資安月報三月號-
社交工程案例分享

康聯生醫
Healthconn

1. 前言
2. 社交工程案例一
3. 社交工程案例二
4. 近日國內重點資安新聞
5. 小測驗

康聯生醫 Healthconn

前言

還記得上期月報的社交工程及三不三要嗎?

透過趨勢科技的小漫畫和大家複習一下：

康聯生醫 Healthconn

前言 (續)


預防勒索軟體綁架電腦
三不三要
不上鉤:
標題特別吸引人的郵件
務必停看聽！
不打開:
不隨便打開email附件檔
不點擊:
不隨意點擊email
夾帶的網址
要備份:
重要資料要備份
要確認:
開啟電子郵件前
要確認寄件者身分
要更新:
病毒碼一定要隨時更新
加入FB 粉絲團
勒索軟體更多文章

社交工程案例一

TOYOTA 2度遭駭客入侵?

TOYOTA 2度遭駭客入侵?

《日經新聞》引用18世紀英國哲學家托馬斯．里德（Thomas Reid）的名言

「鍊條的強度，取決於其最薄弱的環節」（A chain is only as strong as its weakest link）來形容這次事件。

第一次發生在2022年 2 月底，豐田零件主要供應商「小島沖壓工業」遭到網路攻擊，為了停止損害擴大，小島切斷所有對外聯絡網，豐田零件供應系統被迫關閉，造成業務往來癱瘓，豐田最後緊急宣布，全日本所有工廠，包括子公司產線全數暫停，損失金額達到 3.75 億美元。

第二次發生在2022年 3 月份，豐田位於德國的關係企業電裝公司（DENSO CORPORATION）遭植入勒索軟體 Pandora，被竊取了 15 萬 7 千筆的機密資料。DENSO 是僅次於 Robert Bosch 的全球第二大汽車供應商，DENSO 德國據點遭入侵，是2022年針對豐田供應商的第二起網路攻擊事件。

分析師指出，當駭客鎖定整條供應鏈為攻擊對象，就不用等該組織曝露弱點，只需要在依存關係中找到一個潛在安全問題，就有辦法進行攻擊，進而對上百或上千個下游企業造成衝擊。

軟銀的IT子公司SB Technology首席安全研究員辻伸弘在接受日本《彭博》的訪問中表示，這些事件應記取的教訓是：即使一家企業本身的系統堅若磐石，由於許多供應商和關係企業大都仰賴外部的服務，譬如說雲端，所以必須精準掌握（供應商與關係企業）遭受網路攻擊或其他問題發生時，對自身會造成什麼影響。此外，**建立一個備份系統是不可或缺的**。

文字整理自: 天下雜誌、財訊

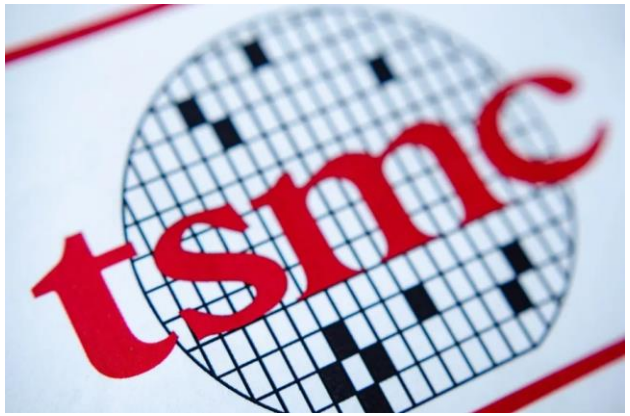
康聯生醫 Healthconn

社交工程案例二

台積電驚傳遭駭客勒索?

康聯生醫
Healthconn

台積電驚傳遭駭客勒索?



2023年6月惡名昭彰的LockBit勒索軟體組織(30日)傳出已鎖定晶圓代工龍頭台積電，竊得台積電資料並勒索7千萬美元。該組織並未明確說明已竊取那些數據與機密文件，但若台積電拒絕付款，其將公布相關資料。

台積電也立即回應指出，此為台積電IT硬體供應商遭受外部團體的網路攻擊，致使包含台積電名稱的資訊遭揭露。現已知悉某IT硬體供應商受到駭客侵害的事件，已知洩漏的資訊皆為該供應商協助的硬體初始設定資料，因所有進入台積電的硬體設備包括其安全設定，皆須在進廠後通過台積電完備程序進行做相對應調整，本次事件不會影響台積電的生產營運，亦無台積電客戶相關資訊的外洩。

事發後，台積電已按照標準作業程序處理，包含立即中止與該硬體供應商的資料交換，後續亦將加強宣導供應商的安全意識與確認安全標準做法。目前此駭客侵害事件已進入司法調查程序。

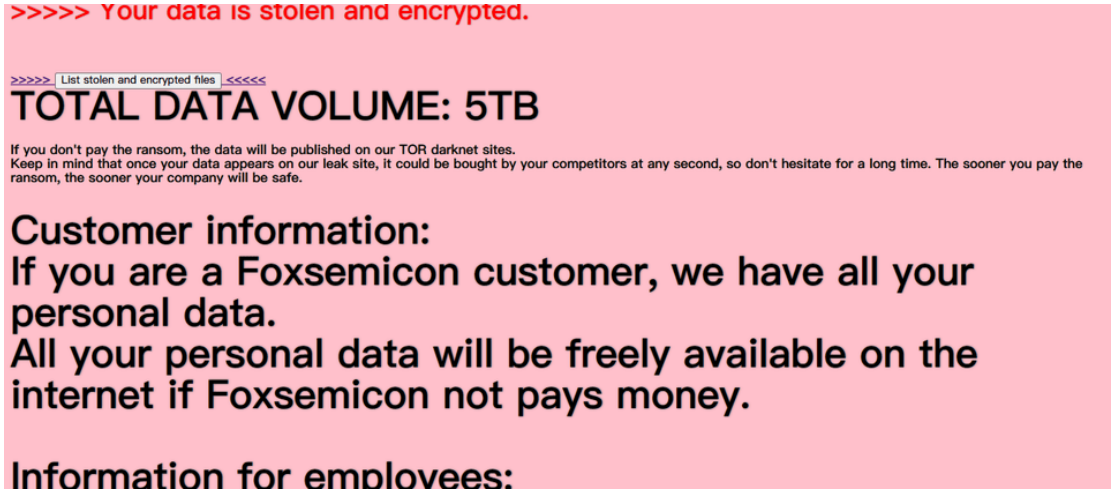
此外，數位發展部表示，業者若發現個資外洩或資安事件，而且需要協助，可通報「台灣電腦網路危機處理暨協調中心」(TWCERT／CC)。

文字整理自: 科技網、鉅亨網

康聯生醫 Healthconn

近日國內重點資安新聞

1. 某公司旗下的半導體設備廠網頁遭到攻擊


>>>>> Your data is stolen and encrypted.

>>>>> List stolen and encrypted files <<<<<

TOTAL DATA VOLUME: 5TB

If you don't pay the ransom, the data will be published on our TOR darknet sites.
Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Customer information:
If you are a Foxsemicon customer, we have all your personal data.
All your personal data will be freely available on the internet if Foxsemicon not pays money.

Information for employees:

2024-01-16

國內某半導體設備廠傳出遭到網路攻擊，駭客直接竄改該公司的網站並公布此事，揚言若不付錢，將公布所有客戶資料。

該公司表示部分資訊系統遭到攻擊，初步評估對運作無重大影響。在偵測到攻擊行動的當下，已全面啟動相關防禦機制及復原作業，並協同外部資安公司進行全面掃描、檢測、資料復原，但未進一步說明遭遇之攻擊類型。

(資料來源：iThome)

2. 駭客對政府機關人員寄送主旨為「投訴政府人員不作為」

2024-02-15

根據數位部資安署資通安全網路月報(113年1月)分析，發現近期駭客利用微軟Outlook電子郵件服務，針對政府機關人員寄送主旨為「投訴政府人員不作為」，內含惡意附檔的社交工程電子郵件，企圖誘騙收件人開啟惡意附檔以植入後門程式，進而竊取機敏資訊，相關情資已提供各機關聯防監控防護建議。

(資料來源：資通安全網路月報（113年1月）)

小測驗

Quiz

看了本期月報精選的社交工程案例及資安新聞後，你是否有從跟著案例中的字句想到了「三不三要」呢？

請簡答～

防範社交工程的三不三要是哪些呢？

若回答得有點模糊，可回到第四頁再次重新複習一次唷！

康聯生醫 Healthconn