Spectre & Meltdown

Every so often there is a pivotal event that causes incredible changes to an industry. The Spectre/Meltdown vulnerability is such an event to the tech industry. The vulnerability was discovered in August of 2017 with the public's notification on January 2, 2018. Every device with a processor in the world is affected to some degree. Yes, even late model cars. This time next year there will be articles analyzing the cost and impact of this vulnerability.

The interesting thing is this is all precautionary. There are no known exploits in the wild as of today, January 15, 2018. However, people who have studied this for the last 5 months tell us that any exploits that do occur will be extremely difficult to remediate. So everyone is taking this seriously.

SOCSoter is a cybersecurity company specializing in working with Managed Service Providers. They released the following:

"Recent announcements of a new vulnerability called meltdown and spectre are spreading. SOCSoter would like to give a quick reference and overview of this emerging threat. First, these issues are related to a vulnerability, as such there needs to be exploit code (malware) that delivers the software capable of taking advantage of the vulnerability on the target system. If the target system successfully executes code that takes advantage of the vulnerability then a malicious application will be able to read data from memory and other running programs including passwords stored in browsers. This vulnerability works on laptops, desktops, mobile devices and cloud infrastructure.

It is our opinion that if an attacker can get a target system to execute code then exploiting these vulnerabilities would be a waste of time, since there are other easier methods of stealing data. These specific exploits may prove to be effective in escalating privilege but only as a secondary attack in already executed malware. Typically, we will always advocate patching as soon as possible but in this case MSP's need to understand that patching could degrade performance. Patches for these vulnerabilities are designed to remove optimized code running at the kernel level that actually helps boost processing speeds of chips. Please test any patches to ensure that there will be no business impact, and performance related to processing speed will not be reduced.

SOCSoter Cyberdefense and Advance Threat Detection services have been updated to detect indicators associated with attacks that may carry these exploits.

Meltdown: breaks isolation between user applications and the operating system
Spectre: breaks isolation between applications "

How is going to affect you?

It really doesn't affect you like it does the "big boys"; Google, Microsoft and Amazon, but the threat is there. The manufacturers of processors and operating systems are taking this vulnerability very seriously. Because the manufacturers of the processors and operating systems are taking this seriously, it pushes responsibilities to the manufacturers of the devices that use the processors, to get the updates out. Every device with a processor will have to have firmware and/or software updates. Every PC, Server, notebook, Tablet, Smart Phone, any device with a processor. That means Dell, Lenovo, HP, Acer, etc. must co-ordinate getting BIOS updates for all the devices that they have made for the last 15 or so years. In most cases the Firmware/BIOS will have to be updated before the software can be patched, so it's a good idea to turn off automatic updates until you know.

Ellegent is dedicated to providing our customers with the best, most responsive support, but this is a staggering task. We have already met our contractual obligations with customers under contract. If you are an Ellegent customer and on BlockTime or hourly **and** on our SystemPulse Management System, we will be analyzing your hardware and checking to see if BIOS updates are out. IF they are, we will be contacting you to do updates.

Patch management and BIOS updates are two different processes, but can be done in sequence or we can do BIOS updates and do patches later. The labor cost of doing software patch updates manually, per machine can be between

$25, $50, $100 or more, depending on how many patches haven't been done. Ellegent Systems has a patch management system associated with our SystemPulse Management System and may save you money in this situation, and in the long run. Our Patch Management system costs $3 per machine per month with a one year commitment, but it requires the machine being on Professional Monitor instead of the free, Essential monitoring. Basic Professional Monitoring starts at $10 per month, so if your equipment is on Essential monitoring or no monitoring with us, the cost per month, per machine would be $13. We can do it month-to-month, but that will require a $50 initial setup fee per machine.

If you would like to discuss any of this give Kevin or Dave a call at 618-624-1138