THREE THINGS: RUSSIA AND CHINA SPYING, KAVANOPE

[*NB: Yes, it's Rayne, not Marcy. Check the byline.]*

Huge news earlier today related to spying. Really big. MASSIVE.

And a MASSIVE cover-up pawned off on the feeble-minded as a 'complete investigation' into Dr. Ford's and Deborah Ramirez's accusations against Brett Kavanaugh.

~ 3 ~

Bloomberg published an epic piece of investigative journalism this morning about China's spying on U.S. businesses by way of tiny chips embedded in server motherboards. The photos in the story are just as important as the must-read story itself as they crystallize a challenge for U.S. intelligence and tech communities. Like this pic:

That tiny pale obelisk to the right of the penny represents one of the malicious chips found in affected Supermicro brand motherboards shipped to the U.S. market – nearly as small as the numbers in the date on the coin. Imagine looking for something this puny before a machine is turned on and begins to launch its operating system. Imagine trying to find it when it is

sandwiched inside the board itself, embedded in the fiberglass on top of which components are cemented.

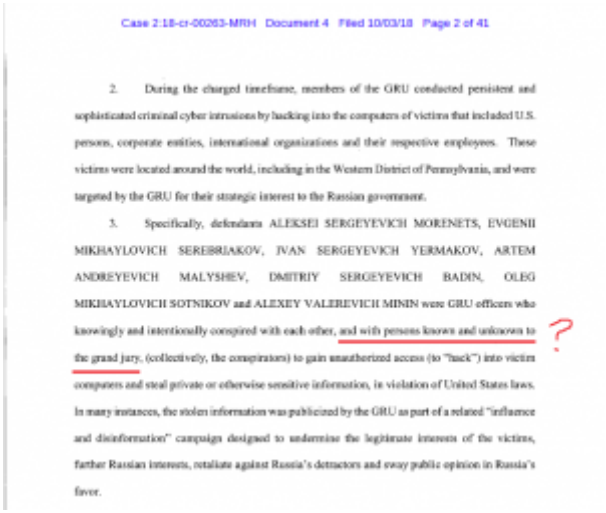
The chip could undermine encryption and passwords, making any system open to those who know about its presence. According to Bloomberg reporters Jordan Robertson and Michael Riley, the chips found their way into motherboards used by Apple and Amazon.

Information security folks are scrambling right now because this report rocks their assumptions about the supply chain and their overall infosec worldview. Quite a few doubt this Bloomberg report, their skepticism heightened by the carefully worded denials offered by affected and relevant parties Apple, Amazon, Supermicro, and China. Apple provided an itemization of what it believed Bloomberg Businessweek got wrong along with its denial.

I’ll have more on this in a future post. Yes, indeedy.

~ 2 ~

A cooperative, organized response by Britain, The Netherlands, U.S., and Canada today included the indictment of seven Russians by the U.S. for conspiracy, conspiracy to commit wire fraud, wire fraud, aggravated identity theft, and conspiracy to launder money. The Russians have been identified as members of a GRU team organized out of a facility in Moscow, working on hacking and a disinformation influence campaign focused on anti-doping entities and non-Russian Olympic athletic competitors.



Case 2:18-cr-00263-MRH Document 4 Filed 10/03/18 Page 2 of 41

2. During the charged timeframe, members of the GRU conducted persistent and sophisticated criminal cyber intrusions by hacking into the computers of victims that included U.S. persons, corporate entities, international organizations and their respective employees. These victims were located around the world, including in the Western District of Pennsylvania, and were targeted by the GRU for their strategic interest to the Russian government.

3. Specifically, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ were GRU officers who knowingly and intentionally conspired with each other, and with persons known and unknown to the grand jury, (collectively, the conspirators) to gain unauthorized access (to "hack") into victim computers and steal private or otherwise sensitive information, in violation of United States laws. In many instances, the stolen information was publicized by the GRU as part of a related "influence and disinformation" campaign designed to undermine the legitimate interests of the victims, further Russian interests, retaliate against Russia's detractors and sway public opinion in Russia's favor.

Note the underlined bit in this excerpt from the indictment (pdf) – the last indictment I copied with similar wording was that of Evgeny Buryakov and his two comrades, the three spies based in New York City who worked with "Male-1", now known to be Carter Page. Who are the *known and unknown*? Persons who have flipped or co-conspirators yet to be named?

The UK released a statement as did the Canadians, and Netherlands issued a joint statement with the UK about the entirety of spying for which this GRU team is believed to be responsible, including an attempt to breach the Organisation for the Prohibition of Chemical Weapons' (OPCW) facility analyzing the Novichok nerve agent used to poison the Skripals in the UK as well as chemicals used against Syrians.

Cryptocurrency news outlets report concerns that this indictment reveals the extent of USDOJ's ability to trace cryptocurrency.

An interesting coincidence took place overnight as well – Russian Deputy Attorney General Saak Karapetyan died last night when an unauthorized helicopter flight crashed northeast of Moscow. Karapetyan had been linked this past January to Natalia Veselnitskaya and an attempt to recruit Switzerland's top investigator as double-agents. But Karapetyan had also been involved in Russia's response to the poisoning of Alexander Litvinenko and the aftermath of the Skripals' poisoning in the UK.

What remarkable timing.

One might wonder if this accident had anything to do with the unusual release of GRU personnel details by the Dutch Military Intelligence and Security Service (MIVD) and the United Kingdom's Ministry of Justice during their joint statement today.

By comparing the released identity documents, passports, automobile registrations and the address provided when cars were rented, the identities of a total 305 GRU agents may have been identified by bellingcat and The Insider including the four out of the seven men wanted by the U.S. for the anti-doping hackingas well as attempted breach of OPCW.

The identity of the four GRU agents accused of targeting the OPCW was cinched by a taxi receipt in one agent's pocket from a location on the road next to the GRU's facility in Russia. Four agents also had consecutive passport numbers.

What remarkably bad opsec.

~ 1 ~

As for the impending vote on Brett Kavanaugh:

– Senator Heidi Heitkamp is voting her conscience – NO on Kavanaugh.
– Senator Joe Manchin is now the lone Dem holdout; he says he's still listening but hasn't seen anything incriminating from Kavanaugh's adulthood. (Gee, I wonder why.)
– Senator Bob Menendez didn't mince words. He said "It's a bullshit investigation." (He should know what a thorough investigation looks like).

And the beer-loving former Yale frat boy had an op-ed published in the Wall Street Journal which pleads with us to lose all intelligence and believe that he is really very neutral. I am not even going to link to that POS which has re-enraged women all over the country.

GTFO.

Continue calling your senators to thank them for

a NO vote on Kavanaugh so that they aren’t hearing right-wing demands alone. Congressional switchboard: (202) 224-3121

~ 0 ~

This is an open thread. Sic ’em.