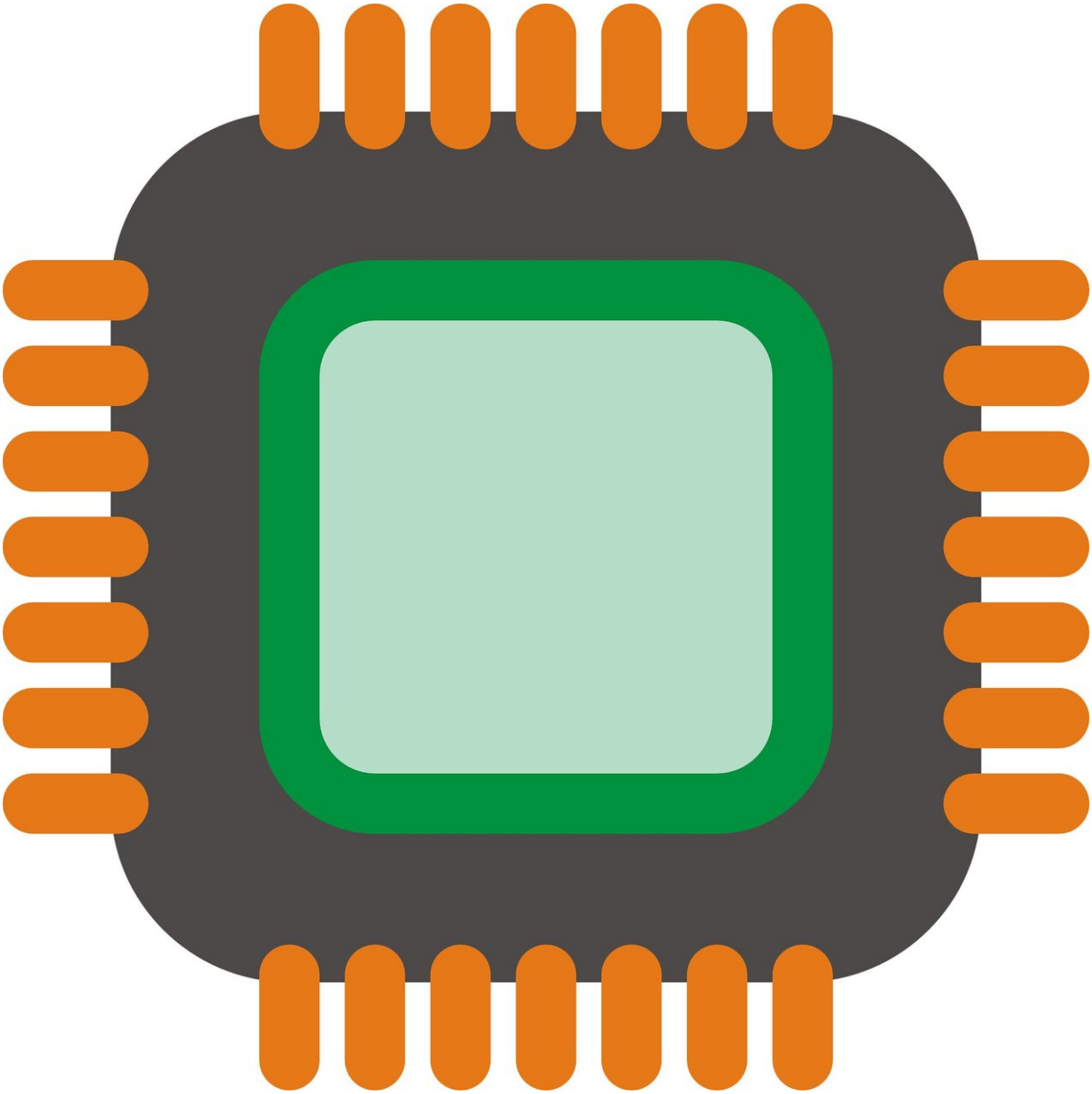
Intel Tiger Lake to have built-in malware defense

June 16 2020, by Peter Grad



Credit: CC0 Public Domain

Intel Corporation announced Monday that its forthcoming Tiger Lake processors will pack a defense mechanism against Spectre-type malware attacks.

Spectre vulnerabilities allowed hackers to break into systems using Intel processors manufactured over two decades and steal passwords, personal photos, emails and other sensitive data stored in the memory of other running programs.

Such control-flow hijacking attacks have always been difficult to mitigate through software programs. Intel's new Control-Flow Enforcement Technology (Intel CET) will install CPU-level defense mechanisms to combat such assaults.

Tom Garrison, vice president of the Client Computing Group and general manager of Security Strategies and Initiatives at Intel Corporation, cited statistics provided by TrendMicro's Zero Day Initiative (ZDI) to underscore the importance of a fortified defense against control-flow threats.

"Sixty-three percent of the 1,097 vulnerabilities disclosed by ZDI from 2019 to today were memory safety related," Garrison said in an online post Monday. "These malware types target operating systems, browsers, readers and many other applications. It takes deep hardware integration at the foundation to deliver effective security features with minimal performance impact."

Intel said the new CPU-based mechanism will offer software developers two approaches to defend against hijacking programs.

Indirect branch tracking provides protection against jump and call-oriented programming attacks. Those attacks exploit memory vulnerabilities by causing stack overflow corruption and employing use-after-free assaults that attempt to access free memory and cause systems to crash.

Shadow stack tracking offers return address protection by copying a program's expected execution flow to compare against actual flow and prevent unauthorized return-oriented-programming attacks.

Intel is expected to release its latest generation of processors later this year in laptops under the Intel Core brand. Tiger Lake is based on the third-generation 10 nm manufacturing process and will replace the Ice Lake processor. It will be available for desktop and server platforms shortly after.

Microsoft has been working with Intel to integrate CET protection in Windows 10. In Windows it will be called Hardware-enforced Stack Protection.

According to Baiju Patel, an Intel Fellow with the Client Computing Group, "Intel has been actively collaborating with Microsoft and other industry partners to address control-flow hijacking by using Intel's CET technology to augment the previous software-only control-flow integrity solutions."

"Intel's CET, when used properly by software," he said, "is a big step in helping to prevent exploits from hijacking the control-flow transfer instructions."

Intel first published CET specifications in 2016, allowing manufacturers time to incorporate necessary changes to accommodate the first Tiger Lake units.

More information: www.businesswire.com/news/home … Answers-Call-Protect