WIKILEAKS PERMADRIP: "OTHER VAULT 7 DOCUMENTS"

WikiLeaks has released the second in what they promise to be many further releases of CIA hacking tools it calls Vault 7. This release, which it dubs Dark Matter, consists of just 12 documents, which means (if WikiLkeak's past claims about how big this leak is are true) the releases could go on forever.

As Motherboard lays out, the tools that got released are old — they date from 2008 to 2013.

> While the documents are somewhat dated at this point, they show how the CIA was perhaps ahead of the curve in finding new ways to hacking and compromising Macs, according to Pedro Vilaca, a security researcher who's been studying Apple computers for years.
>
> Judging from the documents, Vilaca told Motherboard in an online chat, it "looks like CIA were very early adopters of attacks on EFI."
>
> "It looks like CIA is very interested in Mac/iOS targets, which makes sense since high value targets like to use [those]," Vilaca told me. "Also interesting the lag between their tools and public research. Of course there's always unpublished research but cool to see them ahead."

But — because I'm as interested in how Wikileaks is releasing these tools as I am in what it is releasing — it appears that WL may be sitting on more recent documents related to compromising Apple products. WL's press release describes other Vault 7 documents, plural, that refer to more recent versions of a tool designed to attack MacBook Airs. But it includes just one of

those more recent documents in this dump.

> While the DerStake1.4 manual released today dates to 2013, other Vault 7 documents show that as of 2016 the CIA continues to rely on and update these systems and is working on the production of DerStarke2.0.

That *seems* to suggest that there are other, more current Apple tools in WikiLeaks' possession besides the one developmental document linked. If so it raises the same questions I raised here: is it doing so as a pose of responsible release, withholding the active exploits until Apple can fix them? Or is it withholding the best tools for its own purposes, potentially its own or others' use? Or, given this account, perhaps Wikileaks is playing a game of chicken with the CIA, seeing whether CIA will self-disclose the newer, still unreleased exploits before Wikileaks posts them. Thus far, neither side is being forthcoming with affected tech companies, if public reports are to be believed.

In either case, I'm just as interested in what Wikileaks is doing with the files it is sitting on as I am the dated ones that have been released.

Update: In his presser the other day, Julian Assange did provide a list of tech companies he had reached out to.

> In his March 23 press conference, Assange offered the following timeline relating to WikiLeaks' communications with technology firms:
>
> > - March 12: WikiLeaks reached out to Apple, Google, Microsoft and Mozilla.
> >
> > - March 12: Mozilla replied to WikiLeaks, agreeing to its terms. The aforementioned Cisco

> engineer also reached out.

> - March 13: Google “acknowledged receipt of our initial approach but didn’t address the terms,” Assange said.

> - March 15: MikroTek contacted WikiLeaks; it makes a controller that’s widely used in VoIP equipment.

> - March 17: Mozilla replied, asked for more files.

> - March 18: WikiLeaks told Mozilla it’s looking for the information.

> - March 20: First contact from Microsoft “not agreeing to the standard terms, but pointing to their standard procedures,” Assange said, including providing a PGP email key. Google also replied the same day, pointing to their standard procedures, and including a PGP email key.