

# Why Vault 7 matters. It's not about collection of your information, instead it's about control of your mind.

All the people writing about the intrusive nature of the NSA, and the collection of data through the cell-phones by back-door access has got it all wrong. It's not about the collection of data. It's about using your phone to control your mind.

All these "back doors" and secret embedded code within your electronics, your chips, and your cell-phones is not simply about collecting your personal information. That is the obvious purpose, but that is not the ultimate purpose.

The ultimate purpose is to enable the embedding of special algorithms and embedded code that allow the government to manipulate what you see, read and hear. These enormous (and hidden) embedded programs overlay instructions to your mind. They alter the selection of programs that you might want to use, they change the access and ease of access to websites. They alter the type, range and frequency of information on your feeds, and change what you would watch, see and listen to.

Have you ever been on your cell phone, and musing about something... thinking about a memory or an event... and then suddenly you see a link or an article related to a similar type of event?

No. It's not coincidence.

It's intentional.

You are being subconsciously manipulated to act, think, and behave as

part of a herd of humans, that the oligarchy wants to shepherd into certain defined behaviors.

And the revelations by Wiki-leaks in Vault 7 proves this.

## Vault 7

Whenever you mention the “power” that the United States has over the serfs citizens living there, you really need to mention “Vault 7”. “Vault 7” proves, beyond all and any shadow of a doubt, that the United States government has complete *distain* for the Bill of Rights, and everything that it stands for. Americans have no protections. ZERO. Americans exist at the mercy of their government.



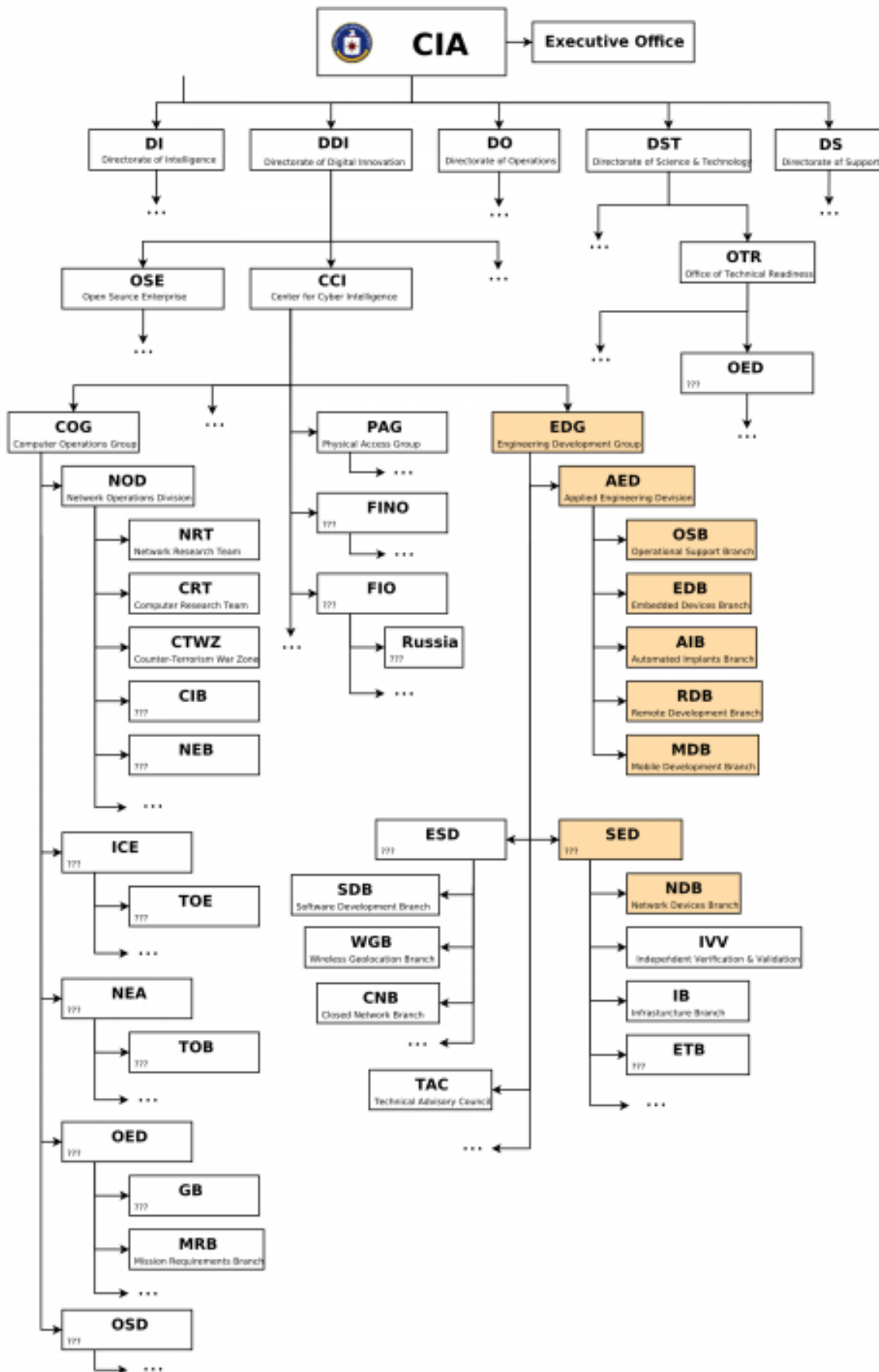
Democrat Senator Feinstein trying to put limits on the the first amendment to the Bill of Rights.

Americans are just monitored cattle. They are monitored by their owners; those handful of Billionaires that fully control the government.

WikiLeaks has published what it claims is the largest-ever release of confidential documents on the CIA. It includes more than 8,000 documents as part of "Vault 7", a series of leaks on the agency, which have allegedly emerged from the CIA's Center For Cyber Intelligence in Langley, and which can be seen on the org chart below, which Wikileaks also released:

A total of 8,761 documents have been published[v] as part of "Year Zero". This "Year Zero" is the first in a series of leaks the whistle-blower organization has been dubbed "Vault 7." WikiLeaks said that "Year Zero" revealed details of the CIA's "global covert hacking program," including "weaponized exploits" used against company products including *"Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones."*

WikiLeaks tweeted the leak, which it claims came from a network inside the CIA's Center for Cyber Intelligence in Langley, Virginia.



Wikileaks released ORG Chart.

Among the more notable disclosures which, if confirmed, “would rock the technology world”, the CIA had managed to bypass encryption on popular phone and messaging services such as Signal, WhatsApp and Telegram. According to the statement from WikiLeaks, government hackers can penetrate Android phones and collect “audio and message traffic before encryption is applied.”

Another profound revelation is that the CIA can engage in “false flag” cyberattacks which portray Russia as the assailant. Discussing the CIA’s Remote Devices Branch’s UMBRAGE group, Wikileaks’ source notes that it “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 (P-SP) avoidance and survey techniques.”

As Kim Dotcom summarizes this finding,

"CIA uses techniques to make cyber attacks look like they originated from enemy state. It turns DNC/Russia hack allegation by CIA into a JOKE"

– Kim Dotcom (@KimDotcom) March 7, 2017

But perhaps what is most notable is the purported emergence of another Snowden-type whistleblower: the source of the information told WikiLeaks in a statement that they wish to initiate a public debate about the “security,

creation, use, proliferation and democratic control of cyberweapons.” Policy questions that should be debated in public include “whether the CIA’s hacking capabilities exceed its mandated powers and the problem of public oversight of the agency,” WikiLeaks claims the source said.

The FAQ section of the release, shown later, provides further details on the extent of the leak, which was “obtained recently and covers through 2016”. The time period covered in the latest leak is between the years 2013 and 2016, according to the CIA timestamps on the documents themselves. Secondly, WikiLeaks has asserted that it has not mined the entire leak and has only verified it, asking that journalists and activists do the leg work.

## Weeping Angel

Among the various techniques profiled by WikiLeaks is “Weeping Angel”, developed by the CIA’s Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones. 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 Kim Dotcom chimed in on Twitter,

BREAKING: CIA turns Smart TVs, iPhones, gaming consoles and many other consumer gadgets into open microphones. [#Vault7](#)

– Kim Dotcom (@KimDotcom) March 7, 2017

Dotcom also added that “Obama accused Russia of cyberattacks while his CIA turned all internet enabled consumer electronics in Russia into listening devices. Wow!”

Obama accused Russia of cyberattacks while his CIA turned all internet enabled consumer electronics in Russia into listening devices. Wow!

– Kim Dotcom (@KimDotcom) March 7, 2017

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.”*

## Key Highlights

- “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.

- Wikileaks claims that 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.
- 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.
- 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.

## CIA targets iPhones, Androids, 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.

Take aways...

- 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 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.

# 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 web servers 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.

Also cars,

- 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.
- 

This is quite suggestive of the CIA having a role in the death of Michael Hastings.

- [Did the CIA kill Michael Hastings? WikiLeaks release says ...](#)
- [New Wikileaks Dump About CIA Hacking Sheds Light On the ...](#)
- [Who was Michael Hastings and why is his death being talked](#)
- [Five Years On, Death of Journalist Michael Hastings ...](#)
- [Michael Hastings crash, incident or assassination?](#)
- [Who Killed Michael Hastings? – New York Magazine](#)
- [Michael Hastings Death Conspiracy: 5 Fast Facts You Need ...](#)
- [The Death of Michael Hastings | SOFREP](#)
- [Suspicious Growing Over Death of Journalist Probing NSA ...](#)
- [Journalist Michael Hastings was investigating CIA director ...](#)

## And computers:

- 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.

## Hoarding of Zero Day exploits:

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.

Take aways...

- 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.
- Please see the [table of contents](#) for the full list of projects described by WikiLeaks’ “Year Zero”. (Over 500 and counting...)

# Proliferation of leaked/hacked Cyberwar programs:

- 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.
- 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 Allen Hamilton, has been subject to unprecedented series of data exfiltrations by its own workers.
- 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.

## The 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 be-

cause you have your cover-for-action story down pat, and all they did was stamp your passport”

## Examples of CIA projects

- 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.
- Umbrage: 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.
- 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. 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.
- ‘Improvise’; 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).
- 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.

## 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.

## 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.

It's easy to have the NSA place "digital fingerprints" on their hacking efforts using these tools, and then blame another nation.

- [Chinese Hackers Charged in Decade-Long Crime and Spying ...](#)
- [US accuses China of hacking coronavirus researchers ...](#)
- [Chinese hacking Archives – CyberScoop](#)
- [U.S. Says China Hackers Stole Secrets, Sought Virus Data ...](#)

UMBAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (P-SP) avoidance and survey techniques.



Unless maintained, the Bill of Rights becomes useless and superannuated.

# 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' questionnaires.

## HIVE

What is an "implant"?

It is the embedded code that instructs your brain what to do and how to behave when you are using electronics technology.

It is the software that has the back of your mind musing about certain things, issues of the day, or getting all emotionally upset about something.

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 unsuspecting 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 Rick-Bobby project.

See the [classified user](#) and [developer guides](#) for HIVE.

## Conclusion

“You could have all the crazy thoughts you wanted, as long as you smiled and kept them to yourself.”

– Mara Purnhagen, Past Midnight

99.9% of the articles (on the internet and in books) discuss how “unconstitutional” the collection of information, by the NSA, is. They argue (and rightfully so) that the United States government should not be doing this, that it is against the Constitution, the law, the purpose of government, and is a dangerous precedent. Ah. We all get this and understand it.

I argue something a little different.

The reason why the United States wants your reading, watching, listening, and Geo-location information (as well as your passwords, your friends, and your associations) is not so much to track your actions and behaviors. But instead, to be able to feed embedded algorithms into your phone.

These hidden and secretive signals direct your subconscious actions.

They control what you look at, what you listen to, and what you are exposed to.

Thus, they “box you in” to a particular “mind set”. And in so doing, they control you.

And the American PTB (Deep State) Oligarchy leadership are believing that

this 2D manipulation of minds will guarantee their successful implementation of change; guarantee that they will remain in power forever, and guarantee that their goals and societal adjustments will occur without any opposition.

But the universe is far more complex than any 2D operation. It's at a bare minimum, an 11D exercise. And pushing this controlling narratives into the minds of millions of Americans will have , or is having...

... unexpected, or unintended consequences.

It should be no surprise that the United States is now balkanized into violently radical warring factions. All of which are attuned to certain predefined narratives. Individual, independent thought no longer exists. You are either "A", or "B" or "C". And they have further classified you in to a direct subcategory all for the purposes of your control. "A-4", or "B-7".

Vault 7 exposes this.

Now a cursory look at the files might (indeed) give you the impression that it's just advanced techniques for the collection and gathering of information. I urge the reader to think past that. Any nation that has an intimate knowledge of your "private papers" and "personal privacy" in real time has the ability to control you.

It's all about control.



The control of what and how you think, by a very powerful government.

And this is why Donald Trump and Mike Pompeo are all up in arms about 5G, and Huawei. It's not that the technology is better, dangerous, or would have "back doors". It is that the stranglehold of the American government control over people would come to an end as less and less people use programs with these embedded algorithms.

If you want to protect yourself from being manipulated by hidden, invisible and secret manipulations, you need to start using phones, and software developed outside of the United States. Those products that are being "banned from American use" such as Huawei and Xiaomi are almost certainly devoid of NSA malware.

Though, perhaps the best thing might be to just move away from all electronic media and live a far simpler life.



A simpler life.

Do you want more?