公務機密宣導

社交工程──以「人性」發動攻擊的手法

案例分享

根據行政院111年7月份資通安全網路月報，駭客藉台灣疫情嚴峻時，利用**機關郵件伺服器寄送主旨為「傳染性肺炎疫情應變計畫」之社交工程郵件**，以提供疫情應變計畫為由，誘騙收件人開啟**惡意郵件附檔**，企圖針對特定機關人員發動電子郵件攻擊。

行政院國家資通安全會報技術服務中心已透過聯防監控月報，提供相關防護建議。

（資料來源：數位發展部資通安全署- 111年7月資通安全網路月報 https://moda.gov.tw/ACS/press/report/1938）

案例分析

社交工程（Social Engineering）是目前十分常見的駭客攻擊手法，係指駭客在網路上假冒熟人（例如：主管、好友、親人等）或其他任何角色（推銷員、網路商店等），以電子郵件、Facebook等聯絡管道，散佈詐騙訊息，誘騙個人開啟含有惡意程式的檔案或造訪惡意網頁，藉以將惡意程式植入受害人電腦，以獲取帳號、通行碼、身分證號碼或其他機敏資料。屬於最常見的社交攻擊手法之一，因成本最低、效果最好，這種針對資訊系統中最弱的一環——「人性」發動攻擊的手法，也成為駭客最愛利用的方式。

除了常見的**EXE檔**、**COM檔**及**BAT檔**等執行檔能夠藏病毒外，開啟**PDF檔**、**Word檔等文件檔案**或**點選超連結**也都可能遭到攻擊！

案例分析

110年亦發生多起駭客透過「**複製政府機關網站之公告訊息製成惡意郵件**」、「**以請求業務窗口協助作為釣魚信件主旨**」等手法，對特定機關發動之社交工程攻擊事件。

近年來社交工程詐騙方式詭譎多變，駭客大量**利用疫情相關消息**等內容製作詐騙與勒索郵件，並夾帶惡意郵件附檔誘騙使用者開啓並連線。

除了各機關須注意**定期進行郵件伺服器漏洞修補，定期變更密碼等防護措施**，以降低資料外洩風險外，**所有使用者也要更加謹慎提防所收到的信件是否為真**，勿輕易開啟不明郵件。

改善及策進作為

1. **定期執行病毒碼更新與資安監控**，以維護資安防護有效性。
2. **不開啟來路不明之郵件**，以免遭社交工程攻擊。必要時，可向信件上顯示的寄件人再次求證是否確實有寄出信件。
3. 若已點開可疑的電子郵件後，**切勿直接下載或開啟附加檔**，也**不隨意點擊郵件中夾帶的網址連結**。
4. **不安裝來路不明的軟體、不瀏覽不明網站**，遇可疑訊息或信件請先查證。

改善及策進作為

5. 如不慎開啟了惡意郵件的附加檔，務必**利用防毒軟體**掃除植入電腦的惡意程式。
6. 如與對方不相識且未曾聯繫，以電子郵件進行交流時，**請先行確認對方有寄出信件後再開啟**，並**避免將郵件帳號提供給無關人員**。
7. 提醒系統委外維護廠商強化及重視自身資安作為，並**嚴禁私設遠端維護機制**。

資料來源

1.數位發展部資通安全署- 111年7月資通安全網路月報https://moda.gov.tw/ACS/press/report/1938

2. iThome-110年國家資通安全報告出爐，APT攻擊與社交工程仍為資安重點項目
https://www.ithome.com.tw/pr/152453

3.清流月刊-中華民國106年5月號「資安木馬屠城記—論社交工程與APT駭客攻擊手法」https://www.mjib.gov.tw/FileUploads/eBooks/1c6ffab1dc9e4209be994652f934bab7/Section_file/8fed11b510d9465ea3e996e065f00dae.pdf

4.桃園市政府都市發展局政風室-「請注意防範社交工程攻擊」https://urdb.tycg.gov.tw/home.jsp?id=107&parentpath=0,2,103&mcustomize=onemessages_view.jsp&dataserno=201406130002&aplistdn=ou=data,ou=ethicsclass,ou=chdevelopment,ou=ap_root,o=tycg,c=tw&toolsflag=Y

花蓮縣政府政風處關心您！