The LoJax Attack: What You Need to Know

By Vali Ali - HP Fellow and Chief Technologist, Personal Systems, HP Inc.

November 8, 2018

After years of research demonstrating that potentially dangerous BIOS/UEFI rootkit attacks were possible, we've recently seen such an attack used in a real-world scenario. At the 2018 Microsoft BlueHat conference, researchers from ESET presented their analysis of this new malware. The malware, named LoJax, was allegedly used by a cyber espionage hacker group popularly known as Fancy Bear (a.k.a. APT 28). Fancy Bear allegedly utilized LoJax against several high-profile targets in Central and Eastern Europe.

BIOS/UEFI Rootkit attacks have long been a concern because they can be difficult to detect, are extremely difficult and costly to remove, and can grant hackers near-total control of the infected PC, including access to corporate networks. In anticipation of this and other such threats, HP made significant investments in BIOS/UEFI security to introduce HP Sure Start for its Commercial PC line in 2014 and has continued to advance its anti-BIOS/UEFI rootkit protections for four generations.

The current LoJax attack is not applicable to PCs that properly lock the BIOS/UEFI and are running the most recent, fully patched version of the BIOS/ UEFI. However, with the discovery of LoJax, we must assume that additional variants are likely to surface which are more sophisticated than the first – i.e., attacks which are more difficult to detect or prevent, or that can target an additional set of vulnerabilities not previously disclosed.

HP Sure Start provides an extra layer of defense that protects against both software-based and physical attacks intended to modify the BIOS/UEFI. **HP Sure Start protects against LoJax and potential future variants of LoJax** that attempt to change BIOS/UEFI code and critical configuration policies, using HP's Endpoint Security Controller, a unique hardware element that also drives solutions like HP Sure Run and HP Sure Recover.

It is important to remember that anti-virus software and other third-party software solutions are insufficient to protect the BIOS/UEFI from these types of attacks. Hardware-enforced security is required, and the only entity that can reliably protect the BIOS/UEFI is the PC hardware provider. HP continues to encourage companies to actively consider hardware and firmware security in their PC purchase discussions and to initiate conversations with their HW vendors. To protect your organization and users, every PC you purchase is a security decision.

Additional technical details are available via HP's whitepaper which can be found here.

Source: https://press.hp.com/us/en/blogs/2018/the-lojax-attack--what-you-need-to-know.html