

TACERT 臺灣學術網路危機處理中心團隊製

2015/10

- 1. 事件簡介
 - 近年來惡意程式越來越多樣化,以往都只是感染主機成為中繼站或殭屍電 腦,但另一種的惡意程式卻會破壞使用者的檔案資料,並且勒索使用者相 當的金額,造成嚴重損害。
 - 學術網路中的確有部分主機遭受過惡意勒索軟體(ransomware)的侵害,然 而往往找不出明確的感染途徑及惡意程式樣本。
 - 3. 受害者往往必須向駭客支付比特幣作為檔案的解密贖金。
 - 本單位取得的惡意程式樣本進行研究分析,主要以Cryptolocker 的惡意 勒索軟體測試。
- Ⅱ. 事件檢測
 - 1. 使用 VM 虛擬主機並且為 Windows 7 系統進行隔離環境測試。
 - 2. 惡意程式樣本名稱為 128[…]d90. exe,實際執行後會先跳出權限存取的 選項,此指令會刪除磁碟的快照備份,讓使用者無法還原系統。

"vssadmin.exe delete shadows /all /Quiet"

💡 使用	者帳戶控制	×
•	您是否要允許下來	〕程式變更這部電腦?
	■ 程式名稱: 已驗證的發行 程式位置: <u>顯示此發行者</u>	適用於 Microsoft® 磁碟區陰影複製服務的命 令列介面 5者: Microsoft Windows "C:\Windows\System32\vssadmin.exe" delete shadows /all /Quiet [憑證的資訊
▲ 陽	藏詳細資料(D)	是(Y) 否(N)
		變更這些通知顯示的時機

- 原本的惡意程式會開始針對內部文件、影音、圖像檔案進行加密,然後惡 意程式主體就會自我刪除。
- 此時會顯示惡意程式執行的紅色視窗,告知使用者你的檔案已經被加密, 而桌面的背景也會備置換成勒索軟體的相關訊息。

	All your documents, photos, databases and other important files have been encrypted with strongest encryption RSA-2048 key, generated for this computer.
	Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
	If you see the main encryptor red window, examine it and follow the instructions. Otherwise, it seems that you or your antivirus deleted the encryptor program. Now you have the last chance to decrypt your files. Open http://tkj3higtqlvohs7z.aw49f4j3n26.com or http://tkj3higtqlvohs7z.dfj3d8w3n27.com , https://tkj3higtqlvohs7z.s5.tor-gateways.de/ in your browser. They are public gates to the secret server. Copy and paste the following Bitcoin address in the input form on server. Avoid missprints. 1PapvW6apwpSk4XKR6oDZXQEi3daz7DfVh Follow the instructions on the server.
	If you have problems with gates, use direct connection: 1. Download Tor Browser from http://torproject.org 2. In the Tor Browser open the http://tkj3higtqlvohs7z.onion/ Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable. Copy and paste the following Bitcoin address in the input form on server. Avoid missprints. 1PapvW6apwpSk4XKR6oDZXQEi3daz7DfVh Follow the instructions on the server.
	🚳 🏉 🧮 💟 🕼 💐 🖾 📨 🗰 🔺 🙀
5.	惡意程式會威脅使用者必須在 96 小時內將贖金透過以下方式付款到駭客

的比特幣的電子錢包中,並告知此加密是透過 RSA-2048 方式,必須用贖

金來取回加密的私鑰。

6. 透過 Virustotal 線上掃毒,該病毒的檢測比例 45/57 相當高,為

Cryptolocker 系列的勒索軟體。

SHA256:	1287ff57	2592401e16831c274	1648a399aada9d4d7744d53d	c40c0d978bbb329d0			
File name:	1287ff57	2592401e16831c274	1648a399aada9d4d7744d53d	:40c0d978bbb329d0.exe)		
Detection r	ratio: 45 / 57						7 ^
Analysis da	ate: 2015-08-	16 17:17:11 UTC (2	weeks ago)				
Analysis	□ File detail	□ Relationships	□ Additional information	Comments 2	□ Votes	Behavioural inf	formation
Antivirus			Result				Update
ALYac			Trojan.GenericKD.231491	14			20150813
AVG			Generic_r.ESS				20150816
AVware			Trojan.Win32.Generic!BT				20150816
Ad-Aware			Trojan.GenericKD.231491	14			20150816
Agnitum			Trojan.Snocry!				20150815
AhnLab-V3			Trojan/Win32.Cryptolocke	r			20150816

7. 测試時候將其中一個資料夾內放入一些文件檔,包含了 docx、x1sx、jpg、

pdf 四種格式檔案做測試,而惡意程式感染後所有文件檔案的附檔名都會

變成 ecc 格式,導致磁碟中所有文件檔案都無法開啟。

0.jpg.ecc	1.docx.ecc	2.docx.ecc
ECC 檔案	ECC 檔案	ECC 檔案
62.1 KB	12.5 KB	17.7 KB
3.docx.ecc	4.xlsx.ecc	5.xlsx.ecc
ECC 檔案	ECC 檔案	ECC 檔案
18.7 KB	8.75 KB	8.59 KB
6.xlsx.ecc	5071624151465.jpg.ecc	EX6100_UM_11Apr2014.pdf.ecc
ECC 檔案	ECC 檔案	ECC 備案
8.69 KB	511 KB	2.18 MB
HELP_RESTORE_FILES.txt 文字文件 2.61 KB	ipad_user_guide.pdf,ecc ECC 檔案 26.2 MB	

8. 當所有磁碟內部的關聯檔案都被加密後,在桌面中產生三個說明檔案,分

別為「CryptoLocker. 1nk、HeLP_ReSTORe_FILeS. bmp 和

HELP_RESTORE_FILES. txt」,其內容都是引導受害者如何進行繳付勒索贖

V 78		8	
	Your personal files are	encrypted!	
	Your files have been safely encrypted on this PC: pho Click "Show encrypted files" Button to view a complet and you can personally verify this.	otos, videos, documents, etc. te list of encrypted files,	
	Encryption was produced using a unique public key R for this computer. To decrypt files you need to obtain	SA-2048 generated 1 the private key.	
ur private key will be destroyed on:	The only copy of the private key, which will allow you is located on a secret server in the Internet; the serv- after a time period specified in this window. Once this has been done, nobody will ever be a In order to decrypt the files press button to or	u to decrypt your files, eer will eliminate the key able to restore files pen your personal page	
8/35/2015	File decryption site and fo	blow the instruction.	
ne left: 95:57:05	in case of "File decryption button" malfunction http://tkj3higtqlvohs7z.dfj3d8w3n27.com https://tkj3higtqlvohs7z.tor2web.blutmagie.dr	use one of our gates: e	
	1PapvW6apwpSk4XKR6oDZXQEi3	er the site: Bdaz7DfVh	
	Click to copy address to clip	pboard	
	if both button and reserve gate not opening, please for	ollow the steps:	
	You must install this browser <u>www.torproject.org/pro</u> After instalation.run the browser and enter address 3	ojects/torbrowser.ntml.en 3kxwiihmkaibht2s.onion	
	Follow the instruction on the web-site. We remind yo the more chances are left to recover the files.	ou that the sooner you do so,	
	Any attempt to remove or corrupt this so in immediate elimination of the private k	ftware will result ey by the server.	1
	Click for Free Decryption on site		



9. 惡意程式執行後會自動開啟 CryptoLocker 捷徑檔案,該惡意程式檔名為

ynlgwty.exe,此程式存於C槽的隱藏資料夾中「\AppData\Roaming\」,

就是自動跳出的紅底黑字視窗程式。

一般 捷徑	相容性 安全性 詳細資料 以前的版本
Ci	yptoLocker
目標類型:	應用程式
目標位置:	Roaming
目標(T):	C:\Users\Dark\AppData\Roaming\ynlgwty.exe
怏速鍵(K):	無
執行(R):	標準視窗
註解(0):	!!!SAFE your files!!!
開取檔案的	过置(F) 變更圖示(C) 進階D)
ynlgwty.exe:13	52 Properties
ynlgwty.exe:13	52 Properties
ynlgwty.exe:13 TCP/IP Image Perfo	52 Properties
ynlgwty.exe:13 TCP/IP Image Perfo Image File	52 Properties
TCP/IP Image Perfo	52 Properties
ynlgwty.exe:13 TCP/IP Image Perfo Image File	52 Properties
ynlgwty.exe:13 TCP/IP Image Perfo Image File Version: n/a Build Tue	52 Properties
ynlgwty.exe:13 TCP/IP Image Perfo Image File Version: n/a Build Tue Path:	52 Properties
TCP/IP Image Perfor Image File Version: n/a Build Tue Path: C:\Users\Dark	52 Properties
ynlgwty.exe:13 TCP/IP Image Perfo Image File Version: n/a Build Tue Path: C:\Users\Dark Command line:	52 Properties
ynlgwty.exe:13 TCP/IP Image Perfo Image File Version: n/a Build Tue Path: C:\Users\Dark Command line: C:\Users\Dark	52 Properties
ynlgwty.exe:13: TCP/IP Image Perfo Image File Version: n/a Build Tue Path: C:\Users\Dark Command line: C:\Users\Dark Current directo	52 Properties
ynlgwty.exe:13: TCP/IP Image Perfo Image File Version: n/a Build Tue Path: C:\Users\Dark Command line: C:\Users\Dark Current directo C:\Windows\S	52 Properties
ynlgwty.exe:13: TCP/IP Image Perfo Image File Version: n/a Build Tue Path: C:\Users\Dark Command line: C:\Users\Dark Current directo C:\Windows\S Autostart Locat	52 Properties

10. 該程式同時會寫入開機自動啟用註冊檔中,程序名稱為 msdedf,檔案

路徑為「\roaming\ynlgwty.exe」。

🖅 Everything 🛛 🛋 Logon	🚼 Explorer	🥭 Internet Explorer	🙆 Scheduled Tasks	Services	Brivers	Codecs	Boot Execute	📑 Ir
Autorun Entry Desci	ription P	ublisher In	nage Path			Time	estamp	
📽 HKLM\SOFTWAP	RE\Microsoft	t\Windows\Curren	tVersion\Run			2015	/8/31 上午 10):23
🔽 📼 VMw VMw	are Tool V	Mware, Inc. c:\	program files\vmv	ware\vmwar	e tools\vm	ool 2014	/11/21 上午 ()5:48
HKLM\SOFTWAF	RE\Microsoft	t\Active Setup\Ins	talled Component	ts		2011	/4/12 下午 03	3:15
🗹 🗟 Brow Wind	ows Mail M	licrosoft Cor c:\j	program files\win	dows mail\v	vinmail.exe	2009	/7/14 上午 07	/:42
🗹 🖻 Direc Wind	ows Mail M	licrosoft Cor c:\j	program files\win	dows mail\v	vinmail.exe	2009	/7/14 上午 07	/:42
🗹 🗟 Intern Wind	ows Mail M	licrosoft Cor c:\;	program files\win	dows mail\v	vinmail.exe	2009	/7/14 上午 07	/:42
🗹 🗟 Intern Wind	ows Mail M	licrosoft Cor c:\;	program files\win	dows mail\v	vinmail.exe	2009	/7/14 上午 07	/:42
🗹 🗟 Micro Wind	ows Mail M	licrosoft Cor c:\j	program files\win	dows mail\v	vinmail.exe	2009	/7/14 上午 07	/:42
🗹 🗟 Micro Wind	ows Mail M	<u>licrosoft Cor c:\</u>	program files\win	dows mail\v	vinmail.exe	2009	/7/14 上午 07	/:42
HKCU\Software\M	licrosoft\Wir	ndows\CurrentVer	sion\Run			2015	/10/1 上午 10):13
🗹 🖻 msdedf		c:\	users\dark\appdat	a\roaming\y	nlgwty.exe	2015	/4/21 下午 08	3:54

11. 開啟惡意程式 ynlgwty.exe 提供的三個贖金網站網址

http://tkj3higtqlvohs7z.dfj3d8w3n27.com 、

https://tkj3higtqlvohs7z.s5.tor-gateways.de/」,一般瀏覽器都無法 正常開啟。

12. Tor Browser 為匿名網路瀏覽器,也就是透過該瀏覽器作為中繼代理, 進而能夠連線到一般 DNS 無法解析的網站,為一種中繼網路。此例表示我 們會使用 185.73.44.58 作為中繼代理,去連到匿名的贖金網站。



13. 因為前三個贖金網址都無法開啟,改用匿名網路瀏覽器 Tor Browser 開啟第四個匿名網址「http://tkj3higtqlvohs7z.onion/」,然而也無法 正常顯示,判斷可能該惡意贖金網站已經被移除。





16. 當主機取得 IP 資訊後惡意程式會轉向德國的 192. 251. 226. 206:137 發

送 Netbois 協定的 UDP 封包, 一般做為同網段網路芳鄰探測使用, 此處研

判可能為向上層中繼站報到。

N Ti	Witness Reconstruction for session ID: 42 (Source 140.: 137, Target 192.251.226.206 : 137) e 8/31/2015 10:37:23 to 8/31/2015 10:37:29 Packet Size 2,208 bytes Payload Size 1,200 bytes prol.2048/17/137 Elans Keen Assembled AppMeta NetworkMeta, Parket Count 24
F E U E E T	

17. 透過 Virustotal 檢測此網站 192.251.226.206,發現到有一家防毒引

Detection ratio:	1 / 63	00/		
Analysis date:	2015-09-11 05:29:37	7 UTC (3 weeks, 2 days	ago)	e r U 🥶
Analysis Addition	tional information 🧼 🗩 Co	omments 🧿 🛛 🖓 🕅	′otes	
Analysis Addit	ional information 🗭 Co	Result	′otes	
Analysis Addi URL Scanner Fortinet	ional information 🌩 Ca	Result Malware site	/otes	
Analysis Addi URL Scanner Fortinet ADMINUSLabs	ional information 🌩 Co	Result Malware site Clean site	/otes	

擎偵測為惡意網址,因此懷疑可能為駭客所用。

18. 隨後惡意程式 ynlgwty. exe 會再向網址 secure2. alphassl. com 的 port

80 連線, 位址為美國的 104.16.28.16, GET 取得一個名為

gsalphag2.crt 憑證公鑰,為產生惡意程式加密檔案私鑰。





20. 主機感染後無法透過 Tor 匿名網路開啟贖金網站,可能贖金網站已經被

相關單位撤除,換言之一旦感染此惡意程式無法還原資料。



1. 使用者可能透過瀏覽器或系統漏洞誤執行到惡意程式 Cryptolocker。

- 2. 主機感染惡意程式後向網站「ipinf.io」取得 IP 位址。
- 3. 惡意程式開始向 192.251.226.206 發送 netbios 協定封包進行報到。
- 4. 惡意程式向 secure2. aplpassl. com 下載 crt 憑證公鑰。。
- 5. 惡意程式向 ocsp. global sign. com HTTP GET 回傳加密私鑰。
- 6. 受害者必須透過Tor Browser 進入洋蔥匿名網路,使用中繼代理主機。
- 7. 無法開啟贖金網站,可能該網站已經被相關單位撤除。
- 8. 駭客能持續監控贖金網站以及散播惡意程式。

Ⅳ.建議與總結

- 使用者可能透過被APT攻擊或網路下載執行到惡意程式而遭受感染,目前 有多數人回報是透過瀏覽器就莫名遭受感染,並未下載執行到可疑檔案。
- 主機一旦被感染後,惡意程式會開始加密所有磁碟中的文件檔、圖片檔和 影音檔案。

- 3. 惡意程式一旦加密完各類檔案後會自我刪除,不讓使用者取得惡意程式。
- 惡意程式隨後會更改系統桌面以及跳出程式紅底畫面,引導受害者如何去 支付贖金來取得解密私鑰。
- CrytoLokcer 號稱使用 RSA-2048 加密,因為沒有私鑰基本上是無法救回 檔案,建議使用者要定期備份重要資料避免無法挽回。
- 理論上感染惡意程式後可以透過 Tor Browser 開啟匿名贖金網站,然而 此例測試發現無法開啟,應該是贖金網站已經被撤除,故若使用者感染此 惡意程式則無法取得私鑰還原。
- 7. 建議使用者將系統重新安裝,避免病毒遺留的影響往後可能再次發生。
- 建議使用者將作業系統更新,並且更新常用套件如 Adobe Flash Player、 Adobe Reader、Java 等,這些漏洞都有可能導致感染 Cryptolocker 勒索 程式。