NO MORE SECRETS: VAULT 7

Several days after Shadow Brokers first announced an auction of a bunch of NSA tools last August, Wikileaks announced it had its own "pristine" copy of the files, which it would soon release.

Wikileaks never did release that archive.

On January 7-8, Shadow Brokers got testy with Wikileaks, suggesting that Wikileaks had grown power hungry.

Shadow Brokers threw in several hashtags, two of which could be throw-offs or cultural references to a range of things (though as always with pop culture references, help me out if I'm missing something obvious). The third — "no more secrets" — in context invokes Sneakers, a movie full of devious US intelligence agencies, double dealing Russians, and the dilemma of what you do when you've got the power that comes from the ability to hack anything.

Moments later, Shadow Brokers called out Wikileaks, invoking (in the language of this season's South Park) Wikileaks' promise to release the file.

Of course, within a week, Shadow Brokers had reneged on a promise of sorts. Less than an hour before calling out Wikileaks for growing power hungry, Shadow Brokers suggested it would sell a range of Windows exploits. Four days later, it instead released a limited (and dated) subset of Windows files — ones curiously implicating Kaspersky Labs. All the "bullshit political talk," SB wrote in a final message, was just marketing.

> Despite theories, it always being about bitcoins for TheShadowBrokers. Free dumps and bullshit political talk was being for marketing attention.

And with that, the entity called Shadow Brokers checked out, still claiming to be in possession of a range of (dated) NSA hacking exploits.

Less than a month later (and over a month before Monday's release), Wikileaks started the prep for the Vault 7 release of CIA's hacking tools. (Given the month of lead hype and persistent attention throughout, I'm not sure why any claimed rapid and "overwhelming" response to the release should be attributed to Russian bots.)

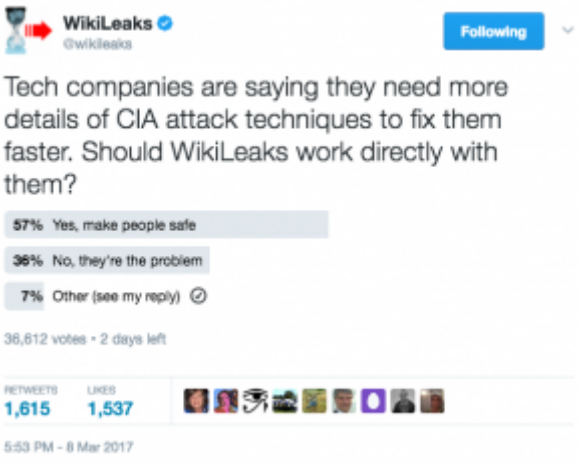
Having been called out for sitting on the Shadow Brokers' files (if, indeed, Wikileaks actually had them), Wikileaks this time gave the appearance of being forthcoming, claiming "the largest ever publication of confidential documents on the [CIA]."

Except …

While Wikileaks released a great deal of information about CIA's hacking, it didn't release the code itself, or the IP addresses that would reveal targets or command and control servers.

> Wikileaks has carefully reviewed the "Year Zero" disclosure and published substantive CIA documentation while avoiding the distribution of 'armed' cyberweapons until a consensus emerges on the technical and political nature of the CIA's program and how such 'weapons' should analyzed, disarmed and published.
>
> Wikileaks has also decided to redact and anonymise some identifying information in "Year Zero" for in depth analysis. These redactions include ten of thousands of CIA targets and attack machines throughout Latin America, Europe and the United States.

Now, perhaps Wikileaks really is doing all this out of a sense of responsibility. More likely, it is designed to create a buzz for more disclosure that WL can use to shift responsibility for further disclosure. Yesterday, Wikileaks even did a silly Twitter poll designed to get thousands to endorse further leaks.



In reality, whether for their own PR reasons or because it reflects the truth, tech companies have been issued statements reassuring users that some of the flaws identified in the Wikileaks dump have already been fixed (and in fact, for some of them, that was already reflected in the Wikileaks documents).

Thus far, however, Wikileaks is sitting on a substantial quantity of recent CIA exploits and may be sitting on a significant quantity of dated NSA exploits. Mind you, the CIA seems to know (belatedly) precisely what Wikileaks has; while NSA has a list of the exploits Shadow Brokers was purportedly trying to sell, it's not clear whether NSA knew exactly what was in that dump. But CIA and NSA can't exactly tell the rest of the world what might be coming at them in the form of repurposed leaked hacking tools.

There has been a lot of conversation — most lacking nuance — about what it means that CIA uses code from other hackers' exploits (including Shamoon, the Iranian exploit that has recently been updated and deployed against European targets). There has been less discussion about what it means that Wikileaks and Shadow Brokers and whatever go-betweens were involved in those leaks might be involved have been sitting on US intelligence community exploits.

That seems like a worthwhile question.

Update: as his delayed presser on this release, Assange stated that he would work with tech

companies to neutralize the exploits, then release them.