MEETUP #4
CYBER SECURITY :
VAULT 7

2017’s Issue

MOF.JS

About Me

Ananta Tri Wijatmiko, S. Kom

- DIII Kebendaharaan Negara - STAN – 2005-2008
- S1 – Sistem Informasi - IKPIA Perbanas 2010-2014
- Bagian Sistem Informasi Pengawasan – Inspektorat Jenderal Kementerian Keuangan

About Me

- Oracle Certified Associate (2011)
- Certified Ethical Hacker (2012 – 2015)
- Microsoft Office Specialist - Office Access 2010 (2015)
- Cisco Certified Network Associate Routing and Switching (2015)
- EC-Council Certified Secure Programmer .Net v8 (2016-2019)
- COBIT 5 Foundation (2017)

Post Twitter Wikileaks

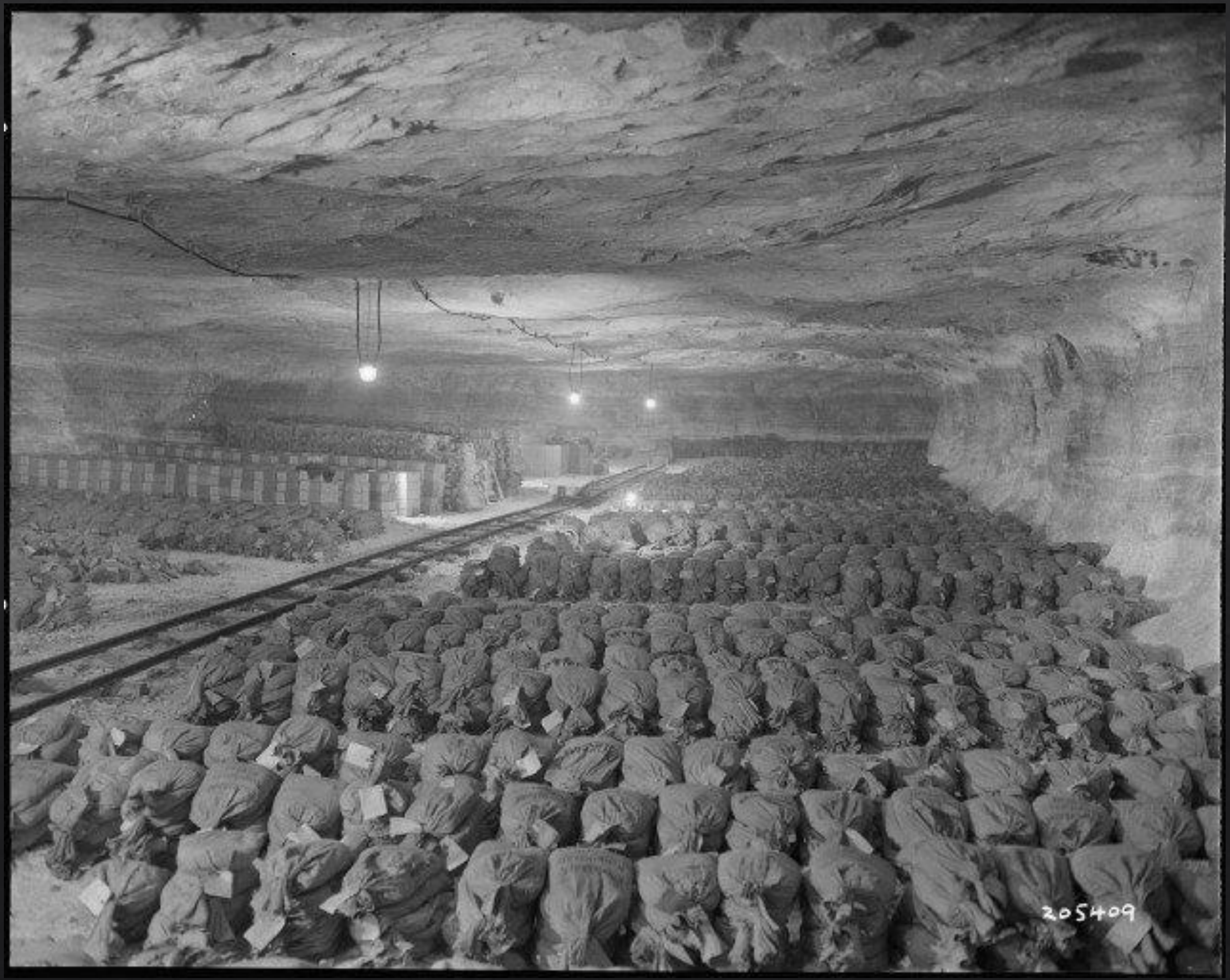
Pada 7 Maret 2017 (hampir 2 tahun yang lalu), Wikileaks mempost gambar-gambar yang merujuk ke sesuatu. Post ini benar-benar membuat orang bertanya apa yang akan dibocorkan oleh Wikileaks dalam waktu dekat. Post itu antara lain :

What is #Vault7?

The **Svalbard Global Seed Vault**

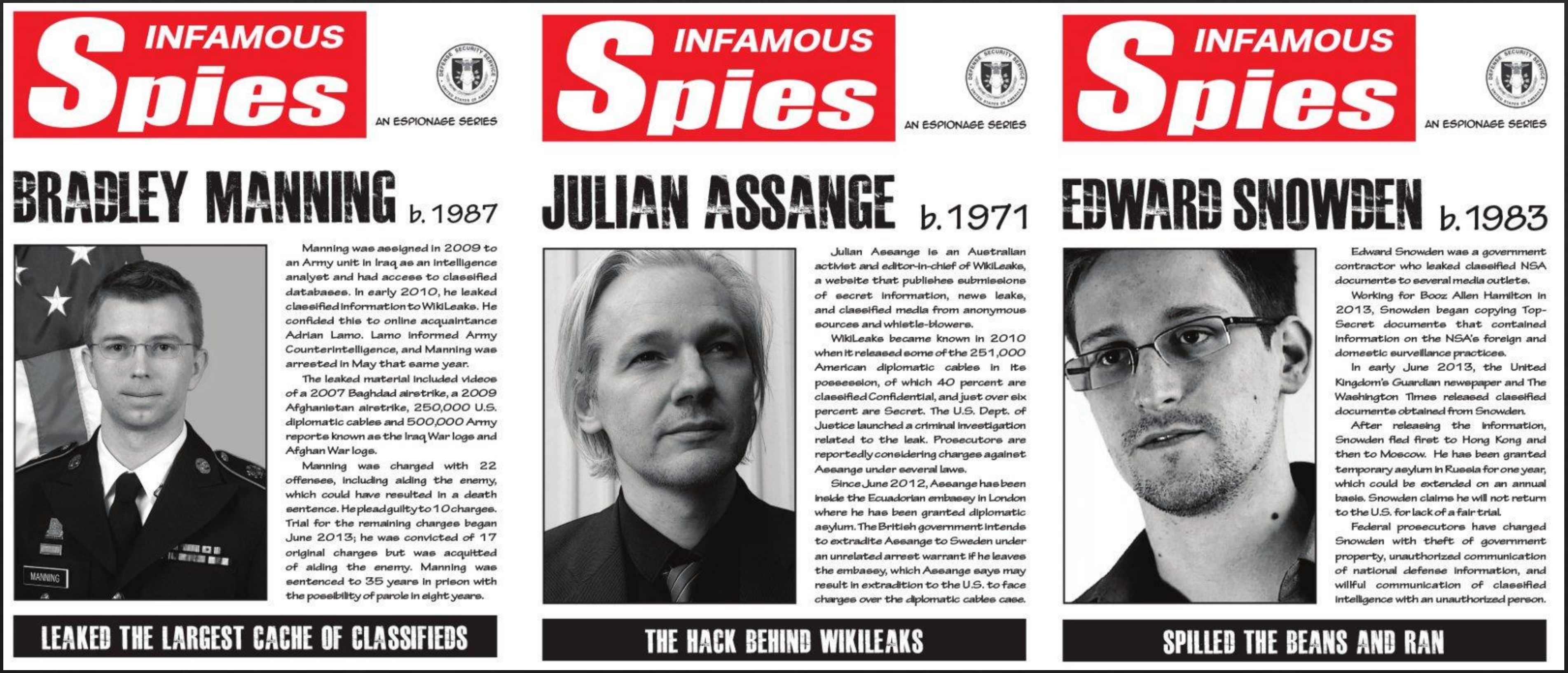
- a secure seed bank on the Norwegian island of Spitsbergen near Longyearbyen in the remote ArcticSvalbard archipelago,
- about 1,300 kilometres (810 mi) from the North Pole.[5] Conservationist Cary Fowler,
- in association with the Consultative Group on International Agricultural Research (CGIAR),[6] started the vault to preserve a wide variety of plant seeds that are duplicate samples, or "spare" copies, of seeds held in gene banks worldwide.
- The seed vault is an attempt to ensure against the loss of seeds in other genebanks during large-scale regional or global crises. The seed vault is managed under terms spelled out in a tripartite agreement between the Norwegian government, the Crop Trust and the Nordic Genetic Resource Center (NordGen).[7]

Where is #Vault7?



When is #Vault7?

Who is #Vault7?



INFAMOUS Spies

AN ESPIONAGE SERIES

BRADLEY MANNING b. 1987

Manning was assigned in 2009 to an Army unit in Iraq as an intelligence analyst and had access to classified databases. In early 2010, he leaked classified information to WikiLeaks. He confided this to online acquaintance Adrian Lamo. Lamo informed Army Counterintelligence, and Manning was arrested in May that same year.

The leaked material included videos of a 2007 Baghdad airstrike, a 2009 Afghanistan airstrike, 250,000 U.S. diplomatic cables and 500,000 Army reports known as the Iraq War logs and Afghan War logs.

Manning was charged with 22 offenses, including aiding the enemy, which could have resulted in a death sentence. He plead guilty to 10 charges. Trial for the remaining charges began June 2013; he was convicted of 17 original charges but was acquitted of aiding the enemy. Manning was sentenced to 35 years in prison with the possibility of parole in eight years.

LEAKED THE LARGEST CACHE OF CLASSIFIEDS

INFAMOUS Spies

AN ESPIONAGE SERIES

JULIAN ASSANGE b. 1971

Julian Assange is an Australian activist and editor-in-chief of WikiLeaks, a website that publishes submissions of secret information, news leaks, and classified media from anonymous sources and whistle-blowers.

WikiLeaks became known in 2010 when it released some of the 251,000 American diplomatic cables in its possession, of which 40 percent are classified Confidential, and just over six percent are Secret. The U.S. Dept. of Justice launched a criminal investigation related to the leak. Prosecutors are reportedly considering charges against Assange under several laws.

Since June 2012, Assange has been inside the Ecuadorian embassy in London where he has been granted diplomatic asylum. The British government intends to extradite Assange to Sweden under an unrelated arrest warrant if he leaves the embassy, which Assange says may result in extradition to the U.S. to face charges over the diplomatic cables case.

THE HACK BEHIND WIKILEAKS

INFAMOUS Spies

AN ESPIONAGE SERIES

EDWARD SNOWDEN b. 1983

Edward Snowden was a government contractor who leaked classified NSA documents to several media outlets.

Working for Booz Allen Hamilton in 2013, Snowden began copying Top-Secret documents that contained information on the NSA's foreign and domestic surveillance practices.

In early June 2013, the United Kingdom's *Guardian* newspaper and The Washington Times released classified documents obtained from Snowden.

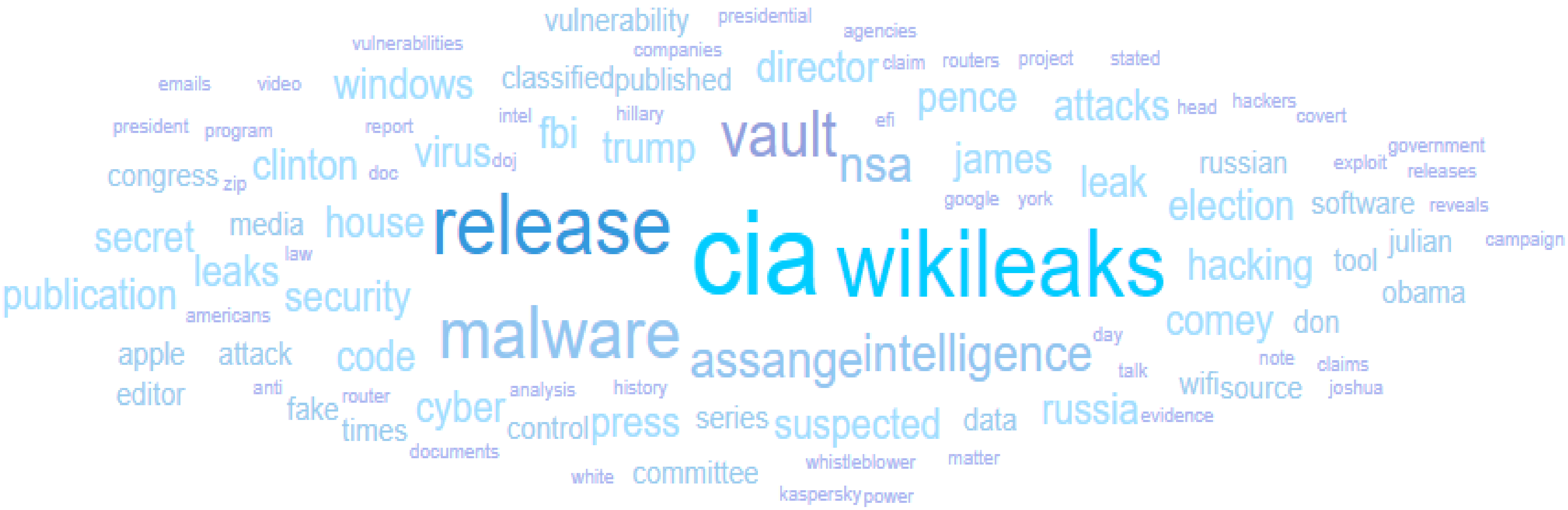
After releasing the information, Snowden fled first to Hong Kong and then to Moscow. He has been granted temporary asylum in Russia for one year, which could be extended on an annual basis. Snowden claims he will not return to the U.S. for lack of a fair trial.

Federal prosecutors have charged Snowden with theft of government property, unauthorized communication of national defense information, and willful communication of classified intelligence with an unauthorized person.

SPILLED THE BEANS AND RAN

Why is #Vault7?

How did #Vault7 make its way to WikiLeaks?


vulnerability
presidential
agencies
vulnerabilities
companies
claim
routers
project
stated
emails
video
windows
classified
published
director
pence
attacks
head
hackers
covert
intel
hillary
efi
president
program
report
fbi
trump
vault
government
virus
doj
nsa
james
russian
exploit
releases
congress
zip
clinton
doc
leak
google
york
election
software
reveals
media
house
release
secret
cia
wikileaks
julian
campaign
law
hacking
tool
leaks
publication
security
obama
americans
malware
comey
don
apple
attack
code
assange
intelligence
day
note
claims
editor
anti
router
analysis
history
talk
wifi
source
joshua
fake
cyber
russia
evidence
times
control
press
series
suspected
data
documents
whistleblower
matter
white
committee
kaspersky
power

Vault 7

- #Vault7 is not a single leak or date, it is a series.
- Ada 24 Series di dalam Vault 7
- Ada 8,761 File pada Vault 7 untuk Part 1 saja.

Vault 7, part one: "Year Zero"

Analisis

Malware CIA menargetkan iPhone, Android, TV pintar

- CIA malware dan tool hacking dibuat oleh EDG (Engineering Development Group),
- Kelompok pengembangan software dalam CCI (Center for Cyber Intelligence), yang merupakan sebuah departemen milik DDI CIA (Direktorat Inovasi Digital).
- DDI adalah salah satu dari lima direktorat utama CIA

Malware CIA menargetkan iPhone, Android, TV pintar

- "Weeping Angel" dikembangkan untuk melakukan Serangan terhadap Samsung smart TV oleh CIA's Embedded Devices Branch (EDB) bekerja sama dengan MI5 / BTSS Inggris. Setelah infestasi, Weeping Angel menempatkan TV target dalam mode 'Fake-Off', sehingga pemiliknya salah percaya bahwa TV mati saat dinyalakan.
- Dalam mode 'Fake-Off' TV beroperasi sebagai bug, merekam percakapan di ruangan dan mengirimkannya melalui Internet ke server CIA rahasia.

Malware CIA menargetkan iPhone, Android, TV pintar

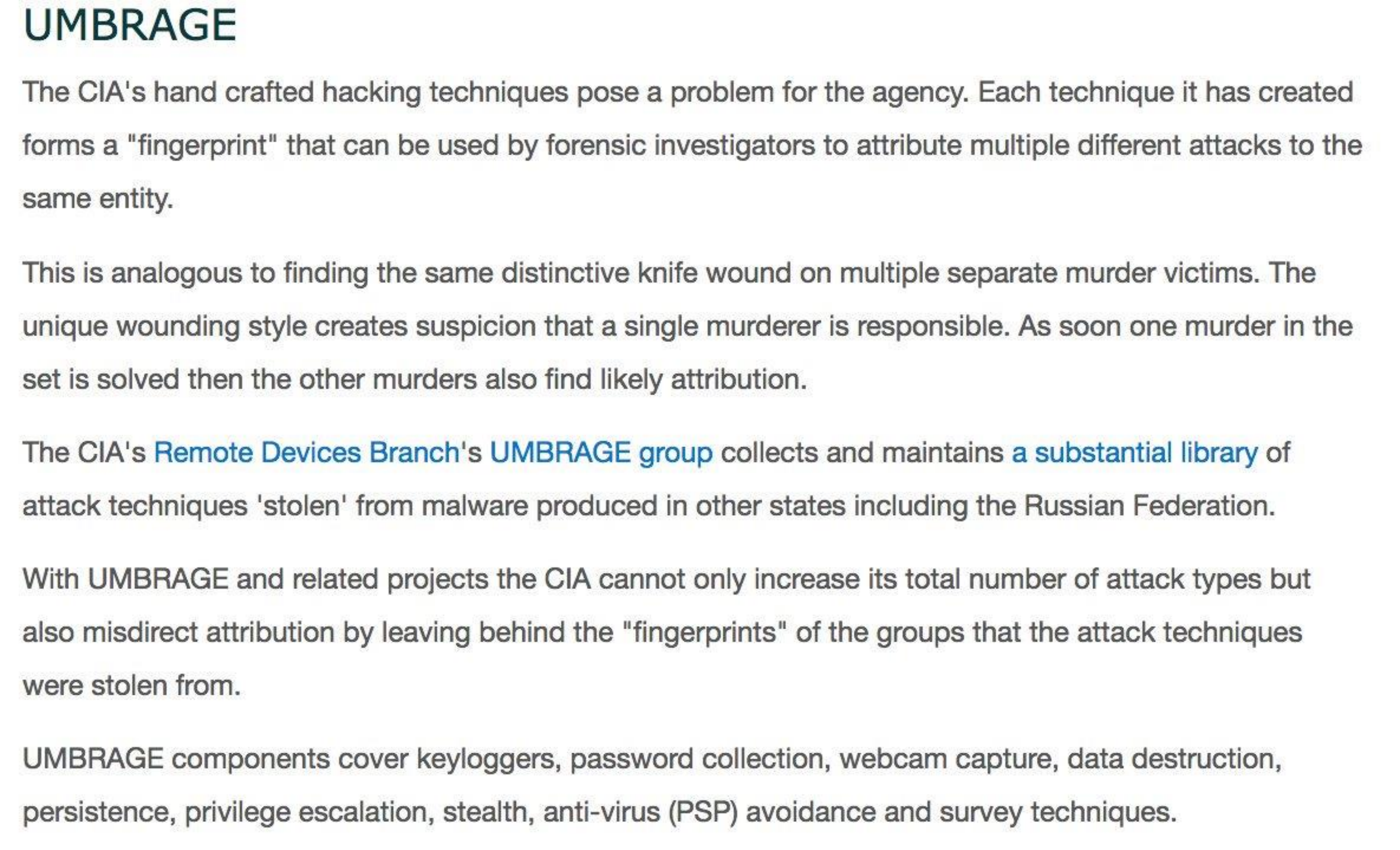
- CIA's Mobile Devices Branch (MDB) mengembangkan banyak serangan untuk meretas dan mengendalikan ponsel pintar populer dari jarak jauh . Ponsel yang terinfeksi dapat diinstruksikan untuk mengirim CIA geolokasi pengguna, komunikasi audio dan teks serta secara aktif mengaktifkan kamera dan mikrofon ponsel.

Malware CIA menargetkan Windows, OSx, Linux, router

- "Hammer Drill" virus yang menginfeksi software melalui CD/DVD
- "Brutal Kangaroo“, sistem yang menyembunyikan data pada images atau area tersembunyi pada disk
- "Assassin" and "Medusa“, automated infestation and control of CIA malware
- CIA juga mengembangkan “automated multi-platform malware attack” dan “control systems” yang mencakup Windows, Mac OS X, Solaris, Linux dan lainnya, seperti "HIVE“, "Cutthroat“, dan "Swindle" tools

Konsulat AS di Frankfurt adalah basis hacker rahasia CIA

- Selain operasinya di Langley, Virginia, CIA juga menggunakan konsulat AS di Frankfurt sebagai pangkalan rahasia bagi peretasnya yang meliputi Eropa, Timur Tengah, dan Afrika.
- Peretas CIA yang beroperasi di konsulat Frankfurt ("Pusat untuk Intelijen Dunia Maya Eropa" atau CCIE) diberikan paspor diplomatik ("hitam") dan sampul Departemen Luar Negeri. Instruksi untuk peretas CIA yang masuk membuat upaya kontra-intelijen Jerman nampak tidak penting:



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.

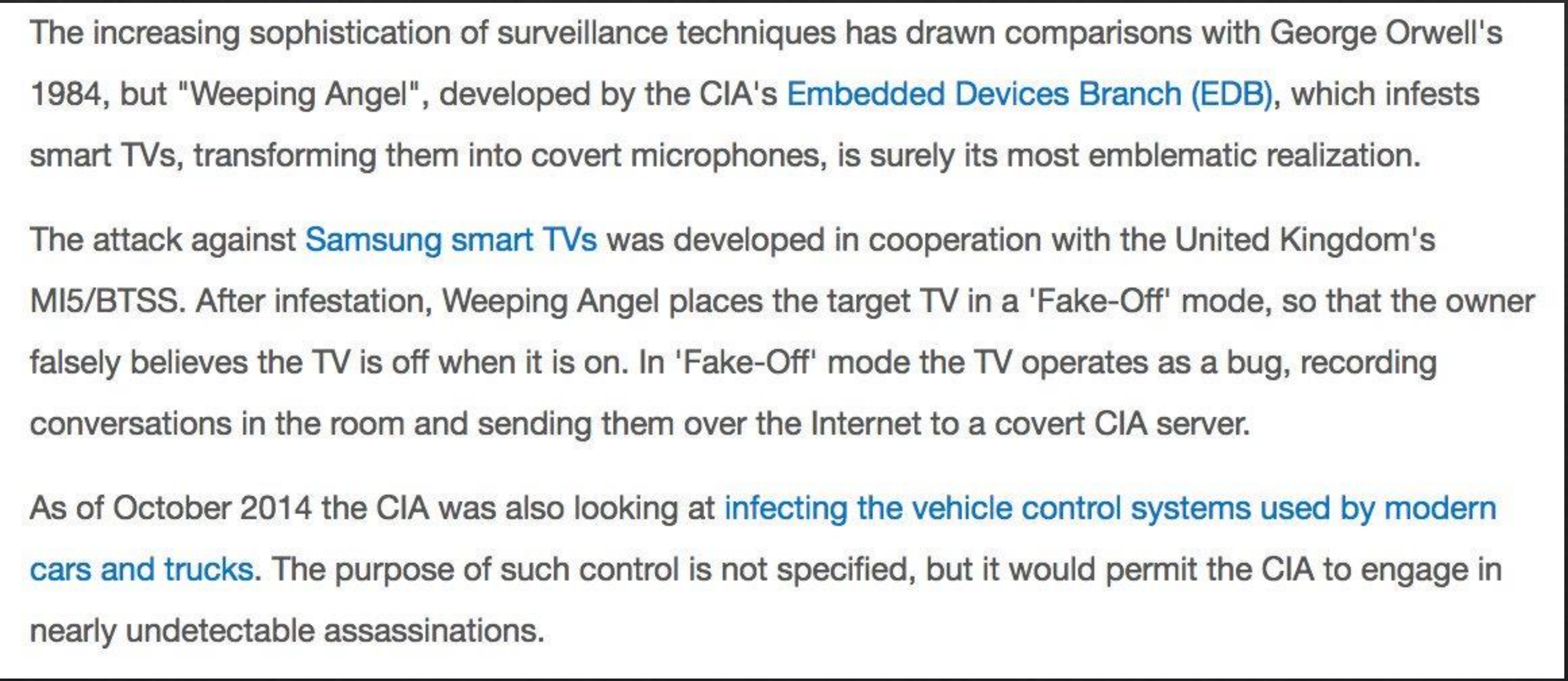
This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution.

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.

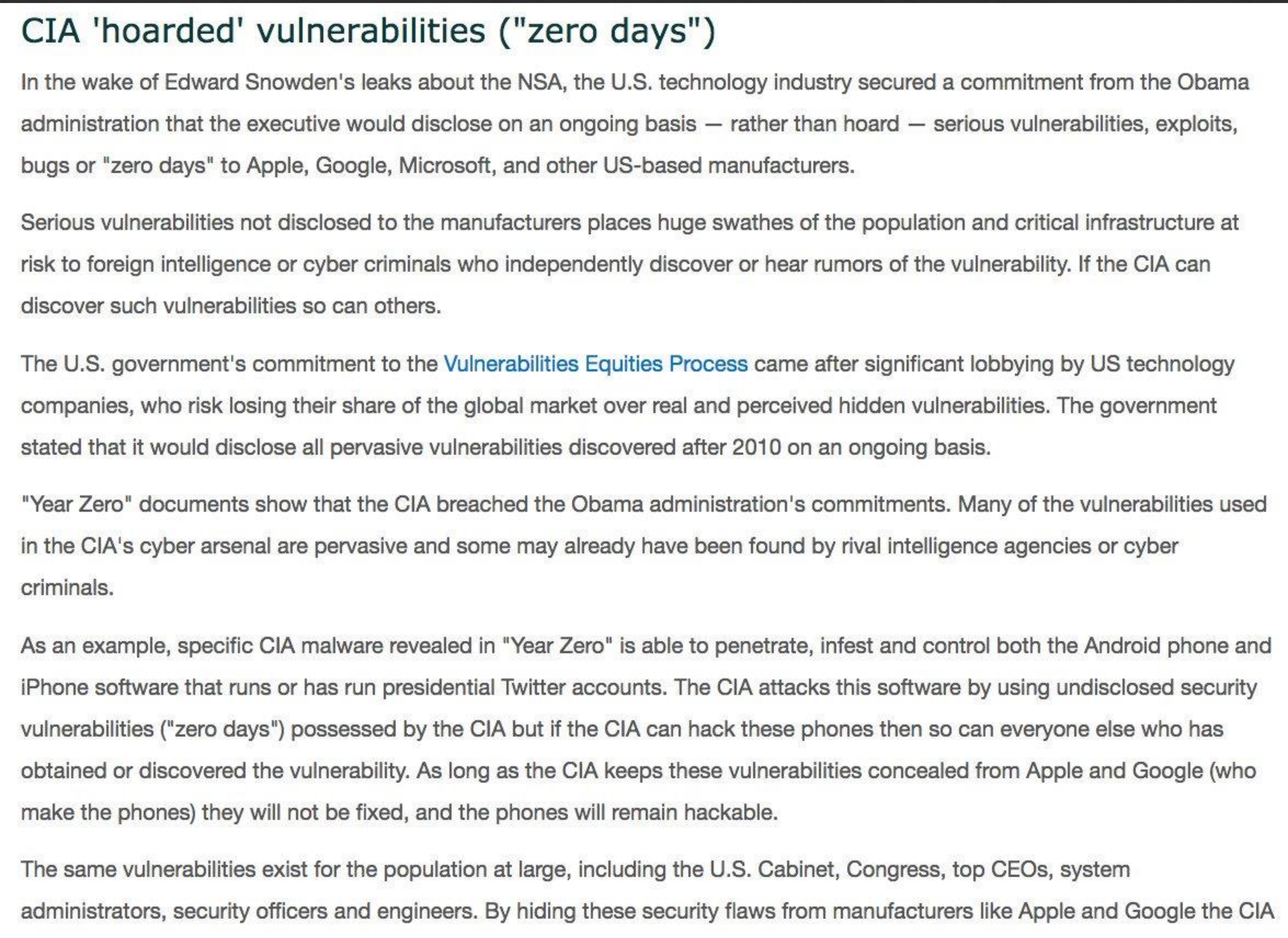
Jointly developed CIA+MI5 malware infests Samsung smart TVs to turn them into covert microphones #Vault7



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.



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.

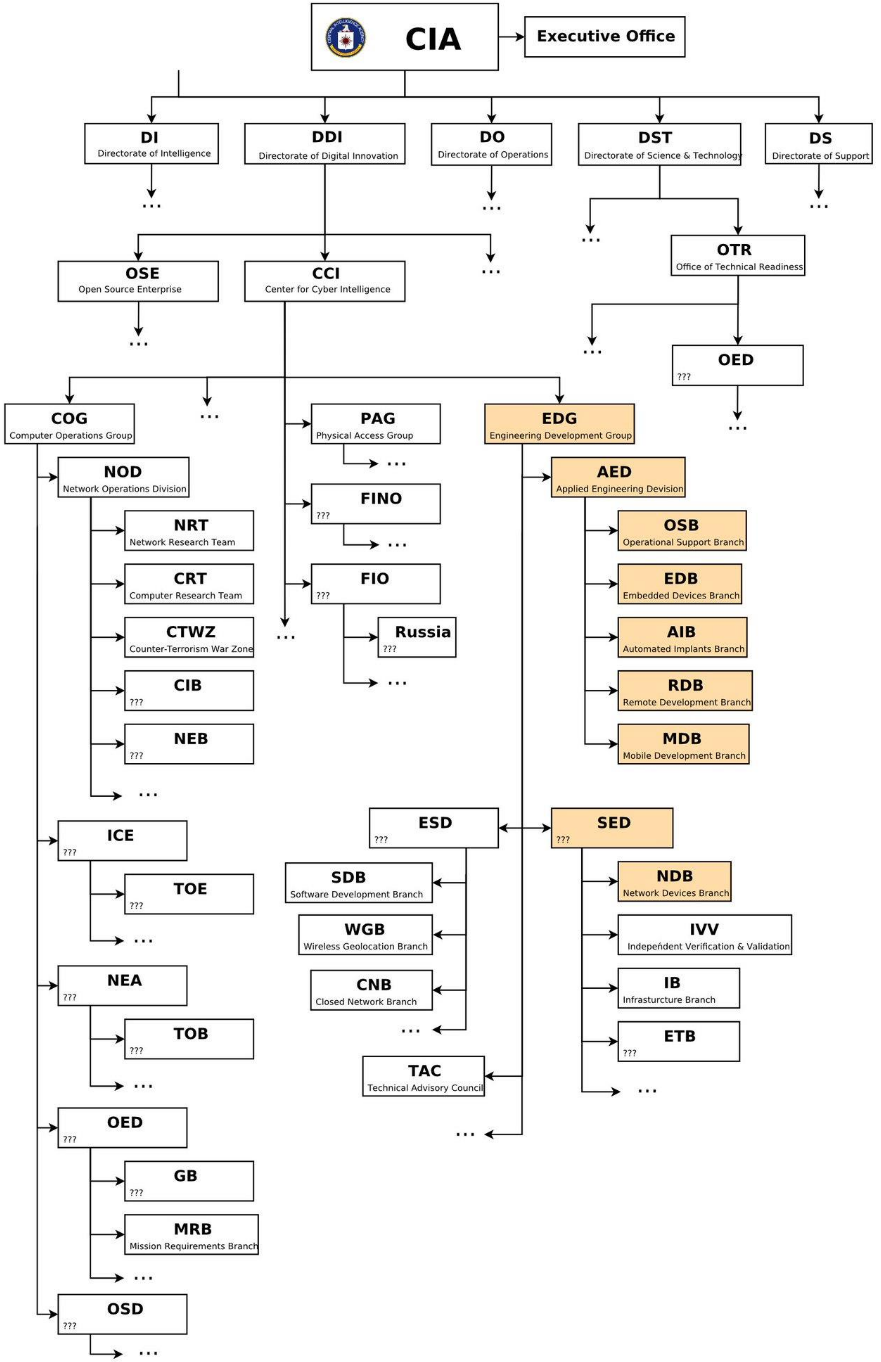
Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others.

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



CIA

Executive Office

DI
Directorate of Intelligence

DDI
Directorate of Digital Innovation

DO
Directorate of Operations

DST
Directorate of Science & Technology

DS
Directorate of Support

OSE
Open Source Enterprise

CCI
Center for Cyber Intelligence

OTR
Office of Technical Readiness

OED
???

COG
Computer Operations Group

PAG
Physical Access Group

EDG
Engineering Development Group

NOD
Network Operations Division

NRT
Network Research Team

CRT
Computer Research Team

CTWZ
Counter-Terrorism War Zone

CIB
???

NEB
???

FINO
???

FIO
???

Russia
???

AED
Applied Engineering Division

OSB
Operational Support Branch

EDB
Embedded Devices Branch

AIB
Automated Implants Branch

RDB
Remote Development Branch

MDB
Mobile Development Branch

ICE
???

TOE
???

NEA
???

TOB
???

OED
???

GB
???

MRB
Mission Requirements Branch

OSD
???

ESD
???

SDB
Software Development Branch

WGB
Wireless Geolocation Branch

CNB
Closed Network Branch

TAC
Technical Advisory Council

SED
???

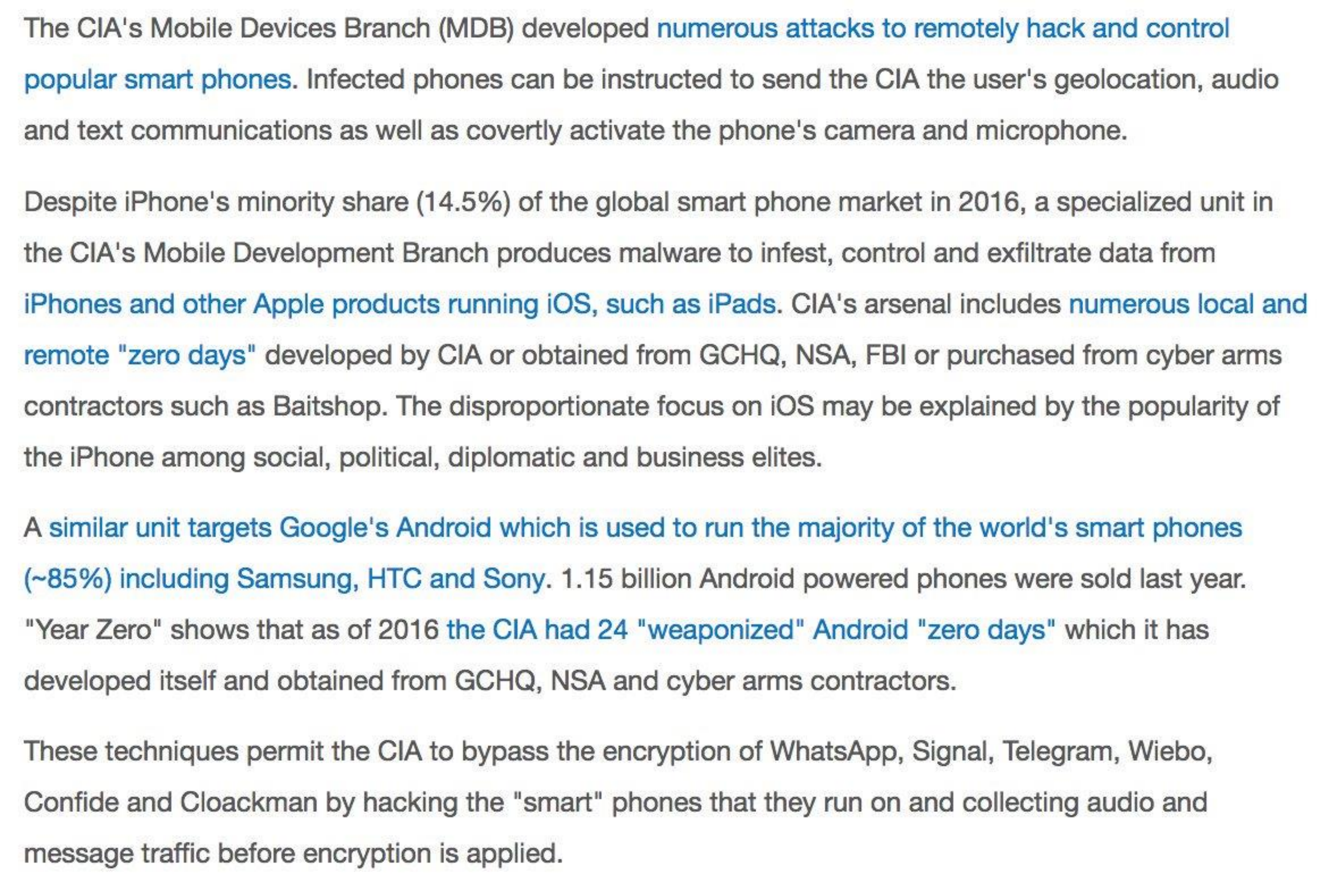
NDB
Network Devices Branch

IVV
Indepehdent Verification & Validation

IB
Infrasturcture Branch

ETB
???

WikiLeaks #Vault7 confirms CIA can effectively bypass Signal + Telegram + WhatsApp + Confide encryption



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.

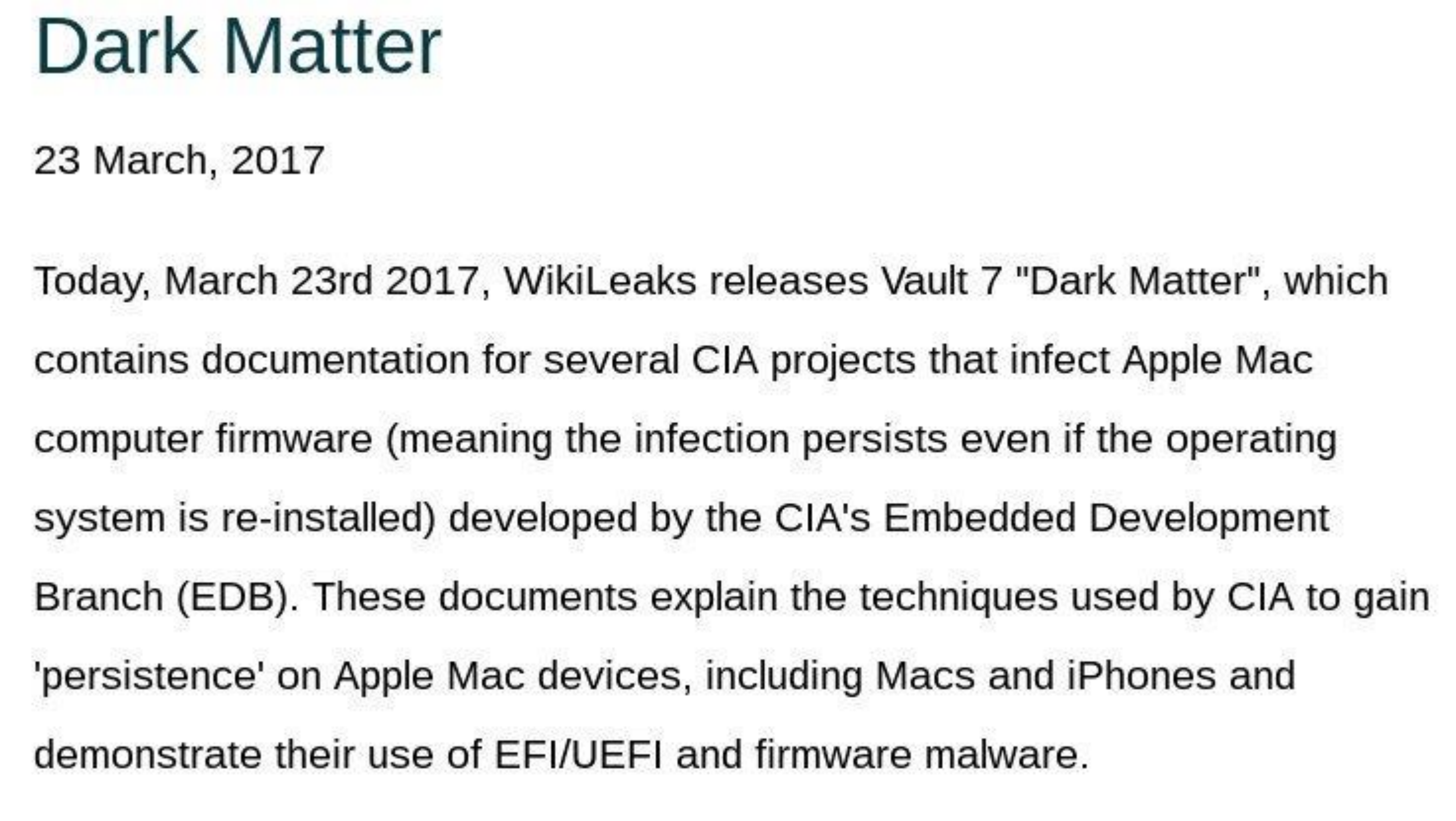
A similar unit targets Google's Android which is used to run the majority of the world's smart phones (~85%) including Samsung, HTC and Sony. 1.15 billion Android powered phones were sold last year. "Year Zero" shows that as of 2016 the CIA had 24 "weaponized" Android "zero days" which it has developed 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 tips for its hackers going to the covert CIA hacking base hidden in the US consulate in Frankfurt

- https://wikileaks.org/ciav7p1/cms/page_26607630.html

Vault 7, part two : “Dark Matter"

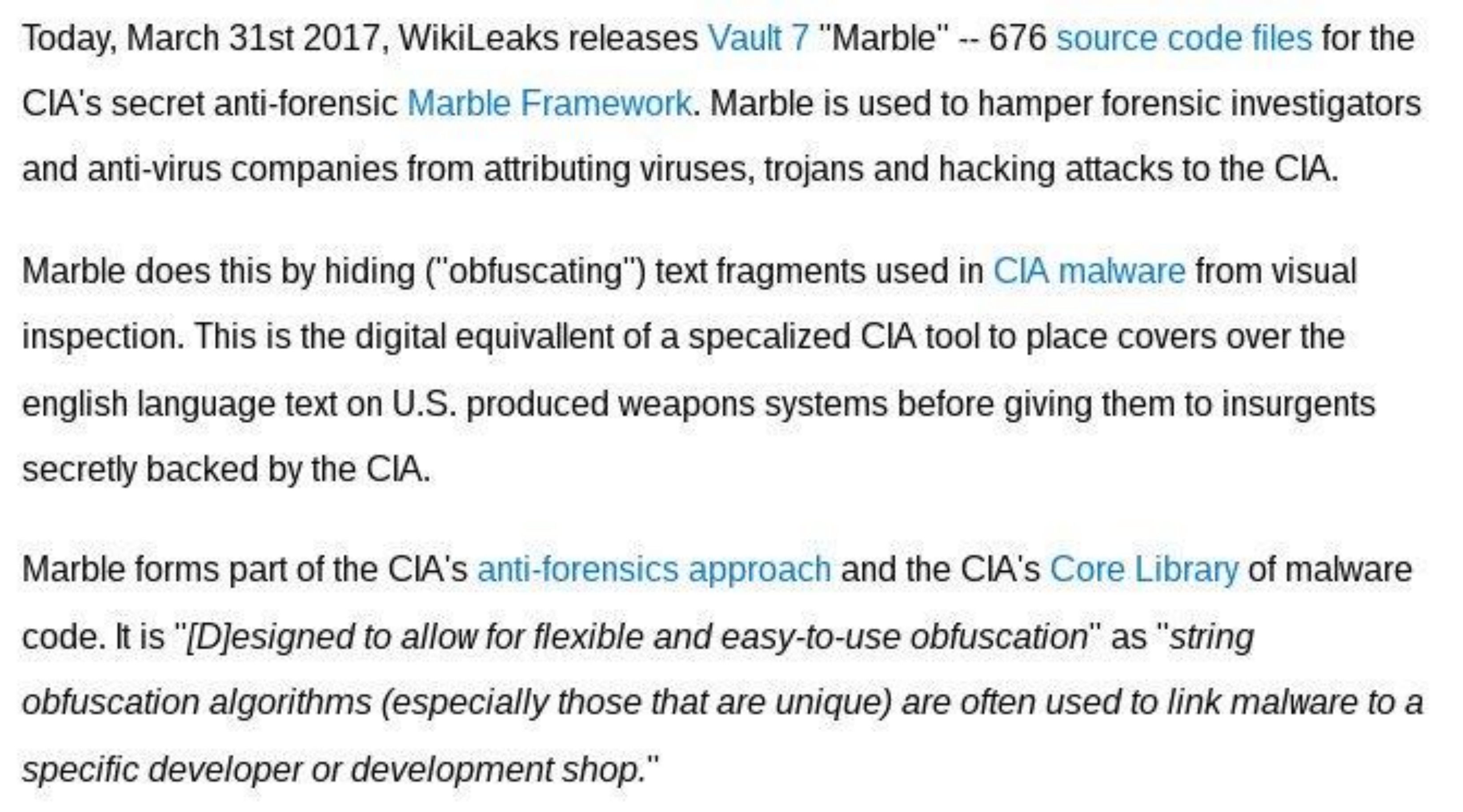


Dark Matter

23 March, 2017

Today, March 23rd 2017, WikiLeaks releases Vault 7 "Dark Matter", which contains documentation for several CIA projects that infect Apple Mac computer firmware (meaning the infection persists even if the operating system is re-installed) developed by the CIA's Embedded Development Branch (EDB). These documents explain the techniques used by CIA to gain 'persistence' on Apple Mac devices, including Macs and iPhones and demonstrate their use of EFI/UEFI and firmware malware.

CIA Vault 7 part 3 "Marble"

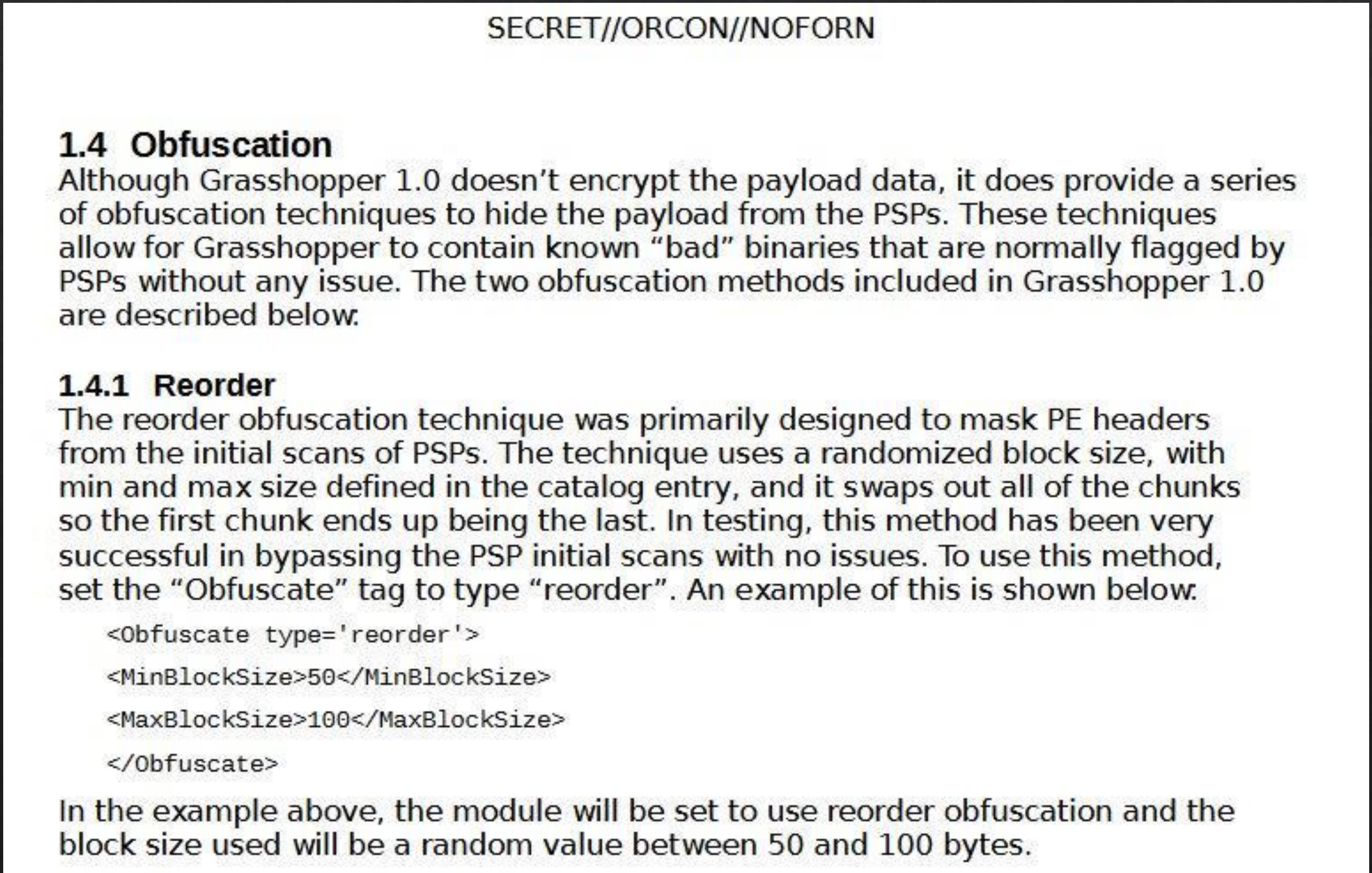


Today, March 31st 2017, WikiLeaks releases Vault 7 "Marble" -- 676 source code files for the CIA's secret anti-forensic Marble Framework. Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA.

Marble does this by hiding ("obfuscating") text fragments used in CIA malware from visual inspection. This is the digital equivallent 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.

Marble forms part of the CIA's anti-forensics approach and the CIA's Core Library of malware code. It is "*[D]esigned to allow for flexible and easy-to-use obfuscation*" as "*string obfuscation algorithms (especially those that are unique) are often used to link malware to a specific developer or development shop.*"

CIA Vault 7 Part 4 "Grasshopper"



SECRET//ORCON//NOFORN

1.4 Obfuscation

Although Grasshopper 1.0 doesn’t encrypt the payload data, it does provide a series of obfuscation techniques to hide the payload from the PSPs. These techniques allow for Grasshopper to contain known “bad” binaries that are normally flagged by PSPs without any issue. The two obfuscation methods included in Grasshopper 1.0 are described below.

1.4.1 Reorder

The reorder obfuscation technique was primarily designed to mask PE headers from the initial scans of PSPs. The technique uses a randomized block size, with min and max size defined in the catalog entry, and it swaps out all of the chunks so the first chunk ends up being the last. In testing, this method has been very successful in bypassing the PSP initial scans with no issues. To use this method, set the “Obfuscate” tag to type “reorder”. An example of this is shown below.

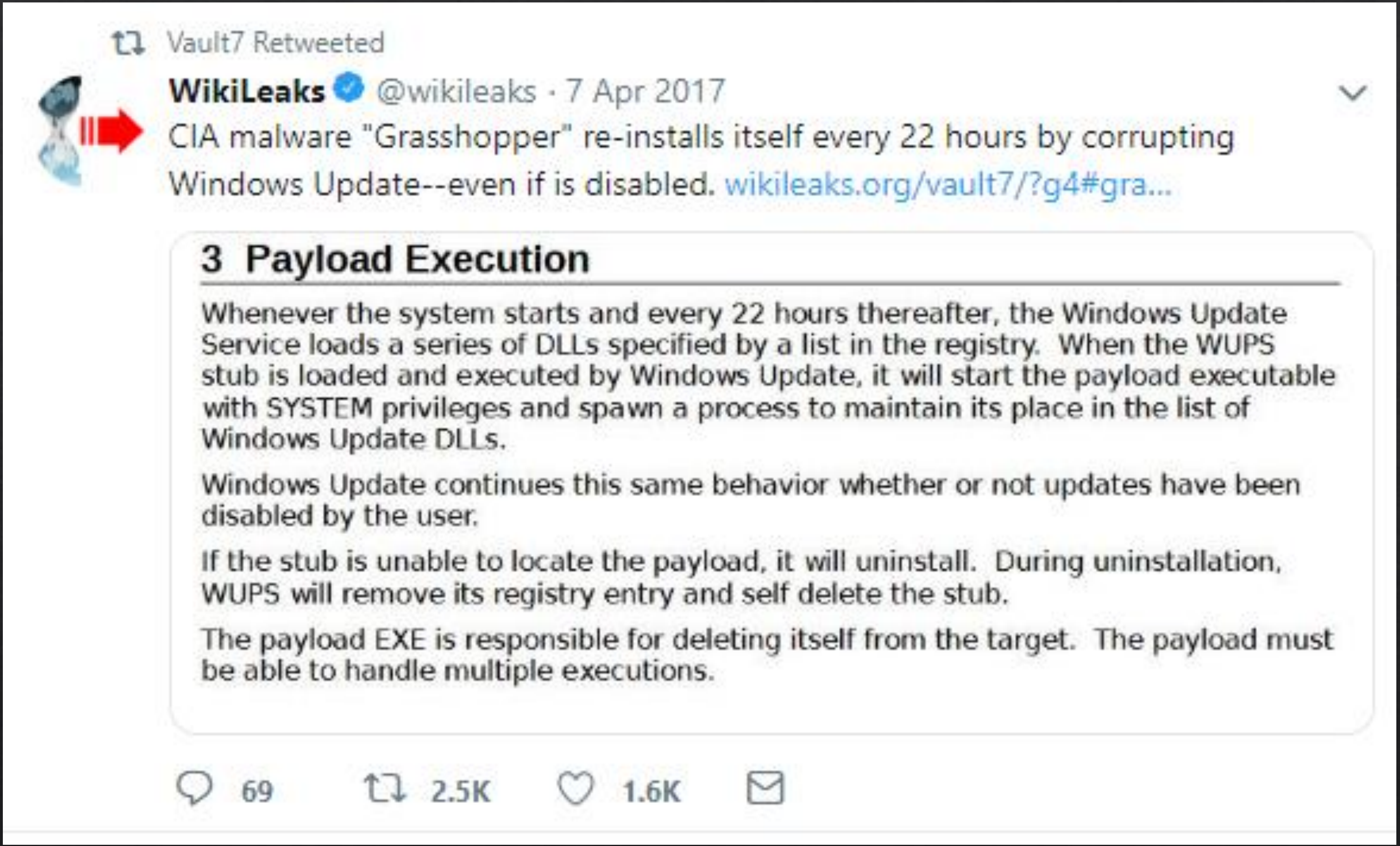
```
<Obfuscate type='reorder'>

<MinBlockSize>50</MinBlockSize>

<MaxBlockSize>100</MaxBlockSize>

</Obfuscate>
```

In the example above, the module will be set to use reorder obfuscation and the block size used will be a random value between 50 and 100 bytes.



Vault7 Retweeted

WikiLeaks @wikileaks · 7 Apr 2017

CIA malware "Grasshopper" re-installs itself every 22 hours by corrupting Windows Update--even if is disabled. wikileaks.org/vault7/?g4#gra...

3 Payload Execution

Whenever the system starts and every 22 hours thereafter, the Windows Update Service loads a series of DLLs specified by a list in the registry. When the WUPS stub is loaded and executed by Windows Update, it will start the payload executable with SYSTEM privileges and spawn a process to maintain its place in the list of Windows Update DLLs.

Windows Update continues this same behavior whether or not updates have been disabled by the user.

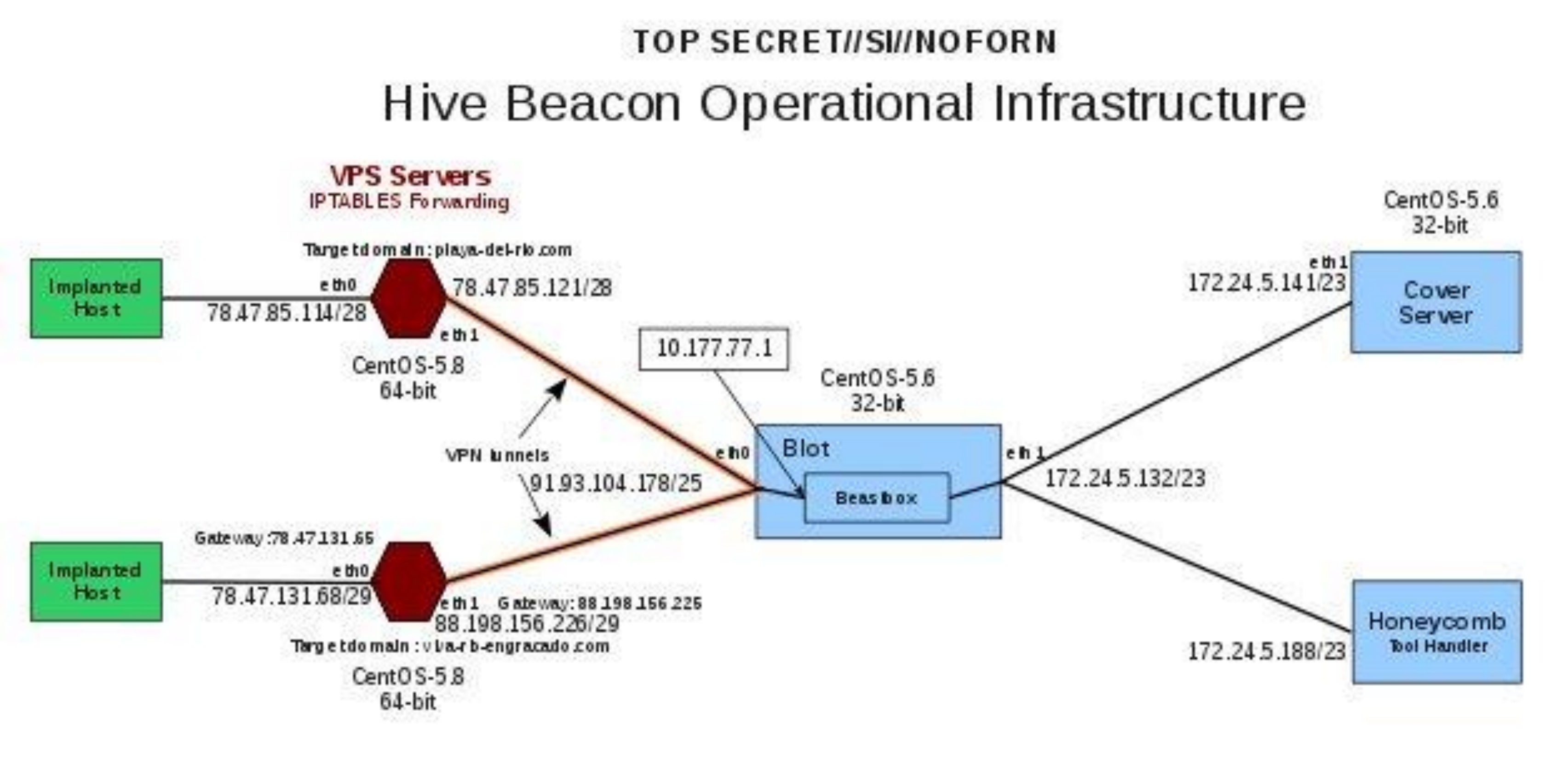
If the stub is unable to locate the payload, it will uninstall. During uninstallation, WUPS will remove its registry entry and self delete the stub.

The payload EXE is responsible for deleting itself from the target. The payload must be able to handle multiple executions.

CIA Vault 7 Part 5 “HIVE"

- Berisi tentang “CIA top-secret virus program” yang dibuat oleh "Embedded Development Branch" (EDB). 6 dokumen yang dipublikasi oleh Wikileaks berhubungan dengan “HIVE multi-platform CIA malware suite”.

- A CIA back-end infrastructure with a public-facing HTTPS interface used by CIA to transfer information from target desktop computers and smartphones to the CIA, and open those devices to receive further commands from CIA operators to execute specific tasks. Also called Listening Post (LP), and Command and Control (C2). All of the above while hiding its presence behind unsuspicious-looking public domains. This masking interface is known as "Switchblade".



TOP SECRET//SI//NOFORN

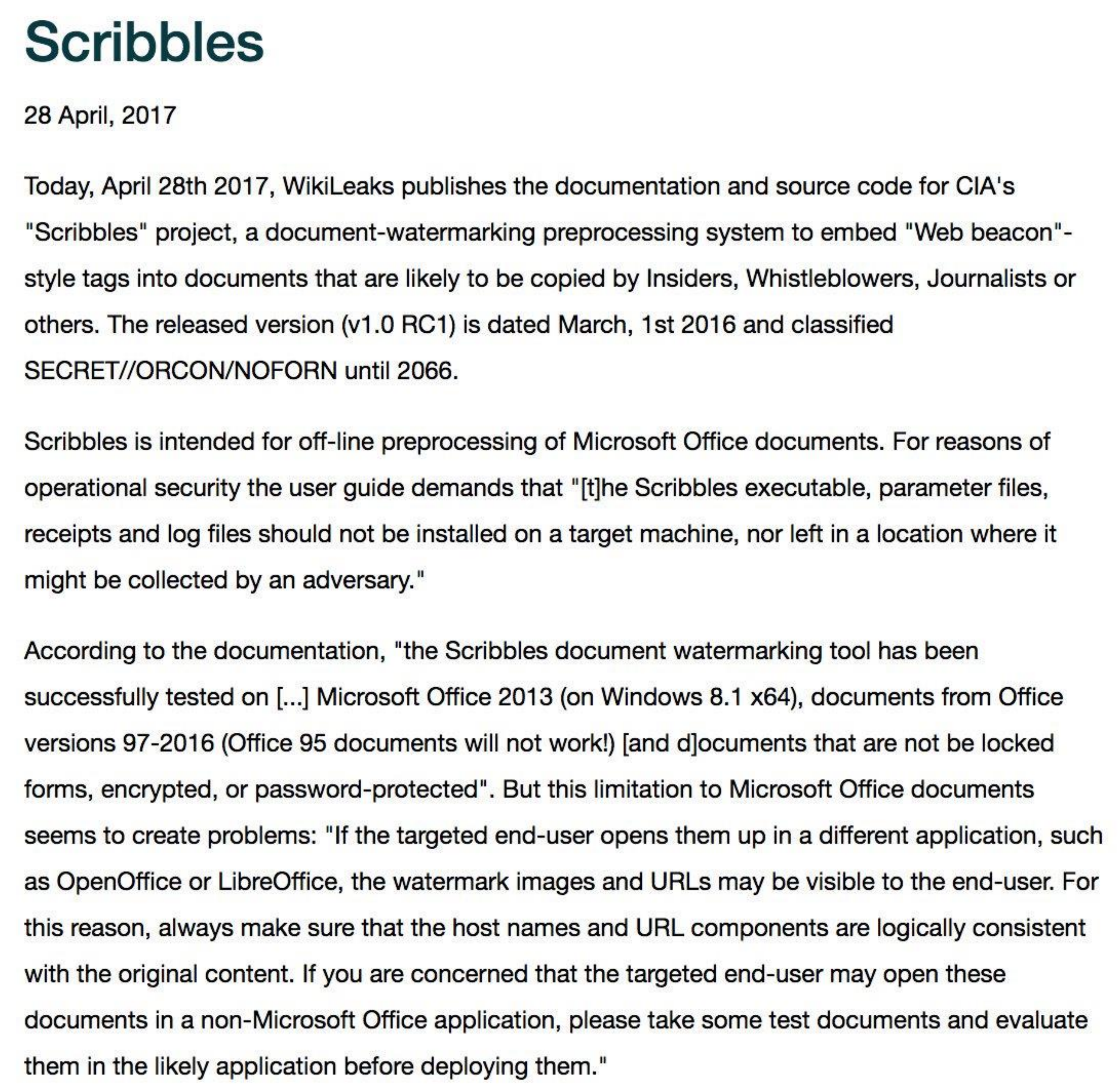
Hive Beacon Operational Infrastructure

CIA Vault 7 Part 6 "Weeping Angel"

- Which is a hacking tool co-developed by the CIA and MI5. Used to exploit a series of smart TVs for the purpose of covert intelligence gathering. Once installed in suitable televisions with a USB stick, the hacking tool enables those televisions' built-in microphones and possibly video cameras to record their surroundings, while the televisions falsely appear to be turned off. The recorded data is then either stored locally into the television's memory or sent over the internet to the CIA. Allegedly both the CIA and MI5 agencies collaborated to develop that malware and coordinated their work in Joint Development Workshops.[29][30][31] As of this part 6 publication, "Weeping Angel" is the second major CIA hacking tool which notably references the British television show, Dr. Who, alongside "Sonic Screwdriver" in "Dark Matter"

CIA Vault 7 Part 7 "Scribbles"

- CIA's anti-leak document watermarking system
- The leak includes documentation and source code of a tool intended to track documents leaked to whistleblowers and journalists by embedding web beacon tags into classified documents to trace who leaked them.[34][35] The tool affects Microsoft Office documents, specifically "Microsoft Office 2013 (on Windows 8.1 x64), documents from Office versions 97-2016 (Office 95 documents will not work!) [and d]ocuments that are not [locked], encrypted, or password-protected".[36] When a CIA watermarked document is opened, an invisible image within the document that is hosted on the agency's server is loaded, generating a HTTP request. The request is then logged on the server, giving the intelligence agency information about who is opening it and where it is being opened. However, if a watermarked document is opened in an alternative word processor the image may be visible to the viewer. The documentation also states that if the document is viewed offline or in protected view, the watermarked image will not be able to contact its home server. This is only overridden when a user enables editing



Scribbles

28 April, 2017

Today, April 28th 2017, WikiLeaks publishes the documentation and source code for CIA's "Scribbles" project, a document-watermarking preprocessing system to embed "Web beacon"-style tags into documents that are likely to be copied by Insiders, Whistleblowers, Journalists or others. The released version (v1.0 RC1) is dated March, 1st 2016 and classified SECRET//ORCON/NOFORN until 2066.

Scribbles is intended for off-line preprocessing of Microsoft Office documents. For reasons of operational security the user guide demands that "[t]he Scribbles executable, parameter files, receipts and log files should not be installed on a target machine, nor left in a location where it might be collected by an adversary."

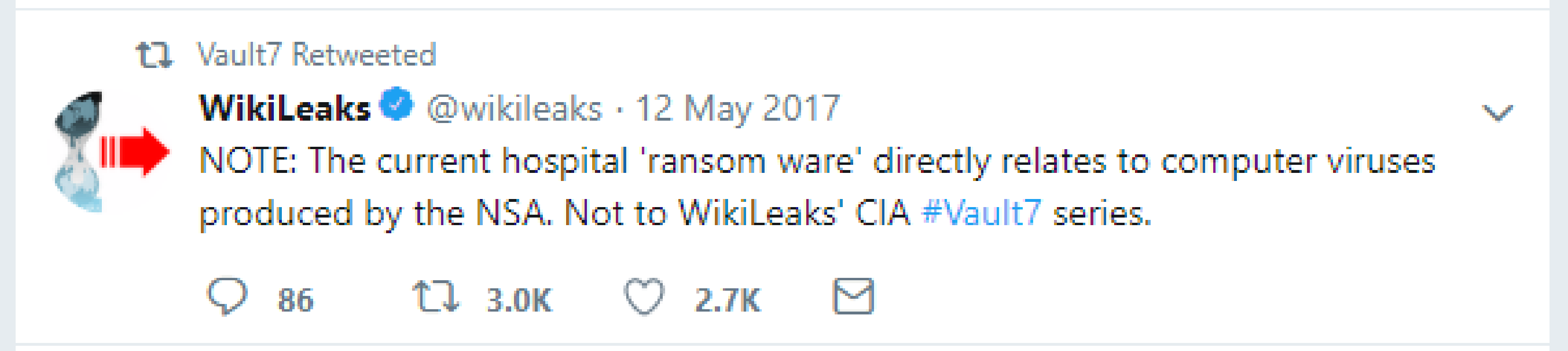
According to the documentation, "the Scribbles document watermarking tool has been successfully tested on [...] Microsoft Office 2013 (on Windows 8.1 x64), documents from Office versions 97-2016 (Office 95 documents will not work!) [and d]ocuments that are not be locked forms, encrypted, or password-protected". But this limitation to Microsoft Office documents seems to create problems: "If the targeted end-user opens them up in a different application, such as OpenOffice or LibreOffice, the watermark images and URLs may be visible to the end-user. For this reason, always make sure that the host names and URL components are logically consistent with the original content. If you are concerned that the targeted end-user may open these documents in a non-Microsoft Office application, please take some test documents and evaluate them in the likely application before deploying them."

CIA Vault 7 Part 8 "Archimedes"

- According to U.S. SANS Institute instructor Jake Williams, who analyzed the published documents, Archimedes is a virus previously codenamed "Fulcrum". According to cyber security expert and ENISA member Pierluigi Paganini, the CIA operators use Archimedes to redirect local area network(LAN) web browser sessions from a targeted computer through a computer controlled by the CIA before the sessions are routed to the users. This type of attack is known as man-in-the-middle (MitM). With their publication WikiLeaks included a number of hashes that they claim can be used to potentially identify the Archimedes virus and guard against it in the future. Paganini stated that potential targeted computers can search for those hashes on their systems to check if their systems had been attacked by the CIA.

- 5 May, 2017
- Today, May 5th 2017, WikiLeaks publishes "Archimedes", a tool used by the CIA to attack a computer inside a Local Area Network (LAN), usually used in offices. It allows the re-directing of traffic from the target computer inside the LAN through a computer infected with this malware and controlled by the CIA. This technique is used by the CIA to redirect the target's computers web browser to an exploitation server while appearing as a normal browsing session.
- The document illustrates a type of attack within a "protected environment" as the the tool is deployed into an existing local network abusing existing machines to bring targeted computers under control and allowing further exploitation and abuse.

- Tweet setelah ini lebih menceritakan kondisi sekarang sebagai dampak dari publikasi dokumen rahasia.



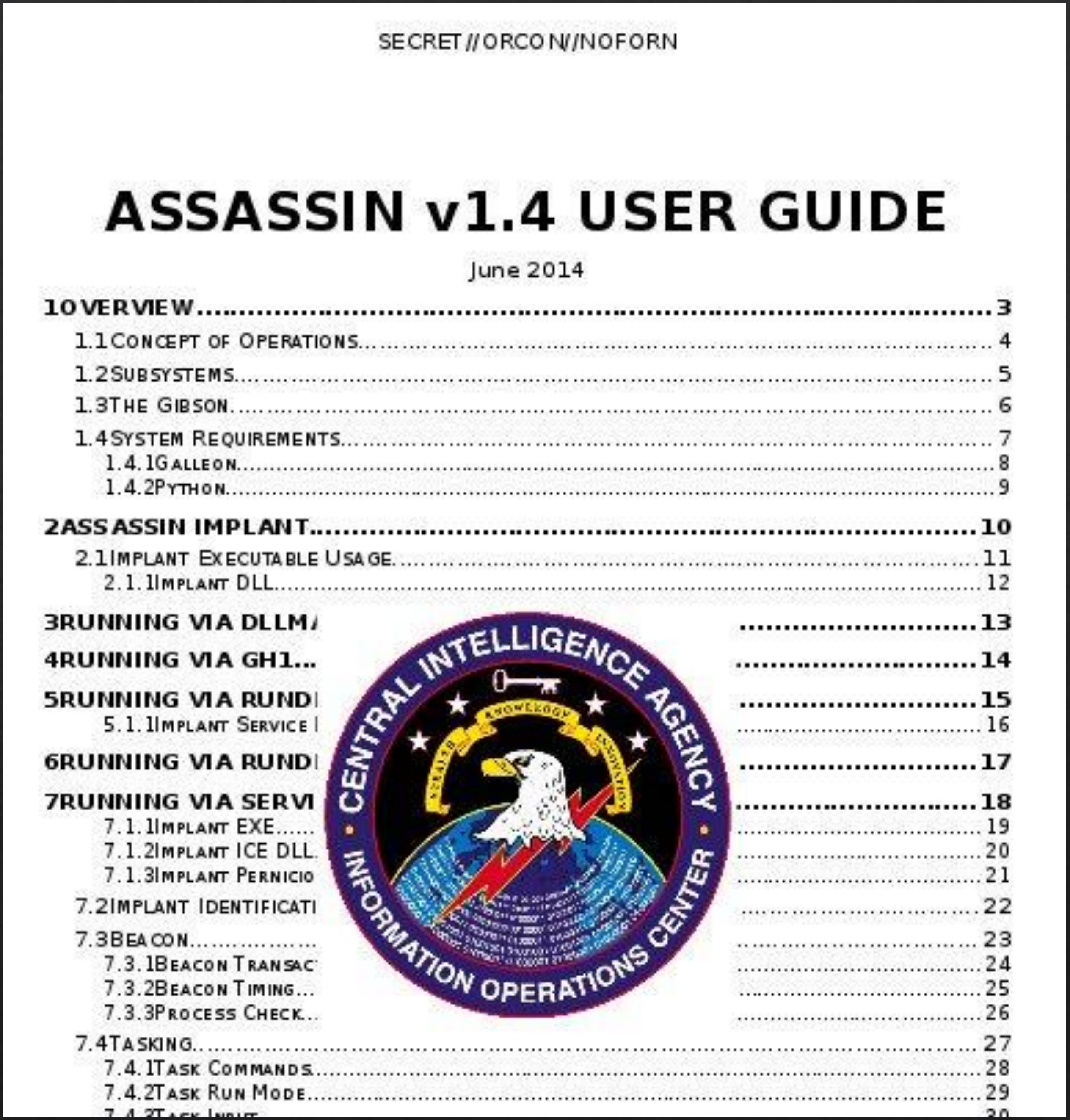
Vault7 Retweeted

WikiLeaks @wikileaks · 12 May 2017

NOTE: The current hospital 'ransom ware' directly relates to computer viruses produced by the NSA. Not to WikiLeaks' CIA #Vault7 series.

CIA Vault 7 Part 9 "AfterMidnight" and "Assassin"

- AfterMidnight is a malware installed on a target personal computer and disguises as a DLL file, which is executed while the user's computer reboots. It then triggers a connection to the CIA's Command and Control (C2) computer, from which it downloads various modules to run. As for Assassin, it is very similar to its AfterMidnight counterpart, but deceptively runs inside a Windows service process. CIA operators reportedly use Assassin as a C2 to execute a series of tasks, collect, and then periodically send user data to the CIA Listening Post(s) (LP). Similar to backdoor Trojan behavior. Both AfterMidnight and Assassin run on Windows operating system, are persistent, and periodically beacon to their configured LP to either request tasks or send private information to the CIA, as well as automatically uninstall themselves on a set date and time.



SECRET//ORCON//NOFORN

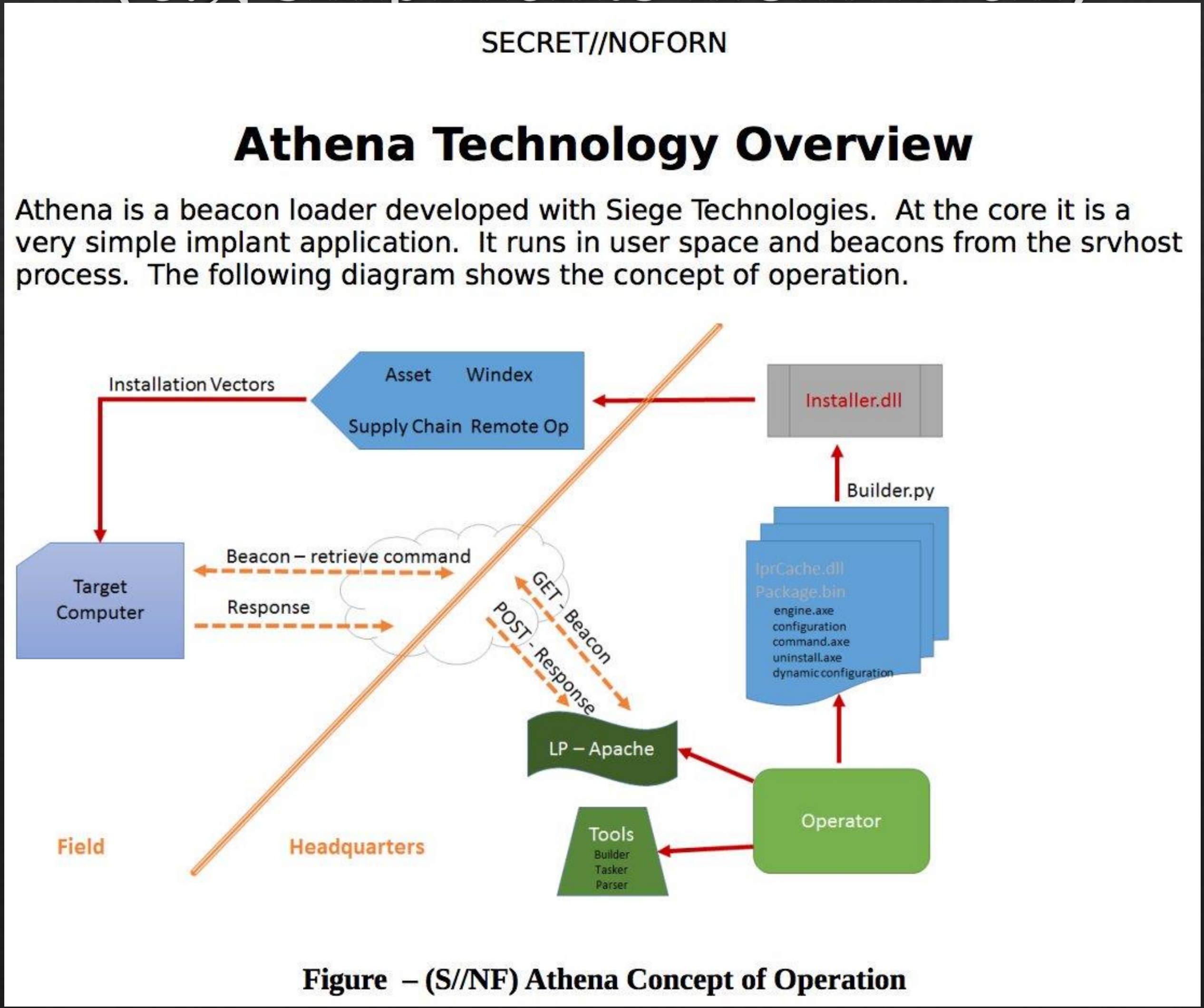
ASSASSIN v1.4 USER GUIDE

June 2014

CIA Vault 7 Part 10 "Athena”

- The published user guide, demo, and related documents were created between September 2015 and February 2016. They are all about a malware allegedly developed for the CIA in August 2015, roughly one month after Microsoft released Windows 10 with their firm statements about how difficult it was to compromise. Both the primary "Athena" malware and its secondary malware named "Hera" are similar in theory to Grasshopper and AfterMidnight malware but with some significant differences. One of those differences is that Athena and Hera were developed by the CIA with a New Hampshire private corporation called Siege Technologies. During a Bloomberg 2014 interview the founder of Siege Technologies confirmed and justified their development of such malware. Athena malware completely hijacks Windows' Remote Access services, while Hera hijacks Windows Dnscache service. Also both Athena and Hera affect all current versions of Windows including, but not limited to, Windows Server 2012 and Windows 10. Another difference is in the types of encryption used between the infected computers and the CIA Listening Posts (LP). As for the similarities, they exploit persistent DLL files to create a backdoor to communicate with CIA's LP, steal private data, then send it to CIA servers, or delete private data on the target computer, as well as Command and Control (C2) for CIA operatives to send additional malicious software to further run specific tasks on the attacked computer. All of the above designed to deceive computer security software. Beside the published detailed documents, WikiLeaks has not provided any evidence suggesting the CIA used Athena or not

CIA's Athena malware is designed to be injected into a target's supply chain (e.g shipments from Dell)



SECRET//NOFORN

Athena Technology Overview

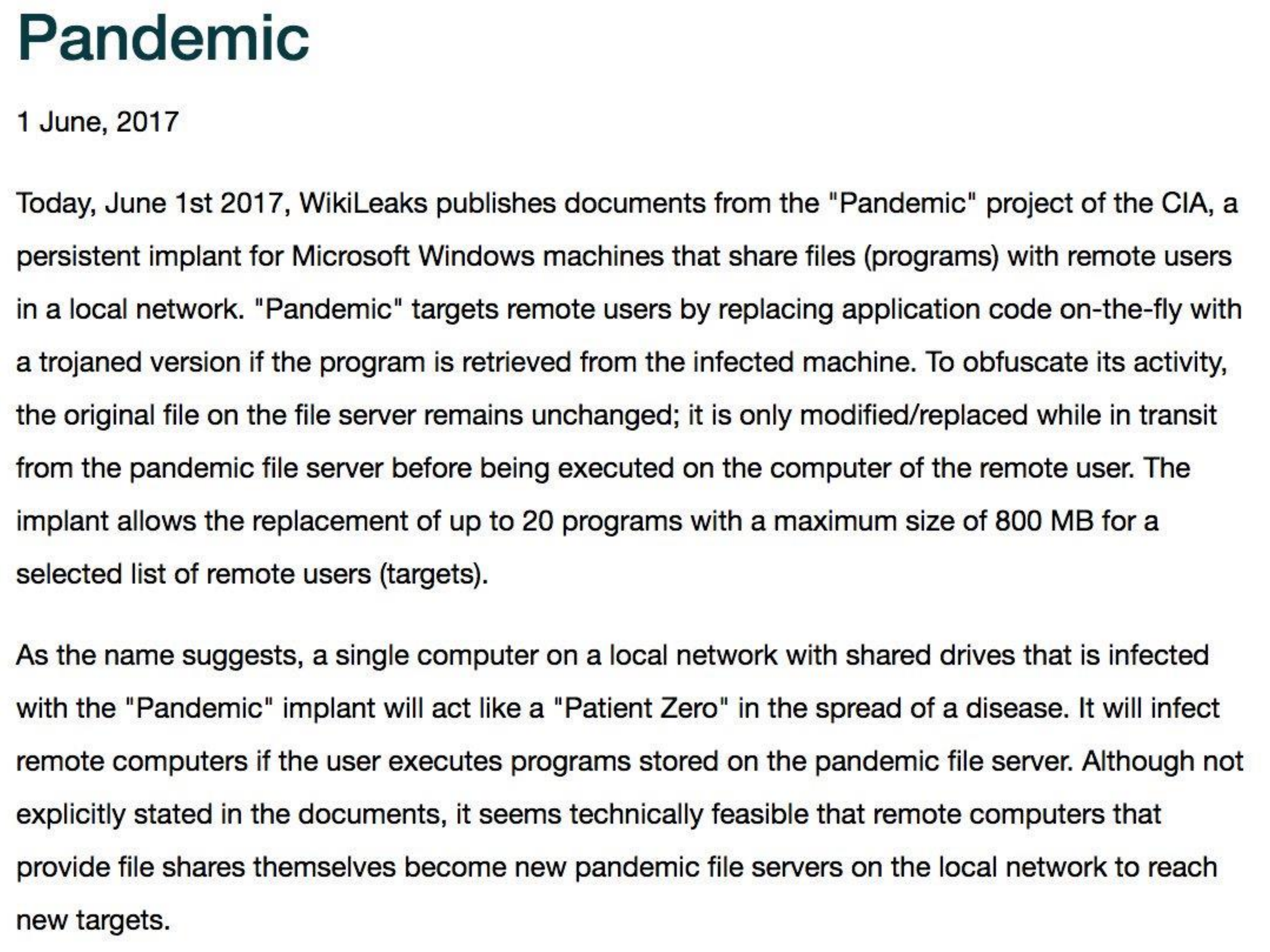
Athena is a beacon loader developed with Siege Technologies. At the core it is a very simple implant application. It runs in user space and beacons from the srvhost process. The following diagram shows the concept of operation.

Installation Vectors
Asset
Windex
Supply Chain
Remote Op
Installer.dll
Builder.py
lprCache.dll
Package.bin
engine.axe
configuration
command.axe
uninstall.axe
dynamic configuration
Target Computer
Beacon – retrieve command
Response
GET - Beacon
POST - Response
LP – Apache
Operator
Tools
Builder
Tasker
Parser
Field
Headquarters

Figure – (S//NF) Athena Concept of Operation

CIA Vault 7 Part 11 "Pandemic"

- This tool serves as a persistent implant affecting Windows machines with shared folders. It functions as a file system filter driver on an infected computer, and listens for Server Message Block traffic while detecting download attempts from other computers on a local network. "Pandemic" will answer a download request on behalf of the infected computer. However, it will replace the legitimate file with malware. In order to obfuscate its activities, "Pandemic" only modifies or replaces the legitimate file in transit, leaving the original on the server unchanged. The implant allows 20 files to be modified at a time, with a maximum individual file size of 800MB. While not stated in the leaked documentation, it is possible that newly infected computers could themselves become "Pandemic" file servers, allowing the implant to reach new targets on a local network.

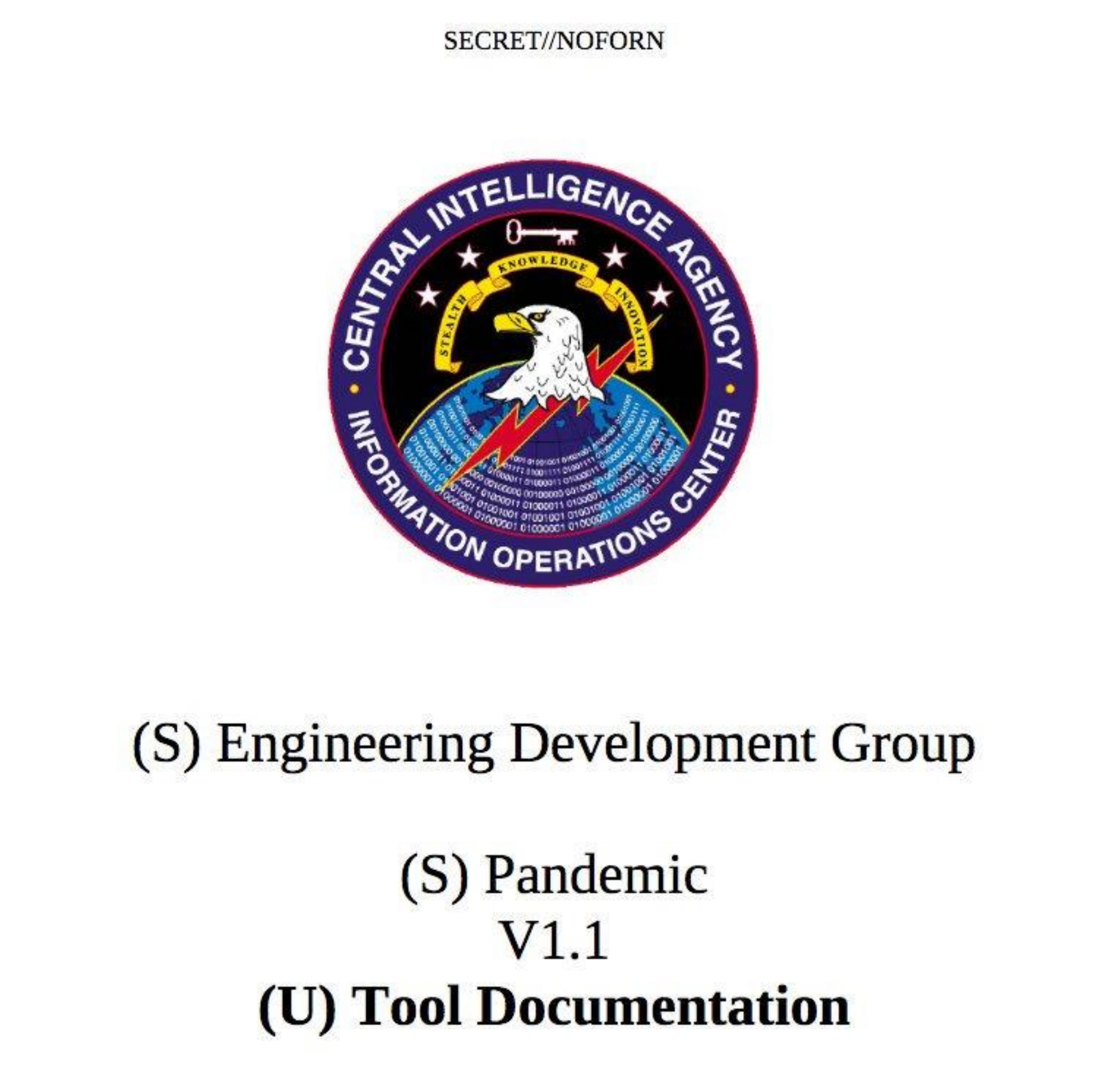


Pandemic

1 June, 2017

Today, June 1st 2017, WikiLeaks publishes documents from the "Pandemic" project of the CIA, a persistent implant for Microsoft Windows machines that share files (programs) with remote users in a local network. "Pandemic" targets remote users by replacing application code on-the-fly with a trojaned version if the program is retrieved from the infected machine. To obfuscate its activity, the original file on the file server remains unchanged; it is only modified/replaced while in transit from the pandemic file server before being executed on the computer of the remote user. The implant allows the replacement of up to 20 programs with a maximum size of 800 MB for a selected list of remote users (targets).

As the name suggests, a single computer on a local network with shared drives that is infected with the "Pandemic" implant will act like a "Patient Zero" in the spread of a disease. It will infect remote computers if the user executes programs stored on the pandemic file server. Although not explicitly stated in the documents, it seems technically feasible that remote computers that provide file shares themselves become new pandemic file servers on the local network to reach new targets.

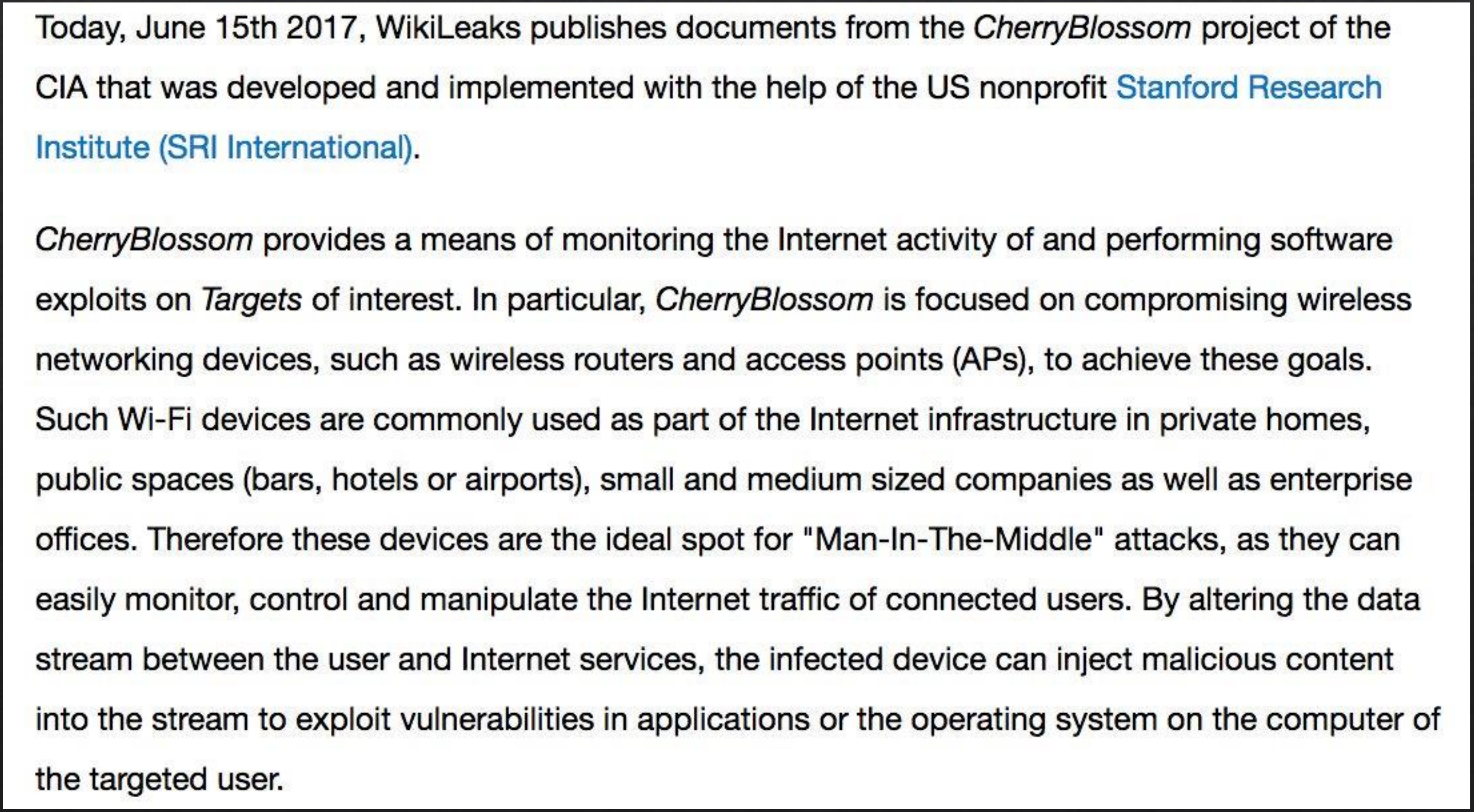


(S) Engineering Development Group

(S) Pandemic
V1.1

(U) Tool Documentation

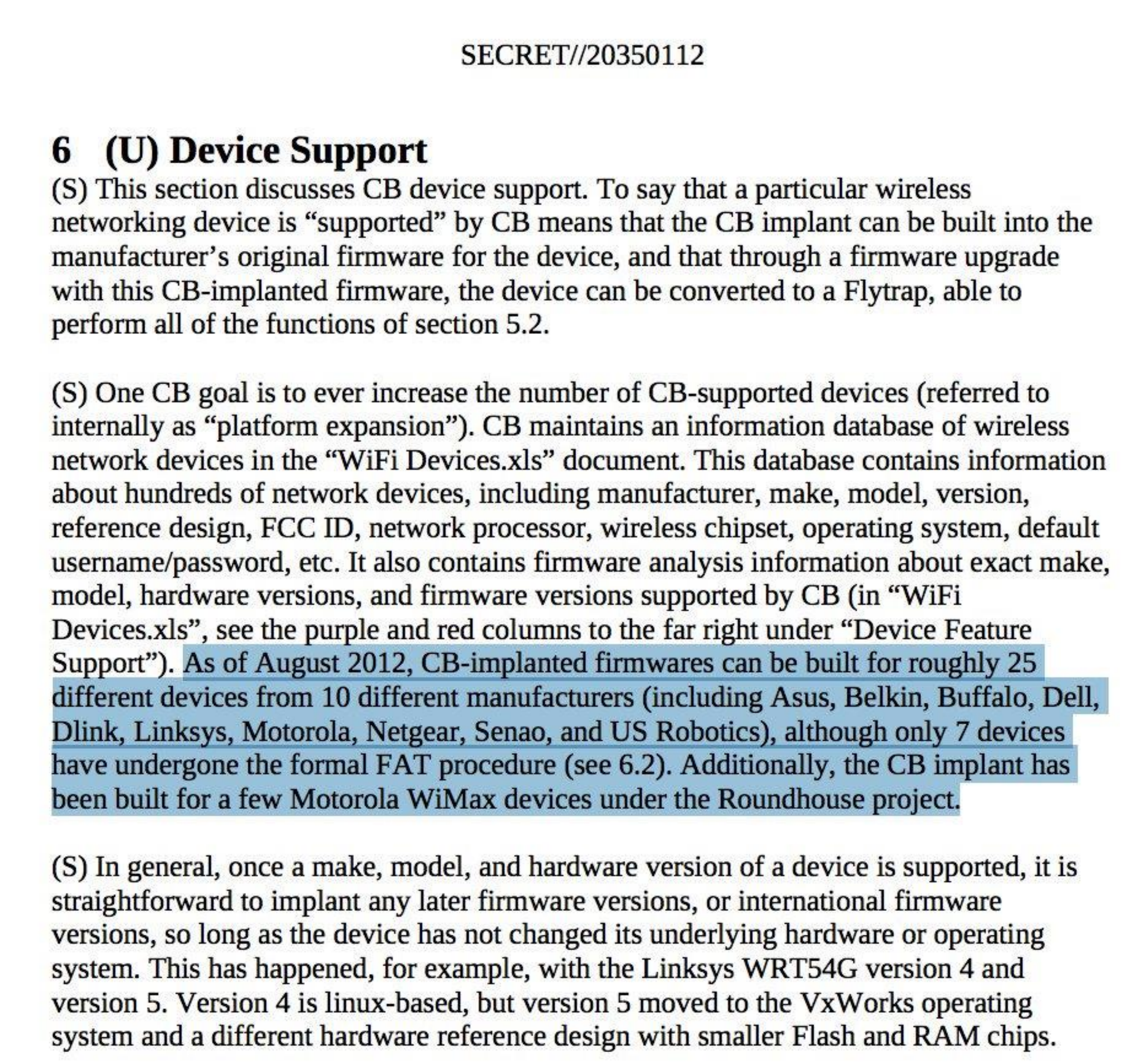
CIA Vault 7 Part 12 "Cherry Blossom"



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.

- CIA 'CherryBlossom' & 'CherryBomb' have been infecting #DLink, #Belkin & #Linksys WiFi routers for years



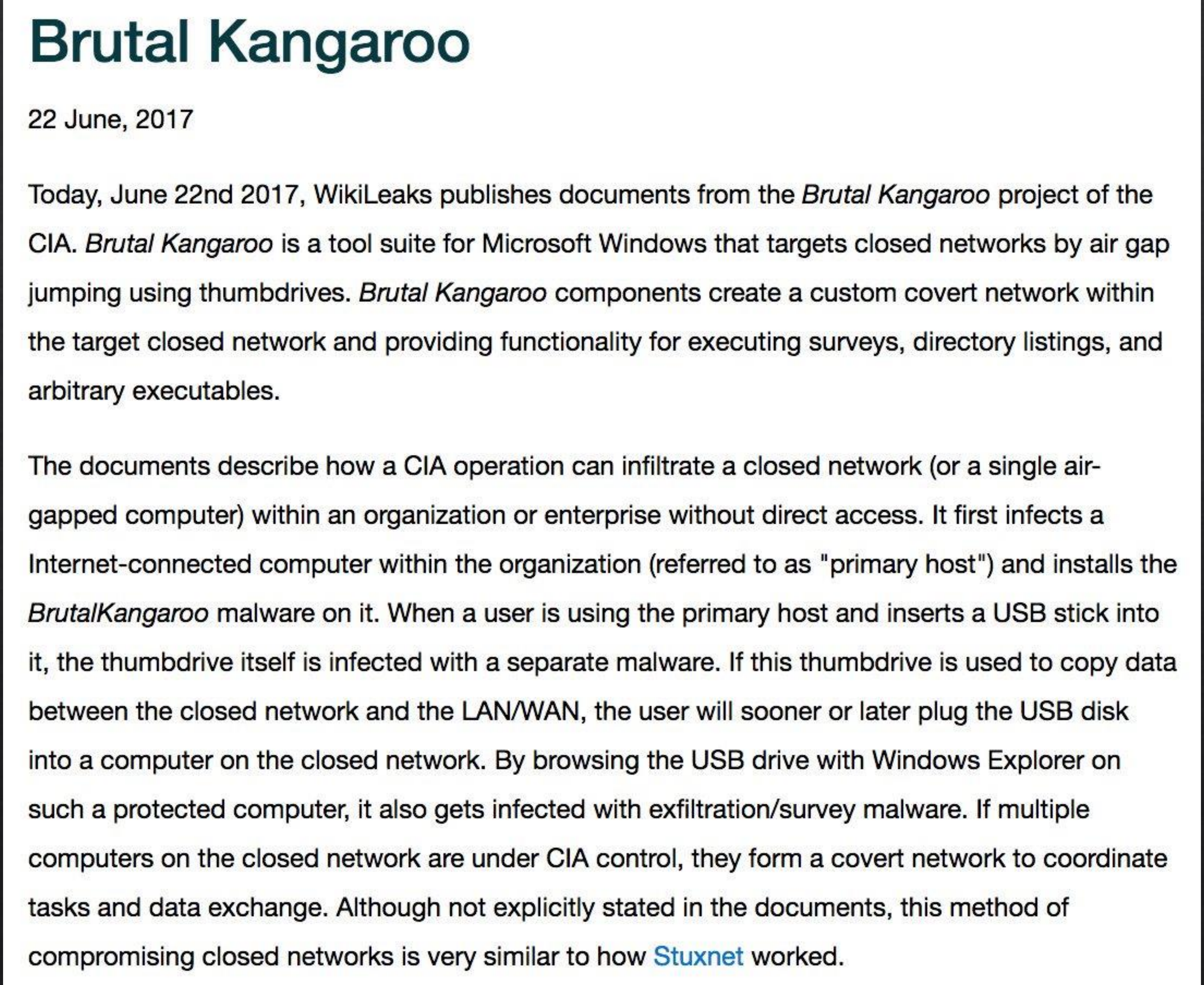
6 (U) Device Support

(S) This section discusses CB device support. To say that a particular wireless networking device is “supported” by CB means that the CB implant can be built into the manufacturer’s original firmware for the device, and that through a firmware upgrade with this CB-implanted firmware, the device can be converted to a Flytrap, able to perform all of the functions of section 5.2.

(S) One CB goal is to ever increase the number of CB-supported devices (referred to internally as “platform expansion”). CB maintains an information database of wireless network devices in the “WiFi Devices.xls” document. This database contains information about hundreds of network devices, including manufacturer, make, model, version, reference design, FCC ID, network processor, wireless chipset, operating system, default username/password, etc. It also contains firmware analysis information about exact make, model, hardware versions, and firmware versions supported by CB (in “WiFi Devices.xls”, see the purple and red columns to the far right under “Device Feature Support”). As of August 2012, CB-implanted firmwares can be built for roughly 25 different devices from 10 different manufacturers (including Asus, Belkin, Buffalo, Dell, Dlink, Linksys, Motorola, Netgear, Senao, and US Robotics), although only 7 devices have undergone the formal FAT procedure (see 6.2). Additionally, the CB implant has been built for a few Motorola WiMax devices under the Roundhouse project.

(S) In general, once a make, model, and hardware version of a device is supported, it is straightforward to implant any later firmware versions, or international firmware versions, so long as the device has not changed its underlying hardware or operating system. This has happened, for example, with the Linksys WRT54G version 4 and version 5. Version 4 is linux-based, but version 5 moved to the VxWorks operating system and a different hardware reference design with smaller Flash and RAM chips.

CIA Vault 7 Part 13 "Brutal Kangaroo"



Brutal Kangaroo

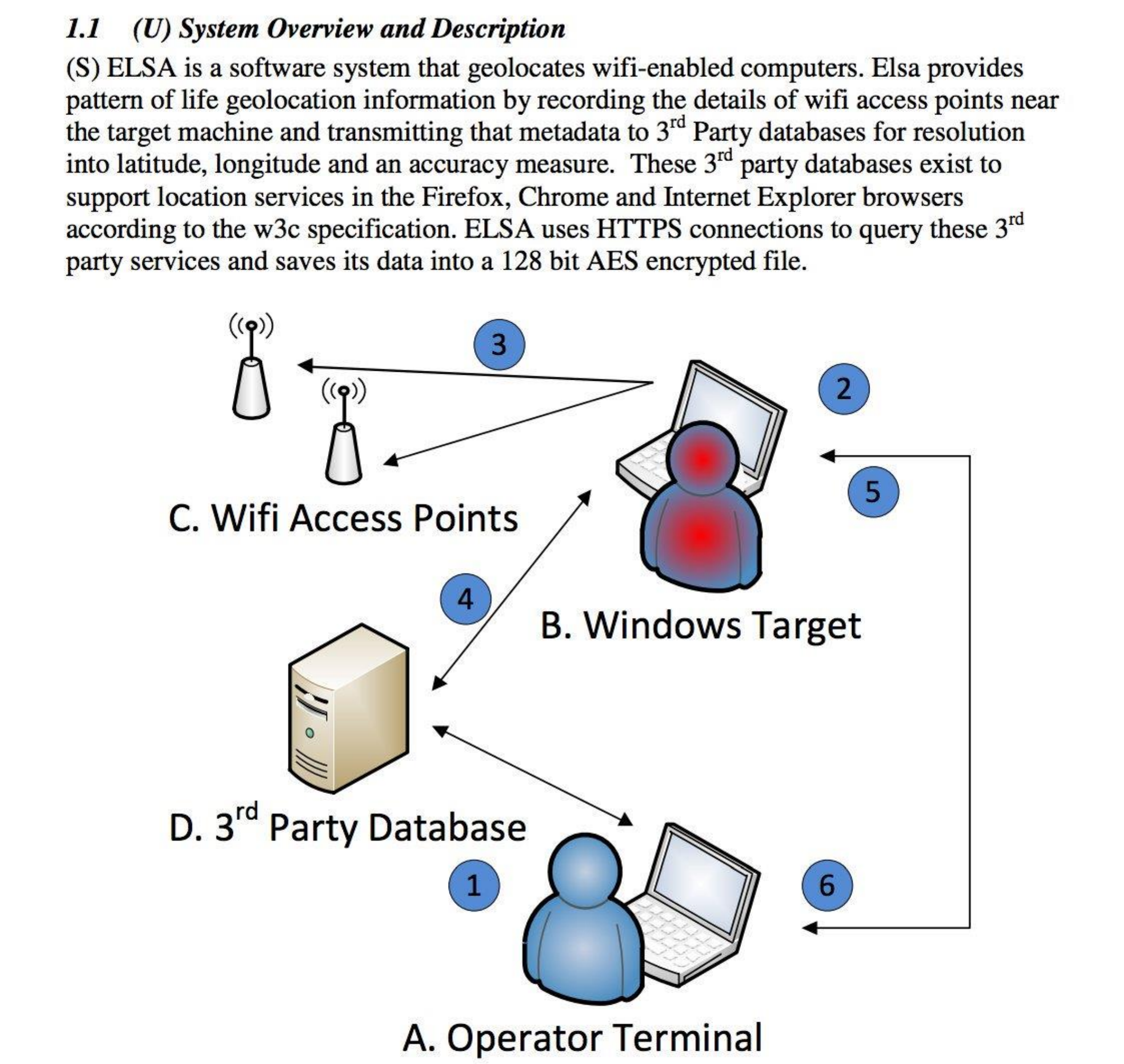
22 June, 2017

Today, June 22nd 2017, WikiLeaks publishes documents from the *Brutal Kangaroo* project of the CIA. *Brutal Kangaroo* is a tool suite for Microsoft Windows that targets closed networks by air gap jumping using thumbdrives. *Brutal Kangaroo* components create a custom covert network within the target closed network and providing functionality for executing surveys, directory listings, and arbitrary executables.

The documents describe how a CIA operation can infiltrate a closed network (or a single air-gapped computer) within an organization or enterprise without direct access. It first infects a Internet-connected computer within the organization (referred to as "primary host") and installs the *BrutalKangaroo* malware on it. When a user is using the primary host and inserts a USB stick into it, the thumbdrive itself is infected with a separate malware. If this thumbdrive is used to copy data between the closed network and the LAN/WAN, the user will sooner or later plug the USB disk into a computer on the closed network. By browsing the USB drive with Windows Explorer on such a protected computer, it also gets infected with exfiltration/survey malware. If multiple computers on the closed network are under CIA control, they form a covert network to coordinate tasks and data exchange. Although not explicitly stated in the documents, this method of compromising closed networks is very similar to how Stuxnet worked.

CIA Vault 7 Part 14 "Elsa"

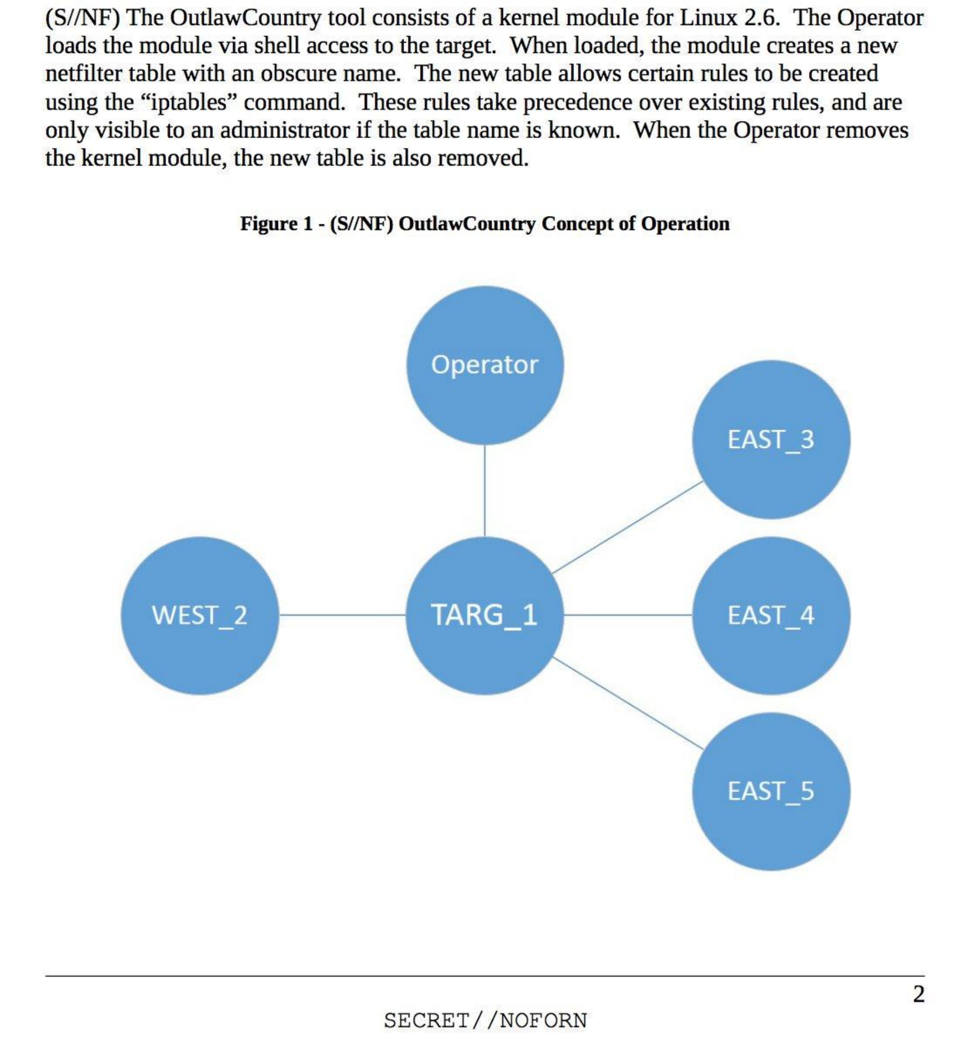
- CIA 'ELSA' implant to geolocate laptops+desktops by intercepting the surrounding WiFi signals



1.1 (U) System Overview and Description

(S) ELSA is a software system that geolocates wifi-enabled computers. Elsa provides pattern of life geolocation information by recording the details of wifi access points near the target machine and transmitting that metadata to 3rd Party databases for resolution into latitude, longitude and an accuracy measure. These 3rd party databases exist to support location services in the Firefox, Chrome and Internet Explorer browsers according to the w3c specification. ELSA uses HTTPS connections to query these 3rd party services and saves its data into a 128 bit AES encrypted file.

CIA Vault 7 Part 15 "OutlawCountry"

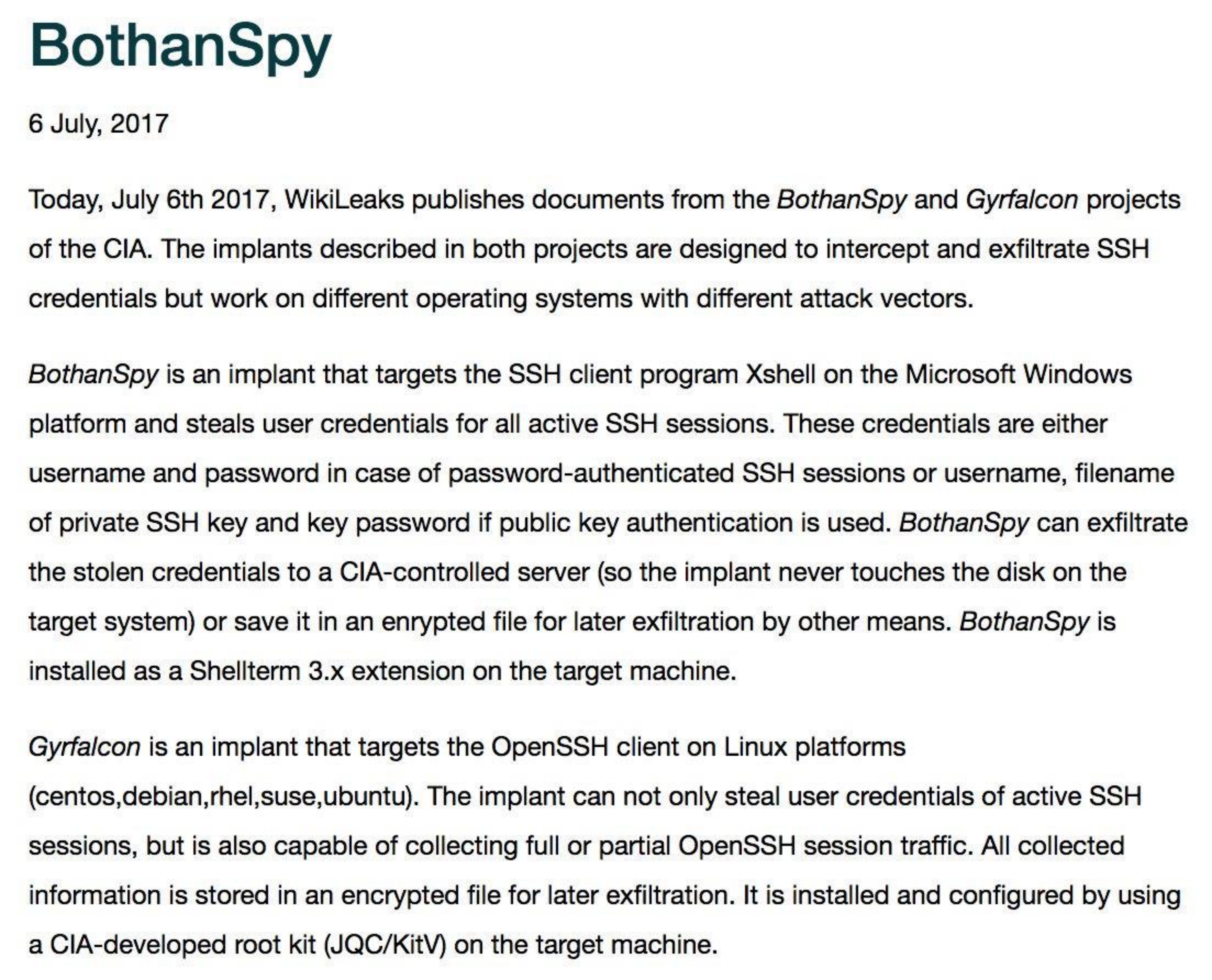


(S//NF) The OutlawCountry tool consists of a kernel module for Linux 2.6. The Operator loads the module via shell access to the target. When loaded, the module creates a new netfilter table with an obscure name. The new table allows certain rules to be created using the "iptables" command. These rules take precedence over existing rules, and are only visible to an administrator if the table name is known. When the Operator removes the kernel module, the new table is also removed.

Figure 1 - (S//NF) OutlawCountry Concept of Operation

CIA Vault 7 Part 16 "BothanSpy"

- #CIA implants targeting SSH on Windows and Linux



BothanSpy

6 July, 2017

Today, July 6th 2017, WikiLeaks publishes documents from the *BothanSpy* and *Gyrfalcon* projects of the CIA. The implants described in both projects are designed to intercept and exfiltrate SSH credentials but work on different operating systems with different attack vectors.

BothanSpy is an implant that targets the SSH client program Xshell on the Microsoft Windows platform and steals user credentials for all active SSH sessions. These credentials are either username and password in case of password-authenticated SSH sessions or username, filename of private SSH key and key password if public key authentication is used. *BothanSpy* can exfiltrate the stolen credentials to a CIA-controlled server (so the implant never touches the disk on the target system) or save it in an enrypted file for later exfiltration by other means. *BothanSpy* is installed as a Shellterm 3.x extension on the target machine.

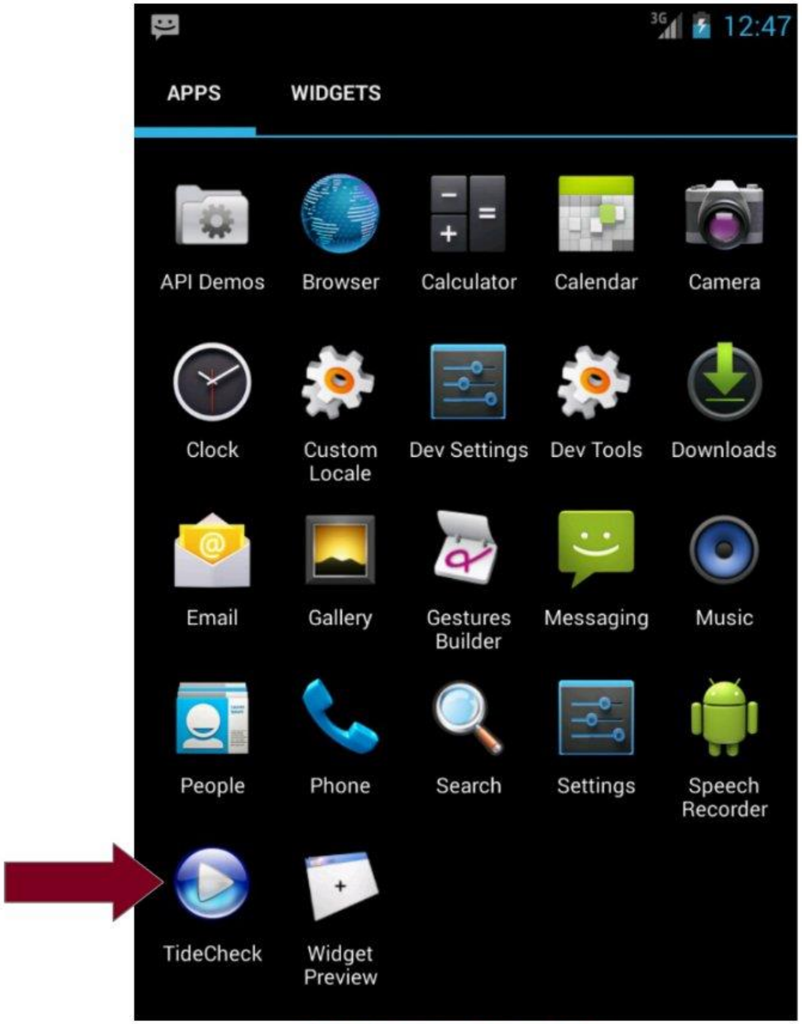
Gyrfalcon is an implant that targets the OpenSSH client on Linux platforms (centos,debian,rhel,suse,ubuntu). The implant can not only steal user credentials of active SSH sessions, but is also capable of collecting full or partial OpenSSH session traffic. All collected information is stored in an encrypted file for later exfiltration. It is installed and configured by using a CIA-developed root kit (JQC/KitV) on the target machine.

CIA Vault 7 Part 17 "Highrise"

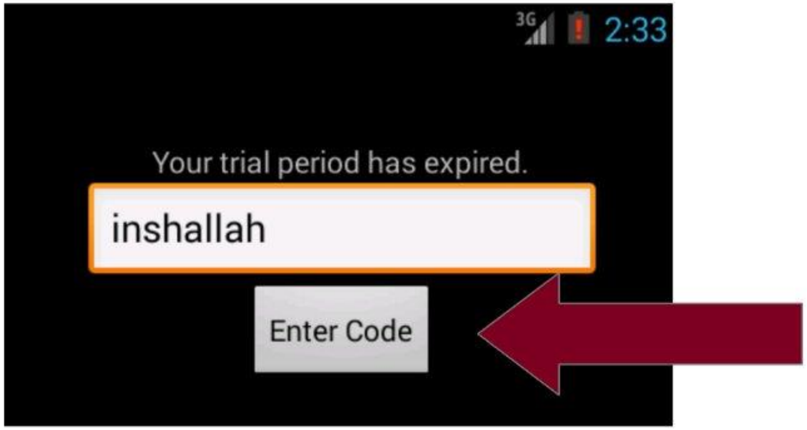
- CIA Android phone SMS proxy 'HighRise' which masquerades as 'TideCheck' to form a covert messaging network

5. (U) Activating HighRise

With HighRise 2.0, the application requires manual activation after installation. This is simply done by finding the TideCheck app in the device's app list and starting it (by selecting it).

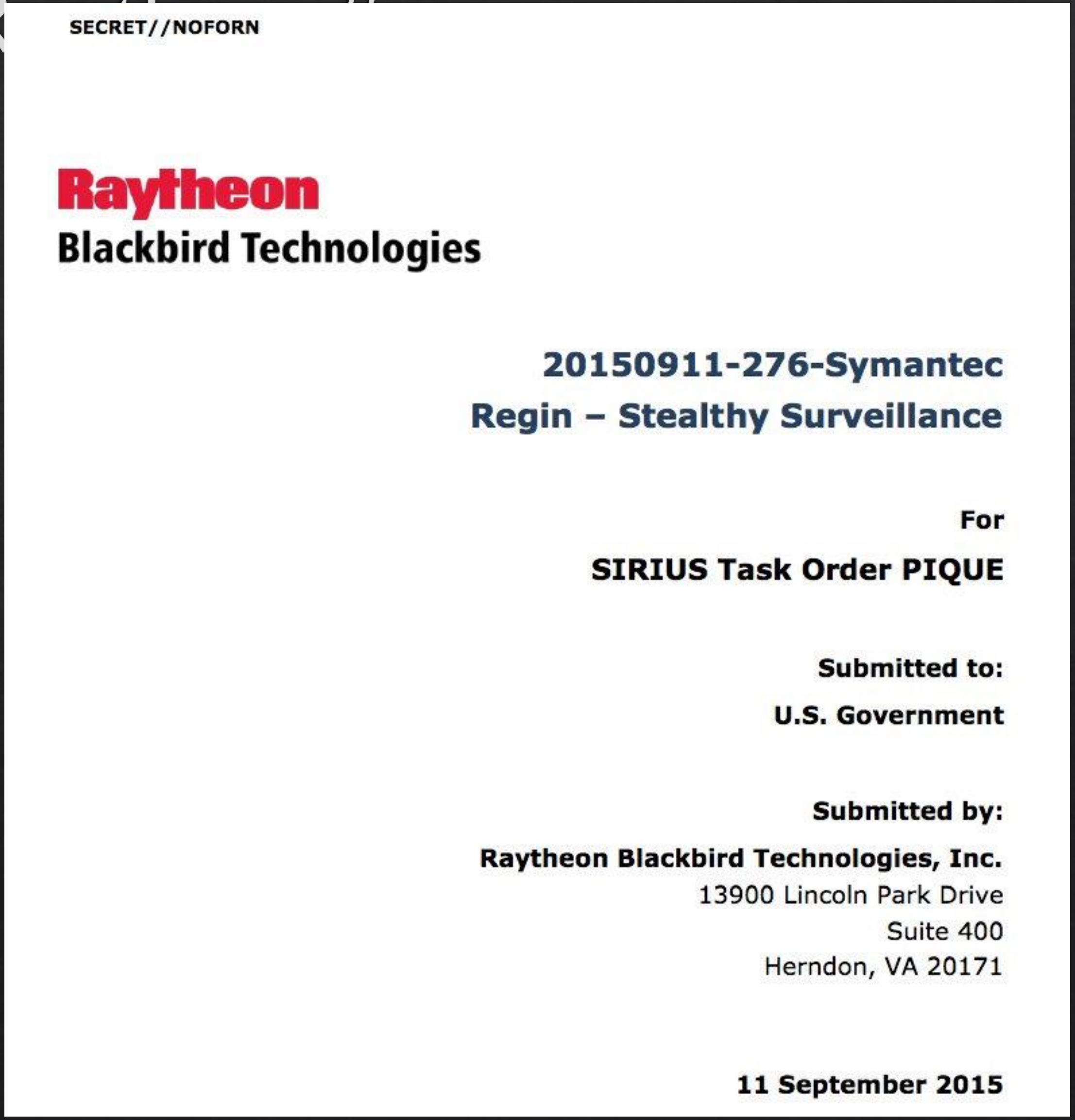


HighRise will start and prompt for a password. Enter ***inshallah*** for the password and then select the button labeled "Enter Code".


Your trial period has expired.

inshallah

CIA Vault 7 Part 18 “UCL / R ”



SECRET//NOFORN

Raytheon
Blackbird Technologies

20150911-276-Symantec
Regin – Stealthy Surveillance

For

SIRIUS Task Order PIQUE

Submitted to:

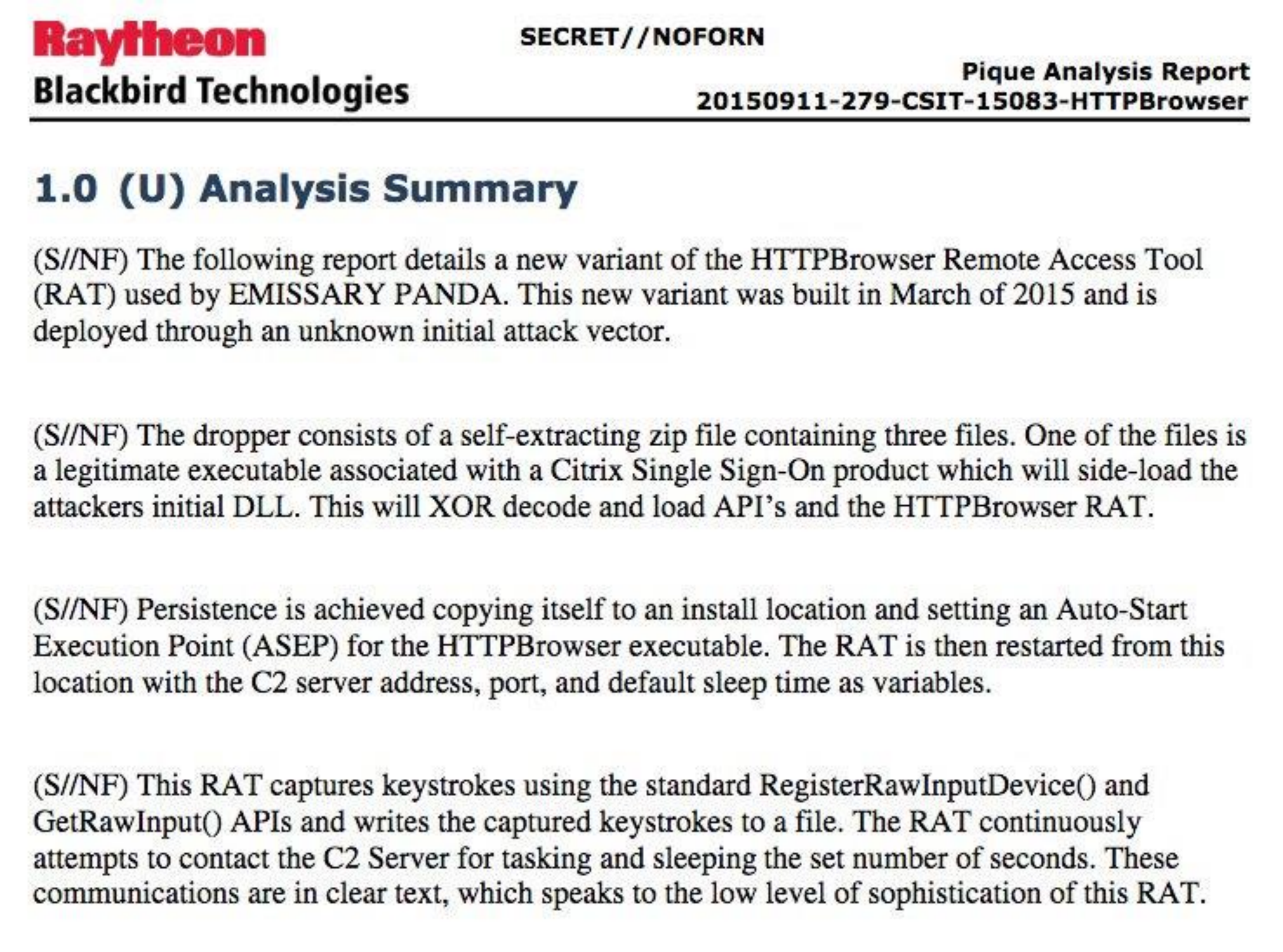
U.S. Government

Submitted by:

Raytheon Blackbird Technologies, Inc.
13900 Lincoln Park Drive
Suite 400
Herndon, VA 20171

11 September 2015

Classified CIA-Raytheon docs on suspected Chinese state malware



Raytheon
Blackbird Technologies

SECRET//NOFORN

Pique Analysis Report
20150911-279-CSIT-15083-HTTPBrowser

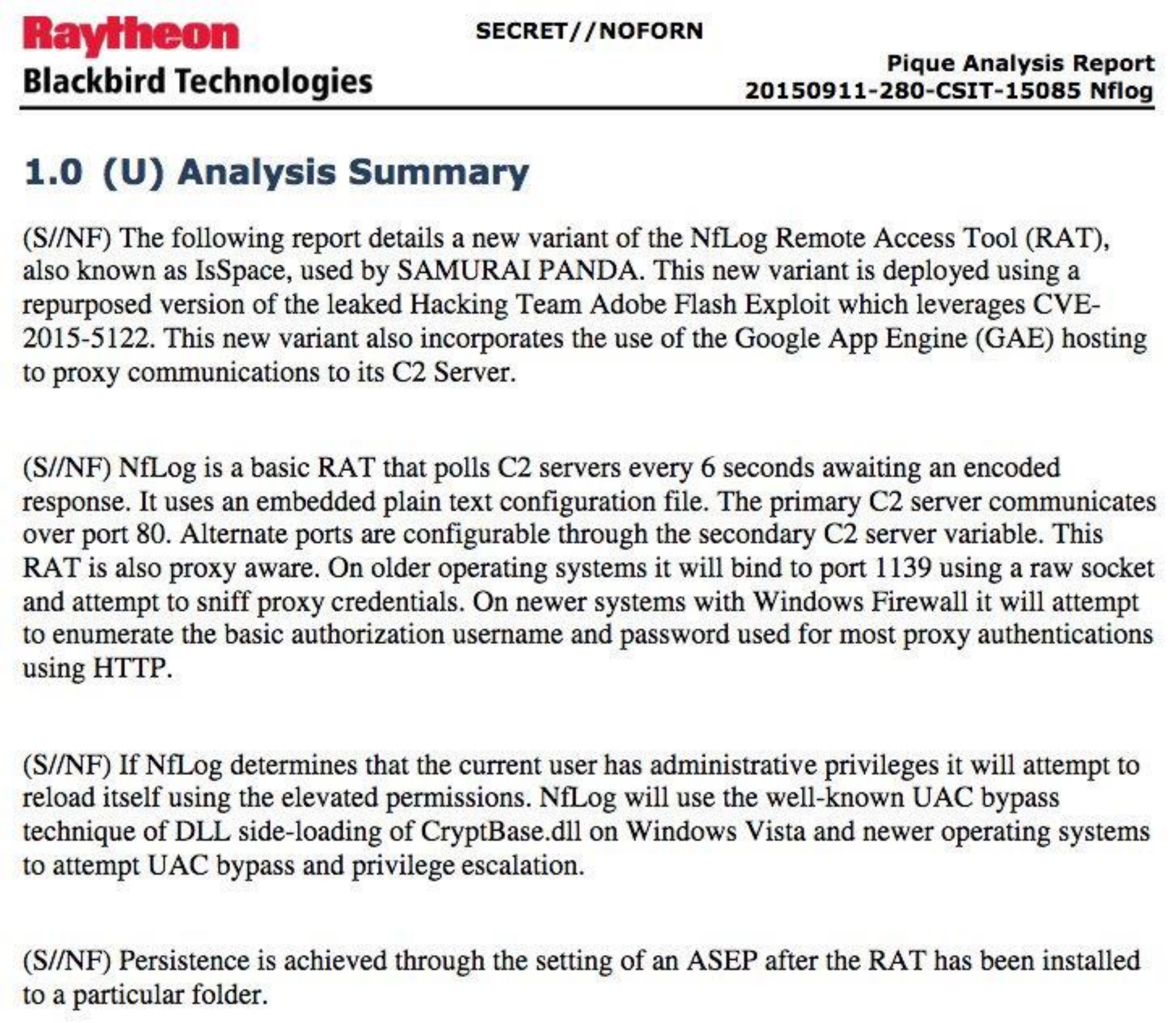
1.0 (U) Analysis Summary

(S//NF) The following report details a new variant of the HTTPBrowser Remote Access Tool (RAT) used by EMISSARY PANDA. This new variant was built in March of 2015 and is deployed through an unknown initial attack vector.

(S//NF) The dropper consists of a self-extracting zip file containing three files. One of the files is a legitimate executable associated with a Citrix Single Sign-On product which will side-load the attackers initial DLL. This will XOR decode and load API's and the HTTPBrowser RAT.

(S//NF) Persistence is achieved copying itself to an install location and setting an Auto-Start Execution Point (ASEP) for the HTTPBrowser executable. The RAT is then restarted from this location with the C2 server address, port, and default sleep time as variables.

(S//NF) This RAT captures keystrokes using the standard RegisterRawInputDevice() and GetRawInput() APIs and writes the captured keystrokes to a file. The RAT continuously attempts to contact the C2 Server for tasking and sleeping the set number of seconds. These communications are in clear text, which speaks to the low level of sophistication of this RAT.



Raytheon
Blackbird Technologies

SECRET//NOFORN

Pique Analysis Report
20150911-280-CSIT-15085 Nflog

1.0 (U) Analysis Summary

(S//NF) The following report details a new variant of the NfLog Remote Access Tool (RAT), also known as IsSpace, used by SAMURAI PANDA. This new variant is deployed using a repurposed version of the leaked Hacking Team Adobe Flash Exploit which leverages CVE-2015-5122. This new variant also incorporates the use of the Google App Engine (GAE) hosting to proxy communications to its C2 Server.

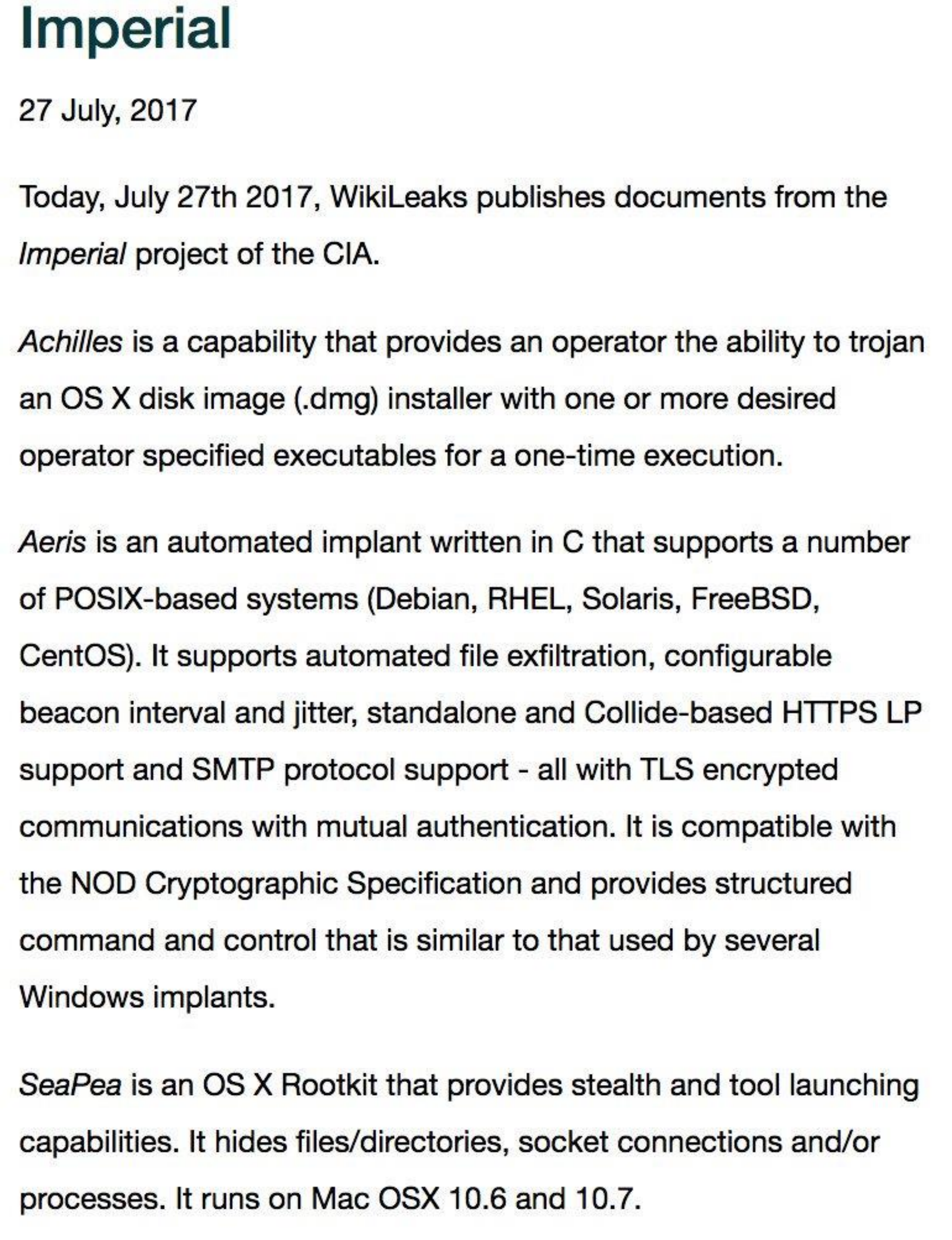
(S//NF) NfLog is a basic RAT that polls C2 servers every 6 seconds awaiting an encoded response. It uses an embedded plain text configuration file. The primary C2 server communicates over port 80. Alternate ports are configurable through the secondary C2 server variable. This RAT is also proxy aware. On older operating systems it will bind to port 1139 using a raw socket and attempt to sniff proxy credentials. On newer systems with Windows Firewall it will attempt to enumerate the basic authorization username and password used for most proxy authentications using HTTP.

(S//NF) If NfLog determines that the current user has administrative privileges it will attempt to reload itself using the elevated permissions. NfLog will use the well-known UAC bypass technique of DLL side-loading of CryptBase.dll on Windows Vista and newer operating systems to attempt UAC bypass and privilege escalation.

(S//NF) Persistence is achieved through the setting of an ASEP after the RAT has been installed to a particular folder.

CIA Vault 7 Part 19 “Imperial ”

Trojans targetting Macs, Debian, RHEL, Solaris, FreeBSD, Centos



Imperial

27 July, 2017

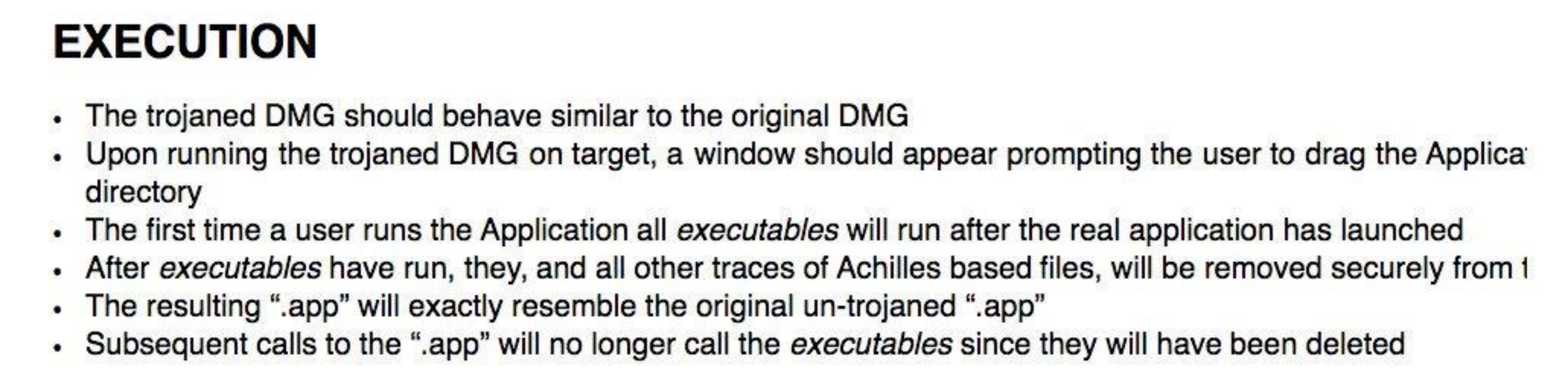
Today, July 27th 2017, WikiLeaks publishes documents from the *Imperial* project of the CIA.

Achilles is a capability that provides an operator the ability to trojan an OS X disk image (.dmg) installer with one or more desired operator specified executables for a one-time execution.

Aeris is an automated implant written in C that supports a number of POSIX-based systems (Debian, RHEL, Solaris, FreeBSD, CentOS). It supports automated file exfiltration, configurable beacon interval and jitter, standalone and Collide-based HTTPS LP support and SMTP protocol support - all with TLS encrypted communications with mutual authentication. It is compatible with the NOD Cryptographic Specification and provides structured command and control that is similar to that used by several Windows implants.

SeaPea is an OS X Rootkit that provides stealth and tool launching capabilities. It hides files/directories, socket connections and/or processes. It runs on Mac OSX 10.6 and 10.7.

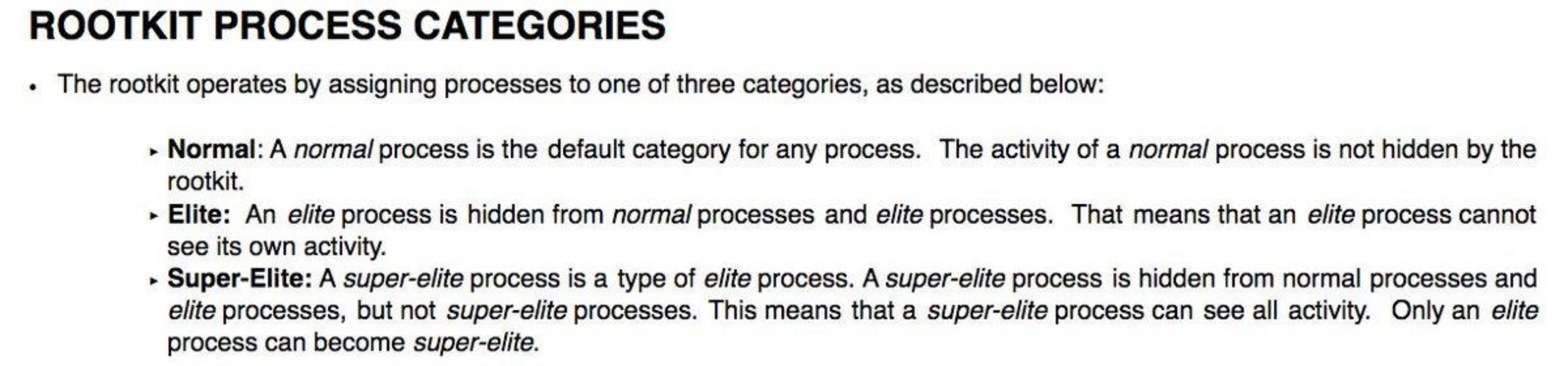
CIA 'Achilles' tool to infect Mac OS X disk images (".dmg")



EXECUTION

- The trojaned DMG should behave similar to the original DMG
- Upon running the trojaned DMG on target, a window should appear prompting the user to drag the Applica directory
- The first time a user runs the Application all *executables* will run after the real application has launched
- After *executables* have run, they, and all other traces of Achilles based files, will be removed securely from t
- The resulting ".app" will exactly resemble the original un-trojaned ".app"
- Subsequent calls to the ".app" will no longer call the *executables* since they will have been deleted

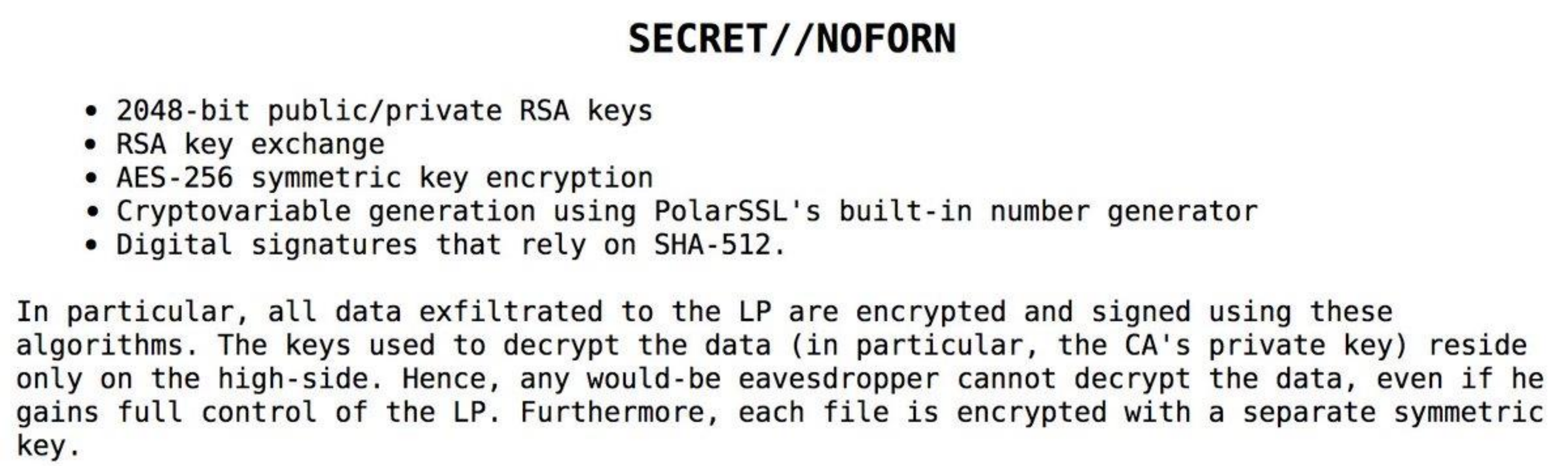
- CIA 'rootkit' to hide CIA activities on the Apple Macs it infiltrates



ROOTKIT PROCESS CATEGORIES

- The rootkit operates by assigning processes to one of three categories, as described below:
  - **Normal**: A *normal* process is the default category for any process. The activity of a *normal* process is not hidden by the rootkit.
  - **Elite:** An *elite* process is hidden from *normal* processes and *elite* processes. That means that an *elite* process cannot see its own activity.
  - **Super-Elite:** A *super-elite* process is a type of *elite* process. A *super-elite* process is hidden from normal processes and *elite* processes, but not *super-elite* processes. This means that a *super-elite* process can see all activity. Only an *elite* process can become *super-elite*.

CIA 'Aeris' implant targeting Debian, Red Hat, Solaris, FreeBSD and Centos users



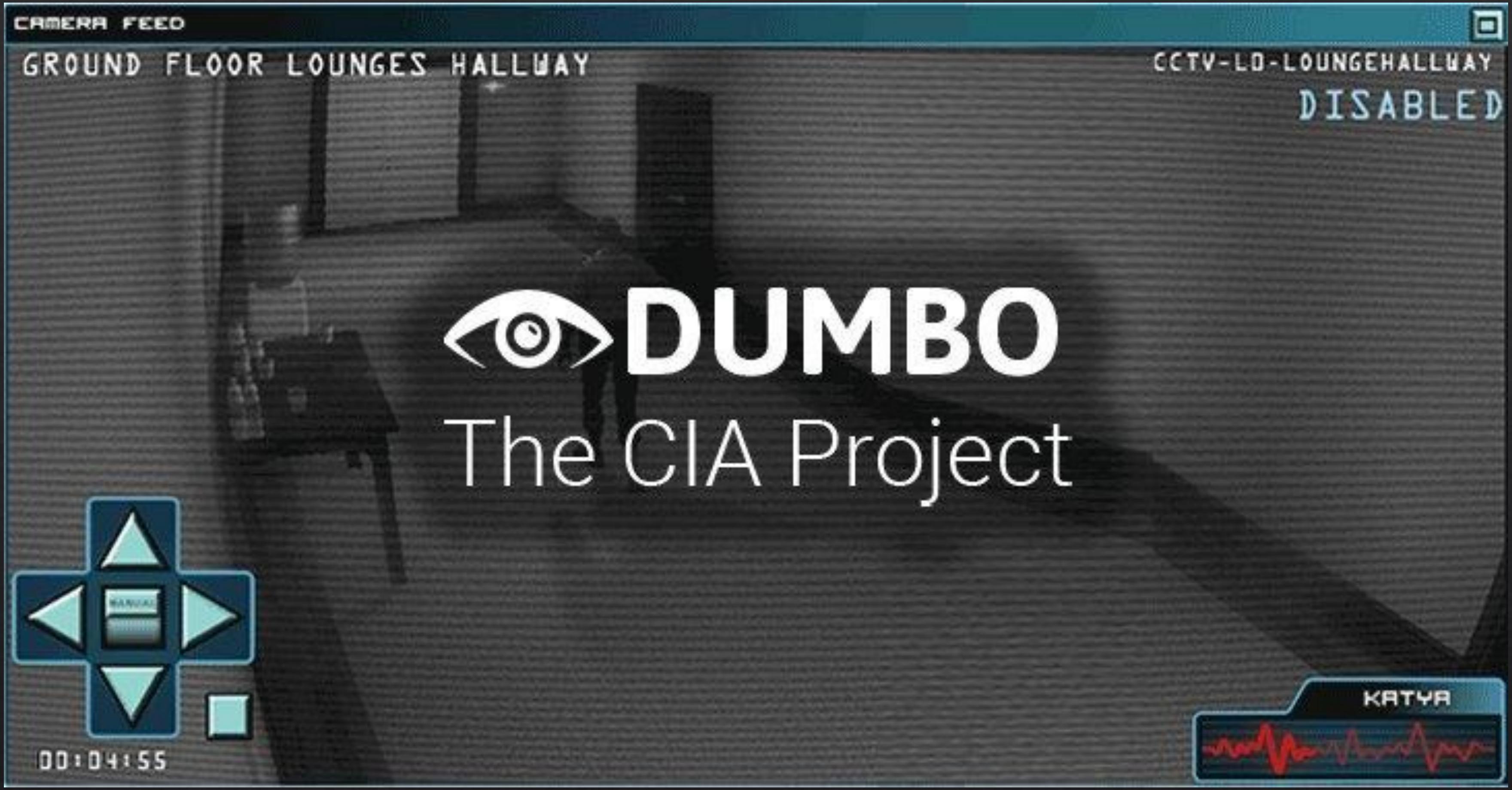
SECRET//NOFORN

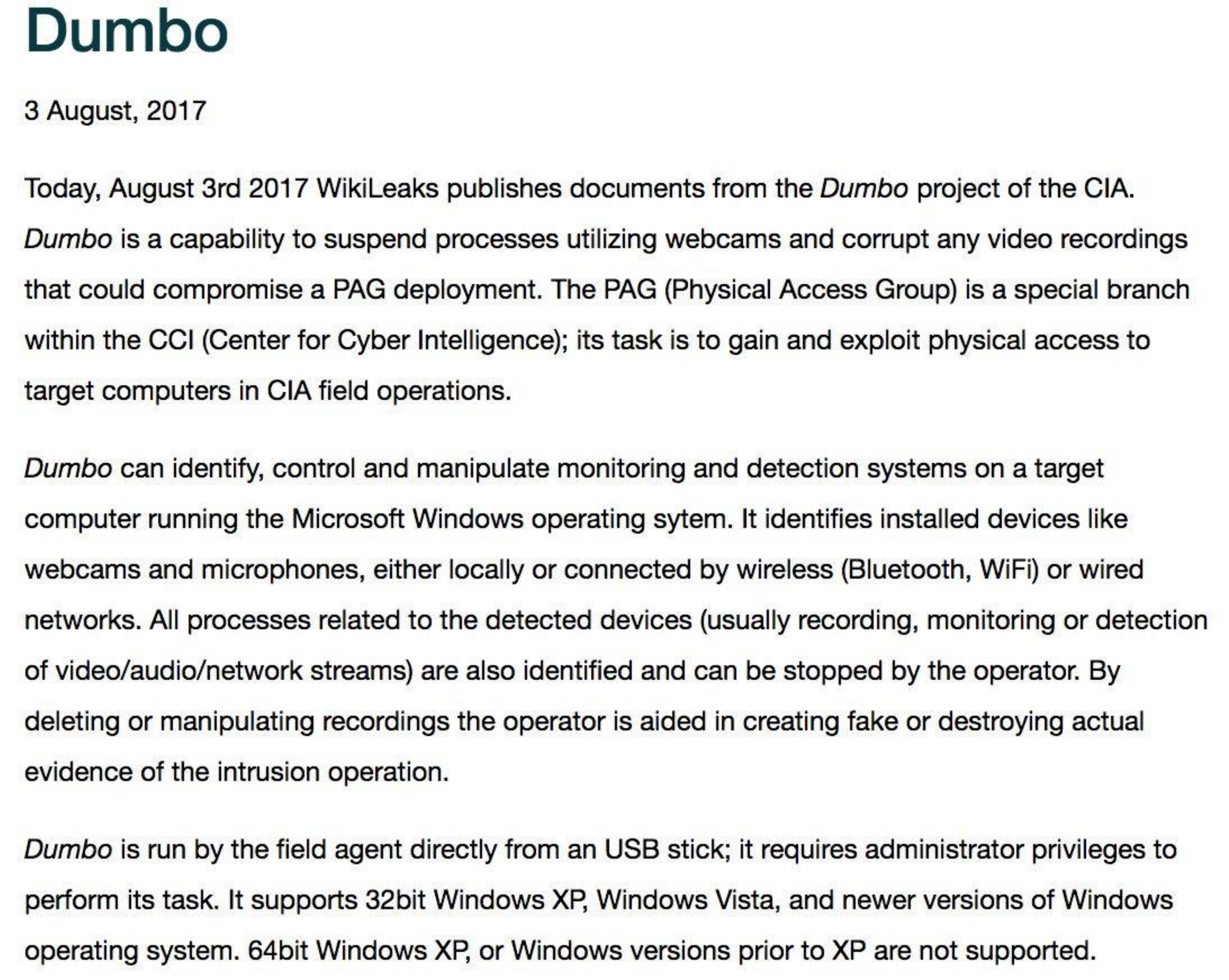
- 2048-bit public/private RSA keys
- RSA key exchange
- AES-256 symmetric key encryption
- Cryptovariable generation using PolarSSL's built-in number generator
- Digital signatures that rely on SHA-512.

In particular, all data exfiltrated to the LP are encrypted and signed using these algorithms. The keys used to decrypt the data (in particular, the CA's private key) reside only on the high-side. Hence, any would-be eavesdropper cannot decrypt the data, even if he gains full control of the LP. Furthermore, each file is encrypted with a separate symmetric key.

CIA Vault 7 Part 20 “Dumbo ”

- A Tool CIA Agents Use to Disable Surveillance Cameras & Mics During Hollywood-Style Covert Operations.
- CIA project 'Dumbo' to switch off security webcams and corrupt recordings to hide physical intrusions


CAMERA FEED
GROUND FLOOR LOUNGES HALLWAY
CCTV-LD-LOUNGEHALLWAY
DISABLED
DUMBO
The CIA Project
MANUAL
00:04:55
KATYA



Dumbo

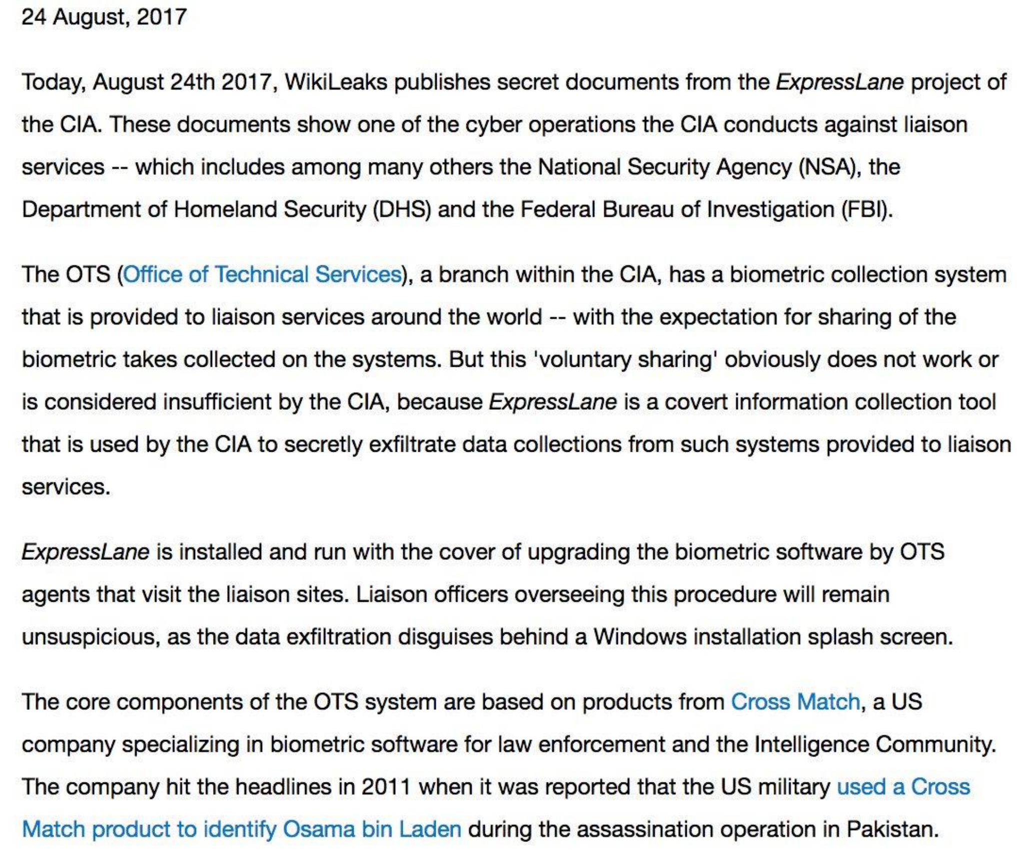
3 August, 2017

Today, August 3rd 2017 WikiLeaks publishes documents from the *Dumbo* project of the CIA. *Dumbo* is a capability to suspend processes utilizing webcams and corrupt any video recordings that could compromise a PAG deployment. The PAG (Physical Access Group) is a special branch within the CCI (Center for Cyber Intelligence); its task is to gain and exploit physical access to target computers in CIA field operations.

Dumbo can identify, control and manipulate monitoring and detection systems on a target computer running the Microsoft Windows operating sytem. It identifies installed devices like webcams and microphones, either locally or connected by wireless (Bluetooth, WiFi) or wired networks. All processes related to the detected devices (usually recording, monitoring or detection of video/audio/network streams) are also identified and can be stopped by the operator. By deleting or manipulating recordings the operator is aided in creating fake or destroying actual evidence of the intrusion operation.

Dumbo is run by the field agent directly from an USB stick; it requires administrator privileges to perform its task. It supports 32bit Windows XP, Windows Vista, and newer versions of Windows operating system. 64bit Windows XP, or Windows versions prior to XP are not supported.

CIA 'Express Lane' system for stealing the biometric databases of its 'partner' agencies around the world



24 August, 2017

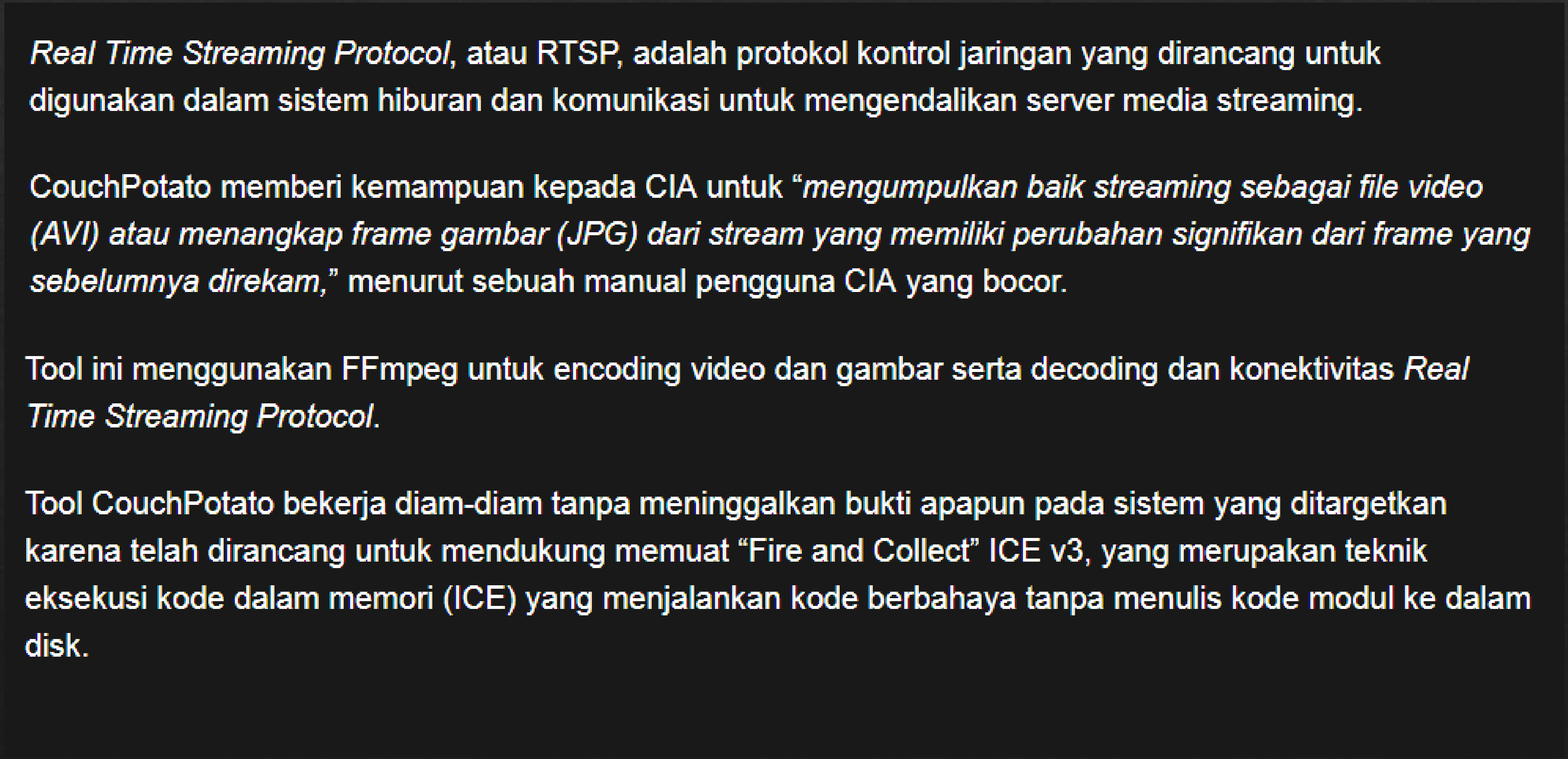
Today, August 24th 2017, WikiLeaks publishes secret documents from the *ExpressLane* project of the CIA. These documents show one of the cyber operations the CIA conducts against liaison services -- which includes among many others the National Security Agency (NSA), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

The OTS (Office of Technical Services), a branch within the CIA, has a biometric collection system that is provided to liaison services around the world -- with the expectation for sharing of the biometric takes collected on the systems. But this 'voluntary sharing' obviously does not work or is considered insufficient by the CIA, because *ExpressLane* is a covert information collection tool that is used by the CIA to secretly exfiltrate data collections from such systems provided to liaison services.

ExpressLane is installed and run with the cover of upgrading the biometric software by OTS agents that visit the liaison sites. Liaison officers overseeing this procedure will remain unsuspicious, as the data exfiltration disguises behind a Windows installation splash screen.

The core components of the OTS system are based on products from Cross Match, a US company specializing in biometric software for law enforcement and the Intelligence Community. The company hit the headlines in 2011 when it was reported that the US military used a Cross Match product to identify Osama bin Laden during the assassination operation in Pakistan.

CIA Vault 7 Part 21 “CouchPotato”



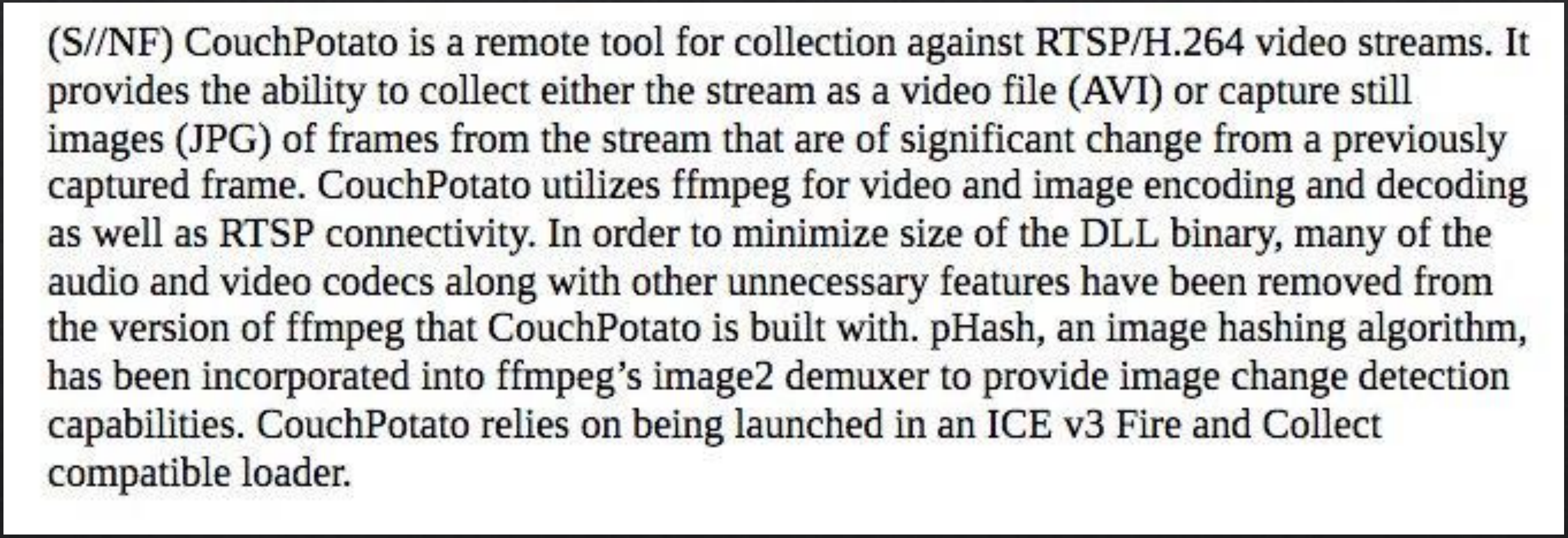
Real Time Streaming Protocol, atau RTSP, adalah protokol kontrol jaringan yang dirancang untuk digunakan dalam sistem hiburan dan komunikasi untuk mengendalikan server media streaming.

CouchPotato memberi kemampuan kepada CIA untuk “*mengumpulkan baik streaming sebagai file video (AVI) atau menangkap frame gambar (JPG) dari stream yang memiliki perubahan signifikan dari frame yang sebelumnya direkam,*” menurut sebuah manual pengguna CIA yang bocor.

Tool ini menggunakan FFmpeg untuk encoding video dan gambar serta decoding dan konektivitas *Real Time Streaming Protocol*.

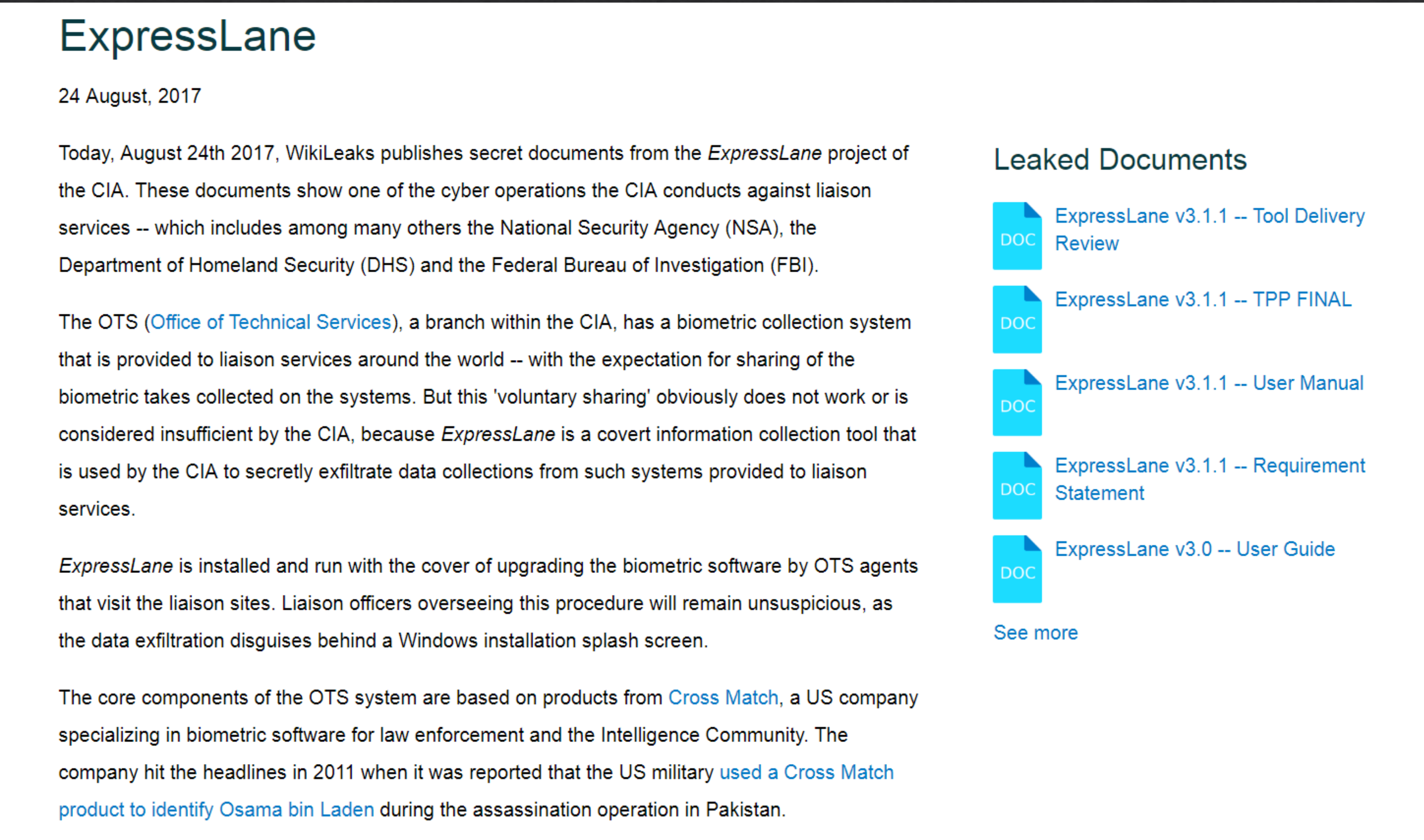
Tool CouchPotato bekerja diam-diam tanpa meninggalkan bukti apapun pada sistem yang ditargetkan karena telah dirancang untuk mendukung memuat “Fire and Collect” ICE v3, yang merupakan teknik eksekusi kode dalam memori (ICE) yang menjalankan kode berbahaya tanpa menulis kode modul ke dalam disk.

CIA system for intercepting video chat and security camera streams. Uses CIA "Fire and Collect" framework



(S//NF) CouchPotato is a remote tool for collection against RTSP/H.264 video streams. It provides the ability to collect either the stream as a video file (AVI) or capture still images (JPG) of frames from the stream that are of significant change from a previously captured frame. CouchPotato utilizes ffmpeg for video and image encoding and decoding as well as RTSP connectivity. In order to minimize size of the DLL binary, many of the audio and video codecs along with other unnecessary features have been removed from the version of ffmpeg that CouchPotato is built with. pHash, an image hashing algorithm, has been incorporated into ffmpeg's image2 demuxer to provide image change detection capabilities. CouchPotato relies on being launched in an ICE v3 Fire and Collect compatible loader.

CIA Vault 7 Part 22 “ExpressLane ”



ExpressLane

24 August, 2017

Today, August 24th 2017, WikiLeaks publishes secret documents from the *ExpressLane* project of the CIA. These documents show one of the cyber operations the CIA conducts against liaison services -- which includes among many others the National Security Agency (NSA), the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

The OTS (Office of Technical Services), a branch within the CIA, has a biometric collection system that is provided to liaison services around the world -- with the expectation for sharing of the biometric takes collected on the systems. But this 'voluntary sharing' obviously does not work or is considered insufficient by the CIA, because *ExpressLane* is a covert information collection tool that is used by the CIA to secretly exfiltrate data collections from such systems provided to liaison services.

ExpressLane is installed and run with the cover of upgrading the biometric software by OTS agents that visit the liaison sites. Liaison officers overseeing this procedure will remain unsuspicious, as the data exfiltration disguises behind a Windows installation splash screen.

The core components of the OTS system are based on products from Cross Match, a US company specializing in biometric software for law enforcement and the Intelligence Community. The company hit the headlines in 2011 when it was reported that the US military used a Cross Match product to identify Osama bin Laden during the assassination operation in Pakistan.

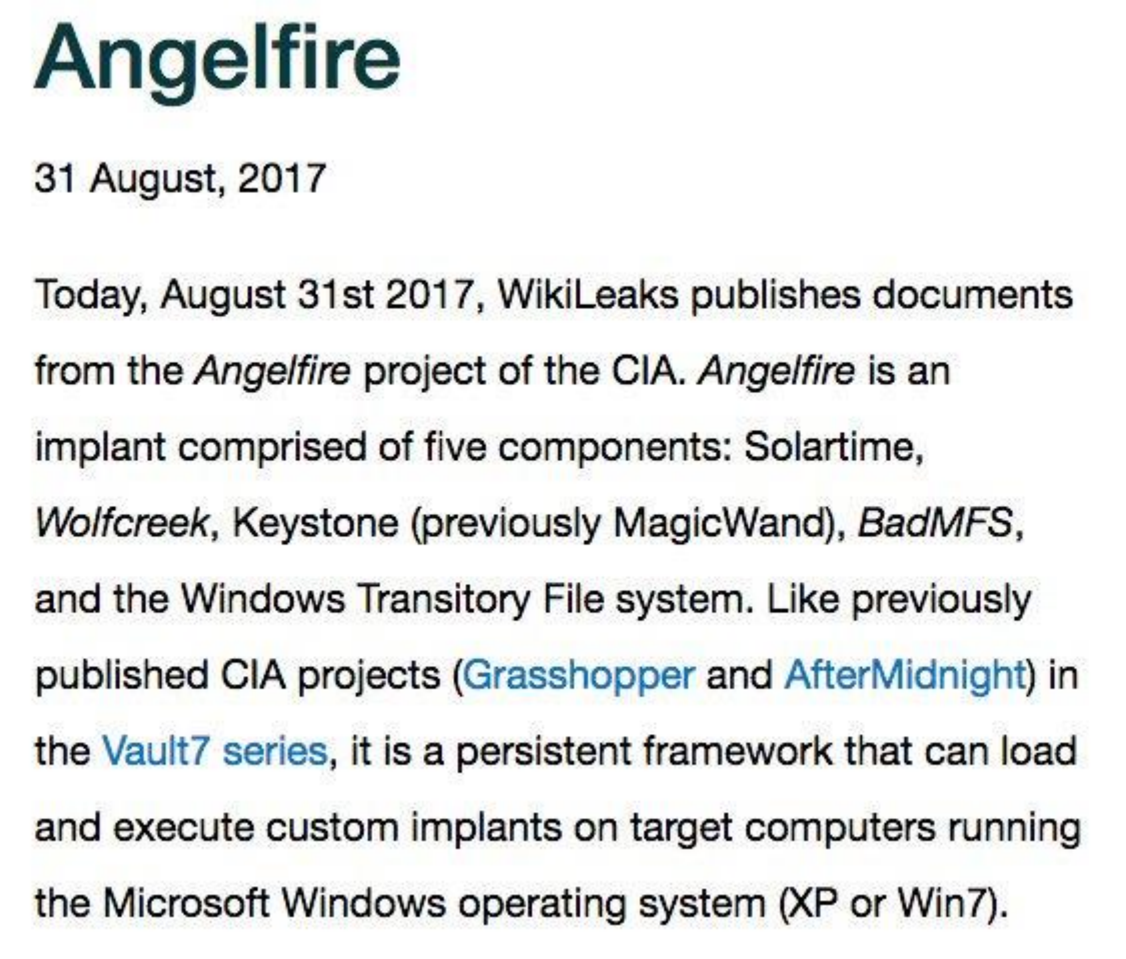
Leaked Documents

- DOC ExpressLane v3.1.1 -- Tool Delivery Review
- DOC ExpressLane v3.1.1 -- TPP FINAL
- DOC ExpressLane v3.1.1 -- User Manual
- DOC ExpressLane v3.1.1 -- Requirement Statement
- DOC ExpressLane v3.0 -- User Guide

See more

CIA Vault 7 Part 23 “Angelfire ”

- covert Windows malware system



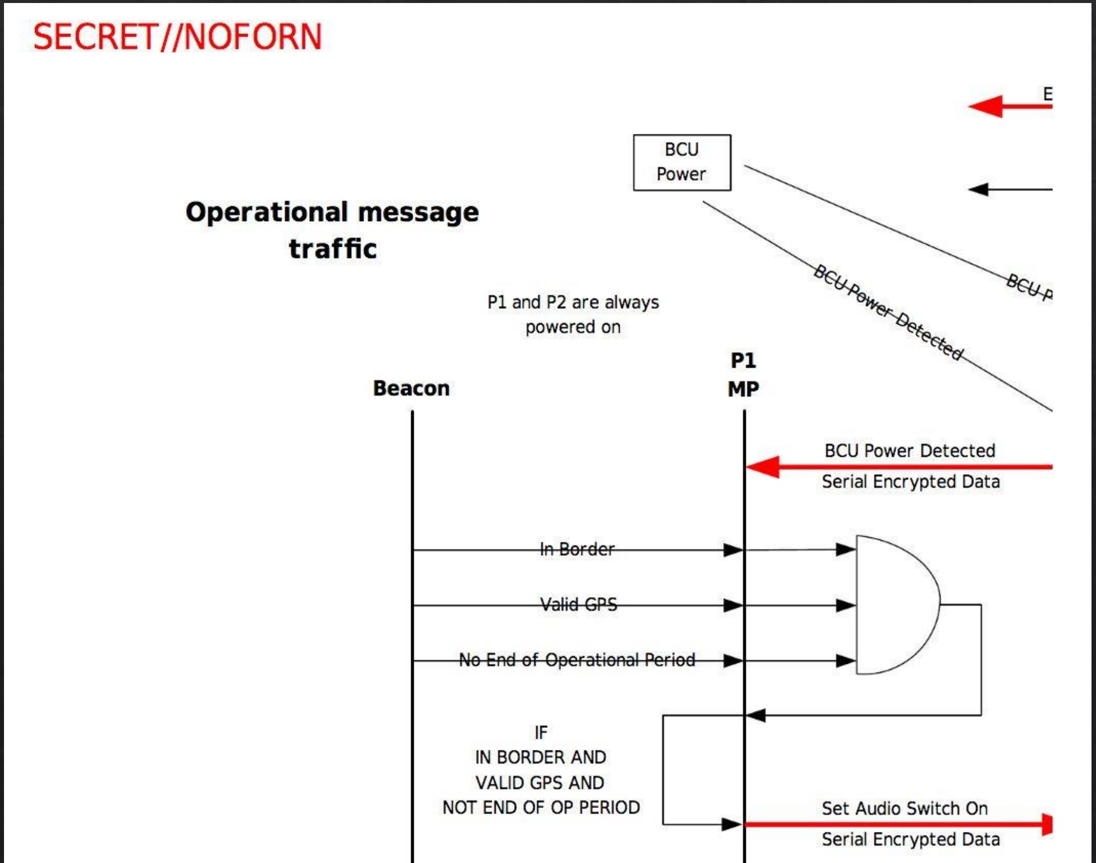
Angelfire

31 August, 2017

Today, August 31st 2017, WikiLeaks publishes documents from the *Angelfire* project of the CIA. *Angelfire* is an implant comprised of five components: Solartime, *Wolfcreek*, Keystone (previously MagicWand), *BadMFS*, and the Windows Transitory File system. Like previously published CIA projects (Grasshopper and AfterMidnight) in the Vault7 series, it is a persistent framework that can load and execute custom implants on target computers running the Microsoft Windows operating system (XP or Win7).

CIA Vault 7 Part 24 “Protego ”

- CIA suspected assassination module for GPS guided missile system 'Protego'



GHIDRA

- includes a suite of software analysis tools for analyzing compiled code on a variety of platforms including Windows, Mac OS, and Linux
- capabilities include disassembly, assembly, decompilation, graphing and scripting, and hundreds of other features
- supports a wide variety of processor instruction sets and executable formats and can be run in both user-interactive and automated modes.
- users may develop their own Ghidra plug-in components and/or scripts using the exposed API

- Ghidra is a software reverse engineering (SRE) framework developed by NSA's Research Directorate for NSA's cybersecurity mission. It helps analyze malicious code and malware like viruses, and can give cybersecurity professionals a better understanding of potential vulnerabilities in their networks and systems.
- NSA will be making Ghidra available to the public as an open source release in time for its first public demonstration at the 2019 RSA Conference this March. For more NSA releases, check out CODE.NSA.GOV for open source, and NSA's Technology Transfer Program for other technology.

- GHIDRA framework, according to the announcement about RSAConference sessions, will be available for Linux, macOS, and Windows-based systems after its release at the conference in March 2019 where it will be "demonstrated for the first time."
- Furthermore, GHIDRA is equipped with GUI capability that makes it compatible with numerous platforms and a wide range of processor instruction sets.
- "The GHIDRA platform includes all the features expected in high-end commercial tools, with new and expanded functionality NSA uniquely developed, and will be released for free public use at RSA," stated the RSAConference announcement.
- Those who have accessed GHIDRA and according to the information disclosed by WikiLeaks' vault 7, this would be a Java-based system that will be subsequently released on the NSA's open source repository.
- It is currently a point of debate whether GHIDRA is better than other reverse engineering options available such as the IDA. However, experts claim that unlike the expensive IDA, GHIDRA is a bit slow and complicated.
- Basically, GHIDRA is disassembling software that can break down all the executable files into assembly code, which can be examined by experts. Various US government agencies have been using it to assess malware strain and malicious software ever since GHIDRA was developed in the early 2000s.
- GHIDRA can assess all major operating systems' binaries including Windows, Linux, macOS, and Android while its modular structure allows the user to add more packages to enjoy additional features.

BONUS

CENTRAL INTELLIGENCE AGENCY
KNOWLEDGE
</>
INFORMATION OPERATIONS CENTER

VAULT 8

- Source code and analysis for CIA software projects including those described in the Vault7 series.
- This publication will enable investigative journalists, forensic experts and the general public to better identify and understand covert CIA infrastructure components.
- Source code published in this series contains software designed to run on servers controlled by the CIA. Like WikiLeaks' earlier Vault7 series, the material published by WikiLeaks does **not** contain 0-days or similar security vulnerabilities which could be repurposed by others.

Sumber : Daftar Pustaka

- https://twitter.com/Vault7Official
- https://twitter.com/wikileaks
- https://www.hackread.com/nsa-reverse-engineering-tool-ghidra-rsaconference/
- https://www.Wikipedia.com

DISKUSI

TERIMA KASIH