en.wikipedia.org /wiki/Vault_7

Vault 7

Contributors to Wikimedia projects ⋮ 47-59 minutes ⋮ 3/7/2017

Logo for documents collectively labeled Vault 7.

Vault 7 is a series of documents that WikiLeaks began to publish on 7 March 2017, detailing the activities and capabilities of the United States Central Intelligence Agency (CIA) to perform electronic surveillance and cyber warfare. The files, dating from 2013 to 2016, include details on the agency's software capabilities, such as the ability to compromise cars, smart TVs,[1] web browsers including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera,[2][3] the operating systems of most smartphones including Apple's iOS, and Google's Android, and computer operating systems including Microsoft Windows, macOS, and Linux.[4][5] A CIA internal audit identified 91 malware tools out of more than 500 tools in use in 2016 being compromised by the release.[6] The tools were developed by the Operations Support Branch of the C.I.A.[7]

The Vault 7 release led the CIA to redefine WikiLeaks as a "non-state hostile intelligence service."[8] In July 2022, former CIA software engineer Joshua Schulte was convicted of leaking the documents to WikiLeaks,[9] and in February 2024 sentenced to 40 years' imprisonment.[10]

History[edit]

In February 2017, WikiLeaks began teasing the release of "Vault 7" with a series of cryptic messages on Twitter, according to media reports.[11] Later on in February, WikiLeaks released classified documents describing how the CIA monitored the 2012 French presidential election.[12] The press release for the leak stated that it was published "as context for its forthcoming CIA Vault 7 series."[13]

In March 2017, US intelligence and law enforcement officials said to the international wire agency Reuters that they had been aware of the CIA security breach which led to Vault 7 since late 2016. Two officials said they were focusing on "contractors" as the possible source of the leaks.[14]

In 2017, federal law enforcement identified CIA software engineer Joshua Adam Schulte as a suspected source of Vault 7.[15][16] Schulte plead not guilty and was convicted in July 2022 of leaking the documents to WikiLeaks.

On 13 April 2017, CIA director Mike Pompeo declared WikiLeaks to be a "hostile intelligence service."[17] In September 2021, Yahoo! News reported that in 2017 in the wake of the Vault 7 leaks, the CIA considered kidnapping or assassinating Assange, spying on associates of WikiLeaks, sowing discord among its members, and stealing their electronic devices. After many months of deliberation, all proposed plans had been scrapped due to a combination of legal and moral objections. Per the 2021 Yahoo News article, a former Trump national security official stated, "We should never act out of a desire for revenge".[18]

The Vault 7 release led the CIA to redefine WikiLeaks as a "non-state hostile intelligence service."[8] In July 2022, former CIA software engineer Joshua Schulte was convicted of leaking the documents to WikiLeaks,[9] and in February 2024 sentenced to 40 years' imprisonment.[10]

Publications[edit]

Part 1 – "Year Zero"[edit]

The first batch of documents named "Year Zero" was published by WikiLeaks on 7 March 2017, consisting of 7,818 web pages with 943 attachments, purportedly from the Center for Cyber Intelligence,[19] which contained more pages than former NSA contractor and leaker, Edward Snowden's NSA release at the time.[20] WikiLeaks had released Year Zero online in a locked archive earlier that week, and revealing the passphrase on the 7th. The passphrase referred to a President Kennedy quote that he wanted “to splinter the CIA in a thousand pieces and scatter it to the winds”.[21]

WikiLeaks did not name the source, but said that the files had "circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive."[1] According to WikiLeaks, the source "wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons" since these tools raise questions that "urgently need to be debated in public, including whether the C.I.A.'s hacking capabilities exceed its mandated powers and the problem of public oversight of the agency."[1]

WikiLeaks attempted to redact names and other identifying information from the documents before their release,[1] but faced criticism for leaving some key details unredacted.[22] WikiLeaks also attempted to allow for connections between people to be drawn via unique identifiers generated by WikiLeaks.[23][24] It also said that it would postpone releasing the source code for the cyber weapons, which is reportedly several hundred million lines long, "until a consensus emerges on the technical and political nature of the C.I.A.'s program and how such 'weapons' should be analyzed, disarmed and published."[1] WikiLeaks founder Julian Assange claimed this was only part of a larger series.[20]

The CIA released a statement saying, "The American public should be deeply troubled by any WikiLeaks disclosure designed to damage the Intelligence Community's ability to protect America against terrorists or other adversaries. Such disclosures not only jeopardize US personnel and operations, but also equip our adversaries with tools and information to do us harm."[25]

In a statement issued on 19 March 2017, Assange said the technology companies who had been contacted had not agreed to, disagreed with, or questioned what he termed as WikiLeaks' standard industry disclosure plan. The standard disclosure time for a vulnerability is 90 days after the company responsible for patching the software is given full details of the flaw.[26] According to WikiLeaks, only Mozilla had been provided with information on the vulnerabilities, while "Google and some other companies" only confirmed receiving the initial notification. WikiLeaks stated: "Most of these lagging companies have conflicts of interest due to their classified work with US government agencies. In practice such associations limit industry staff with US security clearances from fixing holes based on leaked information from the CIA. Should such companies choose to not secure their users against CIA or NSA attacks users may prefer organizations such as Mozilla or European companies that prioritize their users over government contracts".[27][28]

Part 2 – "Dark Matter"[edit]

On 23 March 2017 WikiLeaks published the second release of Vault 7 material, entitled "Dark Matter". The publication included documentation for several CIA efforts to hack Apple's iPhones and Macs.[29][30][31] These included the Sonic

Screwdriver malware that could use the Thunderbolt interface to bypass Apple's password firmware protection.[32]

Part 3 – "Marble"[edit]

On 31 March 2017, WikiLeaks published the third part, "Marble". It contained 676 source code files for the CIA's Marble Framework. It is used to obfuscate, or scramble, malware code in an attempt to make it so that anti-virus firms or investigators cannot understand the code or attribute its source. According to WikiLeaks, the code also included a de-obfuscator to reverse the obfuscation effects.[33][34]

Part 4 – "Grasshopper"[edit]

On 7 April 2017, WikiLeaks published the fourth set, "Grasshopper". The publication contains 27 documents from the CIA's Grasshopper framework, which is used by the CIA to build customized and persistent malware payloads for the Microsoft Windows operating systems. Grasshopper focused on Personal Security Product (PSP) avoidance. PSPs are antivirus software such as MS Security Essentials, Symantec Endpoint or Kaspersky IS.[34][35]

Part 5 – "HIVE"[edit]

On 14 April 2017, WikiLeaks published the fifth part, "HIVE". Based on the CIA top-secret virus program created by its "Embedded Development Branch" (EDB). The six documents published by WikiLeaks are related to the HIVE multi-platform CIA malware suite. A CIA back-end infrastructure with a public-facing HTTPS interface used by CIA to transfer information from target desktop computers and smartphones to the CIA, and open those devices to receive further commands from CIA operators to execute specific tasks, all the while hiding its presence behind unsuspicious-looking public domains through a masking interface known as "Switchblade" (also known as Listening Post (LP) and Command and Control (C2)).[36]

Part 6 – "Weeping Angel"[edit]

On 21 April 2017, WikiLeaks published the sixth part, "Weeping Angel" (named for a monster in the TV show *Doctor Who*[37][38]), a hacking tool co-developed by the CIA and MI5 used to exploit a series of early smart TVs for the purpose of covert intelligence gathering. Once installed in suitable televisions with a USB stick, the hacking tool enables those televisions' built-in microphones and possibly video cameras to record their surroundings, while the televisions falsely appear to be turned off. The recorded data is then either stored locally into the television's memory or sent over the internet to the CIA. Allegedly both the CIA and MI5 agencies collaborated to develop that malware in Joint Development Workshops. Security expert Sarah Zatko said about the data "nothing in this suggests it would be used for mass surveillance," and Consumer Reports said that only some of the earliest smart TVs with built-in microphones and cameras were affected.[39][40][41]

Part 7 – "Scribbles"[edit]

On 28 April 2017, WikiLeaks published the seventh part, "Scribbles". The leak includes documentation and source code of a tool intended to track documents leaked to whistleblowers and journalists by embedding web beacon tags into classified documents to trace who leaked them.[42] The tool affects Microsoft Office documents, specifically "Microsoft Office 2013 (on Windows 8.1 x64), documents from Office versions 97-2016 (Office 95 documents will not work) and documents that are not locked, encrypted, or password-protected". When a CIA watermarked document is opened, an invisible image within the document that is hosted on the agency's server is loaded, generating a HTTP request. The request is then logged on the server, giving the intelligence agency information about who is opening it and where it is being opened. However, if a watermarked document is opened in an alternative word processor the image may be visible to the viewer. The documentation also states that if the document is viewed offline or in protected view, the watermarked image will not be able to contact its home server. This is overridden only when a user enables editing.[43]

Part 8 – "Archimedes"[edit]

On 5 May 2017, WikiLeaks published the eighth part, "Archimedes". According to U.S. SANS Institute instructor Jake Williams, who analyzed the published documents, Archimedes is a virus previously codenamed "Fulcrum". According to cyber security expert and ENISA member Pierluigi Paganini, the CIA operators use Archimedes to redirect local area network (LAN) web browser sessions from a targeted computer through a computer controlled by the CIA before the sessions are routed to the users. This type of attack is known as man-in-the-middle (MitM). With their publication WikiLeaks included a number of hashes that they claim can be used to potentially identify the Archimedes virus and guard against it in the future. Paganini stated that potential targeted computers can search for those hashes on their systems to check if their systems had been attacked by the CIA.[44]

Part 9 – "AfterMidnight" and "Assassin"[edit]

On 12 May 2017, WikiLeaks published part nine, "AfterMidnight" and "Assassin". AfterMidnight is a piece of malware installed on a target personal computer and disguises as a DLL file, which is executed while the user's computer reboots. It then triggers a connection to the CIA's Command and Control (C2) computer, from which it downloads various modules to run. As for Assassin, it is very similar to its AfterMidnight counterpart, but deceptively runs inside a Windows service process. CIA operators reportedly use Assassin as a C2 to execute a series of tasks, collect, and then periodically send user data to the CIA Listening Post(s) (LP). Similar to backdoor Trojan behavior. Both AfterMidnight and Assassin run on Windows operating system, are persistent, and periodically beacon to their configured LP to either request tasks or send private information to the CIA, as well as automatically uninstall themselves on a set date and time.[45]

Part 10 – "Athena"[edit]

On 19 May 2017, WikiLeaks published the tenth part, "Athena". The published user guide, demo, and related documents were created between September 2015 and February 2016. They are all about a malware allegedly developed for the CIA in August 2015, roughly one month after Microsoft released Windows 10 with their firm statements about how difficult it was to compromise. Both the primary "Athena" malware and its secondary malware named "Hera" are similar in theory to Grasshopper and AfterMidnight malware but with some significant differences. One of those differences is that Athena and Hera were developed by the CIA with a New Hampshire private corporation called Siege Technologies. During a Bloomberg 2014 interview the founder of Siege Technologies confirmed and justified their development of such malware. Athena malware completely hijacks Windows' Remote Access services, while Hera hijacks Windows Dnscache service. Both Athena and Hera also affect all current versions of Windows including, but not limited to, Windows Server 2012 and Windows 10. Another difference is in the types of encryption used between the infected computers and the CIA Listening Posts (LP). As for the similarities, they exploit persistent DLL files to create a backdoor to communicate with CIA's LP, steal private data, then send it to CIA servers, or delete private data on the target computer, as well as Command and Control (C2) for CIA operatives to send additional malicious software to further run specific tasks on the attacked computer. All of the above designed to deceive computer security software Beside the published detailed documents, WikiLeaks did not provide any evidence suggesting the CIA used Athena or not.[46]

Part 11 – "Pandemic"[edit]

On 1 June 2017, WikiLeaks published part 11, "Pandemic". This tool is a persistent implant affecting Windows machines with shared folders. It functions as a file system filter driver on an infected computer, and listens for Server Message Block traffic while detecting download attempts from other computers on a local network. "Pandemic" will answer a download request on behalf of the infected computer. However, it will replace the legitimate file with malware. In order to obfuscate its activities, "Pandemic" only modifies or replaces the legitimate file in transit, leaving the original on the server unchanged. The implant allows 20 files to be modified at a time, with a maximum individual file size of 800MB. While not stated in the leaked documentation, it is possible that newly infected computers could themselves become "Pandemic" file servers, allowing the implant to reach new targets on a local network.[47]

Part 12 – "Cherry Blossom"[edit]

On 15 June 2017, WikiLeaks published part 12, entitled "Cherry Blossom". Cherry Blossom used a command and control server called Cherry Tree and custom router firmware called FlyTrap to monitor internet activity of targets, scan for “email addresses, chat usernames, MAC addresses and VoIP numbers" and redirect traffic.[48]

Part 13 – "Brutal Kangaroo"[edit]

On 22 June 2017, WikiLeaks published part 13, the manuals for "Brutal Kangaroo". Brutal Kangaroo was a project focused on CIA malware designed to compromise air-gapped computer networks with infected USB drives. Brutal Kangaroo included the tools Drifting Deadline, the main tool, Shattered Assurance, a server that automates thumb drive infection, Shadow, a tool to coordinate compromised machines, and Broken Promise, a tool for exfiltrating data from the air-gapped networks.[49]

Part 14 – "Elsa"[edit]

On 28 June 2017, WikiLeaks published part 14, the manual for the project entitled "Elsa". Elsa was a tool used for tracking Windows devices on nearby WiFi networks.[50]

Part 15 – "OutlawCountry"[edit]

On 29 June 2017, WikiLeaks published part 15, the manual for project "OutlawCountry". OutlawCountry was a kernel module for Linux 2.6 that let CIA agents spy on Linux servers and redirect outgoing traffic from a Linux computer to a chosen site.[51]

Part 16 – "BothanSpy"[edit]

On 6 July 2017, WikiLeaks published part 16, the manual for project "BothanSpy". BothanSpy was a CIA hacking tool made to steal SSH credentials from Windows computers.[52]

Part 17 – "Highrise"[edit]

On 13 July 2017, WikiLeaks published part 17, the manual for project "Highrise". The Highrise hacking tool, also known as Tidecheck, was used to intercept and redirect SMS messages to Android phones using versions 4.0 through 4.3. Highrise could also be used as an encrypted communications channel between CIA agents and supervisors.[53]

Part 18 – "UCL / Raytheon"[edit]

On 19 July 2017, WikiLeaks published part 18, documents from *Raytheon Blackbird Technologies* for the "UMBRAGE Component Library" (UCL) project reports on malware and their attack vectors. According to WikiLeaks, it analysed malware attacks in the wild and gave "recommendations to the CIA development teams for further investigation and PoC development for their own malware projects." It mostly contained Proof-of-Concept ideas partly based on public documents.[54]

Part 19 – "Imperial"[edit]

On 27 July 2017, WikiLeaks published part 19, manuals for project "Imperial". Imperial included three tools: Achilles, Aeris and SeaPea. Achilles turned MacOS DMG install files into trojan malware. Aeris was a malware implant for POSIX systems, and SeaPea was an OS X rootkit.[55]

Part 20 – "Dumbo"[edit]

On 3 August 2017, WikiLeaks published part 20, manuals for project "Dumbo". Dumbo was a tool that the Agency used to disable webcams, microphones, and other surveillance tools over WiFi and bluetooth to allow field agents to perform their missions.[56]

Part 21 – "CouchPotato"[edit]

On 10 August 2017, WikiLeaks published part 21, the manual for project CouchPotato. CouchPotato was a tool for intercepting and saving remote video streams, which let the CIA tap into other people's surveillance systems.[57]

Part 22 – "ExpressLane"[edit]

On 24 August 2017, WikiLeaks published part 22, the "ExpressLane" project. These documents highlighted one of the cyber operations the CIA conducts against other services it liaises with, including the National Security Agency (NSA), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

ExpressLane, a covert information collection tool, was used by the CIA to exfiltrate the biometric data collection systems of services it liaises with. ExpressLane was installed and run under the cover of upgrading the biometric software of liaison services by the CIA's Office of Technical Services (OTS) agents without their knowledge.[58][*unreliable source*]

Part 23 – "Angelfire"[edit]

On 31 August 2017, WikiLeaks published part 23, the manual for the project Angelfire. Angelfire was a malware framework made to infect computers running Windows XP and Windows 7, made of five parts. Solartime was the malware that modified the boot sector to load Wolfcreek, which was a self-loading driver that loaded other drivers. Keystone was responsible for loading other malware. BadMFS was a covert file system that hid the malware, and Windows Transitory File System was a newer alternative to BadMFS. The manual included a long list of problems with the tools.[59]

Part 24 – "Protego"[edit]

Protego, part 24 of the Vault 7 documents, was published on 7 September 2017. According to WikiLeaks, Protego "is a PIC-based missile control system that was developed by Raytheon."[60][*unreliable source*]

Vault 8[edit]

On 9 November, 2017, WikiLeaks began publishing Vault 8, which it described as "source code and analysis for CIA software projects including those described in the Vault7 series." The stated intention of the Vault 8 publication was to "enable investigative journalists, forensic experts and the general public to better identify and understand covert CIA infrastructure components."[61] The only Vault 8 release has been the source code and development logs for Hive, a covert communications platform for CIA malware. WikiLeaks published the Hive documentation as part of Vault 7 on 14 April 2017.

In October 2021, a new backdoor based on the Hive source code was discovered being used "to collect sensitive information and provide a foothold for subsequent intrusions." Researchers called it xdr33 and released a report on it in

January 2022.[62][63][64] The malware targets an unspecified F5 appliance and allowed hackers to upload and download files.[65] It also allowed network traffic spying and execute commands on the appliance.[64][66]

Organization of cyber warfare[edit]

WikiLeaks said that the documents came from "an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence (CCI) in Langley, Virginia."[67] The documents allowed WikiLeaks to partially determine the structure and organization of the CCI. The CCI reportedly has an entire unit devoted to compromising Apple products.[68]

The cybersecurity firm Symantec analyzed Vault 7 documents and found some of the described software closely matched cyberattacks by "Longhorn," which it had monitored since 2014. Symantec had previously suspected that "Longhorn" was government-sponsored and had tracked its usage against 40 targets in 16 countries.[69][70]

Frankfurt base[edit]

The first portion of the documents made public on 7 March 2017, Vault 7 "Year Zero", revealed that a top secret CIA unit used the German city of Frankfurt as the starting point for hacking attacks on Europe, China and the Middle East. According to the documents, the U.S. government uses its Consulate General Office in Frankfurt as a hacker base for cyber operations. WikiLeaks documents reveal the Frankfurt hackers, part of the Center for Cyber Intelligence Europe (CCIE), were given cover identities and diplomatic passports to obfuscate customs officers to gain entry to Germany.[68][71]

The chief Public Prosecutor General of the Federal Court of Justice in Karlsruhe Peter Frank announced on 8 March 2017 that the government was conducting a preliminary investigation to see if it will launch a major probe into the activities being conducted out of the consulate and also more broadly whether people in Germany were being attacked by the CIA.[72] Germany's foreign minister Sigmar Gabriel from the Social Democratic Party responded to the documents of Vault 7 "Year Zero" that the CIA used Frankfurt as a base for its digital espionage operations, saying that Germany did not have any information about the cyber attacks.[73]

UMBRAGE[edit]

The documents reportedly revealed that the agency had amassed a large collection of cyberattack techniques and malware produced by other hackers. This library was reportedly maintained by the CIA's Remote Devices Branch's UMBRAGE group, with examples of using these techniques and source code contained in the "Umbrage Component Library" git repository.

False flag conspiracy theories[edit]

On the day the Vault 7 documents were first released, WikiLeaks described UMBRAGE as "a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation," and tweeted, "CIA steals other groups virus and malware facilitating false flag attacks."[74] According to WikiLeaks, by recycling the techniques of third parties through UMBRAGE, the CIA can not only increase its total number of attacks,[75] but can also mislead forensic investigators by disguising these attacks as the work of other groups and nations.[1][68] Among the techniques borrowed by UMBRAGE was the file wiping implementation used by Shamoon. According to *PC World*, some of the techniques and code snippets have been used by CIA in its internal projects, whose end result cannot be inferred from the leaks. *PC World* commented that the practice of planting "false flags" to deter attribution was not a new development in cyberattacks: Russian, North Korean and Israeli hacker groups are among those suspected of using false flags.[76]

A conspiracy theory soon emerged alleging that the CIA framed the Russian government for interfering in the 2016 U.S. elections. Conservative commentators such as Sean Hannity and Ann Coulter speculated about this possibility on Twitter, and Rush Limbaugh discussed it on his radio show.[77] Russian foreign minister Sergey Lavrov said that Vault 7 showed that "the CIA could get access to such 'fingerprints' and then use them."[74]

Cybersecurity writers and experts, such as Ben Buchanan and Kevin Poulsen, were skeptical of those theories.[12][78] Poulsen said the theories were "disinformation" being taken advantage of by Russia and spread by bots. He also wrote, "The leaked catalog isn't organized by country of origin, and the specific malware used by the Russian DNC hackers is nowhere on the list." Robert M. Lee, who founded the cybersecurity firm Dragos, said the "narrative emerged far too quickly to have been organic."[12]

According to a study by Kim Zetter in *The Intercept*, UMBRAGE was probably much more focused on speeding up development by repurposing existing tools, rather than on planting false flags.[75] Robert Graham, CEO of Errata Security told *The Intercept* that the source code referenced in the UMBRAGE documents is "extremely public", and is likely used by a multitude of groups and state actors.

Graham added: "What we can conclusively say from the evidence in the documents is that they're creating snippets of code for use in other projects and they're reusing methods in code that they find on the internet. ... Elsewhere they talk about obscuring attacks so you can't see where it's coming from, but there's no concrete plan to do a false flag operation. They're not trying to say 'We're going to make this look like Russia'."[79]

Marble framework[edit]

The documents describe the Marble framework, a string obfuscator used to hide text fragments in malware from visual inspection. Some outlets reported that foreign languages were used to cover up the source of CIA hacks, but technical analysis refuted the idea.[80][81][82] According to WikiLeaks, it reached 1.0 in 2015 and was used by the CIA throughout 2016.[82]

In its release, WikiLeaks said "Marble" was used to insert foreign language text into the malware to mask viruses, trojans and hacking attacks, making it more difficult for them to be tracked to the CIA and to cause forensic investigators to falsely attribute code to the wrong nation. The source code revealed that Marble had examples in Chinese, Russian, Korean, Arabic and Persian.[82]

Analysts called WikiLeaks' description of Marble's main purpose inaccurate, telling *The Hill* its main purpose was probably to avoid detection by antivirus programs.[83]

Marble also contained a deobfuscator tool with which the CIA could reverse text obfuscation.[82][84]

Security researcher Nicholas Weaver from International Computer Science Institute in Berkeley told the Washington Post: "This appears to be one of the most technically damaging leaks ever done by WikiLeaks, as it seems designed to directly disrupt ongoing CIA operations."[85][86]

Compromised technology and software[edit]

CDs/DVDs[edit]

HammerDrill is a CD/DVD collection tool that collects directory walks and files to a configured directory and filename pattern as well as logging CD/DVD insertion and removal events.[87]

Apple products[edit]

After WikiLeaks released the first installment of Vault 7, "Year Zero", Apple stated that "many of the issues leaked today were already patched in the latest iOS," and that the company will "continue work to rapidly address any identified vulnerabilities."[88]

On 23 March 2017, WikiLeaks released "Dark Matter", the second batch of documents in its Vault 7 series, detailing the hacking techniques and tools all focusing on Apple products developed by the Embedded Development Branch (EDB) of the CIA. The leak also revealed the CIA had been targeting the iPhone since 2008, and that some projects attacked Apple's firmware.[89] The "Dark Matter" archive included documents from 2009 and 2013. Apple issued a second statement assuring that based on an "initial analysis, the alleged iPhone vulnerability affected iPhone 3G only and was fixed in 2009 when iPhone 3GS was released." Additionally, a preliminary assessment showed "the alleged Mac vulnerabilities were previously fixed in all Macs launched after 2013".[90][91]

Cisco[edit]

WikiLeaks said on 19 March 2017 on Twitter that the "CIA was secretly exploiting" a vulnerability in a huge range of Cisco router models discovered thanks to the Vault 7 documents.[92][93] The CIA had learned more than a year ago how to exploit flaws in Cisco's widely used internet switches, which direct electronic traffic, to enable eavesdropping. Cisco quickly reassigned staff from other projects to turn their focus solely on analyzing the attack and to figure out how the CIA hacking worked, so they could help customers patch their systems and prevent criminal hackers or spies from using similar methods.[94]

On 20 March, Cisco researchers confirmed that their study of the Vault 7 documents showed the CIA had developed malware which could exploit a flaw found in 318 of Cisco's switch models and alter or take control of the network.[95] Cisco issued a warning on security risks, patches were not available, but Cisco provided mitigation advice.[93]

Smartphones/tablets[edit]

The electronic tools can reportedly compromise both Apple's iOS and Google's Android operating systems. By adding malware to the Android operating system, the tools could gain access to secure communications made on a device.[96]

Messaging services[edit]

According to WikiLeaks, once an Android smartphone is penetrated the agency can collect "audio and message traffic before encryption is applied".[1] Some of the agency's software is reportedly able to gain access to messages sent by instant messaging services.[1] This method of accessing messages differs from obtaining access by decrypting an already encrypted message.[96] While the encryption of messengers that offer end-to-end encryption, such as Telegram, WhatsApp and Signal, wasn't reported to be cracked, their encryption can be bypassed by capturing input before their encryption is applied, by methods such as keylogging and recording the touch input from the user.[96]

Commentators, among them Snowden and cryptographer and security pundit Bruce Schneier, observed that Wikileaks incorrectly implied that the messaging apps themselves, and their underlying encryption, had been compromised - an implication which was in turn reported for a period by the New York Times and other mainstream outlets.[1][97]

Vehicle control systems[edit]

One document reportedly showed that the CIA was researching ways to infect vehicle control systems. WikiLeaks stated, "The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations."[68] This statement brought renewed attention to conspiracy theories surrounding the death of Michael Hastings.[98]

Windows[edit]

The documents refer to a "Windows FAX DLL injection" exploit in Windows XP, Windows Vista and Windows 7 operating systems.[19] This would allow a user with malicious intents to hide its own malware under the DLL of another application. However, a computer must have already been compromised through another method for the injection to take place.[99][*better source needed*]

[edit]

On 7 March 2017, Edward Snowden commented on the importance of the release, stating that it reveals the United States Government to be "developing vulnerabilities in US products" and "then intentionally keeping the holes open", which he considers highly reckless.[100] On 7 March 2017, Nathan White, Senior Legislative Manager at the Internet advocacy group Access Now, writes:[101]

> Today, our digital security has been compromised because the CIA has been stockpiling vulnerabilities rather than working with companies to patch them. The United States is supposed to have a process that helps secure our digital devices and services — the 'Vulnerabilities Equities

> Process.' Many of these vulnerabilities could have been responsibly disclosed and patched. This leak proves the inherent digital risk of stockpiling vulnerabilities rather than fixing them.

On 8 March 2017, Lee Mathews, a contributor to *Forbes*, wrote that most of the hacking techniques described in Vault 7 were already known to many cybersecurity experts.[102] On 8 March 2017, some noted that the revealed techniques and tools are most likely to be used for more targeted surveillance[103][104] revealed by Edward Snowden.[105]

On 8 April 2017, Ashley Gorski, an American Civil Liberties Union staff attorney called it "critical" to understand that "these vulnerabilities can be exploited not just by our government but by foreign governments and cyber criminals around the world." Justin Cappos, professor in the Computer Science and Engineering department at New York University asks "if the government knows of a problem in your phone that bad guys could use to hack your phone and have the ability to spy on you, is that a weakness that they themselves should use for counterterrorism, or for their own spying capabilities, or is it a problem they should fix for everyone?".[106]

On 8 April 2017, Cindy Cohn, executive director of the San Francisco-based international nonprofit digital rights group Electronic Frontier Foundation, said: "If the C.I.A. was walking past your front door and saw that your lock was broken, they should at least tell you and maybe even help you get it fixed." "And worse, they then lost track of the information they had kept from you so that now criminals and hostile foreign governments know about your broken lock."[107] Furthermore, she stated that the CIA had "failed to accurately assess the risk of not disclosing vulnerabilities. Even spy agencies like the CIA have a responsibility to protect the security and privacy of Americans."[108] "The freedom to have a private conversation – free from the worry that a hostile government, a rogue government agent or a competitor or a criminal are listening – is central to a free society". While not as strict as privacy laws in Europe, the Fourth Amendment to the US constitution does guarantee the right to be free from unreasonable searches and seizures.[109]

On 12 May 2017 Microsoft President and Chief Legal Officer Brad Smith wrote "This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks," In other words, Smith expressed concern about the fact that the CIA have stockpiled such computer vulnerabilities, which in turn were stolen from them, as a result the privacy and security of their customers around the world were potentially negatively affected for an extended period.[45][110]

See also[edit]

- Arms control
- Cyber-arms industry
- End-to-end encryption § Endpoint security
- Global surveillance disclosures (2013–present)
- Market for zero-day exploits
- Proactive cyber defence
- The Shadow Brokers
- United States intelligence operations abroad
- Xetron

Notes[edit]

References[edit]

1. ^ Jump up to: *a* *b* *c* *d* *e* *f* *g* *h* *i* *Shane, Scott; Mazzetti, Mark; Rosenberg, Matthew (7 March 2017). "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents". The New York Times.* Retrieved 7 March 2017.
2. **^** Greenberg, Andy (7 March 2017). *"How the CIA Can Hack Your Phone, PC, and TV (Says WikiLeaks)". WIRED.* Retrieved 8 April 2017.
3. **^** *"WikiLeaks posts trove of CIA documents detailing mass hacking". CBS News. 7 March 2017. Retrieved 8 April 2017.*
4. **^** *Miller, Greg (7 March 2017). "WikiLeaks says it has obtained trove of CIA hacking tools".* The Washington Post. Retrieved 15 May 2018.
5. **^** *"Vault7 - Home". wikileaks.org. Retrieved 19 May 2019.*
6. **^** Goretti (10 February 2020). *"US v. Joshua Schulte Trial Transcript 2020-0206".* United States District Court Southern District of New York. Retrieved 8 March 2020.
7. **^** *Patrick Radden Keefe* (6 June 2022). *"The Surreal Case of a C.I.A. Hacker's Revenge". The New Yorker.* Retrieved 8 June 2022.
8. ^ Jump up to: *a* *b* Dorfman, Zach (7 October 2021). *"U.S. prosecution of alleged WikiLeaks 'Vault 7' source hits multiple roadblocks". news.yahoo.com.* Retrieved 29 July 2022.
9. ^ Jump up to: *a* *b* *"Ex-CIA engineer convicted over massive data leak". www.aljazeera.com.* Retrieved 31 July 2022.
10. ^ Jump up to: *a* *b* *"Ex-CIA software engineer sentenced to 40 years for giving secrets to WikiLeaks".* The Guardian. 1 February 2024.
11. **^** *Dwilson, Stephanie Dube (7 February 2017). "What Is Vault 7 on WikiLeaks?". Heavy. Retrieved 12 March 2017.*
12. ^ Jump up to: *a* *b* *c* *Poulsen, Kevin (8 March 2017). "Russia Turns WikiLeaks CIA Dump Into Disinformation".* The Daily Beast. Retrieved 12 March 2017.

13. ^ *"CIA espionage orders for the 2012 French presidential election". WikiLeaks. 16 February 2017. Retrieved 12 March 2017.*
14. ^ Reuters: U.S intel, law enforcement officials aware of CIA breach since late last year, 8 March 2017
15. ^ *Harris, Shane (15 May 2018). "U.S. identifies suspect in major leak of CIA hacking tools". The Washington Post. Retrieved 15 May 2018.*
16. ^ *Shane, Scott; Goldman, Adam (15 May 2018). "Suspect Identified in C.I.A. Leak Was Charged, but Not for the Breach". The New York Times. Retrieved 16 May 2018.*
17. ^ *Windrem, Robert (13 April 2017). "CIA Director Pompeo Calls WikiLeaks a 'Hostile Intelligence Service'. Pompeo also said Julian Assange is making "common cause with dictators" and would have been "on the wrong side of history" in the '30s, '40s and '50s". NBC News. Retrieved 13 February 2021.*
18. ^ *Dorfman, Zach; Naylor, Sean D.; Isikoff, Michael (26 September 2021). "Kidnapping, assassination and a London shoot-out: Inside the CIA's secret war plans against WikiLeaks". Yahoo! News. Retrieved 26 September 2021.*
19. ^ Jump up to: *a b "WikiLeaks claims to release thousands of CIA documents". CBS News. Associated Press. 7 March 2017. Retrieved 7 March 2017.*
20. ^ Jump up to: *a b "WikiLeaks publishes massive trove of CIA spying files in 'Vault 7' release". The Independent. 7 March 2017. Archived from the original on 11 August 2022. Retrieved 7 March 2017.*
21. ^ *Staff writers (10 March 2017). "WikiLeaks password is an anti-CIA JFK quote". News.com.au.*
22. ^ *"WikiLeaks left key details unredacted in CIA leak". CyberScoop. 9 March 2017. Retrieved 5 August 2022.*
23. ^ *"Vault7 - Home". WikiLeaks. "Redactions" section. Retrieved 10 March 2017.*
24. ^ *"Wikileaks publishes docs from what it says are CIA hacking trove". Ars Technica. 7 March 2017. Retrieved 7 March 2017.*
25. ^ *Berke, Jeremy (8 March 2017). "CIA: Americans 'should be deeply troubled' by WikiLeaks' disclosure". Business Insider. Retrieved 10 March 2017.*
26. ^ Chris Evans, Ben Hawkes: Feedback and data-driven updates to Google's disclosure policy, *Google*'s *Project Zero blog*, 13 February 2015
27. ^ Sam Varghese: Vault 7: Plans to expose firms that do not patch flaws, *iTWire*, 20 March 2017
28. ^ Assange chastises companies that haven't responded to CIA vulnerability offers, *The Hill*, 20 March 2017
29. ^ *Uchill, Joe (23 March 2017). "WikiLeaks publishes CIA hacking tactics for Apple products". The Hill. Retrieved 31 March 2017.*
30. ^ *Reisinger, Don (23 March 2017). "WikiLeaks: CIA Has Targeted iPhone Supply Chain Since 2008". Fortune. Retrieved 2 April 2017.*
31. ^ *Prince, S.J. (23 March 2017). "What Time Will WikiLeaks Vault 7 Release 'Dark Matter' CIA Docs?". Heavy.com. Retrieved 31 March 2017.*

32. ^ Gallagher, Sean (23 March 2017). "New WikiLeaks dump: The CIA built Thunderbolt exploit, implants to target Macs". Ars Technica. Retrieved 22 May 2021.
33. ^ Dwilson, Stephanie Dube (31 March 2017). "WikiLeaks Vault 7 Part 3 Reveals CIA Tool Might Mask Hacks as Russian, Chinese, Arabic". Heavy.com. Retrieved 8 April 2017.
34. ^ Jump up to: a b Burgess, Matt (7 April 2017). "WikiLeaks drops 'Grasshopper' documents, part four of its CIA Vault 7 files". WIRED UK. Retrieved 8 April 2017.
35. ^ Supervizer, Payman (7 April 2017). "Wikileaks Vault 7 Series - The Grasshopper Framework". Huffington Post. Retrieved 8 April 2017.
36. ^ Supervizer, Payman (14 April 2017). "Wikileaks Vault 7 Series - Hive". Huffington Post. Retrieved 18 April 2017.
37. ^ Pachal, Pete (7 March 2017). "CIA hack of Samsung TVs was named after a Doctor Who monster". Mashable. Retrieved 8 March 2017.
38. ^ Molina, Brett. "Alleged CIA hack named after super creepy 'Doctor Who' villain". USA TODAY. Retrieved 8 March 2017.
39. ^ Varghese, Sam (23 April 2017). "iTWire - Vault 7: guide to leak data from Samsung TVs released". www.itwire.com. Retrieved 25 April 2017.
40. ^ Brandom, Russell (25 April 2017). "Here's how to use the CIA's 'weeping angel' smart TV hack". The Verge. Retrieved 26 April 2017.
41. ^ "A Closer Look at the TVs From the CIA 'Vault 7' Hack". Consumer Reports. 8 March 2017. Retrieved 5 February 2023.
42. ^ Spring, Tom (28 April 2017). "WikiLeaks Reveals CIA Tool 'Scribbles' For Document Tracking". Threatpost. Retrieved 1 May 2017.
43. ^ "WikiLeaks Publishes CIA Anti-Whistleblowers Tool for Microsoft Office Documents". BleepingComputer. Retrieved 24 September 2017.
44. ^ Paganini, Pierluigi (5 May 2017). "WikiLeaks leaked documents that detail the Archimedes tool used by the CIA in MitM attacks". Security Affairs. Retrieved 13 May 2017.
45. ^ Jump up to: a b Storm, Darlene (15 May 2017). "WikiLeaks posts user guides for CIA malware implants Assassin and AfterMidnight". Computerworld. Retrieved 17 May 2017.
46. ^ Tung, Liam (22 May 2017). "CIA's Windows XP to Windows 10 malware: WikiLeaks reveals Athena | ZDNet". CBS Interactive ZDNet. Retrieved 29 May 2017.
47. ^ "CIA Malware Can Switch Clean Files With Malware When You Download Them via SMB". BleepingComputer. Retrieved 19 September 2017.
48. ^ "Wikileaks Alleges Years of CIA D-Link and Linksys Router Hacking Via 'Cherry Blossom' Program". threatpost.com. 16 June 2017. Retrieved 6 August 2022.
49. ^ "Vault 7: CIA Has Malware for Hacking Air-Gapped Networks via USB Thumb Drives". BleepingComputer. Retrieved 6 August 2022.
50. ^ "Vault 7: CIA Malware for Tracking Windows Devices via WiFi Networks". BleepingComputer. Retrieved 6 August 2022.

51. ^ "OutlawCountry Is CIA's Malware for Hacking Linux Systems". BleepingComputer. Retrieved 6 August 2022.
52. ^ "CIA Malware Can Steal SSH Credentials, Session Traffic". BleepingComputer. Retrieved 6 August 2022.
53. ^ "Vault 7: CIA Developed Android Malware That Works as an SMS Proxy". BleepingComputer. Retrieved 6 August 2022.
54. ^ says, Nigel Cairns (26 July 2017). "WikiLeaks drops another cache of 'Vault7' stolen tools". Naked Security. Retrieved 5 February 2023.
55. ^ "Achilles, Aeris, and SeaPea Are 3 CIA Tools for Hacking Mac and POSIX Systems". BleepingComputer. Retrieved 6 August 2022.
56. ^ "Vault 7: CIA Tool Can Shut Down Webcams and Corrupt Video Recordings". BleepingComputer. Retrieved 6 August 2022.
57. ^ "Vault 7: Wikileaks Divulges CIA Tool for Capturing RTSP and H.264 Video Streams". BleepingComputer. Retrieved 6 August 2022.
58. ^ "WikiLeaks - Vault 7: Projects: ExpressLane". wikileaks.org. Retrieved 1 November 2018.
59. ^ "CIA Developed Windows Malware That Alters Boot Sector to Load More Malware". BleepingComputer. Retrieved 6 August 2022.
60. ^ "WikiLeaks - Vault 7: Projects: Protego". wikileaks.org. Retrieved 1 November 2018.
61. ^ "WikiLeaks Releases Source Code of CIA Cyber-Weapon". BleepingComputer. Retrieved 6 August 2022.
62. ^ Paganini, Pierluigi (16 January 2023). "Experts spotted a backdoor that borrows code from CIA's Hive malware". Security Affairs. Retrieved 21 January 2023.
63. ^ "Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges". 360 Netlab Blog - Network Security Research Lab at 360. 10 January 2023. Retrieved 21 January 2023.
64. ^ Jump up to: a b "New Backdoor Created Using Leaked CIA's Hive Malware Discovered in the Wild". The Hacker News. Retrieved 21 January 2023.
65. ^ "K000132157: xdr33 malware infecting BIG-IP devices". my.f5.com. Retrieved 4 March 2023.
66. ^ Staff, S. C. (17 January 2023). "Novel Hive malware kit-based backdoor emerges". SC Media. Retrieved 5 February 2023.
67. ^ Satter, Raphael (7 March 2017). "WikiLeaks publishes CIA trove alleging wide scale hacking". Boston.com. Retrieved 7 March 2017.
68. ^ Jump up to: a b c d Cody Derespina (7 March 2017). "WikiLeaks releases 'entire hacking capacity of the CIA'". Fox News. Retrieved 7 March 2017.
69. ^ Collins, Keith. "If You Only Work on Your Malware on Weekdays, You Might Be a CIA Hacker". Defense One. Atlantic Media. Retrieved 15 April 2017.
70. ^ "Longhorn: Tools used by cyberespionage group linked to Vault 7". Symantec. Retrieved 15 April 2017.
71. ^ Goetz, John; Obermaier, Frederik (7 March 2017). "Frankfurter US-Konsulat soll Spionagezentrale sein" [Frankfurt's US Consulate appears to

be an espionage center]. *Süddeutsche Zeitung* (in German).

72. ^ Dirk Hautkapp (9 March 2017). "Internet-Methoden der CIA enthüllt". *Westdeutsche Allgemeine Zeitung*. Retrieved 17 April 2017.
73. ^ "German Foreign Minister Gabriel fears arms race with Russia – DW – 03/09/2017". *dw.com*. Retrieved 25 February 2024.
74. ^ Jump up to: [a] [b] Tani, Maxwell (9 March 2017). "Conservative media figures are embracing a wild WikiLeaks conspiracy theory that the CIA hacked the DNC, and then framed Russia". *Business Insider*. Retrieved 12 March 2017.
75. ^ Jump up to: [a] [b] Zetter, Kim (8 March 2017). "WikiLeaks Files Show the CIA Repurposing Hacking Code To Save Time, Not To Frame Russia". *The Intercept*. Retrieved 9 March 2017.
76. ^ "CIA false flag team repurposed Shamoon data wiper, other malware". *PCWorld*. Retrieved 12 March 2017.
77. ^ Blake, Aaron. "Analysis - The dangerous and irresistible GOP conspiracy theory that explains away Trump's Russia problem". *The Washington Post*. Retrieved 12 March 2017.
78. ^ Buchanan, Ben (9 March 2017). "WikiLeaks doesn't raise doubts about who hacked the DNC. We still know it was Russia". *The Washington Post*. Retrieved 12 March 2017.
79. ^ Cimpanu, Catalin. "Vault 7: CIA Borrowed Code from Public Malware". *Bleeping Computer*. Retrieved 8 March 2017.
80. ^ "WikiLeaks, così la Cia depista i raid nei computer: svelato il 'Marble Framework'". *la Repubblica* (in Italian). 31 March 2017. Retrieved 9 January 2023.
81. ^ Manach, Jean-Marc. "WikiLeaks joue à cache-cache avec la CIA". *Libération* (in French). Retrieved 9 January 2023.
82. ^ Jump up to: [a] [b] [c] [d] Cimpanu, Catalin (1 April 2017). "WikiLeaks Dumps Source Code of CIA Tool Called Marble". *Bleeping Computer*. Retrieved 3 April 2017.
83. ^ Uchill, Joe (31 March 2017). "WikiLeaks' latest leak shows how CIA avoids antivirus programs". *The Hill*. Retrieved 31 March 2017.
84. ^ Leyden, John. "WikiLeaks exposes CIA anti-forensics tool that makes Uncle Sam seem fluent in enemy tongues". *www.theregister.com*. Retrieved 25 February 2024.
85. ^ The Washington Post: WikiLeaks' latest release of CIA cyber-tools could blow the cover on agency hacking operations, *The Washington Post*, 31 March 2017
86. ^ Gallagher, Sean (2 April 2017). "Wikileaks releases code that could unmask CIA hacking operations". *Ars Technica*. Retrieved 25 February 2024.
87. ^ "Weeping Angel, Brutal Kangaroo and other secret CIA code names from the Wikileaks surveillance leak". *www.recode.net*. 7 March 2017. Retrieved 19 March 2017.

88. ^ McCormick, Rich (8 March 2017). "Apple says it's already patched 'many' iOS vulnerabilities identified in WikiLeaks' CIA dump". The Verge. Retrieved 8 March 2017.
89. ^ "Wikileaks' 'Dark Matter' release details how US 'hacked into iPhones'". The Independent. 23 March 2017. Retrieved 9 January 2023.
90. ^ Uchill, Joe (23 March 2017). "Apple: Security vulnerabilities revealed by WikiLeaks no longer work". The Hill. Retrieved 24 March 2017.
91. ^ Gallagher, Sean (23 March 2017). "New WikiLeaks dump: The CIA built Thunderbolt exploit, implants to target Macs". Ars Technica. Retrieved 24 March 2017.
92. ^ @wikileaks (19 March 2017). "CIA was secretly exploiting a..." (Tweet) – via Twitter.
93. ^ Jump up to: a b "Cisco Finds Zero-Day Vulnerability in 'Vault 7' Leak | SecurityWeek.Com". www.securityweek.com. 20 March 2017.
94. ^ Joseph Menn: A scramble at Cisco exposes uncomfortable truths about U.S. cyber defense, Reuters, 29. March 2017
95. ^ Goodin, Dan (20 March 2017). "A simple command allows the CIA to commandeer 318 models of Cisco switches". Ars Technica. Retrieved 21 March 2017.
96. ^ Jump up to: a b c Barrett, Brian (7 March 2017). "The CIA Can't Crack Signal and WhatsApp Encryption, No Matter What You've Heard". Wired. Retrieved 8 March 2017.
97. ^ Glaser, April (7 March 2017). "WikiLeaks Reveals The CIA Hacked Into Apple IPhones". ReCode. Retrieved 17 March 2017.
98. ^ "WikiLeaks 'Vault 7' dump reignites conspiracy theories surrounding death of Michael Hastings". The New Zealand Herald. 8 March 2017. Retrieved 8 March 2017.
99. ^ "Notepad++ Fix CIA Hacking Issue". notepad-plus-plus.org. Retrieved 10 March 2017.
100. ^ @Snowden (7 March 2017). "The CIA reports show the USG ..." (Tweet). Retrieved 8 March 2017 – via Twitter.
101. ^ "Alleged CIA documents show urgent need to limit government hacking – Access Now". Access Now. 7 March 2017. Retrieved 8 March 2017.
102. ^ Mathews, Lee. "WikiLeaks Vault 7 CIA Dump Offers Nothing But Old News". Forbes. Retrieved 9 March 2017.
103. ^ Hern, Alex (8 March 2017). "'Am I at risk of being hacked?' What you need to know about the 'Vault 7' documents". The Guardian. Retrieved 11 March 2017.
104. ^ Hern, Alex (8 March 2017). "Apple to 'rapidly address' any security holes as companies respond to CIA leak". The Guardian. Retrieved 11 March 2017.
105. ^ Domonoske, Camila; Myre, Greg (8 March 2017). "The CIA Document Dump Isn't Exactly Snowden 2.0. Here's Why". NPR. Retrieved 15 March 2017.

106. ^ *"Privacy experts say the CIA left Americans open to cyber attacks". Newsweek. 8 April 2017. Retrieved 9 April 2017.*
107. ^ *"Privacy experts say the CIA left Americans open to cyber attacks". Newsweek. 8 April 2017. Retrieved 6 August 2022.*
108. ^ *Whittaker, Zack (9 March 2017). "After CIA leaks, tech giants scramble to patch security flaws". ZDNet. Retrieved 9 April 2017.*
109. ^ Olivia Solon: With the latest WikiLeaks revelations about the CIA – is privacy really dead?, The Guardian, 8 March 2017
110. ^ *Smith, Brad (14 May 2017). "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack - Microsoft on the Issues". Microsoft. Retrieved 17 May 2017.*

External links[edit]

- Vault 7 at WikiLeaks
- Vault 8 at WikiLeaks
- Julian Assange Press Conference and Q&A on CIA/Vault7/YearZero, Thursday 9 March 2017, the official WikiLeaks YouTube channel