IT'S EASY TO [CLAIM TO] ATTRIBUTE HACKS TO CIA AFTER A ONE MONTH TRIAL ON CIA'S TOOLS

Yesterday, closing arguments and charging instructions in the Joshua Schulte trial were presented to the jury. As I've noted, I think the evidence against Schulte is quite compelling, but several things have weakened the government's case. The transcripts for the closing arguments (which will come out tonight) may provide a better sense of how strong the case is. Otherwise, we wait on the jury.

But at least one Chinese InfoSec company is not waiting. One firm just released a report claiming to ID a number of CIA's hacking campaigns against Chinese targets, which it dubs APT-C-39. It explicitly relies on the trial record (though not the most interesting details of it, and some of the details revealed at trial seem to conflict with this report).

> Proficient in the design and development of cyber weapons and possessing knowledge of intelligence operations, Joshua became one of the core backbones of the CIA's many important hacking tools including a key cyber weapon — Vault 7.
>
> In 2016, Joshua took advantage of his admin privilege of the core machine room and a preset backdoor to steal the classified documents of Vault 7 and disclosed to WikiLeaks, which was published on Wikileaks website in 2017.
>
> In 2018, Joshua was arrested and prosecuted by the U.S. Department of Justice for the Vault 7 leaks. On February 4, 2020, at a public hearing in

> the federal court, the federal prosecutor alleged that Joshua, as the core developer and the person in charge of the highest administrator authority of its internal arsenal, has committed "the single biggest leak of classified national defense information in the history of CIA"by disclosing the agency's secret hacking tools to WikiLeaks.

This piece appears to be entirely reversed engineered from the leaked files and the trial record, not actual InfoSec analysis. For example, it treats "Vault 7" as CIA's code name, not some dumb label WikiLeaks assigned to it. It claims to track campaigns from September 2008 through June 2019; yet the trial record says CIA stopped all use of tools developed before Schulte left.

It makes much of compilation time. It is true that most of the work on these tools happen in VA and most of the developers work regular hours. However, there are two remote offices, so tools targeting China could easily be customized in Asian timezones.

> The compilation time of malware is a common method and statistics in the research of APT group attribution. Through the study of the compilation time of malware, we can find out the developer's work schedule, so as to know the approximate time zone of his location.
>
> The following table is the schedule of compilation activities of APT-C-39 (the time is based on the East 8 time zone). It can be seen that the organization's activities are close to the schedule in Eastern U.S. time zone, which is in line with the CIA's location. (Virginia, U.S. Eastern Time).

It also admits that it is speculating about a key point — how CIA would use all this.

> We speculate that in the past eleven years of infiltration attacks, CIA may have already grasped the most classified business information of China, even of many other countries in the world. It does not even rule out the possibility that now CIA is able to track down the real-time global flight status, passenger information, trade freight and other related information. If the guess is true, what unexpected things will CIA do if it has such confidential and important information? Get important figures' travel itinerary, and then pose political threats, or military suppression?

Don't get me wrong. I'm sure the Chinese state is watching the trial closely for clues on CIA's now defunct hacking tools, as well as organizational clues to how it used to be developed (though given China's extensive success spying on the US, doubt they've learned anything even remotely new from this trial). But *this* report, at least, looks to be a opportunistic effort to make the most of the spectacle of the US prosecuting one of its own hackers.

Update: This, from last year, is a more credible report based on Vault 7 leaks. (h/t Catalin Cimpanu)