Cyber Criminals Use Processor Vulnerabilities to Spread Malware

Once security issues go global, cyber criminals tend to exploit them for their own gain. It happened with the global ransomware treats, NotPetya, BadRabbit and WannaCry. Hackers used fraudulent decryption keys to spread malware. Now, they're using malicious Meltdown/Spectre "patches" to spread malware. According to Tech Republic, the malicious patches have been targeting Germany; however, it won't be long until they're spread globally.

The malicious patch is being sent via phishing scams, claiming that the installation of the patch is critical. Within the email, users are asked to go to a certain website to download the patch. Interesting enough, the website they're asked to go to is an https:// page. Often users believe clicking on https:// links are safe because the "s" stands for secure. Although, the data transmitting from the computer to the website is secure, it does not mean the content within the page is safe and not malicious.

Avoid scams such as these by keeping two things in mind. First, valid security patches will not be distributed to users individually. Secondly, any email or website that is urging users to implement patches or updates are signs of red flags. Instead patches will be launched within an automatic update. Unless of course the user has opted out of automatic updates, in which case the patch will launch at the time the software update is manually launched, which can be done through the Settings feature within the operating systems.

What are Spectre and Meltdown?

Spectre and Meltdown are computer chip vulnerabilities present in virtually all computer processors manufactured in the past 10 years. The vulnerabilities could potentially be exploited by malicious actors to bypass data access protections and obtain sensitive data, including passwords and protected health information.

Meltdown is an attack that exploits a hardware vulnerability (CVE-2017-5754) by tricking the CPU into speculatively loading data marked as unreadable or "privileged," allowing side-channel exfiltration. Spectre is an attack involving two vulnerabilities (CVE-2017- 5753, CVE-2017-5715) in the speculative execution features of CPUs. The first vulnerability is exploited to trick the CPU into mispredicting a branch of code of the attacker's choosing, with the second used to trick the CPU into speculatively loading the memory allocated to another application on the system. The Meltdown and Spectre chip vulnerabilities can be exploited to gain access to sensitive data, including passwords, cryptographic keys used to protect PII, PHI, or PCI information handled by an application's database.

Meltdown and Spectre affect computers running on Windows, Mac, Linux and other operating systems. Eradicating the vulnerabilities means replacing chips on all vulnerable devices; however, operating system vendors have been developing patches that will prevent the vulnerabilities from being exploited. Updates have also been made to web browsers to prevent web-based exploitation of the vulnerabilities.

Following the disclosure of the vulnerabilities, HCCIC alerted healthcare organizations about the risk of attack, with the vulnerabilities categorized as a medium threat since local access is generally required to exploit the flaws. However, potentially the flaws can be exploited remotely if users visit a specially

crafted website. Browsers are susceptible due to improper checks on JavaScript code, which could lead to information disclosure of browser data.

Mitigating the Threat of Spectre and Meltdown Attacks

Patching operating systems and browsers will mitigate the vulnerabilities, but there may be a cost. The patches can affect system performance, slowing computers by 5-30%. Such a reduction would be noticeable when running high demand computer applications.

There have also been several compatibility issues with anti-virus software and other programs. It is therefore essential for patches to be thoroughly tested before implementation, especially on high value assets and systems containing PII and PHI.

Due to the compatibility issues, Microsoft is only releasing updates for computers that are running anti-virus software that has been confirmed as compatible with the patch. If anti-virus software is not updated, computers will remain vulnerable as the update will not take place. Most anti-virus software companies have now updated their programs, but not all. Kevin Beaumont is maintaining a list of the patch status of AV software.

Web browsers must also be updated to the latest versions. Microsoft has updated Internet Explorer 11 and Microsoft Edge, and Firefox (57.0.4) and Safari (11.0.2) include the update. Google Chrome has also been patched. Healthcare organizations should ensure they are running the latest versions of browsers on all devices to prevent data leakage and operating systems should be patches as soon as possible. One of the main challenges for healthcare organizations is identifying all vulnerable devices – including computers, medical devices and accessory medical equipment – and ensuring they are fully patched.

The vulnerabilities also affect cloud service providers, as their servers also contain computer chips. There could be leakage of PII and PHI from cloud environments if patches have not been applied.

Amazon AWS and Azure have already been patched to protect against Meltdown and Spectre. Healthcare organizations using other managed cloud service providers or private cloud instances should check that they have been patched and are protected against Meltdown and Spectre.