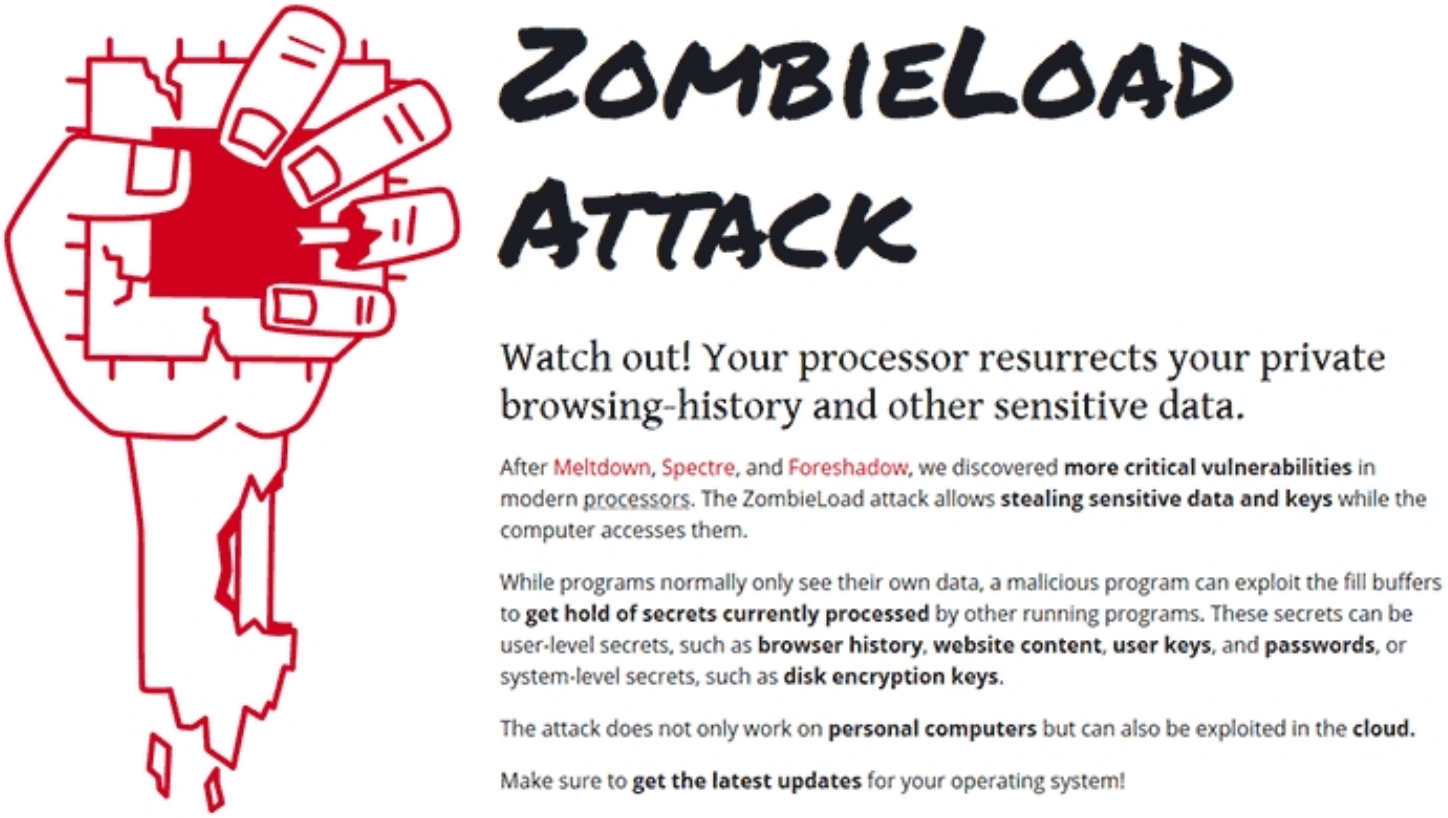
Written by Alice Marshall
15 May 2019

Researchers warn the undead are making their way towards your customers' PCs-- or rather a set of critical vulnerabilities lurking within Intel processors allowing for the colourfully dubbed "ZombieLoad" attack.



Discovered by security researchers from Graz University of Technology, the ZombieLoad vulnerabilities affect all Intel chips dating back to 2011. The attack is similar to the Meltdown and Spectre flaws. Also known as Microarchitectural Data Sampling (MDS), ZombieLoad allows for the leaking of sensitive data, such as passwords, secret keys, account tokens and private messages, stored in a processor. It is a side-channel attack, since it allows hackers to exploit design flaws without need to inject malicious code, and consists of 4 bugs first reported to Intel just a month ago.

The name ZombieLoad comes from a "zombie load," an amount of data the process cannot understand or process. This causes the processor to leak any data currently loaded in the processor core. The researchers provide a proof-of-concept video showing how attackers can

exploit the bugs to check what websites a person is visiting in real-time, and say it can easily allow the stealing of passwords or access tokens.

In turn, Chipzilla says the two most recent generations of Core processors, as well as "some" server chips, already prevent the attack at a hardware level. Everything else requires software updates. Intel already has microcode to patch vulnerable processors, including Xeon, Broadwell, Sandy Bridge, Skylake, Haswell, Kaby Lake, Coffee Lake, Whiskey Lake, Cascade Lake, Atom and Knights. Also releasing patches are Microsoft and Apple, together with Google.

Intel warns the patches might affect the performance of consumer devices by around 3% at worse, while datacentres can take a hit of up to 9%.

Go ZombieLoad Attack

Go Intel Side Channel Vulnerability