以加密勒索軟體為例，拆解網路攻擊鏈—

最佳化端點、電郵與網頁防護實務

保安資訊有限公司 馬進林 經理

www.SaveTime.com.tw 好記:幫您節省時間.的公司.在台灣

We Keep IT Safe，Secure & Save you Time，Cost

加密勒索事件:美國好萊塢長老教會醫療中心
2016/02/17(Hollywood Presbyterian Medical Center)

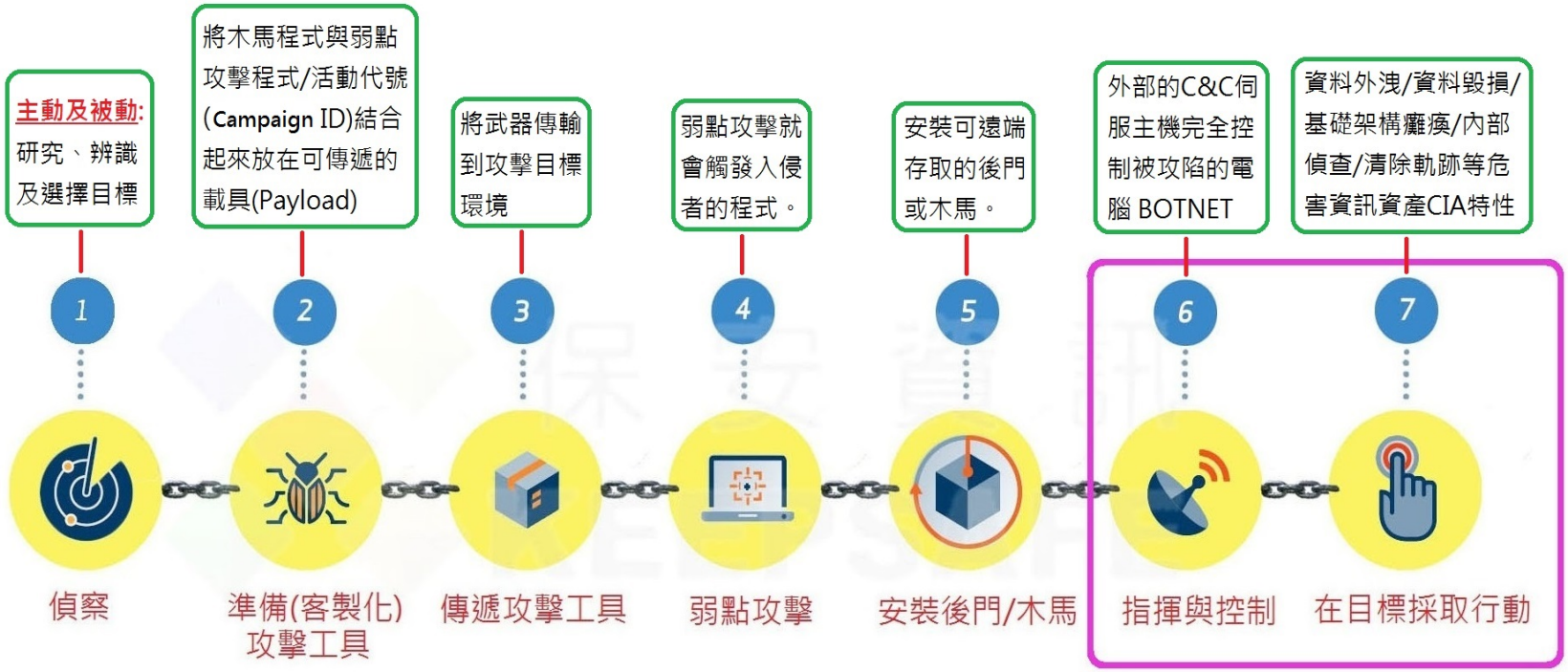
保安資訊
SAVETIME
INFORMATION SECURITY

除支付40元彼特幣($17000)外，病患權益嚴重受損

“知己知彼，百戰百勝”-拆解網路攻擊模式:以洛克希德馬丁公司的網路攻擊鏈(Cyber Kill Chain)框架

保安資訊 SAVETIME INFORMATION SECURITY

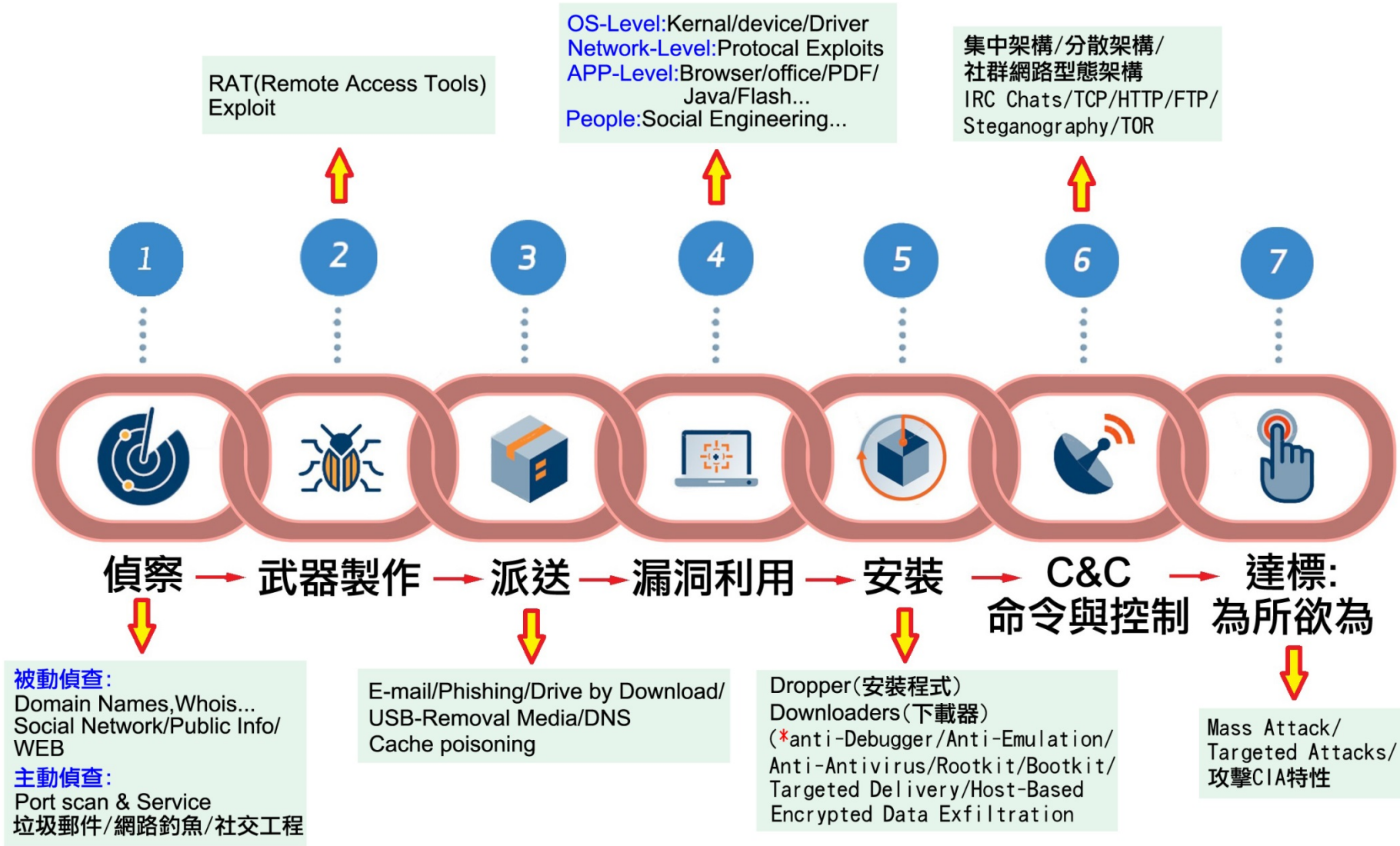
時間軸 | 數小時/數個月 | 數秒鐘 | 數個月至數年



準備階段 | 入侵階段 | 控制及採取行動階段

對應網路攻擊鏈(Cyber Kill Chain)框架-攻擊者常用的攻擊技術(Technical Aspects)

保安資訊 SAVETIME INFORMATION SECURITY



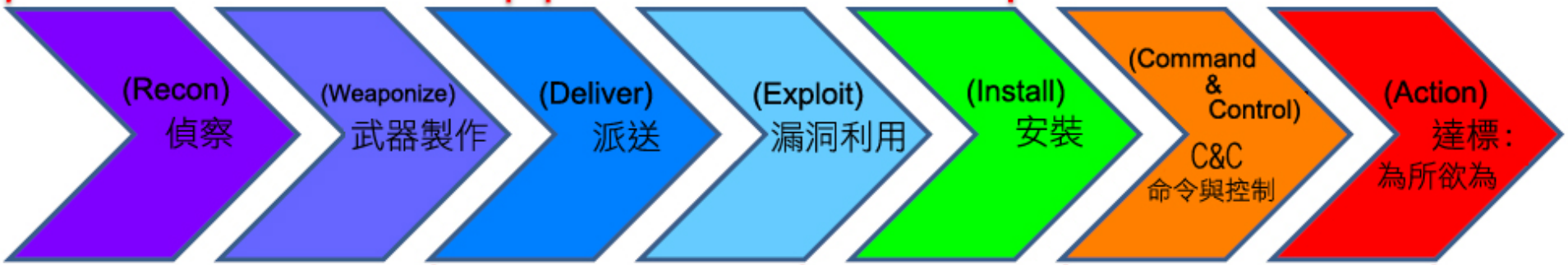
美第二大連鎖商店Target 客戶資料外洩總數可能達1.1億筆，成美國史上最大資料外洩案！(2013/12)

美第二大連鎖商店Target 客戶資料外洩總數可能達1.1億筆，成美國史上最大資料外洩案！(2013/12)

保安資訊 SAVETIME INFORMATION SECURITY

攻擊者利用Target供應鏈廠商的資安漏洞/弱點，進入內部網路並取得灘頭堡(根據地)

攻擊者利用Target對內部網路不嚴謹的管控，從容地進出存放最重要機敏資料的網路

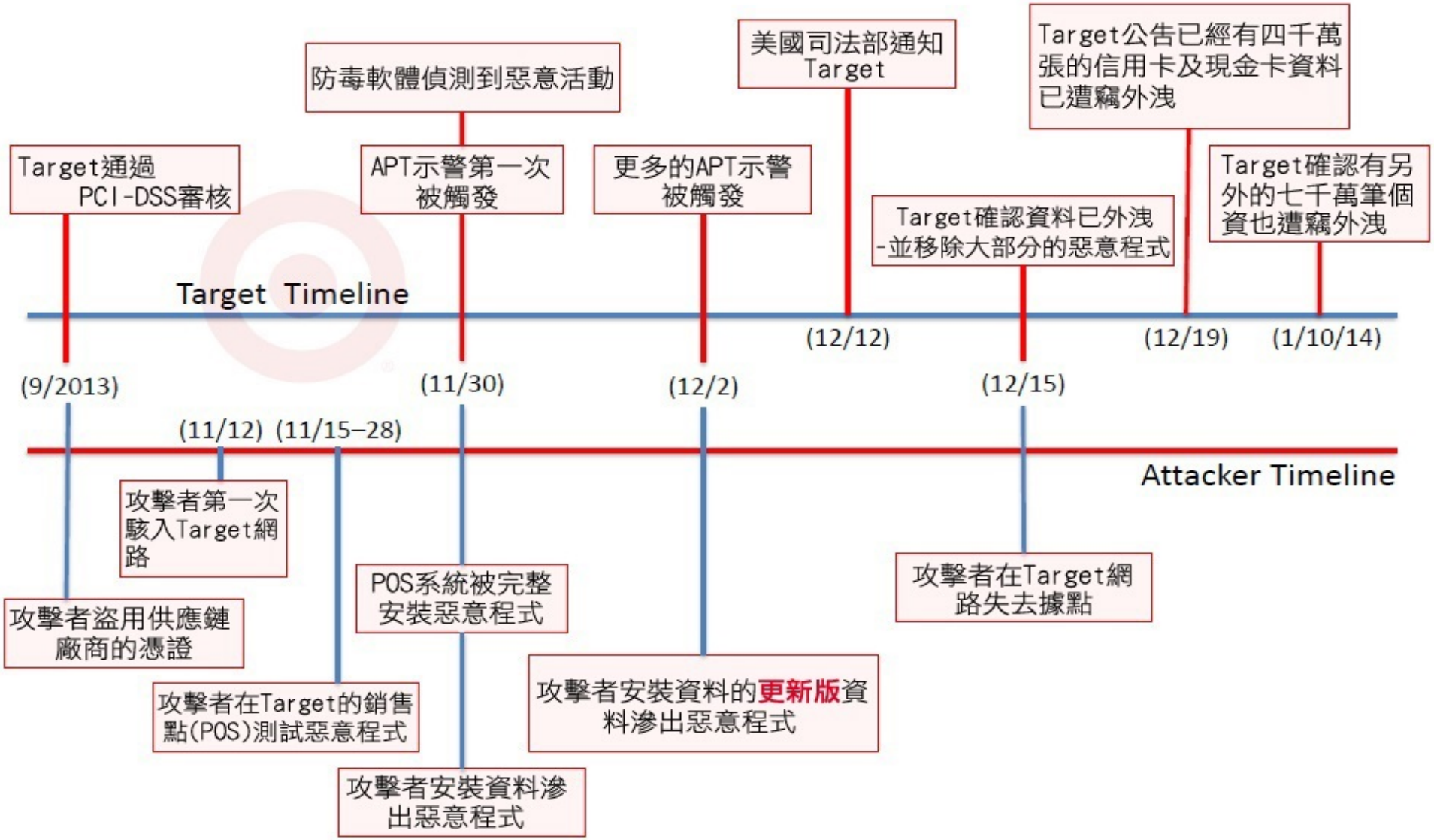


Target錯失來自防毒系統及ATP系統的示警通報，以至於攻擊者可以順利安裝惡意程式

Target錯失來自於入侵防護系統提供的資料外洩資訊，讓駭客得以順利偷竊包含信用卡、現金卡以及個資等高達1. 1億筆客戶資料

美第二大連鎖商店Target 客戶資料外洩總數可能達1.1億筆，成美國史上最大資料外洩案！(2013/12)

保安資訊 SAVETIME INFORMATION SECURITY

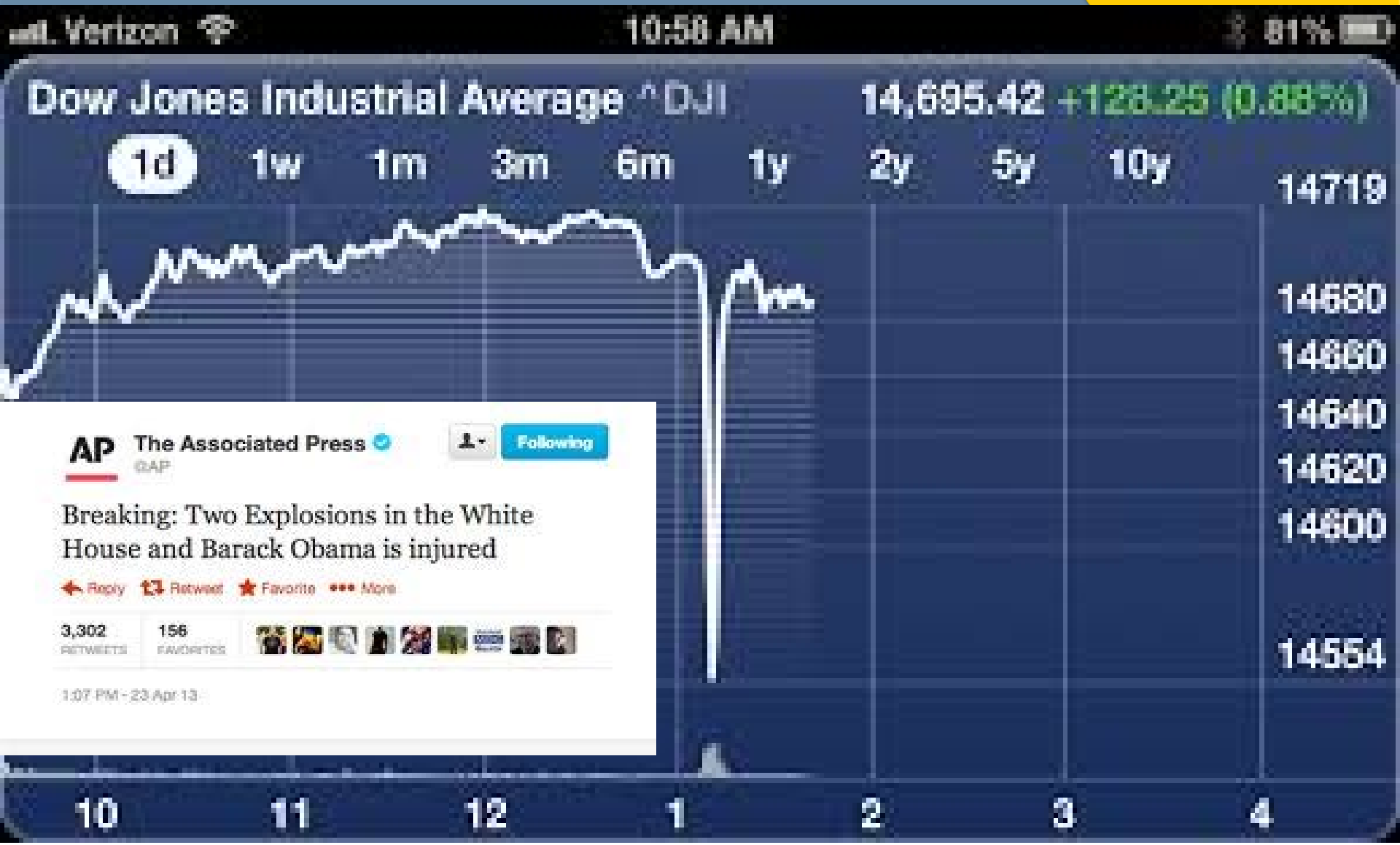


沙烏地阿拉伯國家石油公司-國家級駭客只利用USB發動的Shamoon/Disttrack 攻擊:超過30K台電腦癱瘓

保安資訊 SAVETIME INFORMATION SECURITY

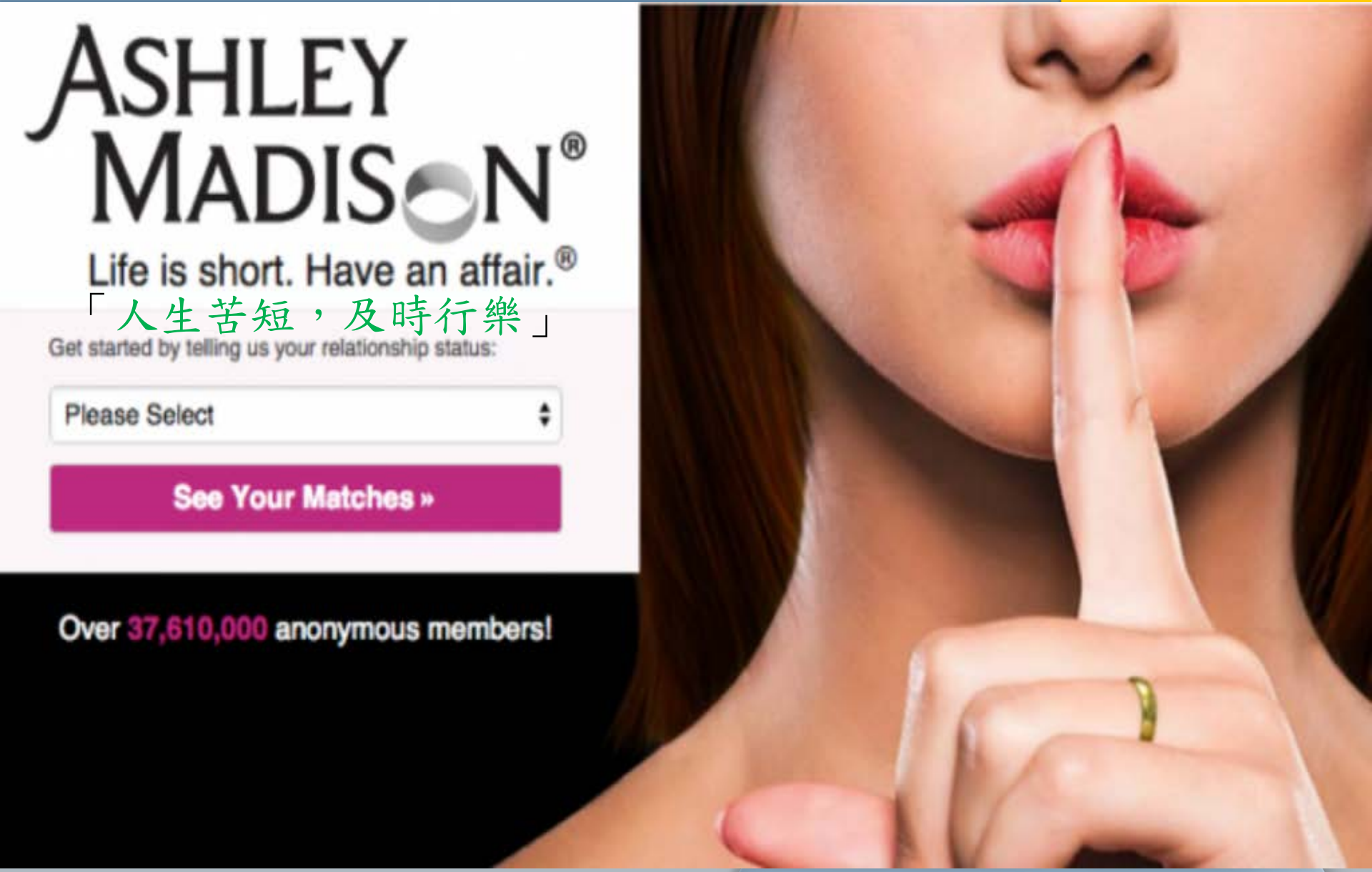
美聯社Twitter帳號被駭，假傳白宮遭炸彈攻擊新聞，宣稱白宮發生兩起爆炸案，且總統歐巴馬受傷，使得DJI指數重挫...

保安資訊 SAVETIME INFORMATION SECURITY



最大偷情網Ashley Madison遭駭-3700萬會的個資、裸照、信用卡等資料，日前已遭駭客全數公布

保安資訊 SAVETIME INFORMATION SECURITY



莫非定律？會發生的事終究會發生!

保安資訊 SAVETIME INFORMATION SECURITY

“There are only two types of companies in the world: The ones that have been hacked, and those that will be.”

“世界上只有兩種公司，一種是已經被駭的公司，另外一種是即將被駭的公司”

- FBI Director Robert Mueller

數位勒索集團所使用的伎倆/技術，以及流程

比較厲害?網路攻擊，運作原理與機制大同小異

防護原則:讓漏洞無法接觸到資產，讓威脅無法接觸到漏洞

保安資訊 SAVETIME INFORMATION SECURITY

- 利用Office 檔案的巨集功能-①**Locky**，後來的變種是假裝成ZIp檔，然後藉由JavaScript 觸發 (②Ransom32 也是)。
- 利用自動化的網頁攻擊套件(Exploit Kit)-利用順道下載(drive by download)/水坑式攻擊(Water Hole)-③TeslaCrypt /④ CryptoWall 4.0 --->Angler Exploit Kit/Radamant ---> Rig Exploit Kit。利用瀏覽器漏洞及外掛程式的漏:Flash/JavaScript/Acrobat (Reader)。
- 漏洞的P2P軟體:最早被發現的Linux-⑤Linux.Encoder.1 /Macintosh-⑥KeRanger 經由使用有漏洞的BitTorrent感染的。
- 利用網路分享的弱點(SMB Share):TorrentLocker 以及 CryptoFortress，**Locky** 甚至無需對應網路磁碟也能加密。
- ⑦Petya-整個硬碟加密，經由Dropbox下載惡意的履歷檔。

何以加密勒索-躍升為資安威脅的主流?

保安資訊 SAVETIME INFORMATION SECURITY

- **廣告是網際網路的原罪，我們已經習慣用自己換取免費。駭客很容易就從單一資料來源獲得大量的財務及個人資訊。**
- **縮減**了CKC的步驟-更快獲益，取代APT/Mega Breach 光環。
- **供需問題**:資料仲介市場上的信用卡、帳號與密碼、個資等..貨源充足，價格已低，並且是買方市場。
- 偷竊的信用卡，個資還要經過地下通路販售，無法掌握預期的收入。
- 無須**錢騾(Money Mule)**-加密勒索透過彼特幣交付贖款，既安全又無需錢騾-目前全球非法洗錢最缺錢騾，不缺信用卡資料。
- 企業重兵佈署APT/DLP方案，增加犯案的風險與成本。
- **狼來了**效應:防護系統的logs 多，誤報也多，IT往往忽略防護系統的示警。而把重點擺在如何防止資料外洩(CK6 & CK7)。

單單一隻CryptoWall加密勒索病毒至少有100億新台幣的地下經濟產值

保安資訊 SAVETIME INFORMATION SECURITY

Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?

Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

I almost understood but what do I have to do?

The first thing you should do is to read the instructions to the end.

Your files have been encrypted with the CryptoWall software, the instructions that you find in folders with encrypted files are not viruses, they are your helpers.
After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions.
Think logically - we are the ones who closed the lock on your files and we are the only ones who have this mysterious key to open them.
Any of your attempts to restore your files with the third-party tools can be fatal for encrypted files.
e encrypted file (as 100% of software to restore files do this, except the special decryption software) you break damage to the file and it will be impossible to decrypt the file.
: when some mosaics items were lost, broken or not put in its place - the picture will not emerge, the software to restore the files will not be able to lay down the picture, and ruin it completely and irreversibly.
Using the software to restore files can ruin your files forever, only through your fault.
rvention of the extraneous software to restore files encrypted with the Cryptowall software may be the point of no return.

---

ese simple rules are violated we will not able to help you, and we will not try because you have been warned.
tention the software to decrypt the files (as well as the private key that come fitted with it) is a paid product.

After purchasing the software package you can:

1. Decrypt all your files.
2. Work with your documents.
3. View your photos and other media content.
4. Continue your habitual and comfortable work at the computer.

If you are aware whole importance and criticality of the situation, then we suggest you go directly to your personal page where you will be given final instructions, as well as guarantees to restore your files.

對應網路攻擊鏈(Cyber Kill Chain)框架-產業標準的建議防護

保安資訊 SAVETIME INFORMATION SECURITY

Phase	Detect (偵測)	Deny (避免)	Disrupt (阻止)	Degrade (降級)	Deceive (誘騙)	Contain (災情控管)
Reconnaissance (偵查)	Web Analytics	Firewall ACL				Firewall ACL
Weaponization (武器化)	NDIS	NIPS				
Delivery (傳遞)	Vigilant user(Security Awareness)	Proxy Filter	Inline AV	Queuing		APP-Aware Firewall
Exploitation (漏洞利用)	HIDS	Patch	DEP			Inter-Zone NIPS
Installation (安裝)	HIDS	'Chroot' Jail	AV			EPP
Command and Control (命令與控制)	NDIS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust zones
Action on Targets(達標)	Audit Logs	Outbound ACL	DLP	Quality of service	Honeypot	Trust zones

對應網路攻擊鏈(Cyber Kill Chain)框架-Symantec 提供業界最完善的防護保護方案

保安資訊 SAVETIME INFORMATION SECURITY

Phase	Detect(偵測)	Deny(避免) or Contain(災情限制/控制)	Disrupt(阻止)、Eradicate(根除) or Deceive(誘騙)	Recover(恢復)
Reconnaissance (偵查)	DeepSight Threat Intelligence、MSS(Managed Security Services) 、CSS(Control Compliance Suite)、SMG(*DHA Protect)	CSS, DCS(Data center Security)	N/A	N/A
Weaponization (武器化)	DeepSight™ Adversary Intelligence	CSS、Altiris ITMS (Symantec™ IT Management Suite)	SMG(Decoy Account)、Symantec.Security.cloud(email/web)	N/A
Delivery (傳遞)	MSS、DeepSight™ Intelligence 、$Blackfin(user training,phishing tests)	ATP、Deepsight Threat Intellgence	SEP(*AV(Sonar/Insight)/*HIPS)	SEP(*Power Eraser)、Veritas
Exploitation (漏洞利用)	SEP(*HIPS/*HI)、DCS、MSS	SEP(*FW)、DCS、ATP、DeepSight™ Intelligence	SEP(AV)、ATP、DCS	Veritas
Installation (安裝)	SEP、ATP、DCS	SEP、Moblity Suite、Authentication Manager、VIP,Managed PKI	SEP(*AV/*HIPS/*HI)、ATP(Sandbox & Correlation)、DCS(Sandbox/完全白名單/帳戶權限限縮)	Incident Response Retainer Services
Command and Control (命令與控制)	SWG、ATP、MSS、DeepSight™ Intelligence 、$BlueCoat	DeepSight™ Intelligence、DLP、ATP	DeepSight™ Intelligence	Incident Response Retainer Services
Action on Targets(達標)	MSS、DLP、DeepSight™ Intelligence	DLP (Symantec Data Loss Prevention)	DLP、ATP	Incident Response Retainer Services

心得分享

保安資訊 SAVETIME INFORMATION SECURITY

- 網路安全是人的問題，而不只是科技的問題。
- 如果你以為科技可以解決安全問題，那你就是不明白問題，也不明白科技~Bruce Schneier。
- 安全性與方便性永遠有互斥性。
- 就資安而言，隨身碟不是什麼好東西-史諾登事件、Stuxnet、沙特阿美都是經由隨身碟的星星之火燎原的。
- Patch!Patch!Patch!
- Backup 321。
- 應用程式白名單政策。
- 限制管理員權限。
- ….

面對加密勒索軟體-如何保安?

保安資訊 SAVETIME INFORMATION SECURITY

NEXT

最佳化端點、電郵與網頁防護實務