‘Empire of Hacking’: The U.S. Central Intelligence Agency — Part I

May 4th, 2023

The U. S. Central Intelligence Agency (CIA) is one of the main intelligence agencies of the federal government of the United States, officially tasked with gathering, processing, and analyzing national security intelligence information from foreign governments, enterprises and citizens, primarily through the use of human intelligence (HUMINT), providing specific advises for the U.S. President and Cabinet as well as conducting covert actions. Headquartered in Langley, Virginia, United States, the CIA has four divisions: the Directorate of Intelligence (DI), the National Clandestine Service (NCS), the Directorate of Science and Technology (DS&T), and the Directorate of Support (DS).

The CIA has been secretly conducting and organizing "Peaceful Evolution" and "Color Revolution" around the world for a long time, and continues to carry out espionage activities.

Since the beginning of the 21st century, with the rapid development of the Internet, the CIA has new opportunities for the infiltration, subversion and upheaval activities. The organizations, enterprises and individuals that use the Internet equipment and software products of the U.S.A have been used as the puppet "agents" by CIA, helping it to be a "shining star" in global cyber espionage wars.

This series of reports reveals the main details of CIA’s cyber attacking weapons, discloses the specific process of typical cyber security incidents occurred in China and other countries, analyzes the CIA's cyber attacks, stealing operations and espionage activities based on a large amount of real cases which the National Computer Virus Emergency Response Center (CVERC) adn 360 Total Security (360) had investigated in, and provides references and advises to victims all around the world.

1 Executive summary

According to the statistics, the CIA has overturned or attempted to overturn at least 50 legitimate governments and created disturbances in other countries over the decades (Even though it has admitted only 7 of them.) such as the secret operations lead the disintegration of the socialist camp in 1980's, the "Velvet Revolution" in the early 1990s, the "Rose Revolution" in Georgia in 2003, the "Orange Revolution" in Ukraine in 2004, the "Tulip Revolution" in Kyrgyzstan in 2005, the "Snow Revolution" in Belarus in 2005, the "Orange Storm" in Azerbaijan in 2005, the "Cedar Revolution" in Lebanon in 2005, the "Saffron Revolution" in Myanmar in 2007, the "Green Revolution" in Iran in 2009, the "Arab Spring" in West Asia and North Africa in 2011, the "Sunflower Movements" in Taiwan, China in 2014, and the second "Color Revolution" in Ukraine in 2014,etc.

After analyzing those events comprehensively and systematically, we find the critical factors to organize the events successfully are the technologies used in information communication and commands on scene. And the United States are in a leading position all over the world in the fields of those technologies. Especially in the 1980s, the United States promoted the Internet to the international market which was widely accepted by all countries in the world, providing unprecedented technological possibilities for the U.S. intelligence agencies to launch "Color Revolutions" abroad.

As the former U.S. Secretary of State Madeleine Albright regards the Internet as the key to beat China,actually, the "Color revolutions" have been fueled by Western powers with the help of the Internet. After the "Arab Spring" happened in West Asia and North Africa, some large multinational Internet companies from the United States started to actively intervene in the covert activities including spearing disinformation, provoking chaos and dissensions, supporting anti-government actions, etc.

First, they provided encrypted network communication services. To guarantee the communication services for protesters from the Middle East, and help them avoid being tracked and arrested, American companies linked to U.S. military developed "TOR" project, which used a technique called onion routing to conceal information about user activities. And all the traffic passed through was encrypted. After being produced, TOR project provided free services helping the anti-government activists from many countries including Iran, Tunisia and Egypt to avoid the censorship and surveillance when participating in movements. Second, they provided the reconnect service of the network. To help the anti-government personnel in countries such as Tunis and Egypt keep in touch with the outside world, Twitter and Google quickly launched a dedicated service called "Speak2Tweet". It allows users to dial-up and upload voice messages, which are automatically converted into tweets and then upload them to the Internet for live events reporting on Twitter and other platforms

Third, they provided on-site command communication tools for demonstrations based on Internet and wireless. The RAND has spent years developing an unconventional regime subverting technology called "stampede" that helped a large number of young people connect to the Internet when joining in the protests. Thus, the efficiency of on-site command for demonstrations is greatly improved.

Fourth, a software called "RIOT" was developed by American companies which could support independent wireless broadband, provide anti-jamming wifi, run without any traditional physical access, such as telephone, cable or satellite connection, and easily avoid government’s censorship and surveillance. With the help of those tools and technologies, the CIA has conducted a large number of "Color Revolutions" around the world.

Fifth, the U.S. Department of State regarded the research and development of "Anti-censorship system" as an important task and had invested more than $30 million in it.

2 The Cyber weapon projects of CIA

On March 7, 2017, the Wikileaks disclosed 8716 secret documents from the CIA cyber intelligence center, which showed the attack patterns of CIA network operation teams, code names of operations, technical details of hacking tools. The Wikileaks named those documents as "Vault7" and "Vault7" had aroused great concern worldwide.

In 2020, the 360 discovered a new APT group, named APT-C-39 (according to 360's code-naming system), which specifically targeted China and her allies as the attack objectives. According to the gathered evidences, APT-C-39 had used multiple cyber weapons leaked from "Vault7", including Athena, Fluxwire, Grasshopper, AfterMidnight, HIVE, ChimayRed, etc., to attack targets from China and other countries since 2011. And the affected industry sectors are including critical information systems and infrastructure, aerospace and astronautics, scientific research institutions, petroleum industry, Internet companies, and government agencies.

In global cyber espionage campaigns, the CIA has exploited a large number of "zero-day"(0day) vulnerabilities, most of them have not yet been publicly disclosed (but partly validated), built botnet and proxy network around the world, and launched attacks against servers, terminals, switches and routers, as well as ICS devices. We have successfully extracted multiple artifacts related to "Vault7" from the victims' network located in China as well as in China's ally countries from Southeast Asian and European. Those malware samples mainly includes:

2.1 Fluxwire

A complex operation management platform of RAT attacks, which supports across 9 major Operating Systems including Windows, Unix, Linux and MacOS alongside with 6 different architectures, can build an autonomic mesh network consists of numerous compromised nodes. The platform supports self-healing, loops, and multi-path routing.

2.2 Athena

A light backdoor for Microsoft Windows, developed by CIA and Siege Technologies Company (acquired by Nehemiah Security in 2016), could be implanted by multiple ways, such as remote installation, supply chain, MitM and physical installation, and then resided as a Microsoft Windows Service. And all the attack modules were decrypted and executed in memory as plug-ins.

2.3 Grasshopper

An advanced configurable backdoor for Microsoft Windows, which can build multiple formats of payloads (EXE, DLL, SYS, PIC, etc.), and supports multiple execution modes. It could be reside hidden and conduct espionage with diverse plug-in modules.

2.4 AfterMidnight

A light backdoor executed as a DLL service on Microsoft Windows. It is dynamically transmitted by HTTPS and can load and execute the "Gremlins" payloads with encryption in the whole process.

2.5 ChimayRed

An exploitation tool suite for routers like MikroTik and can be used for impalnting other light RATs such as "TinyShell" by utilizing vulnerabilities.

2.6 HIVE

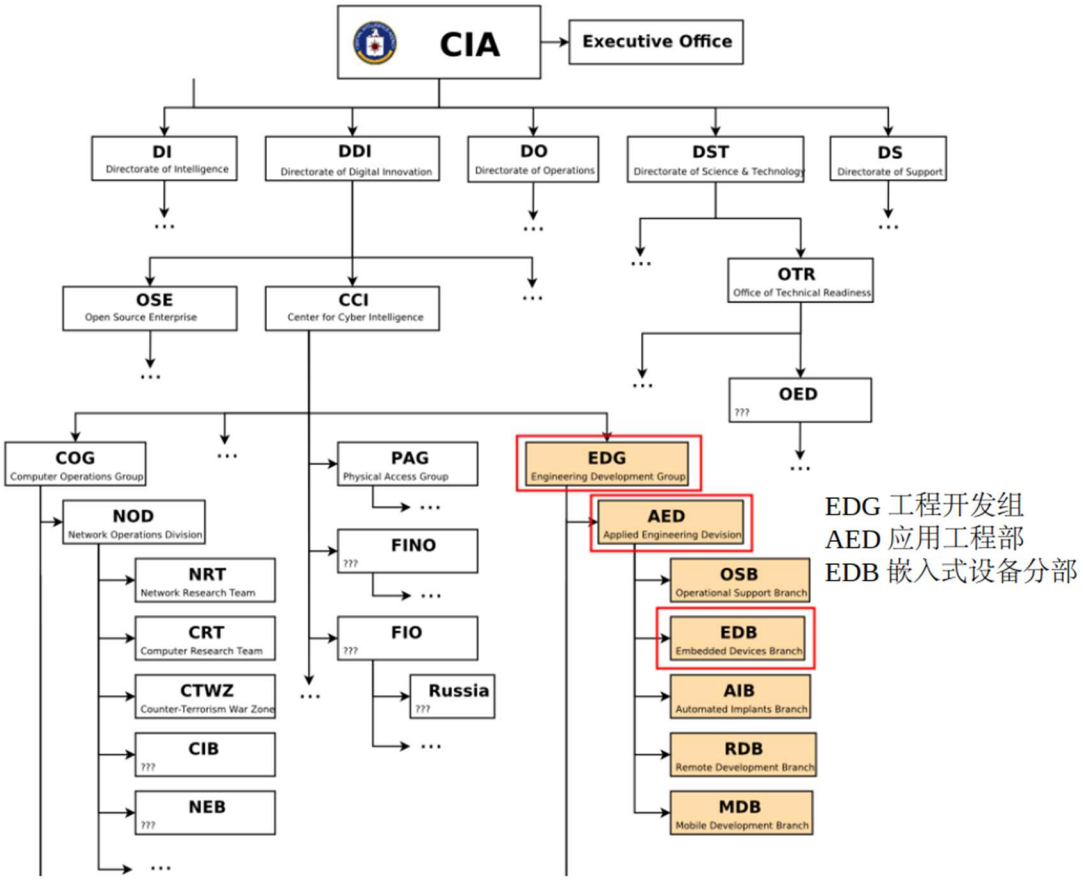
Hive was joint developed by a software development group within the CIA and a subsidiary of U.S. defense giant Northrop Grumman. As an advanced weapon of CIA, HIVE has been used for establishing a global cyber espionage network with multi-layer proxy servers and encrypted data tunnels, so that CIA was able to exfiltrate credentials and sensitive data from targets 24/7.
(*https://www.cverc.org.cn/head/zhaiyao/news20220419-hive.htm*)

2.7 Other related-tools

Vault7 is just a small portion of CIA's cyber-arsenal. Lots of artifacts were discovered in the investigation on cyber espionage operations conducted by CIA, including disguised phishing installers, key-loggers, beacons, USB stealers and other open-source hacking tools.

3. Technical Details of CIA-linked Cyber-Weapons

The 360 discovered a series of targeted attacks against Chinese entities, and collected lots of RATs, Plug-ins and payloads which related to Vault 7 from network of the victims. Further investigation revealed that, most of founded malwares follow the CIA's development specifications contained in Vault 7, such as Network Operations Division In-memory Code Execution Specification, Network Operations Division Cryptographic Requirements and Network Operations Division Persisted DLL Specification. The specifications indicate the standard implementation methods of code-loading, data encryption and persistence, and for CIA internal only.
According to CIA's internal documents leaked by Wikileaks, cyber weapons in Vault 7 were mainly developed by AED, EDB and other subsidiary groups of Engineering Development Group (EDG) of CIA. Most of weapons were manufactured in a CIA's top-secret internal network named "devlan.net", which was a giant development & testing infrastructure built by EDG. The DevLogs of devlan.net showed that over 200 engineers were involved in the HIVE project only.



Further technical analysis shows that, fileless attack was commonly adopted by CIA, malicious code was downloaded and executed directly within memory instead of residing on disk that makes extremely difficult to extract malware samples. However, joint investigation team found an effective way to solve the problem of forensics. For ease of understanding, we divide the cyber-weapons of CIA into 9 categories:

3.1 Framework

We detected and captured Fluxwire, Grasshopper and Athena payloads from multiple victims' network. And those artifacts were attributed to Vault 7 based on technical analysis results of functionalities, attack patterns and network behaviors.

3.2 Delivery

CIA exploited a large number of light-weight downloaders to load and execute payloads of next stage. They could be powerful spyware when integrated with framework, but hard to be identified as malware independent.

3.3 RATs

We were able to capture several plug-in payloads for command and control which working with framework.

3.4 Lateral Movement

There were lots of backdoors implanted by using services of windows remotely with administrator credentials. In addition, the CIA also hijacked the internal network update service of multiple security solutions for deploying backdoors, to further implement lateral movement in the intranet.

3.5 Exfiltration

Joint Investigation Team accidentally extracted a data-exfiltration tool used by CIA, and it turned out to be one of the 48 advanced cyber-weapons described in '*ANT catalog*' which was the confidential document leaked from NSA. Therefore we assume that CIA and NSA may jointly attack the same victim target, or share cyber-weapons, techniques and human resources with each other. Thus, more evidence leads to the attribution of APT-C-39.

3.6 Exploitation

During the investigation, it was found that CIA had established a huge covert network with lots of proxy and VPS over the Internet at least since 2015. CIA exploited zero-day vulnerabilities to compromise IoT devices and network servers and added them to the covert network. Therefore, this one-stone-for-two-birds strategy enabled CIA hided their activities and transferred the blame to other countries. For example, CIA utilized a vulnerability kit with code name "ChimayRed" to attack multiple models of MikroTik brand routers, include a large number of network devices in China. During those attacks, CIA would first modify the router's startup script, make sure the backdoor is executed persistently even after the router rebooted. After that, CIA would fix the CGI program to avoid being exploited by other attackers. Eventually, CIA implanted in those routers with the exclusive backdoors such as 'HIVE' and 'TinyShell'.

3.7 Disguised software

CIA customized backdoors to specifications of targets and disguised malwares as legitimate programs. Then, CIA would deliver backdoors via social engineering attack.

3.8 Anti-AV

CIA had possessed numbers of weapons with the ability of turned off commercial anti-virus software by killing or terminating processes of AV solutions remotely to achieve persistent of the CIA's weapons.

3.9 Off-the-shelf tools

Off-the-shelf tools were also utilized in CIA's operations. During operations, CIA would gain initial-access to the victim's network by targeting spearphishing and exploiting weaknesses on public-facing servers or network devices. After that, CIA explored the network to find their target and subsequently compromised it. The hosts compromised by CIA would be monitored 24/7 and sensitive data would be lost such as key-logs and content of clipboard. And the documents on USB device would also have been stolen once plugged into infected devices. Furthermore, CIA would gain remote access to the camera, microphone, GPS on the infected hosts.

4. Conclusion

American cyber hegemony, manipulated by the U.S. government is expanding across the globe. As one of the three major intelligence agencies of the U.S. government, CIA has long been committed to growing the abilities of cyber espionage and conducted cyber attacks automatically, systematically and smartly. The 8,716 files discolsed by the Wikipedia have sufficiently illustrated that U.S. own the largest cyber arsenal through building numerous hacking tools and cyber attacking weapons. With proven results of investigation, we have noticed that, the cyber weapons that made by U.S. strictly follow the malware developing specifications and standards of their own, and targeted almost all types of platform including IoTs with many attack patterns. With the help of cyber weapon projects, the U.S. intelligence are able to spying on any country as they want, and invest at any cost of money, technology and human resources. Since the U.S. government remains committed to expanding American cyber hegemony, it is deserved to be recognized as the "Empire of Hacking".

This new series of reports revealed that CIA targets at Chinese network over a long period of time and has an attempt to discover and study more cyber attacks and data breach activities conducted by U.S. intelligence.