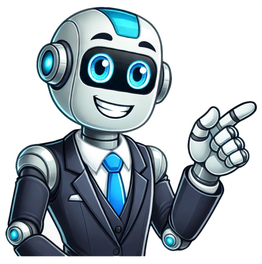
Click to prove you're human



Vault 7 est une série de documents que WikiLeaks a commencé à publier le 7 mars 2017, qui détaille des activités de la Central Intelligence Agency (CIA) dans le domaine de la surveillance électronique et de la cyberguerre. Vault 7 Publication 7 mars 2017 Éditeurs clés WikiLeaks Objet Surveillance de masse aux États-Unis (en)Cyberguerre Personnes et entités impliquées Central Intelligence Agency Site web wikileaks.org/ciav7p1 modifier La première publication, nommée Year Zero[1], est formée de 8 761 documents, supposément issus du Center for Cyber Intelligence[2],[3]. Les fichiers, datés de 2013 à 2016, comportent des détails sur les fonctionnalités des logiciels de l'agence, telles que la possibilité de compromettre des télévisions connectées, des navigateurs web (y compris Firefox, Google Chrome et Microsoft Edge), et les systèmes d'exploitation de la plupart des smartphones (y compris iOS d'Apple et Android de Google) et ordinateurs (notamment Windows, macOS et Linux). Par la suite, WikiLeaks publie régulièrement de nouveaux documents traitant d'une méthode ou d'un outil en particulier. Ainsi, Dark Matter[4], parue le 23 mars 2017, révèle comment la CIA a pu pirater des produits Apple. Le 31 mars, Marble Framework[5] indique les outils qu'utilise l'Agence pour masquer et brouiller les pistes après une attaque informatique. Grasshopper Framework, publié le 5 avril, est une « trousse à outils » modulaire pour infecter des ordinateurs sous Microsoft Windows[6],[7] Wikileaks a commencé à parler de « Vault 7 » au début du mois de février 2017 à travers une série de tweets énigmatiques[8]. Le 16 février 2017, Wikileaks publie des documents de la CIA décrivant comment celle-ci surveille l'élection présidentielle française de 2012[9]. Les articles de presse au sujet de cette révélation indiquent que la publication a eu lieu « en vue de la série Vault 7 de la CIA à venir »[10]. Le 8 mars 2017, les autorités américaines chargées des services de renseignements américains et de la justice ont indiqué à l'agence de presse internationale Reuters qu'ils sont au courant d'une faille de sécurité à la CIA, qui a conduit à Vault 7 depuis la fin 2016. Les deux représentants ont dit qu'ils s'orientent vers les « contractuels » en tant que source la plus plausible de la fuite[11]. Le premier lot de documents diffusé se composait de 7 818 pages web comprenant 943 pièces jointes, supposément issues du Centre for Cyber Intelligence[12], qui contient déjà plusieurs pages de la publication de documents de la NSA par Edward Snowden[13]. WikiLeaks n'a pas donné le nom de la source, mais a indiqué que les dossiers avaient « circulé entre des hackeurs de l'ancien gouvernement des États-Unis et des entrepreneurs de manière non autorisée, l'un d'eux ayant fourni à WikiLeaks une partie des archives ». Selon WikiLeaks, la source « souhaite lancer un débat public sur la sécurité, la création, l'utilisation, la prolifération et le contrôle démocratique de cyberarmes » puisque ces outils ont soulevé des questions qui « ont urgemment besoin d'être débattues en public, notamment le fait que les capacités d'intrusion de la CIA dépassent son mandat et le problème de la supervision publique de l'agence ». WikiLeaks a caviardé les noms et d'autres informations d'identification des documents avant leur publication, tout en essayant de permettre des liens entre les personnes pouvant être repérées via des identificateurs uniques générés par WikiLeaks[14]. Il a aussi été indiqué qu'il allait reporter la publication du code source des cyberarmes, qui serait composé de plusieurs centaines de millions de lignes, « jusqu'à ce qu'un consensus émerge sur la nature technique et politique du programme de la CIA et la manière dont ces « armes » devraient être analysées, désarmées et publiées ». Le fondateur de WikiLeaks, Julian Assange, a affirmé que ce n'était qu'une partie d'une grande série, en disant : « Vault 7 est la publication la plus complète de fichiers d'espionnage américain jamais rendus publique ». Le 8 mars 2017, des représentants du renseignement et de la justice américaine ont déclaré à l'agence de presse internationale Reuters qu'ils étaient au courant des problèmes de sécurité de la CIA, qui ont conduit à Vault 7 depuis la fin 2016. Les deux fonctionnaires ont dit qu'ils se sont concentrés sur les « entrepreneurs » comme la source la plus vraisemblable de la fuite[15]. La CIA a publié une déclaration disant « Le peuple américain devrait être profondément troublé par toute divulgation de WikiLeaks conçue pour endommager les capacités de la communauté du renseignement à protéger l'Amérique contre des terroristes ou d'autres adversaires. De telles divulgations ne mettent pas seulement en péril le personnel et les opérations américains, mais aussi équipent nos adversaires avec des outils et des informations pour nous faire du tort[16] ». Quand il a été interrogé sur l'authenticité des documents, le porte-parole de la CIA et ancien directeur du renseignement national Michael Hayden a répondu que l'organisation n'a « pas de commentaire à faire sur l'authenticité ou le contenu des prétendus documents issus du renseignement »[17], mais, s'exprimant sous couvert de l'anonymat, des responsables actuels et anciens du renseignement ont déclaré que les documents semblent authentiques[18]. Selon Edward Snowden, ancien employé de la NSA et lanceur d'alerte, les documents « semblent authentiques ». Robert M. Chesney, professeur de droit à l'université du Texas et directeur du programme de politique publique et de la technologie au Center for Strategic and International Studies (CSIS), a comparé Vault 7 aux outils de piratage de la NSA divulgués en 2016 par un groupe se faisant appeler The Shadow Brokers. Les outils électroniques pourraient compromettre à la fois les systèmes d'exploitation iOS d'Apple et Android de Google. En ajoutant des logiciels malveillants sur le système d'exploitation Android, l'agence peut avoir accès aux communications sécurisées d'un appareil[19]. Apple a déclaré que « la plupart des problèmes publiés aujourd'hui ont déjà été corrigé dans le dernier iOS » et que la compagnie « va continuer à travailler pour répondre rapidement à toutes les vulnérabilités identifiées[20] ». Selon WikiLeaks, une fois qu'un smartphone Android a été infiltré, l'agence peut collecter le « trafic audio et textuel avant que le chiffrement ne soit appliqué ». Certains logiciels de l'agence seraient en mesure d'accéder à des messages envoyés par les services de messagerie instantanée. Cette méthode de consultation des messages diffère de l'obtention de l'accès par le décryptage de messages déjà chiffrés, ce qui n'a pas encore été signalé. Bien que le chiffrement des services de messagerie sécurisés qui offrent le chiffrement de bout en bout, tel que le Telegram, WhatsApp et Signal, n'a pas été signalé comme étant craqué, leur chiffrement peut être contourné en capturant l'entrée avant que le chiffrement ne soit appliqué, par des méthodes tel qu'un enregistrement de frappe ou de la saisie tactile par l'utilisateur. Un document montrerait que la CIA a recherché des moyens pour infecter les systèmes de contrôle de véhicule. WikiLeaks a déclaré « le but de ce contrôle n'est pas indiqué, mais il permettrait à la CIA de s'engager dans des assassinats presque indétectable[21] ». Cette déclaration a apporté un regain d'attention pour les théories du complot entourant la mort du journaliste Michael Hastings[22]. L'une des suites logicielles, dont le nom de code serait « Weeping Angel » (« ange qui pleure »), est annoncée comme étant en mesure d'utiliser les téléviseurs connectés de Samsung comme des dispositifs d'écoute secrets. En juin 2014, la CIA. avec les services de renseignement britanniques du MI5 a organisé un atelier commun pour améliorer le code « Weeping Angel », qui semble avoir particulièrement ciblé les téléviseurs Samsung de la série F8000 sortis en 2013. Il permettrait à un téléviseur connecté infecté d'être utilisé « comme un mouchard, enregistrant les conversations de la pièce et de les envoyer sur internet sur un serveur secret de la CIA.», même si elle semble être éteinte. Les documents font référence à une faille « injection de DLL FAX de Windows » exploitée dans les systèmes d'exploitation Windows XP, Windows Vista et Windows 7. Cela permettrait à un utilisateur malveillant de tenter de cacher ses logiciels malveillants dans la DLL d'une autre application. Cependant, un ordinateur doit déjà avoir été compromis par une autre méthode pour que l'injection puisse avoir lieu[23]. Les fuites ont également révélé que le code de copier-coller permettait une élévation des privilèges dans un environnement Windows 7. Ce code permet de contourner la fenêtre User Account Control (UAC), qui s'affiche lorsqu'un programme tente de s'exécuter avec des privilèges administrateur, sans que l'utilisateur en ait connaissance[24]. Le code de copier-coller qui était inclus dans les fuites permet l'exploitation des systèmes utilisant un système de démarrage UEFI en modifiant le noyau du système d'exploitation qui est chargé en mémoire vive avant la sortie de la séquence d'amorçage UEFI. Le code de copier-coller permet à un attaquant d'insérer un hook personnalisé qui peut être utilisé pour modifier arbitrairement le noyau du système d'exploitation en mémoire immédiatement avant que le contrôle de l'exécution ne soit confiée au noyau[25]. Le 31 mars 2017, WikiLeaks révèle 676 fichiers de code source d'un framework (c'est-à-dire un ensemble d'outils et de composants logiciels à la base d'un logiciel) baptisé Marble. Celui-ci est utilisé pour empêcher les enquêteurs et les sociétés d'antivirus d'attribuer des virus, des chevaux de Troie et des attaques à la CIA[26]. Marble fait cela grâce à la technique d'offuscation, en insérant des fragments de texte en anglais mais aussi en chinois, russe, coréen, arabe et farsi (principale langue parlée en Iran). Le but est d'amener les enquêteurs à attribuer le code à d'autres attaquants, par exemple en considérant que la langue du créateur du logiciel malveillant n'est pas l'anglais américain, mais le chinois puis en feignant de vouloir dissimuler l'utilisation du chinois, attirant les enquêteurs encore plus fortement vers une mauvaise conclusion[27]. Marble était utilisé par l'Agence en 2016. Il a atteint sa version 1.0 en 2015. Le framework Marble est utilisé uniquement pour l'offuscation et ne contient pas de vulnérabilité ou d'exploit en lui-même[26] Le 23 mars 2017, WikiLeaks dévoile la documentation de plusieurs projets de la CIA ayant pour but d'infecter le firmware des Macs d'Apple (ce qui signifie que l'infection persiste même si le système d'exploitation est réinstallé) et développée par le service « Embedded Development Branch » (EDB) de l'agence. Ces documents expliquent les techniques utilisées par la CIA pour gagner de la « persistance » sur les appareils Apple[28]. Le projet « Sonic Screwdriver », par exemple, permet à un attaquant, à partir d'un firmware modifié d'un adaptateur Apple Thunderbolt vers Ethernet, de prendre le contrôle d'un ordinateur de bureau ou portable Mac pendant qu'il démarre et même si ce dernier est protégé par un mot de passe[29]. Le manuel de « NightSkies » indique que ce programme malveillant s'attaquant aux données de l'utilisateur était déjà à sa version 1.2 en 2008 (soit un an après la sortie du premier iPhone), et expressément conçu pour être physiquement installé sur les iPhones fraîchement sortie d'usine[30]. D'après WikiLeaks, il est probable que la plupart des attaques physiques de la CIA contre les produits Apple ont infecté directement les chaines d'approvisionnement de l'organisation ciblée, en interceptant les ventes par correspondances et les envois postaux (en ouvrant les colis, infectant les appareils, et renvoyant le colis) partant des États-Unis ou autre autrement[28]. Apple précise qu'au moment de la révélation de ces documents, la plupart des failles décrites ont été corrigées et ne sont plus exploitables dans les appareils de la marque[31]. (en) Cet article est partiellement ou en totalité issu de l'article de Wikipédia en anglais intitulé « Vault 7 » (voir la liste des auteurs). ↑ « Ce que l'on sait des méthodes d'espionnage de la CIA », sur liberation.fr, 8 mars 2017. ↑ (en) « WikiLeaks posts alleged CIA trove depicting mass hacking », CBS News/Associated Press, sur CBS News, 7 mars 2017 (consulté le 7 mars 2017) ↑ (en) « WikiLeaks publishes 'biggest ever leak of secret CIA documents' », sur theguardian.com, 7 mars 2017. ↑ (en) Aaron Mamiit, « WikiLeaks Exposes CIA Tools Targeting MacBooks And iPhones: Here's What They Do », sur techtimes.com, 24 mars 2017 (consulté le 5 juin 2023). ↑ (en) Ellen Nakashima, « WikiLeaks' latest release of CIA cyber-tools could blow the cover on agency hacking operations », sur Washington Post, 31 mars 2017 (consulté le 5 juin 2023). ↑ (en) Bruce Schneier, « Fourth WikiLeaks CIA Attack Tool Dump », sur schneier.com, 10 avril 2017 (consulté le 5 juin 2023) ↑ (en) Dan Goodin, « WikiLeaks just dropped the CIA's secret how-to for infecting Windows », sur Ars Technica, 7 avril 2017 (consulté le 5 juin 2023). ↑ (en) Stephanie Dube Dwilson, « What Is Vault 7 on WikiLeaks? », 7 février 2017 (consulté le 18 juin 2017). ↑ (en) Kevin Poulsen, « Russia Turns WikiLeaks CIA Dump Into Disinformation », The Daily Beast, 8 mars 2017 (consulté le 18 juin 2017). ↑ (en) « CIA espionage orders for the 2012 French presidential election », WikiLeaks, 16 février 2017 (consulté le 18 juin 2017). ↑ (en) « U.S intel, law enforcement officials aware of CIA breach since late last year », Reuters, 8 mars 2017. ↑ (en) Associated Press, « WikiLeaks claims to release thousands of CIA documents », CBS News, 7 mars 2017 (lire en ligne, consulté le 7 mars 2017) ↑ (en) « WikiLeaks publishes massive trove of CIA spying files in 'Vault 7' release », The Independent, 7 mars 2017 (consulté le 7 mars 2017). ↑ (en) « Vault7 - Home », WikiLeaks (consulté le 10 mars 2017), "Redactions" section ↑ (en) Reuters, « U.S intel, law enforcement officials aware of CIA breach since late last year », 8 mars 2017 ↑ (en) Jeremy Berke, « CIA: Americans 'should be deeply troubled' by WikiLeaks' disclosure », Business Insider, 8 mars 2017 (consulté le 10 mars 2017) ↑ (en) Scott Shane, Mark Mazzetti et Matthew Rosenberg, « WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents », The New York Times, 7 mars 2017 (lire en ligne, consulté le 7 mars 2017). ↑ (en) Brian Ross, James Gordon Meek, Randy Kreider et Liz Kreutz, « WikiLeaks docs allege CIA can hack smartphones, expose Frankfurt listening post », ABC News, 8 mars 2017. ↑ (en) Brian Barrett, « The CIA Can't Crack Signal and WhatsApp Encryption, No Matter What You've Heard », Wired, 7 mars 2017 (consulté le 8 mars 2017) ↑ (en) Rich McCormick, « Apple says it's already patched 'many' iOS vulnerabilities identified in WikiLeaks' CIA dump », The Verge, 8 mars 2017 (consulté le 8 mars 2017) ↑ (en) « WikiLeaks 'Vault 7' dump reignites conspiracy theories surrounding death of Michael Hastings », The New Zealand Herald, 8 mars 2017 (consulté le 8 mars 2017) ↑ (en) S. J. Prince, « WikiLeaks Vault 7 Conspiracy: Michael Hastings Assassinated by CIA Remote Car Hack? », sur Heavy.com, 7 mars 2017 (consulté le 8 mars 2017). ↑ (en) « Notepad++ Fix CIA Hacking Issue », sur notepad-plus-plus.org (consulté le 10 mars 2017). ↑ (en) « Elevated COM Object UAC Bypass (WIN 7) ». ↑ (en) « ExitBootServices Hooking », WikiLeaks. ↑ a et b (en) « Vault 7: Projects, Marble Framework », sur WikiLeaks, 31 mars 2017 (consulté le 2 avril 2017). ↑ (en) « Vault 7: Documents, Marble Framework », sur wikileaks.org, 31 mars 2017 (consulté le 2 avril 2017). ↑ a et b (en) « Vault 7: Projects, Dark Matter », sur WikiLeaks, 23 mars 2017 (consulté le 1er avril 2017). ↑ (en) « Vault 7: Projects, Sonic Screwdriver », sur wikileaks.org, 23 mars 2017 (consulté le 1er avril 2017) ↑ (en) « Vault 7: Projects, NightSkies v1.2 - User Guide », sur wikileaks.org, 23 mars 2017 (consulté le 1er avril 2017) ↑ « Vault7 - Apple assure avoir corrigé « bon nombre » des failles exploitées par la CIA », 8 mars 2017 (en) « Vault 7: CIA Hacking Tools Revealed », sur wikileaks.org (consulté le 11 mars 2017).   Portail du renseignement   Portail de la sécurité de l'information   Portail des États-Unis   Portail des années 2010 Ce document provient de « . Chaque soir, le JDD vous présente les infos dont vous allez entendre parler le lendemain : le déplacement d'Emmanuel Macron au Conseil européen à Bruxelles ; la niche parlementaire de l'UDR à l'Assemblée ; le concert en hommage aux victimes du festival Nova en Israël ; le brevet des collèges... À New York, Zohran Mamdani a suscité la surprise. Ce socialiste musulman et propalestinien de 33 ans a remporté contre toute attente la primaire démocrate, devançant l'ancien gouverneur de l'État de New York, Andrew Cuomo. « Une excellente nouvelle » pour Jean-Luc Mélenchon. CHRONIQUE. Trump n'a pas attendu que la diplomatie échoue : il a frappé. En ciblant les sites nucléaires iraniens, le locataire de la Maison-Blanche assume une vision sans complexes de la puissance des États-Unis. Et prouve que la force seule peut s'imposer aux tyrans. Une centaine d'activistes propalestiniens se sont introduits dans les locaux de l'entreprise OIP Land Systems à Tournai, en Belgique, et ont détruit des véhicules militaires. Ces blindés étaient destinés à l'Ukraine, dans le cadre de sa guerre contre la Russie. Le préjudice est estimé à un million d'euros. Sur Truth Social, le président américain a révélé un message de félicitations écrit par le chef de l'OTAN, Mark Rutte, qui salue son action en Iran et son rôle dans le renforcement des dépenses de défense européennes. L'objectif d'Israël et des Etats-Unis est clairement affiché : faire tomber le régime des mollahs. Mais pour mettre qui à la place ? Aucun leader suffisamment légitime n'existe. La situation dans le pays pourrait bien tourner à la guerre civile. Les juges ont estimé que Joshua Schulte avait fait fuiter des milliers d'informations par esprit de vengeance, non pas souhait de transparence.Par J.Cl. Les informations collectées par Joshua Schulte avaient été révélées par Wikileaks, l'organisation de Julian Assange, révélant l'arsenal cyber de la CIA. AFP/Saul LoebIl avait déjà été condamné, restait à fixer sa peine. Un ancien ingénieur logiciel de la Central Intelligence Agency (CIA) américaine qui avait été reconnu coupable d'avoir commis le plus grand vol d'informations classifiées de l'histoire de l'agence a été condamné jeudi soir à 40 ans de prison. Dans une lettre d'accusation de 24 pages, les procureurs fédéraux réclamaient une peine d'emprisonnement à vie pour piratage informatique, crime d'espionnage et le fait d'avoir possédé de nombreux contenus pédopornographiques. Le juge de district américain Jesse Furman a estimé que 480 mois de prison - 400 pour sa participation au scandale WikiLeaks, 80 pour la pédopornographie - représentaient une juste peine pour Joshua Schulte. Il est en détention depuis son arrestation en août 2017 à Manhattan et Brooklyn et dénonce des conditions de détention proches du « nazisme », au titre desquelles son avocat demandait neuf ans d'emprisonnement suivis de cinq ans de liberté surveillée.L'informaticien, aujourd'hui âgé de 35 ans, a travaillé pour la CIA de 2010 à 2015. Il a remis à WikiLeaks un ensemble de documents connus sous le nom de Vault 7, « l'une des violations les plus odieuses et les plus effrontées de la loi sur l'espionnage de l'histoire des États-Unis » selon les procureurs. Vault 7 détaillait l'arsenal de cybersurveillance de la CIA, qui travaillait à placer des logiciels de piratage et des virus informatiques dans les téléviseurs reliés à Internet, dans les navigateurs web les plus couramment utilisés, les systèmes d'exploitation des smartphones, mais aussi dans les voitures.WikiLeaks avait publié 8 761 documents en mars 2017, pour « lancer un débat public sur la sécurité, la création, l'utilisation, la prolifération et le contrôle démocratique des cyberarmes », avait à l'époque déclaré WikiLeaks, conscient de donner aux hackers du monde entier les mêmes outils que les agents du renseignement américain.Quelques années après les fuites - dont Schulte n'est pas à l'origine - qui avaient montré comment et avec quelle ampleur les États-Unis espionnaient leurs alliés, notamment la France, par le biais de leurs « grandes oreilles », ces nouvelles révélations avaient plongé Washington dans l'embarras.La CIA a accusé son ancien geek d'avoir « mis directement en danger le personnel, les programmes et les biens de la CIA » et d'avoir « compromis la sécurité nationale des États-Unis ». L'effet des divulgations a été un « Pearl Harbor numérique », a comparé le juge Furman, se disant « époustouflé par l'absence totale de remords et d'acceptation de la responsabilité de M. Schulte ».Contrairement à Edward Snowden et Julian Assange, qui avaient agi par refus du secret, les procureurs ont accusé Schulte d'avoir transmis les documents pour se venger des supérieurs qui l'avaient réaffecté, avaient révoqué certains de ses privilèges informatiques et l'avaient critiqué pour son comportement de plus en plus obstiné.En septembre dernier, celui qui se faisait appeler « Kinetic Panda », « Voldemort » ou « Nuclear option » a aussi été reconnu coupable d'avoir consulté plus de 3 000 images et vidéos cryptées d'abus sexuels sur des enfants, conservées dans les recoins de sa soixantaine d'appareils électroniques.« Aujourd'hui, Joshua Schulte a été puni à juste titre non seulement pour sa trahison envers notre pays, mais aussi pour sa possession de matériel pédopornographique horrible », a déclaré James Smith, directeur adjoint du FBI, dans un communiqué publié à l'issue du prononcé de la sentence. « La gravité de ses actes est évidente, et la peine imposée reflète l'ampleur de la menace inquiétante et nuisible posée par son comportement criminel ». Après sa série Vault 7 lancée en mars 2017 sur les outils d'espionnage exfiltrés des murs de la CIA, WikiLeaks ouvre une nouvelle saison, Vault 8, consacrée au code source des applications de surveillance en question. « Cette publication permettra aux journalistes d'investigation, aux experts judiciaires et au grand public de mieux identifier et comprendre les composantes secrètes de l'infrastructure de la CIA », justifie la plateforme de Julian Assange pour les lanceurs d'alertes. Qui s'empresse de préciser qu'aucun des documents publiés ne contiennent de vulnérabilité 0-Day ou de faille de sécurité susceptible d'être re-exploitée par des tiers. La première révélation de Vault 8 porte sur Hive (ruche), un composant « majeur » de l'infrastructure de l'agence américaine du renseignement de contrôle de ses malware. Hive fournit en effet une plate-forme de communication entre les serveurs infectés (surveillés) et ceux de la CIA afin d'exfiltrer des informations mais aussi de recevoir des instructions. Et ce, sans que son éventuelle découverte puisse permettre de remonter jusqu'à l'agence de renseignement. Serveurs publics Schématiquement, Hive active de multiples opérations à partir de plusieurs implants sur les ordinateurs cibles, explique Wikileaks. Pour chaque opération, un domaine est créé. Domaine exécuté sur des serveurs loués auprès d'hébergeurs commerciaux en tant que VPS. Ces serveurs privés virtuels servent alors de relais avec les propres serveurs de la CIA (appelés « Blot ») hébergés derrière une connexion VPN (réseau virtuel privé). Toujours selon WikiLeaks, les domaines créés par la CIA offrent des contenus anodins susceptibles de n'inspirer aucune méfiance à un visiteur qui tomberait dessus (par hasard ou pas). A l'insu du visiteur, les sites Web leurres servent de passerelles pour propager des malware de la CIA, favorisant la connexion avec les serveurs Blot de l'agence de renseignement (et donc la collecte discrète de données). Faux certificats trompeurs Qui plus est, le code de Hive génère de faux certificats. Comme, par exemple, un certificat attribué à Kaspersky Lab et signé par Thawte Consulting. Ce qui oblige Kaspersky à prendre la parole pour se défendre sur Twitter. We've investigated the Vault 8 report and confirm the certificates in our name are fake. Our customers, private keys and services are safe and unaffected - Eugene Kaspersky (@e_kaspersky) 9 novembre 2017 « De cette façon, si l'organisation cible regarde le trafic réseau sortant de son réseau, elle tendra à attribuer l'exfiltration des données de la CIA à des entités non impliquées dont l'identité a été usurpée », affirme Wikileaks. Hive n'est pas sans faire penser à un autre malware, FuzzBunch, utilisé par la NSA dont les outils de hacking ont été dérobés par les Shadow Brokers. Avec le résultat que l'ont sait. Entre les mains de cybercriminels, les outils de l'agence nationale de la sécurité américaine se sont transformés en ransomware Wannacry et autre Petya. Même si WikiLeaks s'engage à ne publier du code sans 0-Day, le pire est à craindre avec la publication de la vingtaine d'outils précédemment inscrit dans la liste Vault 7. Lire également Vault 7 : WikiLeaks dans le rôle de l'arroseur arrosé Quand la CIA installait des spywares pour surveiller le FBI et la NSA Comment la CIA suit les PC à la trace à l'aide du Wifi Photo via Pixabay (CC0 Creative Commons) 15 June, 2017 Today, June 15th 2017, WikiLeaks publishes documents from the CherryBlossom project of the CIA that was developed and implemented with the help of the US nonprofit Stanford Research Institute (SRI International). CherryBlossom provides a means of monitoring the Internet activity of and performing software exploits on Targets of interest. In particular, CherryBlossom is focused on compromising wireless networking devices, such as wireless routers and access points (APs), to achieve these goals. Such Wi-Fi devices are commonly used as part of the Internet infrastructure in private homes, public spaces (bars, hotels or airports), small and medium sized companies as well as enterprise offices. Therefore these devices are the ideal spot for "Man-In-The-Middle" attacks, as they can easily monitor, control and manipulate the Internet traffic of connected users. By altering the data stream between the user and Internet services, the infected device can inject malicious content into the stream to exploit vulnerabilities in applications or the operating system on the computer of the targeted user. The wireless device itself is compromized by implanting a customized CherryBlossom firmware on it; some devices allow upgrading their firmware over a wireless link, so no physical access to the device is necessary for a successful infection. Once the new firmware on the device is flashed, the router or access point will become a so-called FlyTrap. A FlyTrap will beacon over the Internet to a Command & Control server referred to as the CherryTree. The beaconed information contains device status and security information that the CherryTree logs to a database. In response to this information, the CherryTree sends a Mission with operator-defined tasking. An operator can use CherryWeb, a browser-based user interface to view Flytrap status and security info, plan Mission tasking, view Mission-related data, and perform system administration tasks. Missions may include tasking on Targets to monitor, actions/exploits to perform on a Target, and instructions on when and how to send the next beacon. Tasks for a Flytrap include (among others) the scan for email addresses, chat usernames, MAC addresses and VoIP numbers in passing network traffic to trigger additional actions, the copying of the full network traffic of a Target, the redirection of a Target's browser (e.g., to Windex for browser exploitation) or the proxying of a Target's network connections. FlyTrap can also setup VPN tunnels to a CherryBlossom-owned VPN server to give an operator access to clients on the Flytrap's WLAN/LAN for further exploitation. When the Flytrap detects a Target, it will send an Alert to the CherryTree and commence any actions/exploits against the Target. The CherryTree logs Alerts to a database, and, potentially distributes Alert information to interested parties (via Catapult). Le site WikiLeaks avait publié 8.761 documents extrêmement sensibles en mars 2017 grâce à un homme : un informaticien de la CIA qui travaillait pour une unité d'élite spécialisée dans le cyberespionnage. Joshua Schulte, 35 ans, a été condamné jeudi à 40 ans de prison pour « la plus grave fuite de données » de l'histoire de l'agence américaine de renseignement, selon l'accusation.« Il a gravement nui à la sécurité nationale des Etats-Unis »« Joshua Schulte a trahi son pays en commettant l'un des actes d'espionnage les plus éhontés de l'histoire américaine », a commenté jeudi le procureur fédéral de New York Damian Williams dans un communiqué. « Il a gravement nui à la sécurité nationale des Etats-Unis et directement mis en danger les vies d'employés de la CIA, persistant dans son attitude même après son arrestation » en 2017, a affirmé le vice-ministre de la Justice chargé de la division Sécurité nationale, Matthew Olsen, cité dans le texte.En 2016, il avait commencé à rassembler la collection « Vault 7 », des outils de piratage, des logiciels malveillants et des virus informatiques. WikiLeaks avait commencé à les publier en mars 2017, embarrassant grandement l'agence et fournissant aux pirates professionnels et amateurs du monde entier les mêmes outils que les agents du renseignement américain.Un esprit de vengeance ?« La source souhaite lancer un débat public sur la sécurité, la création, l'utilisation, la prolifération et le contrôle démocratique des cyberarmes », avait à l'époque déclaré WikiLeaks. Mais l'accusation affirme que la motivation de Joshua Schulte était de se venger de la CIA, dont il reprochait à la direction de ne pas avoir pris son parti dans des conflits internes.Joshua Schulte a été reconnu coupable en juillet 2022 de huit chefs d'accusation d'espionnage. Il a également été reconnu coupable en septembre 2023 de détention de pédopornographie, une importante collection de vidéos ayant été découverte dans ses ordinateurs pendant une perquisition à son domicile. Contents • Press Release • Analysis • Examples • Frequently Asked Questions Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency. The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election. Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive. "Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones. Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force — its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities. By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified. In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons. Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike. Julian Assange, WikiLeaks editor stated that "There is an extreme proliferation risk in the development of cyber 'weapons'. Comparisons can be drawn between the uncontrolled proliferation of such 'weapons', which results from the inability to contain them combined with their high market value, and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective." Wikileaks has carefully reviewed the "Year Zero" disclosure and published substantive CIA documentation while avoiding the distribution of 'armed' cyberweapons until a consensus emerges on the technical and political nature of the CIA's program and how such 'weapons' should analyzed, disarmed and published. Wikileaks has also decided to redact and anonymise some identifying information in "Year Zero" for in depth analysis. These redactions include ten of thousands of CIA targets and attack machines throughout Latin America, Europe and the United States. While we are aware of the imperfect results of any approach chosen, we remain committed to our publishing model and note that the quantity of published pages in "Vault 7" part one ("Year Zero") already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks. CIA malware targets iPhone, Android, smart TVs CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA (see this organizational chart of the CIA for more details). The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide. The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization. The attack against Samsung smart TVs was developed in cooperation with the United Kingdom's MI5/BTSS. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server. As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks. The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations. The CIA's Mobile Devices Branch (MDB) developed numerous attacks to remotely hack and control popular smart phones. Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone. Despite iPhone's minority share (14.5%) of the global smart phone market in 2016, a specialized unit in the CIA's Mobile Development Branch produces malware to infest, control and exfiltrate data from iPhones and other Apple products running iOS, such as iPads. CIA's arsenal includes numerous local and remote "zero days" developed by CIA or obtained from GCHQ, NSA, FBI or purchased from cyber arms contractors such as Baitshop. The disproportionate focus on iOS may be explained by the popularity of the iPhone among social, political, diplomatic and business elites. A similar unit targets Google's Android which is used to run the majority of the world's smart phones (~85%) including Samsung, HTC and Sony. 1.15 billion Android powered phones were sold last year. "Year Zero" shows that as of 2016 the CIA had 24 "weaponized" Android "zero days" which it has developed itself and obtained from GCHQ, NSA and cyber arms contractors. These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is applied. CIA malware targets Windows, OSx, Linux, routers The CIA also runs a very substantial effort to infect and control Microsoft Windows users with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" which infects software distributed on CD/DVDs, infectors for removable media such as USBs, systems to hide data in images or in covert disk areas ("Brutal Kangaroo") and to keep its malware infestations going. Many of these infection efforts are pulled together by the CIA's Automated Implant Branch (AIB), which has developed several attack systems for automated infestation and control of CIA malware, such as "Assassin" and "Medusa". Attacks against Internet infrastructure and webservers are developed by the CIA's Network Devices Branch (NDB). The CIA has developed automated multi-platform malware attack and control systems covering Windows, Mac OS X, Solaris, Linux and more, such as EDB's "HIVE" and the related "Cutthroat" and "Swindle" tools, which are described in the examples section below. CIA 'hoarded' vulnerabilities ("zero days") In the wake of Edward Snowden's leaks about the NSA, the U.S. technology industry secured a commitment from the Obama administration that the executive would disclose on an ongoing basis — rather than hoard — serious vulnerabilities, exploits, bugs or "zero days" to Apple, Google, Microsoft, and other US-based manufacturers. Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others. The U.S. government's commitment to the Vulnerabilities Equities Process came after significant lobbying by US technology companies, who risk losing their share of the global market over real and perceived hidden vulnerabilities. The government stated that it would disclose all pervasive vulnerabilities discovered after 2010 on an ongoing basis. "Year Zero" documents show that the CIA breached the Obama administration's commitments. Many of the vulnerabilities used in the CIA's cyber arsenal are pervasive and some may already have been found by rival intelligence agencies or cyber criminals. As an example, specific CIA malware revealed in "Year Zero" is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter accounts. The CIA attacks this software by using undisclosed security vulnerabilities ("zero days") possessed by the CIA but if the CIA can hack these phones then so can everyone else who has obtained or discovered the vulnerability. As long as the CIA keeps these vulnerabilities concealed from Apple and Google (who make the phones) they will not be fixed, and the phones will remain hackable. The same vulnerabilities exist for the population at large, including the U.S. Cabinet, Congress, top CEOs, system administrators, security officers and engineers. By hiding these security flaws from manufacturers like Apple and Google the CIA ensures that it can hack everyone &mdsh; at the expense of leaving everyone hackable. 'Cyberwar' programs are a serious proliferation risk Cyber 'weapons' are not possible to keep under effective control. While nuclear proliferation has been restrained by the enormous costs and visible infrastructure involved in assembling enough fissile material to produce a critical nuclear mass, cyber 'weapons', once developed, are very hard to retain. Cyber 'weapons' are in fact just computer programs which can be pirated like any other. Since they are entirely comprised of information they can be copied quickly with no marginal cost. Securing such 'weapons' is particularly difficult since the same people who develop and use them have the skills to exfiltrate copies without leaving traces — sometimes by using the very same 'weapons' against the organizations that contain them. There are substantial price incentives for government hackers and consultants to obtain copies since there is a global "vulnerability market" that will pay hundreds of thousands to millions of dollars for copies of such 'weapons'. Similarly, contractors and companies who obtain such 'weapons' sometimes use them for their own purposes, obtaining advantage over their competitors in selling 'hacking' services. Over the last three years the United States intelligence sector, which consists of government agencies such as the CIA and NSA and their contractors, such as Booz Allan Hamilton, has been subject to unprecedented series of data exfiltrations by its own workers. A number of intelligence community members not yet publicly named have been arrested or subject to federal criminal investigations in separate incidents. Most visibly, on February 8, 2017 a U.S. federal grand jury indicted Harold T. Martin III with 20 counts of mishandling classified information. The Department of Justice alleged that it seized some 50,000 gigabytes of information from Harold T. Martin III that he had obtained from classified programs at NSA and CIA, including the source code for numerous hacking tools. Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by peer states, cyber mafia and teenage hackers alike. U.S. Consulate in Frankfurt is a covert CIA hacker base In addition to its operations in Langley, Virginia the CIA also uses the U.S. consulate in Frankfurt as a covert base for its hackers covering Europe, the Middle East and Africa. CIA hackers operating out of the Frankfurt consulate ("Center for Cyber Intelligence Europe" or CCIE) are given diplomatic ("black") passports and State Department cover. The instructions for incoming CIA hackers make Germany's counter-intelligence efforts appear inconsequential: "Breeze through German Customs because you have your cover-for-action story down pat, and all they did was stamp your passport" Your Cover Story (for this trip) Q: Why are you here? A: Supporting technical consultations at the Consulate. Two earlier WikiLeaks publications give further detail on CIA approaches to customs and secondary screening procedures. Once in Frankfurt CIA hackers can travel without further border checks to the 25 European countries that are part of the Shengen open border area — including France, Italy and Switzerland. A number of the CIA's electronic attack methods are designed for physical proximity. These attack methods are able to penetrate high security networks that are disconnected from the internet, such as police record database. In these cases, a CIA officer, agent or allied intelligence officer acting under instructions, physically infiltrates the targeted workplace. The attacker is provided with a USB containing malware developed for the CIA for this purpose, which is inserted into the targeted computer. The attacker then infects and exfiltrates data to removable media. For example, the CIA attack system Fine Dining, provides 24 decoy applications for CIA spies to use. To witnesses, the spy appears to be running a program showing videos (e.g VLC), presenting slides (Prezi), playing a computer game (Breakout2, 2048) or even running a fake virus scanner (Kaspersky, McAfee, Sophos). But while the decoy application is on the screen, the underlaying system is automatically infected and ransacked. How the CIA dramatically increased proliferation risks In what is surely one of the most astounding intelligence own goals in living memory, the CIA structured its classification regime such that for the most market valuable part of "Vault 7" — the CIA's weaponized malware (implants + zero days), Listening Posts (LP), and Command and Control (C2) systems — the agency has little legal recourse. The CIA made these systems unclassified. Why the CIA chose to make its cyberarsenal unclassified reveals how concepts developed for military use do not easily crossover to the 'battlefield' of cyber 'war'. To attack its targets, the CIA usually requires that its implants communicate with their control programs over the internet. If CIA implants, Command & Control and Listening Post software were classified, then CIA officers could be prosecuted or dismissed for violating rules that prohibit placing classified information onto the Internet. Consequently the CIA has secretly made most of its cyber spying/war code unclassified. The U.S. government is not able to assert copyright either, due to restrictions in the U.S. Constitution. This means that cyber 'arms' manufactures and computer hackers can freely "pirate" these 'weapons' if they are obtained. The CIA has primarily had to rely on obfuscation to protect its malware secrets. Conventional weapons such as missiles may be fired at the enemy (i.e into an unsecured area). Proximity to or impact with the target detonates the ordnance including its classified parts. Hence military personnel do not violate classification rules by firing ordnance with classified parts. Ordnance will likely explode. If it does not, that is not the operator's intent. Over the last decade U.S. hacking operations have been increasingly dressed up in military jargon to tap into Department of Defense funding streams. For instance, attempted "malware injections" (commercial jargon) or "implant drops" (NSA jargon) are being called "fires" as if a weapon was being fired. However the analogy is questionable. Unlike bullets, bombs or missiles, most CIA malware is designed to live for days or even years after it has reached its 'target'. CIA malware does not "explode on impact" but rather permanently infests its target. In order to infect target's device, copies of the malware must be placed on the target's devices, giving physical possession of the malware to the target. To exfiltrate data back to the CIA or to await further instructions the malware must communicate with CIA Command & Control (C2) systems placed on internet connected servers. But such servers are typically not approved to hold classified information, so CIA command and control systems are also made unclassified. A successful 'attack' on a target's computer system is more like a series of complex stock maneuvers in a hostile take-over bid or the careful planting of rumors in order to gain control over an organization's leadership rather than the firing of a weapons system. If there is a military analogy to be made, the infestation of a target is perhaps akin to the execution of a whole series of military maneuvers against the target's territory including observation, infiltration, occupation and exploitation. Evading forensics and anti-virus A series of standards lay out CIA malware infestation patterns which are likely to assist forensic crime scene investigators as well as Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens and anti-virus companies attribute and defend against attacks. "Tradecraft DO's and DON'Ts" contains CIA rules on how its malware should be written to avoid fingerprints implicating the "CIA, US government, or its witting partner companies" in "forensic review". Similar secret standards cover the use of encryption to hide CIA hacker and malware communication (pdf), describing targets & exfiltrated data (pdf) as well as executing payloads (pdf) and persisting (pdf) in the target's machines over time. CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in AV defeats, Personal Security Products, Detecting and defeating PSPs and PSP/Debugger/RE Avoidance. For example, Comodo was defeated by CIA malware placing itself in the Window's "Recycle Bin". While Comodo 6.x has a "Gaping Hole of DOOM". CIA hackers discussed what the NSA's "Equation Group" hackers did wrong and how the CIA's malware makers could avoid similar exposure. The CIA's Engineering Development Group (EDG) management system contains around 500 different projects (only some of which are documented by "Year Zero") each with their own sub-projects, malware and hacker tools. The majority of these projects relate to tools that are used for penetration, infestation ("implanting"), control, and exfiltration. Another branch of development focuses on the development and operation of Listening Posts (LP) and Command and Control (C2) systems used to communicate with and control CIA implants; special projects are used to target specific hardware from routers to smart TVs. Some example projects are described below, but see the table of contents for the full list of projects described by WikiLeaks' "Year Zero". UMBRAGE The CIA's hand crafted hacking techniques pose a problem for the agency. Each technique it has created forms a "fingerprint" that can be used by forensic investigators to attribute multiple different attacks to the same entity. This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution. The CIA's Remote Devices Branch's UMBRAGE group collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation. With UMBRAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from. UMBRAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques. Fine Dining Fine Dining comes with a standardized questionnaire i.e menu that CIA case officers fill out. The questionnaire is used by the agency's OSB (Operational Support Branch) to transform the requests of case officers into technical requirements for hacking attacks (typically "exfiltrating" information from computer systems) for specific operations. The questionnaire allows the OSB to identify how to adapt existing tools for the operation, and communicate this to CIA malware configuration staff. The OSB functions as the interface between CIA operational staff and the relevant technical support staff. Among the list of possible targets of the collection are 'Asset', 'Liason Asset', 'System Administrator', 'Foreign Information Operations', 'Foreign Intelligence Agencies' and 'Foreign Government Entities'. Notably absent is any reference to extremists or transnational criminals. The 'Case Officer' is also asked to specify the environment of the target like the type of computer, operating system used, Internet connectivity and installed anti-virus utilities (PSPs) as well as a list of file types to be exfiltrated like Office documents, audio, video, images or custom file types. The 'menu' also asks for information if recurring access to the target is possible and how long unobserved access to the computer can be maintained. This information is used by the CIA's 'JQJIMPROVISE' software (see below) to configure a set of CIA malware suited to the specific needs of an operation. Improvise (JQJIMPROVISE) 'Improvise' is a toolset for configuration, post-processing, payload setup and execution vector selection for survey/exfiltration tools supporting all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor). Its configuration utilities like Margarita allows the NOC (Network Operation Center) to customize tools based on requirements from 'Fine Dining' questionairies. HIVE is a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers) and Linux platforms and a Listening Post (LP)/Command and Control (C2) infrastructure to communicate with these implants. The implants are configured to communicate via HTTPS with the webserver of a cover domain; each operation utilizing these implants has a separate cover domain and the infrastructure can handle any number of cover domains. Each cover domain resolves to an IP address that is located at a commercial VPS (Virtual Private Server) provider. The public-facing server forwards all incoming traffic via a VPN to a 'Blot' server that handles actual connection requests from clients. It is setup for optional SSL client authentication: if a client sends a valid client certificate (only implants can do that), the connection is forwarded to the 'Honeycomb' toolserver that communicates with the implant; if a valid certificate is missing (which is the case if someone tries to open the cover domain website by accident), the traffic is forwarded to a cover server that delivers an unsuspicious looking website. The Honeycomb toolserver receives exfiltrated information from the implant; an operator can also task the implant to execute jobs on the target computer, so the toolserver acts as a C2 (command and control) server for the implant. Similar functionality (though limited to Windows) is provided by the RickBobby project. See the classified user and developer guides for HIVE. Why now? WikiLeaks published as soon as its verification and analysis were ready. In Febuary the Trump administration has issued an Executive Order calling for a "Cyberwar" review to be prepared within 30 days. While the review increases the timeliness and relevance of the publication it did not play a role in setting the publication date. Names, email addresses and external IP addresses have been redacted in the released pages (70,875 redactions in total) until further analysis is complete. Over-redaction: Some items may have been redacted that are not employees, contractors, targets or otherwise related to the agency, but are, for example, authors of documentation for otherwise public projects that are used by the agency. Identity vs. person: the redacted names are replaced by user IDs (numbers) to allow readers to assign multiple pages to a single author. Given the redaction process used a single person may be represented by more than one assigned identifier but no identifier refers to more than one real person. Archive attachments (zip, tar.gz, ...) are replaced with a PDF listing all the file names in the archive. As the archive content is assessed it may be made available; until then the archive is redacted. Attachments with other binary content are replaced by a hex dump of the content to prevent accidental invocation of binaries that may have been infected with weaponized CIA malware. As the content is assessed it may be made available; until then the content is redacted. The tens of thousands of routable IP addresses references (including more than 22 thousand within the United States) that correspond to possible targets, CIA covert listening post servers, intermediary and test systems, are redacted for further exclusive investigation. Binary files of non-public origin are only available as dumps to prevent accidental invocation of CIA malware infected binaries. Organizational Chart The organizational chart corresponds to the material published by WikiLeaks so far. Since the organizational structure of the CIA below the level of Directorates is not public, the placement of the EDG and its branches within the org chart of the agency is reconstructed from information contained in the documents released so far. It is intended to be used as a rough outline of the internal organization; please be aware that the reconstructed org chart is incomplete and that internal reorganizations occur frequently. Wiki pages "Year Zero" contains 7818 web pages with 943 attachments from the internal development groupware. The software used for this purpose is called Confluence, a proprietary software from Atlassian. Webpages in this system (like in Wikipedia) have a version history that can provide interesting insights on how a document evolved over time; the 7818 documents include these page histories for 1136 latest versions. The order of named pages within each level is determined by date (oldest first). Page content is not present if it was originally dynamically created by the Confluence software (as indicated on the re-constructed page). What time period is covered? The years 2013 to 2016. The sort order of the pages within each level is determined by date (oldest first). WikiLeaks has obtained the CIA's creation/last modification date for each page but these do not yet appear for technical reasons. Usually the date can be discerned or approximated from the content and the page order. If it is critical to know the exact time/date contact WikiLeaks. What is "Vault 7" "Vault 7" is a substantial collection of material about CIA activities obtained by WikiLeaks. When was each part of "Vault 7" obtained? Part one was obtained recently and covers through 2016. Details on the other parts will be available at the time of publication. Is each part of "Vault 7" from a different source? Details on the other parts will be available at the time of publication. What is the total size of "Vault 7"? The series is the largest intelligence publication in history. How did WikiLeaks obtain each part of "Vault 7"? Sources trust WikiLeaks to not reveal information that might help identify them. Isn't WikiLeaks worried that the CIA will act against its staff to stop the series? No. That would be certainly counter-productive. Has WikiLeaks already 'mined' all the best stories? No. WikiLeaks has intentionally not written up hundreds of impactful stories to encourage others to find them and so create expertise in the area for subsequent parts in the series. They're there. Look. Those who demonstrate journalistic excellence may be considered for early access to future parts. Won't other journalists find all the best stories before me? Unlikely. There are very considerably more stories than there are journalists or academics who are in a position to write them.