What is #Vault7?

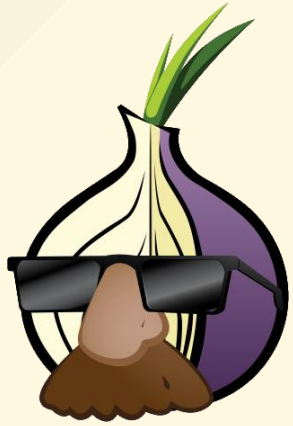
A Quick Primer on Part 1: "Year Zero"

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.

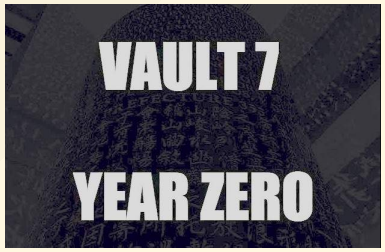
The #Vault7 archive

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?

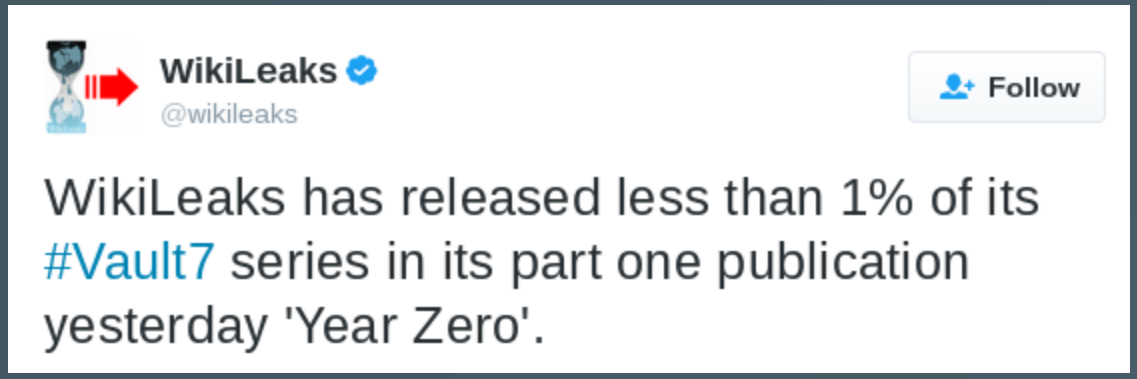


7818 pages with **943 attachments** from CIA internal Confluence groupware/wiki. The format is similar to Intellipedia, but specifically for the CIA's devs, sysadmins, crackers/hackers.

- Software vulns, cracking tools, VM 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.

Feeling Surveillance Fatigue?

Better get over it.



Let's not fall into despair or indifference.

WL is just revealing a world we already live in.

Comparisons, so far...

The Snowden trove:

- Leaked to a small group of reporters, experts.
- Redacted and released as an intermittent series of articles in major news outlets.
- Not all published, but pace will likely increase.
- Revealed targeted surveillance on a global scale as well as targeted surveillance, software vulns.
- NSA internal training, documentation, & presentations had the most media impact.

#Vault7:

- Circulated by CIA staff/contractors, then shared with WikiLeaks. WL has redacted content and code.

- Primary source published in batches, the standard WL approach (indexing, search tools, & highlighting).

- "Year Zero" focuses on software exploits, malware.

- So far, much of the release is CIA internal training, documentation, tips & tricks for being a spy.

Are Signal & WhatsApp broken?

There's no evidence the CIA broke the Signal protocol itself, which WhatsApp also uses. No private chat app, Telegram or any other, has been mentioned as being cracked.

The underlying operating systems iOS and Android have been pwned. We don't know the full extent of the Android pwnage (all AOSP? just some firmware?)

- If your text, audio, and video are being recorded before a private chat app can encrypt them, what's the use?

This highlights the importance of controlling, upgrading, and switching your OS.

Is there any good news?

Encryption curbs mass surveillance.

Edward Snowden ✓
@Snowden

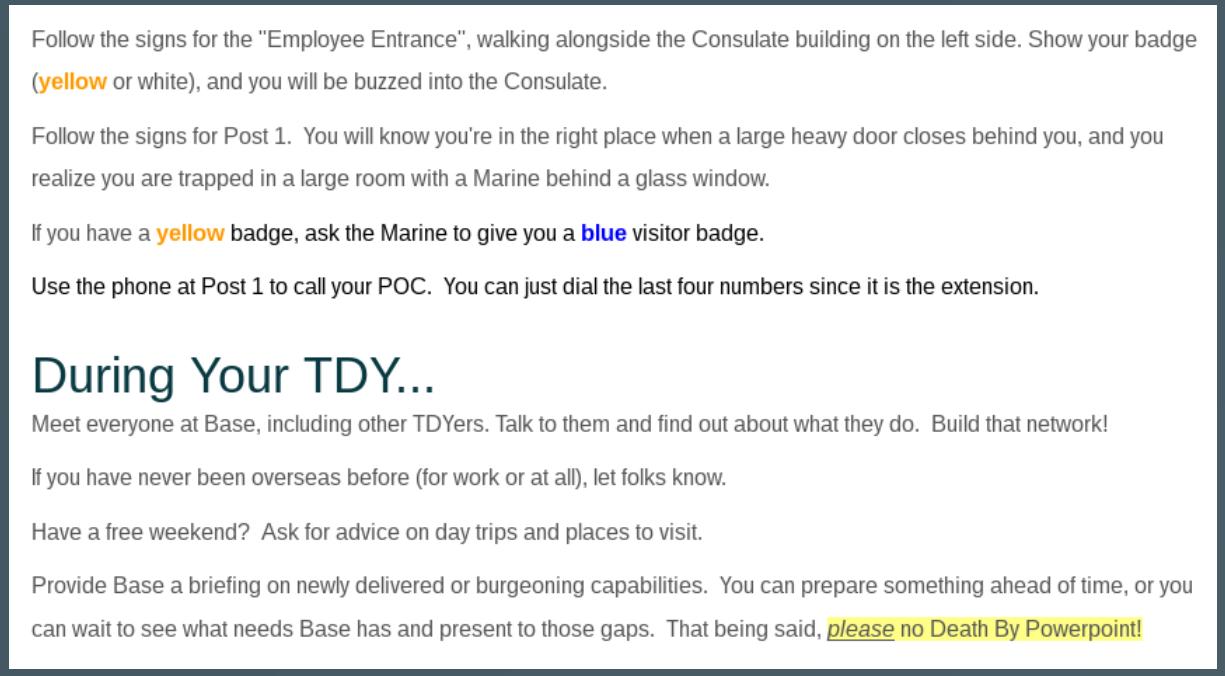
Follow

It may not feel like it, but computer security is getting better.

Open Whisper Systems @whispersystems
Ubiquitous e2e encryption is pushing intelligence agencies from undetectable mass surveillance to expensive, high-risk, targeted attacks.

- Apps like Signal, WhatsApp, and Telegram *can* work **as long as the implementation is sound**, the **OS is secure**, and **ALL of the source code is open**.
- Some of the CIA malware is already being stopped.

Let's take the CIA's advice and avoid "Death by PowerPoint"



Follow the signs for the "Employee Entrance", walking alongside the Consulate building on the left side. Show your badge (yellow or white), and you will be buzzed into the Consulate.

Follow the signs for Post 1. You will know you're in the right place when a large heavy door closes behind you, and you realize you are trapped in a large room with a Marine behind a glass window.

If you have a yellow badge, ask the Marine to give you a blue visitor badge.

Use the phone at Post 1 to call your POC. You can just dial the last four numbers since it is the extension.

During Your TDY...

Meet everyone at Base, including other TDYers. Talk to them and find out about what they do. Build that network!

If you have never been overseas before (for work or at all), let folks know.

Have a free weekend? Ask for advice on day trips and places to visit.

Provide Base a briefing on newly delivered or burgeoning capabilities. You can prepare something ahead of time, or you can wait to see what needs Base has and present to those gaps. That being said, *please* no Death By Powerpoint!

Let's skim through a list of #Vault7 revelations so far, and discuss a few of them.

#Vault7 Part 1, "Year Zero"

- CIA tech espionage has grown massively, its "own NSA" by 2016, the Center for Cyber Intelligence.
- CIA malware pwns iPhones, iPads.
- CIA malware pwns many (most? all?) Android devices.
- CIA malware pwns newer Samsung SmartTVs, spying with camera and microphone while in "Fake-Off".
- CIA can remotely control motor vehicle computers, potentially using them in assassinations.
- Apple devices are disproportionately targeted, perhaps because of popularity in powerful social & business circles.

#Vault7 Part 1, "Year Zero"

- CIA hoards 0-days, which it has now lost control over.
- CIA has a huge arsenal to pwn Microsoft Windows.
- "Hammer Drill" infects CD/DVDs via Windows burning software Nero.
- Other exploits hide on USB keys and on hard drives.
- Network Devices Branch attacks Internet infrastructure.
- CIA remotely undermines Web server and SSL/TLS security, creating MITM attacks and spoofing websites.
- Anti-virus software is almost useless against CIA malware.

#Vault7 Part 1, "Year Zero"

- The U.S. Consulate in Frankfurt, Germany is the "Center for Cyber Intelligence Europe", used for operations across Europe, Africa, and the Middle East.
- CIA devs discussed what the NSA's "Equation Group" hackers did wrong, how CIA malware-makers can do better.
- CIA re-purposes exploits from other countries & actors, keeping a huge library of malware.
- CIA has a library of virtual machine images for remote command and control, including a "PocketPutin".
- Malware is designed to mimic Russian authorship.
- Routers are targeted routinely, especially Cisco devices.