ON THE KASPERSKY HACK

When the news first broke that Kaspersky had found NSA's hacking tools on the computer of a TAO employee working at home, I recalled that Kaspersky had revealed it had gotten hacked in June 2015, right around the time of this breach (and after Kaspersky released a series of reports on US, British, and Israeli spying). Last night, the NYT reported that Israel discovered NSA documents on Kaspersky's systems while they were hacking the Russian antivirus company.

> Israeli intelligence officers informed the N.S.A. that in the course of their Kaspersky hack, they uncovered evidence that Russian government hackers were using Kaspersky's access to aggressively scan for American government classified programs, and pulling any findings back to Russian intelligence systems. They provided their N.S.A. counterparts with solid evidence of the Kremlin campaign in the form of screenshots and other documentation, according to the people briefed on the events.

The WaPo, matching NYT's story, has yet another ridiculous explanation for why the TAO employee was working at home (though one that probably gets closer to the truth than the other three given thus far),

> "There wasn't any malice," said one person familiar with the case, who, like others interviewed, spoke on the condition of anonymity to discuss an ongoing case. "It's just that he was trying to complete the mission, and he needed the tools to do it."

But the WaPo also reveals that the National Intelligence Council completed a report last

month judging that FSB likely had access to Kaspersky's source code.

> Late last month, the National Intelligence Council completed a classified report that it shared with NATO allies concluding that the FSB had "probable access" to Kaspersky customer databases and source code. That access, it concluded, could help enable cyberattacks against U.S. government, commercial and industrial control networks.

Those scoops have drowned out this one from Cyberscoop, which explained that the reason the US first came to suspect Kaspersky is because the FSB told the US to stop snooping on the antivirus firm.

> In the first half of 2015, Kaspersky was making aggressive sales pitches to numerous U.S. intelligence and law enforcement agencies, including the FBI and NSA, multiple U.S. officials told CyberScoop. The sales pitch caught officials' attention inside the FBI's Counterterrorism Division when Kaspersky representatives boasted they could leverage their product in order to facilitate the capture of targets tied to terrorism in the Middle East. While some were intrigued by the offer, other more technical members of the intelligence community took the pitch to mean that Kaspersky's anti-virus software could effectively be used as a spying tool, according to current U.S. intelligence officials who received briefings on the matter.
>
> The flirtation between the FBI and Kaspersky went far enough that the bureau began looking closely at the company and interviewing employees in what's been described by a U.S. intelligence official as "due diligence"

> after Counterterrorism Division officials viewed Kaspersky's offerings with interest.
>
> The examination of Kaspersky was immediately noticed in Moscow. In the middle of July 2015, a group of CIA officials were called into a Moscow meeting with officials from the FSB, the successor to the KGB. The message, delivered as a diplomatic démarche, was clear: Do not interfere with Kaspersky.

These stories still are almost certainly revealing just a fraction of the story. All ignore Kaspersky's reports laying out US and allies' spying tools (explaining why Israel might hack Kaspersky and share the details, if not the work). And the most logical explanation for the FSB démarche is that Kaspersky — as they said at the time — reported the hack to their relevant law enforcement agency, which is the FSB, who in turn yelled at the CIA.

None of that is to minimize the intrusiveness of Kaspersky's software. It's just to remind that the US does this stuff too, and like Russia, requires compliance from US based software companies (though recent court decisions have required compliance on data for the entire globe).

Which is something the NYT admits, but doesn't detail.

> The N.S.A. bans its analysts from using Kaspersky antivirus at the agency, in large part because the agency has exploited antivirus software for its own foreign hacking operations and knows the same technique is used by its adversaries.

Finally, one other thing that could be going on here: all these entities do piggyback hacks on each other, and in fact it's the first thing most of their tools do when they breach targeted

systems — look who else is already there so you can see what they're stealing and usually take your own copy.

Which means it's possible that Russia found the NSA files by piggybacking on Israel. Or vice versa. Or, it could be nothing more complex than FSB taking the files it found while it responded to the Kaspersky hack and using them themselves.

None of this yet explains where the Shadow Brokers' tools came from (though I think the method may be similar). But I'll return to that later this week.