北美資訊安全現況之簡析

110.09.09

駐舊金山經濟組撰擬

前言：

近年來，網路攻擊在全球日益猖獗，越加頻繁的網路攻擊與資料外洩，造成的影響越來越嚴重，其中最常見的就是使用「勒索軟體」(Ransomware)，駭客使用惡意病毒將系統加密，而受害者必須繳納贖金以取回電腦的控制權。華爾街日報 2021 年 6 月報導顯示[1]，近年來全美相關案件每年已超過 2,000 起，且損失金額於 2020 年明顯增加，達三千萬美元(詳圖 1)。同時，各行各業無一倖免，網路駭客攻擊事件已遍佈食品業、交通業以及醫療產業，如 2021 年燃油管線營運業者「殖民管線公司」（Colonial Pipeline）以及肉品加工業者 JBS 紛遭遇網路攻擊，本報告將先說明近期駭客攻擊日益嚴重之原因，再進一步針對依產業及北美地區之駭客攻擊進行分析。

圖 1：近年駭客攻擊案件及損失統計圖

一、駭客攻擊日益增加之主因：

上述報導並針對駭客攻擊案件持續成長進行分析，並歸納 4 類原因如下：

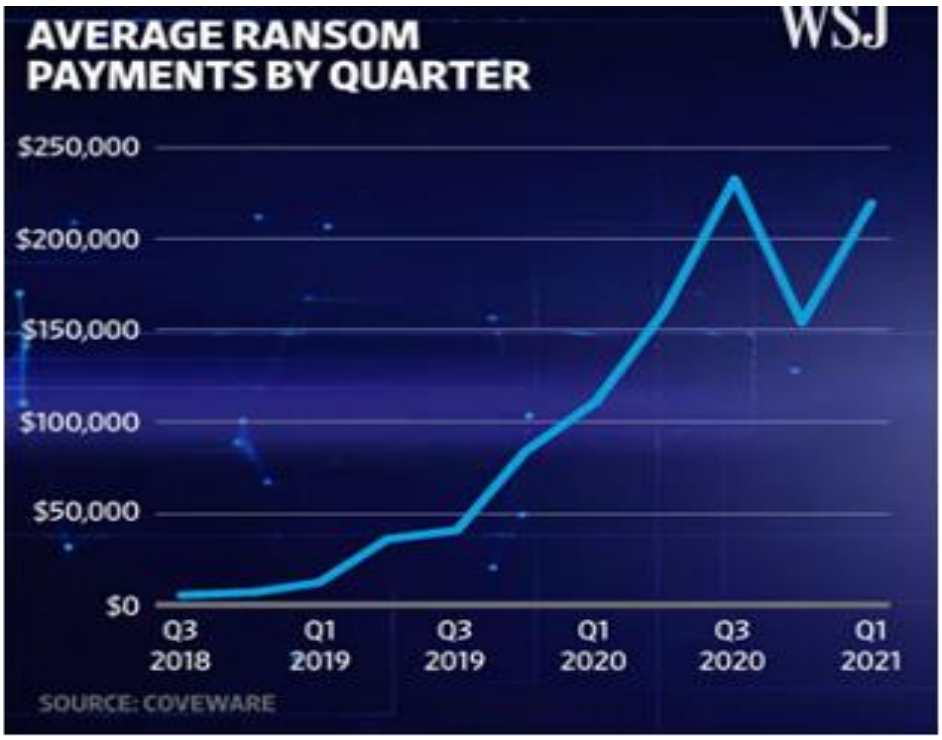
(一) 受害者自身之疏失：主要為電腦使用者不定期更新軟體，導致軟體資安防護機制無法即時更新，並因疏忽而點擊詐騙型電子郵件之「釣魚連結」(phishing link)，使駭客獲得用戶密碼等個資，美電信業者 Verizon 並於 2021 年矽谷網路安全高峰會(Cyber Security

[1] https://www.wsj.com/video/why-ransomware-attacks-are-on-the-rise-and-how-the-us-can-fight-them/8B1F50DA-FB21-4186-8E33-398A639EEC23.html?mod

Summit Silicon Valley 2021)表示，目前 85%的資料外洩案件都涉及使用者操作不當，而過去一年因疫情居家工作盛行，在無企業網路安全部門監管下，釣魚式攻擊的成功率大增，使得資料外洩案件數亦同步成長，如 2021 年對美國燃油管線營運業者 Colonial Pipeline 的攻擊就屬於這一類。

(二) 駭客攻擊的利潤成長：近年來駭客透過勒索軟體攻擊所獲得之利潤有明顯成長（詳圖 2），在高額利潤誘使下，助長犯罪案件成長。如 2021 年 JBS 肉品加工公司因駭客攻擊事件賠了 1,100 萬美元，而 Colonial Pipeline 則賠了 440 萬美元。

圖 2：近年駭客攻擊所獲贖金統計圖



(三) 駭客攻擊團隊化：駭客可以與其他駭客小組合作，針對犯罪過程進行分工，提升整體攻擊能力，造成犯罪案件層出不窮。

(四) 俄羅斯因素：調查專家指出，很多駭客攻擊來自俄羅斯與東歐國家。且目前這些國家對資訊安全的法規尚未成熟，未能有效遏止相關犯罪，形成發動駭客攻擊的溫床。

此外，該報導也建議個人或企業使用者應使用雙重認證，增加駭客竊取資料之難度，並注意使用電腦過程中的不尋常的現象(unusual activity)，降低遭駭之風險。

二、 北美之資訊安全研析：

美國電信商 Verizon 於 2021 年 6 月發布 2021 資料缺口調查報告(2021 Data Breach Investigations Report,下稱該報告)[2]，並分析北美等地區之駭客攻擊指出，相較全球其他地區，

[2] https://www.verizon.com/business/solutions/secure-your-business/business-security-tips/?cmp=knc:ggl:ac:ent:security:8003162844&utm_term=verizon%20data%20breach%20report&utm_medium=knc&utm_source=ggl&utm_campaign=security&utm_content=ac:ent:8003162844&utm_term=verizon%20data%20breach%20report&gclid=Cj0KCQjw4eaJBhDMARIsANhrQADQoVOXB26SvdevQbhtIFb8D1BSNMEDaQrzFXx8w2ikVK_

北美地區對資安相關法律修訂最為完善，尤其是醫療及公共行政等領域。背後原因為該區域面臨最為頻繁的攻擊事件，相較於 2020 年度亞太地區的 5,255 起案件，以及歐洲、中亞和非洲地區的 5,379 起案件，北美地區總共發生了 13,256 起案件，為有效抑制網路犯罪，有關當局因此逐步建立起完善之法律規範。

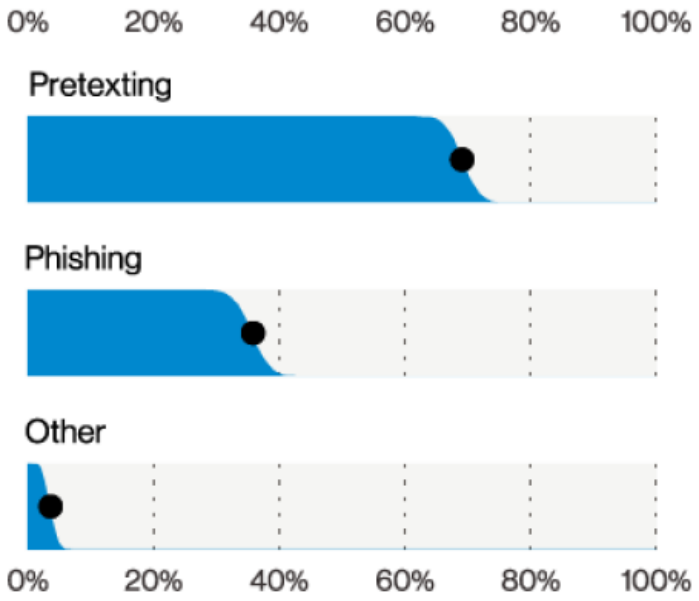
上述案件中，以社交軟體攻擊(Social Engineering)、侵入系統(System Intrusion)、簡易網站攻擊(Basic Web Application Attacks)等為最常見之攻擊類型(詳圖 3)。

圖 3：駭客攻擊案件類型統計圖

以社交軟體攻擊來說，駭客最常使用的手法為詐欺冒充法(Pretexting,近 70%)及釣魚法(Phishing,近 30%)。這兩者最大的差別為最終目的的不同。詐欺冒充法主要希望獲取金錢，而釣魚法主要是希望侵入系統以及竊取個人憑證與機密資料(詳圖 4)。

而透過釣魚法，駭客也可以進一步進行網路勒索(ransomware)，要求企業或個人繳納贖金以取回資料。駭客主要針對的資料以個人憑證占最大部分(58%)，緊接著為個人資料(34%)以及其他(27%)，公司內部資料(11%)。Maze Group 為第一個駭客成功攻擊的群體，而近期越來越多群組開始網路勒索活動。

圖 4：駭客攻擊手法類型統計圖



三、 各產業之分析：

Verizon 之報告並針對全球 29,207 起案件進行分析，發現每個產業面臨的駭客攻擊頻率也不相同，係因各個產業網路化及使用電子化之差距頗大，導致駭客攻擊的曝險程度也不相同。透過各個產業在 2020 年遇到的駭客攻擊統計表，可以觀察到娛樂產業是遭受最多駭客攻擊 (詳圖 5)。

圖 5：各產業受害客攻擊之分析表

Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

四、 美國公私部門近期對提升資訊安全之對策：

為有效因應日益嚴重之網路駭客攻擊案件，美國網路安全暨基礎設施安全局（CISA），於2021 年 8 月宣布，將與 Google、微軟、AWS 以及其他網路安全公司，推動網路國防聯合協同計畫[3]（Joint Cyber Defense Collaborative，JCDC），盼結合美國聯邦政府、各州地方政府、民間業者共同發展及推動該計畫，以強化美國網路安全。

目前參與該計畫的民間業者中，科技業包括 Amazon Web Service（AWS）、微軟及 Google Cloud，電信業計有 AT&T 及 Verizon，資安及網路設備業者則有 FireEye Mandiant、CrowdStrike 及 Palo Alto Networks。網路安全相關的政府機關則包括國防部、美國網路作戰司令部、國安局、聯邦調查局、司法部、國家情報總監辦公室（Office of the Director of National Intelligence）等單位。

另外美國總統拜登在同(8)月會見了私人企業與教育界的領袖，商討如何共同解決資安威脅，會後民間業者也作出承諾[4]，其中，Google[5]及微軟將在未來 5 年分別投入 100 億及 200 億美元的資金，來推動供應鏈、開源碼與架構的安全性；IBM 也將培育資安人才，預計未來 3 年內訓練出 15 萬名資安人才；蘋果則計畫建立一個新專案來改善該公司供應鏈的安全性，將與其供應鏈業者合作，大規模落實雙重認證、安全訓練、漏洞修復、事件紀錄及意外回應等，以共同提升美國資訊安全環境。

[3] https://www.cisa.gov/jcdc

[4] https://www.cnbc.com/2021/08/25/google-microsoft-plan-to-spend-billions-on-cybersecurity-after-meeting-with-biden.html

[5] https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-august-2021