THE CONFLICTING HOMEWORK EXPLANATIONS IN THREE KASPERSKY STORIES

There are now three versions of the Kaspersky story from yesterday, reporting that a TAO employee brought files home from work and used them on his laptop running Kaspersky AV, which ultimately led to Russia getting the files. I'm interested in the three different explanations for why he brought the files home.

WSJ says he brought them home "possibly to continue working beyond his normal office hours."

> People familiar with the matter said he is thought to have purposely taken home numerous documents and other materials from NSA headquarters, possibly to continue working beyond his normal office hours.

WaPo (which has been reporting on this guy since last November) says he brought files he was working on to replace ones burned by Snowden.

> The employee had taken classified material home to work on it on his computer,
>
> [snip]
>
> The material the employee took included hacking tools he was helping to develop to replace others that were considered compromised following the breach of NSA material by former contractor Edward Snowden, said one individual familiar with the matter.

NYT says he brought files home to refer to as he worked on his resume.

> Officials believe he took the material home — an egregious violation of agency rules and the law — because he wanted to refer to it as he worked on his résumé

While the WSJ and WaPo stories don't conflict, they are different, with the poignant detail that NSA lost hacking files even as it tried to replace Snowden ones.

Meanwhile, none of these stories say this guy got any punishment besides removal from his job (from all his jobs? does he still work for the US government?). And while the NYT says prosecutors in Maryland are "handling" his case, they don't believe he has been charged.

> While federal prosecutors in Maryland are handling the case, the agency employee who took the documents home does not appear to have been charged.

But *all of these stories* go way too easy on this guy, as compared to the way sources would treat any other person (aside from James Cartwright) caught improperly handling classified information. As the WSJ makes clear, Admiral Rogers — not this guy — was supposed to lose his job as a result of this breach.

> Then-Defense Secretary Ash Carter and then-Director of National Intelligence James Clapper pushed President Barack Obama to remove Adm. Rogers as NSA head, due in part to the number of data breaches on his watch, according to several officials familiar with the matter.

So I suspect there is a more complex story about why he had these files at home, if that's in fact what he did.

Remember, NSA's hackers don't launch attacks

sitting in Fort Meade. They launch the attacks from some other location. Both Shadow Brokers…

> We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons.

And WikiLeaks have said that's how they got their US hacking files.

> Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

In other words, I suspect at least part of this story is an attempt to package this compromise (which is not the Shadow Brokers source, but may be the same method) in a way that doesn't make the NSA look totally incompetent.

Update: In this thread, Jonathan Nichols points out that the Vulnerabilities Equities Process has a big loophole.

> Vulnerabilities identified during the course of federally-sponsored open and unclassified research, whether in the public domain or at a government agency, FFRDC, National Lab, or other company doing work on behalf of the USG need not be put through the process. Information related to such vulnerabilities,

> however, does require notification to the Executive Secretariat, which shall notify process participants for purposes of general USG awareness.

That is, one way to avoid the VEP process altogether (and therefore potential notice to companies) is to conduct the research to develop the systems on unclassified systems. Which would be an especially big problem if you were running KAV.

Which might also explain why none of the stories explaining how this guy's files got compromised make sense.