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


80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
整體罪案
科技罪案
67,740
66,439
60,646
56,017
54,225
59,225
63,232
64,428
70,048
42923
6,778
6,862
5,939
5,567
7,838
8,322
12,916
16,159
22,797
15637
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023 上半年
科技罪案
佔整體罪案
10%
10%
10%
10%
14%
14%
20%
25%
33%
36%

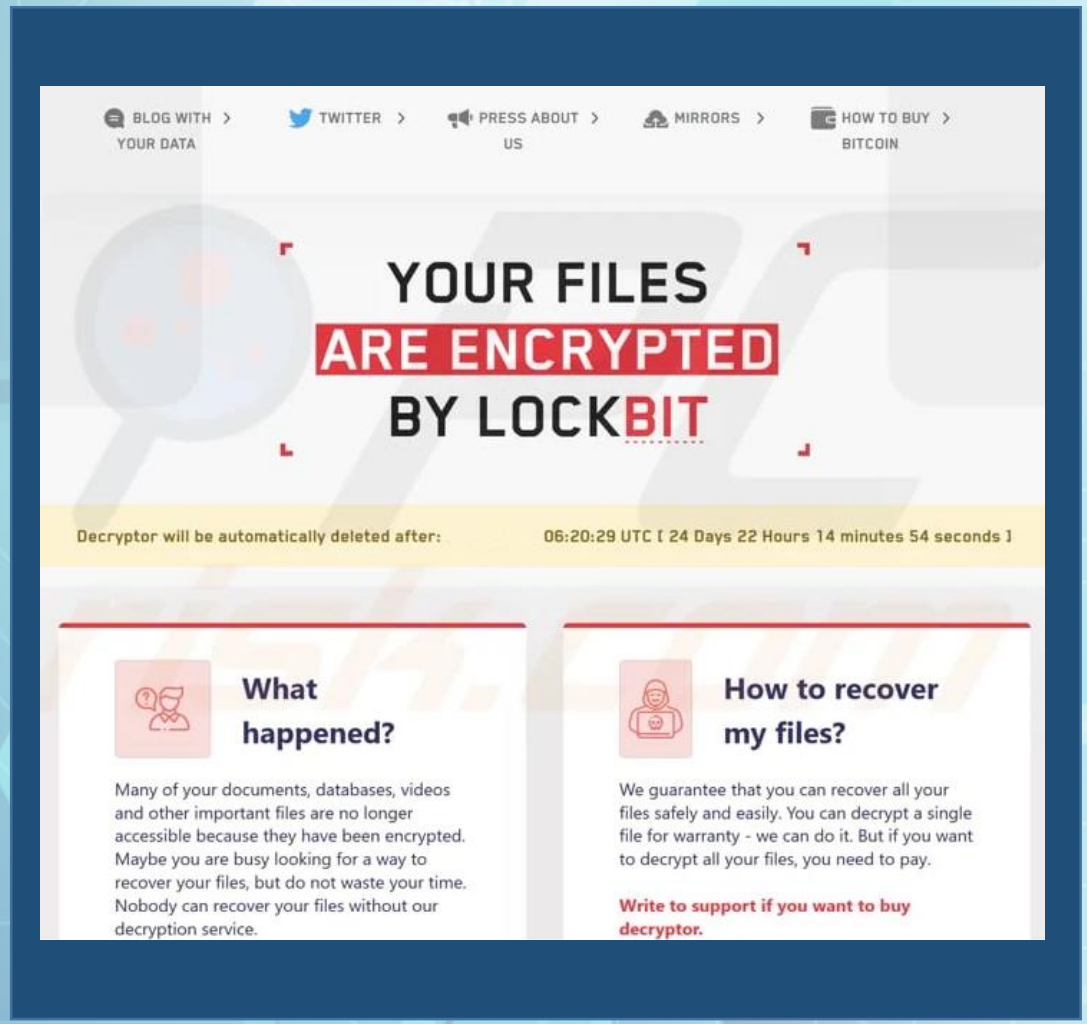
香港網絡安全事件


18000
16000
14000
12000
10000
8000
6000
4000
2000
0
4,527
8,793
10,938
16,108
5,620
3,416
2022 Q1
2022 Q2
2022 Q3
2022 Q4
2023 Q1
2023 Q2
網頁塗改
釣魚網站
殭屍網絡

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

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

釣魚攻擊 騎劫帳號


白撞訊息
如何騎劫
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：whastapp.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.whaiitas.cyou
假
WhatsApp官方 - WhatsApp中文网
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
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
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

DIGITAL INFORMATION WORLD

Remote Work Caused Data Breaches for 62% of Organizations

2023-03-10

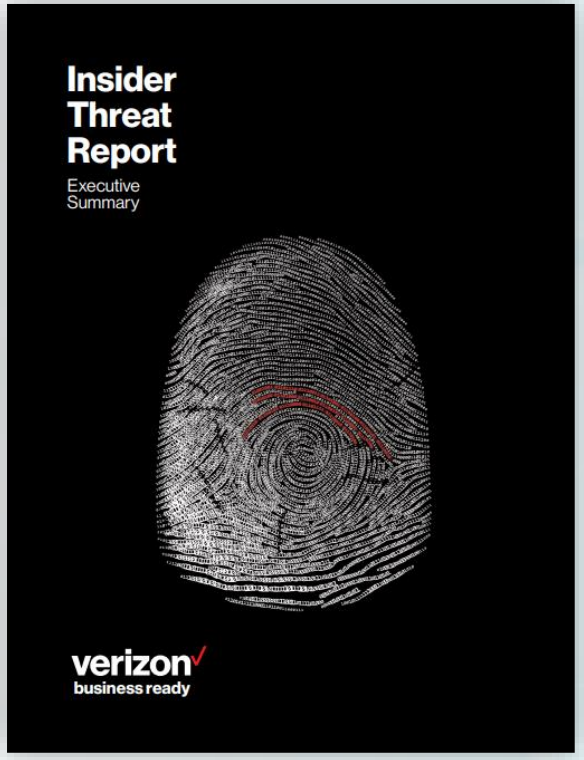
可能出現的保安風險

- 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

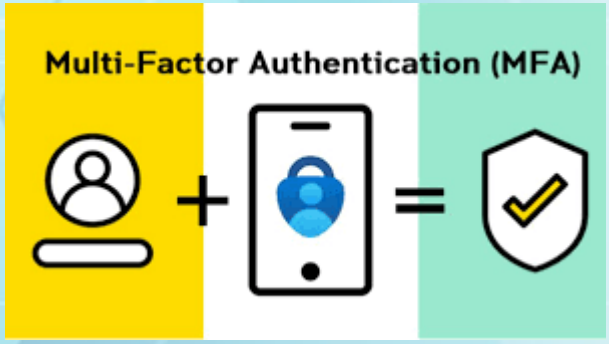


雲端計算

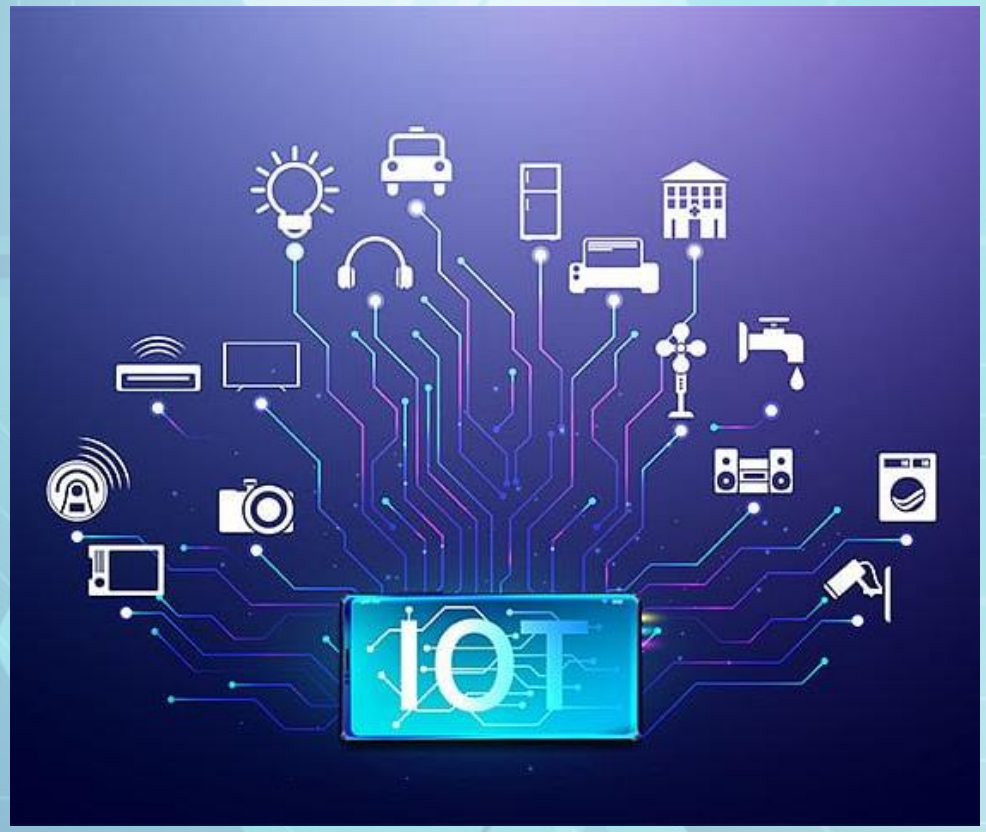
CLOUDTECH

2022-10-03

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



物聯網



- 藉入侵物聯絡裝置進入網絡
- 被用作發動殭屍網絡攻擊

建立
網絡韌性

甚麼是網絡韌性?

面臨絡危機和攻擊時，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

識別

- 識別重要的安全漏洞
- 識別高價值和關鍵資產

保護

保護關鍵基礎設施和服務
- 保護關鍵業務系統
- 保護端點和關口
- 保護移動員工和客戶

偵測

實施檢測系統以識別攻擊
並評估受影響系統

復原

快速、準確、高效地恢覆
系統和數據

反應

收集和分析有關事件的信息，作出
最佳行動方案

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

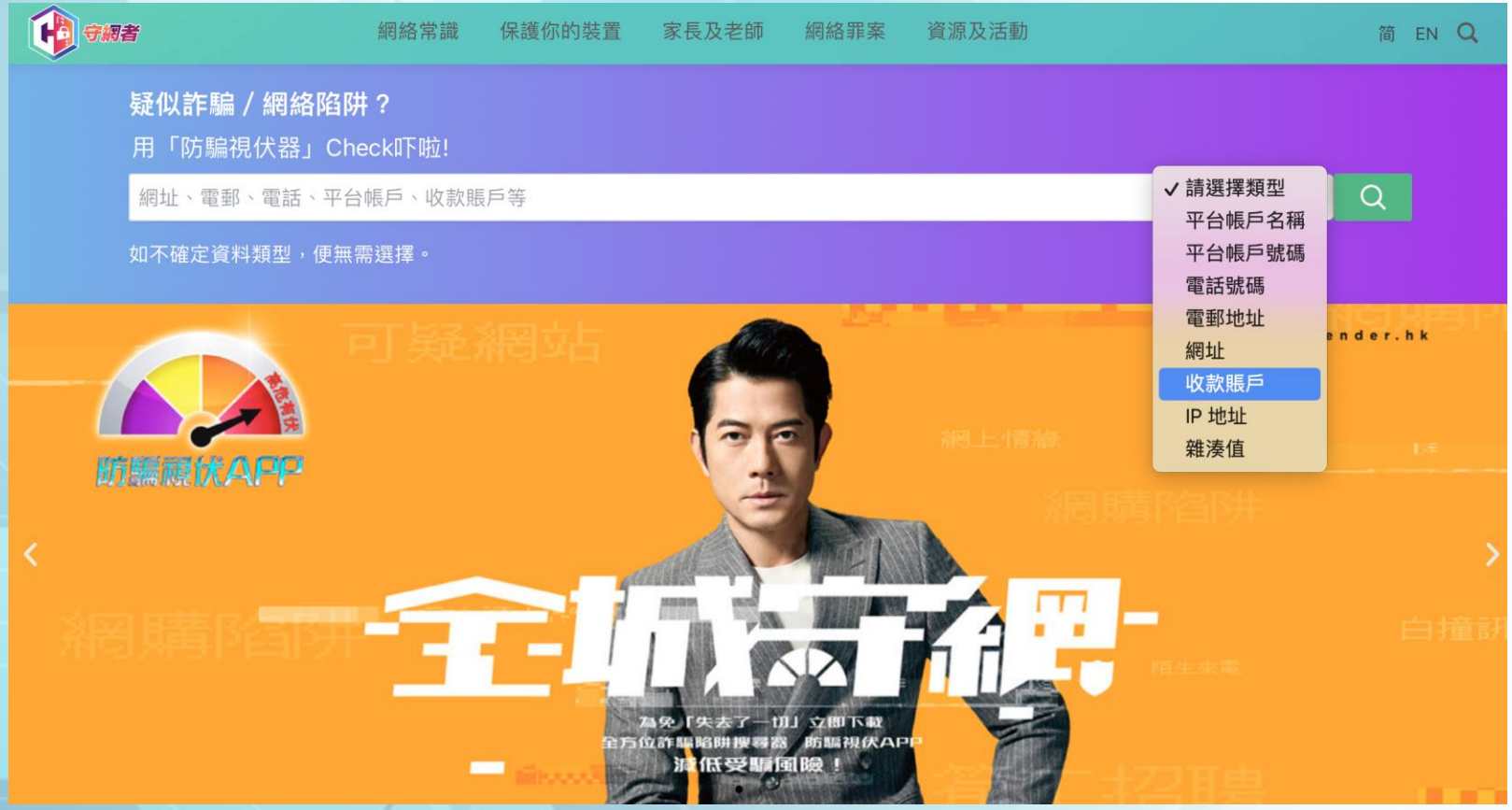
https://cyberdefender.hk/security_tools/

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 <def1ogistics@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。
e-GUARD
偵測可疑電郵
Identify Suspicious Emails

防騙視伏器 / 防騙視伏App



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

釣魚電郵演習

CyberDefender.hk

Scameter+

CYBER 守網者 DEFENDER