Issued 1/16/18

Windows Users Targeted by Fake Meltdown and Spectre Update

Windows users are currently being targeted by a fake Meltdown and Spectre update that deploys malware on a vulnerable host and has the capability to download additional payloads. Security company Malwarebytes warns that the fake patch is mostly aimed at German users, but it can easily be modified into English. Spreading as an exe file called Intel-AMD-SecurityPatch-10-1-v1, the fake Meltdown and Spectre update deploys Smoke Loader on a compromised host. Smoke Loader is a form of malware that opens the door to more payloads which can be then used for a variety of purposes, including stealing credentials and other sensitive data. Once it infects a PC, the malware attempts to connect to several Russian domains and sends encrypted information, the security company explains. “We identified a recently registered domain that is offering an information page with various links to external resources about Meltdown and Spectre and how it affects processors. While it appears to come from the German Federal Office for Information Security (BSI), this SSL-enabled phishing site is not affiliated with any legitimate or official government entity,” Malwarebytes says. Links to the website hosting the malicious patch are typically spreading using classic methods like email and messaging, and users are recommended to avoid downloading security patches from other sources than the official ones. Microsoft has already released Meltdown and Spectre updates and they are available on Windows Update or right on the company’s Update Catalog for manual downloads.