boot firmware, also known as the BIOS or UEFI.

BIOS protection for HP Commercial Printers

HP's legacy in BIOS security doesn't just apply to PCs. HP introduced HP Sure Start to protect and heal the BIOS for HP Commercial Printers in 2015.

Conclusion

After years of research demonstrating that BIOS or UEFI rootkit attacks were possible, we've seen a UEFI rootkit used in a real-world attack. In anticipation of this and other types of threats, HP introduced HP Sure Start in 2014 and has continued to advance its anti-rootkit protections for four generations, providing critical protection against what may become an increasingly common and dangerous attack vector.

Learn more:
hp.com/go/computersecurity

HP Sure Start Gen4 technical white paper:
http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-2197ENW

HP Sure Start Gen4 info sheet:
http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-2562ENW

4AA7-4019ENW

October 2018