What is #Vault7?

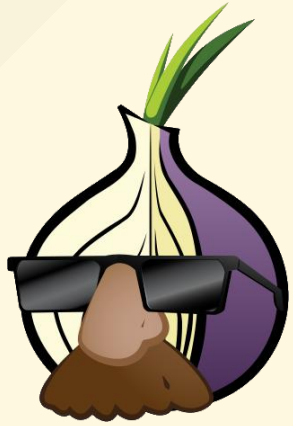
A Quick Primer on Part 1: "Year Zero"

March 8, 2017 | Sean O'Brien

sean@webio.me | sean.obrien@yale.edu | secure contact info

> 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.

Before We Begin



If you have the Tor Browser Bundle, you should probably use it.

> Download TBB ➡
>
> *It's Firefox, but anonymous! Security plugins pre-installed.*

We are **justifiably paranoid** when digging into this material. Consider your Threat Model.

- WL Twitter account is followed by millions. There is still power in crowds, but no longer anonymity.
- Browsing WikiLeaks.org is considered subversive.

The #Vault7 archive

WL has been teasing this release, and has promised 2017 "will blow you away".

- Part 1 is "Year Zero", referring to 0-day vulns.
- Released as a 514MB encrypted 7-zip file **WikiLeaks-Year-Zero-2017-v1.7z**, SHA-256 sum:

  ad5b92d2aeb2443fe292dafe7b80a8c567b925180b0a66ca212910eb253d6431
- You would need a BitTorrent client to download.
- Password is a JFK quote.
- **Disclaimer:** I am **NOT** recommending that you download the archive or browse it online.

So, what's in Part 1?

7818 pages with 943 attachments from the CIA's internal Confluence groupware/wiki. The format is similar to Intellipedia, but specifically for the CIA's devs, sysadmins, crackers/hackers.

- Software vulns and cracking tools are often listed in pretty tables.
- No binaries or scripts (CIA malware, etc.) were released, but the archive was passed around long before WL got a copy (late 2016?).
- Usernames, real names, IP addresses, and more have been redacted.