WIKILEAKS DUMPS CIA'S HACKING TOOLS

Today, Wikileaks released a big chunk of documents pertaining to CIA's hacking tools.

People will — and already have — treated this as yet another Russian effort to use Wikileaks as a cutout to release documents it wants out there. And that may well be the case. It would follow closely on the release, by Shadow Brokers, of a small subset of what were billed as NSA hacking tools (more on that in a bit).

Wikileaks attributes the files to two sources. First, it suggests a "US government hacker and contractor … provided WikiLeaks with portions of the archive."

> 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 an apparent reference to this source, Wikileaks explains,

> In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the

> security, creation, use, proliferation and democratic control of cyberweapons.

It also notes that developers may steal tools without a trace (though speaks of this in terms of proliferation, not this leak).

> Securing such ‘weapons’ is particularly difficult since the same people who develop and use them have the skills to exfiltrate copies without leaving traces — sometimes by using the very same ‘weapons’ against the organizations that contain them.

But Wikileaks also suggests that, because the CIA doesn’t classify its attack tools, it leaves them more vulnerable to theft.

> In what is surely one of the most astounding intelligence own goals in living memory, the CIA structured its classification regime such that for the most market valuable part of “Vault 7” — the CIA’s weaponized malware (implants + zero days), Listening Posts (LP), and Command and Control (C2) systems — the agency has little legal recourse.
>
> The CIA made these systems unclassified.
>
> Why the CIA chose to make its cyberarsenal unclassified reveals how concepts developed for military use do not easily crossover to the ‘battlefield’ of cyber ‘war’.
>
> To attack its targets, the CIA usually requires that its implants communicate with their control programs over the internet. If CIA implants, Command & Control and Listening Post software were classified, then CIA officers could be prosecuted or dismissed for violating rules that prohibit placing classified information onto the Internet. Consequently the CIA has secretly made

> most of its cyber spying/war code unclassified. The U.S. government is not able to assert copyright either, due to restrictions in the U.S. Constitution. This means that cyber 'arms' manufactures and computer hackers can freely "pirate" these 'weapons' if they are obtained. The CIA has primarily had to rely on obfuscation to protect its malware secrets.

Wikileaks is trying to appear more responsible than it was with recent leaks, which doxed private individuals. It explains that it has anonymized names. (It very helpfully replaces those names with numbers, which leaves enough specificity such that over 30 CIA hackers will know Wikileaks has detailed information on them, down to their favorite memes.) And it has withheld the actual exploits, until such time — it claims — that further consensus can be developed on how such weapons should be analyzed. In addition, Wikileaks has withheld targets.

> 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. While we are aware of the imperfect results of any approach chosen, we remain committed to our publishing model and note that the quantity of published pages in "Vault 7" part one ("Year Zero") already eclipses the total number of pages

> published over the first three years of the Edward Snowden NSA leaks.

Several comments about this: First, whether for reasonable or unreasonable purpose, withholding such details (for now) is responsible. It prevents Wikileaks' release from expanding the use of these tools. Wikileaks' password for some of these files is, "SplinterItIntoAThousandPiecesAndScatterItIntoTheWinds," suggesting the motive.

Of course, by revealing that these tools exist, but not releasing them, Wikileaks could (hypothetically) itself use them. Wikileaks doesn't explain how it obtained upcoming parts of this release, but it's possible that someone used CIA's tools against itself.

In addition, by not revealing CIA's targets, Wikileaks both explicitly and implicitly prevents CIA (and the US generally) to offer the excuse they always offer for their surveillance tools: that they're chasing terrorists — though of course, this is just a matter of agency vocabulary.

> Among the list of possible targets of the collection are 'Asset', 'Liason [sic] Asset', 'System Administrator', 'Foreign Information Operations', 'Foreign Intelligence Agencies' and 'Foreign Government Entities'. Notably absent is any reference to extremists or transnational criminals.

We will no doubt have further debate about whether Wikileaks was responsible or not with this dump. But consider: various contractors (and to a much lesser degree, the US intelligence community) have been releasing details about Russian hacking for months. That is deemed to be in the common interest, because it permits targets to prevent being hacked by a state actor.

Any hacking CIA does comes *on top of* the

simplified spying the US can do thanks to the presence of most tech companies in the US.

So why should CIA hacking be treated any differently than FSB or GRU hacking, at least by the non-American part of the world?

This leak may well be what Wikileaks claims it to be — a concerned insider exposing the CIA's excesses. Or perhaps it's part of a larger Russian op. (Those two things could even both be true.) But as we talk about cybersecurity, we would do well to remember that all nation-state hackers pose a threat to the digital commons.