SOPHOS
Cybersecurity evolved.

# Sophos 2021 年威脅報告

## 在不確定的世界中引領網路安全

作者 SophosLabs、Sophos Managed Threat Response、
Sophos Rapid Response、Sophos AI 與 Cloud Security

# 目錄

共用的力量 2

執行摘要 3

勒索軟體的未來 5
- 資料竊取創造出第二個敲詐市場 5
- 贖金隨著攻擊的增加而增加 7
- 勒索軟體快速回應人員的每日工作 8

對企業的日常威脅 - 礦坑中的金絲雀 9
- 針對 Windows 和 Linux 伺服器的攻擊 9
- 低估「商用」惡意軟體的後果 11
- 遞送機制 13
- 資訊安全：二十年回顧 16

將 COVID-19 視為攻擊的戰力加乘因子 18
- 家是新的邊界 18
- 犯罪軟體即服務 19
- 垃圾郵件、詐騙和違約事件 20
- 遠距工作提高了安全雲端運算的重要性 23
- CCTC 對快速回應大規模威脅的定義 25

不要鬆懈：威脅會從非傳統平台而來 26
- Android Joker 惡意軟體數量激增 26
- 廣告和 PUA 與惡意軟體的區別越來越大 27
- 以子之矛，攻子之盾：將安全工具用於犯罪用途 29
- 數位流行病學 31

# 共用的力量

## Sophos 技術長 Joe Levy

### 「如果你想快點走，就一個人走，但是如果你想走遠一點，那就一起走。」

對網路安全產業來說，這個非洲諺語再貼切不過了。透過具有強烈的團隊合作精神的集體合作，我們所達成的成就遠遠超過了個別廠商和網路犯罪的單打獨鬥。

但是，藉由改進我們的方法，並更全面地共用威脅情報、擴大能為共用和協作做出貢獻 (並從中受益) 的參與社群，網路安全廠商才有辦法繼續提高攻擊者的門檻，並帶來更長遠、更具影響力的改變。

本著合作的精神，Sophos 在 2017 年加入 Cyber Threat Alliance (CTA)，該組織致力於打破多年來阻礙資訊安全產業競爭對手彼此合作的各種障礙。CTA 已經成功超越了一開始的初衷，是一個共用威脅情報的存放庫和化解差異的組織，已經成為網路安全產業的聯合國。

透過與 CTA 的合作，Sophos 能從聯盟提供的預警和廠商之間的資料交換獲益，可以更妥善地保護我們的客戶。Sophos 也貢獻自己的威脅情報來分擔保護其他廠商客戶的責任。

2020 年 3 月，隨著全球迅速實施封鎖來遏阻 COVID-19 的擴散，Sophos 首席科學家 Joshua Saxe 在Twitter 上發出號召。為了反制犯罪集團開始將 COVID-19 用於一系列犯罪活動中，超過 4,000 名資訊安全分析人員齊聚一堂，並在當天建立的 Slack 頻道中共同組成 COVID-19 網路威脅聯盟 (COVID-19 Cyber Threat Coalition, CCTC)。該頻道為社群建立了一個持久性的「中心」，以在危機時刻發揮作用，並在 CTA 的主導下盡可能實現非營利的狀態。

最終，這些共用威脅情報的合作帶給我們的遠不只是組織本身。用另一個盲人摸象的寓言來比喻，我們可以知道，沒有一個廠商能夠只靠自己的主觀經驗就能提供全面或絕對的保護。統合眾人的經驗才能瞭解複雜事物的真正面貌。這些合作保護數百萬人免於網路犯罪的傷害，但這並不僅它們成功的**原因**。它們之所以成功，是因為成員和創始人的核心動機是保護任何人免受傷害。不是利潤導向，而只是想捍衛那些需要幫助的人，因為大野狼似乎就在門口。

事實證明該模型是正確的，並可填補任何廠商都無法單獨提供的關鍵防護缺口，但我們可以用它完成更多事情。作為一個產業，未來我們希望共用機器學習模型或培訓資料集，就像我們今天共用封鎖清單或 Yara 規則一樣。我們還可以強化和協助如 STIX 和 ATT&CK 架構等新出現的標準。我們還可以參加特定產業的 ISAC 和 ISAO。

未來將是更加緊密相連的世界，我們都會因此而更好，並得到更好的保護。

# 執行摘要

《Sophos 2021 年威脅報告》內容涵蓋 Sophos 在過去 12 個月中從 SophosLabs 對惡意軟體和垃圾郵件分析，以及 Sophos Rapid Response、Cloud Security 和 Data Science 團隊在工作中獲得的深入資訊。我們日常工作中保護客戶的各種努力，可幫助您深入瞭解威脅狀態、指導事件回應人員和 IT 安全專業人員，了解未來一年他們應該致力於哪些方面來保護網路和端點。

我們將報告分為四個主要部分：討論勒索軟體如何自行轉變以及這種威脅的發展方向；分析大型組織面臨的最常見攻擊，以及為什麼礦坑中的金絲雀 (比喻危險指標) 仍是重大威脅；全球疫情將如何影響 2020 年的資訊安全；以及攻擊鎖定過去不被視為企業受攻擊面的平台的調查。

總結報告的主要內容：

# 勒索軟體

- 勒索軟體威脅執行者繼續以更快的速度翻新技術和犯罪手段
- 現在，更多勒索軟體團體加入資料竊取的行列，他們會威脅受害者即將公布敏感資料而進行敲詐
- 隨著勒索軟體團體用更多心力攻擊大型組織，索取的贖金數字也急劇上升
- 此外，勒索軟體攻擊中獨立的威脅執行者團體，與地下犯罪分子的合作似乎更為緊密了，它們的行為更像是網路犯罪聯盟，而不是獨立團體。
- 以前需要數週或數天才能進行的勒索軟體攻擊，現在可能只需要幾個小時即可完成

# 「日常」威脅

- 同時執行 Windows 和 Linux 的伺服器平台已成為攻擊的主要目標，並被用於從內部攻擊組織
- 如 RDP 和 VPN 集訊器等常見服務，仍然是攻擊網路邊界時的重點，威脅執行者也使用 RDP 在受破壞的網路內橫向移動
- 即使是低階的「商用」惡意軟體，也會造成重大影響，因為越來越多惡意軟體系列成為其他惡意軟體的「內容發佈網路」
- 在調查中我們發現，忽略基本安全保健的一或多個方面，是導致許多最具破壞性的攻擊成功的根本原因

## COVID-19

- 在家工作帶來了全新的挑戰，因為組織的安全範圍將擴展到受各種安全等級保護的數千個家庭網路
- 雲端運算滿足了許多企業對安全運算環境的需求，但仍有著傳統企業網路沒有的獨特挑戰
- 威脅執行者曾試圖挽回自己的聲譽，承諾不會對參與拯救生命的衛生組織發動攻擊，但他們後來食言了
- 犯罪企業已成為服務性經濟，使新的犯罪分子更能輕鬆上手
- 2020 年，來自世界各地的網路安全專業人員組成了一支快速反應部隊，以應對利用新冠病毒相關事物進行社交工程的潛在威脅

## 非傳統平台

- 現在，攻擊者經常會利用許多滲透測試人員在處理即時、作用中攻擊時，率先使用的「紅隊」工具和公用程式
- 儘管行動平台業者努力監控應用程式中是否包含惡意程式碼，但攻擊者仍持續開發能夠躲過這些程式碼掃描的技術
- 早期被歸類為「可能不需要」的軟體，因為會投放大量廣告 (但不是惡意軟體)，採取的策略和公開的惡意軟體越來越難以區分
- 資料科學家將從生物流行病學界借來的方法應用於垃圾郵件攻擊和惡意軟體裝載，作為彌補偵測缺口的方法

# 勒索軟體的未來

整個 2020 年，出現的勒索軟體攻擊使得已如驚弓之鳥的人們更為痛苦。疫情破壞了人們的生活和生計，許多勒索軟體系列也是如此，它們沒有停止鎖定健康和教育領域，即使醫院已經成為 COVID-19 的戰場，而學校從三月後得要盡力找出新方式來教育孩子。

您無法在疫情期間透過募款義賣來籌到足夠的贖金，但部份學校在受到攻擊鎖定的第一天，就使用安全的備份恢復運作。

勒索軟體操作者率先找出躲避端點安全產品並快速傳播的新方法，甚至還對遭鎖定的個人或公司提出解法 (從他們的角度)，建議他們建立良好的備份並將其安全地保存在勒索軟體無法觸及的地方。

但看似形形色色的勒索軟體並不像看起來那樣種類繁多。隨著時間過去，我們調查了越來越多的攻擊，Sophos 分析人員發現一些勒索軟體系列似乎已經共用程式碼，而且某些勒索軟體集團似乎開始協作而非競爭。

考慮以上事實，我們很難準確地預測勒索軟體犯罪分子的下一步。勒索軟體開發者和操作者花了很多時間研究如何克服端點安全產品的防禦。我們要對抗他們的對策。他們在制定新策略時展現出創造力和通用性；我們則以韌性研究他們的行為並聰明的方法加以阻擋。

# 資料竊取創造出第二個敲詐市場

直到今年，所有對勒索軟體完全沒有經驗的安全公司，仍然一致採用傳統的作法：鎖定明顯的入侵方法，例如面向網際網路的 RDP 埠；建立良好的離線備份；並快速解決小型、無害的惡意軟體 (例如 Dridex 或 Emotet) 的感染，以免它們傳遞具殺傷力的裝載。

例如，鎖定美國多個校區的幾次備受矚目的勒索攻擊失敗了，部分原因是 IT 管理員為重要資料建立了完整的備份。

為了抵銷受害者的防備工作，部份勒索軟體系列採取其他手段，目的是加大受害者支付贖金的壓力，即使每個包含重要資料的備份都是安全的。它們不僅會綁架這些機器作為人質，而且還會竊取機器上的資料，威脅受害者如果不支付贖金，就將資料公佈給全世界。

在過去的半年中，Sophos 分析人員觀察到勒索軟體攻擊者使用一個通用的工具集 (緩慢增加中)，從受害者網路中竊取資料。端點安全產品不會偵測出這一組任何人都可能擁有的知名合法公用程式。使用這種作法的勒索軟體系列不斷增加，包括了 Doppelpaymer、REvil、Clop、DarkSide、Netwalker、Ragnar Locker 和 Conti 等。攻擊者會經營「外洩資料」的網站並公開他們竊取的資料；REvil 允許任何人直接從其網站上購買資料。

犯罪分子使用這個工具集來複製敏感的內部資訊，將其壓縮為封存檔，然後再將其傳輸到網路之外 - 受害者無法接觸之處。到目前為止，我們已經發現他們使用以下工具：

- Total Commander (內建 FTP 用戶端的檔案管理程式)
- 7zip (封存檔建立軟體)
- WinRAR (封存檔建立軟體)
- psftp (PuTTY 的 SFTP 用戶端)
- Windows cURL

在竊取資料時，攻擊者什麼都不挑，整個資料夾都偷走，無論其中包含那些檔案類型。(在加密攻擊時，勒索軟體通常優先處理重要的檔案類型，排除其他許多類型)

大小無關緊要。它們似乎不在意被鎖定的目標有多少資料。對每個企業來說，目錄結構都是唯一的，某些檔案類型的壓縮程度比其他檔案更好。在部署勒索軟體之前，我們看到受害者已經被竊取了至少 5 GB 到多達 400 GB 的壓縮資料。

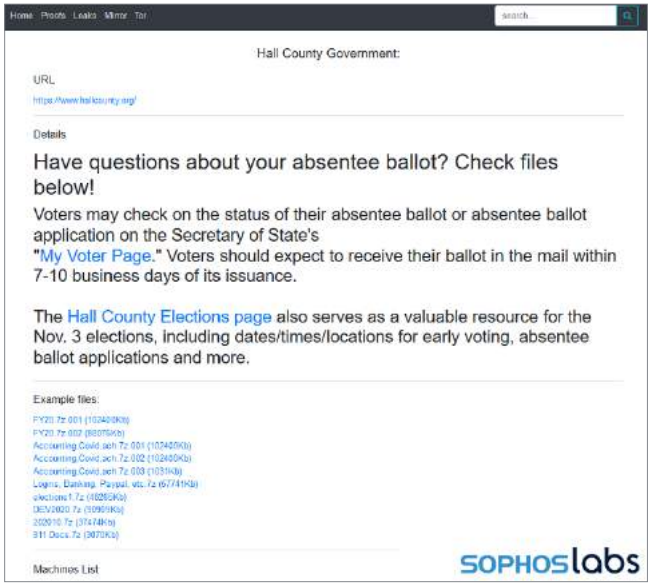



圖 1。2020 年 10 月，Doppelpaymer 勒索軟體外洩的頁面顯示，攻擊者攻擊了美國喬治亞州霍爾縣的網路。外洩的內容包括一個名為「選舉」的檔案，裡面有 2020 年州初選的選票樣張、2018 年選舉的民意調查人員名單及其電話號碼，以及其他敏感檔案。美聯社報導說，勒索軟體對該縣用來驗證選票的簽章驗證資料庫進行了加密。來源：SophosLabs。

犯罪分子通常會將竊取的資料傳送到合法的雲端儲存服務，使該活動很難被發現，因為它們都是常見的一般網路流量目的地。對於攻擊者而言，以下是最常用來儲存外洩資料的 3 種雲端儲存服務：

- Google 雲端硬碟
- Amazon S3 (Simple Storage Service)
- Mega.nz
- 私人 FTP 伺服器

在攻擊的最後一個階段，勒索軟體攻擊者會更傾向尋找包含重要資料備份的本地伺服器。找到後，它們會先刪除 (或加密) 這些備份，然後再對整個網路進行加密攻擊。

離線儲存一份關鍵資料的備份，比以往任何時候都更為重要。如果它被勒索軟體犯罪分子找到，就會被破壞掉。

# 贖金隨著攻擊的增加而增加

很難相信，兩年前 Sophos 的分析人員還對勒索軟體 SamSam 帶來的 600 萬美元收入感到驚訝。在 2020 年 Sophos 回應的一次攻擊中，勒索軟體操作者勒索的金額，是 SamSam 犯罪集團 32 個月收入的兩倍以上。

現在，我們將勒索軟體分級：攻擊大型企業網路的重量級、鎖定公民社會 (公共安全和地方政府) 和中小型企業的沉量級，以及針對個人電腦和家庭使用者的羽量級。重量級中的重量級絕對令人印象深刻，但其高額的贖金和低階勒索軟體贖金不能相提並論。

Sophos 擁有一支專門的團隊，負責調查勒索軟體攻擊並經常與遭到鎖定的目標合作。該團隊可以在事後對攻擊事件進行鑑識，甚至可以在攻擊進行時中斷攻擊。當有機會阻止或控制傷害時，Sophos Rapid Response 團隊會參與回應，但有時攻擊發生得太快，被鎖定的目標無能為力，只能決定是否支付贖金，此時 Sophos 就不會再介入。

這時就是像 Coveware 這樣的公司出場的時候。該公司會代表被勒索的目標與攻擊者進行高風險的談判。Coveware 技術長 Alex Holdtman 證實了我們的懷疑，重量級勒索軟體是出現天價贖金的主因。

**平均贖金支出 (每季)**

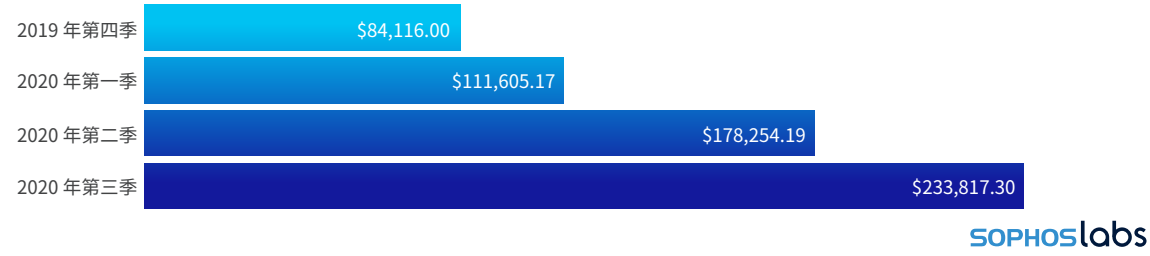



圖 2在過去一季，平均贖金增加了 21%，在過去的一年中幾乎增加了兩倍。來源：Coveware。

在過去一季，平均贖金增加了 21 %，但 Coveware 認為，平均值是因為受到一兩次非常鉅額的贖金的影響。最近一季的平均贖金相當於 233,817.30 美元，以加密貨幣支付。一年前，平均贖金為 84,116 美元。

勒索軟體的威脅執行者了解停機會造成多大的損失，並不斷測試他們在勒索攻擊中可以威脅得手的上限。

幾個勒索軟體系列已經把敲詐當成副業，以促使交易完成。如前面報告所述，Netwalker 等集團就是使用了此一策略。如此一來，即使遭鎖定目標擁有完全可復原的資料備份，仍有可能被迫付款，以免勒索軟體犯罪分子外界發佈其內部資訊。

低階的／勒索軟體需求一直增加，但 Holdtman 表示，它們遠不及大魚重要。有許多小型企業和個人受到攻擊，但對他們來說，得手的贖金相對少得多。

# 勒索軟體快速回應人員的每日工作

當某個組織被當時仍然活躍的 Maze 勒索軟體作為目標時，他們尋求 Sophos Rapid Response 團隊的協助。我們調查並積極回應了仍在進行中的攻擊。接下來是攻擊進行時的每日摘要。

**第一天之前**

在攻擊開始活動之前的某個時刻，操作者會破壞被鎖定網路上的一部電腦。

然後，這台電腦就被用作網路中的「灘頭堡」。很多時候，攻擊者將使用遠端桌面通訊協定 (RDP) 用它連線到其他電腦。

**第一天**

當 Cobalt Strike SMB 指標被以服務型態安裝到一部未受保護的網域控制站 (DC) 時，就是出現惡意活動的第一個證據。攻擊者可以使用弱密碼來利用 Domain Admin 帳戶，從已經被入侵的電腦控制 DC。

**第二天**

攻擊者建立、執行然後刪除一系列排程好的工作和批次指令碼。從調查人員看到的證據來看，這些工作類似於往後用於部署勒索軟體攻擊的技術。攻擊者可能正在測試他們想要使用的方法。

透過被入侵的 Domain Admin 帳戶和 RDP 存取，攻擊者可以透過網路橫向移動到其他重要的伺服器。

他們使用合法的網路掃描工具 Advanced IP Scanner 開始對應網路，並列出 IP 地址列表以供後續部署勒索軟體之用。攻擊者會建立一個單獨的 IP 地址列表，它們都是被鎖定 IT 管理員所使用的電腦。

接下來，攻擊者會使用 Microsoft 工具 ntdsutil 傾印 Active Directory 的雜湊憑證資料庫。

攻擊者執行各種 WMI 命令來收集遭入侵機器的資訊，然後再將注意力轉向資料外洩：他們會找出檔案伺服器，並使用遭入侵的 Domain Admin 帳戶透過 RDP 遠端存取它。他們開始壓縮檔案伺服器上的檔案夾。

攻擊者將檔案移動到網域域控制站，然後嘗試在 DC 上安裝雲端儲存應用程式 Mega。這個動作被系統安全措施阻擋，因此他們改使用 Web 版本，然後上傳壓縮檔案。

**第三天**

整天都在繼續向 Mega 傳輸資料。

**第四天和第五天**

在此期間未觀察到惡意活動。在先前的事件中，我們觀察到勒索軟體攻擊者會等到周末或假日期間才發動攻擊，因為此時 IT 安全團隊無法正常工作或密切關注網路的動態。

**第六天**

一個星期日。使用遭入侵的 Domain Admin 帳戶和製作好的 IP 地址列表，發動第一次 Maze 勒索軟體攻擊。攻擊目標為 700 多台電腦，該攻擊會立即被安全措施偵測並加以阻止。攻擊者可能沒有意識到攻擊已被阻止，或者他們希望利用被竊資料來威脅受害者就足夠了，因為此時他們發出 1,500 萬美元的勒索要求。

**第七天**

安全團隊安裝其他安全措施，並進行 24/7 全天候威脅監控。事件回應調查開始，快速識別遭入侵的 admin 帳戶並找到幾個惡意檔案，然後阻止攻擊者與遭入侵機器之間的通訊。

**第八天**

發現攻擊者使用的其他工具和技術，以及與資料外洩有關的證據。更多檔案和帳戶被阻擋下來。

**第九天**

儘管安全團隊進行防禦，攻擊者仍持有對網路和不同帳戶的使用權限，並發起了第二次攻擊。這次攻擊類似於第一次：在 DC 上執行命令，循環使用 txt 檔案中包含的 IP 地址列表。

這次攻擊很快就被識別出來。系統會自動偵測到勒索軟體，然後停用並刪除遭入侵的帳戶和惡意軟體裝載。沒有檔案被加密。

攻擊者顯然不想放棄，再試一次。第二次攻擊後的幾個小時，第三波嘗試就出現了。

到目前為止，攻擊都只是鎖定單一電腦，看起來似乎放棄了。這是提取竊取資料的主檔案伺服器。

Maze 攻擊者採用了不同的方法，其部署虛擬機器 (VM) 的完整副本和 VirtualBox 虛擬機器管理程式安裝程式，2020 年 9 月 Sophos 已經在 SophosLabs Uncut 上詳細說明了這一個攻擊。

第三波攻擊的結果與之前相同：Sophos Rapid Response 團隊偵測並阻擋了該攻擊，沒有檔案被加密。該團隊幫助客戶封鎖了犯罪集團，攻擊者無法再繼續攻擊。

# 對企業的日常威脅 - 礦坑中的金絲雀

如果您對網路攻擊的一切認識都來自新聞報導，您可能誤以為天要塌下來了。鎖定大型組織的攻擊每天都在發生，但它們並非都是黑天鵝事件，會如同重大資料外洩般使公司的發展 (或股價) 暴跌，並影響信譽。許多攻擊更為平凡無奇，包含 SophosLabs 團隊列為「一般嫌疑犯」中的「頭號通緝犯」的惡意軟體。

但是，儘管我們已經掌握和遏止了這些攻擊以及它們所遞送的部份某些惡意軟體，但如果不能迅速且有效地加以處理，每一次攻擊都可能使情況變得更糟。以帶著鳥兒為比喻，這些日常攻擊就好比礦坑中的金絲雀，可能是會迅速失控的有毒物質的早期跡象。

# 針對 Windows 和 Linux 伺服器的攻擊

儘管我們在 2020 年回應的絕大多數安全事件，都和執行各種 Windows 版本的桌上型電腦或筆記型電腦有關，但我們看到針對 Windows 和非 Windows 伺服器的攻擊有穩定增加的趨勢。一般來說，長久以來伺服器一直是具吸引力的攻擊目標，原因很多：它們經常長時間無人看守或不受監控地運作；伺服器通常比筆記型電腦搭載更多的 CPU 和記憶體；伺服器可能擁有網路上的特殊權限，例如可以取得組織營運時最敏感、最有價值的資料。這使它們成為持續性攻擊者的絕佳立足點。這些特性在 2021 年仍不會改變，Sophos 預計鎖定伺服器的攻擊將繼續增加。

針對伺服器的大多數攻擊都符合三種設定之一 - 勒索軟體、加密挖礦程式和資料外洩，攻擊者會根據每種設定採用不同的策略和技術。伺服器管理員的最佳做法，是避免從伺服器執行一般桌面應用程式以防感染，例如電子郵件用戶端或 Web 瀏覽器，因此針對伺服器的攻擊需要改變策略。

面對網際網路且執行 Windows 的伺服器會遭到永無休止的 RDP 暴力破解攻擊，至少在過去 3 年中，這種攻擊策略最常與勒索軟體攻擊相關 (並且可以預測到)。Sophos Rapid Response 小組調查時經常發現，勒索軟體攻擊的根本原因和透過 RDP 初步存取目標的網路有關，然後攻擊會使用這些機器在網路中立足並控制 DC 伺服器，最後再利用它們發動其餘的攻擊。

相比之下，加密劫持攻擊的目標，更傾向於鎖定 Windows 中以及通常運作在伺服器硬體上的應用程式 (例如資料庫軟體) 中的多種弱點。

例如，Lemon_Duck 加密挖礦程式會對執行 Microsoft SQL Server 的網際網路伺服器進行暴力 (brute-force) 攻擊。攻擊者一旦猜出正確的資料庫密碼，便會使用資料庫本身重新組合加密挖礦程式的裝載，將其寫入伺服器的檔案系統並執行它。然後，遭感染的電腦將試圖利用 EternalBlue 和/或 SMBGhost 弱點來傳播這個加密挖礦程式。

Lemon_Duck 是不限平台的攻擊者，可以感染 Linux 伺服器。該惡意軟體會試圖從一個相對較小的列表中使用暴力攻擊猜測 SSH 密碼。如果成功，攻擊者將上傳惡意的 shellcode，然後利用 Redis 服務中的弱點來建立立足點。加密挖礦程式還可以隱藏自己，透過執行命令以從 Hadoop 叢集中自行啟動。

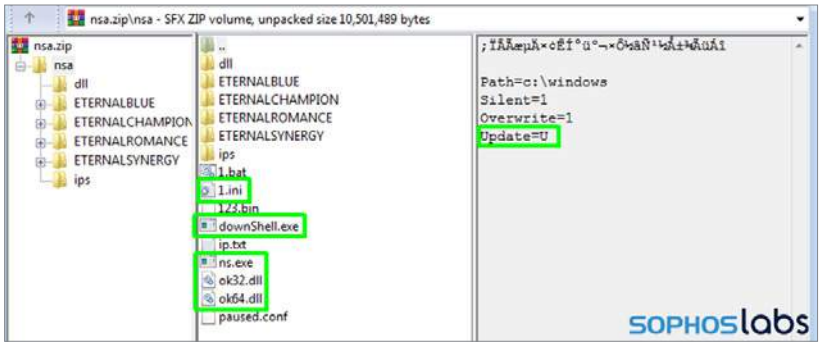



圖 3。一種更有生產力的密碼挖礦程式 MyKings，會散佈包含殭屍網路 (以綠色顯示) 元件的 Zip 檔，以及 Shadow Brokers 從 NSA 外洩取得的一些漏洞利用攻擊。來源：SophosLabs。

有時，攻擊者會鎖定在伺服器，因為他們想要竊取儲存伺服器上的高價值資料，而不是快速回收或持續性的小額加密貨幣。2020 年，Sophos 發現了一個針對 Linux 伺服器的攻擊者，我們稱之為 Cloud Snooper。有問題的伺服器託管在雲端運算叢集中，並發展出一個巧妙的訊息中繼系統來躲避偵測，在一般 HTTP 連線中夾帶它們的命令和控制訊息。


圖 4。用「披著羊皮的狼」比喻，說明 Cloud Snooper APT 惡意軟體如何以傳統的 HTTP 請求和回應作幌子來隱藏其命令和外洩的資料，並利用一種會監控網路流量並即時重新寫入 TCP/IP 封包的工具。來源：SophosLabs。

在過去，伺服器管理員不會在伺服器上安裝端點保護產品，但是隨著這類攻擊出現，傳統觀念已經發生了轉變。

# 低估「商用」惡意軟體的後果

並非每個人都受到民族國家發起的進階型持續威脅 (APT) 的零時差弱點攻擊。大多數攻擊都是利用一般方式傳播普通惡意軟體，通常是垃圾郵件、外表看似沒有問題的附件或連結，並盡量鼓勵目標開啟該附件。Sophos 每月會收到數千起此類常見惡意軟體的遙測結果，通常表明受我們產品保護的電腦已經阻止了該起攻擊。

在惡意軟體完全取得控制權的未受保護電腦中，它將解析目標電腦；擷取任何登入憑證或儲存的密碼以控制某些有價值的網站 (通常但不限於銀行或金融服務帳戶)；然後將該資訊發送回給背後的操作者，並等待進一步說明，這些說明可能會在幾秒鐘內或幾天後送達。

但是，不要認為這些惡意軟體的能耐**就只有這樣**，而陷入一種錯誤的安全感。如果讓這些惡意威脅持續存在，它們可能會引起更大的問題。如前面的報告所述，SophosLabs 團隊維護著一份「頭號通緝犯」惡意軟體列表，分析人員將專心研究那些頑固存在的系列。以下我們整理了部分惡意軟體的簡短摘要。

### Dridex 和 Zloader

**最常見的惡意軟體類型之一是載入程式 (loader)。**載入程式的功能主要是幫操作者或與操作者簽約的人員，交付另一種惡意軟體裝載。Dridex 和 Zloader 惡意軟體系列都是成熟、歷史悠久的載入程式平台。攻擊者同時使用 Dridex 和 Zloader 收集遭鎖定系統的資訊，並將其回傳給犯罪分子，犯罪分子可以根據殭屍程式回傳的資訊，從容地決定將提供哪些元件或裝載。

Dridex 載入程式的核心功能是聯繫其命令和控制 (C2) 伺服器，取得一或多個加密的裝載，然後進行部署。對於分析人員來說，攔截這些裝載非常困難，因為威脅執行者只會根據需要散佈它們，例如隱藏的 VNC (一個遠端控制應用程式) 或 SOCKS 代理伺服器。這些裝載使攻擊者能夠針對使用者裝置的相關內容執行動作。它們還能讓犯罪分子接觸到受害者系統上無法直接由系統存取的資源。

判斷感染期間發生什麼情況的伺服器端邏輯可能比較難懂，但是我們可以推斷出一些規則，因為這些殭屍程式不想感染惡意軟體分析人員使用的電腦。該殭屍程式會向其操作員發送已安裝程式的列表。如果該電腦有分析工具或虛擬機器元件存在，殭屍程式就不會向它傳遞裝載。在 Zloader 的情況中，殭屍程式操作員會透過垃圾郵件傳播惡意軟體；如果您花了太長時間感染電腦，則在垃圾郵件送出後的 8 到 12 小時內，它們就會停止發送裝載。

它也必須是一台真正乾淨的電腦，但也不能太乾淨。普通的 Windows 電腦不會中毒，帶有很多工具的全方位電腦也不會中毒。

## Agent Tesla 和 RATicate，Infostealer 和 RAT

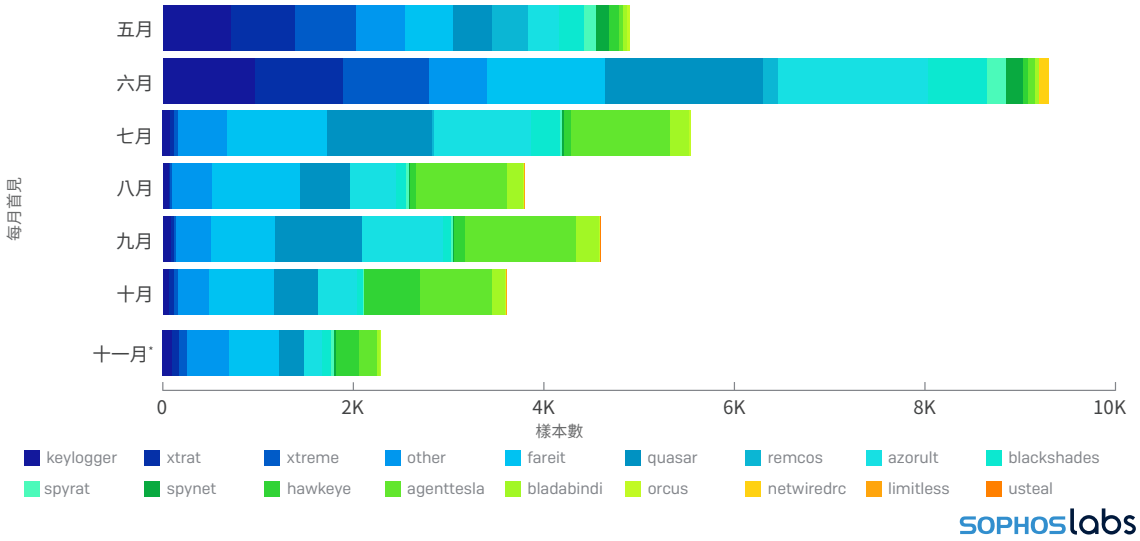



圖 5。我們利用內部沙箱系統執行所有新發現的遠端存取木馬程式 (RAT) 惡意軟體。該表說明我們在 7 個月內遇到了多少個新的獨特樣本，我們後來將其分類為 18 個最常見的 RAT 系列，並按系列名稱分類。*部分月份資料。來源：SophosLabs。

**遠端訪問木馬程式 (或稱 RAT)，以及資訊竊取軟體 (Infostealer) 是最古老的惡意軟體形式**。顧名思義，RAT 使攻擊者能夠遠端控制受感染的電腦。資訊竊取軟體還會盜用它們的名稱，竊取和外洩憑證以及其他敏感資訊。在過去的一年中，我們處理過的兩個「頭號通緝犯」系列是 Agent Tesla (一個資訊竊取軟體) 和 RATicate (一個 RAT)。

像載入程式一樣，RAT 通常也具有一種機制，以便可以傳遞其他裝載，包括自身的更新版本。我們觀察到 RATicate 會分發其他惡意軟體，包括 Agent Tesla。我們還看到這些 RAT 系列由相同的 IP 地址或伺服器提供服務或與之通訊，暗示本來彼此不相關的集團共用了某些東西。

## Trickbot 被擊落了

Trickbot 一直是一種令人討厭的持續性惡意軟體，至少出現四年了。這個惡名昭彰的殭屍網路首創了許多現在常見的行為和特徵：例如它使用 TLS 與 C2 基礎結構進行通訊。該殭屍程式和幾起備受矚目的勒索軟體攻擊有關，而且本身就具有竊取憑證的能力。

```
    "type"   :  "TEXT",
    "size"   :  101
},
"controllers"   :  [   {
   "url"   :  "https://127.0.0.1.1"
}  ],
"controllers"   :  {
```

SOPHOSlabs

圖 6。Trickbot 被一行程式碼擊落。來源：SophosLabs。

2020 年 10 月，在我們準備本報告時，Microsoft 和美國司法部宣布他們已經奪取了幾台伺服器，並透過殭屍網路的命令和控制系統發送了一個命令，使大約 90% 的殭屍網路停止與該命令和控制基礎架構進行通訊。

調查人員設法將「有毒」的設定上傳到每個殭屍程式下載的 Trickbot 基礎架構中。該設定會欺騙殭屍網路，使其認為它主要的命令和控制伺服器就是它正在其上運作的受感染電腦。殭屍網路隨後與真正的 C2 伺服器失去聯繫，無法再取得裝載或指令。

這個動作對 Trickbot 背後的操作員產生巨大的影響，但他們應該會慢慢地恢復正常運作。

# 遞送機制

惡意軟體或攻擊者可以經由多種方式存取目標電腦或滲透網路。大多數惡意軟體攻擊都是使用老方法，包括使用包含惡意檔案連結或附件的電子郵件，或者攻擊者會針對 RDP 或網路邊界上面對網際網路的其他易受攻擊服務，採取更積極的行為。

### RDP，勒索軟體的第一大攻擊媒介

Windows 遠端桌面通訊協定 (RDP) 是目前所有 Windows 版本中都有提供的標準服務。IT 系統管理員或電腦使用者只需花費很少的精力，就可以利用 RDP 在不實際接觸電腦的情況下登入電腦，這在疫情期間非常有用，因為每個人都突然被迫在家中工作。不幸的是，在過去三年中，勒索軟體威脅執行者一直濫用同樣的遠端存取平台來入侵網路並為企業造成大規模破壞 (且速度不斷加快)，進而從被鎖定的組織那裡獲得越來越多的收益。

### RDP 試圖登入每個誘捕系統

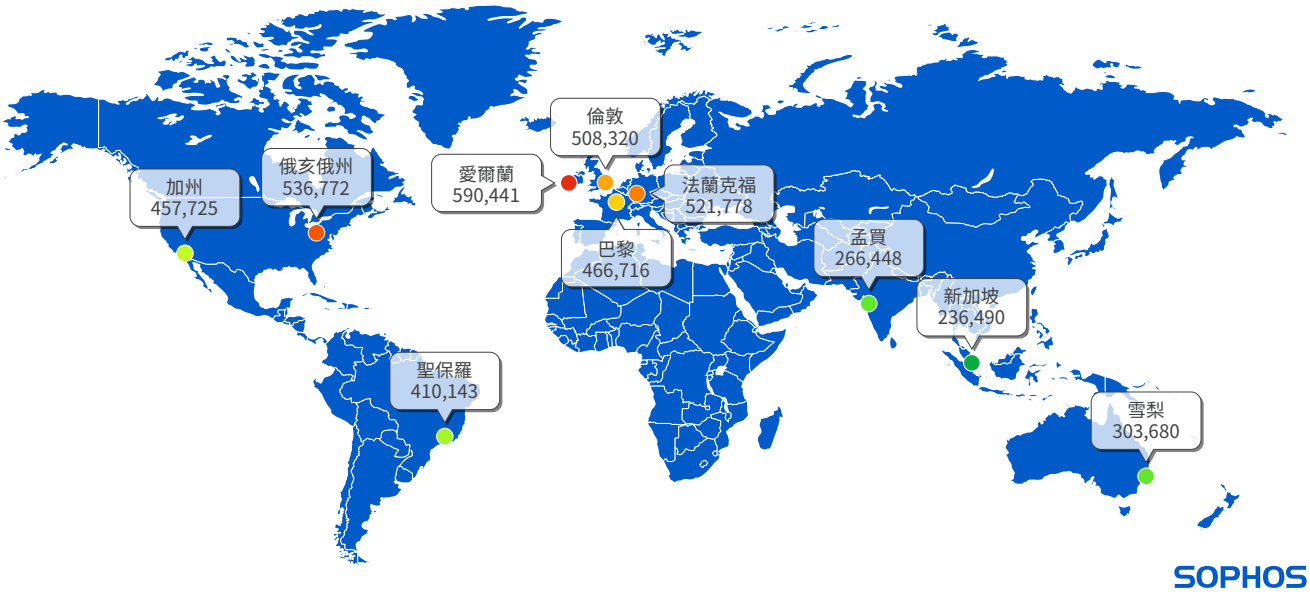



圖 7。我們向世界各地的資料中心提供了誘捕系統，並允許攻擊者進行暴力攻擊。誘捕系統機器被認為是資料中心組織的一部份，沒有以任何方式表明身分。此圖說明在測試的一個月期間，每個誘捕系統位置受到了多少次攻擊。

COVID-19 封鎖期間的影響只會加劇這個問題，因為越來越多的組織和員工因環境而不得不依靠 RDP 來保持運作。主要風險在於，RDP 設計時並未考量承受來自公眾網際網路的猛烈攻擊。如果 RDP 密碼不夠強，容易被自動登入嘗試猜中或暴力破解，攻擊者就會在網路中立足並可以為所欲為。

根據回應重大事件的 Sophos 團隊回報，RDP 仍然是所處理的勒索軟體事件的首要「根本原因」之一。給 IT 管理員的建議與以往一樣：RDP 永遠不應對公共網際網路開放，而應置於使用者必須用 VPN 或其他零信任設施進行連線的防火牆後面；此外系統管理員應加強 Windows 密碼原則，並要求使用更長的密碼和多因素驗證權杖或 App。

在疫情封鎖之前所進行的研究中，Sophos 在全球 10 個資料中心架設了誘捕系統，以更加了解問題的嚴重程度。在 30 天內，誘捕系統平均遭到 467,000 次 RDP 登入嘗試，或每個位置每小時 600 次。研究表明，攻擊每個誘捕系統的登入嘗試頻率和兇猛程度都不斷增加，直到我們拔掉插頭為止。

### 所有失敗登入嘗試中使用的前五個使用者名稱

| 使用者名稱 | 失敗的登入嘗試 |
|---|---|
| administrator | 2,647,428 |
| admin | 376,206 |
| user | 79,384 |
| ssm-user | 53,447 |
| test | 42,117 |

圖 8。遠端桌面暴力破解嘗試會鎖定最常見的 Windows 使用者名稱，包括預設的「administrator」帳戶。

來源：SophosLabs。

### 商業電子郵件洩漏和商業電子郵件詐騙

商業電子郵件洩漏 (BEC) 是一種特定垃圾郵件的正式名稱，該垃圾郵件以詐欺性的金錢要求為中心。在 BEC 攻擊中，垃圾郵件製造者發送的郵件看起來像是來自公司內部的高階主管，指示層級較低的某人執行某種財務轉移或代表該名主管完成大筆交易。攻擊者可以透過偽裝內部電子郵件的外觀來進行這項操作 (有時稱為「企業電子郵件詐騙」(Business Email Spoofing)，或者會嘗試控制組織自己郵件伺服器上的帳戶，然後使用該帳戶來發送詐騙請求。

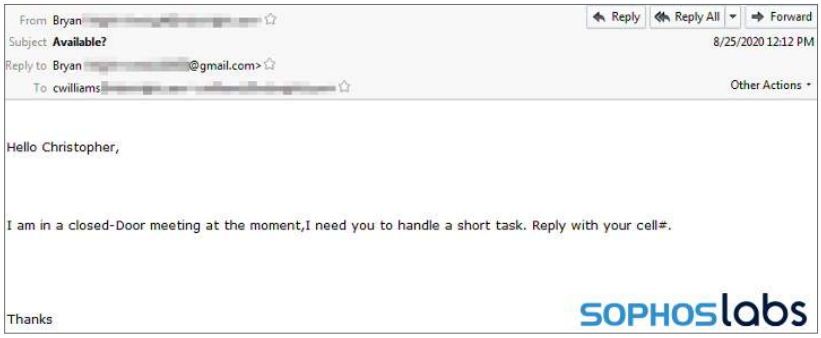



圖 9。在這個企業電子郵件洩露的真實範例中，詐騙者冒充高階主管要求員工回應他的緊急請求。電子郵件的回覆地址 (Gmail 帳戶) 與寄件者標頭中的地址不同，如果收件者細看郵件標頭，則該郵件漏洞百出。來源：SophosLabs。

BEC 攻擊者會冒充高階主管，要求被鎖定的員工購買昂貴的禮品卡或加快某種金融交易。攻擊通常是針對被鎖定的個人和組織而來的。BEC 電子郵件看起來不像是惡意垃圾郵件，因為它們不採用類似垃圾郵件的模式。它們 (通常) 不包含附件或惡意連結，並且看起來好像來自被鎖定的組織內部，有時甚至包含組織的典型郵件「簽名檔」或其他員工可以辨認的元素，使其比傳統的惡意垃圾郵件更具說服力。

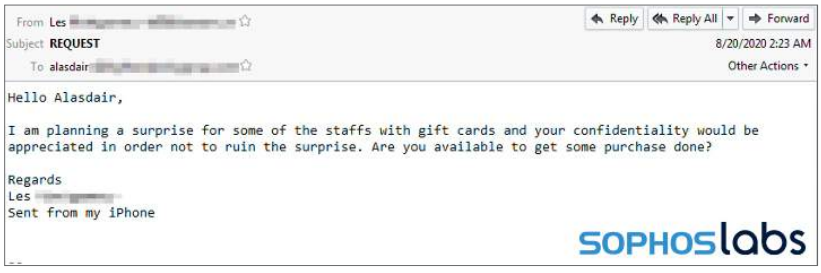



圖 10。在被鎖定者確認初始請求後，詐騙分子會提供聽起來合理的藉口開始「要求」。來源：SophosLabs。

BEC 詐騙是利用被詐騙的目標 (員工) 與詐騙寄件人 (高階主管) 在實體上相距甚遠，而且還必須取決於被鎖定者是否能快速行動，在任何人知道發生了什麼事並阻止被鎖定者前購買禮品卡或進行銀行轉帳。當 BEC 詐騙分子知道高階主管不在辦公室時，他們可能會偽造一個假訊息。

這些詐騙請求通常會在攻擊者與被鎖定者之間來回幾趟。對話一開始可能是對被鎖定者提出簡單請求，讓他回應詐騙者，並演變成一系列的訊息，最終再用合理的藉口「要求」進行購買。


圖 11。在攻擊過程中的某個時間點，BEC 詐騙者會發出一個反常的要求，例如突然大筆金額轉帳給一個被鎖定者不熟悉的帳戶。因此，警覺性高的員工將有再一次質疑請求的機會：既然是要送出的禮品，高階主管為什麼要在禮品卡背面加上相片，並刮掉 PIN 碼？來源：SophosLabs。

回到我們大多數人在辦公室工作的場景，被鎖定者和寄件者之間的實體距離會讓詐騙無所遁形。但是，在我們目前的分散式工作環境中，高階主管和員工不太可能處於同一個實體地點，這減少了人們走到主管辦公桌並確認請求的機會。

BEC 詐騙在 COVID-19 之前就已存在，但是隨著越來越多人採取遠距工作，BEC 騙局正蠢蠢欲動。這種攻擊利用人們希望幫助他人的天性，是一種特別令人反感的詐騙手法。如果您遇到此類電子郵件，請相信自己的直覺，並儘可能直接洽詢對方，或者如果無法聯繫到他們，則應尋求他人的指示。處理這些請求時員工的真實性越高，在造成任何損害之前就更可能發現該騙局。

### 怪異的科學：復古的 Office 臭蟲再次來襲

談到惡意 Office 文件以及它們試圖使用的漏洞利用攻擊時，老方法通常會被反覆利用，它們在 Microsoft 推出更新後消失，然後 (有時) 又浮出水面。多年來，SophosLabs 一直追蹤攻擊者如何在惡意文件中崁入各種快速變化的漏洞利用技術。使用惡意文件當成惡意軟體裝載跳板的犯罪分子大多偏愛新近被揭露的弱點，因為並非每個人都會立即安裝修補程式，而且有時安全公司需要花一些時間，根據新載體的行為或其他特徵來建立有效的「安全網」。

我們在過去一年中見過的大多數惡意文件，都是使用稱為建構器 (builder) 的工具產生的，該工具為攻擊者提供一個真正的點擊式選單系統，使他們可以準確選擇要在惡意文件裡使用哪些漏洞利用技術。目前端點保護工具能夠更有效地識別出這些較現代的漏洞利用技術，因為它們通常是在文件中嵌入指令碼。惡意文件開發者似乎更加深入，找出了一個非常老的漏洞，能幫助隱藏檔案中的巨集或其他惡意內容。

該漏洞俗稱 **VelvetSweatshop**，儘管它實際上根本不是漏洞。實際上，Microsoft 在 Microsift Office 2003 就有 VelvetSweatshop，儘管直到 2013 年才發現它被濫用，當時這個瑕疵被用於協助 Excel 工作簿攻擊 CVE-2012-0158 弱點。標記為「唯讀」的 Excel 工作表或 Word .doc 檔只是一個受密碼保護的文件，內建密碼為 VelvetSweatshop。

今年，我們看到了許多惡意的 Excel 工作表，這些工作表使用該技術來逃避進階型威脅偵測。由於經過加密，真正的惡意內容被隱藏在強大的加密技術後面，掃描程式無法破解、也無法掃描它，除非支援攻擊者使用的最新演算法。由於其使用了預設密碼，因此 Excel 會在不提示輸入密碼的情況下開啟解碼後的內容，因此從執行的角度來看，其根本沒有加密。端點安全程式新增支援加密和預設密碼，但犯罪分子一直在尋找具有相同功能且尚未被防毒掃描程式實作的其他加密演算法。

發現這個夠老的程式錯誤真是令人驚訝，用人類做比喻，就好比是上學的最後一年。但是，將其武器化的文件製造者嘗試利用它也就不足為奇了。

# 資訊安全：二十年回顧

年度報告使我們有機會回顧過去一年中的重大事件，但我們認為，回顧過去的二十年，能為我們為什麼走到今日的威脅環境提供背景資訊。千禧年象徵著一個里程碑，那時資訊安全已成為一門專業學科和真正的產業。威脅和事件的時間序，代表了威脅行為演變過程中重要且具有代表性的時刻。

隨著企業和個人都將網際網路用於商業和娛樂，大型網路已成為多種新興蠕蟲 (自我傳播的惡意軟體) 的垂涎目標。蠕蟲累計感染了全球數千萬個系統，損失和補救成本超過 1,000 億美元。

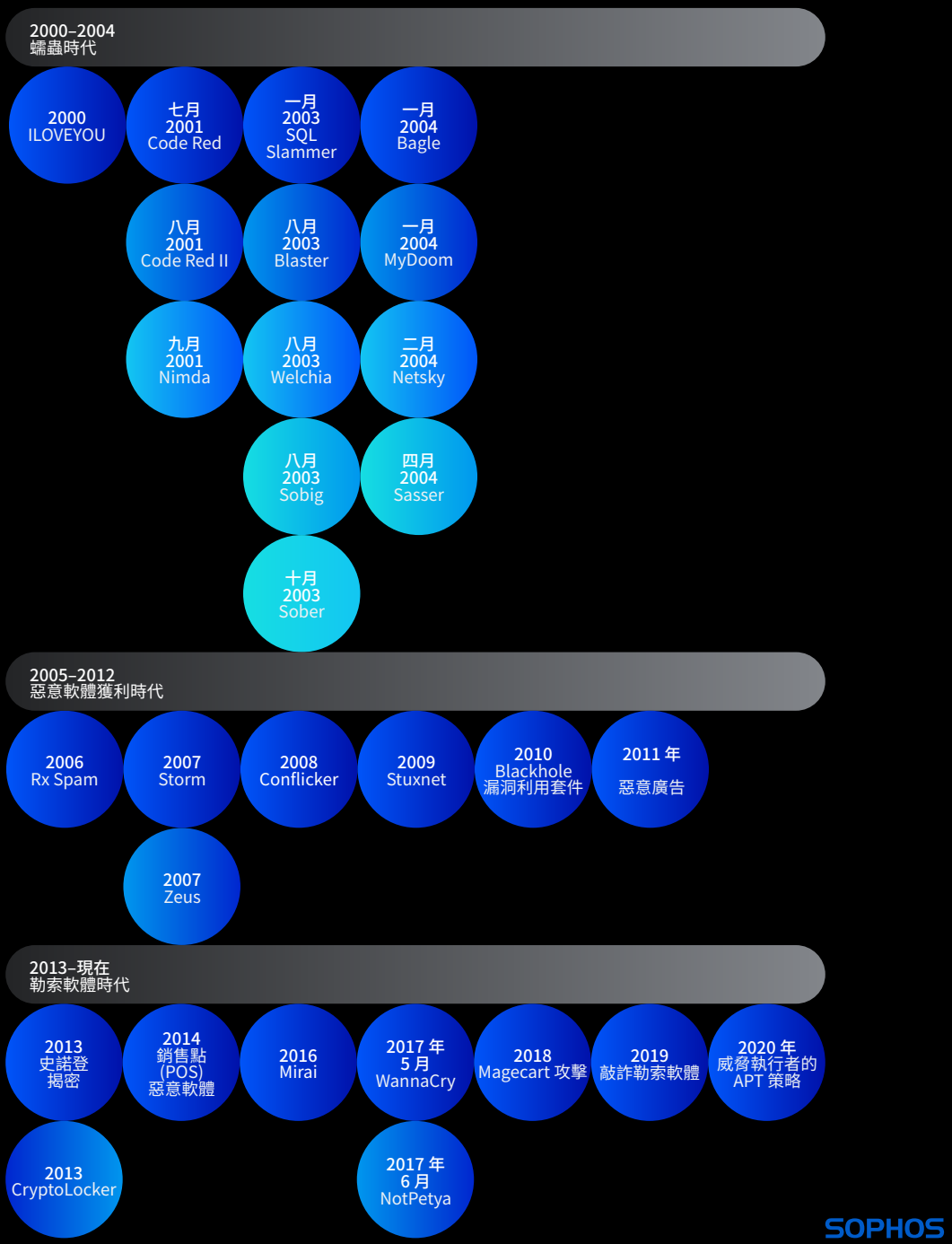



圖 12。來源：Sophos

## 2000-2004 年 - 蠕蟲時代

### 2000 年 - ILOVEYOU
ILOVEYOU 蠕蟲使用了一種社交工程技巧，而這種技巧一直持續到今天：它以垃圾郵件附件的形式出現，最終感染了 10% 的與網際網路連線的 Windows 電腦。

### 2001 年 7 月 - CodeRed
CodeRed 以當時發現者正在喝的 Mountain Dew (百事公司旗下碳酸飲料品牌) 的一種口味命名，該威脅使用 IIS 中的緩衝區溢出弱點傳播自己並破壞網站。一個月後它發布升級版本，該版本會在連線到網路的電腦上安裝後門程式。

### 2001 年 8 月 - CodeRed II

### 2001 年 9 月 - Nimda

### 2003 年 1 月 - SQL Slammer
Slammer 只佔 376 個位元組，利用了 Microsoft 資料庫應用程式中的緩衝區溢出漏洞。每隔 8.5 秒，Slammer 的感染電腦數就增加一倍，僅 15 分鐘就使網際網路大規模癱瘓。

### 2003 年 8 月 - Blaster
Blaster 是在第一個 Patch Tuesday 之前幾個月，對一個 Microsoft 修補程式進行反向工程而開發的。它利用了 Windows XP 和 2000 系統 RPC 服務中的緩衝區溢出弱點。如果某天在該月份中大於 15，或者該月份是 9 月或更晚，則對 Windowsupdate.com 發起 DDoS 攻擊。

### 2003 年 8 月 - Welchia

### 2003 年 8 月 - Sobig

### 2003 年 10 月 - Sober

### 2004 年 1 月 - Bagle

### 2004 年 1 月 - MyDoom
據估計，在 2004 年發送的所有電子郵件中，有 25% 源自 MyDoom 蠕蟲。該蠕蟲透過電子郵件將自己發送給新的受害者，並涉及一次阻斷服務 (DDoS) 攻擊。

### 2004 年 2 月 - Netsky

### 2004 年 4 月 - Sasser

## 2005-2012 年 - 惡意軟體獲利時代
直到 2005 年左右，惡意軟體事件才被歸於好奇心或破壞。專為隱匿和牟利的殭屍網路惡意軟體佔了主導地位。這個時代也看到了所謂的藥品垃圾郵件的開始。鎖定軟體弱點的漏洞利用成為惡意軟體的關鍵部分，進而造成惡意廣告行為。只要有可能牟利，網路犯罪分子就會利用這些機會。

### 2006 年 – Rx 垃圾郵件
原來是一種單純的騷擾 (或是傳播蠕蟲的一種方式)，演變成一種利潤豐厚的業務，主要是銷售透過垃圾郵件宣傳假的處方藥。據估計，藥品垃圾郵件發送者僅賣藥就可以賺到數十億美元，而其實大多數人只要去看醫生都可以買到這些藥品。

### 2007 年 - Storm

### 2007 年 - Zeus

### 2008 年 - Conficker
Conficker 迅速感染了全球數百萬台電腦，但並沒有造成太大損害。我們仍然不知道蠕蟲的真正用途，但是直到今天，仍有數千台主機受到感染，並且 Conficker 的掃描流量通常會被偵測為網際網路「背景輻射」的一部分。

### 2009 年 - Stuxnet
Stuxnet 是首批針對實體系統的一種數位武器：伊朗用於濃縮鈾的核濃縮離心機。Stuxnet 不可磨滅的影響，是它永久打開了民族國家將惡意軟體用作戰爭工具的大門。

### 2010 年 - Blackhole 漏洞利用工具套件
漏洞利用工具套件 (針對軟體弱點的工具套件) 將網路犯罪生態系統的不同部分結合在一起。Blackhole 漏洞利用工具套件的開發者開始提供服務時，犯罪軟體即服務 (Crimeware-as-a-Service) 就誕生了。

### 2011 年 - 惡意廣告

## 2013 年至今 - 勒索軟體時代
勒索軟體對這個時代產生了最深遠的影響。儘管蠕蟲、銀行木馬程式、惡意廣告和垃圾郵件持續存在，但它們都無法與勒索軟體的破壞力相提並論。在過去七年中，勒索軟體攻擊造成的損失估計達數兆美元。勒索軟體也很可能是與人類死亡相關的第一種惡意軟體。此外，當今的許多威脅最終都會使用勒索軟體，並且像漏洞利用工具套件一樣，它為已經非常繁榮的網路犯罪生態系統提供了氮氣加速器般的助力。

### 2013 年 - 史諾登揭密

### 2013 年 - CryptoLocker
在其短暫的出現時間裡，CryptoLocker 將兩種現有技術 (加密和加密貨幣) 結合，為未來的犯罪分子提供了一個成功的解決方案。CryptoLocker 永遠改變了威脅狀態，其餘震到今天仍然存在。出現三個月後，CryptoLocker 使用的比特幣錢包進帳了將近 3,000 萬美元。

### 2014 年 - 銷售點 (POS) 惡意軟體

### 2016 年 - Miral

### 2017 年 5 月 - WannaCry
WannaCry 是散播最廣的勒索軟體 - 蠕蟲病毒混合體，(再次) 證明了沒有及時修補會帶來可怕的後果。它使用竊取自美國國家安全局 (NSA) 並由 The Shadow Brokers 公開發布的漏洞利用技術。該攻擊迫使 Microsoft 發行了未受支援產品的專屬更新。

### 2017 年 6 月 - NotPetya
NotPetya 打擊了一些全球最大的航運和物流公司，據說造成超過 100 億美元的損失。一些受影響的公司尚未完全復原。

### 2018 年 - Magecart 攻擊

### 2019 年 - Extortion 勒索軟體
在對南非約翰尼斯堡市的一次攻擊中，Maze 勒索軟體的犯罪分子率先使用了敲詐的手段。他們不僅加密和竊取了資料，而且還威脅要在公司不付款的情況下公布被竊的資料。這個手法已被許多其他勒索軟體同業複製，用來攻擊擁有良好備份的受害者。

### 2020 年 - 威脅執行者的 APT 策略
過去幾年開始採用民族國家的工具和策略，到 2020 年時成為主流。專業的網路犯罪集團使用複雜的工具 (例如 Cobalt Strike) 來達到毀滅性的效果，而某些集團 (Dharma) 則將其改良成傻瓜工具套件，以供新手使用。

# 將 COVID-19 視為攻擊的戰力加乘因子

新型冠狀病毒 (COVID-19) 極大幅度地影響了網路安全的各個方面。攻擊者竟然還大膽地鎖定了剛到家的上班族。公眾領域已經充滿了焦慮和恐懼，而頻繁的垃圾郵件活動、勒索軟體鎖定已有資金壓力的脆弱或倒閉的機構或個人，以及因個人防護設備到衛生紙都缺乏而出現的租借詐騙和牟利等行為，都使得這種情況加劇。

# 家是新的邊界

正常的生活在 2020 年 3 月結束，當時可以遠距工作的員工和幾乎所有年紀的學生都被瘋狂送回家，以阻止 COVID-19 傳播並緩解醫院病患過多的壓力。突然之間，我們在家工作不完全是為生活而工作。

許多人在沒有上下班的情況下努力尋找新的常態。對 VPN 存取和多因素驗證服務的需求激增。Chromebook 成為搶手商品。Zoom 在兩個月內就出現了大約十年的成長。Microsoft、Adobe、Apple 和 Google 都透過各種方式發布了多個平台的更新和維護修補程式版本。

### COVID-19 和新冠病毒電子郵件騙局的興起

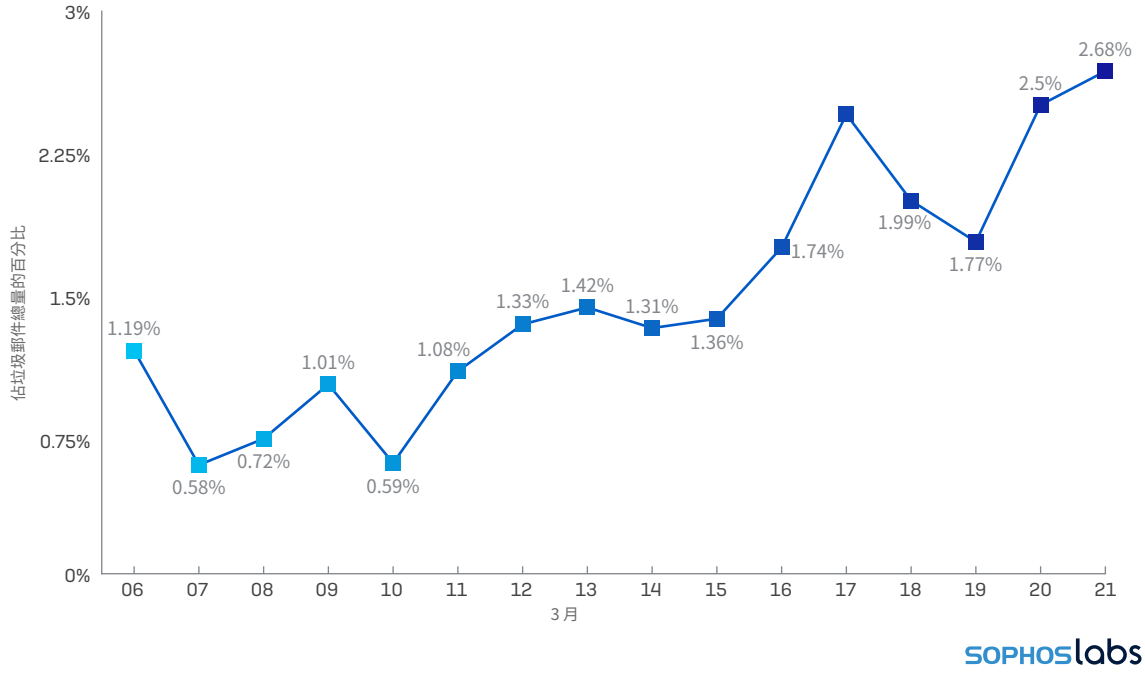



圖 13。在全球封鎖後的幾週內，大量垃圾郵件中都提到了 COVID-19 或 Coronavirus (新冠病毒)。來源：SophosLabs。

COVID-19 使我們所有人都成了自己的 IT 部門，得要管理修補程式、安全更新和連線問題，以防我們無法參加會議或孩子們無法參加虛擬教室。網路和端點上對耳機、麥克風、更好的照明以及安全性的需求激增。這意味著即使是年幼的孩童，也應該接受速成課程，了解網路釣魚、垃圾郵件、網路酸民、網路霸凌，以及偽裝成立即可玩且免費的受歡迎遊戲的惡意軟體。

這並不容易，我們仍然沒有回復到像 2020 年 2 月那樣的正常運作，但是許多人發現，從某種意義上說，新常態可能會是一個進步。越來越多的辦公室決定，即使在封鎖結束後仍持續採取遠距工作，讓人們可以返回職場，這將對環境和人們的生活品質都有很大的好處。

隨著工作場所範圍擴大和擴展以涵蓋偏遠地區的大部份員工，情況會變得更加嚴峻，我們必須將家庭網路視為最後一道防線。客廳櫥櫃裡的數據機現在成了網路邊界。我們需要重新思考如何為這種結構提供深度的防禦。

# 犯罪軟體即服務

為了幫助理解，您可以將惡意軟體製造者視為一種軟體新創公司。一開始雜亂無章，但成功的開發者最終會贏得忠實的追隨者。惡意軟體的商業模式可能與合法軟體一樣多。

這裡我們故意使用「犯罪軟體」這個比較寬鬆的詞；某些惡意軟體開發者或是使惡意軟體易於交付或透過新功能增強的工具開發者，並不是直接出售產品，而是採取授權，就好像您可能會購買 Adobe Creative Suite 的年度授權一樣。我們稱這類商業模型為「犯罪軟體即服務」(CaaS)，而它似乎已成為新常態。

Emotet 是 CaaS 惡意軟體最惡名昭彰的例子之一。傳遞垃圾郵件的木馬程式已經存在多年，並調整成可為可能犯罪者提供平穩的操作為核心。Emotet 是安全研究人員統稱為載入程式的惡意軟體類型之一。Emotet 主要用途是將其他惡意軟體傳播到被鎖定的電腦。它透過一個複雜的網路來完成這項工作，將武器化的垃圾郵件散佈到大量目標。

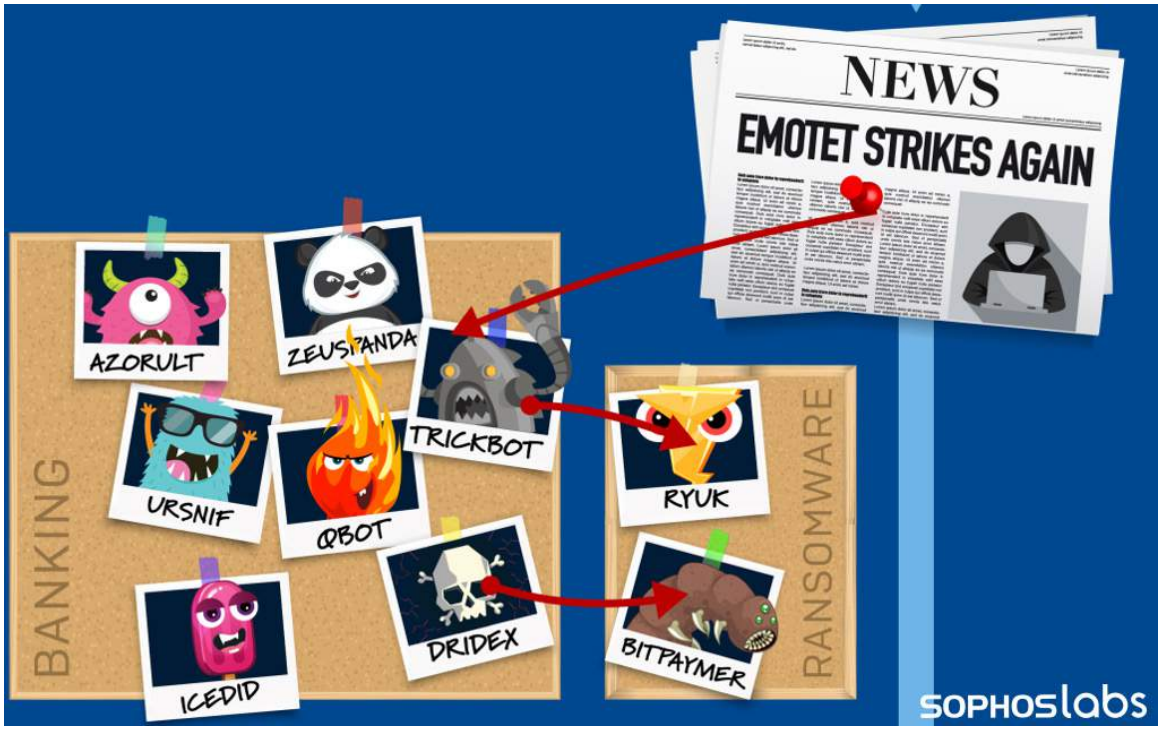



圖 14。來源：SophosLabs。

然而，今年以來，Emotet 經歷過兩個黑暗時期。在最近 5 個月內，該惡意軟體一直與 C2 伺服器保持通訊，在此期間，通常內含攻擊的垃圾郵件完全消失了。七月，發送 Emotet 的垃圾郵件又神祕地恢復了。

Dharma 勒索軟體是另一個有名的 CaaS 惡意軟體。與其他贖金更高的勒索軟體不同，Dharma 維持固定的小額贖金。原因是因為 Dharma 的商業模式：這是一款輔助性質的勒索軟體，適用於需要幫手的犯罪分子。這些犯罪分子要繳交基本的訂閱費用，便可以從 Dharma 開發者那裡獲得裝載，並與他們一起分享任何攻擊所得。

隨著攻擊者擴展成專業分工，犯罪分子與獨立承包商、自由工作者和相關機構合作的商業模式似乎不會很快消失。

# 垃圾郵件、詐騙和違約事件

全球各地封鎖後，接踵而來的是大量的垃圾郵件詐騙行為。如果時機正確，最有效的垃圾郵件活動會造成急迫感，促使收件者對郵件採取行動。這是一種眾所周知的心理技巧，因為如果您仔細看一下垃圾郵件的內容，可能就會發現它是偽造的。如果垃圾郵件發送者觸發了恐懼反應，那麼您還沒有思考就會採取行動，然後陷入陷阱。

COVID-19 已經讓所有人都繃緊神經，因此垃圾郵件發送者甚至無需特別費力。

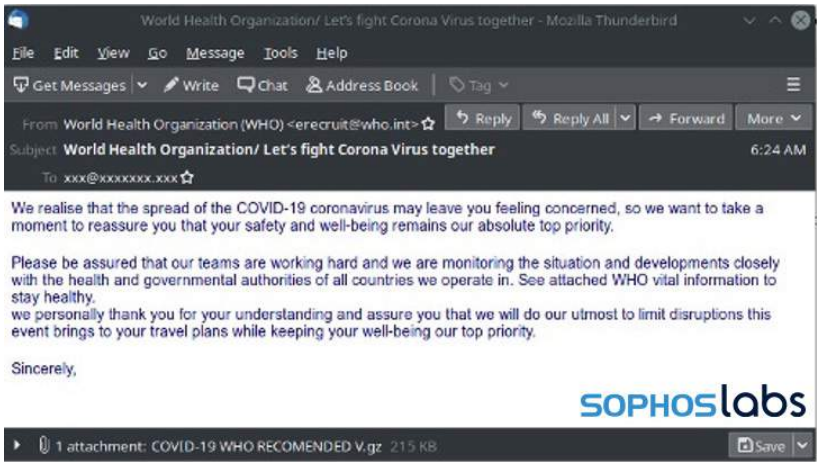



圖 15◦來源：SophosLabs◦

在封鎖的幾週後，我們決定仔細研究另一種出現成長的現象：網域註冊。在幾週內，人們每天註冊了成千上萬個新網域名稱，其中包含字串 COVID-19、Corona 或 virus 的任意組合。

| Domain | First Seen | Nameserver | Ns Ip |
|---|---|---|---|
| coronavirusshaquilleoneal.com | 2020-03-14 07:00:38 | ns-cloud-b1.googledomains.com | 216.239.32.107 |

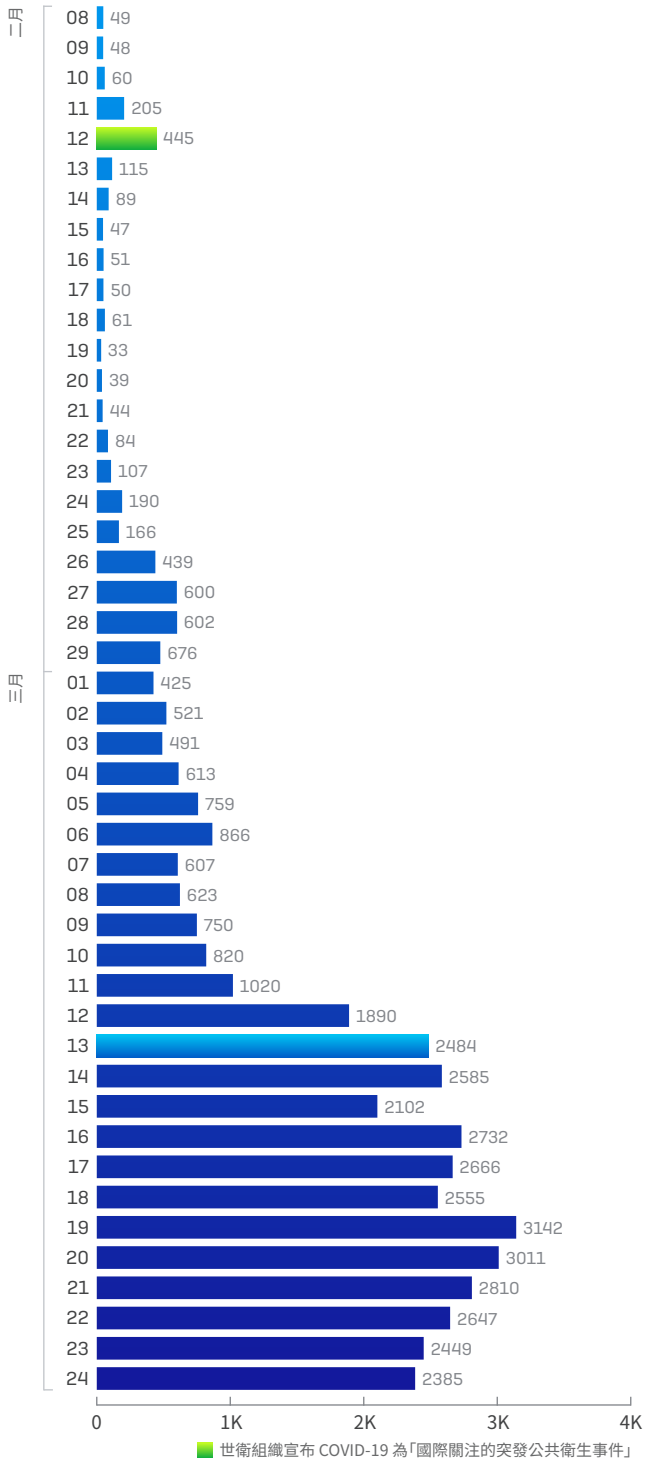
SOPHOSlabs

圖 16◦來源：SophosLabs◦

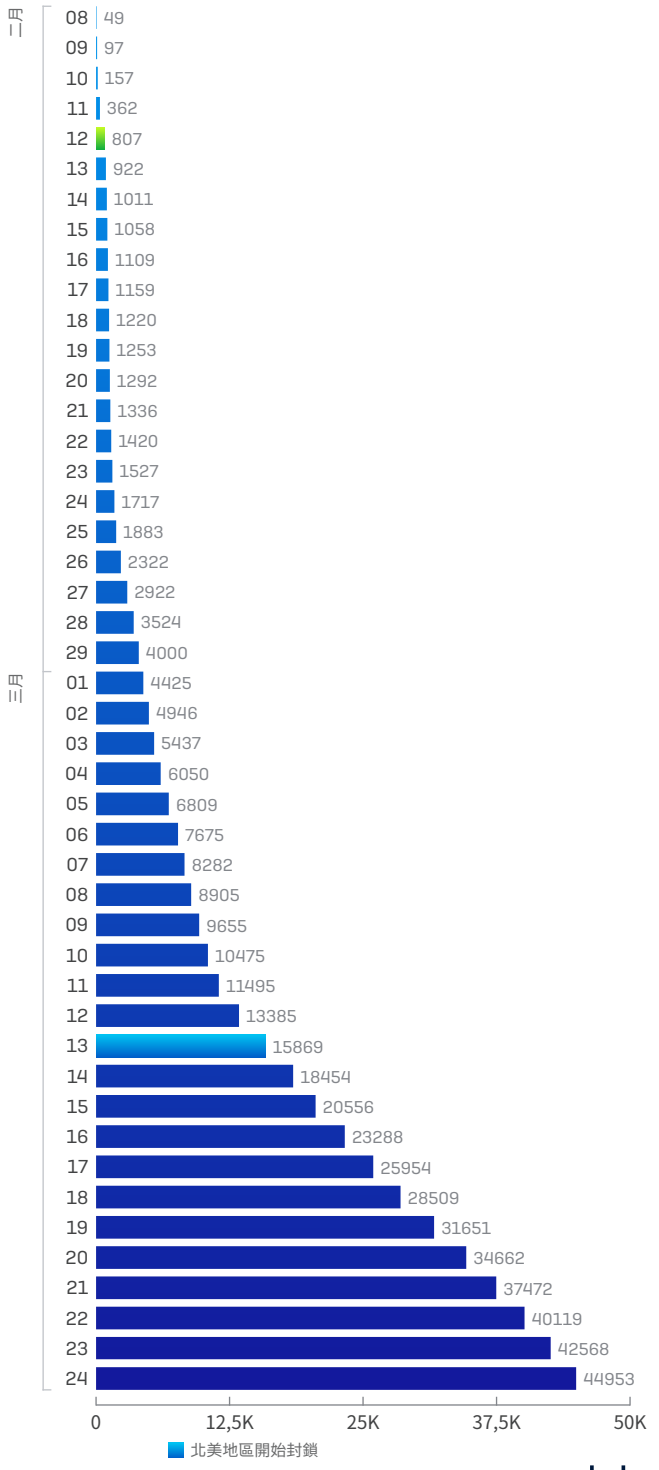
其中一些網站明顯就是笑話，而另一些則與合法、區域或國家衛生當局使用的網站非常相似。

我們還在 TLS 憑證透明度日誌中尋找和 COVID-19 相關的網域和子網域。憑證透明度日誌，在追蹤擁有自己的 TLS 憑證 (未顯示在原始網域註冊資料中的資訊) 和網域名稱的子網域時非常有用。

**每天新註冊的 COVID 網域**




**到目前為止，新註冊的 COVID 網域總數**




SOPHOSlabs

圖 17。在 COVID-19 危機爆發的最初幾個月中，人們每天註冊數千個網域，並盡可能取得 TLS 憑證的授權，名稱包含字串「COVID-19」或「corona」。來源：SophosLabs。

## 每月使用「COVID-19」或「Corona」主機名稱的新 TLS 憑證

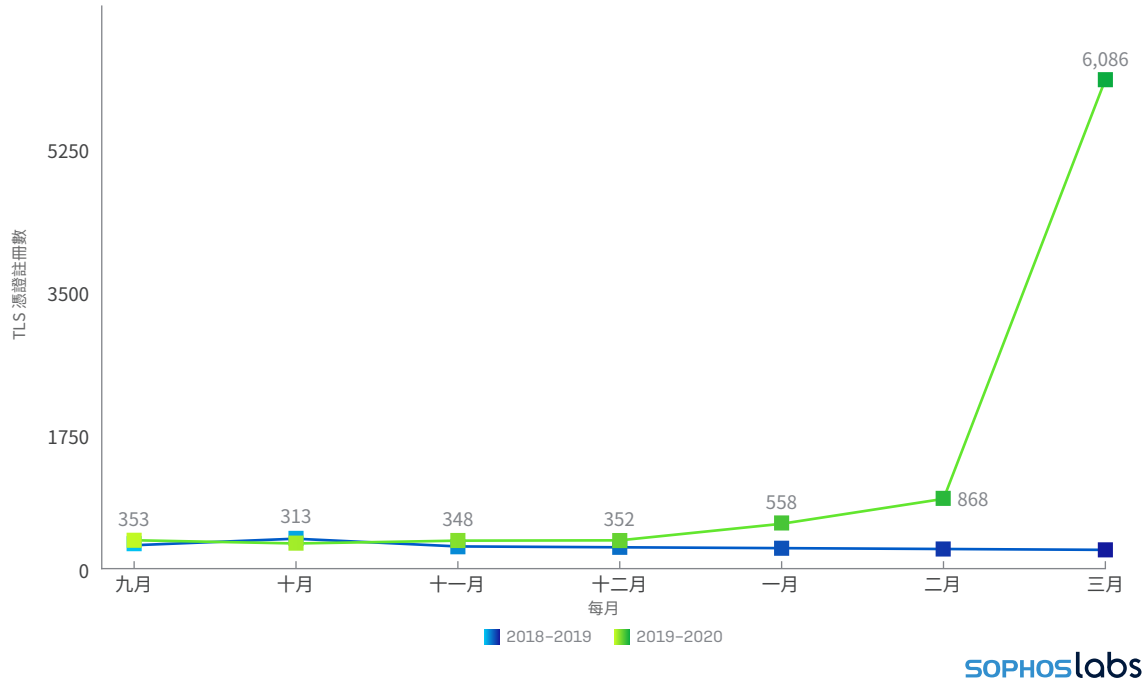



圖 18。同一時間，和疫情有關的 TLS 憑證註冊與網域註冊都暴增。來源：SophosLabs。

在三月，我們每天看到平均有 200 多個 COVID-19 網域的憑證請求，往後幾個月這個數字還繼續攀升。六月時，平均每天達到 625 個。到了十月，數字達到每天 951 個新 TLS 憑證請求的高峰。

這些網域名稱大多數仍然是合法或良性的，儘管許多網域仍然只是空殼，沒有任何內容，這表明註冊人可能想要「網域作舊」，只是先申請這些網域以供日後進行信譽查核之用。

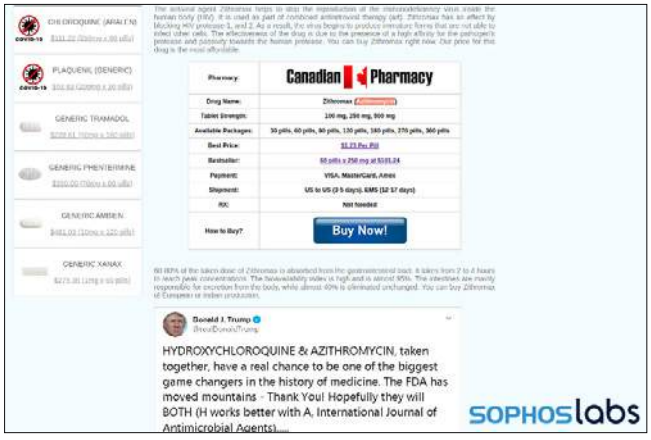



圖 19。即使惡名昭彰的藥丸騙子也無法抗拒 Twitter 帶來的奇蹟療法，甚至還在廣告中發佈推文。

來源：SophosLabs。

一小部分 (低於 1%) 被確定與網路釣魚或惡意軟體相關。許多網域都是短暫的，只有短短一天後就無法解析主機名稱。

# 遠距工作提高了安全雲端運算的重要性

2020 年 3 月開始 COVID-19 封鎖時，人們和工作場所出現了前所未有的快速變化，這個情況一直持續到今天。我們的工作、求學、參加活動和會議以及娛樂自己的方式，都可能永遠都已經改變，雲端運算是支持這種快速發展的基本要件，但它面臨著許多挑戰。

使用權限的過度提供、雲端中資產和資源的可見度有限，以及缺乏審核，都可能使雲端環境更容易受到網路威脅的影響，而惡意軟體對雲端的危害與在其他地方一樣嚴重。例如，加密劫持是雲端中日益嚴重的問題。當運算週期繁重的加密挖礦程式處理序在實體機器上執行並導致電費增加時，這些機器的效能已經很差了。當它們執行雲端執行個體時，不良影響還會更嚴重：雲端提供者會按照虛擬工作站使用的 CPU 週期向被鎖定者收費，這些虛擬工作站會執行大量數學運算來挖出價值幾美分的加密貨幣。

此外，許多分散的遠端員工遭到勒索軟體攻擊的打擊，犯罪分子會以攻擊實體機器的相同方式鎖定雲端基礎架構。畢竟，勒索軟體可以像對實體儲存一樣輕鬆地加密虛擬硬碟或目標的儲存。雲端基礎架構遭受勒索軟體攻擊的組織，不僅會發現自己得支付資料加密所用周期的費用，而且還會遭到勒索。

### 去年遇到安全事件的組織

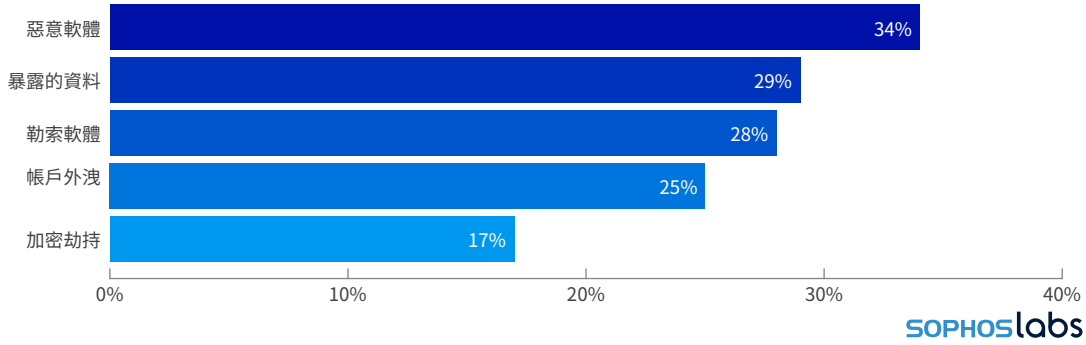



圖 20。在我們的《2020 年雲端安全報告》中，Sophos 針對 3,500 多名IT 專業人員調查了使用雲端的經驗，發現困擾實體網路的許多安全問題已轉化為虛擬問題。來源：SophosLabs。

在鎖定期間，IT 部門需要一種方法來提供虛擬服務台，就像他們在許多工作場所關閉之前為真正的服務台配備人員一樣。COVID-19 要求造成的重大改變分成三波。

在封鎖開始的最初幾週是第一波 (進入波)，開始成形。由於成千上萬的員工突然無法上班，他們需要使用組織環境中的資源，對虛擬私人網路 (VPN) 或使用其他零信任設施的需求快速成長，因此現有資源不堪負荷。除 VPN 之外，組織發現他們需要新增防火牆和其他安全裝置、部署現代化的統一威脅管理系統，以補強由雲端服務提供的基本第 3 層 (Layer 3) 防火牆。

在 COVID-19 之前，由於工作場所的員工數量遠遠超過出差或遠端工作人員，因此 VPN 的使用量是適中的。在三月、五月，然後是六月之後，對於這些員工來說，VPN 成為使組織正常運轉的重要生命線 (如果原本還不是的話)。

但是，這些組織也很快意識到，員工不應在家中使用個人裝置存取 VPN，而且新的筆記型電腦供不應求，對那些已經為分散式員工的 IT 需求而疲於奔命的組織又造成了新的挑戰。由於實體機器不夠，組織轉向虛擬機器看似無限的資源，以滿足對安全運算工作區的需求。此時第二次浪潮開始 - 虛擬桌面浪潮。

隨著越來越多員工轉而使用虛擬的企業桌上型電腦，將這些桌上型電腦託管在雲端的做法既實用又划算，但仍然需要保護。

突然之間，IT 部門必須支援成千上萬個員工的 VM，並突然需要可見度工具來清點和安全地設定不斷增加的虛擬伺服器、虛擬桌面和其他雲端服務的雲端資產，我們稱之為雲端管理浪潮。

### 攻擊時間表


圖 21。我們調查的加密劫持攻擊，一開始是開發人員無意中將雲端憑證嵌入到公共存放庫中的程式碼中。

攻擊者發現這一點，然後使用這些憑據透過本機雲端提供商的 API 進行了攻擊 - 利用數百個 VM 執行個體來挖掘比特幣。同時，它們會自動執行這些執行個體的功能，以使難以終止。後來，他們撤銷了其他合法使用者的使用權限。

來源：SophosLabs。

COVID-19 時代的象徵，就是人類生活的各個方面都發生了巨大的變化，包括從事了多少工作。在路透社最近的一項調查中，接受調查的 97% 的 CEO 和 CTO 表示，封鎖措施加速了他們轉移到新技術的速度。但在預算緊張且充滿不確定性時，這些 CTO 中有三分之二的人表示他們的責任就是盡可能以具成本效益的方式實作這些變更。

在 Sophos 的最新《雲端安全報告》中，我們發現，和雲端運算有關的大多數安全事件均歸結為兩個主要原因，即憑證被盜或被篡改，或是設定錯誤導致出現安全缺口。在接受調查的 3,700 多名 IT 專業人員中，有 70% 的受訪者聲稱他們所支援的雲端基礎架構在調查進行的前 12 個月中曾遭受破壞。

# CCTC 對快速回應大規模威脅的定義


圖 22。來源：Sophos。

Sophos 首席科學家 Joshua Saxe 在開始 COVID-19 封鎖大約一周後，向全球發出了志願者呼籲。這項虛擬冰桶號召迅速組成了 COVID-19 網路威脅聯盟 (CCTC)，該組織有 4,000 多名成員，只為一個目標服務：致力於因應任何利用社會大眾對 COVID-19 的恐懼，無論是名稱或聯想文字，所進行的任何威脅或社交工程行為。

位在美國芝加哥的安全分析師和播客，同樣也是 CCTC 成員的 Nick Espinosa 表示：「我不是消防員，我不知道如何撲滅建築物的火災，但我可以協助一支可以強化關鍵基礎設施 (如醫院) 防禦能力的團隊。」

這是非常必要的努力。從封鎖一開始，攻擊者就不斷散佈垃圾郵件、惡意軟體和各種其他威脅，這些威脅都以一種或另一種形式使用這個令人生懼的最新流行病術語。正如主要報告中所提，每天都有人們註冊數千個新網域，名稱中都包含 COVID-19、corona 或 CoV。Sophos 追蹤已經連線到 TLS 憑證的網域，並在憑證資料中使用上述文字字串比對，發現了數千個符合的結果。

## COVID-19 網路威脅聯盟成員人數成長

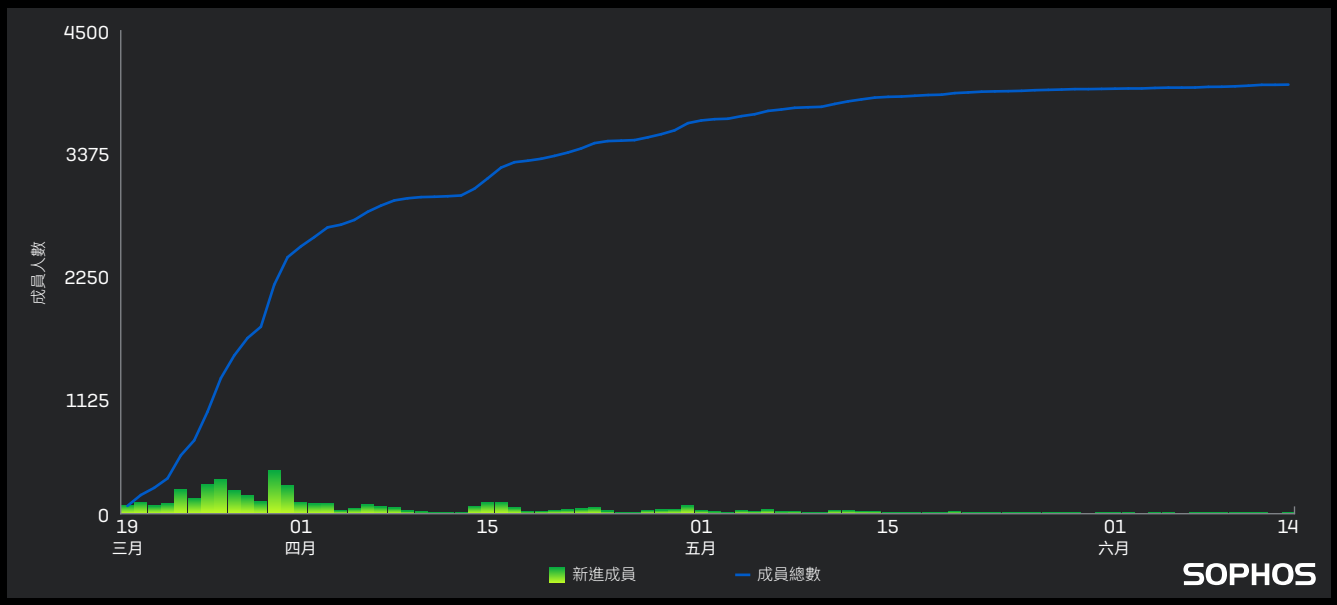



圖 23。來源：Sophos。

由於 COVID-19 所帶來的威脅非常獨特，濫用這一場全球危機的惡意垃圾郵件特別惡劣和具攻擊性。Espinosa 說：「我們發現犯罪分子以 COVID-19 為誘餌，而且入侵呈現爆炸式增加。」垃圾郵件活動迅速增加，垃圾郵件製造者四處散佈來自世界衛生組織、美國疾病預防控制中心、英國 NHS、藥品公司，或美國和英國以外國家/地區的國家衛生部門的官方聲明。

分析人員還看到二進位檔案內的字串引用了 COVID-19，並將其用於離地攻擊 LOLscripts 中的變數。

CCTC 參與者利用匆忙架設的 Slack 共用各種事件的樣本和情報。起初組織有點混亂，但很快就形成了基本結構。Espinosa 說：「這麼多人齊心協力，彙整了如此多的資訊。」

CCTC 的產品 (即收集的輸出) 是情報摘要，列出最新收集的入侵指標 (IoC)。任何人都可以免費使用該資訊。這些 IoC 以不限廠商的方式補強了現有的防禦技術。當 CCTC 與網路威脅聯盟 (Cyber Threat Alliance，CTA) 建立合作夥伴關係時，參與 CTA 的安全廠商即可擷取並防禦這些威脅，以增強 CCTC 威脅情報的保護作用。

Espinosa 認為，安全專業人員為了一個共同目標而快速聯手的這一刻，感覺非常溫馨。他說：「我們一開始可能雜亂無章。」但該團隊很快就自發性地組織起來。CCTC 共用平台的完成意味著，將來需要對如同 COVID-19 的疫情做出反應的任何人都不必從頭開始，可以更輕鬆地應對威脅，用健康方面來比喻，就是類似於一個自我免疫系統。

# 不要鬆懈：威脅會從非傳統平台而來

圍繞我們生活的這個世界的運算裝置，看起來並不像電腦或伺服器，包括：路由器、手機、防火牆、智慧型電視、串流媒體盒、VoIP 網路電話盒、攝影機和視訊門鈴、網路儲存，以及一些品牌的廚房和洗衣裝置等。

雖然它們看起來不像傳統電腦，並不意味著它們不會被以相同的方式濫用或惡意使用。

# Android Joker 惡意軟體數量激增

Android 使用者會發現，自己正處於 Google (擁有 Android 平台及主要的 Google Play Store) 和想要將自己的惡意軟體列入 Google Play 商店下載的惡意軟體開發者之間的軍備競賽之中。Google 花了許多年設計一個系統，目的是檢查提交給 Google Play Store 的 Android 應用程式的來源程式碼，以尋找對 Android 使用者有惡意企圖或導致不良後果的程式碼區塊。惡意軟體 App 開發者必須努力躲避這一項 Google Play Store 的程式碼檢查。

Joker 又名 Bread，是一款厲害的 SMS 和收費詐騙 App，它是惡意軟體系列中成功逃避這些程式碼檢查的成功範例之一。自去年研究人員首次發現以來，Google 已從 Google Play Store 刪除了數千種經過 Joker 修改的惡意 App。儘管我們為消除這個惡意軟體付出了巨大的心力，但 Joker 仍然不斷捲土重來。

Joker 以各種不同 App 的名義出現：成為公用程式和工具、桌布、翻譯器、傳訊裝置等，都只是複製自許多熱門 App。請記住，Joker 實際上會可能嵌入在 App 中，其外觀和運作方式，和您使用的真實版本 App 幾乎完全一樣。Joker App 只是在深層埋了一些額外的惡意軟體程式碼，某個第三方檔案庫 App 撰寫者會因為各種正當理由而定期將其編譯到 App 中。

Joker 成功躲避 Google Play Store 安全程式碼檢查的原因有以下幾個：

1. 無論是簡單的字串替換或複雜的商業封裝程式，惡意 App 都使用模糊技術，以減慢分析速度並欺騙 Google Play Store。
2. 當 Joker 的開發者啟動該 App 時，它絕對不包含惡意程式碼。如此一來，即可在 Google Play Store 中建立 App 是安全無虞的歷史記錄。更新之後，惡意程式碼只會出現在 App 中。
3. 該 App 若不是在執行時解密其裝載，就是稍後動態進行下載。

Joker 惡意軟體使用本機程式碼 (JNI)，而不是更常見的 DEX。本機程式碼使用 C 語言編寫，會減慢分析惡意程式碼的速度。相比之下，DEX 是 Java 程式碼的變種，更容易會被反編譯為人類可讀的內容。該惡意軟體使用這個 JNI 程式碼發送 SMS 簡訊，用以牟利和作為聯絡其命令和控製網路的一種方式。透過電話網路 (而不是網際網路) 使用 JNI 和專用訊號，有助於 Joker 躲避不使用 JNI 的自動 DEX 掃描器。

在與 Google 對新 App 進行自動程式碼審查的鬥爭中，Joker 顯然已經取得優勢，我們認為 Joker 不會在 2021 年放慢速度，並且很快就會有競爭對手加入。

# 廣告和 PUA 與惡意軟體的區別越來越小

惡意廣告仍然是威脅各種裝置的主要來源。最近，我們深入探討了目前惡意軟體攻擊以外的兩種惡意廣告威脅的趨勢：使用「瀏覽器鎖定」網頁的技術支援詐騙，以及與詐騙或騙錢軟體 (fleeceware) App 連結的行動裝置廣告。Sophos 將這些攻擊歸類為「假警報」，企圖恐嚇目標的惡意廣告，讓目標採取行動來填飽騙子的荷包。

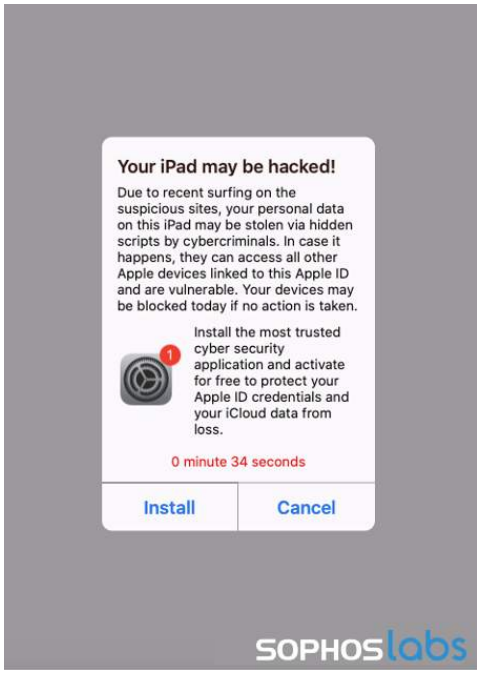



圖 24。來源：SophosLabs

技術支援詐騙通常會試圖引導目標讓他們可以從遠端存取其電腦，然後說服他們購買價格過高的技術支援軟體和服務，或者詐騙取得目標的信用卡資料。儘管這些騙局中，許多在過去都是直接仰賴電話推銷，但許多詐騙操作者已經轉成「提取」模式，也就是使用惡意網路廣告，試圖說服使用者的電腦已經因為安全原因而被鎖定，然後指揮使用者聯絡詐騙分子 (就是自己)。

為了達成這個目的，詐騙者會部署網站套件，其中包含很難離開頁面的指令碼，如「邪惡游標」(evil cursor) 的變種 (使滑鼠指標指向並非實際所在的某個位置，或者使其隱形) 和「無限下載」攻擊使瀏覽器不堪負荷，同時試圖讓畫面看起來像來自 Microsoft 或 Apple 的警示。我們發現其中一些工具套件，會攻擊 SophosLabs 攻擊性安全團隊今年稍早在 Firefox 中發現的一個弱點，而其他工具套件則對其他瀏覽器進行了類似的攻擊，而這些都是經由惡

意的「彈出式」網路廣告所傳播。

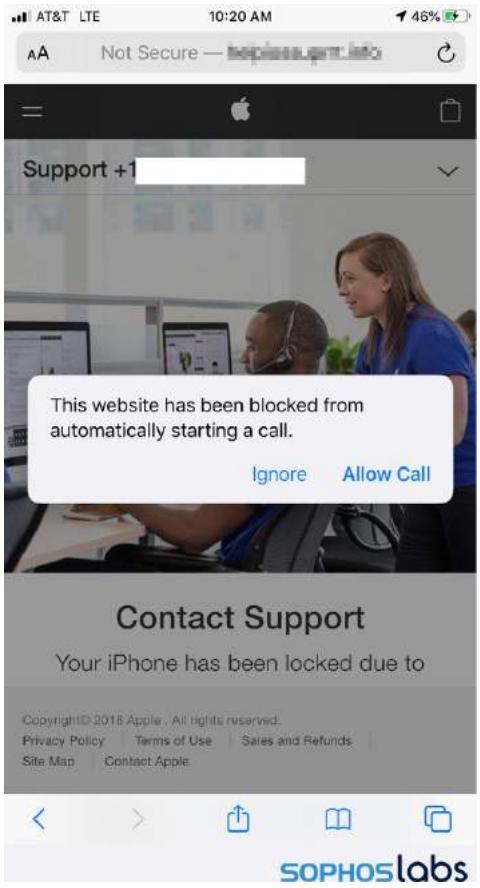



圖 25。來源：SophosLabs

這個支援 PC 和 Mac 瀏覽器上這些攻擊的廣告網路基礎架構，還會進行技術支援詐騙和連結到可能有害的行動應用程式的假警報——包括聲稱是虛擬私人網路服務的應用程式，和可以移除惡意軟體的「清理」工具，而其內建訂閱費用 (在某些情況下，連結的是真正的 Android 惡意軟體)。Sophos 發向了一組發送這些廣告的廣告活動伺服器，其使用一個俄羅斯程式開發者專為進行這類活動所設計的商用軟體。

# 以子之矛，攻子之盾：將安全工具用於犯罪用途

有些攻擊根本不使用惡意軟體，或者等到攻擊結束時才發送惡意軟體，它們只使用網路上電腦作業系統上已經有的工具。其他犯罪分子可能會利用資訊安全產業兩個大型部門 (事件回應人員和滲透測試人員) 使用的一系列工具。

資訊安全社群已經定義出很少或不使用惡意軟體的攻擊方式，而是利用作業系統的現有元件或流行的軟體封裝來進行離地攻擊 (LOL)。這些攻擊通常使用一或多種形式的自動化，這些自動化以本機指令碼的形式出現，例如 PowerShell、批次處理檔案或 VBScript 指令碼 (統稱為 LOLscript)。攻擊者使用這些 LOLscript，透過離地的二進位檔案 (應用程式，亦俗稱 LOLbin) 來執行一連串命令。

這些專為產業「紅隊」市場設計的軟體中，包含了您自己的攻擊方法。在這種情況下，攻擊者將部署和使用網路管理員和滲透測試人員常用的現成安全工具。包括 Cobalt Strike 以及 Metasploit 架構元件等工具，它們原本的目的都是用於安全評估和技術測試。

### ATT&CK 矩陣上的 Netwalker 威脅執行者工具集

| 初步使用 | 執行 | 權限提升 | 防禦躲避 | 存取憑證 | 探索 | 橫向運動 | 產生影響 |
|---|---|---|---|---|---|---|---|
| 對 Tomcat 進行漏洞利用 | PowerShell 指令碼 | CVE-2020-0796 | 無檔案載入 | mimikatz | SoftPerfect 網路掃描器 | psexec | Netwalker 勒索軟體 |
| 對 Weblogic 進行漏洞利用 | psexec | CVE-2019-1458 | Eset AV 移除程式 | Mimidogz | NLBrute | Teamviewer | Zeppelin 勒索軟體 |
| 網路釣魚電子郵件 | | CVE-2017-0213 | Gordon's Eset password recovery | Mimikittenz | | Anydesk | Smaug 勒索軟體 |
| | | CVE-2015-1701 | Trend Micro 安全代理程式解除安裝工具 | Windows Credentials Editor | | | 資料外洩 |
| | | | Microsoft Security Client 解除安裝 | pwdump | | | |
| | | | | NLBrute | | | |
| | | | | LaZagne | | | |
| | | | | WinPwn | | | |

SOPHOSlabs

圖 26。Netwalker 勒索軟體攻擊執行者使用的工具集，會在攻擊的不同時間點使用許多開放原始碼、免費軟體和商用公用程式。來源：SophosLabs。

這些工具對攻擊者有價值的原因很多：由於經常以合法用途使用它們 (用於稽核或以其他方式提高系統安全)，因此防毒或安全解決方案也很難徹底偵測此類工具或活動。因此，Sophos 必須更深入地研究 LOLscript 的行為來識別潛在的惡意活動。當然，比起從頭開始打造自己的工具，使用現有的東西要容易得多。

在過去一年中，使用 LOLscript 和反向 Shell 並不是什麼新鮮事，但到 2020 年，它們已普遍出現在複雜、手動操作的勒索軟體入侵攻擊中。實際上，我們觀察到在攻擊過程中，攻擊工具的數量和種類似乎都增加了。

### Dharma RaaS 攻擊工具攻擊鏈

| 初步使用 | 執行 | 權限提升 | 防禦躲避 | 存取憑證 | 探索 | 橫向運動 | 外洩 | 產生影響 |
|---|---|---|---|---|---|---|---|---|
| RDP 憑證噴灑 | PowerShell | CVE-2019-1388 | 停用惡意軟體防護 | mimikatz | PCHunter | 群組原則對象 | PowerShell 螢幕截圖寄送程式 | Dharma 勒索軟體 |
| RDP 憑證被竊 | WMI | CVE-2018-8120 | Revo 移除安裝程式 | Remote Desktop Passview | Process Hacker | 遠端桌面 | TOR | |
| | AutoIT | CVE-2017-0213 | IOBit Uninstaller | LaZagne | GMER | WinRM 遠端管理 | dropmefiles[.]com | |
| | 命令列/RDP | | | NLBrute | Advanced IP Scanner | | | |
| | | | | Hash Suite Tools | NS2.EXE | | | |

SOPHOSlabs

圖 27。來源：SophosLabs。

攻擊工具種類繁多，涵蓋商用應用程式到開放原始碼 GitHub 存放庫，功能可能包括：

- 類似於殭屍網路的命令和控制架構
- Shellcode 產生和模糊化
- 躲避防毒和沙箱偵測
- 提取密碼或憑證
- Kerberoasting (保持網域管理員權限的持久性)
- 暴力破解各種服務使用的密碼的能力
- 系統資料外洩

在這些工具中，大多數在「開箱即用」狀態下都是良性裝載或根本沒有裝載，但是在過去，我們已經能夠根據行為偵測技術，從得到的內容相關資訊偵測到許多此類工具參與惡意活動的事實。

根據我們的遙測，我們發現最常用的十種攻擊工具是 (按使用頻率排列) Metasploit、BloodHound、mimikatz、PowerShell Empire、Cobalt Strike、Veil Evasion、Hydra THC、Enigma、Nishang 和 Shellter。Metasploit 無疑是最常見的工具，出現頻率是第二常見攻擊工具 BloodHound 的兩倍。

Sophos 目前追蹤了多達 99 種不同攻擊工具的使用情況。到 2021 年，攻擊者似乎會繼續使用這些編寫良好的工具。

# 數位流行病學

多少百分比的運算裝置感染了未偵測到的惡意軟體？未偵測到的威脅執行了多少百分比的命令列執行動作？未偵測到目標型網路釣魚電子郵件的百分比是多少？這些百分比隨產業、地理位置和網路狀況而有什麼變化？

提出這樣的問題，類似於詢問「有多少百分比的人感染了 COVID-19？」在許多人可能永遠無法進行病毒檢測的情況下，執行的檢測可能有明顯的假陽性和假陰性比例。

換句話說：很難。

儘管存在這些難題，流行病學家每天都會回應 COVID-19 的關鍵問題。不幸的是，網路安全研究人員並沒有對網路攻擊做同樣的事情。在不確定性下，我們用來推理的工具、技術和程序，都落後於流行病學家。沒有任何藉口，現在是時候讓我們建立自己的工具來了解所面臨威脅的性質，準確地向受保護者報告風險，並做出努力方向為何的決定。

為了幫助完成這個任務，Sophos AI 已著手建立一套以流行病學為靈感的統計模型，從總體上來估計惡意軟體感染的發生率。我們將強大的資料收集管道 (可從 1 億個端點收集資料) 與一組貝氏 (Bayesian) 統計方法結合起來，使我們能夠解決這些難題，以全面了解這個模型在「該領域」的效能。

例如，思考以下問題：「每周有多少惡意軟體實際上在影響我們的客戶？我們偵測到多少？」

如果我們已經知道哪些檔案是惡意軟體，哪些檔案對所有檔案都是無害的，那麼我們已經達成目的了！不幸的是，我們有兩個問題。

1. 我們實際上並不知道任何特定檔案背後的基本事實——任何端點產品都會漏掉一些惡意軟體，並且不可避免地會出現誤報 (正常檔案被標記為惡意軟體)
2. 在良性檔案和惡意檔案之間的平衡，絕大多數傾向良性檔案，因此我們可能無法利用手動分析來解決這個問題。我們必須對被端點產品標記為良性的數千個檔案進行深入分析，才能找出一個惡意的威脅

為了解決這些問題，我們採用貝氏統計法。用非常簡單的術語來說，我們建立了資料的「產生」模型：一個數學程式，可以猜測參數 (「到底有多少惡意軟體？」)，然後將這些猜測轉換成模擬我們可能看到的端點偵測結果。然後，我們嘗試不同的猜測，看看哪些模擬與觀察到的現實相符，然後反向工作找到我們感興趣參數的合理值。

例如，假設我們在特定的一周內有 2,000 個端點偵測，且評估模型的偽陽、偽陰率良好。我們可以模擬惡意軟體率為 0%、2%、5% 時的環境，並查看模擬對端點偵測的預測；如果我們發現某些惡意軟體發生率接近 2,000 次偵測，那麼這 (可能) 就是一個合理的數值。


圖 28。提出惡意軟體速率、進行採樣、查看模擬是否與觀察到的現實相符、計算得出的速率，然後重複進行。來源：SophosAI。

您可以重複這個過程數百萬次，以建立合理的惡意軟體速率值分佈，並且由於我們使用貝氏方法，因此估計時就已經「內含」誤差帶。在我們的範例中，模型認為「惡意軟體占檔案的百分比是多少？」的可能性最大，略高於 3%，但從大約 2.75% 到 3.35% 的任何值都是合理的。

一旦我們對這個數字有概念 – 每一百個客戶端點中有多少個檔案可能是惡意軟體 – 漏掉的偵測和誤報就變得非常容易估計。如果我們查看 5 月某一周來自深度學習 ML 的惡意軟體偵測系統的資料 (未啟用任何特徵碼、行為或啟發式選項)，我們可以填滿偽陽、偽陰、真陽、真陰的完整矩陣，並完成我們對模型效能的概觀。此時，我們看到雖然確實有一些假陰性，但假陽性的數量很少並且偏向零，真陽性的數量很多，並且偏向 161,000 (樣本中陽性結果的總數)。從規模上看，我們可以看到，這三個數值都遠遠比不上真陰性 (我們的 ML 標記為良性的良性檔案) 的數量。

這個以流行病學為靈感的工具，使我們能夠從 PE 檔案中大海撈針。

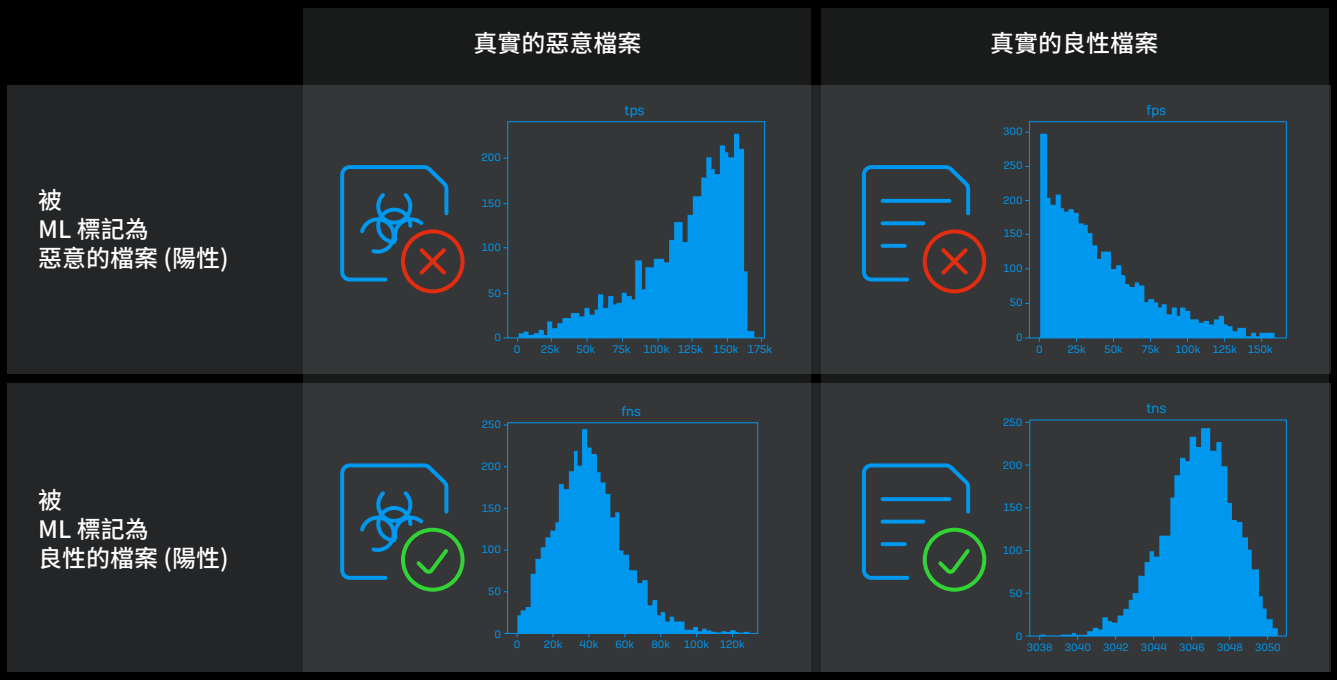



圖 29。2020 年 5 月上旬 ML 模型偽陽與偽陰的分析。來源：SophosAI。

台灣業務窗口
電子郵件：Sales.Taiwan@Sophos.com



20-11-01 ZHTW (DD)

SOPHOS