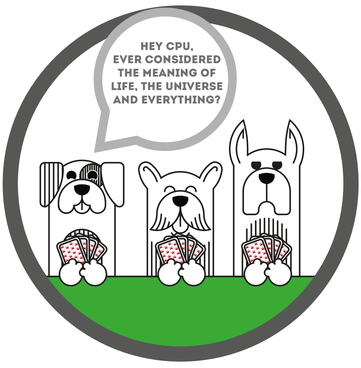
What is the **Spectre** bug?

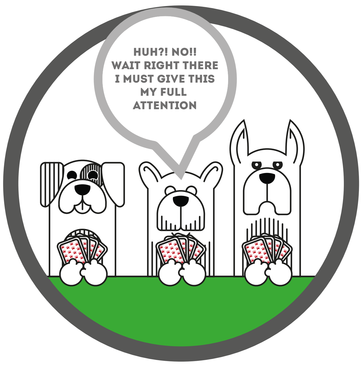
The Spectre bug works in a very similar way to the **Meltdown bug** in method, using cached data from the CPU to get what it wants by exploiting branch prediction and **speculative execution**. This dastardly devil doesn't try and look into the depths of your computer but will try and look at your other programs to get personal information. For example, if a malicious attack came from an internet advert it could attempt to read other browser tabs and windows from cached data, capturing all sorts of personal information.

Spectre affects Intel, Apple, ARM and AMD processors.

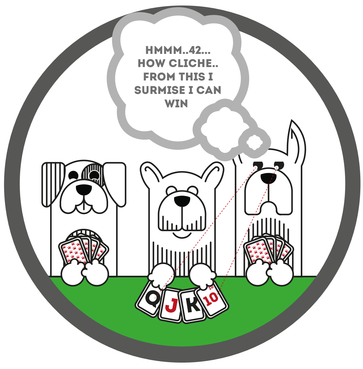
Spectre is a sneaky foe, one way to describe it is like a game of cards.



A program will trick the processor into thinking hard about one thing in particular.



The CPU is thinking so hard that other important data from other running programs (that usually wouldn't be exposed) moves to cached memory.



While this data is unprotected, malicious software maybe able to read this data. This could be details from another running program or an open browser tab.

Another way of looking at this is, that by bombarding the CPU, it gets really busy but is still thinking speculatively. With the heavy volume of requests coming in, the solutions that the CPU is lining up speculatively that are incorrect, go to a cache. While cached, this information could be open to interrogation from malicious sources via a side channel.

Help is at hand

Patches are available to fix your devices, visit:
https://xtravirt.com/cybersecurity/#spectre-meltdown
to see the latest news and trusted patches for Meltdown and Spectre

What is the **Meltdown** bug?

5 things you should know about **Speculative Execution**