Click Here

WikiLeaks describes its latest release of files allegedly obtained from the CIA as the largest ever publication of confidential documents in the agency's history.But what is in it? Here is a quick digest of the documents according to the website's report.Disclaimer: Although WikiLeaks has proven to provide legitimate resources, the latest "leak" has not yet been confirmed to be true by US security services or other organisations involved.Equally, the claimed provenance of the "leaks" coming from within the CIA HQ in Langley, Virginia, may be bogus. Russian intelligence have form for feeding WikiLeaks data. Image: Julian Assange compared the spread of cyber weapons to the global arms trade WikiLeaks has called the release "Vault 7", "Part 1", and "Year Zero" - which implies it is planning on releasing further information. In their words the "leak" is a "substantial collection of material about CIA activities obtained by Wikileaks".In total, it contains 8,761 documents and files which allegedly detail CIA hacking practices between 2013 and 2016.Who "leaked" the info? On its website, Wikileaks says: "Sources trust Wikileaks to not reveal information that might help identify them."However, they claim the information has come from "an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virginia". In other words, they claim it was leaked to them from the inside. They add the supposed whistleblower's motivation was "to initiate a public debate about the security, creation, use, proliferation and democratic control of cyber weapons." Image: iPhones were also allegedly targeted with malware What does the "leak" say CIA hackers can do?The report outlines in great detail the scope, scale and capabilities of the CIA in cyber espionage. The "leak" is entitled "Zero Day" as it lists all the so-called "zero day" exploits that have been allegedly developed by the CIA to hack targets.Wikipedia defines a "zero day" vulnerability as a computer software weakness "that hackers can exploit to adversely affect computer programs, data, additional computers or a network".It adds: "It is known as a 'zero day' because it is not publicly reported or announced before becoming active, leaving the software's author with zero days in which to create patches or advise workarounds to mitigate its actions."The "leak" claims that the CIA has built up an incredible arsenal of "zero day" attacks including malware (malicious code), viruses, Trojans and other cyber exploit weapons.WikiLeaks says the agency is able to hack into Apple's iPhone and iPad, Google's Android, Microsoft's Windows and the Linux operating system. Image: The leak claims recorded conversations were sent 'over the internet to a covert CIA server' There is nothing new there but it is also alleged that the CIA can access users' messages on encrypted services like WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking smartphones.The report also claims that the CIA is able to use our own hardware to spy on us, for example by hacking Samsung smart TVs and turning them into covert microphones.What is the scale of the CIA hacking operation?The "leak" says that the scale of the CIA's operation meant that by 2016 the agency had "utilised more code than that used to run Facebook."WikiLeaks claims that in effect the CIA has created its own National Security Agency "with even less accountability".In addition to its operations in Langley, Virginia, "Vault 7" alleges that the CIA also uses the US consulate in Frankfurt "as a covert base for its hackers covering Europe, the Middle East and Africa".Once in Frankfurt, the report says, hackers can travel without further border checks to the 25 European countries that are part of the Schengen open border area.Criticism of CIA operationsThese revelations alone, if true, will be extremely embarrassing to the security agency. In effect, it shows what is under the hood of the secretive and extremely successful spying organisation.However, WikiLeaks doesn't stop there. It criticises the agency's practices in detail. For example, it claims that a section of the CIA's hacking unit is sloppy. Image: The WikiLeaks release appears to give an eye-opening look at CIA documents It says: "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."It also claims that these techniques are not good enough to hide the CIA's tracks. The lines of code that the agency uses are said to be leaving "fingerprints that can be used by forensic investigators to attribute multiple different attacks to the same entity."In simple terms, this is like a murderer using the same distinctive knife wound on multiple victims.Another criticism is that if the CIA built up such a wealthy dossier of "zero day" attacks and failed to warn the organisations at risk the agency is putting the nation at risk.As WikiLeaks puts it: "Serious vulnerabilities not disclosed to the manufacturers place huge swathes of the population and critical infrastructure at risk."Other claimsThe "leak" doesn't stop at surveillance. WikiLeaks accuses the CIA of much worse."Vault 7" alleges that in 2014 the agency looked into "infecting the vehicle control systems used by modern cars and trucks", allowing it to "engage in nearly undetectable assassinations". WL Research Community - user contributed research based on documents published by WikiLeaks From our.wikileaks.org Welcome to the WL Research Community. We are a group of volunteers who compile summarized information from data published by WikiLeaks. Join us as we bring truth to light on some of the most powerful political and corporate entities in the world. Interested in joining? Checkout our Getting Started guide. Recent Publications Mar 31, 2017 - continues the Vault 7 series with Marble 676 source code files for the CIA's secret anti-forensic Marble Framework. Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA.Marble does this by hiding ("obfuscating") text fragments used in CIA malware from visual inspection. This is the digital equivalent of a specalized CIA tool to place covers over the english language text on U.S. produced weapons systems before giving them to insurgents secretly backed by the CIA. Publication Research Browse Category Search on WikiLeaks Nov 29, 2016 - WikiLeaks publishes in searchable format more than 60 thousand emails from private intelligence firm HBGary. The publication today marks the early release of US political prisoner Barrett Brown, who was detained in 2012 and sentenced to 63 months in prison in connection with his journalism on Stratfor and HBGary. Publication Research Browse Category Search on WikiLeaks Investigations Browse All InvestigationsOther All Publications Publication Categories / Tags Browse Publication Vault 7: CIA Hacking Tools Revealed United States, Intelligence, National Security Browse Documents CIA espionage orders for the 2012 French presidential election United States, France, Intelligence Read Document Berats Box Turkey, Energy Search Emails German BND Inquiry Materials NSA, BND, Germany Search Documents HBGary Emails HBGary, United States Search Emails Yemen Files Yemen, United States Browse Documents & Emails Podesta Emails Clintons Custom Search DNC Emails DNC, Politics Custom Search Hillary Clinton Email Archive Clintons, United States Custom Search Public Library of U.S. Diplomacy PLUSD, Politics, United States Custom Search Trade in Services Agreement TISA, Trade Browse Documents Trans Pacific Partnership TPP, Trade Browse Documents Transatlantic Trade and Investment Partnership TTIP, Trade Browse Documents The Saudi Cables Saudi Arabia Custom Search The Syria Files Syria Custom Search AKP Emails Turkey Custom Search IMF Internal Greek Disaster Greece Browse Documents NSA Targets World Leaders NSA, European Union, Germany Browse Documents EU Military Operations Refugees European Union Browse Documents The New Dirty War for Africa's Uranium and Minderal Rights Africa Browse Documents The SourceAmerica Tapes United States Browse Documents CIA Director John Brennan Emails CIA Browse Documents NSA World Spying NSA Browse Documents Hacking Team Emails Investigations Custom Search German BDN Inquiry into NSA Investigations Browse Documents Sony Emails Investigations Custom Search CIA Travel Advice Investigations Browse Documents Spy Files Surveillance Browse Documents Pirate Bay Founder Prosecution Sweden Browse Documents Detainee Policies Investigations Browse Documents Global Intelligence Files Stratfor Browse Documents Guantnamo Files GITMO Browse Documents Iraq War Logs Iraq Search Documents Afghan War Logs Afghanistan Search Documents 8 March 2017We have no comment on the authenticity of purported intelligence documents released by Wikileaks or on the status of any investigation into the source of the documents. However, there are several critical points we would like to make.CIAs mission is to aggressively collect foreign intelligence overseas to protect America from terrorists, hostile nation states and other adversaries. It is CIAs job to be innovative, cutting-edge, and the first line of defense in protecting this country from enemies abroad. America deserves nothing less.It is also important to note that CIA is legally prohibited from conducting electronic surveillance targeting individuals here at home, including our fellow Americans, and CIA does not do so. CIAs activities are subject to rigorous oversight to ensure that they comply fully with U.S. law and the Constitution.The American public should be deeply troubled by any Wikileaks disclosure designed to damage the Intelligence Communitys ability to protect America against terrorists and other adversaries. Such disclosures not only jeopardize U.S. personnel and operations, but also equip our adversaries with tools and information to do us harm.# # #Update March 9 10:59am PT: The CIA has spoken out against the WikiLeaks document dump, including in a statement sent to TechRadar.Like Apple, Google has chimed in with a statement on the security of its products, saying it's "confident that security updates and protections in both Chrome and Android already shield users from many of these alleged vulnerabilities."Finally, WikiLeaks founder Julian Assange said on March 9 the group would give tech companies exclusive access to the information it has in hand, allowing them to gather more details on the CIA's hacking methods. This would let tech firms "develop fixes" before WikiLeaks releases the information to the general public. Assange says some tech companies have asked for details on the CIA's techniques, according to USA Today.You may like Read on for more...Surprise, everyone, the US Central Intelligence Agency (CIA) allegedly has the means to hack everyday electronics.The revelation comes from WikiLeaks, which has released thousands of purported CIA Vault 7 files pertaining to hacking tools the agency could use to spy on targets, tools that include various malwares, trojans, and even remote control systems.With a trove of data released in one fell swoop, just as many questions have arisen, including what devices the CIA could allegedly access and how this might have happened. Weve put together this guide to get you up to speed on the WikiLeaks Vault 7 document dump.Sign up for breaking news, reviews, opinion, top tech deals, and more.What is Vault 7?The basic gist is this: WikiLeaks, the organization headed by Julian Assange and known for leaking thousands of documents about various topics - including details about the inner workings of Scientology and Afghan war logs - has struck once again with details on alleged CIA tools that could be used conduct mass spying programs. The documents cover CIA activity from 2013 through 2016.Officially, the CIA cannot legally use those tools against US citizens, however the agency could use them against non-US citizens. And as we saw with the Edward Snowden leaks, just because spying on citizens is illegal, this doesnt mean it's not happening.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, explains the documents.The CIA allegedly has a range of tools at its disposal that could easily be used in spying programs. And as we know from the Edward Snowden NSA leaks, the subjects of spying could be either guilty of wrongdoing, or completely innocent.Its important to highlight that the leaked documents so far have not been verified. The CIA has not yet issued a statement about the leak, and at the time of publication, the ageny hadn't returned our request for comment on the issue.Still, a source for the Wall Street Journal has said the leaks are legitimate, and even Snowden has weighed in to say that he believes the data is authentic.Still working through the publication, but what @Wikileaks has here is genuinely a big deal. Looks authentic.March 7, 2017There is certainly questionable timing to the release. WikiLeaks assures that it published the documents as soon as its verification and analysis were ready, however the leaks also come at a time when President Donald Trump has spoken out against the intelligence community over other leaks that suggest campaign officials spoke to Russian intelligence officials in the months before the election.As Engadget notes, intentional or not, the new data steers attention towards the CIA and away from what the organization may have learned about the Trump campaign. None of this is to say that we think the documents are a fabrication on the contrary, its looking more and more like they are authentic. It is, however, important to note there is evidence enough to be suspicious of them.What devices were allegedly hacked?Politics aside, if the documents are legit, the CIA was able to access a number of devices in its surveillance efforts, many of which you probably own or are familiar with. We've included tips on how to shore up security on these devices as well.Samsung Smart TVsPerhaps the most interesting revelation is the CIAs alleged use of smart TVs for spying.In a document called Weeping Angel, the CIA is described as using a fake-off mode, which essentially causes a TVs screen to look like its turned off when in reality it is still on and recording audio in the room.The document even goes a step further and describes how the hack could be improved, including capturing video, too.Unfortunately, theres not much you can do about your smart TV being used to spy if you want to retain its full use. If, however, youre fine with doing away with voice control in return for increased privacy, you can disable the microphone in you TVs settings. Its important to note that you should also check the permissions for individual apps, and ensure that none of them relate to the microphone.iPhones and Android phonesOn top of Samsung TVs, the CIA is also purportedly tapped into smartphones.The agency reportedly developed as many as 24 zero day exploits for Android and an undisclosed number of iPhone exploits. A zero day exploit refers to a bug included in a device that the original manufacturer isnt aware is there.In most cases, this equates to a small glitch in one of the millions of lines of code housed in a handset. The glitch can be manipulated by hackers, however, including the CIA.Apple spoke up on March 7 to say most of the vulnerabilities described in the Vault 7 data dump were patched in the newest version of iOS. Here's the company's full statement, provided to TechCrunch by an Apple spokesperson:"Apple is deeply committed to safeguarding our customers privacy and security. The technology built into todays iPhone represents the best data security available to consumers, and were constantly working to keep it that way.Our products and software are designed to quickly get security updates into the hands of our customers, with nearly 80% of users running the latest version of our operating system. While our initial analysis indicates that many of the issues leaked today were already patched in the latest iOS, we will continue work to rapidly address any identified vulnerabilities. We always urge customers to download the latest iOS to make sure they have the most recent security updates."Google also spoke up on March 9, noting in a statement to Recode that its security updates and protections for Chrome and Android should shield users from the alleged vulnerabilities outlined in the documents:"As weve reviewed the documents, we're confident that security updates and protections in both Chrome and Android already shield users from many of these alleged vulnerabilities," Heather Adkins, Google's director of information security and privacy said."Our analysis is ongoing and we will implement any further necessary protections. We've always made security a top priority and we continue to invest in our defenses."A big part of the leak was the news that the CIA could look at messages from encrypted messaging services like WhatsApp, Telegram and Weibo, however its important to note it does not appear as though the agency has hacked those specific apps, but rather the underlying operating system that the apps run on.Many device manufacturers offer rewards to developers who find zero day exploits, so the best thing for your phone may just be to ensure that it always has the latest update.Windows, OS X and Linux devicesAccording to the documents, the CIA has also put substantial effort into infecting and controlling Windows, OS X, and Linux-based computers.Not only does it also use zero day exploits on those computers, but it has also developed malware that can infect CDs and DVDs, write itself onto USB drives, and hide in covert disk areas to avoid detection.Theres unfortunately not much that can be done about these exploits, however its generally a good idea to download and use antivirus software like AVG, and ensure that it always has the latest update.Connected carsAccording to the documents, the CIA has even put research into how it can infect the computers inside internet-connected cars.This stems from a 2014 meeting of the CIAs Embedded Development Branch, which is apparently a sector of the agency that handles hacking into electronic devices to turn them into covert microphones. Not only that, but WikiLeaks notes that the ability to hack into connected cars would enable the CIA to use the cars for undetectable assassinations.Theres almost nothing that can be done about this. If you car gets software updates, ensure that it always has the latest one.CIA's responseAfter initially staying quiet, the CIA has issued a few statements on the WikiLeaks data dump.The first landed March 8 via NBC Nightly News on Twitter. The agency said it had "no comment on the authenticity of purported intelligence documents released by WikiLeaks or on the status of any investigation into the source of the documents."While that may have sufficed, the agency went on to make "several critical points" about its role as an intelligence agency, what it can and cannot do as far as electronic surveillance and a warning against WikiLeak's actions: JUST IN: CIA responds to new WikiLeaks release; claims such disclosures "jeopardize US personnel and operations" and "help our adversaries." pic.twitter.com/Fu3MKxGnkFMarch 8, 2017CIA spokesperson Jonathan Liu also provided a statement to TechRadar on March 9:"As weve said previously, Julian Assange is not exactly a bastion of truth and integrity," Liu said. "Despite the efforts of Assange and his ilk, CIA continues to aggressively collect foreign intelligence overseas to protect America from terrorists, hostile nation states and other adversaries."Liu also said the CIA's earlier statement still stands.What now?The documents uncovered by WikiLeaks, if accurate, will undoubtedly be studied over the next few weeks and months, and well likely hear more details about the CIAs alleged spying when that information becomes available.As for keeping your devices secure - or as secure as they can be - try to update your electronics frequently and use antivirus software to avoid any malware that can be detected. Last but not least, stay informed, keeping an eye on information thats released about the documents in the coming days and weeks.Michelle Fitzsimmons contributed to this reportThe best free security software 2017WikiLeaks has released a huge set of files that it calls "Year Zero" and which mark the biggest exposure of CIA spying secrets ever.The massive set of documents over 8,000 pages in all include a host of hacking secrets that could embarrass intelligence agencies and the US government, as well as undermining spying efforts across the world.Here are six of the biggest secrets and pieces of information yet to emerge from the huge dump.1) The CIA has the ability to break into Android and iPhone handsets, and all kinds of computersThe US intelligence agency has been involved in a concerted effort to write various kinds of malware to spy on just about every piece of electronic equipment that people use. That includes iPhones, Androids and computers running Windows, macOS and Linux.If that software is as powerful as WikiLeaks claims, it could be used to remotely control those devices and switch them on and off. Once that happened, a vast array of data would be made available including users' locations, messages they had sent, and potentially everything heard by the microphone or seen by the camera.2) Doing so would make apps like Signal, Telegram and WhatsApp entirely insecureEncrypted messaging apps are only as secure as the device they are used on if an operating system is compromised, then the messages can be read before they encrypted and sent to the other user. WikiLeaks claims that has happened, potentially meaning that messages have been compromised even if all of the usual precautions had been taken.3) The CIA could use smart TVs to listen in on conversations that happened around themOne of the most eye-catching programmes detailed in the documents is "Weeping Angel". That allows intelligence agencies to install special software that allows TVs to be turned into listening devices so that even when they appear to be switched off, they're actually on.That's just one of the technologies created by the Embedded Devices Branch, the CIA division at the centre of much of the leaks of new information. 4) The agency explored hacking into cars and crashing them, allowing 'nearly undetectable assassinations'Many of the documents reference tools that appear to have dangerous and unknown uses. One file, for instance, shows that the CIA were looking into ways of remotely controlling cars and vans by hacking into them."The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations," WikiLeaks notes, in an unproven piece of speculation.5) The CIA hid vulnerabilities that could be used by hackers from other countries or governmentsWikiLeaks claims that its source handed over the documents in order to provoke a debate about the power of intelligence agencies and how their information should be exposed. Perhaps central to that is the accusation that the CIA was "hoarding" exploits that it had found rather than handing them over to the companies that could fix them, and so make users safe, as they had promised to do.Such bugs were found in the biggest consumer electronics in the world, including phones and computers made Apple, Google and Microsoft. But those companies didn't get the chance to fix those exploits because the agency kept them secret in order to keep using them, the documents suggest."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," a WikiLeaks statement read. "If the CIA can discover such vulnerabilities so can others."WikiLeaks noted that those unfixed exploits affected everyone using the equipment, including "the U.S. Cabinet, Congress, top CEOs, system administrators, security officers and engineers".6) More information is comingThe documents have still not been looked through entirely. There are 8,378 pages of files, some of which have already been analysed but many of which hasn't.The files are being shared publicly on the WikiLeaks website and the organisation has encouraged its supporters to keep looking through the documents in the hope of finding more stories.And that's not to mention the other sets of documents that are coming. The "Year Zero" leaks are just the first in a series of "Vault 7" dumps, Julian Assange said.When taken together, those "Vault 7" leaks will make up the biggest intelligence publication in history, WikiLeaks claimed. 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 Targets browser (e.g., to Windex for browser exploitation) or the proxying of a Targets network connections. FlyTrap can also setup VPN tunnels to a CherryBlossom-owned VPN server to give an operator access to clients on the Flytraps 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). WikiLeaks today released what it claims is the largest leak of intelligence documents in history. It contains 8,761 documents from the CIA detailing some of its hacking arsenal. The release, code-named Vault 7 by WikiLeaks, covers documents from 2013 to 2016 obtained from the CIAs Centre for Cyber Intelligence. They cover information about the CIAs operations as well as code and other details of its hacking tools including malware, viruses, trojans, weaponized zero day exploits and malware remote control systems. One attack detailed by WikiLeaks turns a Samsung Smart TV into a listening device, fooling the owner to believe the device is switched off using a Fake-Off mode. The CIA apparently was also looking at infecting vehicle control systems as a way of potentially enabling undetectable assassinations, according to WikiLeaks. One of the greatest focus areas of the hacking tools was getting access to both Apple and Android phones and tablets using zero-day exploits. These are vulnerabilities that are unknown to the vendor, and have yet to be patched. This would allow the CIA to remotely infect a phone and listen in or capture information from the screen, including what a user was typing for example. This, and other techniques, would allow the CIA to bypass the security in apps like WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by collecting the messages before they had been encrypted. If it is true that the CIA is exploiting zero-day vulnerabilities, then it may be in contravention of an Obama administration policy from 2014 that made it government policy to disclose any zero-day exploits it discovered, unless there was a a clear national security or law enforcement reason to keep it secret. Another potentially alarming revelation is the alleged existence of a group within the CIA called UMBRAGE that collects malware developed by other groups and governments around the world. It can then use this malware, or its fingerprint, to conduct attacks and direct suspicion elsewhere. Year Zero According to WikiLeaks, this is only the first part of the leak, titled Year Zero, with more to come. WikiLeaks press release gives an overview on the range of the hacking tools and software, and the organisational structure of the groups responsible for producing them. WikiLeaks hasnt released any code, saying that it has avoided the distribution of armed cyberweapons until a consensus emerges on the technical and political nature of the CIAs program and how such weapons should [be] analyzed, disarmed and published. WikiLeaks founder, Julian Assange, made a statement warning of the proliferation risk posted by cyber weapons: 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 founder, Julian Assange, says this CIA leak raises concerns about cyber weapon proliferation. EPA/FACUNDO ARRIZABALAGA There hasnt been time for there to be any validation that what WikiLeaks has published is actually from the CIA. But given the scale of the leak, it seems likely to be the case. WikiLeaks has indicated that its source wants there to be a public debate about the nature of the CIAs operations and the fact that it had, in effect, created its own NSA with less accountability regarding its actions and budgets. This release of documents from the CIA follows on from a much smaller release of some of the NSAs cyber weapons last year. In that case, the hackers, calling themselves the Shadow Brokers, tried to sell the information that they had stolen. At the time, it was thought that this hack was likely to be the work of an insider but could have also been the work of the Russian secret services as part of a general cyber campaign aimed at disrupting the US elections. This release also follows the much larger release of NSA documents by Edward Snowden in 2013. While WikiLeaks may have a point in trying to engender a debate around the development, hoarding and proliferation of cyber weapons of this type, it is also running a very real risk of itself acting as a vector for their dissemination. It is not known how securely this information is stored by WikiLeaks or who has access to it, nor how WikiLeaks intends to publish the software itself. WikiLeaks has redacted a large amount of information from the documents 70,875 redactions in total including the names of CIA employees, contractors, targets and tens of thousands of IP addresses of possible targets and CIA servers. Damage done The damage that this release is likely to do to the CIA and its operations is likely to be substantial. WikiLeaks has stated that this leak is the first of several. How the CIA chooses to respond is yet to be seen, but it is likely to have made Julian Assanges chance of freedom outside the walls of the Ecuadorian Embassy even less likely than it already was. The fact that the CIA would have an arsenal of this type or be engaging in cyber espionage is hardly a revelation. WikiLeaks attempts to make the fact that the CIA was involved in this activity a topic of debate will be difficult simply because this is not surprising, nor is it news. The fact that an insider leaked this information is more of an issue, as is the possibility of it being another example of a foreign state using WikiLeaks to undermine and discredit the US secret services. US intelligence officials have declined to comment on the disclosure by WikiLeaks, in all probability because they would need to analyse what information has actually been posted and assess the resulting damage it may have caused. 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.

How much is a 1776 to 1976 quarter worth. How much is a 1776 to 1976 d quarter dollar worth. Quarter dollar 1776 to 1976. Quarter dollar 1776 to 1976 worth. How much is 1776 to 1976 one dollar worth. Quarter dollar 1776 to 1976 value. Quarter dollar 1776 to 1976 price. How much is a 1776 to 1976 quarter dollar coin worth. Are 1776 to 1976 quarters worth anything.