從加密勒索攻擊看企業資料安全風險

達友科技

FORCEPOINT
POWERED BY Raytheon

什麼是加密勒索(Ransomware)攻擊?

‘Ransomware‘是一種惡意軟體，藉由侵入使用者電腦、加密所有重要文件、影像、數據資料，逼迫使用者交付贖金以取回資料。

*.jpg, *.jpeg, *.raw, *.tif, *.gif, *.png, *.bmp, *.3dm, *.max, *.accdb, *.db, *.dbf, *.mdb, *.pdb, *.sql, *.*sav*, *.*spv*, *.*grle*, *.*mlx*, *.*sv5*, *.*game*, *.*slot*, *.dwg, *.dxf, *.c, *.cpp, *.cs, *.h, *.php, *.asp, *.rb, *.java, *.jar, *.class, *.aaf, *.aep, *.aepx, *.plb, *.prel, *.prproj, *.aet, *.ppj, *.psd, *.indd, *.indl, *.indt, *.indb, *.inx, *.idml, *.pmd, *.xqx, *.xqx, *.ai, *.eps, *.ps, *.svg, *.swf, *.fla, *.as3, *.as, *.txt, *.doc, *.dot, *.docx, *.docm, *.dotx, *.dotm, *.docb, *.rtf, *.wpd, *.wps, *.msg, *.pdf, *.xls, *.xlt, *.xlm, *.xlsx, *.xlsm, *.xltx, *.xltm, *.xlsb, *.xla, *.xlam, *.xll, *.xlw, *.ppt, *.pot, *.pps, *.pptx, *.pptm, *.potx, *.potm, *.ppam, *.ppsx, *.ppsm, *.sldx, *.sldm, *.wav, *.mp3, *.aif, *.iff, *.m3u, *.m4u, *.mid, *.mpa, *.wma, *.ra, *.avi, *.mov, *.mp4, *.3gp, *.mpeg, *.3g2, *.asf, *.asx, *.flv, *.mpg, *.wmv, *.vob, *.m3u8, *.csv, *.efx, *.sdf, *.vcf, *.xml, *.ses, *.dat

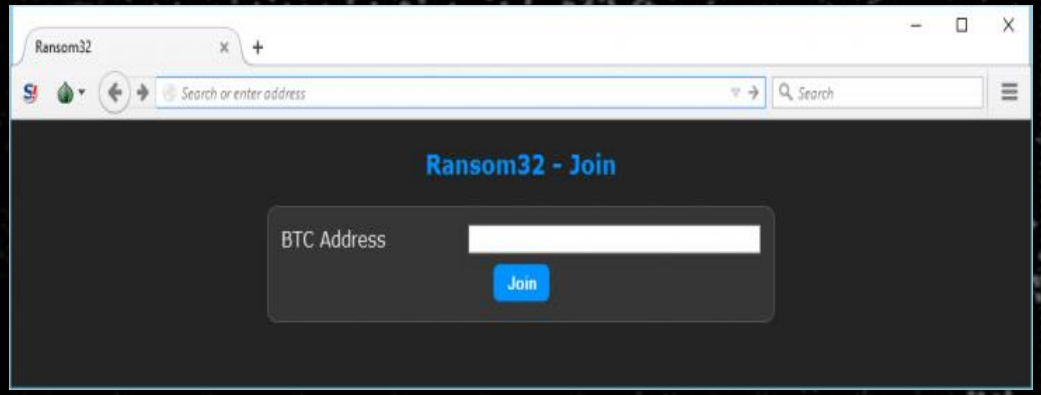
公司重要文件。程式碼。資料庫檔案。產品設計圖。產品計畫。交易紀錄。專案資料。產品配方。客戶聯絡資訊。影音創作。與朋友家人的珍貴照片、影片。重要研究論文。

加密勒索攻擊二三事

- 以CryptoLocker而言，首二個月高達攻擊者獲得2700萬美金的贖金交付。
- 被加密的檔案除非付贖金取得加密私鑰，否則幾乎無法回復 (RSA金鑰加密長度已達4096位元)
- 某些勒索軟體具備缺陷，即使付出贖款仍然無法回復檔案。
- 一旦中毒，使用者必須在短時間內(三天)採取行動，否則
  - 贖金加倍
  - 銷毀解密私鑰
- 藉由比特幣(Bitcoin)電子貨幣的匿名性，助長了攻擊者取得贖金的便利性—
  - 使用者非常容易繳付贖金，甚至在便利商店也可以
  - 攻擊者非常難以被追蹤，付出的風險非常低

FORCEPOINT
POWERED BY Raytheon

雲端自助連鎖加盟，大家一起來當加密勒索駭客



FORCEPOINT
POWERED BY Raytheon

http://blog.emsisoft.com/2016/01/01/meet-ransom32-the-first-javascript-ransomware/

當企業遭受加密勒索攻擊.....

http://blog.emsisoft.com/2016/01/01/meet-ransom32-the-first-javascript-ransomware/

當企業遭受加密勒索攻擊.....

公司要倒了嗎…
因為會計部的堅持erp伺服器在他們單位
(他們認為他們是完全獨立單位)
也有會計部資訊組
會資組今天上午erp當掉打來資訊部說
他用伺服器update 順便 check mail
運氣很好，免費中獎 iphone 6S
點了以後沒有反應
重開機發現資料都被加密了……
中了cryptolocker
問我們怎麼辦？！拜托就解

這位同事可以打包了吧？
我也可以找新公司了吧？
別問我為什麼沒有防毒

他們家不歸我們家管
就讓你獨立吧!
豬隊友

ERP Day 4 Part 1
【豬會計部、會計資訊組、掩蓋、資訊部的正義】

在10點開會以前、資訊部開了個小會
主任說大家最近很有空、因為有人出包了。
我朋友這邊有些缺額有興趣的自己跟我說。
要推薦函的也跟我說一定寫正面的！
大家要有心裡準備、我也可能位置不保了。
（超感動 要落淚了）

(節錄重點)
會主：報告、各位長官這次我們ERP系統資料被加密所以系統產生當機
總經理：很好阿！加密才安全、是加密所以電腦跑不動嗎，需要多少預算？
會主：因為廠商建議我們加密、結果因為設備老舊所以意外的失敗了！
(ME: WHAT THE FUCK??)

ERP Day 4 Part3
董事長
1.會計部主任調離主管現職、副主任代理
2.會計資訊組組長、x調離現職、整組重編
3.你們三個自己應該心裡有數、我會請律師處理
3.下個月薪水照發、這個月誰有加班自己去人資部簽名
4.月底公佈在一樓誰亂簽、被自己單位同事揭發沒有信用的人我們不需要
5.伺服器搬回資訊部機房、由資訊部統一管理

接下來就是恢復期也沒什麼好收看了？
公司有列印習慣與邊冊、所以資料只差一週
設定全要重來真的是哇靠
討論後決定格式化、全新重來也不錯
只補2015資料其他的再找時間補打、會計年底結帳最重要
資訊主任怕揭發遇不測
以上為屬事實位於台北市
資安教育不能等
END

FORCEPOINT
POWERED BY Raytheon

攻擊主要途徑

網際網路

電子郵件

攻擊途徑→網際網路 

- 利用水坑式攻擊手法
- 高達六~七成的網路流量是HTTPS加密
- 利用應用程式或系統漏洞
  - 近期利用Adobe Flash漏洞，以廣告輪播方式散布

攻擊途徑→電子郵件

- 利用社交工程攻擊手法，如寄送發票、訂單、電子帳單、罰單、繳稅通知、郵寄快遞通知。
- 近期著名的Locky利用MSOffice巨集夾帶惡意程式

為什麼可以穿透企業防禦?

- 變種太快，防毒特徵碼無法防禦零時差攻擊。
- 在關鍵的網際網路與電子郵件管道缺乏進階安全防禦能力

FORCEPOINT
POWERED BY Raytheon

加密勒索攻擊與企業資料安全風險

- 一旦核心資料、系統、資料庫遭到加密攻擊，企業將面臨重大損失甚至無法營運。
- 企業檔案伺服器共用資料夾/共享磁碟，也暴露在高度風險當中
- 其他攻擊亦可利用同樣手法入侵企業，某些作為資料竊取意圖的潛伏惡意軟體造成的隱性傷害更是難以衡量

如何因應加密勒索攻擊→墊高攻擊成功門檻

- 確保作業系統與應用程式維持最新的更新狀態，停止使用高風險應用軟體
- 建立網際網路進出流量的進階安全與HTTPS解密分析能力
  包含分析資料往外傳輸分析(阻斷加密金鑰回傳與加密資料竊取)
- 建立電子郵件社交工程與進階威脅安全分析能力
- 利用檔案與URL沙箱防護零時差/變種攻擊
- 定期備份重要資料，且務必確保有離線版本
- 實施軟體或系統更嚴謹的鎖定政策
- 強化企業員工資安意識

FORCEPOINT
POWERED BY Raytheon

你現在的WEBSENSE有幫公司保護到最新的攻擊手法嗎？

項次	攻擊手法	Websense防禦工具	對應產品	對應產品	對應產品
1	Advanced Persistent Threat (APT)	RTSC/ Anti-Malware Engines / Behavorial Sandboxing	AP-web(WSG)	sandbox	
2	Adware	Anti-Malware Engines	AP-web(WSG)		
3	Anonymity services	RTCC	AP-web(WSG)		
4	Auto-generated domains	Reputation Analysis	AP-web(WSG)		
5	Backdoor	Anti-Malware Engines	AP-web(WSG)		
6	Blackhat SEO	RTSC/ URL Classification	Web Filter/WSS	AP-web(WSG)	
7	Botnet Command & Control	RTSC/ RTDC/ URL Classification	Web Filter/WSS	AP-web(WSG)	
8	Custom packed files	Anti-Malware Engines	AP-web(WSG)		
9	Data stealers	Anti-Malware Engines	AP-web(WSG)		
10	Dialers	Anti-Malware Engines	AP-web(WSG)		
11	Drive-by downloads	RTSC / Behavorial Sandboxing	AP-web(WSG)	sandbox	
12	Dynamic DNS	URL Classification	Web Filter/WSS		
13	Elevated risk profiles	RTSC / Behavorial Sandboxing	AP-web(WSG)	sandbox	
14	Embedded code (e.g., inside PDF, SWF files)	RTSC /Anti-Malware Engines	AP-web(WSG)		
15	Emerging exploits	RTSC	AP-web(WSG)		
16	Exploit code	RTSC	AP-web(WSG)		
17	Exploit kits	RTSC	AP-web(WSG)		
18	Fast flux	Reputation Analysis	AP-web(WSG)		
19	File infectors	Anti-Malware Engines	AP-web(WSG)		
20	Hacking tools	RTSC/ Anti-Malware Engines/ URL Classification	Web Filter/WSS	AP-web(WSG)	

FORCEPOINT
POWERED BY Raytheon

你現在的WEBSENSE有幫公司保護到最新的攻擊手法嗎？

項次	攻擊手法	Websense防禦工具	對應產品	對應產品	對應產品
21	Hijacked websites	RTSC/URL Classification	Web Filter/WSS	AP-web(WSG)	
22	Illegal content	RTCC	AP-web(WSG)		
23	Keyloggers	Anti-Malware Engines	AP-web(WSG)		
24	Low reputation domains	Reputation Analysis	AP-web(WSG)		
25	Malicious Active X	RTSC	AP-web(WSG)		
26	Malicious Applet	RTSC/ Anti-Malware Engines	AP-web(WSG)		
27	Malicious binaries (e.g., Windows Executables)	Anti-Malware Engines	AP-web(WSG)		
28	Malicious browser plug-in	RTSC/ Anti-Malware Engines	AP-web(WSG)		
29	Malicious flash files	Anti-Malware Engines	AP-web(WSG)		
30	Malicious insider threat	RTDC	AP-Data(Gateway DLP)		
31	Malicious JavaScript	RTSC	AP-web(WSG)		
32	Malicious Obfuscated code	RTSC	AP-web(WSG)		
33	Malicious packers	Anti-Malware Engines	AP-web(WSG)		
34	Malicious PDF	Anti-Malware Engines	AP-web(WSG)		
35	Malicious RIA	RTSC/ Anti-Malware Engines	AP-web(WSG)		
36	Malicious URL Redirection	RTSC/ URL Classification	Web Filter/WSS	AP-web(WSG)	
37	Malicious Visual Basic scripts	RTSC	AP-web(WSG)		
38	Malicious/suspicious embedded iframes	RTSC	AP-web(WSG)		
39	Man-in-the-middle	RTSC	AP-web(WSG)		
40	Packed files	Anti-Malware Engines	AP-web(WSG)		

FORCEPOINT
POWERED BY Raytheon

你現在的WEBSENSE有幫公司保護到最新的攻擊手法嗎？

項次	攻擊手法	Websense防禦工具	對應產品	對應產品	對應產品
41	Password stealers	Anti-Malware Engines	AP-web(WSG)		
42	Phishing	RTSC/ URL Classification	Web Filter/WSS	AP-web(WSG)	
43	Polymorphic binaries	Anti-Malware Engines	AP-web(WSG)		
44	Porn/gambling/illegal drugs	RTCC	AP-web(WSG)		
45	Potentially unwanted software	Anti-Malware Engines	AP-web(WSG)		
46	Productivity Loss	RTCC	AP-web(WSG)		
47	Remote Access Trojans (RATs)	Anti-Malware Engines	AP-web(WSG)		
48	Rogue/Fake AV	RTSC/ Anti-Malware Engines	AP-web(WSG)		
49	Rootkits	Anti-Malware Engines	AP-web(WSG)		
50	Shell code	RTSC	AP-web(WSG)		
51	Social engineering	RTSC	AP-web(WSG)		
52	Social web threats	RTCC/ RTSC	AP-web(WSG)		
53	Spam links	RTSC/ URL Classification	Web Filter/WSS	AP-web(WSG)	
54	Spyware	Anti-Malware Engines	AP-web(WSG)		
55	Targeted attacks	RTSC/ Anti-Malware Engines/ Behavorial Sandboxing	AP-web(WSG)	sandbox	
56	Trojan downloader	Anti-Malware Engines	AP-web(WSG)		
57	Trojan dropper	Anti-Malware Engines	AP-web(WSG)		
58	Viruses	Anti-Malware Engines	AP-web(WSG)		
59	Web spam	RTSC/ URL Classification	Web Filter/WSS	AP-web(WSG)	
60	Website Defacements	RTSC/ URL Classification	Web Filter/WSS	AP-web(WSG)	
61	Worms	Anti-Malware Engines	AP-web(WSG)		
62	XSS (cross-site scripts)	RTSC	AP-web(WSG)		
63	Zero-day exploit code	RTSC/ Anti-Malware Engines/ URL Classification/ Behavorial Sandboxing	Web Filter/WSS	AP-web(WSG)	sandbox

FORCEPOINT
POWERED BY Raytheon

Thanks

FORCEPOINT
POWERED BY Raytheon

