區網網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

主管機關政策討論

資通安全管理法草案

資通安全管理法

法案里程碑

日期	重要內容
105年8月1日	行政院資安處成立，成為政院資安專責機構
105年8月31日	資安處完成資安管理法草案
105年10月中旬	資安管理法提報行政院，**公布行政院版**
105年11月下旬	政院37條**優先法案中，排名第24名**
105年12月1日	台灣駭客年會(HITCON)**蔡英文總統致詞**
105年12月底	科技政委吳政忠要求，**年底前完成**資安管理法立法
106年3月16日	國安會將協助於立法院**第三會期完成立法**

資通安全管理法(續)

法案結構 5個章節，計24條

資通安全管理法草案

第1章 總則(§1~§8)	立法目的、名詞定義、資通安全產業之推動、行政院職責、幕僚任務委任或委託、資安責任等級分級、情資分享機制、資通委外監督
第2章 公務機關資通安全管理(§9~§14)	資通安全管理與維護計畫、資通安全長之設置、年度資通安全報告之提出、資通安全查核、通報應變措施、獎懲措施
第3章 非公務機關資通安全管理(§15~§18)	關鍵基礎設施提供者資通安全維護之管理與監督、受指定之非公務機關所提供之產品或服務資通安全管理之管理與監督、資通安全事件通報應變、行政檢查
第4章 罰則(§19~§22)	行政處分
第5章 附則(§23~§24)	施行細則授權、施行日期

出處:資安處,北區ASOC整理

資通安全管理法(續)

法條編號	重點摘要	北區ASOC協助事項
第九條	公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，**訂定、修正及實施資通安全維護計畫**。	**資通安全維護計畫：** 協助下轄區網中心諮詢資通安全維護計畫資安技術部分。
第十一條	公務機關應於年度終了後，向上級或監督機關**提出資通安全維護計畫之實施情形。**	**資通安全維護計畫：** 協助下轄區網中心諮詢資通安全維護計畫資安技術部分。
第十二條	公務機關應查核其所屬或監督公務機關之資通安全維護計畫實施情形。 受**查核機關之資通安全維護計畫實施有缺失或待改善者，應提出矯正計畫，送交上級或監督機關。**	**資通安全維護計畫矯正：** 協助下轄區網中心，當受上級或監督機關查核資通安全維護計畫，需撰寫矯正計畫之資安技術部分諮詢。

出處:北區ASOC整理

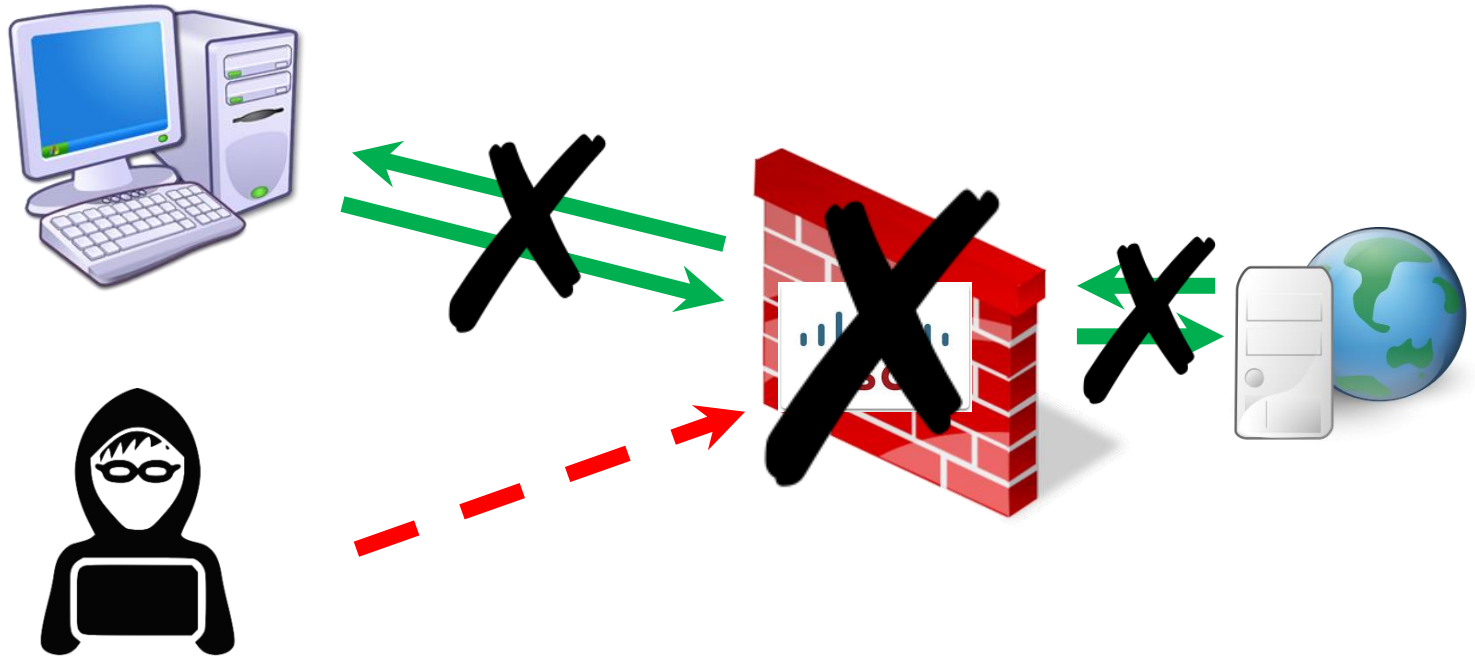
資通安全管理法(續)

法條編號	重點摘要	北區ASOC協助事項
第十三條	公務機關為因應資通安全事件，應訂定通報及應變機制。 公務機關**發生資通安全事件時，除應通報上級或監督機關外，並應通報行政院；**無上級機關者，應通報行政院。 公務機關應向上級或監督機關**提出資通安全事件調查、處理及改善報告，並送交行政院**；無上級機關者，應送交行政院。	1.通報機制 教育部已建立資安事件通報機制，103年與104年度北區ASOC分別通報 10,928與12,590 件第一二級事件 2.資通安全事件調查、處理及改善報告協助下轄區網中心諮詢資通安全事件調查處理及改善之 資安技術。
第十四條	**公務機關所屬人員未遵守本法相關資通安全義務**，致國家或社會受有重大損害時，除依法追訴行為人相關法律責任外，並應**追究行為人、其服務機關資通安全長及相關人員之行政責任。**	

出處:北區ASOC整理

資安案例分享

BlackNurse Attack



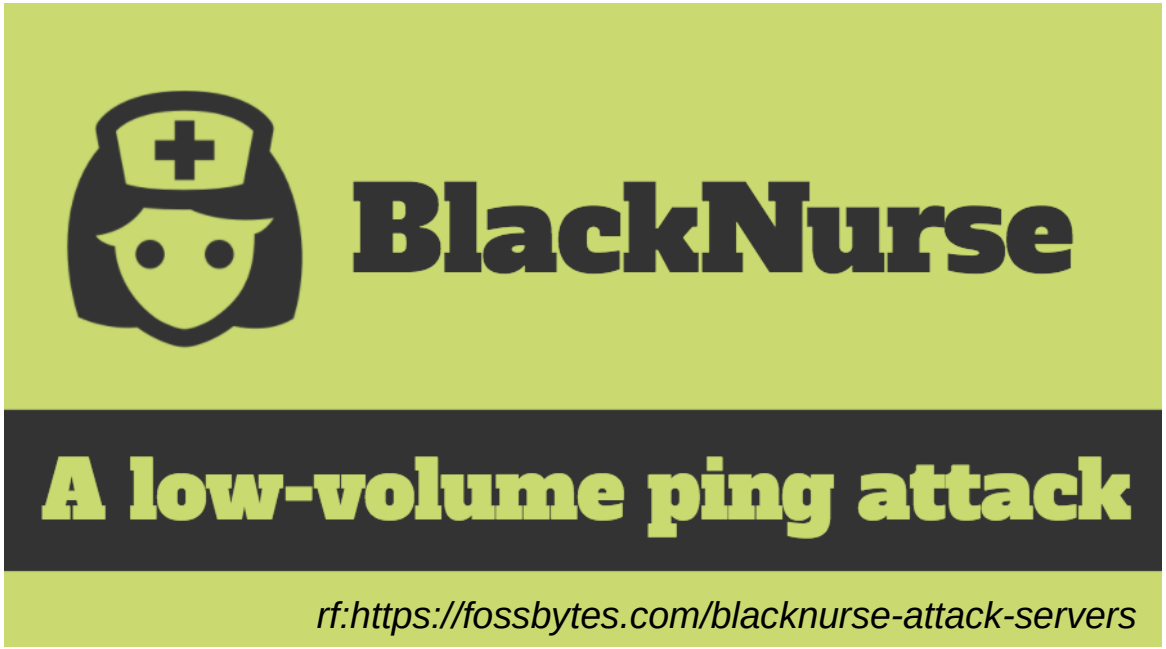
TDC-SOC近期發現了一種新型的ICMP Attack，並名為「BlackNurse」。與以往的ICMP Flooding Attack（Ping of Death）或DDoS攻擊模式不同，BlackNurse僅需要發送少量的（小於20Mbit/sec）Destination Unreachable封包訊息，便可耗盡某些特定設備防火牆的CPU資源，達成DoS（Denial of Service）的目的。

BlackNurse Attack

Devices verified by TDC to be vulnerable to the BlackNurse attack

- Cisco ASA 5506, 5515, 5525 (default settings)
- Cisco ASA 5550 and 5515-X (latest generation)
- Cisco Router 897 (unless rate-limited)
- Palo Alto (unverified)
- SonicWall (if misconfigured)
- Zyxel NWA3560-N (wireless attack from LAN Side)
- Zyxel Zywall USG50

BlackNurse Attack



rf:https://fossbytes.com/blacknurse-attack-servers

防禦方式：

1. 於防火牆設備關閉接收ICMP類型的封包訊息（不適用於某些特定Cisco設備）。
2. 於上游設備關閉接受ICMP類型的封包訊息。
3. 升級設備CPU效能。
4. 更換防火牆設備。

勒索加密病毒新型態攻擊-透過Facebook散佈感染

勒索軟體Locky-簡介

近期勒索軟體Locky出現新型態的散佈感染方式，透過竊取得來的Facebook帳號，以私訊方式隨機向好友發送偽造的圖片檔，誘使使用者下載並安裝瀏覽器外掛程式，伺機植入勒索軟體Locky。

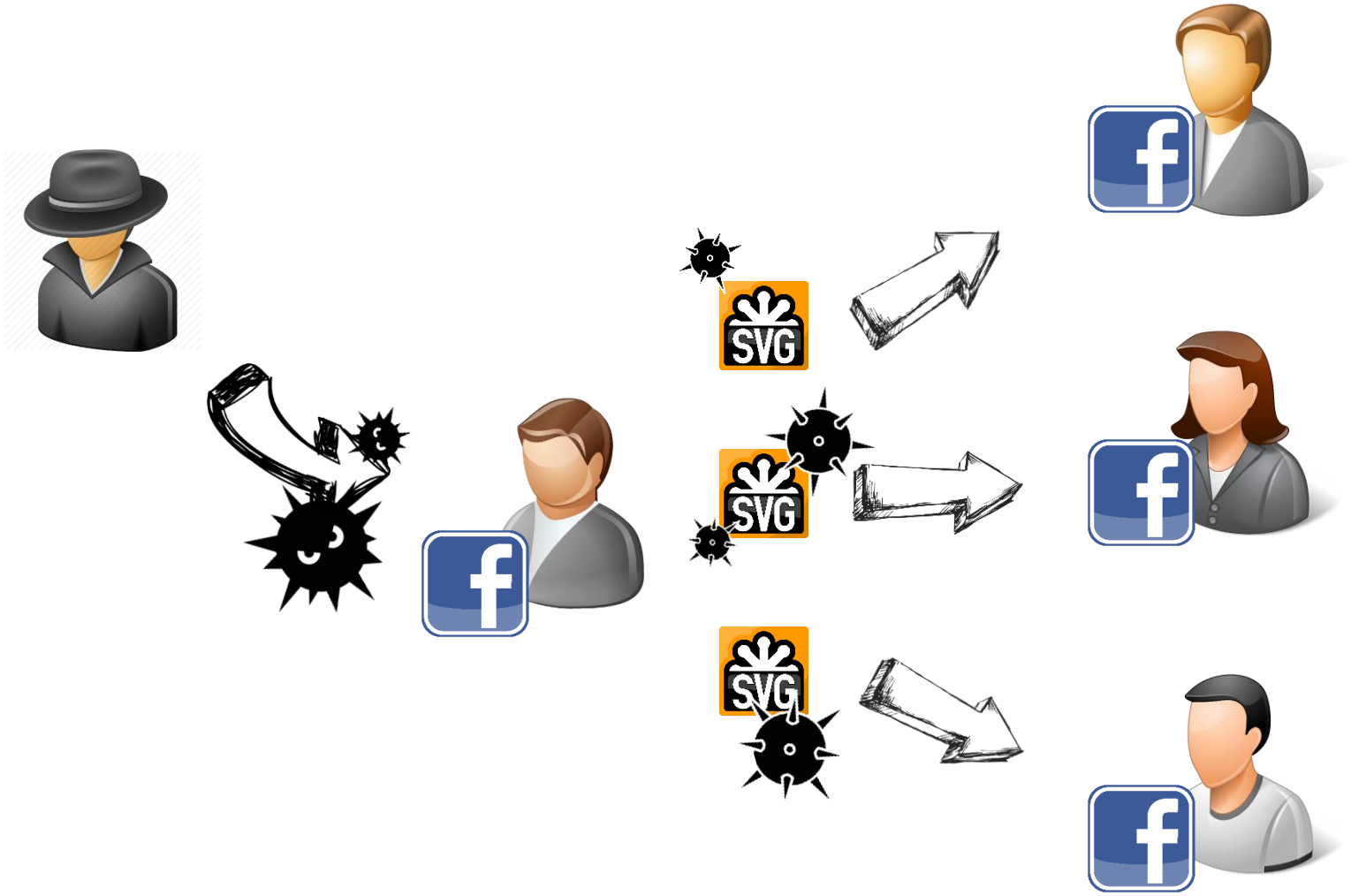
由於是透過Facebook好友名單來發送訊息，受害者容易降低警覺心，並在不知情的情況下受到感染。

出處:北區ASOC整理

勒索加密病毒新型態攻擊-

透過Facebook散佈感染

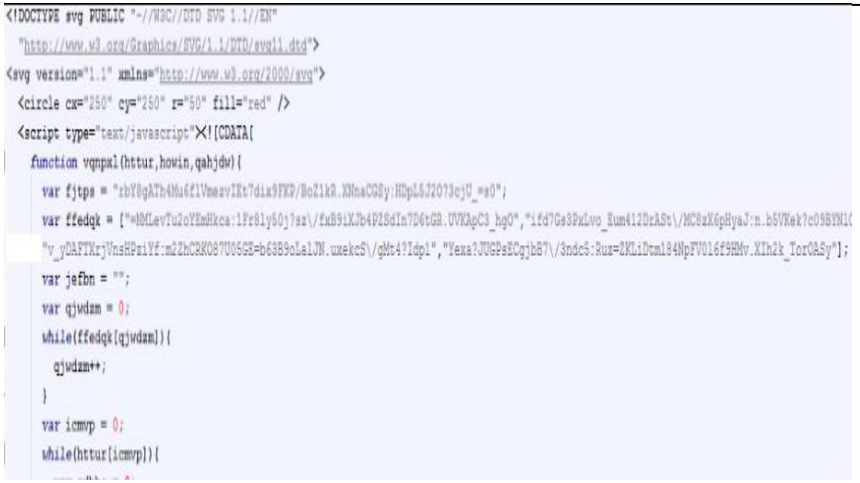
勒索軟體Locky-攻擊流程



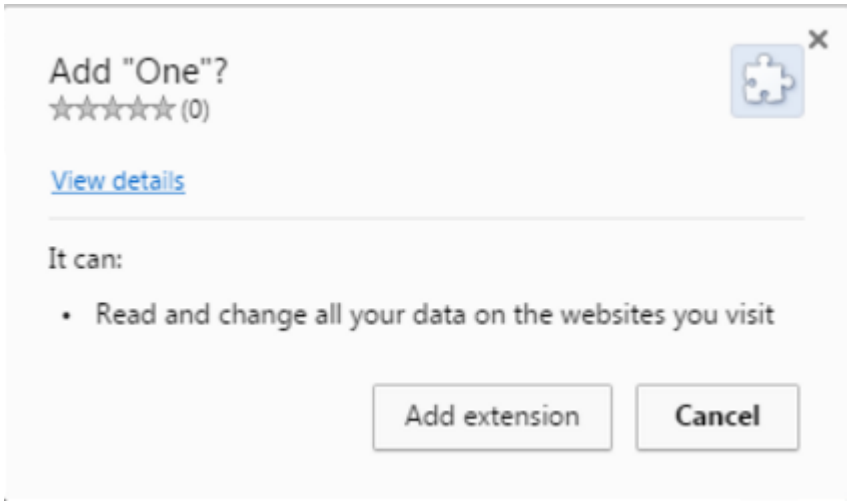
出處:北區ASOC整理

勒索加密病毒新型態攻擊-透過Facebook散佈感染

勒索軟體Locky-攻擊特色



1.)透過SVG圖片可以內嵌Javascript程式碼的方式，來規避臉書訊息傳遞的安全規則，檢視攻擊者所傳送的圖片檔，可以發現內含轉導至惡意網站的程式碼。



2.)惡意程式偽裝成瀏覽器的擴充程式，並提示使用者若不安裝擴充程式，就看不到影片內容，若使用者未察覺朋友帳戶已遭入侵，則被入侵感染機率相當高。

出處:北區ASOC整理

印表機自動列印勒索文件
事件說明

- **揭露**
  - 02/06 iThome報導白帽駭客揭露網路印表機風險，並提出示警
- **受害**
  - 02/13 開始陸續接獲本校系所與單位反應印表機列印出勒索訊息
- **預警**
  - 提供網路印表機防護建議措施供網管與全校使用者參考處理
  - 預防3月1日可能發生之網路攻擊，啟動DDoS偵測與清洗機制，資安團隊與網路維運團隊至計中待命

印表機自動列印勒索文件事件說明(續)

- **檢測**
  - 分析受害網路印表機網路流向紀錄
  - 掃描受害網路印表機開啟通訊埠(port)
  - 掃描台大區網實體IP開啟通訊埠 9100

印表機自動列印勒索文件攻擊手法分析

透過port 9100
傳送勒索文件

受害印表機
xxx.xxx.xxx.xxx:9100

印出

My name is Emerson Rodrigues

Your network will be destroyed starting 03/01/2017 if you don't pay protection fee - 3 Bitcoins @ 15t4Ay5w8byURMZHMPKRexi7NxLMuvbtEv

If you don't pay by 02/20/2017, my virus will start to destroy your files and the price to stop will increase to 5 BTC and will go up 10 BTC for every day of attack.

This is not a joke.

If you do not pay, the virus will destroy all your files. Its propagating in your network right now while you re Reading this print job.

Prevent it all with just 3 BTC @ 15t4Ay5w8byURMZHMPKRexi7NxLMuvbtEv

Contact ElliotRodger@Openmailbox.org for instructions.

Bitcoin is anonymous, nobody will ever know you cooperated.

勒索文件

印表機自動列印勒索文件

勒索訊息樣本

My name is Emerson Rodrigues

Your network will be destroyed starting 03/01/2017 if you don't pay protection fee - 3 Bitcoins @ 15t4Ay5w8byURMZHMPKRexi7NxLMuvbtEv

If you don't pay by 02/20/2017, my virus will start to destroy your files and the price to stop will increase to 5 BTC and will go up 10 BTC for every day of attack.

This is not a joke.

If you do not pay, the virus will destroy all your files. Its propagating in your network right now while you re Reading this print job.

Prevent it all with just 3 BTC @ 15t4Ay5w8byURMZHMPKRexi7NxLMuvbtEv

Contact ElliotRodger@Openmailbox.org for instructions.

Bitcoin is anonymous, nobody will ever know you cooperated.

印表機自動列印勒索文件處理建議措施

- 不使用實體IP位址(如140.112.x.x)改用虛擬IP位址(如10.1.x.x)。如無法避免使用實體IP位址，建議設備前端需有防火牆控管，管制外部IP連線或掃描，阻擋外部存取 9100通訊埠
- 如印表機可設定WEB介面開啟ACL ，限制可存取之IP位址
- 設定網路印表機之強健密碼，以避免駭客取得管理權限遠端安裝攻擊程式，導致印表機成為對外攻擊成員之一
- 關閉印表機韌體與遠端更新服務RFU (remote firmware update)

Q & A