

香港網絡安全 最新趨勢



香港警務處
網絡安全及科技罪案調查科
葉卓譽總督察



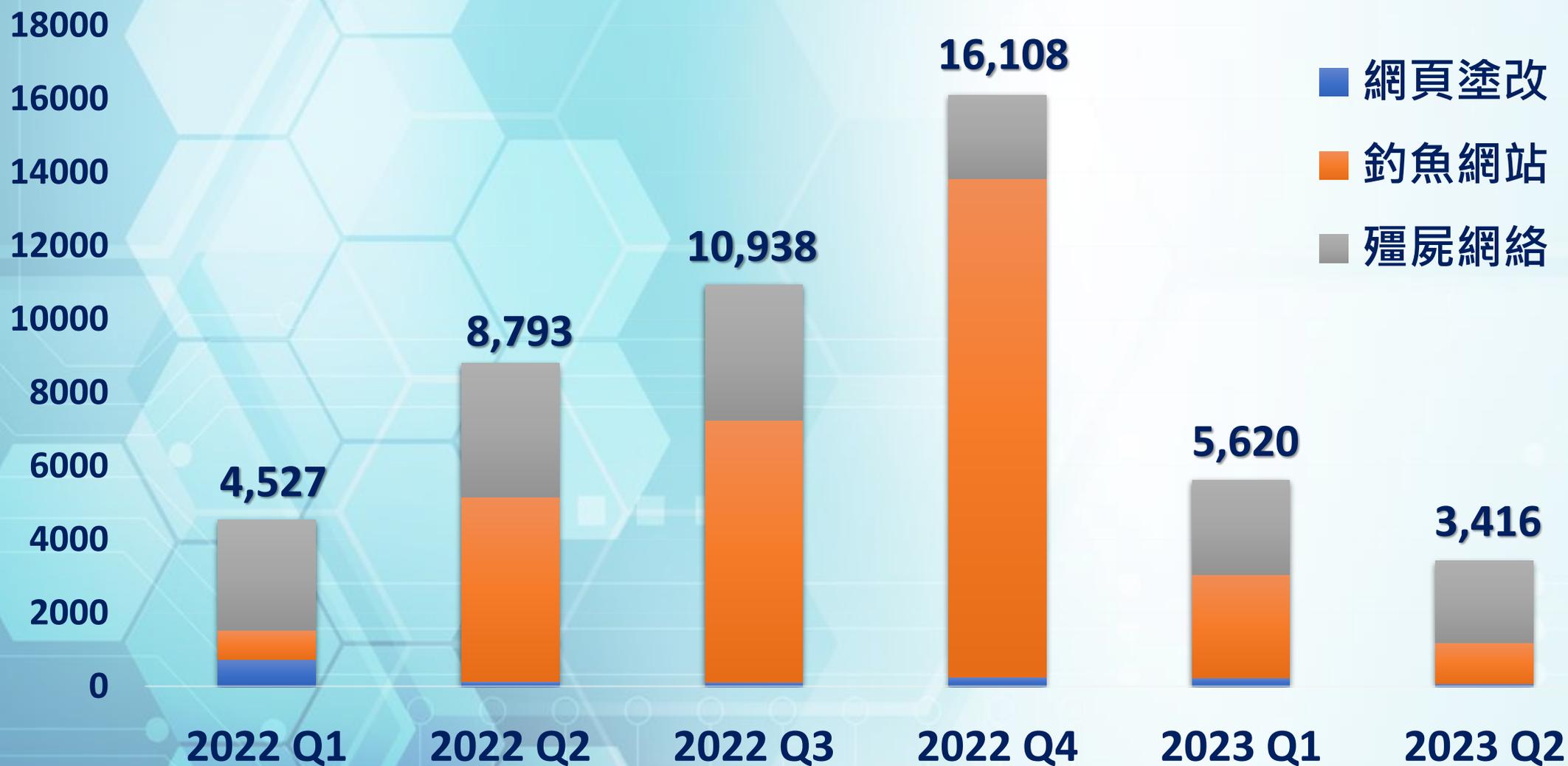
近期網絡安全事故的觀察

- 由不同黑客組織策劃
 - Trigona (俄羅斯)
 - Blackcat (俄羅斯)
 - Dharma ransomware (伊朗)
- 沒有共同關聯
- 純粹為取得經濟利益

香港科技罪案趨勢



香港網絡安全事件



常見網絡安全風險



釣魚攻擊



商業電郵騙案



勒索軟件

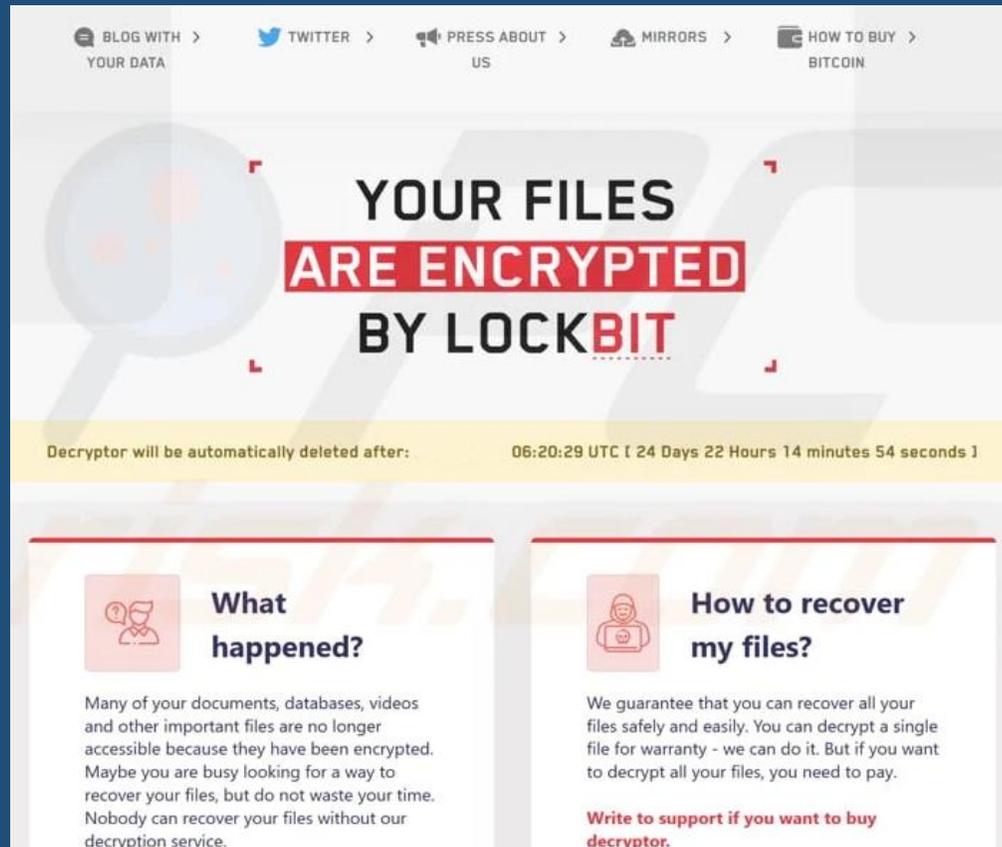


物聯網

勒索軟件

犯案手法

- 透過釣魚網站或電郵散播惡意程式
- 將用戶電腦檔案加密
- 要求用戶在特定時限以比特幣等繳付贖金



The screenshot shows a ransomware website with a dark blue header containing navigation links: 'BLOG WITH > YOUR DATA', 'TWITTER >', 'PRESS ABOUT > US', 'MIRRORS >', and 'HOW TO BUY > BITCOIN'. The main content area features a large magnifying glass icon and the text 'YOUR FILES ARE ENCRYPTED BY LOCKBIT', where 'ARE ENCRYPTED' is highlighted in a red box. Below this, a yellow banner indicates a countdown: 'Decryptor will be automatically deleted after: 06:20:29 UTC [24 Days 22 Hours 14 minutes 54 seconds]'. The page is divided into two columns. The left column, titled 'What happened?' with a question mark icon, explains that files are encrypted and offers a decryption service. The right column, titled 'How to recover my files?' with a person icon, guarantees file recovery for a fee and includes the text 'Write to support if you want to buy decryptor.'

勒索軟件

雙重勒索

- 釣魚攻擊、系統漏洞等感染目標電腦
- 電腦內資料無法讀取
- 竊取敏感資料
- 網上公開被盜取的文件

三重勒索

- 竊取目標公司敏感資料
- 與客戶或生意伙伴往來的商業機密
- 威脅目標公司及客戶或生意伙伴

四重勒索

- 三重勒索後，發動分散式阻斷服務攻擊
- 制造大量網絡流量癱瘓及竊取敏感資料
- 迫使目標公司繳付贖金



勒索軟件

受感染後應如何處理？

-  切斷受感染電腦的網絡連線
-  關上電腦的電源
-  記下感染前曾經執行過的程式和檔案、開啓過的電郵及瀏覽過的網站
-  從備份把電腦復原
-  切勿繳付贖金

保安貼士

- 定期備份資料
- 安裝最新修補程式
- 更新抗惡意程式碼軟件
- 定期全面掃描電腦
- 開啓可疑的電郵及短訊或連結
- 瀏覽可疑網站或下載任何檔案

黑客從哪裏 進入系統?



釣魚攻擊 取得登入憑證等

假冒csl. 釣魚短訊

假

CSL積分提示您，您的賬戶當前積分(9560積分)，將於今日內到期，請及時兌換積分獎賞：<https://csl.y578e.com/>



積分兌換查詢

請輸入手機號碼

查詢

假冒易通行 釣魚訊息

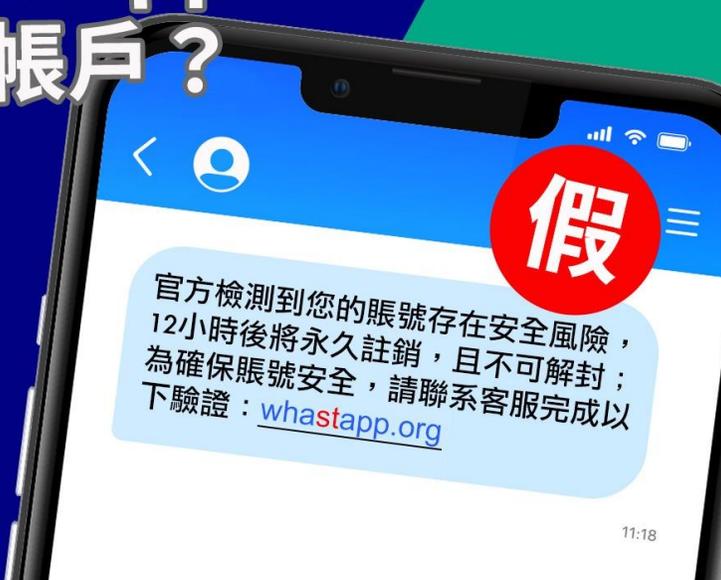
假

[易通行：自動繳費不成功]
你未能成功透過指定儲值戶口繳付
隧道費HK\$20請透過
<https://gov.hk.etolli.co>
繳費，並立即完成付款。



釣魚攻擊 騎劫帳號

白撞訊息
如何騎劫
WhatsApp
WhatsApp 帳戶?



假

官方檢測到您的賬號存在安全風險，
12小時後將永久註銷，且不可解封；
為確保賬號安全，請聯系客服完成以下
驗證：whatsapp.org



11:18

無收釣魚短訊 無印象泄露驗證碼
WhatsApp帳戶都被騎劫?
好可能因為去咗假網站↓↓

Search

whatsapp

贊助

waa.whaitas.cyou **假**

WhatsApp官方 - WhatsApp中文網
最新高 端 加密让 您的个人消息和通话更有安全保障。直接从电脑发送和接收WhatsApp 消息。

贊助

waa9.edllkikk.com **假**

WhatsApp电脑版 - WhatsApp官网
可助您触达全球客户，规模化打造引人入胜的体验，提高业务销量以及建立客户忠诚度。用文字，也能肆意展现自我，发布动态来分享每日点滴。

https://www.whatsapp.com **真**

WhatsApp | 安全、可靠的免費私人訊息和通話功能
使用WhatsApp Messenger 與親朋好友保持聯繫。WhatsApp 提供簡單安全又可擴展的訊息和通話服務，並且在世界各地的手機上皆可免費下載使用。



釣魚攻擊 惡意軟件入侵裝置



釣魚電郵演習 2023



個人層面

15.9%

曾點擊釣魚電郵



公司層面

61.6%

至少有一名員工
打開釣魚電郵

弱密碼

2023年最常用密碼

1. 123456	11. abc123	21. princess
2. password	12. 1234	22. letmein
3. 123456789	13. password1	23. 654321
4. 12345	14. iloveyou	24. monkey
5. 12345678	15. 1q2w3e4r	25. 27653
6. qwerty	16. 000000	26. 1qaz2wsx
7. 1234567	17. qwerty123	27. 123321
8. 111111	18. zaq12wsx	28. qwertyuiop
9. 1234567890	19. dragon	29. superman
10. 123123	20. sunshine	30. asdfghjkl

遠端控制

D DIGITAL
INFORMATION
WORLD

Remote Work Caused Data Breaches for 62% of Organizations

2023-03-10

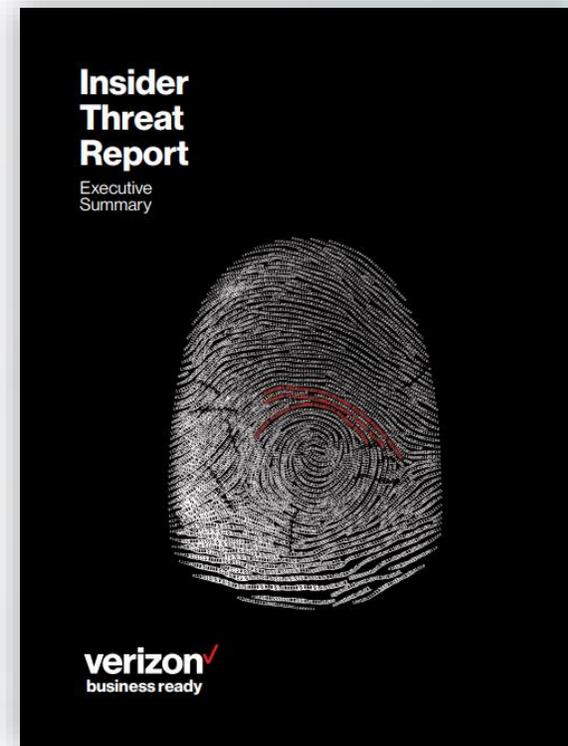
可能出現的保安風險

- 家中網絡保安程度低
- 員工個人電腦受感染
- 家中裝置受感染

內部威脅

特徵

- 錯誤訪問
- 頻密訪問
- 任意訪問
- 非辦公時間訪問

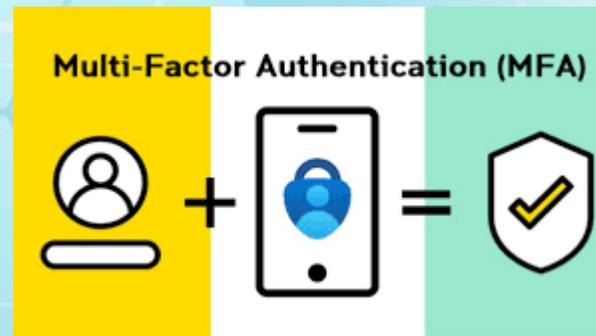


雲端計算

CLOUDTECH

2022-10-03

81% of companies had a cloud security incident in the last year



建立 網絡韌性



甚麼是網絡韌性？

面臨網絡危機和攻擊時，使用網絡資源去**預測**、**承受**、**恢覆**和**適應**的能力。

Source: NIST SP 800-172

網絡韌性週期



Source: NIST: Cybersecurity Framework Overview

建立網絡韌性- 策略思維

- 準備好災難復原計劃
- 實施零信任架構
- 明智選擇並定期監督服務供應商
- 限制對敏感文件和資產的訪問
- 教育員工、供應商和合作夥伴



電腦設備防護工具

電腦掃描及清洗工具



https://cyberdefender.hk/security_tools/



流動裝置應用程式

可疑電郵偵測系統

[⚠️ ⚠️ FROM NEW SENDER ⚠️ ⚠️] Payment Details 📄



寄件者 DEF Logistics <def1logistics@aol.com>

收件者 wills@vanguard-email.com <wills@vanguard-email.com>

日期 2023-07-31 12:01

📧 概覽 ⓘ 標頭 ☰ 純文字

ALERT !!

**The Email domain is first seen.
Beware of any hyperlink, attachment and
BANK ACCOUNT information unless you ensure
the authenticity of the sender.**

注意 !!

這是首次接收到的電郵地址。除非您確保其真確性，
否則請留意當中所附有的超連結，附件或銀行帳戶資料。
如有疑問，請尋求技術人員的支援。





防騙視伏器 / 防騙視伏App

守網者 網絡常識 保護你的裝置 家長及老師 網絡罪案 資源及活動 簡 EN Q

疑似詐騙 / 網絡陷阱?
用「防騙視伏器」Check吓啦!

網址、電郵、電話、平台帳戶、收款賬戶等

如不確定資料類型，便無需選擇。

- 請選擇類型
- 平台帳戶名稱
- 平台帳戶號碼
- 電話號碼
- 電郵地址
- 網址
- 收款賬戶
- IP 地址
- 雜湊值

可疑網站 網上情線 網購陷阱 白撞誘 陌生來電 招聘

防騙視伏APP

全城守網

為免「失去了一切」立即下載
全方位詐騙陷阱搜尋器 防騙視伏APP
減低受騙風險!

防騙視伏器

未有記錄 提防中伏 疑似有伏 高度有伏

一站式詐騙陷阱搜尋器

立即搜尋

網址 電話號碼
平台用戶名稱 社交帳號
收款帳號
電郵地址 IP地址

更多活動

守網者 最新消息 防騙視伏器 有用連結 設定

Cyberdefender.hk/scameter





防騙視伏器 / 防騙視伏App 搜尋結果



紅色代表「高危有伏」：

輸入的資料與詐騙舉報有關，或網絡安全風險屬高危級別



橙色代表「疑似有伏」：

有相近的詐騙舉報資料，或網絡安全風險屬中高級別



黃色代表「可能有伏」：

你仍需提防中伏

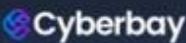


紫色代表「未有記錄」：

但不代表無伏，應時刻保持警惕



漏洞檢測計劃

主辦單位：   策略合作夥伴：

狩網運動2023

2023年6月至7月·香港

全港首個公私營合辦的
漏洞檢測計劃

企業免費獲得

- 網頁漏洞檢測服務
- 網絡安全報告
- 一對一諮詢服務

**IT專才登記成為
賞金獵人**
賺取額外收入



釣魚電郵演習

釣魚電郵演習2023

提高員工防範可疑電郵的意識

立即登記

費用全免 >>>

2023年5月13日截止報名



CyberDefender.hk



CYBER 守網者
DEFENDER

Scamster+

