WikiLeaks: CIA Has a Covert Global Hacking Program

Tuesday, WikiLeaks struck back at the “Deep State” in a big way with the release of its CIA document dossier known by the code name “Vault 7.”

In a press release to the media, the transparency organization suggests this is the first of several document dumps to be had, and is subsequently named “Year Zero.” This series comprises 8,761 documents and files from “an isolated, high-security network situated inside the CIA’s Center for Cyber Intelligence” in Langley, Va.

The press release included the following statement:

> 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.
>
> “Year Zero” introduces the scope and direction of the CIA’s global covert hacking program, its malware arsenal and dozens of “zero day” weaponized exploits against a wide range of U.S. and European company products, include Apple’s iPhone, Google’s Android and Microsoft’s Windows and even Samsung TVs, which are turned into covert microphones.
>
> Since 2001, the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous

drone fleet, but a very different type of covert, globe-spanning force—its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often-controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.

By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified.

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.

Once a single cyber "weapon" is "loose," it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike.

Julian Assange, WikiLeaks editor, stated that "There is an extreme proliferation risk in the development of cyber 'weapons'. Comparisons can be drawn between the uncontrolled proliferation of such 'weapons,' which results from the inability to contain them combined with their high market value and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and

> cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective."
>
> 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 anonymize some identifying information in "Year Zero" for in-depth analysis. These redactions include tens 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.

Click here to read the Vault 7 documents. Click here to learn more about the document dump itself. Last month, WikiLeaks also released what it termed an "introductory disclosure" of documents about the CIA's targeting of French political parties and candidates in the run-up to the 2012 elections there. {eoa}