LAKHSHYA
CYBER SECURITY LABS

VOLUME 1

Vault 7

THE BEGINNING

TABLE OF CONTENTS

1.0 Introduction

A host of documents belonging to the CIA was released by WikiLeaks, codenamed ‘Vault7’ on 7 March 2017. It was a haunting day for the CIA when it lost control over its entire arsenal of hacking tools. The release on ‘Vault7’ contains all the covert methods that can be used for hacking. This information can give anyone the same kind of hacking capabilities to compromise and control as that of the CIA.

The Central Intelligence Agency (CIA) is a civilian foreign intelligence service of the United States federal government. It collects national security information from around the world and provides intelligence for the President and Cabinet. The CIA has no power to enforce a law and is mainly focused on overseas intelligence gathering, with only limited domestic intelligence collection.

One of its successful operations was the Neptune Spear Operation, which was established to gather the location of Osama Bin Laden.

WikiLeaks is an international non-profit organization, created by Julian Assange. It focuses on revealing confidential information of any corporate, government organization, non-government organization etc. Few of the major leaks are

- Fear of Uranium in Pakistan (2007)
- War in Afghanistan (2010)
- The Secret war in Yemen (2010)
- US presidential election campaign (2016), etc.

Vault7 follows this series. So far, the documents published by WikiLeaks are considered to be hundred percent true with no false positives.

THE TIMELINE OF WIKILEAKS' VAULT 7 SERIES IS AS FOLLOWS

MARCH 7, 2017
YEAR ZERO

MARCH 23, 2017
DARK MATTER

MARCH 31, 2017
MARBLE FRAMEWORK

APRIL 7, 2017
GRASSHOPPER

APRIL 14, 2017
HIVE

APRIL 21, 2017
WEEPING ANGEL

2.0 Year Zero

A trove of 8761 confidential documents was published as part of "Year Zero" on 7 March 2017.

The documents revealed a huge list of hacking tools including malware, viruses, trojans, "zero day" exploits, remote control systems etc. The release includes hacking into Apple's iPhone, Google's Android, Microsoft's Windows, Samsung TVs, bypassing encryptions of popular mobile applications and hacking into the vehicle control systems. The release also constituted the internal organizational structure of the CIA.

These documents were considered to be a part of isolated, highly secured networks situated inside the CIA’s Centre for Cyber Intelligence in LangleyLangely, Virginia. The documents were considered to be circulated among the former U.S government hackers and contractors, where someone among them gave a part of these documents to WikiLeaks. The identity of the Whistleblower is not known so far.

According to the Vulnerabilities Equities Process committed by the Obama administration, the vulnerabilities discovered after 2010 must be disclosed. A transgression committed by the CIA was on "hoarding" zero day vulnerabilities, rather than disclosing them to the manufacturers of the respective products. Hiding the security flaws from the manufacturers can leave the product vulnerable to many possible attacks in the wild.

The purpose of the release was to initiate a public debate about security, proliferation risks and democratic control of cyber weapons. The release is claimed to be the largest ever publication made by WikiLeaks. The first release under “Vault7” is the “Year Zero” after which subsequent releases were made namely Dark Matter, Marble Framework, Grasshopper, Hive, Weeping Angel, etc.

3.0 Dark Matter

On the release of Year Zero, Apple addressed most of the vulnerabilities to be already patched.

With the advent of the release "Dark Matter" on 23 March 2017, CIA's covert hacking technique against Apple products were revealed.

The release contains documentation, the techniques used to infect Apple devices and make them persistent.

According to the release, the tools used against Apple devices were Sonic Screwdriver, NightSkies, DarkSeaSkies, Trion, DerStake, etc.

The document on Sonic Screwdriver, which dates back to 2012, describes how CIA agents could infect a Mac with malware using a Thunderbolt-to-Ethernet adapter. 'Sonic Screwdriver' – named after Doctor whose trademark tool – described by the CIA as a "mechanism for executing code on peripheral devices while a Mac laptop or desktop is booting".

The NightSkies, a tool dating back to 2008 was the most remarkable. WikiLeaks says it was "expressly designed to be physically installed onto factory fresh iPhones. i.e. the CIA has been infecting the iPhone supply chain of its targets since at least 2008." NightSkies allowed the CIA to gain "full remote command and control" of iPhones and access files, such as text messages, call logs and contacts.

The DarkSeaSkies is a persistent implant for the MacBook Air which dates back to 2009.It consists of DarkMatter, SeaPea and DarkSkies. The module DarkMatter provides persistence on the device, SeaPea hides the malware's processing files and networking necessary for the operation of the covert tools, and DarkSkies acts as the beacon.

For the malware to be active, the MacBook Air periodically checks the connection to the internet, or else the Malware will delete itself.

Triton is an automated implant for the Mac OS X which allows tasks to be retrieved remotely and executed on the machine. DerStarke 1.4 is a diskless, EFI a persistent version of Triton.

The malware was injected into Apple products through the supply chain by inhibiting mail orders and other shipments. This is done unboxing the product, infecting the device with malware and resending it.

4.0 Marble framework

The third most technically damaging release on 31 March 2017 contains 676 source code files which revealed the mechanism on how the CIA managed to attribute the attack on others.

It is considered to be the CIA's anti-forensic tool, which hides the text of any virus, trojans or malware from visual inspection. That is it obfuscates (hides) text in such a way that it makes it difficult for the forensic experts to point back at the CIA. This would allow the author of the malware to be identified as the suspect.

For instance, the framework contains test examples in multiple languages: it is possible to create a malware and set its language as being Chinese, Russian, Korean, Arabic and Farsi. Thus, the CIA created malware that could potentially be customized to appear as if it emerged from another country. It also supports the ability to "add foreign languages" to any malware. The below figure depicts it well.

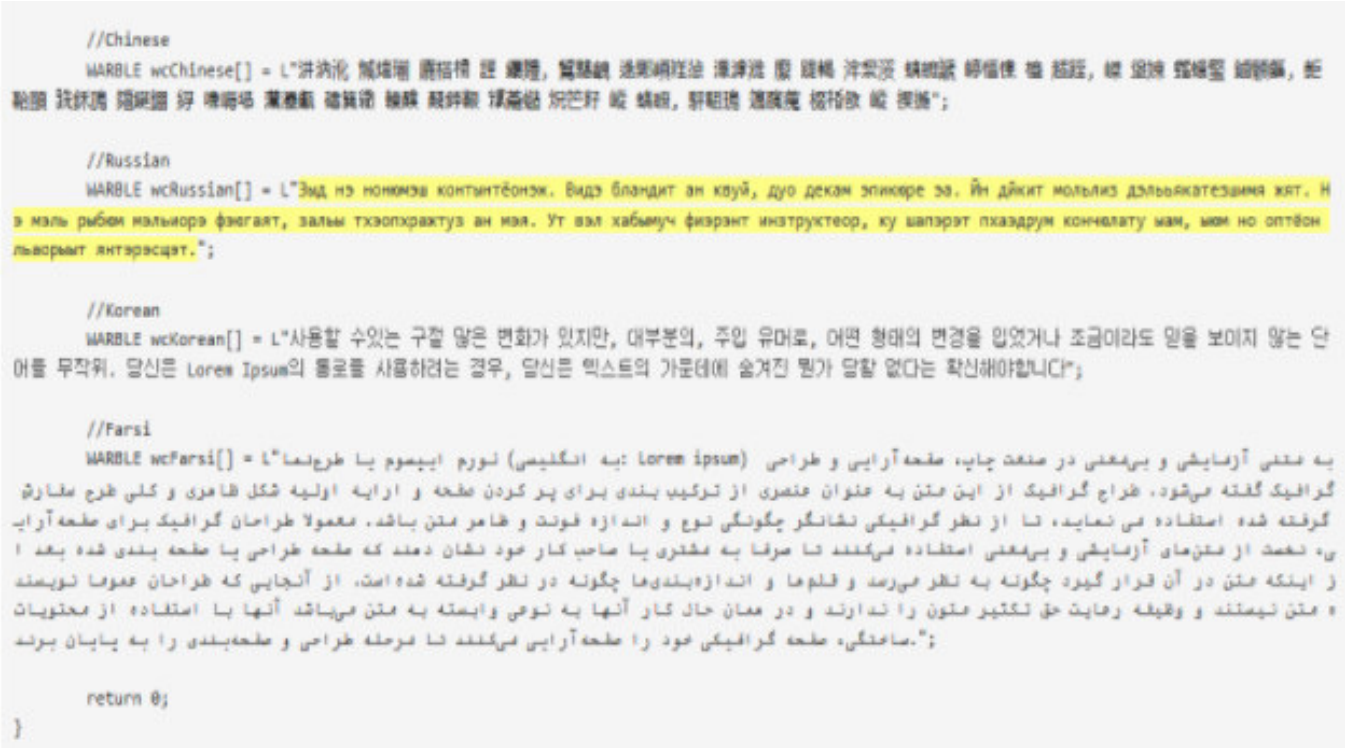

Fig 1. Multiple Language selection

“This would permit a forensic attribution double game, for example by pretending that the spoken language of the malware creator was not American English, but Chinese, but then showing attempts to conceal the use of Chinese, drawing forensic investigators even more strongly to the wrong conclusion,” WikiLeaks explains.

The release comes along with a de-obfuscator which reverses the algorithm used in obfuscation technique. This shows that only the CIA has the ability to reverse back the obfuscation used. It is believed that this framework was used to hack the email account of John Podesta, Chairman at Hillary campaign and attributed the attack over to Russia.

5.0 Grasshopper

A cyber-espionage framework, released on 7 April 2017 which targets Windows users.

The leak consists of 27 documents showing details to build customized malware payloads for Microsoft Windows operating systems and making them persistent.

The framework has the ability to determine what version of Microsoft Windows the target device is running on, or if a particular Antivirus product is running or not. So far, it had evaded the detection on anti-virus products such as ‘MS Security Essentials’, ‘Rising’, ‘Symantec Endpoint’ or ‘Kaspersky IS’. Based on the above requirements the payload is customized to work on the target without being detected.

The framework consists of a variety of persistence module namely WUPS, Stolen goods, crab, scrub, netman, burmuda, wheat. Among the persistence modules, WUPS module reinstalls itself after every 22 hours even if the update is disabled.

The stolen goods persistence module is indeed stolen from a Russian-built banking trojan, Carberp that first appeared in 2013. CIA made use of only the persistence mechanism used by the Carberp not the entire trojan.
By this, the framework puts the entire Windows user at stake.

6.0 Hive

A back-end infrastructure malware that affects multiple platforms, released on 14 April 2017.

The HIVE project is developed by CIA's Embedded Development Branch (EDB).The release made by WikiLeaks consists of six documents that explain how covertly CIA used its malware implant to realize specific tasks on compromised machines.

The multi-platform malware suite affects a variety of operating systems, they include

- Linux
- Windows
- Solaris
- MikroTik (used in Internet routers)
- AVTech Network Video Recorders (often used in CCTV recording).

The software implant has two primary functions – a beacon and an interactive shell.

- Beacons are small, often inexpensive devices that enable more accurate location detection within a narrow range than GPS, cell tower triangulation, and Wi-Fi proximity. In other terms, keeps an accurate tab on the location and movement of the target.

- Shells are command terminals through which an attacker can interact with the system giving them full control over the target system. Both are designed to provide an initial foothold to deploy other “full featured tools".

Hive is considered to be CIA's top secret virus control system which makes use of the back end infrastructure malware. The malware uses public HTTPS interface of a legitimate looking cover domain and transfers exfiltrated information directly to the CIA's server through a Virtual Private Network (VPN).

In response, the CIA executes commands to accomplish specific tasks on the target system. The figure below explains the above mechanism.

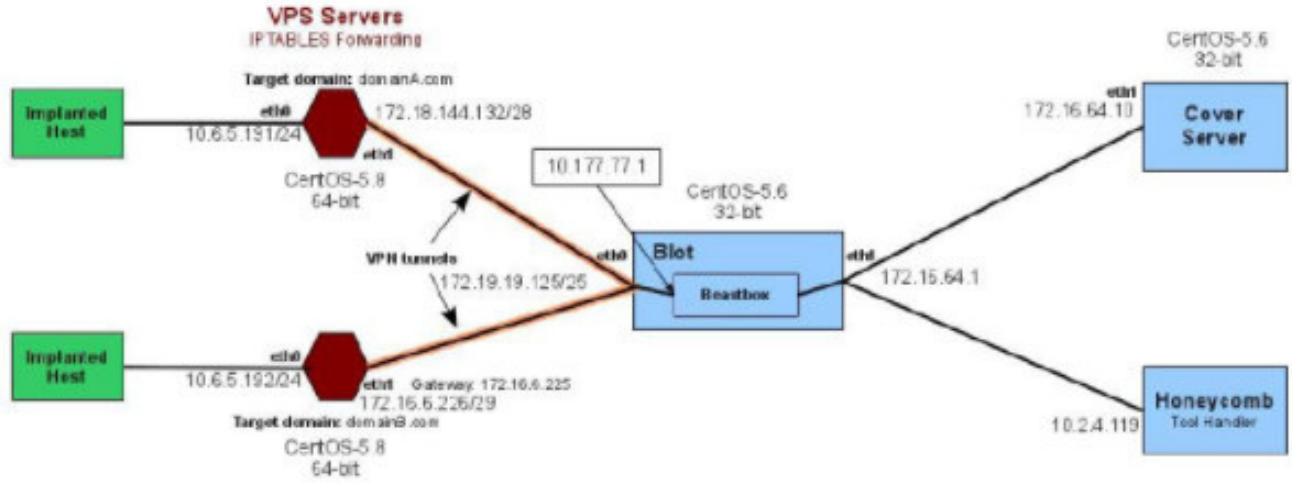

Fig 2 . HIVE mechanism

7.0 Weeping Angel

The release was on an implant designed for Samsung F Series Smart Television on 21 April 2017.

It contains a user guide on the installation of the malware implant. The implant is designed to record conversations in a room while the television is in "Fake off" mode.

Fig 3. TV in fake off mode

“Extending” is a tool developed by MI5/BTSS, UK’s intelligence agency, from which the Weeping Angel was derived. This tool was developed to monitor and take control of Samsung F Series Smart television. The tool can be injected over the television by configuring it through Linux, and injecting in a USB drive to the television.

The tool covertly records the voice over the microphone with the internet enabled on the television. The recorded conversation either gets stored on a drive in the TV or it is transferred through USB or through the internet in the range of an attacker. A Live Listening Tool can also be deployed to cast the audio in real-time.

For the implant to be operational, it has to be connected to the internet, with the inbuilt microphones. The implant interrupts the use of the wireless card on TV, that is, it has the capability to de-authenticate itself from the home network connection and get connected to the CIA's Wi-Fi for uploading the recorded conversation. CIA was able to compromise firmware versions 1111, 1112, and 1116.

The implant on the television can be detected with the presence of tell-tale blue LED glowing at the back side of the TV.

The implant will not work with few of the conditions when: the Airplane mode is ON, runs without administrative rights, the virtual wireless appliance is disabled in device manager, and the voice recognition is turned ON. Since it takes 30 seconds for the Extending tool to start running after the TV is powered ON "Fake off" mode is not impetuously achieved after switching it OFF immediately.

CIA claims, in future releases of the implant, they will be able to record from the microphone simultaneously with other applications e.g. Skype. However, the subsequent versions of Samsung TVs with updated firmware is not impacted with this exploit.

Further releases are meant to be added in the future. Stay tuned.

ABOUT LAKHSHYA CYBER SECURITY LABS

Lakhshya Cyber Security Labs is a Centre of Excellence (CoE) of the leading Middle East based Information Security organization, Paramount Computer Systems. Lakshya Labs is focused on research, development, thought leadership, solutions development and support in leading edge Information Security and Cyber Security areas.

WEBSITE: http://www.lakshyalabs.com

FACEBOOK: https://www.facebook.com/CSRlakshya/

FB Group: https://www.facebook.com/groups/352653085150658/

TWITTER: https://twitter.com/lakshyalabs

LINKEDIN: https://www.linkedin.com/company/lakshya-labs