WIKIPEDIA

Vault 7

Vault 7 is a series of documents that WikiLeaks began to publish on 7 March 2017, that detail activities and capabilities of the United States' Central Intelligence Agency to perform electronic surveillance and cyber warfare. The files, dated 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 Software ASA),[2][3][4] and the operating systems of most smartphones (including Apple's iOS and Google's Android), as well as other operating systems such as Microsoft Windows, macOS, and Linux.[5][6] A CIA internal audit identified 91 malware tools out of more than 500 tools in use in 2016 being compromised by the release.[7]

Official Publishing Logo for documents collectively labeled Vault 7.

Contents

History

Publications

- Part 1 - "Year Zero"
- Part 2 - "Dark Matter"
- Part 3 - "Marble"
- Part 4 - "Grasshopper"
- Part 5 - "HIVE"
- Part 6 - "Weeping Angel"
- Part 7 - "Scribbles"
- Part 8 - "Archimedes"
- Part 9 - "AfterMidnight" and "Assassin"
- Part 10 - "Athena"
- Part 11 - "Pandemic"
- Part 12 - "Cherry Blossom"
- Part 13 - "Brutal Kangaroo"
- Part 14 - "Elsa"
- Part 15 - "OutlawCountry"
- Part 16 - "BothanSpy"
- Part 17 - "Highrise"

- Part 18 - "UCL / Raytheon"
- Part 19 - "Imperial"
- Part 20 - "Dumbo"
- Part 21 - "CouchPotato"
- Part 22 - "ExpressLane"
- Part 23 - "Angelfire"
- Part 24 - "Protego"

Authenticity

Organization of cyber warfare
- Frankfurt base

UMBRAGE
- False flag theories

Marble framework

Compromised technology and software
- CDs/DVDs
- Apple products
- Cisco
- Smartphones/tablets
  - Messaging services
- Vehicle control systems
- Windows

Commentary

See also

Notes

References

External links

History

During January and February 2017, the United States Justice Department was negotiating through Julian Assange's attorney Adam Waldman[a] for immunity and safe passage for Assange to leave the Ecuadorian Embassy in London and to travel to the United States both to discuss risk minimization of future Wikileaks releases including redactions and to testify that Russia was not the source for the WikiLeaks releases in 2016.[b] In mid February 2017, Waldman, who was pro bono, asked Senator Mark Warner who was co chairman of the United States Senate Intelligence Committee[c] if he had any questions to ask Assange. Warner abruptly contacted FBI Director James Comey and told

Waldman "stand down and end the negotiations with Assange" which Waldman complied. However, David Laufman who was Waldman's counterpart with the Justice Department replied, "That's B.S. You're not standing down and neither am I." According to Ray McGovern on 28 March 2017, Waldman and Laufman were very near an agreement between the Justice Department and Assange for "risk mitigation approaches relating to CIA documents in WikiLeaks' possession or control, such as the redaction of Agency personnel in hostile jurisdictions," in return for "an acceptable immunity and safe passage agreement" but a formal agreement was never reached and the very damaging disclosure about "Marble Framework" was released by WikiLeaks on 31 March 2017.[11][12][13]

In February 2017, WikiLeaks began teasing the release of "Vault 7" with a series of cryptic messages on Twitter, according to media reports.[14] Later on in February, WikiLeaks released classified documents describing how the CIA monitored the 2012 French presidential election.[15] The press release for the leak stated that it was published "as context for its forthcoming CIA Vault 7 series."[16]

In March 2017, US intelligence and law enforcement officials said to the international wire agency Reuters that they have 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.[17]

In 2017, federal law enforcement identified CIA software engineer Joshua Adam Schulte as a suspected source of Vault 7.[18][19]

On 13 April 2017, CIA director Mike Pompeo declared Wikileaks to be a "hostile intelligence service."[20]

Publications

Part 1 - "Year Zero"

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,[21] which already contains more pages than former NSA contractor and leaker, Edward Snowden's NSA release.[22] 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 redacted names and other identifying information from the documents before their release,[1] while attempting 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.[22]

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"

On 23 March 2017 WikiLeaks published Vault 7 part 2 "Dark Matter". The publication included documentation for several CIA efforts to hack Apple's iPhones and Macs.[29][30][31]

Part 3 - "Marble"

On 31 March 2017, WikiLeaks published Vault 7 part 3 "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.[32][33][34]

Part 4 - "Grasshopper"

On 7 April 2017, WikiLeaks published Vault 7 part 4 dubbed "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"

On 14 April 2017, WikiLeaks published Vault 7 part 5, titled "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 called Listening Post (LP) and Command and Control (C2).[36]

Part 6 - "Weeping Angel"

On 21 April 2017, WikiLeaks published Vault 7 part 6, code-named "Weeping Angel", a hacking tool co-developed by the CIA and MI5 used to exploit a series of 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 and coordinated their work in Joint Development Workshops.[37][38] As of this part 6 publication, "Weeping Angel" is the second major CIA hacking tool which notably references the British television show, *Doctor Who*, alongside "Sonic Screwdriver" in "Dark Matter".[39][40]

Part 7 - "Scribbles"

On 28 April 2017, WikiLeaks published Vault 7 part 7 "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.[41][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 d]ocuments that are not [locked], encrypted, or password-protected".[43] 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.[44]

Part 8 - "Archimedes"

On 5 May 2017, WikiLeaks published Vault 7 part 8 "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.[45]

Part 9 - "AfterMidnight" and "Assassin"

On 12 May 2017, WikiLeaks published Vault 7 part 9 "AfterMidnight" and "Assassin". AfterMidnight is a 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.[46][47]

Part 10 - "Athena"

On 19 May 2017, WikiLeaks published Vault 7 part 10 "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. Also both Athena and Hera 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 has not provided any evidence suggesting the CIA used Athena or not.[48][49][50]

Part 11 - "Pandemic"

On 1 June 2017, WikiLeaks published Vault 7 part 11 "Pandemic". This tool serves as 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.[51]

Part 12 - "Cherry Blossom"

On 15 June 2017, WikiLeaks published Vault 7 part 12 "Cherry Blossom".[52]

Part 13 - "Brutal Kangaroo"

On 22 June 2017, WikiLeaks published Vault 7 part 13 "Brutal Kangaroo".[53]

Part 14 - "Elsa"

On 28 June 2017, WikiLeaks published Vault 7 part 14 "Elsa".[54]

Part 15 - "OutlawCountry"

On 29 June 2017, WikiLeaks published Vault 7 part 15 "OutlawCountry".[55]

Part 16 - "BothanSpy"

On 6 July 2017, WikiLeaks published Vault 7 part 16 "BothanSpy".[56]

Part 17 - "Highrise"

On 13 July 2017, WikiLeaks published Vault 7 part 17 "Highrise".[57]

Part 18 - "UCL / Raytheon"

UCL / Raytheon - 19 July 2017[58]

Part 19 - "Imperial"

Imperial - 27 July 2017[59]

Part 20 - "Dumbo"

Dumbo - 3 August 2017[60]

Part 21 - "CouchPotato"

CouchPotato - 10 August 2017[61]

Part 22 - "ExpressLane"

WikiLeaks publishes secret documents from the "ExpressLane" project of the CIA. These documents show one of the cyber operations the CIA conducts against liaison services—which includes among many others the National Security Agency (NSA), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

The OTS (Office of Technical Services), a branch within the CIA, has a biometric collection system that is provided to liaison services around the world—with the expectation for sharing of the biometric takes collected on the systems. But this 'voluntary sharing' obviously does not work or is considered insufficient by the CIA, because ExpressLane is a covert information collection tool that is used by the CIA to secretly exfiltrate data collections from such systems provided to liaison services.

ExpressLane is installed and run with the cover of upgrading the biometric software by OTS agents that visit the liaison sites. Liaison officers overseeing this procedure will remain unsuspicious, as the data exfiltration disguises behind a Windows installation splash screen.

The core components of the OTS system are based on products from Cross Match, a US company specializing in biometric software for law enforcement and the Intelligence Community. The company hit the headlines in 2011 when it was reported that the US military used a Cross Match product to identify Osama bin Laden during the assassination operation in Pakistan.- 24 August 2017[62]

Part 23 - "Angelfire"

Angelfire - 31 August 2017[63]

Part 24 - "Protego"

Protego - 7 September 2017[64]

Authenticity

> Tucker Carlson: So, 51,000 people retweeted that. So a lot of people thought that was plausible, they believe you, you're the President -- you're in charge of the agencies. Every intelligence agency reports to you. Why not immediately go to them and gather evidence to support that?
>
> Donald Trump: Because I don't want to do anything that's going to violate any strength of an agency. We have enough problems.
>
> And by the way, with the CIA, I just want people to know, the CIA was hacked, and a lot of things taken -- that was during the Obama years. That was not during us. That was during the Obama situation. Mike Pompeo is there now doing a fantastic job.
>
> — transcript, *Tucker Carlson Tonight*, March 16, 2017, (Fox News)[65]

When asked about their authenticity, former Director of the Central Intelligence Agency Michael Hayden replied that the organization does "not comment on the authenticity or content of purported intelligence documents."[1] However, speaking on condition of anonymity, current and former intelligence officials said that the documents appear to be genuine.[66] Edward Snowden tweeted shortly after the documents' release that they looked authentic.[67] Robert M. Chesney, a law professor at the University of Texas and Director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS), likened the Vault 7 to NSA hacking tools disclosed in 2016 by a group calling itself The Shadow Brokers.[1]

On 15 March 2017, President Donald Trump stated during an interview that "the CIA was hacked, and a lot of things taken".[68] The following day in a statement, Democratic Congressman Adam Schiff, the Ranking Member of the House Intelligence Committee, wrote in a news release, "In his effort to once again blame Obama, the President appeared to have discussed something that, if true and accurate, would otherwise be considered classified information."[69] Schiff also said that the president has the power to declassify whatever he wants.[70]

Organization of cyber warfare

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."[71] 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.[67]

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.[72][73]

Frankfurt base

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.[67][74]

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.[75] 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.[76]

UMBRAGE

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. According to WikiLeaks, by recycling the techniques of third-parties through UMBRAGE, the CIA can not only increase its total number of attacks,[77] but can also mislead forensic investigators by disguising these attacks as the work of other groups and nations.[1][67] 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.[78]

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.[77] 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]

False flag theories

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."[80] 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.[81] Russian foreign minister Sergey Lavrov said that Vault 7 showed that "the CIA could get access to such 'fingerprints' and then use them."[80]

Cybersecurity writers, such as Ben Buchanan and Kevin Poulsen, were skeptical of those theories.[15][82] Poulsen 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."[15]

Marble framework

The documents describe the Marble framework, a string obfuscator used to hide text fragments in malware from visual inspection. As part of the program, foreign languages were used to cover up the source of CIA hacks.[83][84][85] According to WikiLeaks, it reached 1.0 in 2015 and was used by the CIA throughout 2016.[86]

In its release, WikiLeaks described the primary purpose of "Marble" as 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.[87] The source code revealed that Marble had examples in Chinese, Russian, Korean, Arabic and Persian.[88] These were the languages of the US's main cyber-adversaries – China, Russia, North Korea, and Iran.[89]

Analysts called WikiLeaks' description of Marble's main purpose inaccurate, telling *The Hill* its main purpose was probably to avoid detection by antivirus programs.[90]

Marble also contained a deobfuscator tool with which the CIA could reverse text obfuscation.[89]

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."[91][92]

Compromised technology and software

CDs/DVDs

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. v2.0 adds a gap jumping capability that Trojans 32-bit executables as they are being burned to disc by Nero. Additionally, v2.0 adds a status, termination and an on-demand collection feature controlled by HammerDrillStatus.dll, HammerDrillKiller.dll and HammerDrillCollector.dll. The logging now also fingerprints discs by hashing the first two blocks of the ISO image, which enables unique identification of multi-sessions discs even as data is added and removed. The log also logs anytime a HammerDrill trojaned binary is seen on a disc.[93][94]

Apple products

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."[95]

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, a year after the device was released. These EDB projects attacked Apple's firmware, meaning that the attack code would persist even if the device was rebooted.[96][97] 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".[98][99]

Cisco

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.[100][101] 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.[102]

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.[103]

Cisco issued a warning on security risks, patches were not available, but Cisco provided mitigation advice.[101]

Smartphones/tablets

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.[104]

Messaging services

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.[104] 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.[104] 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][105]

Vehicle control systems

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."[67][106] This statement brought renewed attention to conspiracy theories surrounding the death of Michael Hastings.[106][107]

Windows

The documents refer to a "Windows FAX DLL injection" exploit in Windows XP, Windows Vista and Windows 7 operating systems.[21] 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.[108]

Commentary

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.[109]

On 7 March 2017, Nathan White, Senior Legislative Manager at the Internet advocacy group Access Now, writes:[110]

> 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.[111]

On 8 March 2017, Some note that the revealed techniques and tools are most likely to be used for more targeted surveillance[112][113] revealed by Edward Snowden.[114]

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?".[115]

On 8 April 2017, Cindy Cohn, executive director of the international non-profit digital rights group based in San Francisco 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." [116] 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."[117] "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.[118]

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, while they failed to inform Microsoft in a timely fashion about their security breach, as a result the privacy and security of their customers around the world were potentially negatively affected for an extended period and caused widespread damage.[46][119]

See also

- Arms control
- Cyber-arms industry
- End-to-end encryption § Endpoint security
- Global surveillance disclosures (2013–present)
- Market for zero-day exploits
- List of material published by WikiLeaks
- Operation Leakspin
- Proactive cyber defence
- Xetron
- United States intelligence operations abroad

Notes

a. Adam Waldman was Oleg Deripaska's attorney from 8 May 2009, to 5 April 2018, as well as Sergei Lavrov and visited Julian Assange nine times in 2017 at the Ecuadorian Embassy in London as his pro bono attorney.[8][9][10] Anastasia Vashukevich was with Deripaska in Lech, Austria when he spoke to Waldman in January 2017 just after Waldman had spoken to Julian Assange on January 12-13, 2017.[9]

b. DCLeaks was a Russian government release of sensitive information during 2016.

c. According to Ray McGovern, Senator Warner kept Senator Richard Burr, who was the other co-chairman of the Senate Intelligence Committee, informed of Warner's interactions with Waldman.

References

1. Shane, Scott; Mazzetti, Mark; Rosenberg, Matthew (7 March 2017). "WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents" (https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html). *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)" (https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/). *WIRED*. Retrieved 8 April 2017.
3. Murdock, Jason (7 March 2017). "Vault 7: CIA hacking tools were used to spy on iOS, Android and Samsung smart TVs" (http://www.ibtimes.co.uk/vault-7-cia-hacking-tools-were-used-spy-ios-a

ndroid-samsung-smart-tvs-1610263). *International Business Times UK*. Retrieved 8 April 2017.

4. "WikiLeaks posts trove of CIA documents detailing mass hacking" (http://www.cbsnews.com/news/wikileaks-cia-documents-released-cyber-intelligence/). *CBS News*. 7 March 2017. Retrieved 8 April 2017.
5. Miller, Greg (7 March 2017). "WikiLeaks says it has obtained trove of CIA hacking tools" (https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html). *The Washington Post*. Retrieved 15 May 2018.
6. "Vault7 - Home" (https://wikileaks.org/ciav7p1/). *wikileaks.org*. Retrieved 19 May 2019.
7. Goretti (10 February 2020). "US v. Joshua Schulte Trial Transcript 2020-0206" (https://www.documentcloud.org/documents/6771808-20200206-REDACTED.html). *United States District Court Southern District of New York*. Retrieved 8 March 2020.
8. Kirchgaessner, Stephanie; Harding, Luke (20 June 2018). "US lobbyist for Russian oligarch visited Julian Assange nine times last year: It is unclear whether Adam Waldman's 2017 visits had connection to Oleg Deripaska" (https://www.theguardian.com/media/2018/jun/20/us-lobbyist-for-russian-oligarch-visited-julian-assange-nine-times-last-year). *The Guardian*. Retrieved 13 February 2021.
9. "American lobbyist Adam Waldman met with Oleg Deripaska before visiting Julian Assange in London" (https://www.proekt.media/en/article-en/adam-waldman-eng/). *Проект Медиа (Proekt)*. 11 December 2018. Retrieved 13 February 2021.
10. Neufeld, K. Louise (4 July 2018). "It's Official: Adam Waldman of The Endeavor Law Firm No Longer Represents Deripaska's Rusal" (https://medium.com/@ninaandtito/its-official-adam-waldman-of-the-endeavor-law-firm-no-longer-represents-deripaska-s-rusal-641290015e93). *The Medium*. Retrieved 13 February 2021.
11. McGovern, Ray (22 February 2020). "Assange Extradition: Did Sen. Warner and Comey Crush Assange Immunity Deal? The U.S. was in talks for a deal with Julian Assange but then FBI Director James Comey ordered an end to negotiations after Assange offered to prove Russia was not involved in the DNC leak, as Ray McGovern explains" (https://consortiumnews.com/2020/02/22/did-sen-warner-and-comey-collude-on-russia-gate/). *Consortium News*. Retrieved 13 February 2021.
12. "Coming up Tuesday's 'Rising:' How the DOJ almost offered an immunity deal to Julian Assange" (https://thehill.com/hilltv/rising/394049-coming-up-tuesdays-rising-how-the-doj-almost-offered-an-immunity-deal-to-julian). *The Hill*. 25 June 2018. Retrieved 13 February 2021.
13. Solomon, John (25 June 2018). "How Comey intervened to kill WikiLeaks' immunity deal" (https://thehill.com/opinion/white-house/394036-How-Comey-intervened-to-kill-Wikileaks-immunity-deal). *The Hill*. Retrieved 13 February 2021.
14. Dwilson, Stephanie Dube (7 February 2017). "What Is Vault 7 on WikiLeaks?" (http://heavy.com/tech/2017/02/what-is-vault-7-wikileaks-theories-vault7-tweets-photos-analysis-clues-twitter-who-where-when-why-how/). *Heavy*. Retrieved 12 March 2017.
15. Poulsen, Kevin (8 March 2017). "Russia Turns WikiLeaks CIA Dump Into Disinformation" (http://www.thedailybeast.com/articles/2017/03/08/who-s-behind-the-massive-cia-leak.html). *The Daily Beast*. Retrieved 12 March 2017.
16. "CIA espionage orders for the 2012 French presidential election" (https://wikileaks.org/cia-france-elections-2012/). WikiLeaks. 16 February 2017. Retrieved 12 March 2017.
17. Reuters: U.S intel, law enforcement officials aware of CIA breach since late last year (https://www

17. Reuters. U.S intel, law enforcement officials aware of CIA breach since late last year (https://www.reuters.com/article/us-cia-wikileaks-leak-idUSKBN16F2CZ), 8 March 2017
18. Harris, Shane (15 May 2018). "U.S. identifies suspect in major leak of CIA hacking tools" (https://www.washingtonpost.com/world/national-security/us-identifies-suspect-in-major-leak-of-cia-hacking-tools/2018/05/15/5d5ef3f8-5865-11e8-8836-a4a123c359ab_story.html). *The Washington Post*. Retrieved 15 May 2018.
19. Shane, Scott; Goldman, Adam (15 May 2018). "Suspect Identified in C.I.A. Leak Was Charged, but Not for the Breach" (https://www.nytimes.com/2018/05/15/us/cia-hacking-tools-leak.html). *The New York Times*. Retrieved 16 May 2018.
20. 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" (https://www.nbcnews.com/news/us-news/cia-director-pompeo-calls-wikileaks-hostile-intelligence-service-n746311). *NBC News*. Retrieved 13 February 2021.
21. "WikiLeaks claims to release thousands of CIA documents" (http://www.cbsnews.com/news/wikileaks-cia-documents-released-cyber-intelligence/). CBS News. Associated Press. 7 March 2017. Retrieved 7 March 2017.
22. "WikiLeaks publishes massive trove of CIA spying files in 'Vault 7' release" (https://www.independent.co.uk/life-style/gadgets-and-tech/news/wikileaks-cia-vault-7-julian-assange-year-zero-documents-download-spying-secrets-a7616031.html). *The Independent*. 7 March 2017. Retrieved 7 March 2017.
23. "Vault7 - Home" (https://wikileaks.org/ciav7p1/). WikiLeaks. "Redactions" section. Retrieved 10 March 2017.
24. "Wikileaks publishes docs from what it says are CIA hacking trove" (https://arstechnica.com/security/2017/03/wikileaks-publishes-what-it-says-is-trove-of-cia-hacking-tools/). *Ars Technica*. 7 March 2017. Retrieved 7 March 2017.
25. Berke, Jeremy (8 March 2017). "CIA: Americans 'should be deeply troubled' by WikiLeaks' disclosure" (http://www.businessinsider.com/cia-responds-to-wikileaks-disclosure-2017-3). *Business Insider*. Retrieved 10 March 2017.
26. Chris Evans, Ben Hawkes: Feedback and data-driven updates to Google's disclosure policy (https://googleprojectzero.blogspot.de/2015/02/feedback-and-data-driven-updates-to.html), *Google's Project Zero blog*, 13 February 2015
27. Sam Varghese: Vault 7: Plans to expose firms that do not patch flaws (http://www.itwire.com/security/77349-vault-7-plans-to-expose-firms-that-do-not-patch-flaws.html), *iTWire*, 20 March 2017
28. Assange chastises companies that haven't responded to CIA vulnerability offers (http://thehill.com/policy/cybersecurity/324749-assange-chastises-companies-who-havent-responded-to-cia-vulnerability), *The Hill*, 20 March 2017
29. Uchill, Joe (23 March 2017). "WikiLeaks publishes CIA hacking tactics for Apple products" (http://thehill.com/policy/cybersecurity/325443-wikileaks-publishes-cia-apple-hacking-tactics). *The Hill*. Retrieved 31 March 2017.
30. Reisinger, Don (23 March 2017). "WikiLeaks Says CIA Has Targeted iPhone Supply Chain Since 2008" (http://fortune.com/2017/03/23/apple-wikileaks-iphone/). *Fortune*. Retrieved 2 April 2017.
31. Prince, S.J. (23 March 2017). "What Time Will WikiLeaks Vault 7 Release 'Dark Matter' CIA Docs?" (http://heavy.com/news/2017/03/what-time-will-wikileaks-vault-7-dark-matter-release-password-passcode/). *Heavy.com*. Retrieved 31 March 2017.

32. Mascarenhas, Hyacinth (1 April 2017). "WikiLeaks 'Marble' files: Latest leak exposes how CIA disguises its own hacking attacks" (http://www.ibtimes.co.uk/wikileaks-marble-files-latest-leak-exposes-how-cia-disguises-its-own-hacking-attacks-1614811). *International Business Times*. Retrieved 3 April 2017.
33. Dwilson, Stephanie Dube (31 March 2017). "WikiLeaks Vault 7 Part 3 Reveals CIA Tool Might Mask Hacks as Russian, Chinese, Arabic" (http://heavy.com/tech/2017/03/wikileaks-vault-7-part-3-marble-cia-tool-to-mask-hacks-hacking-russian-chinese-arabic-decoy-languages-attribute/). *Heavy.com*. Retrieved 8 April 2017.
34. Burgess, Matt (7 April 2017). "WikiLeaks drops 'Grasshopper' documents, part four of its CIA Vault 7 files" (https://www.wired.co.uk/article/cia-files-wikileaks-vault-7). *WIRED UK*. Retrieved 8 April 2017.
35. Supervizer, Payman (7 April 2017). "Wikileaks Vault 7 Series - The Grasshopper Framework" (http://www.huffingtonpost.com/entry/wikileaks-vault-7-series-the-grasshopper-framework_us_58e7bf35e4b0acd784ca57a7). *Huffington Post*. Retrieved 8 April 2017.
36. Supervizer, Payman (14 April 2017). "Wikileaks Vault 7 Series - Hive" (http://www.huffingtonpost.com/entry/wikileaks-vault-7-series-hive_us_58f0a299e4b0156697224e4a). *Huffington Post*. Retrieved 18 April 2017.
37. Varghese, Sam (23 April 2017). "iTWire - Vault 7: guide to leak data from Samsung TVs released" (http://www.itwire.com/security/77764-vault-7-guide-to-leak-data-from-samsung-tvs-released.html). *www.itwire.com*. Retrieved 25 April 2017.
38. Brandom, Russell (25 April 2017). "Here's how to use the CIA's 'weeping angel' smart TV hack" (https://www.theverge.com/2017/4/25/15421326/smart-tv-hacking-cia-samsung-weeping-angel-vulnerability). *The Verge*. Retrieved 26 April 2017.
39. Pachal, Pete. "CIA hack of Samsung TVs was named after a Doctor Who monster" (http://mashable.com/2017/03/07/cia-samsung-tv-hack-weeping-angel/). *Mashable*. Retrieved 8 March 2017.
40. Molina, Brett. "Alleged CIA hack named after super creepy 'Doctor Who' villain" (https://www.usatoday.com/story/tech/talkingtech/2017/03/07/alleged-cia-technique-named-after-doctor-who-villain/98853924/). *USA TODAY*. Retrieved 8 March 2017.
41. Spring, Tom (28 April 2017). "WikiLeaks Reveals CIA Tool 'Scribbles' For Document Tracking" (https://threatpost.com/wikileaks-reveals-cia-tool-scribbles-for-document-tracking/125299/). *Threatpost*. Retrieved 1 May 2017.
42. Ashok, India (1 May 2017). "WikiLeaks publishes user guide and source code for CIA's secret leaker-tracking tool Scribbles" (http://www.ibtimes.co.uk/wikileaks-publishes-user-guide-source-code-cias-secret-leaker-tracking-tool-scribbles-1619399). *International Business Times UK*. Retrieved 4 May 2017.
43. "WikiLeaks - Vault 7: Projects" (https://wikileaks.org/vault7/#Scribbles). *wikileaks.org*. Retrieved 24 September 2017.
44. "WikiLeaks Publishes CIA Anti-Whistleblowers Tool for Microsoft Office Documents" (https://www.bleepingcomputer.com/news/gaming/wikileaks-publishes-cia-anti-whistleblowers-tool-for-microsoft-office-documents/). *BleepingComputer*. Retrieved 24 September 2017.
45. Paganini, Pierluigi (5 May 2017). "WikiLeaks leaked documents that detail the Archimedes tool used by the CIA in MitM attacks" (http://securityaffairs.co/wordpress/58775/hacking/cia-archimedes-tool.html). *Security Affairs*. Retrieved 13 May 2017.
46. Storm, Darlene (15 May 2017). "WikiLeaks posts user guides for CIA malware implants Assassin and AfterMidnight" (http://www.computerworld.com/article/3196987/security/wikileaks-posts-user

and AfterMidnight" (http://www.computerworld.com/article/3196987/security/wikileaks-posts-user-guides-for-cia-malware-implants-assassin-and-aftermidnight.html). *Computerworld*. Retrieved 17 May 2017.

47. Ashok, India (17 May 2017). "New WikiLeaks dump reveals how the CIA hacks, spies and sabotages software" (http://www.ibtimes.co.uk/new-wikileaks-dump-reveals-how-cia-hacks-spies-sabotages-software-1621980). *International Business Times UK*. Retrieved 29 May 2017.
48. Ashok, India (20 May 2017). "What is WikiLeaks' new dump Athena? All Windows versions can be hacked by this CIA spyware" (http://www.ibtimes.co.uk/wikileaks-new-dump-reveals-all-windows-versions-can-be-targeted-by-cia-spy-malware-athena-1622508). *International Business Times UK*. Retrieved 29 May 2017.
49. Ronamai, Raymond (22 May 2017). "What is Athena malware? Windows 10, XP Pro, 8.1, and others under target, says WikiLeaks" (http://www.ibtimes.co.in/what-athena-malware-windows-10-xp-pro-8-1-others-under-target-says-wikileaks-727723). *International Business Times, India Edition*. Retrieved 29 May 2017.
50. Tung, Liam (22 May 2017). "CIA's Windows XP to Windows 10 malware: WikiLeaks reveals Athena | ZDNet" (https://www.zdnet.com/article/cias-windows-xp-to-windows-10-malware-wikileaks-reveals-athena/). *CBS Interactive ZDNet*. Retrieved 29 May 2017.
51. "CIA Malware Can Switch Clean Files With Malware When You Download Them via SMB" (https://www.bleepingcomputer.com/news/security/cia-malware-can-switch-clean-files-with-malware-when-you-download-them-via-smb/). *BleepingComputer*. Retrieved 19 September 2017.
52. "WikiLeaks - Vault 7: Projects: Cherry Blossom" (https://wikileaks.org/vault7/#Cherry%20Blossom). *wikileaks.org*. Retrieved 1 November 2018.
53. "WikiLeaks - Vault 7: Projects: Brutal Kangaroo" (https://wikileaks.org/vault7/#Brutal%20Kangaroo). *wikileaks.org*. Retrieved 1 November 2018.
54. "WikiLeaks - Vault 7: Projects: Elsa" (https://wikileaks.org/vault7/#Elsa). *wikileaks.org*. Retrieved 1 November 2018.
55. "WikiLeaks - Vault 7: Projects: OutlawCountry" (https://wikileaks.org/vault7/#OutlawCountry). *wikileaks.org*. Retrieved 1 November 2018.
56. "WikiLeaks - Vault 7: Projects: BothanSpy" (https://wikileaks.org/vault7/#BothanSpy). *wikileaks.org*. Retrieved 1 November 2018.
57. "WikiLeaks - Vault 7: Projects: Highrise" (https://wikileaks.org/vault7/#Highrise). *wikileaks.org*. Retrieved 1 November 2018.
58. "WikiLeaks - Vault 7: Projects: UCL / Raytheon" (https://wikileaks.org/vault7/#UCL%20/%20Raytheon). *wikileaks.org*. Retrieved 1 November 2018.
59. "WikiLeaks - Vault 7: Projects: Imperial" (https://wikileaks.org/vault7/#Imperial). *wikileaks.org*. Retrieved 1 November 2018.
60. "WikiLeaks - Vault 7: Projects: Dumbo" (https://wikileaks.org/vault7/#Dumbo). *wikileaks.org*. Retrieved 1 November 2018.
61. "WikiLeaks - Vault 7: Projects: CouchPotato" (https://wikileaks.org/vault7/#CouchPotato). *wikileaks.org*. Retrieved 1 November 2018.
62. "WikiLeaks - Vault 7: Projects: ExpressLane" (https://wikileaks.org/vault7/#ExpressLane). *wikileaks.org*. Retrieved 1 November 2018.
63. "WikiLeaks - Vault 7: Projects: Angelfire" (https://wikileaks.org/vault7/#Angelfire). *wikileaks.org*. Retrieved 1 November 2018.

64. "WikiLeaks - Vault 7: Projects: Protego" (https://wikileaks.org/vault7/#Protego). *wikileaks.org*. Retrieved 1 November 2018.
65. Schwartz, Ian (16 March 2017). "Carlson To Trump: Why Not Gather Evidence, Confront Intelligence Agencies If You Were Wiretapped?" (http://www.realclearpolitics.com/video/2017/03/16/carlson_to_trump_why_not_gather_evidence_confront_intelligence_agencies_if_you_were_wiretapped.html). *RealClearPolitics*. Retrieved 16 March 2017.
66. Ross, Brian; Gordon Meek, James; Kreider, Randy; Kreutz, Liz (8 March 2017). "WikiLeaks docs allege CIA can hack smartphones, expose Frankfurt listening post" (https://abcnews.go.com/International/wikileaks-docs-allege-cia-hack-smartphones-exposes-frankfurt/story?id=45977302). ABC News.
67. Cody Derespina (7 March 2017). "WikiLeaks releases 'entire hacking capacity of the CIA'" (http://www.foxnews.com/us/2017/03/07/wikileaks-releases-entire-hacking-capacity-cia.html). *Fox News*. Retrieved 7 March 2017.
68. Carlson, Tucker (15 March 2017). "Trump: 'Wiretap covers a lot of different things'" (http://www.foxnews.com/on-air/tucker-carlson-tonight/index.html#/v/5361147496001). *Fox News*. p. (Video). Retrieved 16 March 2017.
69. Beavers, Olivia (16 March 2017). "Dem lawmaker: Trump might've leaked classified information" (http://thehill.com/policy/national-security/324313-dem-lawmaker-trump-mightve-leaked-classified-information). *The Hill*. Retrieved 16 March 2017.
70. Sherfinski, David (16 March 2017). "Adam Schiff: Trump might have disclosed classified info in TV interview" (https://www.washingtontimes.com/news/2017/mar/16/adam-schiff-donald-trump-might-have-disclosed-clas). *The Washington Times*.
71. Satter, Raphael (7 March 2017). "WikiLeaks publishes CIA trove alleging wide scale hacking" (https://www.boston.com/news/national-news/2017/03/07/wikileaks-publishes-cia-trove-alleging-wide-scale-hacking). *Boston.com*. Retrieved 7 March 2017.
72. Collins, Keith. "If You Only Work on Your Malware on Weekdays, You Might Be a CIA Hacker" (http://www.defenseone.com/technology/2017/04/if-you-only-work-your-malware-weekdays-you-might-be-cia-hacker/136923/). *Defense One*. Atlantic Media. Retrieved 15 April 2017.
73. "Longhorn: Tools used by cyberespionage group linked to Vault 7" (https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7). Symantec. Retrieved 15 April 2017.
74. Goetz, John; Obermaier, Frederik (7 March 2017). "Frankfurter US-Konsulat soll Spionagezentrale sein" (http://www.sueddeutsche.de/politik/wikileaks-frankfurter-us-generalkonsulat-soll-spionagezentrale-sein-1.3409364) [Frankfurt's US Consulate appears to be an espionage center]. *Süddeutsche Zeitung* (in German).
75. Dirk Hautkapp (9 March 2017). "Internet-Methoden der CIA enthüllt" (https://www.waz.de/politik/internet-methoden-der-cia-enthuellt-id209874865.html). *Westdeutsche Allgemeine Zeitung*. Retrieved 17 April 2017.
76. German Foreign Minister Gabriel fears new arms race with Russia (http://www.dw.com/en/german-foreign-minister-gabriel-fears-new-arms-race-with-russia/a-37863822), *Deutsche Welle*, 9 March 2017
77. Zetter, Kim. "WikiLeaks Files Show the CIA Repurposing Hacking Code To Save Time, Not To Frame Russia" (https://theintercept.com/2017/03/08/wikileaks-files-show-the-cia-repurposing-foreign-hacking-code-to-save-time-not-to-frame-russia/). *The Intercept*. Retrieved 9 March 2017.
78. "CIA false flag team repurposed Shamoon data wiper, other malware" (http://www.pcworld.com/art

78. "CIA false flag team repurposed Shamoon data wiper, other malware" (http://www.pcworld.com/article/3178365/security/cia-false-flag-team-repurposed-shamoon-data-wiper-other-malware.html). *PCWorld*. Retrieved 12 March 2017.
79. Cimpanu, Catalin. "Vault 7: CIA Borrowed Code from Public Malware" (https://www.bleepingcomputer.com/news/security/vault-7-cia-borrowed-code-from-public-malware/). *Bleeping Computer*. Retrieved 8 March 2017.
80. 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" (http://www.businessinsider.com/sean-hannity-wikileaks-conspiracy-theory-cia-hacked-2017-3). *Business Insider*. Retrieved 12 March 2017.
81. Blake, Aaron. "Analysis - The dangerous and irresistible GOP conspiracy theory that explains away Trump's Russia problem" (https://www.washingtonpost.com/news/the-fix/wp/2017/03/10/the-dangerous-and-irresistible-gop-conspiracy-theory-that-explains-away-trumps-russia-problem/). *The Washington Post*. Retrieved 12 March 2017.
82. Buchanan, Ben (9 March 2017). "WikiLeaks doesn't raise doubts about who hacked the DNC. We still know it was Russia" (https://www.washingtonpost.com/opinions/russia-likely-hacked-the-dnc-and-new-wikileaks-revelations-strengthen-the-case/2017/03/09/e5fe55e8-04d6-11e7-b1e9-a05d3c21f7cf_story.html). *The Washington Post*. Retrieved 12 March 2017.
83. Jacques Cheminat: Marble Framework: le double jeu perfide des hackers de la CIA (http://www.silicon.fr/marble-framework-le-double-jeu-perfide-sur-le-hacking-de-la-cia-171177.html), *silicon.fr*, 31 March 2017
84. Stefania Maurizi: WikiLeaks, così la Cia depista i raid nei computer: svelato il 'Marble Framework' (http://www.repubblica.it/esteri/2017/03/31/news/wikileaks_usa_cia_spionaggio_depistaggio-161859197/), *La Repubblica*, 31 March 2017
85. Jean-Marc Manach: WikiLeaks joue à cache-cache avec la CIA (http://www.liberation.fr/futurs/2017/03/31/wikileaks-joue-a-cache-cache-avec-la-cia_1559706), Libération, 31 March 2017
86. Cimpanu, Catalin (1 April 2017). "WikiLeaks Dumps Source Code of CIA Tool Called Marble" (https://www.bleepingcomputer.com/news/government/wikileaks-dumps-source-code-of-cia-tool-called-marble/). *Bleeping Computer*. Retrieved 3 April 2017.
87. Sam Varghese: WikiLeaks releases third tranche of CIA files (http://www.itwire.com/security/77508-wikileaks-releases-third-tranche-of-cia-files.html), *iTWire', 1 April 2017*
88. Dwilson, Stephanie Dube (31 March 2017). "WikiLeaks Vault 7 Part 3 Reveals CIA Tool Might Mask Hacks as Russian, Chinese, Arabic" (http://heavy.com/tech/2017/03/wikileaks-vault-7-part-3-marble-cia-tool-to-mask-hacks-hacking-russian-chinese-arabic-decoy-languages-attribute/). *Heavy.com*. Retrieved 31 March 2017.
89. John Leyden: WikiLeaks exposes CIA anti-forensics tool that makes Uncle Sam seem fluent in enemy tongues (https://www.theregister.co.uk/2017/03/31/wikileaks_cia/), The Register, 31 March 2017
90. Uchill, Joe (31 March 2017). "WikiLeaks' latest leak shows how CIA avoids antivirus programs" (http://thehill.com/policy/cybersecurity/326691-wikileaks-newest-cia-source-code-leak-shows-how-cia-avoids-anti-virus). *The Hill*. Retrieved 31 March 2017.
91. The Washington Post: WikiLeaks' latest release of CIA cyber-tools could blow the cover on agency hacking operations (https://www.washingtonpost.com/world/national-security/wikileaks-latest-release-of-cia-cyber-tools-could-blow-the-cover-on-agency-hacking-operations/2017/03/31/63fc3616-1636-11e7-833c-503e1f6394c9_story.html), *The Washington Post*, 31 March 2017

92. Wikileaks releases code that could unmask CIA hacking operations (https://arstechnica.com/security/2017/04/wikileaks-releases-code-that-could-unmask-cia-hacking-operations/), *Ars Technica*, 2 April 2017
93. "HammerDrill v2.0" (https://wikileaks.org/ciav7p1/cms/page_17072172.html). *wikileaks.org*. Retrieved 19 March 2017.
94. "Weeping Angel, Brutal Kangaroo and other secret CIA code names from the Wikileaks surveillance leak" (http://www.recode.net/2017/3/7/14846926/cia-code-names-surveillance-wikileaks). *www.recode.net*. Retrieved 19 March 2017.
95. McCormick, Rich (8 March 2017). "Apple says it's already patched 'many' iOS vulnerabilities identified in WikiLeaks' CIA dump" (https://www.theverge.com/2017/3/8/14851266/apple-patch-wikileaks-cia-dump-ios). *The Verge*. Retrieved 8 March 2017.
96. Releases Dark Matter (https://wikileaks.org/vault7/darkmatter/releases), *WikiLeaks*, 23 March 2017
97. WikiLeaks CIA files: New 'Dark Matter' release details how US 'hacked into Apple products' (https://www.independent.co.uk/life-style/gadgets-and-tech/news/wikileaks-cia-dark-matter-hacking-leak-apple-iphone-ipad-new-vault-7-files-latest-a7646751.html), *The Independent*, 23 March 2017
98. Uchill, Joe (23 March 2017). "Apple: Security vulnerabilities revealed by WikiLeaks no longer work" (http://thehill.com/business-a-lobbying/325579-apple-new-wikileaked-vulnerabilities-no-longer-work). *The Hill*. Retrieved 24 March 2017.
99. Gallagher, Sean (23 March 2017). "New WikiLeaks dump: The CIA built Thunderbolt exploit, implants to target Macs" (https://arstechnica.com/security/2017/03/new-wikileaks-dump-the-cia-built-thunderbolt-exploit-implants-to-target-macs/). *Ars Technica*. Retrieved 24 March 2017.
00. https://twitter.com/wikileaks/status/843573087950069764
01. http://www.securityweek.com/cisco-finds-zero-day-vulnerability-vault-7-leak
02. Joseph Menn: A scramble at Cisco exposes uncomfortable truths about U.S. cyber defense (https://www.reuters.com/article/us-usa-cyber-defense-idUSKBN17013U), Reuters, 29. March 2017
03. Goodin, Dan (20 March 2017). "A simple command allows the CIA to commandeer 318 models of Cisco switches" (https://arstechnica.com/security/2017/03/a-simple-command-allows-the-cia-to-commandeer-318-models-of-cisco-switches/). *Ars Technica*. Retrieved 21 March 2017.
04. Barrett, Brian (7 March 2017). "The CIA Can't Crack Signal and WhatsApp Encryption, No Matter What You've Heard" (https://www.wired.com/2017/03/wikileaks-cia-hack-signal-encrypted-chat-apps/). Wired. Retrieved 8 March 2017.
05. Glaser, April (7 March 2017). "WikiLeaks Reveals The CIA Hacked Into Apple IPhones" (http://www.recode.net/2017/3/7/14843494/wikileaks-cia-hacked-apple-iphone-google-androidsamsung). *ReCode*. Retrieved 17 March 2017.
06. "WikiLeaks 'Vault 7' dump reignites conspiracy theories surrounding death of Michael Hastings" (http://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=11814476). *The New Zealand Herald*. 8 March 2017. Retrieved 8 March 2017.
07. Prince, S. J. (7 March 2017). "WikiLeaks Vault 7 Conspiracy: Michael Hastings Assassinated by CIA Remote Car Hack?" (http://heavy.com/news/2017/03/wikileaks-vault-7-remote-car-hack-assassination-michael-hastings-conspiracy/). *Heavy.com*. Retrieved 8 March 2017.
08. "Notepad++ Fix CIA Hacking Issue" (https://notepad-plus-plus.org/news/notepad-7.3.3-fix-cia-hacking-issue.html). *notepad-plus-plus.org*. Retrieved 10 March 2017.
09. @Snowden (7 March 2017). "The CIA reports show the USG ..." (https://twitter.com/Snowden/stat

us/839171129331830784) (Tweet). Retrieved 8 March 2017 – via Twitter.
10. "Alleged CIA documents show urgent need to limit government hacking – Access Now" (https://www.accessnow.org/alleged-cia-documents-highlight-urgent-need-limits-government-hacking/). Access Now. 7 March 2017. Retrieved 8 March 2017.
11. Mathews, Lee. "WikiLeaks Vault 7 CIA Dump Offers Nothing But Old News" (https://www.forbes.com/sites/leemathews/2017/03/08/the-wikileaks-vault-7-cia-dump-shouldnt-terrify-you/). *Forbes*. Retrieved 9 March 2017.
12. Hern, Alex (8 March 2017). " 'Am I at risk of being hacked?' What you need to know about the 'Vault 7' documents" (https://www.theguardian.com/technology/2017/mar/08/wikileaks-vault-7-cia-documents-hacked-what-you-need-to-know). *The Guardian*. Retrieved 11 March 2017.
13. Hern, Alex (8 March 2017). "Apple to 'rapidly address' any security holes as companies respond to CIA leak" (https://www.theguardian.com/technology/2017/mar/08/wikileaks-cia-leak-apple-vault-7-documents). *The Guardian*. Retrieved 11 March 2017.
14. Domonoske, Camila; Myre, Greg. "The CIA Document Dump Isn't Exactly Snowden 2.0. Here's Why" (https://www.npr.org/sections/thetwo-way/2017/03/08/519205172/the-cia-document-dump-isn-t-exactly-snowden-2-0-here-s-why). *NPR*. Retrieved 15 March 2017.
15. "Privacy experts say the CIA left Americans open to cyber attacks" (http://www.newsweek.com/privacy-experts-cia-americans-open-cyber-attacks-580659). Newsweek. 8 April 2017. Retrieved 9 April 2017.
16. Riotta, Chris (24 March 2017). "Is Privacy Real? The CIA Is Jeopardizing America's Digital Security, Experts Warn" (http://www.ibtimes.com/privacy-real-cia-jeopardizing-americas-digital-security-experts-warn-2514062). *International Business Times*. Retrieved 9 April 2017.
17. Whittaker, Zack (9 March 2017). "After CIA leaks, tech giants scramble to patch security flaws" (https://www.zdnet.com/article/tech-giants-scramble-for-cia-hacking-fixes-most-flaws-patched/). *ZDNet*. Retrieved 9 April 2017.
18. Olivia Solon: With the latest WikiLeaks revelations about the CIA – is privacy really dead? (https://www.theguardian.com/world/2017/mar/09/with-the-latest-wikileaks-revelations-about-the-cia-is-privacy-really-dead), The Guardian, 8 March 2017
19. 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" (https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/). *Microsoft*. Retrieved 17 May 2017.

External links

- Vault 7 at WikiLeaks (https://wikileaks.org/ciav7p1/)
- Julian Assange Press Conference and Q&A on CIA/Vault7/YearZero (https://www.youtube.com/watch?v=Se6XWhKOE2Q), Thursday 9 March 2017, the official WikiLeaks YouTube channel