WannaCry勒索軟體報告

大綱

1) 簡介
2) 技術
3) 受災情況
4) 案例
5) 暫時性解決方案
6) 補充資訊
7) 資料來源

簡介

簡介

- WannaCry勒索軟體（直譯「想哭」，另稱WannaCrypt、WanaCrypt0r 2.0、Wanna Decryptor)是一種利用NSA的「永恆之藍」（EternalBlue）攻擊系統漏洞工具，透過全球網路對使用Windows作業系統的電腦進行攻擊；屬於加密性勒索軟體蠕蟲（Encrypting Ransomware Worm）。
- 此勒索軟體利用AES-128和RSA演算法加密，把受感染電腦內的檔案加密，造成使用者損失與困擾；並且在五月中旬爆發全球電腦大規模感染。
- 北區校園網路最早在五月上旬就有大量觸發該事件且告警，而北區ASOC於觸發隔天開出大量資安事件單。

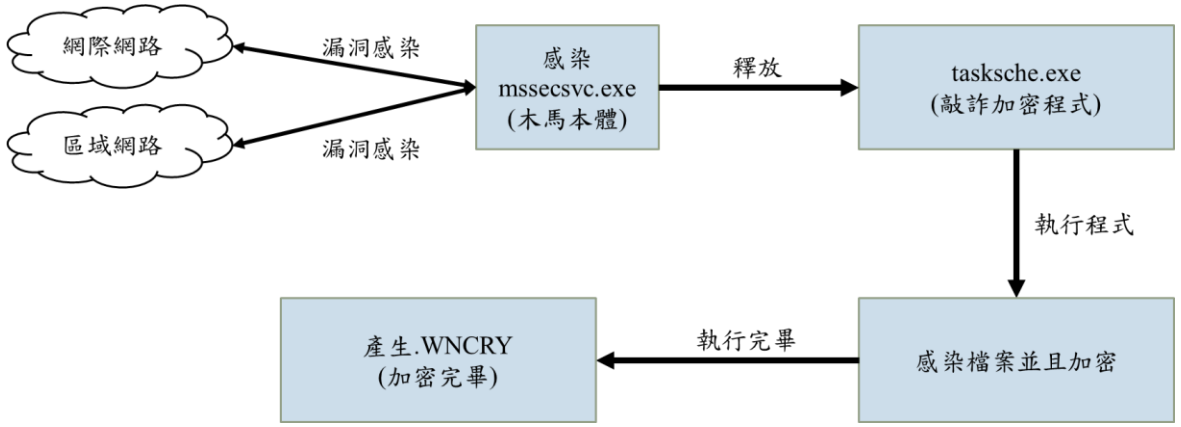
ASOC

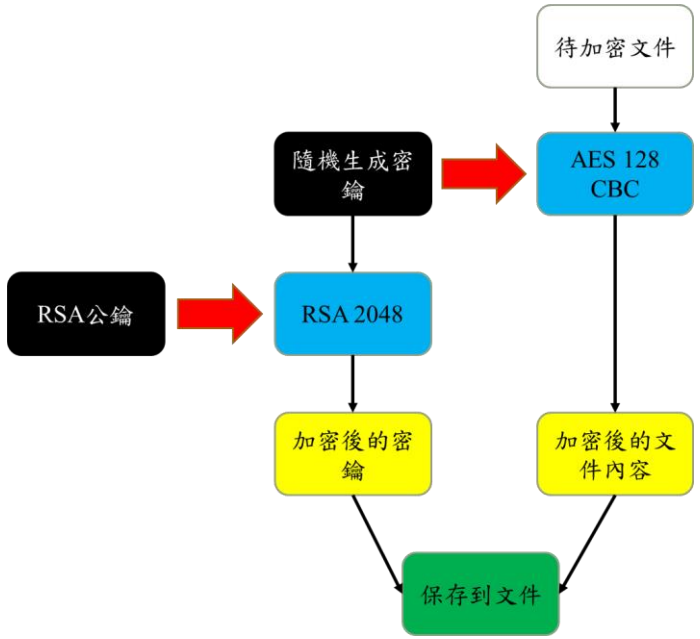
事件編號	攻擊名稱	事件單狀態	事件名稱	攻擊開始時間	問題IP Address	開單時間	所屬區網中心	學校名稱	AISAC代號	AISAC類型	IP單位
0000933143	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 06:05:09 下午	45.32.212.213	05/10/2017 08:15:13 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933149	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 06:36:08 下午	104.156.230.150	05/10/2017 08:15:42 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933152	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 06:45:15 下午	185.92.220.133	05/10/2017 08:15:56 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933156	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 06:52:53 下午	45.32.23.153	05/10/2017 08:16:15 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933157	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 06:54:11 下午	45.63.71.160	05/10/2017 08:16:20 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933161	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:05:05 下午	183.249.194.149	05/10/2017 08:16:42 上午	宜蘭區網中心		402	對外攻擊	ELSE
0000933163	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:07:31 下午	108.61.204.181	05/10/2017 08:16:53 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933167	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:13:00 下午	45.32.156.26	05/10/2017 08:17:11 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933168	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:13:38 下午	45.76.25.78	05/10/2017 08:17:17 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933171	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:41:39 下午	104.156.245.216	05/10/2017 08:17:30 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933172	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:43:48 下午	45.76.187.91	05/10/2017 08:17:36 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933173	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:43:50 下午	45.32.1.224	05/10/2017 08:17:41 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933174	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:50:38 下午	45.77.27.45	05/10/2017 08:17:47 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933175	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:52:05 下午	45.63.34.252	05/10/2017 08:17:52 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933176	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:53:02 下午	45.76.234.180	05/10/2017 08:17:57 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933178	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:54:58 下午	45.76.68.100	05/10/2017 08:18:08 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933179	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:55:29 下午	45.76.82.143	05/10/2017 08:18:19 上午	台北區網中心(台大SF)		402	對外攻擊	ELSE
0000933182	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:56:41 下午	45.32.1.111	05/10/2017 08:18:35 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933183	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 07:58:46 下午	45.32.232.70	05/10/2017 08:18:40 上午	宜蘭區網中心		402	對外攻擊	ELSE
0000933185	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:01:21 下午	45.32.192.193	05/10/2017 08:18:51 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933186	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:01:46 下午	45.77.7.74	05/10/2017 08:18:56 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933187	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:03:25 下午	45.32.175.212	05/10/2017 08:19:02 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933189	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:04:38 下午	45.76.32.5	05/10/2017 08:19:10 上午	宜蘭區網中心		402	對外攻擊	ELSE
0000933190	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:04:48 下午	45.76.117.91	05/10/2017 08:19:15 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933195	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:07:32 下午	45.63.24.95	05/10/2017 08:19:39 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933196	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:08:03 下午	108.61.205.245	05/10/2017 08:19:44 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE
0000933197	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:10:31 下午	45.32.174.51	05/10/2017 08:19:50 上午	竹苗區網中心(交大)		402	對外攻擊	ELSE
0000933198	外部主機進行提升權限攻擊	結案完成	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	05/09/2017 08:13:50 下午	104.207.150.97	05/10/2017 08:19:55 上午	台北-2區網中心(政大SF)		402	對外攻擊	ELSE

技術

技術

1. 利用CVE-2017-0144(SMB漏洞)攻入目標機器，取得權限後下載木馬程式
2. 對區域網路和網際網路進行連接埠掃描，擴大感染範圍；釋放敲詐加密程式
3. 執行敲詐加密程式，使用RSA 2048和CBC模式AES加密文件內容
4. 保存加密後的.WNCRY檔，刪除原始文件檔
5. 完成文件加密後釋放說明文檔，跳出勒索文件





受災情況

5/15 當天統計紀錄

- 範圍: 150個國家，超過20萬台電腦受害

(來源: http://www.appledaily.com.tw/realtimenews/article/new/20170515/1118638/)

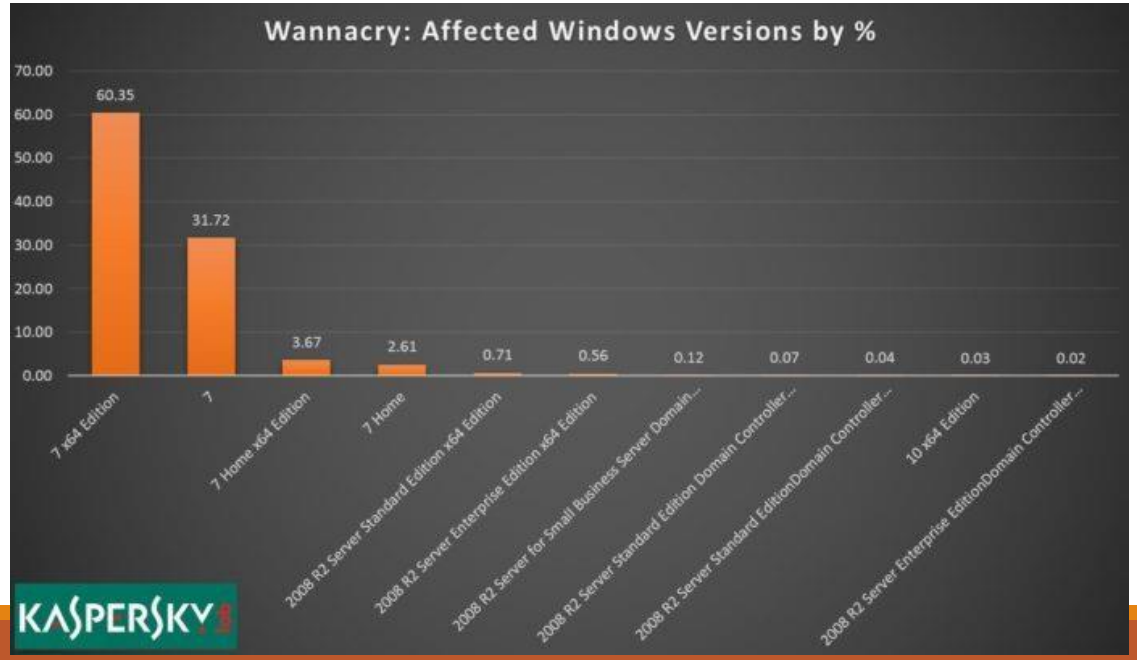
- 北區校園網路情況:
  - 中央: 防火牆上有阻擋port 445。
  - 宜大: 防火牆上有阻擋port 445。
  - 清大: 學校電腦有設定自動更新，截至今早沒有發生。
  - 交大: 防火牆上有阻擋port 445。
  - 暨南: 4/26在IPS上有規則觸發，已設為drop封包。
  - 政大: 因前幾天的通報已有做阻擋。
  - 台大:防火牆上有阻擋port 445。
- 通報情況:

台大區網從5/10至5/15早上約有兩千五百筆資安事件單

受害作業系統統計

- 截至5/21日為止，根據 Kaspersky Lab 的數據顯示，受到 WannaCry 攻擊的電腦之中，最大宗為Windows 7(所有版本合計占約98%)；其次為windows 2008 R2 Server(所有版本合計占約2%)；剩下比例為其他Windows作業系統所占。

- 此現象說明Windows 7 仍為是世界上最普及的系統，且大部分使用者可能沒有時常更新作業系統的更新檔；而 Windows 10會因強制自動更新而降低此事件發生率。最後要提到的是 Windows XP 。

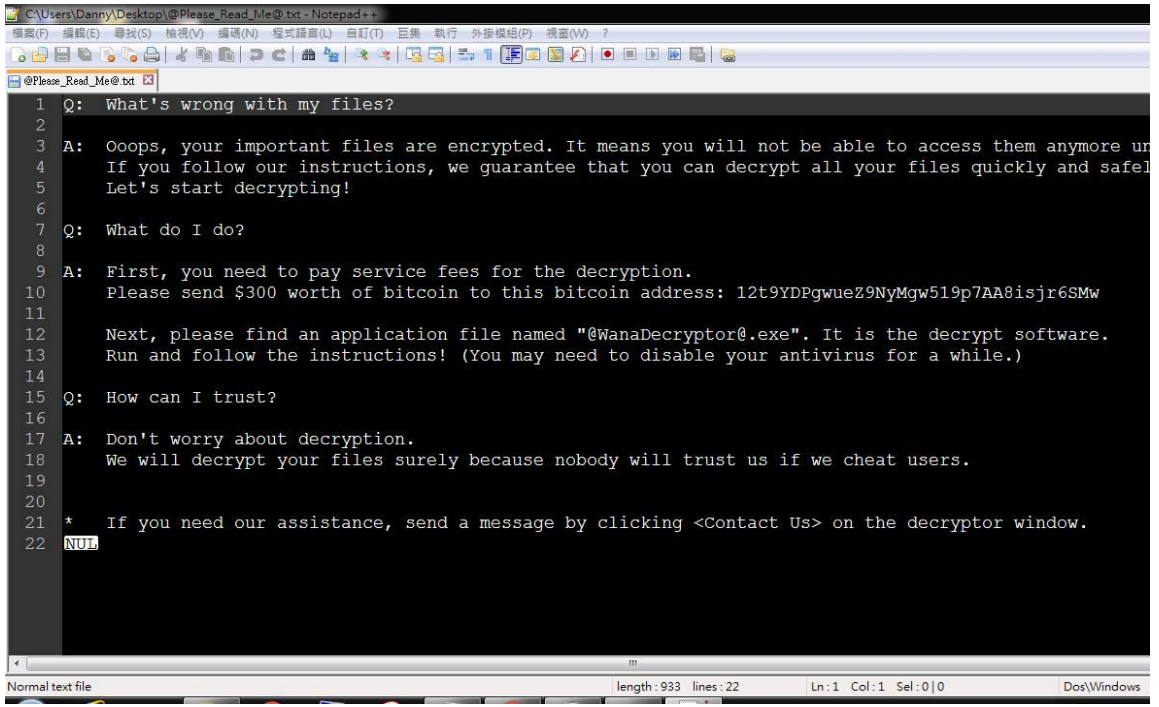


圖片來源:https://unwire.hk/2017/05/21/wannacry-victim-statistics/tech-secure/

案例

案例一 學生個人電腦


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (traditiona
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪
Payment will be raised on
1/4/1970 08:00:00
Time Left
00:00:00:00
Your files will be lost on
1/8/1970 08:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


C:\Users\Danny\Desktop\@Please_Read_Me@.txt - Notepad++
@Please_Read_Me@.txt
Q: What's wrong with my files?
A: Ooops, your important files are encrypted. It means you will not be able to access them anymore un
If you follow our instructions, we guarantee that you can decrypt all your files quickly and safel
Let's start decrypting!
Q: What do I do?
A: First, you need to pay service fees for the decryption.
Please send $300 worth of bitcoin to this bitcoin address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt software.
Run and follow the instructions! (You may need to disable your antivirus for a while.)
Q: How can I trust?
A: Don't worry about decryption.
We will decrypt your files surely because nobody will trust us if we cheat users.
* If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.
Normal text file
length : 933 lines : 22
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows

案例二 恩主公醫院

- 新聞標題: 恩主公醫院淪陷！「勒索病毒」入侵醫療推車電腦：檔案已鎖碼
- 新聞內容:新型勒索病毒WannaCry肆虐全球，至今不但有超過150個國家受害，如今連新北市恩主公醫院的電腦也難逃一劫，被勒索將近300美元的比特幣。對此，恩主公醫院表示，病患個資未受到影響，目前已逐一清查院內電腦，並重灌中毒的醫療推車電腦。(節錄部分)

- 新聞來源: http://www.ettoday.net/news/20170514/924318.htm (東森新聞雲)

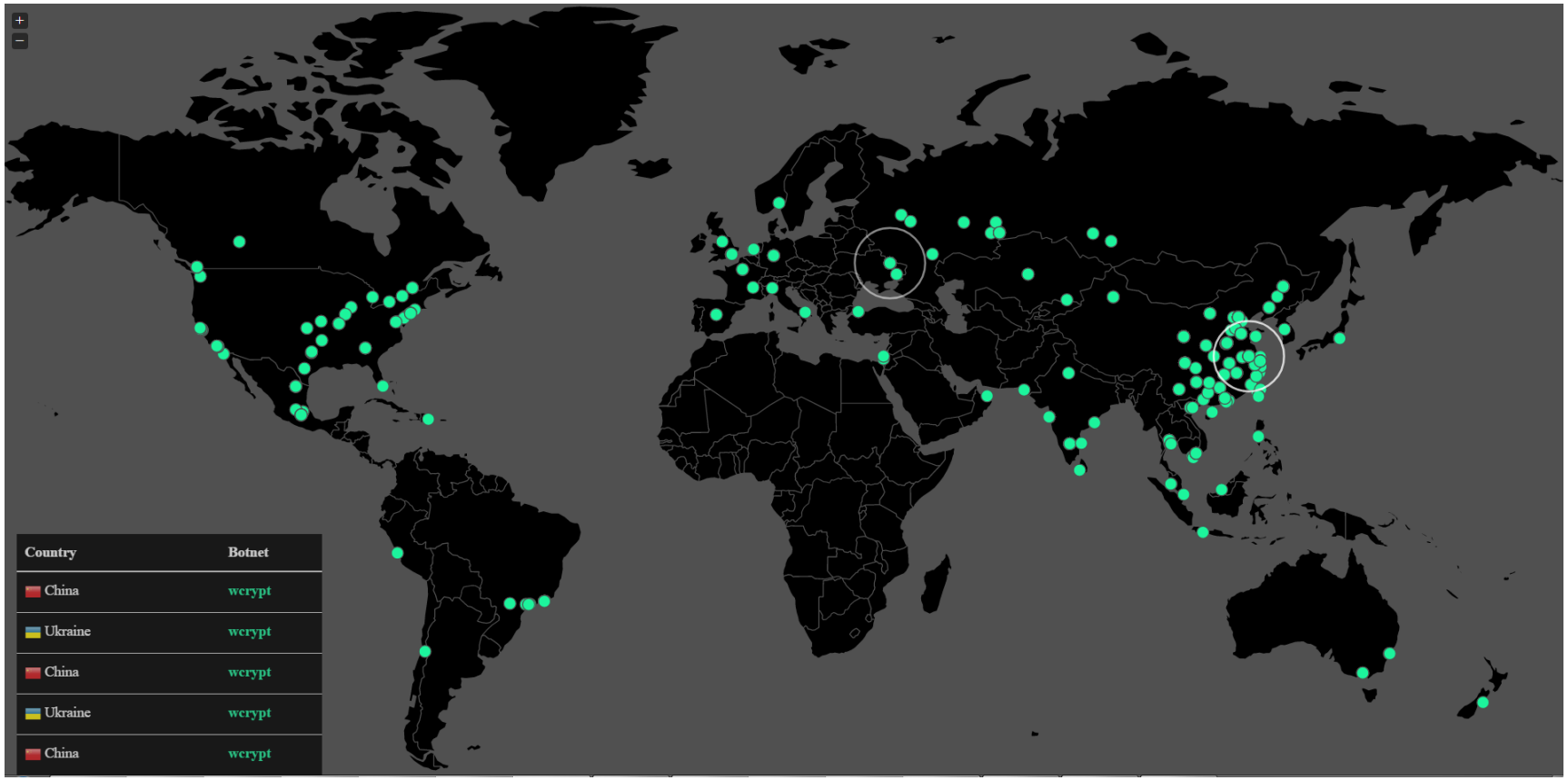
案例三 中國石油(中國)

- 新聞標題:勒索病毒新增受害人，中國2萬加油站斷網
- 新聞內容:勒索病毒「WannaCry」肆虐全球，中國新增受害者，中國國營的中國石油天然氣集團傳出災情，中石油旗下2萬座加油站從周六凌晨突然斷網，無法使用網路支付等功能，經35個小時後，昨中午12時已有8成恢復連網。 (節錄部分)

- 新聞來源: http://www.appledaily.com.tw/realtimenews/article/international/20170515/1118738/(蘋果日報)
- 圖片來源: https://www.bnext.com.tw/article/44481/ransomware-virus-attacks-across-the-globe-fear-of-loss-imponderable (數位時代)

案例四 全球勒索病毒受災情況

網站網址: https://intel.malwaretech.com/WannaCrypt.html



暫時性解決方案

暫時性解決方案(5/15)

- ✓ 由英國經營Blog-MalwareTech的網友所發現。
- ✓ 透過勒索病毒的反分析機制漏洞來破解。
  - WannaCry勒索病毒的反分析機制是利用向DNS 查詢尚未註冊的網域名稱 iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
    1. (正常情況下)如果DNS回應此網域查無IP尚未註冊，則WannaCry勒索病毒便會認為安全，可以繼續擴散。
    2. 但是如果DNS回應了此網域的IP， WannaCry病毒會覺得自己可能已被置於沙盒(Sandbox)測試環境中，便會停止活動與擴散，以防被研究人員分析破解，縮短病毒的壽命。
       - 沙盒(Sandbox)測試環境通常是資安滲透測試人員用來研究攻擊手法，所建立的一個與外界隔絕的虛擬環境。
- ✓ 而這名網友於是利用這個機制，真的去將這個網域註冊，讓全世界的WannaCry病毒都以為自己身處於「沙盒(Sandbox)測試環境。」
- ✓ 然而這個解決方案只是暫時性的，網路上已陸續發現2.0的病毒變種用來更新這漏洞，所以病毒都更新了，我們也必須盡快將作業系統更新至最新版本，這才是目前最安全的做法。

補充資訊

補充資訊-關於微軟安全性套件

- 在WannaCry事件爆發後，微軟也緊急在5月13日提供作業系統的安全性更新檔，如圖片所示:

微軟安全性套件(防堵WannaCry攻擊)	
Windows XP	KB4012598
Windows Vista SP2	KB4012598
Windows 7 SP1	KB4012212、KB4012215
Windows 8	KB4012598
Windows 8.1	KB4012213、KB4012216
Windows RT 8.1	KB4012216
Windows 10	KB4012606
Windows 10 1511版	KB4013198
Windows 10 1607版	KB4013429
Windows Server 2003	KB4012598
Windows Server 2008 SP2	KB4012598
Windows Server 2008 R2 SP1	KB4012212、KB4012215
Windows Server 2012	KB4012214、KB4012217
Windows Server 2012 R2	KB4012213、KB4012216
Windows Server 2016	KB4013429

補充資訊-ASOC防護方式

- 在入侵預防系統-SourceFire (Intrusion Prevention System)啟用規則(Rule ID:41978,41984,42329到42332,42340)即可即時防護
- ASOC內的所有電腦即時更新最新版的系統更新檔、防毒軟體
- 關掉SMBv1服務及關閉445連接埠(port 445)

資料來源

資料來源

- 簡介:
  1. https://zh.wikipedia.org/wiki/WannaCry (維基百科-WannaCry)
- 技術:
  1. http://www.freebuf.com/articles/system/134578.html
  2. https://blog.trendmicro.com.tw/?p=49656
- 受災情況:
  1. http://www.appledaily.com.tw/realtimenews/article/new/20170515/1118638/
  2. https://unwire.hk/2017/05/21/wannacry-victim-statistics/tech-secure/

資料來源

- 案例:

1.新聞來源: http://www.ettoday.net/news/20170514/924318.htm (東森新聞雲)

2.新聞來源: http://www.appledaily.com.tw/realtimenews/article/international/20170515/1118738/(蘋果日報)

3.圖片來源: https://www.bnext.com.tw/article/44481/ransomware-virus-attacks-across-the-globe-fear-of-loss-imponderable (數位時代)

- 暫時性解決方案:

1.https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

- 補充資訊:

1. http://www.ithome.com.tw/news/114154