This is a side project I've been looking at. Not a particular news story but one that may develop over time. I quote Wiki for this one, even though I don't trust them.

So, the world has now (more or less) patched all Intel and AMD computer systems, including other types of machines, against the Spectre.

https://support.microsoft.com/en-gb/help/4073757/protect-your-windows-devices-against-spectre-meltdown

But was there a reason behind this, and I don't mean some kid in his bedroom wanting to use all the pc's on the web to break into the CIA etc.?

Firstly, there are the 'Russian attacks', which a lot of people feel are false flags, but like I've said before, that's not the purpose of this site, but I may find things that are related, and may be useful.

The main thing in the news for the past years of 2017 onwards (especially since Donald Trump took office), is that Russia will attack us. Not boots on the ground etc., but electronically.

Yes, there was the Salisbury attack, but I'm not looking at that. I'm looking at something that may happen in the future.

Take Kaspersky. The antivirus that we all have used before is deemed to be spying on the US, so they have banned it from government computers. Facebook is banning it from their suggestions.

Now, take all the news articles on Mainstream Media, and over time, if you hear something and read about it for so long, you'll start to believe it. It's just basic psychology.

So, we have been told that they will attack. And in some of the latest, they say that thousands and thousands and thousands will die. But not by boots on the ground, but by damaging the infrastructure. Just think of the film Die Hard 4, and in it they create a fire sale. It's basically the same thing. I wonder if that film (or similar) will be shown a few months before the actual event happens?

My theory then goes to the latest patches. Spectre was observed a few years back, but not patched. Why? Well, back then when not everyone had computers, the internet wasn't like it is now, etc. it would have been pointless. But not in the modern 'we all need to be on' times.

Just reading the article in Wiki, and interesting enough, this was written:

https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)

"Spectre was discovered independently by Jann Horn from Google's Project Zero and Paul Kocher in collaboration with Daniel Genkin, Mike Hamburg, Moritz Lipp and Yuval Yarom."

Strange that it's Google once again that rears its ugly head. And remember, even those that were in 2014, Russia wasn't on the radar in the news or in peoples subconscious. So, that is why it never came to fruition, in my eyes.

So, look to this scenario. In a year or so, when the seeds are sown in peoples mind, all the computer systems are patched (remember, some are corporate so need to be tested on certain systems), then all of a sudden, an attack is made on the computers in the UK. Not your home ones, nope. But any system that is in hospitals, nuclear power stations, water treatment plants etc.

Those going down will cause the massive deaths. And who will everyone think has caused it? Russia, of course.

--

Now the Google issue was apparently just recently, but according to Wiki, the use of crypto analysis on chipsets was discovered as far back as 2002. Now of course, the details that have emerged may have been found earlier, but the powers that be won't say that.

Reading up on the exploit:

"The Spectre paper displays the attack in four essential steps:

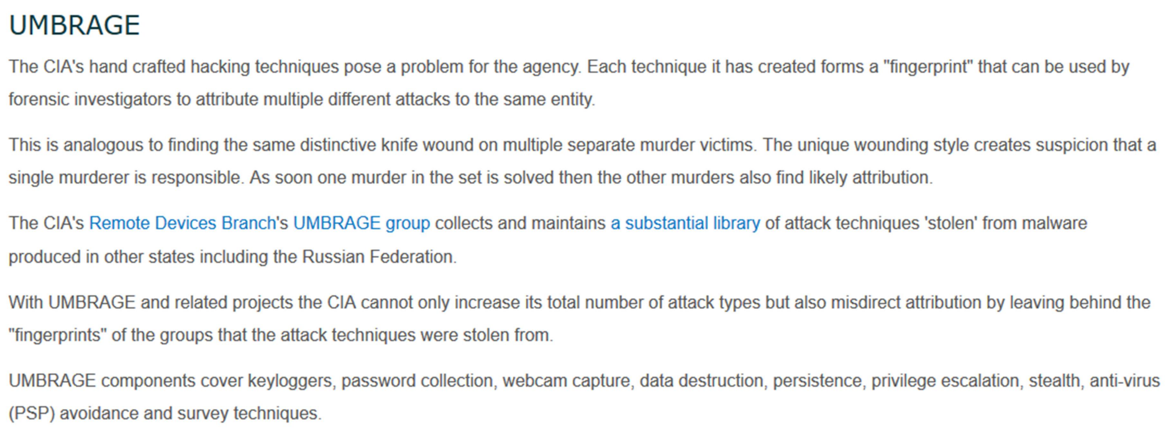
First, it shows that branch prediction logic in modern processors can be trained to reliably hit or miss based on the internal workings of a malicious program.

It then goes on to show that the subsequent difference between cache hits and misses can be reliably timed, so that what should have been a simple non-functional difference can in fact be subverted into a covert channel which extracts information from an unrelated process's inner workings.

Thirdly, the paper synthesizes the results with return-oriented programming exploits and other principles with a simple example program and a JavaScript snippet run under a sandboxing browser; in both cases, the entire address space of the victim process (i.e. the contents of a running program) is shown to be readable by simply exploiting speculative execution of conditional branches in code generated by a stock compiler or the JavaScript machinery present in an extant browser. The basic idea is to search existing code for places where speculation touches upon otherwise inaccessible data, manipulate the processor into a state where speculative execution has to touch that data, and then time the side effect of the processor being faster, if its by-now-prepared prefetch machinery indeed did load a cache line.

Finally, the paper concludes by generalizing the attack to any non-functional state of the victim process. It briefly discusses even such highly non-obvious non-functional effects as bus arbitration latency."

Strangely enough, the first part about a malicious program being used. WikiLeaks recently released loads of tools/exploits etc. that were 'stolen' from the NSA/CIA. Strangely enough, one of those tools was called Umbrage. Here is a brief overview:



UMBRAGE

The CIA's hand crafted hacking techniques pose a problem for the agency. Each technique it has created forms a "fingerprint" that can be used by forensic investigators to attribute multiple different attacks to the same entity.

This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution.

The CIA's Remote Devices Branch's UMBRAGE group collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation.

With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from.

UMBRAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques.

https://wikileaks.org/ciav7p1/

Look at some of the actual wording here. Each technique creates a 'fingerprint' that can be attributed to the same entity. They have a collection (library) stolen, even from Russia.

Fine so far…but wait what's this: They can misdirect attribution by leaving behind fingerprints.

What that means is, they can run something and make out its coming from someone else. So, could the 'North Korea is behind the hacks!!' be false? And could the Russian attack (not yet) be the same?

I will start to research some of the tools at Wiki, but I have a feeling they were released on purpose. But that's another story.

So, with this in mind, they have just released Umbrage at the back end of 2017, and the exploit was apparently found in June 2017.

Just looking at some of the files that Umbrage uses are listed here:

https://wikileaks.org/ciav7p1/cms/page_2621753.html

Now, you can look at this yourself, but I've picked out ones that are possibly related to this article.

First up is Webcam Capture:

https://wikileaks.org/ciav7p1/cms/page_3375226.html

This uses DarkComet RAT to monitor usage etc. It was actually used in the Syrian war, and as you may know, Russia is their ally. It's since had its download links removed, but not before the CIA grabbed it.

Now this one is interesting as it links back to Kaspersky:

https://wikileaks.org/ciav7p1/cms/page_2621772.html

“Kaspersky's sandbox environment has been known to have gaps in what it emulates when examining a process. One such example was found while testing a technique found in known-malware.

While testing this technique's effectiveness, it was found that this technique was effective against Kaspersky's scanner when the executable was placed on the target system.

… Kaspersky fails to flag the file as malicious”

So, for this malware, it targets Kaspersky, and it fails to be flagged as malicious. So, could this be why they said to not use it? Not sure, maybe they said it was spying, as they didn’t want the average user to see that the main reason was a malware that the CIA has, that can attack easily, or that it can also crash the sandbox that it uses.

Ah, looks like the actual source of the code is called “Nuclear Exploit Pack”. This is about it:

https://blog.checkpoint.com/2016/05/17/inside-nuclears-core-unraveling-a-ransomware-as-a-service-infrastructure/

And check this bit out:

“Nuclear’s infrastructure is not the work of a lone wolf. According to our findings, the leading developer is located in Krasnodar, Russia.”

There is the Russia link, well one of them. And the majority of attacks were in the US. Were some of them using Umbrage or is that just a coincidence?

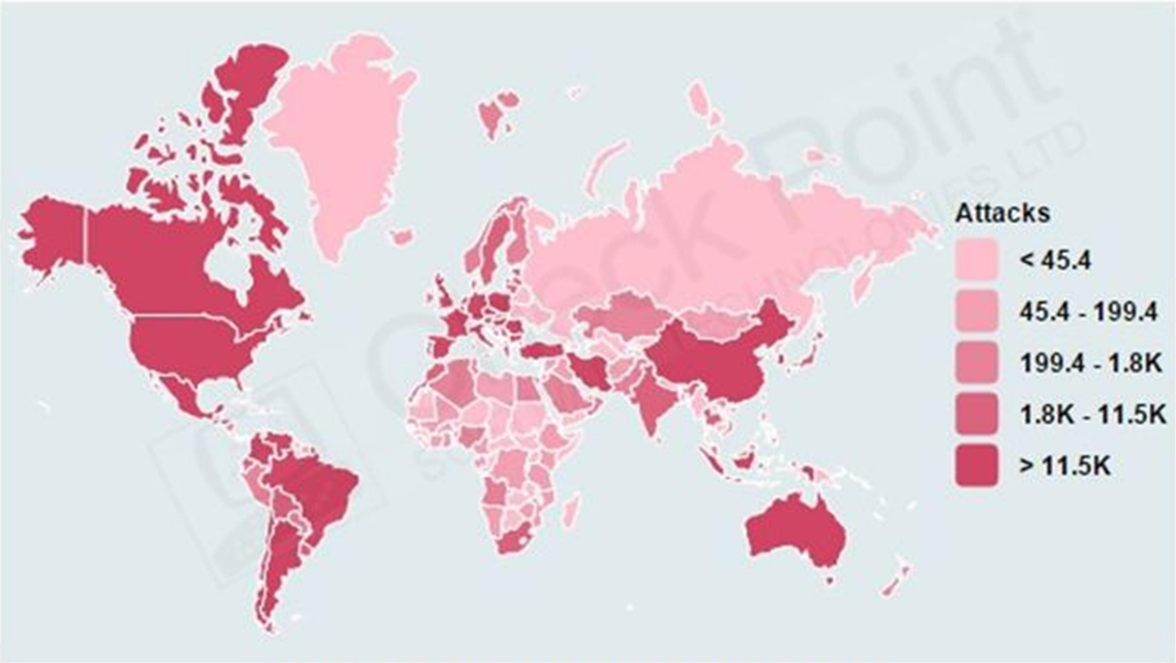


Figure 4: Attack Distribution Worldwide

Here is another that is just about Kaspersky:

https://wikileaks.org/ciav7p1/cms/page_3375327.html

But I could spend years sifting through the trove of documents etc. It's just interesting that one of the tools that was released happened to have signatures in, that can 'show' that an exploit or hack can be attributed to another country of the CIA's choosing.

Anyway, hopefully you enjoyed reading this article. Computers, especially the malware/hacking side is an area that many don't know fully about. Heard of yes, but not researched, as it's a very complicated area of computers, if you want to delve deeper.

As always, thank you for reading, and please leave a comment ☺