Vault 7: CIA Hacking Tools Revealed

Contents

- Press Release
- Analysis
- Examples
- Frequently Asked Questions

Press Release

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.

Analysis

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.

Examples

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

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.

Frequently Asked Questions

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.

Redactions

Names, email addresses and external IP addresses have been redacted in the released pages (70,875 redactions in total) until further analysis is complete.

1. **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.
2. **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.
3. **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.
4. **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.
5. 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.
6. **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.

Top

WL Research Community - user contributed research based on documents published by WikiLeaks.

Tor is an encrypted anonymising network that makes it harder to intercept internet communications, or see where communications are coming from or going to.

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity.

The Courage Foundation is an international organisation that supports those who risk life or liberty to make significant contributions to the historical record.

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network.