Acronis

2022 年
報告

2022 年 Acronis 網路威脅報告

勒索軟體攻防戰：一年回顧

Acronis
2022 年網路威脅報告

目錄

作者：

Alexander Ivanyuk
Acronis 產品與技術定位部資深總監

Candid Wuest
Acronis 網路防護研究部副總裁

Copyright © 2002-2021 Acronis International GmbH.

介紹與摘要

Acronis 是業界首家能執行全方位、整合式網路防護來保護所有資料、應用程式和系統的公司。網路防護需要對威脅進行研究和監控，以及遵循五大面向 (SAPAS)：安全、易用性、隱私權、真實性和安全性。基於此策略，我們在全球建立了四個網路防護營運中心 (CPOC)，全年無休 (24/7) 地監控和研究網路威脅。

自 2003 年成立以來，Acronis 一直是資料防護領域的公認領導者。爲了回應針對備份檔案、代理程式和軟體的網路威脅的攀升，公司在 2016 年推出了其創新 Acronis Active Protection 防勒索軟體技術，該技術使其成爲將防勒索軟體防禦功能整合在其備份解決方案中的首個資料防護廠商。該機器智慧和行為型偵測技術已擴展為可處理所有形式的惡意軟體和其他潛在的網路威脅。

我們的旗艦產品 Acronis Cyber Protect Cloud 為服務供應商提供了整合式備份、災難復原、防毒、防惡意軟體、電子郵件安全性、URL 篩選服務以及端點防護管理功能，讓他們向客戶提供全方位的網路防護服務。還以 Acronis Cyber Protect 15 形式直接向企業提供了相同的技術。

該報告涵蓋依我們的檢測和分析人員在 2021 年下半年之所見分析得出的威脅態勢。

在 Acronis 網路威脅報告：2021 年中查看 2021 年上半年的調查結果。

該報告代表一個全球視角，以超過 650,000 個、遍佈於世界各地的特有端點為基礎撰寫。而這兒主要關注的是 Windows 作業系統的威脅，因爲與 macOS 相比它們更為流行。我們將看到態勢的發展，在明年的報告中會包含關於 macOS 威脅的資料，因爲這些威脅近期出現了突增。

Copyright © 2002-2021 Acronis International GmbH.

2021 年下半年的五個重要數據：

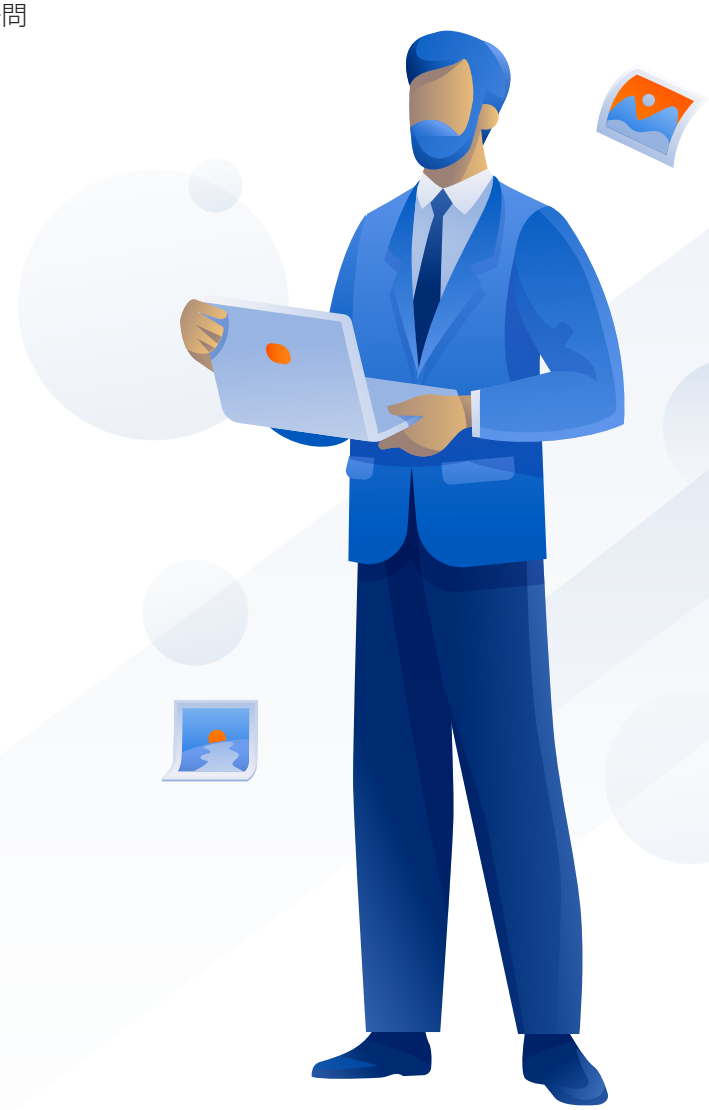
- 2021 年第 3 季度遭受攻擊次數最多的國家/地區是美國、德國和加拿大。
- 僅 10 月 Acronis 就在端點上攔截了 376,000 個 URL。
- 2021 年第 2 到第 3 季度，遭攔截的網路釣魚電子郵件增加了 23%，遭攔截的惡意軟體電子郵件增加了 40%。
- 預計到 2021 年底，勒索軟體造成的損失將超過 200 億美元。
- 隨著攻擊頻率的不斷增加，僅 20% 的公司指出他們沒有遭受攻擊，而去年是 32%。

以下是我們在 2021 年下半年觀察到的網路安全趨勢：

- 勒索軟體仍然是政府、醫療保健和其他關鍵組織等大中型企業的頭號威脅。
- 合作夥伴 (Managed Service Provider) 遭受攻擊，責任問題已提出。
- 弱點正被廣泛利用。
- Linux 和 macOS 已越來越多地引起網路罪犯的關注。

在此報告中，您將發現：

- 在 2021 年下半年觀察到的重大安全性/威脅趨勢。
- 爲什麼會加密貨幣面臨越來越多的威脅。
- 合作夥伴 (Managed Service Provider) 和代替作業系統爲什麼越來越容易遭受威脅。
- 一般惡意軟體統計資料和重要系列審核。
- 含最危險威脅之深入分析的勒索軟體統計資料。
- 哪些弱點會促成攻擊成功進行。
- 對 2022 年的安全性建議與威脅預測。



Copyright © 2002-2021 Acronis International GmbH.

2021 年重要的網路威脅和趨勢

第 1 部分

1. 勒索軟體攻擊一直居高不下

2021 年下半年勒索軟體攻擊活動猖獗，整個行業因大量大事件而遭受重創。這些勒索軟體團體不僅十分活躍，而且開始變得更具有攻擊性。例如，Ragnar Locker 勒索軟體團隊宣稱，如果受害者報警或尋求任何種類的專業協助，它們便會立即發佈所有偷竊來的資料。這些網路罪犯聲稱，專業的贖金談判人員只會讓受害者的處境變得更糟。如果受害者仍然決定讓這些贖金談判人員參與進來，攻擊者有信心他們會以某種方式發現。去年，Ragnar Locker 入侵了 Campari，然後支付了 Facebook 廣告費用，爲的是公開向其受害者施壓，要求其支付 1500 萬美元的贖金，否則會公佈他們被竊取的 2TB 資料。

然而，行業和執法官員進行了不屈的鬥爭。在歐洲刑警組織、法國國家憲兵隊、烏克蘭國家警署和美國聯邦調查局的協助下，兩個勒索軟體運營商被逮捕了。這兩個運營商勒索了高達 7000 萬歐元的贖金。警方查獲了 375,000 美元的現金、兩部豪車以及 130 萬美元的加密貨幣。雖然目前還不知道這兩個運營商的主謀是誰，但他們涉嫌對歐洲和北美的行業群體進行了有組織的攻擊。美國司法部宣稱對 REvil 勒索軟體子公司在 7 月 2 日針對 Kaseya MSP 平台的攻擊進行了指控，並從另一個 REvil 合作夥伴處查獲了超過 600 萬美元。DOJ 還聲稱，執行單位從另一個 REvil 勒索軟體子公司處查獲了 610 萬美元。這些只是針對勒索軟體集團執行的執法活動的一部分。雖然兩個運營商的成員已被捕，但幾個月后他們會重新露面或更換名字，成爲數百名勒索軟體運營商中的一員，繼續竊取和加密資料。

事實上，情況已變得如此糟糕，以致於在 11 月，美國宣佈了一個獎金獎勵計劃，將針對每個 REvil (Sodinokibi) 和 DarkSide 勒索軟體成員獎勵高達 1000 萬美元。該獎金作爲美國國務部的跨國有組織犯罪獎勵計劃 (TOCRP) 的一部分提供，目的是為了獲取能夠逮捕跨國組織犯罪團體成員或將其定罪的情報。此外，如果提供能逮捕試圖參與這兩個勒索軟體團體之任何個人的情報，將獎勵 5,000,000 美元。

FBI 最近公佈了 Ako 或 ThunderX 勒索軟體團體 (在最近的重塑后，也稱爲 Ranzy Locker) 有關的一些令人驚訝的數字。据 FBI 稱，該團體在過去的這一年入侵了美國多個行業的 30 多家公司。該警報表明，無論您的公司是屬於建築、製造、學術、資訊技術、交通運輸或任何其他部門，所有人都面臨著風險。該團體利用暴力密碼破解 RDP 認證和 Microsoft Exchange 漏洞來獲取其受害者基礎架構的存取權。

Copyright © 2002-2021 Acronis International GmbH.

過往攻擊事件

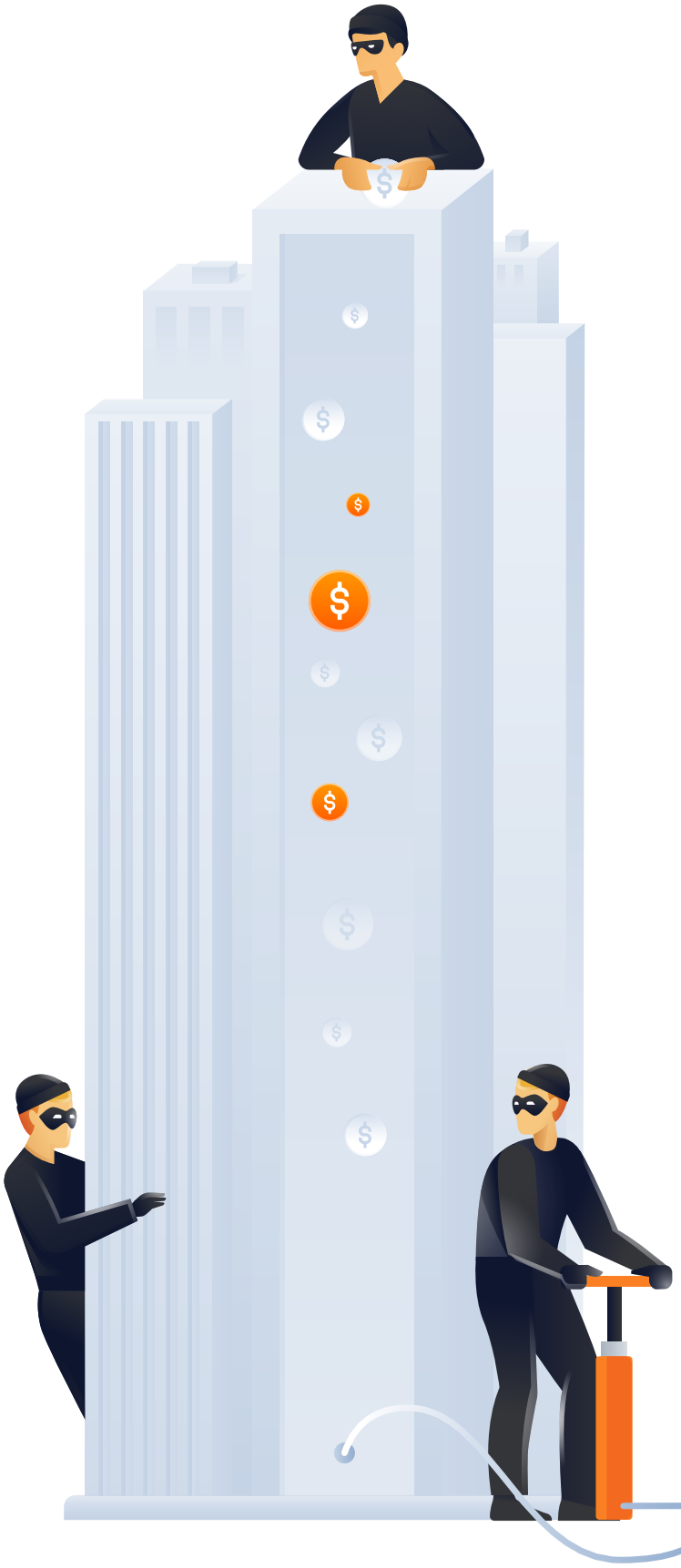
在 7 到 11 月觀察到的**一些大事件**。在發生了 400 多起涉及 Conti 的案件之後，CISA 發出了一個警報。Conti 的勒索軟體最先出現在 2020 年 5 月，并且它們一直是成功的勒索者。

例如，總部位於日本的電子產品跨國公司 JVCKenwood 和 Sandhills Global 已被 Conti 勒索軟體攻擊。Conti 宣稱已竊取 1.7TB 的資料，並索取 700 萬美元的贖金。Conti 還要求 Graff 珠寶支付包含 11,000 客戶的資料的贖金，金額達數千萬英鎊。Graff 的年收入超過 6 億美元。到目前爲止，Conti 已洩漏 Graff 的 69,000 份機密文件，其中包括發票、收據以及信用單據。歐洲最大客戶服務和呼叫中心供應商之一 GSS，以及經典婚紗設計師 Vera Wang 集團也遭到了 Conti 勒索軟體的攻擊。

Prodaft 最近的一項研究揭露了有關 Conti 集團使用的後端伺服器的一些有趣細節。據悉，Conti 集團在 9 月收到了 1000 萬美元的付款，在 11 月已超過 750 萬美元。

跨國技術諮詢機構 Accenture 已成爲 LockBit 勒索軟體團體的最新受害者。Accenture 是一家全球財富 500 強公司，擁有 50 萬多名員工和超過 440 億美元的年收入，主要為包括 Cisco、Alibaba 以及 Google 在內的客戶提供服務。LockBit 在此次攻擊中似乎竊取了高達 6TB 的資料，並要求 5000 萬美元的贖金。之後，Accenture 從備份中恢復了資料，並聲稱對正常運營沒有重大的影響。

LockBit 勒索團體的另一個大受害者是 Bangkok Airways，該公司在 11 個國家/地區雇用了 3,000 多名員工，年收入超過 6.85 億美元。LockBit 宣稱已將 Bangkok Airways 200GB 的資料發佈到一個合法檔案共用服務，并且該航空公司已證實，被竊取的資料包括乘客的全名、國籍、性別、電話號碼、電子郵件地址、護照資訊以及其他機密資料。



Copyright © 2002-2021 Acronis International GmbH.

新惡意份子

相對較新的 Hive 勒索軟體團體剛在 11 月入侵了電子零售巨頭 MediaMarkt，最初要求 2.4 億美元的贖金，造成荷蘭和德國的 IT 系統關閉和商店運營中斷。記住這一點，MediaMarkt 是歐洲最大的消費電子產品零售商，在 13 個國家/地區有超過 1,000 家商店，所以要求的贖金並不令人感到意外。MediaMarkt 擁有大約 53,000 名員工，年銷售總額達 208 億歐元。

在此次攻擊之前，Hive 團體開發了特定版本的勒索軟體來加密 Linux 和 FreeBSD。由於全球前 100 萬伺服器中的 96.3% 目前在 Linux 上執行，以及 90% 的雲端基礎架構在 Linux 上運作，這對於惡意份子而言是一個非常合理的舉動。Babuk、DarkSide、HelloKitty 以及其他勒索軟體團體全都建立了自己的 Linux 加密程式。

Hive 團體還攻擊了密蘇里州 Delta 醫療中心。透過此次攻擊，他們竊取了 95,000 份，總共大小 400GB 的患者記錄，其中包括患者姓名、社會安全號碼、病例以及電話號碼等機密資訊。醫療行業的另一個受害者是非盈利紀念醫療系統。紀念醫療系統有 64 個診所、超過 3,000 名員工，所有證據表明，超過 200,000 名患者的資料被竊取。

另一個在 7 月才開始運營的新成員是 BlackMatter 勒索軟體集團，該集團被認爲是從 DarkSide 集團分離出來的，雖然在 11 月初他們已宣稱由於「來自主管機關的壓力」而關閉。該專案的生命周期很短，但是在此期間造成了很多破壞。例如，BlackMatter 勒索軟體集團入侵了愛荷華州的農業公司 New Cooperative。据 New Cooperative 稱，美國 40% 的糧食生產通過他們的軟體運行，而他們是一個農場服務提供者，年收入估計在 5 億到 10 億美元之間，是拜登政府提出的「16 個關鍵部門」之一。他們被竊取了 1,000 GB 的資料，並被勒索 590 萬美元的贖金。

BlackMatter 還攻擊了總部位於日本的科技製造商 Olympus，該公司在 9 月和 10 月被入侵了兩次。爲了抵禦攻擊，受影響的系統被迫下線，并且已向外部合作夥伴發出了通知。此次攻擊對美國、加拿大和拉丁美洲的系統造成了影響。

BlackMatter 的另一個受害者是 Marketron。Marketron 為媒體行業的 6,000 多名客戶提供伺服器維護服務，預計收入達 2550 萬美元。

在過去幾個月的某一時刻，BlackMatter 新增了一模組來加密 Linux VMware ESXi 伺服器。他們的勒索軟體向其 ELF 64 位元加密程式中新增了 VMware ESXi 程式庫。這讓他們可以列出所有 VM 主機，然後在加密其映像之前將其關閉。該集團還公開尋找可以提供收入超過 1 億美元的公司之企業網路存取權的人。

自 7 月起，BlackMatter 已總共入侵了至少 40 家公司，雖然很有可能還有很多其他公司尚未公開披露。

AVOS Locker 勒索軟體，我們已經在本報告的另一部分對其進行了詳細的分析，是犯罪現場的另一個重要的新成員。在此報告期間內，其運營商聲稱從太平洋銀行竊取了機密資料。太平洋銀行是第三大銀行，業務集中於韓裔美國人社群，收入估計為 6720 萬美元。

AVOS Locker 還入侵了以電腦主機板而聞名的台灣硬體製造商 Gigabyte。這是該公司在三個月內發生的第二次事件。AVOS Locker 集團接著公佈了 15MB 竊取來的資料作爲他們攻擊的證據，其中包括密碼和使用者名稱、員工薪資詳細資料、護照掃描件、與客戶簽署的保密合約以及其他機密資訊。

此外還出現了 LockFile 勒索軟體，它充分利用了諸如 PetitPotam 和 ProxyShell 之類的弱點。LockFile 最初被發現攻擊的是美國一家金融組織，並迅速讓自己與衆不同。它的目標主要是美國和亞洲的組織，但也在世界各地出現過，攻擊對象為金融、製造業、法律、旅行、工程以及商業服務部門。與 BlackMatter、LockBit 2.0 和 DarkSide 相似，該勒索軟體使用間歇性檔案加密技術來躲避偵測，但 LockFile 僅對檔案的每隔 16 個位元組進行加密。

Copyright © 2002-2021 Acronis International GmbH.

2. 網路釣魚和惡意電子郵件仍然是主要的感染載體

Acronis CPOC 在 2021 年 10 月攔截了 376,000 個網路釣魚和惡意 URL。相較於第三季度 58,000 的月平均數量構成了一個激增。

很不幸，很多含有惡意內容（尤其是 URL）的電子郵件仍然突破了基本的電子郵件篩選器並最終到達了使用者的端點。我們還發現攻擊者將惡意 URL 的 QR 碼嵌入到網路釣魚電子郵件中。很多安全解決方案還無法處理 QR 碼，但終端使用者習慣用他們的智慧型手機來追蹤連結。這是爲什麼擁有一個多層次防禦機制非常重要的另一個原因。

月份	已阻止的 URL
7 月	57,588
8 月	33,012
9 月	83,804
10 月	376,451

藉由採用 Perception Point 技術的 Acronis Advanced Email Security，我們發現，與第二季度相比，第三季度阻止的網路釣魚電子郵件增加了 23%，而惡意電子郵件數量在第三季度則增加了 40%。

Acronis 網路整備性報告 2021 最近的一項研究顯示，IT 系統管理員將網路釣魚列爲他們遇到的最大威脅，58% 的受訪者稱他們遇到過此類攻擊。儘管如此，只有 20% 的人針對其 IT 安全性堆疊優先使用 URL 篩選解決方案。

此外，波耐蒙研究所最近的一項研究揭露了有關網路釣魚攻擊成本的一些驚人統計資料。本研究考查了與這些攻擊相關的所有費用，包括生產力的復原和損失，這些費用實際上超過了支付給網路罪犯的款項。網路釣魚攻擊的成本在過去六年急劇攀升，目前美國大型公司每年的成本為 1480 萬美元，相當於每位員工約 1,500 美元。相比之下，在 2015 年該數字為 380 萬美元。這意味著在短短六年內，網路釣魚攻擊的成本幾乎翻了兩番。在 2020 年，商務電子郵件入侵（BEC）攻擊的成本顯著上升，透過僞造員工、合作夥伴或廠商等常見策略從美國組織竊取了超過 18 億美元的資金。

Copyright © 2002-2021 Acronis International GmbH.

重大事件

一個使用開放式重新導向程式連結避開安全性軟體的**大型認證網路釣魚活動**正在進行中。此最新活動將 Zoom 之類的知名品牌與開放式重新導向連結結合在一起，以引誘個人與這些連結進行互動。這些連結會進一步將使用者重新導向到 CAPTCHA 驗證頁面，這樣新增了合法性並讓自動化安全性分析更加困難，然後才會提示使用者提供認證。

一項名爲 BulletProofLink 的網路釣魚作業被發現為攻擊者提供進行網路釣魚攻擊所需的一切。此項作業提供了從網路釣魚工具組和範本到託管服務以及其他有用工具等一切內容。該服務提供了 100 多個仿冒 Microsoft 等知名品牌的網路釣魚範本，甚至還建立了獨特的子網域來與其活動相關聯，單次就產生了 300,000 多個子網域。BulletProofLink 提供的服務每月收費高達 800 美元，而個人服務的費用則要低一些。例如，一次性託管連結可能只需 50 美元，而首次使用的客戶甚至還有 10% 的折扣。

另一個全新的網路釣魚攻擊是僞裝成看似合法的 UPS 電子郵件，但實際上是利用 UPS 主網站中的弱點。電子郵件中的所有連結都是合法的，除了開啟追蹤包裹頁面中的按鈕。它包含一個惡意承載，此承載會充分利用 XSS 弱點來最終下載一個惡意 Word 文件，此文件轉而又會提供一個惡意承載。這樣的攻擊表明攻擊者有多狡猾，以及發現網路釣魚電子郵件是多麼棘手。

一個以推送 TeamTNT 惡意軟體而聞名的惡意軟體團體發起了一項名爲 Chimaera 的新活動，該活動一直在無差別地攻擊多個作業系統。TeamTNT 已向其工具庫中新增了大量的工具，其中包括 shell 指令碼、加密貨幣採礦軟體、IRC 以及開放原始碼工具等。全球超過 5,000 次感染都被認爲是該集團造成的，開放原始碼工具正在被 TeamTNT 用來竊取使用者名稱和密碼，并且一直在攻擊 Windows 和多個 Linux 發行版本，以及 AWS、Docker 和 Kubernetes。在過去，它們還被發現攻擊了 macOS 系統。

網路釣魚不需要那麼先進才能成功。一名英國青少年透過僞造流行的 Love2Shop 禮品卡在線上商店賺取了 270 多萬美元。該網站是一個網路釣魚網站，收集在該網站上輸入的所有付款卡詳情以及其他私人資料，而受害者不會收到他們承諾的禮品卡。隨後，執行單位還發現該少年名下有 12,000 張付款卡以及大約 200 個支付寶賬戶。這名少年在幾周內從網站賺取了 44 萬美元，接著將這些錢投資了比特幣，這些比特幣增值 10 倍，價值達 300 多萬美元。

隨著加密貨幣變得越來越常見，我們看到並將看到更多針對加密交易和加密貨幣所有者的攻擊。例如，加密交易 Coinbase 最近披露，今年早些時候至少有 6,000 名客戶成爲網路釣魚活動的受害者，造成他們賬戶中的資金被盜。攻擊者獲取了 Coinbase 客戶的電子郵件地址、密碼以及電話號碼，該公司認爲這是由於社交工程所致，例如電子郵件網路釣魚攻擊。一旦登入客戶帳戶，攻擊者就可以從竊取這些賬戶中的資金。雖然 Coinbase 需要雙重要素驗證，由於 SMS 帳戶復原過程中存在瑕疵，使用 SMS 進行該驗證的帳戶容易受到攻擊。該瑕疵現已被修補，不過是在帳戶中的資金被取出之後。Coinbase 選擇對客戶進行補償，但大多數受害者並沒有那麼幸運。Acronis Advanced Email Security 會掃描進入收件匣的所有電子郵件，並阻止網路釣魚和其他惡意電子郵件被看到。這樣可以在攻擊開始之前就停止攻擊，從而確保帳戶和資料的安全。

Copyright © 2002-2021 Acronis International GmbH.

3. Linux 和 macOS 遭受攻擊

除了 Linux 勒索軟體，但這並不是此作業系統面臨的唯一威脅。惡意份子已經越來越關注 Linux，因爲有數百萬的機器連接至網際網路（主要是伺服器），這為開發新的惡意軟體提供了足夠的動機。除了勒索軟體之外，網路罪犯還專注於加密貨幣採礦軟體、木馬程式以及更複雜的惡意軟體，例如 Rootkit。

目前，一個之前不知名的 Linux 惡意軟體系列正在將目標放在東南亞的組織。該威脅被追蹤為 FontOnLake 或 HCRootkit。FontOnLake 是一個模組化 Rootkit，目前似乎正在積極開發中，包括遠端存取支援、認證竊取和充當 Proxy 伺服器等功能。使用 FontOnLake 的攻擊似乎是有針對性的，旨在收集資料，以及進行其他惡意行動。該惡意軟體可躲避很多傳統防毒解決方案的偵測，並在受感染的系統上將常見的合法二進位內容取代為修改后的內容。雖然這個 Rootkit 早在 2020 年 5 月起已遠離人們的視線，但現在可以被 Acronis Cyber Protect for Linux 中包含的多層偵測引擎偵測到，從而讓您的資料和系統免受這個以及其他 Linux 惡意軟體的侵害，保證其安全。

Cobalt Strike 是一個由安全研究員用於滲透測試的合法工具，現已被發現自然環境中支援 Linux 型攻擊。Cobalt Strike 被網路罪犯使用的次數每年增加了 161%。已使用該工具找到數千個組織，并且 SolarWinds 攻擊中也使用了它。直到最近，Cobalt Strike 還面臨著無法在 Windows 以外的任何系統上運作的困難。但自 8 月以來，攻擊者使用了一個名爲 Vermilion Strike 的實作，主要針對 90% 的雲端伺服器。此 ELF 格式的惡意軟體效仿 Geacon，這是一個開放原始碼、Golang 型版本的 Beacon。

與任何其他作業系統一樣，Linux 發行版也存在被惡意軟體積極利用的弱點。并且新的弱點經常被發現。例如，在 10 月，Linux 核心的透明處理序間通訊（TIPC）模組中的一個重大安全瑕疵已被披露并已提供了修補程式。此弱點（標記為 CVE-2021-43267）可在本機或遠端被利用，以獲取核心權限，從而讓攻擊者入侵整個系統。TIPC 模組存在於整合了所有重要 Linux 發行版的核心模組中，但不是由系統自動載入。

隨著 Mac 的市場份額的不斷增長，Apple 的 macOS 也成爲了網路罪犯的目標。一些 Windows 惡意軟體被植入到 Mac 中，還有一些專為利用 macOS 弱點而建立的特定惡意軟體。新的弱點正被定期發現和修補。例如，在 10 月底，Apple 修補了 macOS Big Sur 和 Monterey 作業系統中的一個弱點，該弱點可被濫用以避開 SIP 安全性功能和安裝核心 Rootkit。諷刺的是，一個代號為 Shrootless 的弱點已被 Microsoft 研究員發現，其發現該弱點存在於 macOS 軟體安裝精靈 system_installd 中。

Copyright © 2002-2021 Acronis International GmbH.

摘要

如我們所見，主要的威脅和惡意軟體在 2021 年下半年會繼續進行它們的惡意攻擊。

由於執法單位的高度重視以及數百萬利潤岌岌可危，勒索軟體策略尤其經歷了巨大的變革。此外，越來越多的攻擊針對替代作業系統，特別是伺服器硬體上執行的 Linux 版本。在這種持續的緊急狀態下，擁有適當的多層網路防護非常重要，這樣會盡可能覆蓋更多的垂直領域和作業系統，還可以在有內容錯過時復原機器和資料。**Acronis Cyber Protect** 正是此類解決方案：旨在為機器和資料提供極佳的防護，以及行業最好的復原時間。

Copyright © 2002-2021 Acronis International GmbH.

一般惡意軟體威脅

第 2 部分

2021 年第三季度，Acronis 平均 13.6% 的客戶成功在其端點上阻止了至少一次惡意軟體攻擊。該數字在 10 月幾乎翻了一倍，達到 25.3%，表明第四季度出現了突增。這些高百分比表明，儘管組織進行了安全意識訓練和修補，很多威脅仍會到達端點。

月份	遭受惡意軟體攔截的客戶百分比
1 月	16.1%
2 月	13.7%
3 月	15.9%
4 月	16.1%
5 月	13.6%
6 月	12.1%
7 月	13.2%
8 月	11.7%
9 月	15.9%
10 月	25.3%
11 月*	20.5%

Acronis **網路整備性報告 2021** 最近的一項研究顯示，回應的 IT 管理員中有 37% 的人確認在去年遇到了惡意軟體攻擊，惡意軟體攻擊排名第三，位於網路釣魚和 DDoS 攻擊之後。此調查結果令人驚訝的是，雖然該數字從去年的 22% 增加到 37%，但是仍然偏低，這表明公司要麼有很好的篩選機制 (例如電子郵件篩選) 來屏蔽大多數惡意軟體；或者，可能性更大的是，它們無法發現所有的攻擊。

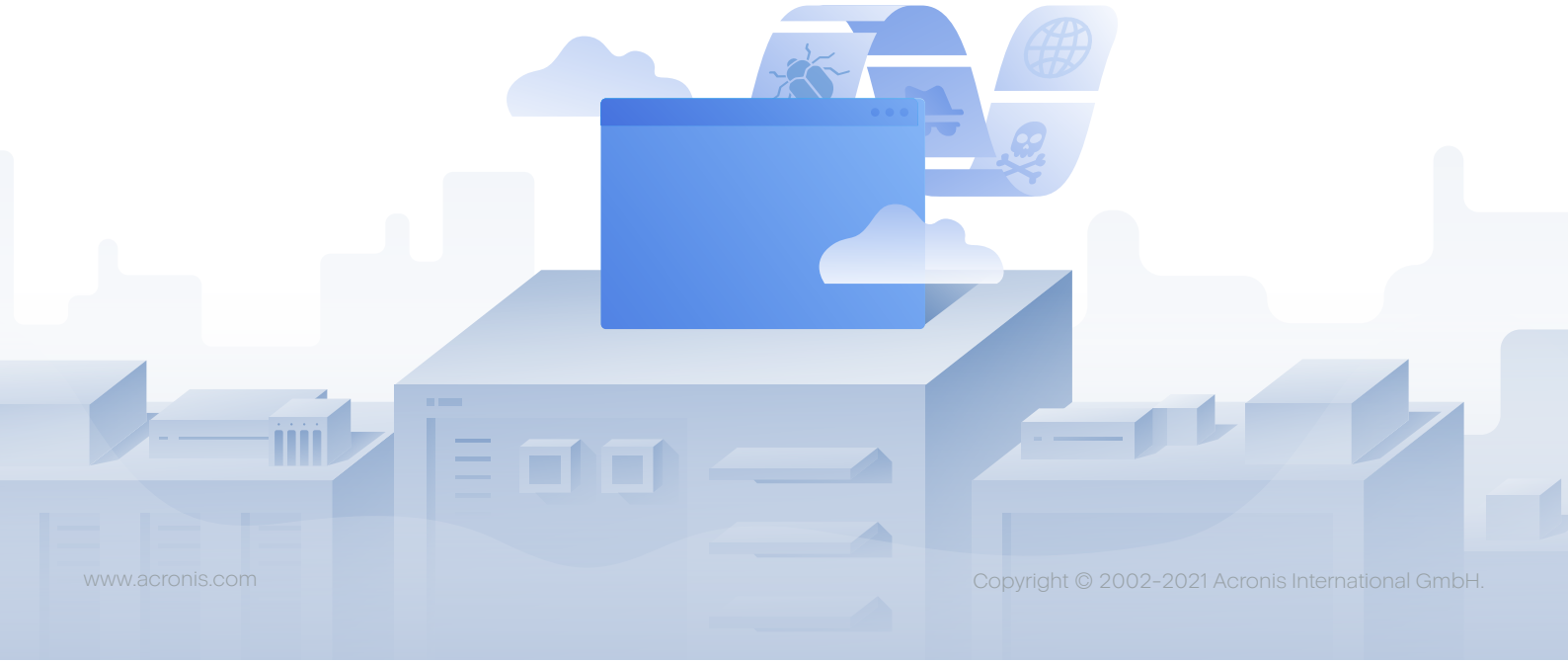
自然環境中出現的新惡意軟體樣本數量在 2021 年些微下降。例如，獨立惡意軟體檢測實驗室 AV-Test 在 2021 年第一季度每天記錄了 600,000 多個新惡意軟體樣本，但在第二季度該數字減少了 17%，下降到每天 507,000 個。在第三季度，該數字又減少了 28%，下降到每天 363,000 個。造成這些下降的原因是，一些集團轉向更有針對性的部署，或逮捕了 Emotet 等活躍電子郵件惡意軟體集團，儘管 Emotet 在 11 月捲土重來，并將推動第四季度數字的上升。

Copyright © 2002-2021 Acronis International GmbH.

2021 年第三季度擁有最多惡意軟體感染數量的國家/地區是**美國，佔 27.2%**，其次是**德國 11.5%**，及**加拿大 5.9%**，與第二季度的數字非常相似。

以下是我們在 2021 年下半年觀察到和追蹤到的前 10 個惡意軟體系列：

系列產品名稱	百分比
Trickbot	7%
AgentTesla	6%
NJrat	5%
Remcos	5%
Formbook	4%
Jupyter	3%
RedLineStealer	3%
XMRig	3%
Zloader	2%
Qbot	2%



Copyright © 2002-2021 Acronis International GmbH.

木馬程式和非法挖礦攻擊

在一般惡意軟體端，我們也遇到了一些有趣且令人擔憂的態勢。例如，在自然環境中發現了世界最大的殭屍網路之一，被感染的裝置超過 160 萬台。殭屍網路之所以被稱爲「Pink」，是因爲其程式碼中有很多函式名稱以該詞開頭。Pink 殭屍網路的主要目標是發起阻斷服務 (DoS) 攻擊，以及插入廣告讓那些僅瀏覽 HTTP 網站的不知情受害者看到。殭屍網路將加密通讯与 GitHub 之類的服務、命令與控制項 (C2) 伺服器以及對等 (P2P) 網路結合使用來控制 Bot。

另一個殭屍網路 MyKings 已經存在至少五年了，現在與以前一樣活躍。新研究表明了殭屍網路是多麼地忙碌，並揭露它透過兩項技術中的其中一個來利用受感染的電腦挖掘或竊取加密貨幣。其中一個技術是在系統上安裝一個加密貨幣採礦軟體以使用受害者的電腦惡意挖掘加密貨幣，而另一策略是使用其剪貼簿盜竊木馬程式偵測加密錢包何時被複製，並將剪貼簿內容取代為受攻擊者控制的加密錢包。MyKings 因此迅速賺得至少 2470 萬美元，早在 2017 年的報告顯示，他們每月在 Monero 中賺取了 230 萬美元，有超過 500,000 台被感染的電腦。

隨著加密貨幣的增長，網路罪犯開始改進和開發新的惡意軟體，旨在竊取加密貨幣。研究人員發現了一種全新的 Golang 加密蠕蟲，現在速度提升了 15% 且效率更高。使用該蠕蟲的攻擊者將掃描 WordPress 提供的 XML-RPC，以及 Oracle WebLogic 伺服器中是否有弱點。一旦這些弱點被成功利用，XMRig 接著就會隨蠕蟲一起安裝，該蠕蟲會將其散播到其他敏感目錄中。

另一個範例是 HolesWarm 惡意軟體，它利用 Linux 和 Windows 伺服器中的 20 多個已知弱點來進行散播。已經有超過 1,000 個伺服器在 2021 年被入侵，尤其是在雲端環境中，并且該數字仍在增加。在這種情況下，一旦伺服器被入侵，即會安裝一個 Monero 加密貨幣挖礦程式來為網路罪犯創造利潤。

在 2021 年下半年還發現了更複雜的威脅。最近的研究顯示，北韓 APT 集團 Lazarus，即策劃了臭名昭著的 WannaCry 勒索軟體攻擊以及 2014 年對 Sony Pictures 的攻擊的組織，一直將 IT 供應鏈作爲目標。最近的攻擊中使用了一個全新 BLINDINGCAN 遠端存取木馬程式 (RAT) 的變種，該程式同時以拉脫維亞公司和韓國智囊團為目標。BLINDINGCAN 允許攻擊者擷取已安裝磁碟的資訊、電腦的作業系統和處理器資訊和其他資料，以及建立和執行執行序和檔案等。

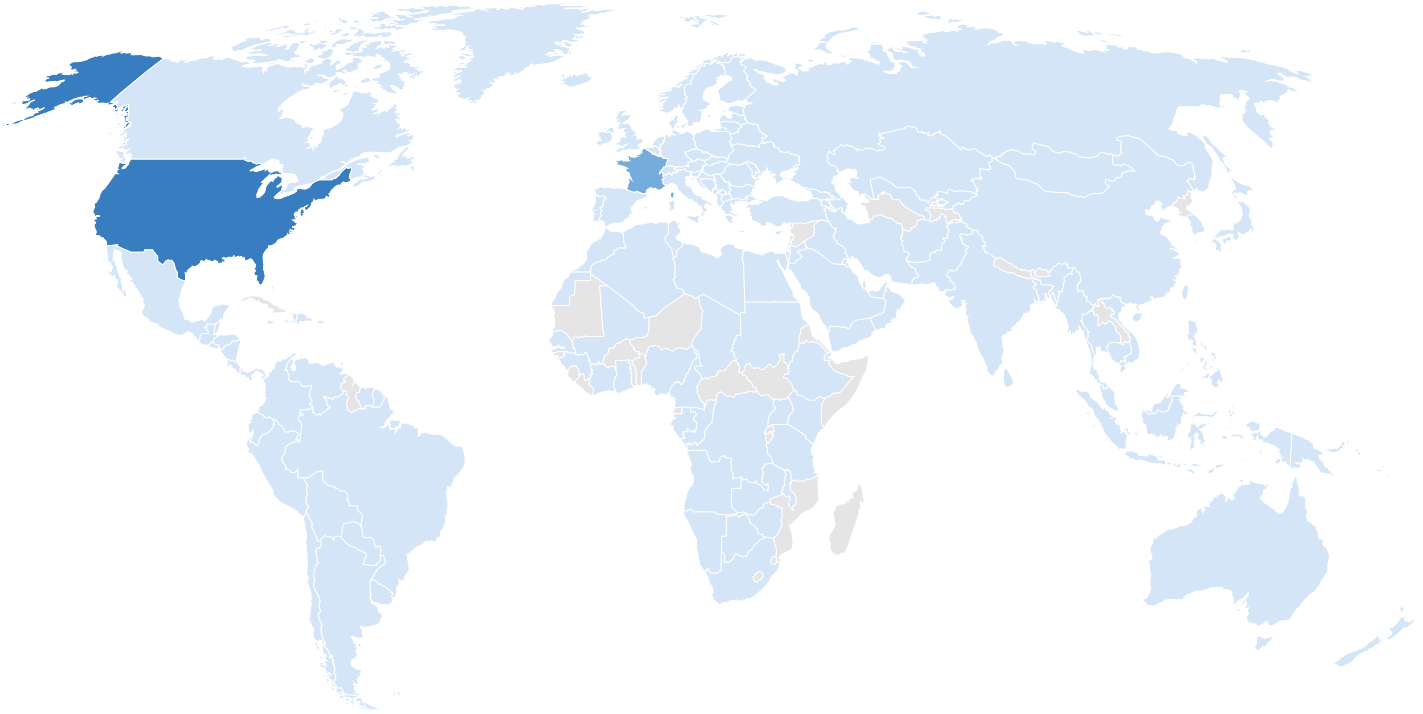
一個名爲 Water Basilisk 的新無檔案型惡意軟體活動正在使用 HCrypt 的一個新變種來將若干遠端存取木馬程式 (RAT) 安裝到受害者的電腦中。HCrypt 是一個常見的加密即服務，攻擊者用它來安裝 RAT，因爲它的無檔案特性讓其很難被偵測到。該加密工具主要依賴 VBScript 和 Powershell 命令來下載惡意承載並將其安裝到受害者的系統中。在此特定攻擊的最後階段，安裝了常見的 RAT，例如 NjRat、Nanocore 以及 QuasarRat 等。在一些情況中，還發現了安裝了一個比特幣或以太幣劫持程式，將剪貼簿中的比特幣或以太幣錢包地址取代為攻擊者控制的錢包地址。

Copyright © 2002-2021 Acronis International GmbH.

依國家/地區排列的每月佔全球偵測數量的百分比

國家/地區	2021 年 7 月	2021 年 8 月	2021 年 9 月	2021 年 10 月
美國	44.4%	65.2%	23.9%	25.4%
法國	14.7%	18.2%	19.5%	14.4%
希臘	0.1%	0.1%	2.7%	6.3%
英國	0.7%	0.9%	1.6%	6.2%
西班牙	2.7%	0.2%	0.6%	6.1%
日本	2.5%	2.1%	6.1%	5.9%
德國	13.4%	1.7%	6.3%	5.8%
以色列	0.1%	0.1%	0.1%	4.7%
土耳其	0.8%	0.5%	0.9%	3.2%
加拿大	0.7%	0.5%	8.3%	2.6%

2021 年第 3 季度惡意軟體偵測數量



偵測數量百分比 2.3% 49%

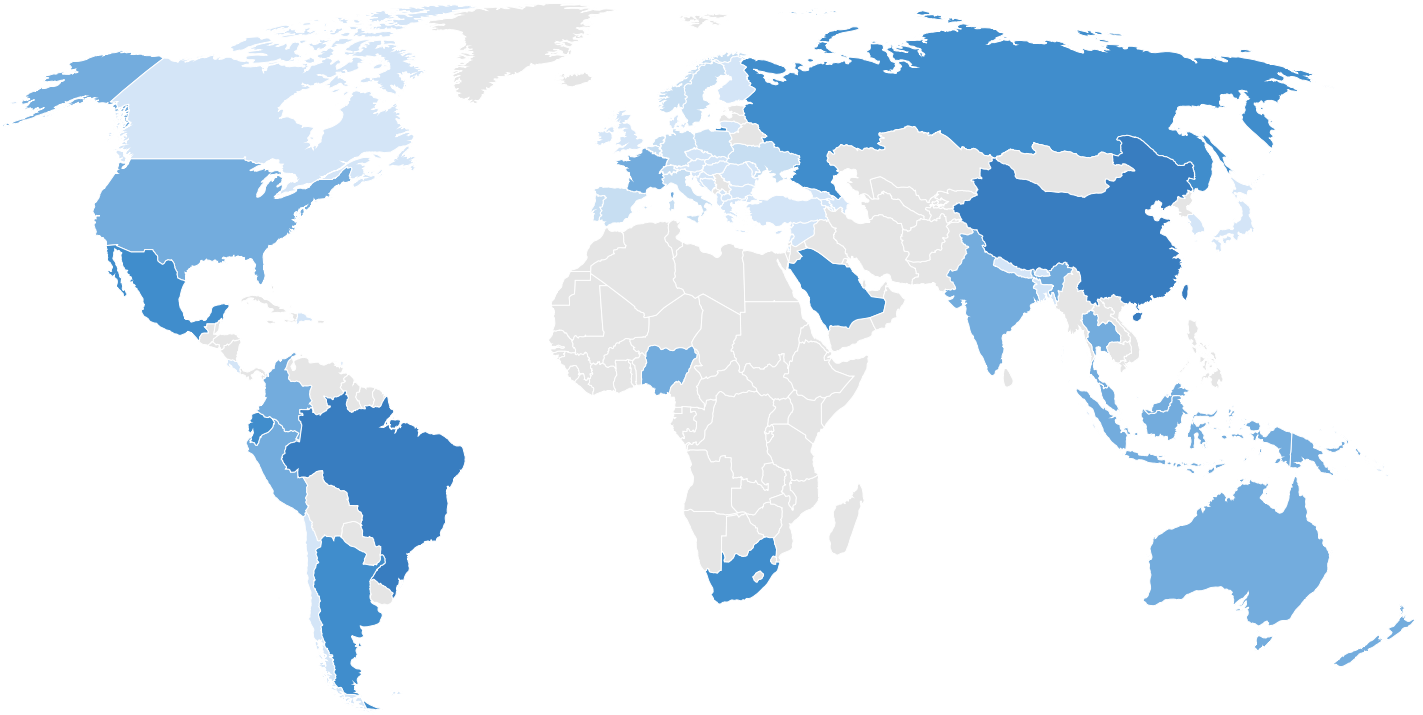
Copyright © 2002-2021 Acronis International GmbH.

如果我們標準化每個國家/地區每個活躍用戶端的偵測數量，我們就會看到稍微不同的分佈。下表顯示了 2021 年第三季度每個國家/地區至少有一次惡意軟體偵測的標準化用戶端百分比。

排名	國家/地區	2021 年第三季度偵測到惡意軟體的用戶端數量百分比，標準化
1	台灣	63.6%
2	新加坡	57.4%
3	中國	55.5%
4	巴西	55.2%
5	摩爾多瓦共和國	50.5%
6	俄羅斯	49.5%
7	希臘	43.3%
8	保加利亞	41.3%
9	韓國	40.6%
10	以色列	39.7%
11	土耳其	39.4%
12	厄瓜多爾	37.8%
13	阿根廷	37.8%
14	阿拉伯聯合大公國	37.5%
15	泰國	37.1%
16	南非	35.9%
17	墨西哥	35.2%
18	匈牙利	32.5%
19	斯洛伐克	32.0%
20	葡萄牙	30.5%
21	海地	30.2%
22	西班牙	29.4%
23	印尼	28.9%
24	沙烏地阿拉伯	28.6%
25	斯洛維尼亞	28.2%

Copyright © 2002-2021 Acronis International GmbH.

2021 年第三季度標準化的偵測數量



偵測數量百分比 0% 63%

勒索軟體威脅

在「重要趨勢」一節中已經提到，勒索軟體仍是企業的頭號網路威脅。在本節中，將重點關注 2021 年 7 月 1 日到 10 月 31 日、由我們的威脅診斷 Acronis Active Protection 阻止的資料。

以下是在 2021 年觀察到和追蹤到的前 10 個活躍勒索軟體系列。請記住，部分組織嘗試用一個廣泛的途徑盡可能感染更多的使用者，而其他組織則重點關注高價值目標，他們僅試圖進行少量的感染，但追求高回報。因此，單獨的威脅偵測量並不能表明威脅的危險程度。此外，很多集團勒索將勒索軟體當作一項服務業務，以致於攻擊者可能在類似的攻擊中使用多個威脅系列。

還應注意的是，在第三季度，很多勒索軟體集團已經銷聲匿跡、用新名稱重組，或在執法活動中失去了其部分成員和基礎架構，從而讓根據唯一的名稱進行追蹤變得更具挑戰性。

1. LockBit	2. Conti	3. Pysa	4. Grief	5. Hive
6. CIOP	7. Marketo	8. Everest	9. LV	10. REvil

Copyright © 2002-2021 Acronis International GmbH.

每日勒索軟體偵測數量

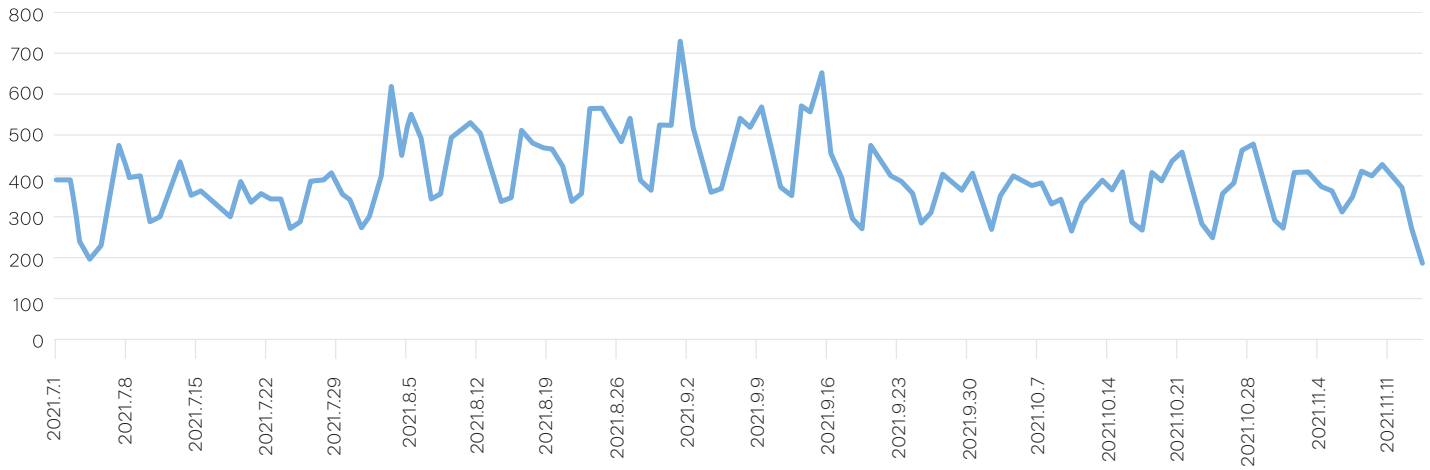
在夏季達到高點后，勒索軟體案件數量在第三季度有些許下降。從 7 月到 8 月，我們在全球範圍阻止的勒索軟體攻擊增加了 32.7%，接著在 9 月減少了 7%，在 10 月減少了 16%。

此波動背後的原因有很多。一方面，針對勒索軟體集團進行了執法行動後，進行了幾次抓捕行動，從而帶來了更大的壓力。另一個方面，一些攻擊在攻擊鏈早期被阻止，例如，在電子郵件誘餌或惡意 URL 中，以致最終勒索軟體從未被下載，因此無法計入此圖表中。

每個地區每月的勒索軟體偵測數量的變化

月份	歐洲、中東及非洲地區	美洲	亞洲	全球
7 月到 8 月	26.5%	19.4%	64.7%	32.7%
8 月到 9 月	-6.2%	-2.9%	-9.1%	-7.0%
9 月到 10 月	-13.2%	-21.0%	-17.2%	-16.0%

全球每日勒索軟體偵測數量



Copyright © 2002-2021 Acronis International GmbH.

前 10 個國家/地區：依區域排列的勒索軟體偵測數量佔比

亞洲

國家/地區	2021 年第 3 季度區域性勒索軟體偵測數量百分比	2021 年第 2 季度區域性勒索軟體偵測數量百分比
日本	31.61%	38.09%
以色列	8.49%	2.55%
中國	7.92%	8.59%
印度	7.34%	3.65%
韓國	5.50%	5.51%
土耳其	5.44%	5.51%
台灣	4.91%	5.43%
菲律賓	4.70%	4.16%
泰國	2.95%	2.55%
印尼	2.75%	2.06%

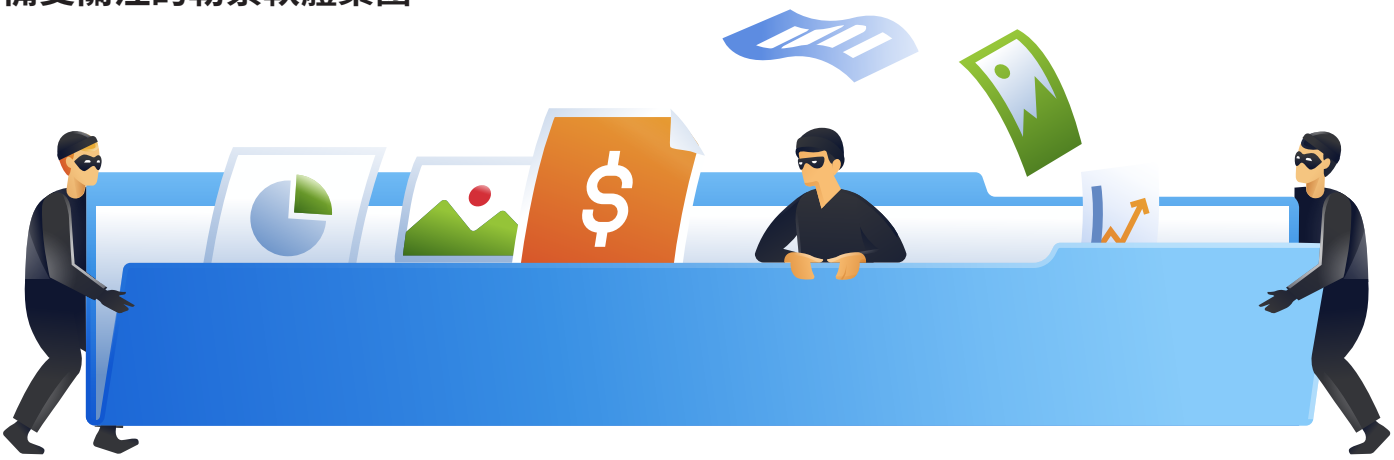
歐洲、中東及非洲地區

國家/地區	2021 年第 3 季度區域性勒索軟體偵測數量百分比	2021 年第 2 季度區域性勒索軟體偵測數量百分比
德國	43.37%	45.17%
英國	9.64%	9.46%
法國	9.00%	9.37%
瑞士	7.98%	8.45%
義大利	5.65%	5.50%
荷蘭	3.28%	4.04%
西班牙	3.07%	2.85%
奧地利	3.01%	3.13%
比利時	2.31%	2.33%
捷克共和國	1.65%	1.38%

Copyright © 2002-2021 Acronis International GmbH.

國家/地區	2021 年第 3 季度區域性勒索軟體偵測數量百分比	2021 年第 2 季度區域性勒索軟體偵測數量百分比
美國	79.03%	79.64%
加拿大	12.05%	12.14%
墨西哥	2.20%	2.15%
巴西	1.73%	2.09%
阿根廷	0.93%	0.49%
哥倫比亞	0.86%	0.64%
智利	0.44%	0.48%
祕魯	0.39%	0.46%
玻利維亞	0.29%	0.11%
瓜地馬拉	0.26%	0.22%

備受關注的勒索軟體集團



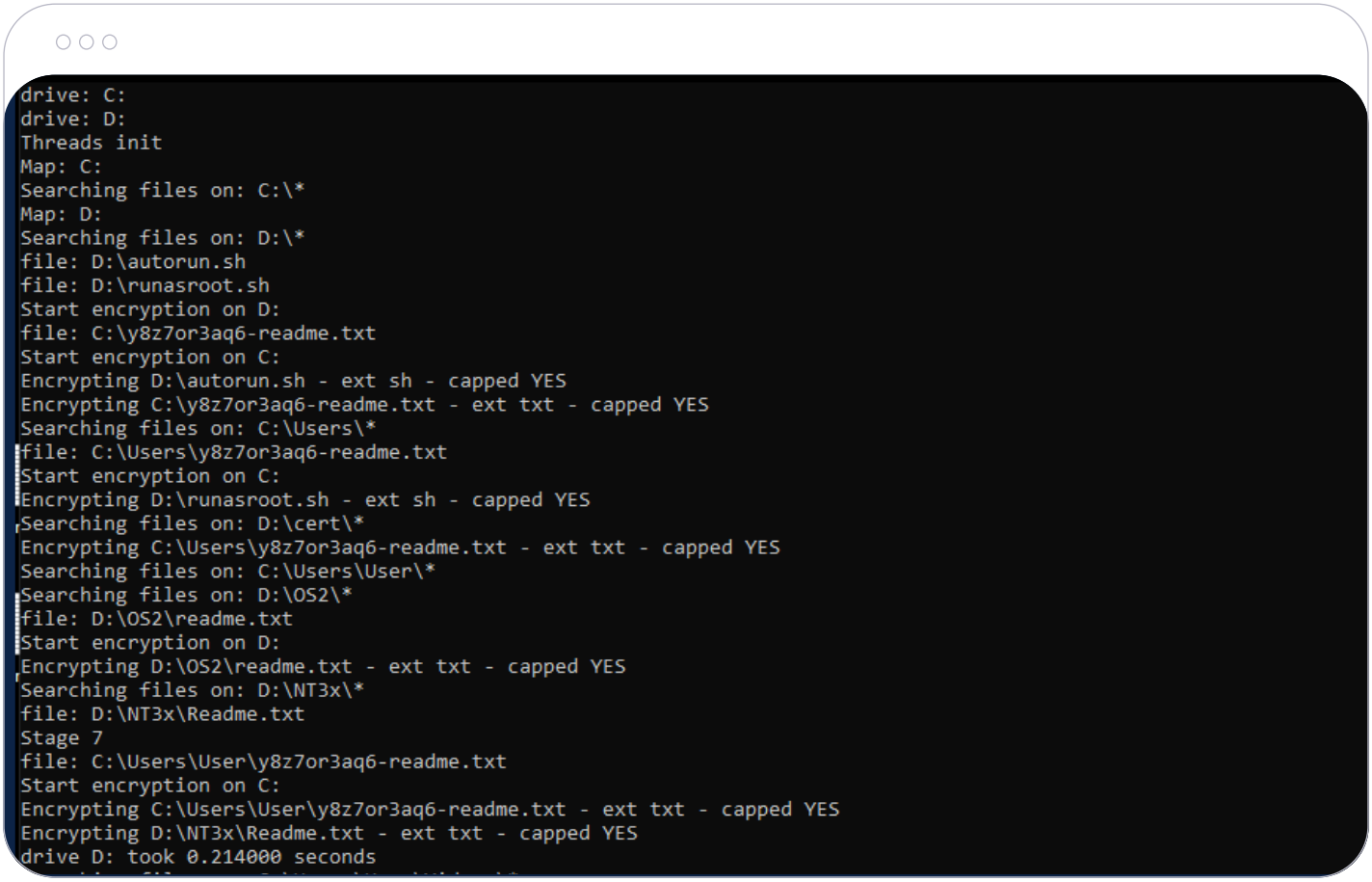
AvosLocker 勒索軟體

勒索軟體 AvosLocker 在 2021 年 6 月底被發現。如 **Twitter 貼文**中所指，罪犯開始透過各種 DarkWeb 論壇搜尋附屬公司。他們還聲稱招聘了滲透測試人員，這些測試人員已與 Active Directory 和可遠端存取遭駭客入侵的基礎架構的「存取代理人」進行了合作。在另一篇貼文中，他們提供了勒索軟體即服務，此服務將提供一段以 C++ 撰寫、具有可覆寫受害者檔案的多執行緒功能的惡意程式碼，使用已加密的內容（而非透過建立檔案複本）。AvosLocker 以垃圾電子郵件的形式散播，主要目標為 Windows 機器，針對檔案加密使用 AES-256-CBC，針對檔案金鑰加密使用 RSA-1024。它將加密網路共用，並終結可能會阻止存取的相關聯執行序。

Copyright © 2002-2021 Acronis International GmbH.

執行

依預設，勒索軟體以主控台應用程式的方式工作，將執行記錄輸出到主控台。一般由在遠端存取機器的攻擊者手動執行。



該記錄表明，AvosLocker 會先尋找可存取的驅動程式並列出根據副檔名篩選的所有檔案，這些檔案將隨後被加密。加密的檔案會在原始檔案名中附加「.avos」或「.avos2」副檔名。

如前面所述，勒索軟體由攻擊者手動在機器上部署。在執行期間，它會產生已執行動作的記錄，以便攻擊者能夠實時觀察程式正在執行什麼作業。爲了躲避簽章型偵測，勒索軟體將使用字串混淆處理。AvosLocker 不會使用任何 packer 或加密程式來隱藏其內容。

可以使用下列命令列引數選取作業模式：

- **'h'** - 啟用隱藏模式。
- **'n'** - 啟用網路共用資料夾和磁碟機加密。

Copyright © 2002-2021 Acronis International GmbH.

```
sub_408E36      proc near               ; CODE XREF:

var_18          = byte ptr -18h
var_17          = byte ptr -17h
var_10          = xmmword ptr -10h

                push    ebp
                mov     ebp, esp
                sub     esp, 18h
                push    esi
                mov     esi, ecx
                test    esi, esi
                jz      loc_408EE8
                push    esi
                call    sub_42CBD0
                pop     ecx
                cmp     eax, 1
                jb      loc_408EE8
                push    ebx
                push    68h ; 'h'       ; hide
                push    esi
                call    sub_427810
                pop     ecx
                xor     ebx, ebx
                pop     ecx
                test    eax, eax
                jz      short loc_408E9D ; network
                movaps  xmm0, ds:xmmword_458210
                mov     ecx, ebx
                movups  [ebp+var_10], xmm0
loc_408E75:                             ; CODE XREF: sub_
                mov     al, byte ptr [ebp+var_10]
                xor     byte ptr [ebp+ecx+var_10+1], al
                inc     ecx
                cmp     ecx, 0Eh
                jb      short loc_408E75
                lea     eax, [ebp+var_10+1]
                mov     byte ptr [ebp+var_10+0Fh], bl
                push    eax
                call    sub_401466
                pop     ecx
                push    ebx             ; nCmdShow
                call    ds:GetConsoleWindow
                push    eax             ; hWnd
                call    ds:ShowWindow
loc_408E9D:                             ; CODE XREF: sub_
                push    6Eh ; 'n'       ; network
                push    esi
                call    sub_427810
                pop     ecx
                pop     ecx
                test    eax, eax
                jz      short loc_408EE7
                movaps  xmm0, ds:xmmword_458AE0
                mov     ecx, ebx
                movups  xmmword ptr [ebp-18h], xmm0
                mov     dword ptr [ebp+var_10+8], 6C67226
                mov     dword ptr [ebp+var_10+0Ch], 86F77
loc_408EC6:                             ; CODE XREF: sub
```

此勒索軟體會檢查 Mutex‘ievah8eVki3Ho4oo’，以防一次執行多個執行個體。如果 Mutex 已經存在，則勒索軟體會結束。

```
.text:00408F1D loc_408F1D:                             ; CODE XREF: sub_408EEB+3D↓j
.text:00408F1D                  mov     al, [ebp+Name]
.text:00408F20                  xor     [ebp+ecx+Name+1], al
.text:00408F24                  inc     ecx
.text:00408F25                  cmp     ecx, 10h
.text:00408F28                  jb      short loc_408F1D
.text:00408F2A                  mov     byte ptr [ebp+var_14+1], bl
.text:00408F2D                  lea     eax, [ebp+Name+1]
.text:00408F30                  push    eax             ; lpName
.text:00408F31                  push    1               ; bInitialOwner
.text:00408F33                  push    ebx             ; lpMutexAttributes
.text:00408F34                  call    ds:CreateMutexA
.text:00408F3A                  test    eax, eax
.text:00408F3C                  jz      loc_40909F
.text:00408F42                  call    ds:GetLastError
.text:00408F48                  cmp     eax, 0B7h ; '·' ; check if ransomware is already running
.text:00408F4D                  jz      loc_40909F
.text:00408F53                  call    sub_4293F5      ; clock
.text:00408F58                  mov     edi, eax
.text:00408F5A                  mov     [ebp+var_28], edi
```

這讓惡意程式碼分析和偵測變得更加困難。

Copyright © 2002-2021 Acronis International GmbH.

檔案加密

關於資料加密，AvosLocker 針對檔案加密使用 AES-256-CBC，使用 RSA-1024 來加密產生的檔案金鑰。此模式在勒索軟體集團中似乎很受歡迎，因爲這使得受害者不得不購買一個解密軟體來還原其檔案。

主 RSA 公開金鑰以二進位進行硬式編碼處理：

```
.data:00460208 aBeginPublicKey_0 db '-----BEGIN PUBLIC KEY-----',0Ah
.data:00460208                                         ; DATA XREF: sub_408EEB+72↑o
.data:00460208                   db 'MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA12M9w7AbAwkIOSUh0DgI',0Ah
.data:00460208                   db 'FQUJGNhRQxdfkiQ4rh9xw1HFnfdTbLpFm8wQqsgSEK1IwtScazTANyOC8s8yzi7p',0Ah
.data:00460208                   db 'oSSZnGnGF84Wwn3wYh8i2FK9HyKoc+cQ1Lzju0+ZXvnA09LLiOBU6k/avPpjH7Ht',0Ah
.data:00460208                   db 'nlJvdcBjlZ6LVlcNb+ydZfsFaQHWaSnH2hRTFF4l1iwL2XusaXtWom1pl1oCo6sg',0Ah
.data:00460208                   db 'ZB7yuwikFFaWosazVfylr5jn0pxSsVnav2wFgri4RbXFhISe0tIAE4damx+6hf2V',0Ah
.data:00460208                   db 'xyGPVn3Riy+zyO9JsNmQoADmc7wJ7bWKvEo/iIfoVI/2lpD/HfZeTXi7uBPYzBkg',0Ah
.data:00460208                   db 'twIDAQAB',0Ah
.data:00460208                   db '-----END PUBLIC KEY-----',0
.data:004603CB                   align 10h
```

如果主 RSA 公開金鑰不可用，就會產生新的 RSA 金鑰組。爲了解鎖應用程式目前開啓的使用者檔案，例如資料庫和文件，加密鎖定軟體會終結與這些檔案類型相關聯的執行序。相關聯的執行序清單可使用 **RmGetList() WinAPI 呼叫**取得：

```
.text:00402CFB    lea     eax, [ebp+dwRebootReasons]
.text:00402D01    mov     [ebp+pnProcInfo], 0Ah
.text:00402D0B    push    eax             ; lpdwRebootReasons
.text:00402D0C    lea     eax, [ebp+var_1A6C]
.text:00402D12    push    eax             ; rgAffectedApps
.text:00402D13    lea     eax, [ebp+pnProcInfo]
.text:00402D19    push    eax             ; pnProcInfo
.text:00402D1A    lea     eax, [ebp+pnProcInfoNeeded]
.text:00402D20    push    eax             ; pnProcInfoNeeded
.text:00402D21    push    [ebp+pSessionHandle] ; dwSessionHandle
.text:00402D27    call    ds:RmGetList
.text:00402D2D    test    eax, eax
.text:00402D2F    jnz     loc_402FA1
.text:00402D35    and     [ebp+var_1A9C], eax
.text:00402D3B    cmp     [ebp+pnProcInfo], eax
.text:00402D41    jbe     loc_402FA1
.text:00402D47    lea     eax, [ebp+var_1A6C]
.text:00402D4D    mov     [ebp+var_1A90], eax
```


Copyright © 2002-2021 Acronis International GmbH.

將為每個檔案產生一個唯一 **AES 金鑰**和**初始化向量 (IV)**。

```
.text:004082CE loc_4082CE:                             ; CODE XREF: sub_407E8A+3F91j
.text:004082CE                 lea     edx, [ebp+var_B0] ; aes key
.text:004082D4                 lea     ecx, [ebp+var_4A8] ; aes ctx
.text:004082DA                 call    sub_4010A0      ; AES init
.text:004082DF                 push    10h
.text:004082E1                 lea     eax, [ebp+var_30]
.text:004082E4                 push    eax
.text:004082E5                 lea     eax, [ebp+var_3B8]
.text:004082EB                 push    eax
.text:004082EC                 call    sub_4257B0
.text:004082F1                 add     esp, 0Ch
.text:004082F4                 call    sub_4293F5
.text:004082F9                 mov     eax, large fs:30h
.text:004082FF                 mov     eax, [eax+0Ch]
.text:00408302                 mov     eax, [eax+0Ch]
```

之後，**檔案內容將由加密的資料取代**，這使得還原原始檔案變得更加困難。

```
loc_408575:                                ; CODE XREF: sub_40
                                           ; sub_407E8A+6E1↑j
                push    0
                lea     eax, [ebp+var_3A8]
                push    eax
                push    edi
                lea     eax, [ebp+var_70]
                push    eax
                push    ebx
                call    [ebp+var_4D4]   ; read file
                mov     eax, [ebp+var_3A8]
                push    1
                push    0
                neg     eax
                push    eax
                push    ebx
                call    [ebp+var_4B8]   ; set file pointer
                mov     edx, [ebp+var_3A8]
                push    40h ; '@'
```


Copyright © 2002-2021 Acronis International GmbH.

```
.text:00408637 loc_408637:                             ; CODE XREF: sub_407E8A+7
.text:00408637                                         ; sub_407E8A+796↑j
.text:00408637                 push    ecx
.text:00408638                 lea     edx, [ebp+var_70]
.text:0040863B                 lea     ecx, [ebp+var_4A8]
.text:00408641                 call    sub_401329      ; aes crypt
.text:00408646                 pop     ecx
.text:00408647                 push    0
.text:00408649                 lea     eax, [ebp+var_3A4]
.text:0040864F                 push    eax
.text:00408650                 push    edi
.text:00408651                 lea     eax, [ebp+var_70]
.text:00408654                 push    eax
.text:00408655                 push    ebx
.text:00408656                 call    esi             ; write file
```

隨機金鑰的產生借助於 **CryptGenRandom() WinAPI 函式**完成，此函式是 Microsoft 密碼編譯提供者的一部分。

```
.text:00403179                 push    0F0000040h      ; dwFlags
.text:0040317E                 mov     [ebx+4], eax
.text:00403181                 xor     eax, eax
.text:00403183                 push    1               ; dwProvType
.text:00403185                 push    eax             ; szProvider
.text:00403186                 push    eax             ; szContainer
.text:00403187                 mov     [ebp+phProv], eax
.text:0040318D                 lea     eax, [ebp+phProv]
.text:00403193                 push    eax             ; phProv
.text:00403194                 call    ds:CryptAcquireContextA
.text:0040319A                 mov     esi, 200h
.text:0040319F                 test    eax, eax
.text:004031A1                 jz      short loc_403200
.text:004031A3                 lea     eax, [ebp+pbBuffer]
.text:004031A9                 push    eax             ; pbBuffer
.text:004031AA                 push    esi             ; dwLen
.text:004031AB                 push    [ebp+phProv]    ; hProv
.text:004031B1                 call    ds:CryptGenRandom
.text:004031B7                 test    eax, eax
.text:004031B9                 jnz     short loc_4031F0
.text:004031BB                 mov     ecx, esi
.text:004031BD                 call    sub_4030C9      ; rand
```


Copyright © 2002-2021 Acronis International GmbH.

檔案被加密後，勒索軟體將在已加密檔案的結束處儲存一個使用主 RSA 公開金鑰加密、Base64 編碼的 AES 檔案金鑰。

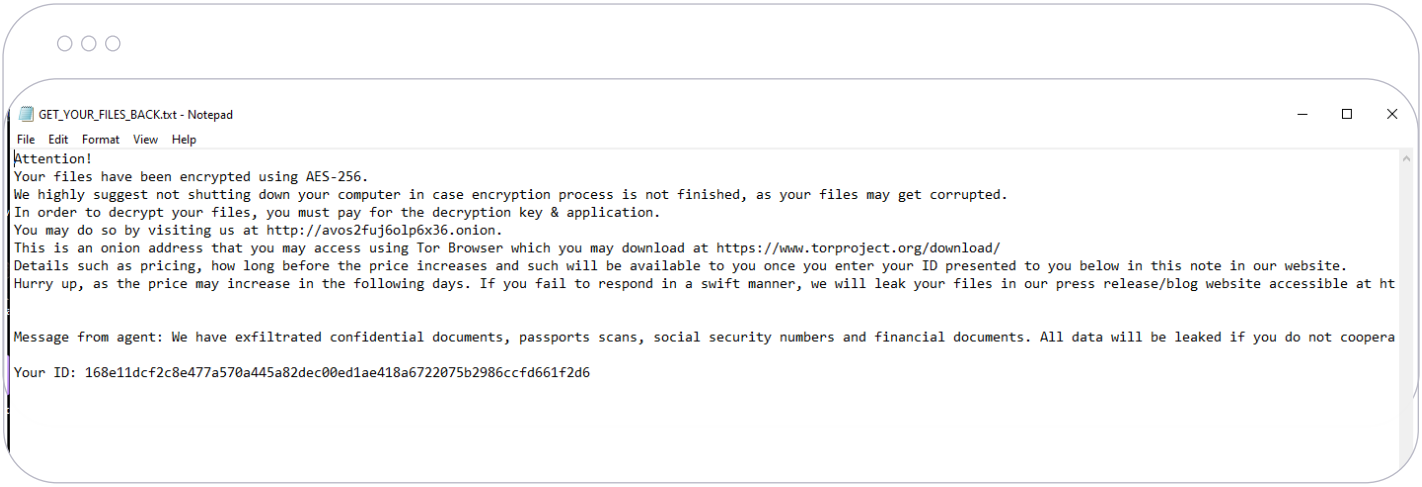
勒索軟體在多個執行緒中執行檔案加密。命令列引數「n」已指定時，則它開始會加密網路資源。具有以下副檔名的檔案將被搜尋到並儲存在清單 (隨後提交以進行加密) 中：

ndoc docx xls xlsx ppt pptx pst ost msg eml vsd vsdx txt csv rtf wks wk1 pdf dwg onetoc2 snt jpeg jpg docb docm dot dotm dotx xlsm xlsb xlw xlt xlm xlc xltx xltm pptm pot pps ppsm ppsx ppam potx potm edb hwp 602 sxi sti sldx sldm sldm vdi vmdk vmx gpg aes ARC PAQ bz2 tbk bak tar tgz gz 7z rar zip backup iso vcd bmp png gif raw cgm tif tiff nef psd ai svg djvu m4u m3u mid wma flv 3g2 mkv 3gp mp4 mov avi asf mpeg vob mpg wmv fla swf wav mp3 sh class jar java rb asp php jsp brd sch dch dip pl vb vbs ps1 bat cmd js asm h pas cpp c cs suo sln ldf mdf ibd myi myd frm odb dbf db mdb accdb sql sqlitedb sqlite3 asc lay6 lay mml sxm otg odg uop std sxd otp odp wb2 slk dif stc sxc ots ods 3dm max 3ds uot stw sxw ott odt pem p12 csr crt key pfx der dat

Copyright © 2002-2021 Acronis International GmbH.

贖金備註

AvosLocker 提交了一份贖金備註 **GET_YOUR_FILES_BACK.txt**，其中包含資料洩漏網站和受害者 ID 的連結。



進入資料洩漏網站時，**受害者會被要求提供贖金備註儲存的 I.D.。**該資料洩漏網站接著會提供客戶支援功能。還有包含拒絕付款之受害者的外洩資料的「新聞發佈」。

結論

AvosLocker 是現代勒索軟體即服務的典型範例，提供了一個包含對稱式 AES-256-CBC 和非對稱式 RSA-1024 演算法的增強式加密方案，這些演算法可在多個執行緒中執行。複製的檔案不會被加密，但檔案的內容將被取代為加密的資料。該勒索軟體配備有基本的混淆處理演算法，以防止二進位被 AV 簽名掃描器偵測到。此外，AvosLocker 還可以將網路資源與本機和對應磁碟機一起加密。與其他 RaaS 集團一樣，AvosLocker 也擁有自己的資料洩漏網站，罪犯在該網站中提供受害者支援，以及發佈那些尚未付款之受害者的被竊取資料。

Copyright © 2002-2021 Acronis International GmbH.

惡意網站

2021 年第三季度，平均 1.9% 的端點嘗試了存取一些惡意 URL，較第二季度的 1.8% 稍微上升。10 月，我們發現突增到 4.3%，這與我們發現進入使用者收件匣之網路釣魚電子郵件數量的突增有關。

月份	點擊了惡意 URL 之使用者的百分比
1 月	3.2%
2 月	2.9%
3 月	2.1%
4 月	1.8%
5 月	1.9%
6 月	1.8%
7 月	1.9%
8 月	1.8%
9 月	2.1%
10 月	4.3%

2021 年第三季度惡意 URL 阻止率最高的是美國，佔 26.8%，其次是德國的 20%，以及加拿大的 8.7%，這些被阻止的 URL 中有 65% 由 HTTPS 加密，這使得網路分析和篩選變得更加困難。

我們觀察到越來越多的集團關注瀏覽器使用者代理程式請求網站。自動化掃描工具以乾淨的引誘網站（而非真正承載）形式提供，它不會模仿一般使用者。類似的情況還會發生在將取代 URL 引數的解決方案上，例如電子郵件地址，出於隱私原因，在它們被傳遞到網站時。一些工具組擁有一個總和檢查碼，此檢查碼可偵測該變更並改爲提供一個良性網站。已知誘轉型詐騙策略也出現了小幅增加，該策略中電子郵件中的 URL 會指向一個開始很乾淨的網站，幾小時後會切換最終的惡意承載，希望任何初始電子郵件掃描器已將連結標記爲非惡意。

Copyright © 2002-2021 Acronis International GmbH.

2021 年第 3 季度被阻止 URL 數量最多的前 20 個國家/地區：

排名	國家/地區	被阻止的 URL 數量的百分比，2021 年第 3 季度
1	美國	26.8%
2	德國	20.0%
3	加拿大	8.7%
4	英國	7.2%
5	義大利	5.1%
6	荷蘭	3.4%
7	新加坡	3.2%
8	比利時	3.1%
9	法國	3.0%
10	日本	2.9%
11	澳大利亞	2.0%
12	瑞士	1.9%
13	西班牙	1.8%
14	泰國	1.6%
15	奧地利	0.9%
16	俄羅斯	0.8%
17	巴西	0.7%
18	哥斯大黎加	0.7%
19	祕魯	0.7%
20	土耳其	0.6%

Copyright © 2002-2021 Acronis International GmbH.

Windows OS 與軟體中的弱點

第 3 部分

由於弱點是滲透系統的關鍵因素之一，因此它們不斷地被搜尋、使用，並最終被修補 (不幸的是，修補並不總是成功且不準時)。2021 年下半年這種情況并沒有任何突破性進展，而是證明了一個令人擔憂的事實，即越來越多的關鍵弱點正在被網路罪犯發現和利用。從 7 月到 10 月我們每個月都進行了完整的分析，軟體廠商發佈的修補程式數量仍然是以數十個為單位計算 (而不是幾百)。

和以前一樣，最常用的瀏覽器 Google Chrome 也遭受了猛烈的攻擊。他們不得不為瀏覽器發佈一個緊急安全性修補程式，以修補自然環境中正在被積極利用的零時差弱點。Google 沒有提供關於 CVE-2021-37973 弱點的技術詳情，但此弱點是接著 19 個其他弱點之後被發現和修補的，這些弱點會對 Mac、Windows 及 Linux 版本的 Chrome 產生影響。隨後，Google 發佈了 Windows、Mac 和 Linux 版 Chrome 更新 95.0.4638.69，以修補包含兩個被積極利用的零時差攻擊在內的七個弱點。CVE-2021-38000 和 CVE-2021-38003 這兩個零時差攻擊弱點已被評為高嚴重性。它們皆由 Google 自己的威脅分析團隊發現。

這些最新發現使得今年到目前爲止 Chrome 瀏覽器中已修補的零時差攻擊弱點總數達到 15。這相當於每個月 1.5 個零時差攻擊弱點。

Microsoft 在修補其產品中弱點這方面一直做得不錯。從 7 月開始：它們發佈了 117 個軟體安全性修正程式，其中包括 Pwn2Own 競賽參與者在 Exchange Server 中發現的遠端程式碼執行 (RCE) 弱點。有 13 個弱點被認爲嚴重，9 個是零時差攻擊，其中有 4 個正在自然環境中被積極利用。然而，Microsoft Exchange Server 中的一組三個舊弱點可能被鏈接起來，從而讓攻擊者執行未驗證的遠端程式碼執行。此在受害者機器上執行任意程式碼和指令的潛能使得威脅執行者掃描容易受到攻擊的伺服器。這三個弱點中有兩個是在四月 Microsoft 修補程式星期二錯誤修復中修補，第三個是在五月修補的。然而，儘管提供了修補程式，Exchange 誘捕系統顯示，攻擊者在過去的幾周仍積極地在未修補的伺服器上搜尋並利用這些弱點。

8 月，有 44 個弱點被涵蓋，其中一個十分有趣：攻擊者使用了 CVE-2021-36948，其利用了 Windows Update Medic 服務中的弱點。這個新服務可讓使用者修復受損狀態下的 Windows 更新元件，以便裝置能繼續接收更新。該瑕疵是一個「權限提高」弱點，會影響 Windows 10 和 Windows Server 2019，這意味著它可以與另一個弱點結合使用，讓攻擊者以系統管理員身份在容易遭受攻擊的系統上執行其選擇的程式碼。

Copyright © 2002-2021 Acronis International GmbH.

9 月發行了 85 個修補程式，包括一個針對當月發現的 MSHTML 弱點，以及 Open Management Infrastructure 中的一個嚴重遠端程式碼執行弱點，和兩個其他嚴重弱點，餘下的弱點根據 Microsoft 的弱點評級被認爲是重要。三個嚴重弱點由 Microsoft 修補，包括一個針對 Win32k (Windows 使用的驅動程式)，該弱點可能導致權限提高。它正在被積極地利用。這兩個辦公室套件的弱點仍在按嚴重性進行分級，但可能非常嚴重。

除了 Microsoft 發行的針對 37 個產品的 85 個修補程式，Apple 還在九月修補了五個弱點。macOS 和 Safari 中已修補的 Apple 弱點允許任意程式碼的執行，而 Chrome 更新則包含九個弱點的修補程式，這些弱點包含兩個已在自然環境中被利用的零時差攻擊弱點。

Microsoft 的 10 月 (星期二) 修補程式修復了四個零時差攻擊和 81 個瑕疵，其中有一個針對 Microsoft Edge，正在被修補中。OpenOffice 和 LibreOffice 都收到了針對類似問題的三個獨立修補程式。

11 月，Microsoft 針對 Microsoft Windows 和 Windows 元件 Azure、AzureRTOS、AzureSphere、MicrosoftDynamics、Microsoft Edge、Exchange Server、Microsoft Office 和 Office 元件、Windows Hyper-V、Windows Defender，及 Visual Studio 中的 55 個新 CVE 發行了修補程式。其中 6 個的嚴重性等級為嚴重，49 個為重要。兩個弱點在發行時被列爲正在被積極利用。

Adobe 也做了大量的修補工作。7 月，它發行了五個修補程式，用來解決 Adobe Dimension、Illustrator、Framemaker、Acrobat Reader 以及 Adobe Bridge 中的 29 個 CVE。8 月，又解決了 29 個 CVE，填補了 Adobe Connect 和 Magento 中的弱點。Magento 嚴重級別的修補程式修復了各種錯誤，其中最嚴重的可允許遠端程式碼的執行。九月，Adobe 發行了 15 個修補程式，涵蓋 59 個 CVE；10 月，Adobe Reader、Acrobat Reader for Android、Adobe Campaign Standard、Commerce、Ops-CLI 以及 Adobe Connect 中有 10 個 CVE。但重要的是，在今年十月的安全性修補程式後的兩周，Adobe 又發佈了 14 個安全性公告，涵蓋 92 個 CVE 列出的錯誤。這些修補程式包含 61 個嚴重錯誤，其中很多都允許任意程式碼的執行。

威脅執行者正在不斷地利用弱點和零時差攻擊，因此保持修補程式的更新非常重要。Acronis Cyber Protect 透過其修補程式管理解決方案讓這變得很簡單，更新變得既快又輕鬆。

Copyright © 2002-2021 Acronis International GmbH.

2022 年
安全性預測

第 4 部分

隨著 COVID-19 疫情的散播，每個人都必須適應一個完全不同、充滿挑戰的生活習慣，幾乎沒人做好該準備。這完全改變了 2021 年的安全性態勢。以下是可能定義 2022 年網路安全性態勢的重要趨勢。

1. 儘管美國和國際/歐洲刑警組織做出了努力，勒索軟體仍在不斷地增長和發展

勒索軟體是目前最賺錢的網路攻擊之一。儘管最進進行了幾次抓捕行動，但目前還看不見結束的跡象。勒索軟體將進一步擴展到 macOS 和 Linux，以及虛擬系統、雲端和 OT/IoT 等新環境中。連接至可存取網路的任何內容都是潛在的目標。這將越來越多地在現實世界中造成後果和影響，從而還要求官方法規和制裁。竊取資料來進行雙重敲詐勒索以及停用安全工具將成爲常態；但對於內部威脅和個人資料而言，它還會變得更加個人化。

混亂情況將繼續，因爲一些集團會繼續進行品牌重塑來抵禦調查，而勒索軟體即服務將并購更小等級的集團，允許不同系列的重疊使用。展望未來，我們能夠預計到這種彈性和靈活性會持續，因此，到 2022 年底，勒索軟體作業相較於我們今天所看到的可能更無法識別。

Copyright © 2002-2021 Acronis International GmbH.

2. 加密貨幣將成爲攻擊者的最愛

隨著比特幣價格的居高不下，攻擊數量因威脅執行者追蹤利潤而不斷地增加。在相當長的一段時間，終端使用者一直在與網路釣魚攻擊、infostealer 和在記憶體中交換錢包地址的惡意軟體作鬥爭。我們預計會看到更多這類直接針對智慧合約的攻擊 — 攻擊加密貨幣核心的程式。我們還預計，針對 Web 3.0 應用程式的攻擊在 2022 年會更頻繁地出現。這些新的市場為複雜的攻擊 (例如閃貸攻擊) 提供了新的機會，可能會讓攻擊者從加密貨幣流動池抽取數百萬美元。

3. 網路釣魚將繼續成爲主要的感染載體

各種形式的惡意電子郵件和網路釣魚目前仍在最高點。儘管一直在進行意識宣傳活動，使用者仍會落入它們的圈套，讓攻擊者入侵其組織。我們不期望 AI 在 2022 年完全接管網路釣魚，但是希望隨著這些各種資料泄露，自動化和個人化資訊會增加，讓其更高效。針對 OAuth 和 MFA 的新伎倆將繼續為攻擊者帶來利潤，允許他們接管帳戶，儘管 Google 等公司計劃自動註冊 1.5 億使用者到 2FA。為避開常見的防網路釣魚工具，商務電子郵件入侵 (BEC) 等攻擊將使用替代訊息服務，例如簡訊、Slack 或 Teams 聊天。這與合法電子郵件通訊服務的劫持密切相關，例如在 11 月，FBI 自己的電子郵件服務遭入侵並開始傳送垃圾電子郵件。

4. 合作夥伴 (MSP) 會透過他們使用的工具成爲目標

攻擊者正在追蹤那些可讓他們獲取公司網路存取權的信任連接。軟體供應鏈攻擊是這些方式中的一種，但即使沒有廠商的完全妥協，還是有類似的方式進入。攻擊者將追蹤管理員使用的管理工具，例如專業服務自動化 (PSA) 軟體或遠端監控與管理 (RMM) 工具。它們是通往王國的鑰匙，網路罪犯將用它們來對付您。服務供應商尤其會更頻繁地成爲目標，因爲他們通常擁有很多自動化工具來高效地推出新軟體。不幸的是，目前攻擊者這樣做是爲了散播惡意軟體。這可以與原始程式碼層級上的供應鏈攻擊一起或并行進行。我們預計，當所使用的應用程式或程式庫的原始程式碼被惡意修改時，會出現越來越多的攻擊。

5. 信任在雲端層級上受損：API 攻擊

雲端服務正在激增，無伺服器運算、邊緣運算以及 API 服務也在激增。與 Kubernetes 之類的容器協作結合在一起，執行序可更高效地自動化並動態適應各種情形。攻擊者將嘗試透過追蹤此類 API 來中斷此高度自動化，這可能會嚴重影響一個公司的業務處理。

6. 所有人的資料外洩

儘管資料隱私權法規有所加强，但報告的資料外洩數量也會繼續增加。這不僅僅是因爲它們必須報告出來，還因爲複雜的互動和 IT 系統。很多公司已經不知道它們所有的資料在哪，以及如何存取資料。而來自 IoT 服務和 M2M 通訊的自動化資料交換進一步增加了資料的傳播。不幸的是，我們預計，在 2022 年會看到很多大規模的資料外泄。這些資料外泄會讓攻擊者輕鬆地充實他們的目標檔案。

Copyright © 2002-2021 Acronis International GmbH.

7. AI 中的對抗性攻擊

由於 AI 越來越頻繁地被用來 IT 系統中的異常和保護其中的任何寶貴資產，攻擊者將越來越多地嘗試攻擊 AI 模型中的邏輯是可以理解的。在 AI 模型內成功地逆轉決策可讓攻擊者保持不被發現或產生一個不想要狀態的阻斷服務攻擊。還可以讓他們識別時間問題，而緩慢的變化不會被視爲異常，因此不會被阻止。

8. 安全性產品的統一：單一廠商模式

爲了更好地準備應對上述的所有威脅，企業必須偏袒那些在一個產品或一系列產品下提供了更廣覆蓋範圍的安全性廠商。這有助於最小化供應鏈攻擊，並實現更快的互動和復原，這對保持業務正常運轉至關重要。網路罪犯受利潤驅動，將試圖透過自動化他們的業務並攻擊最容易暴露的公司來最大化他們的收益。他們積極地抓住他們能夠發現的每個機會，因此擁有 MFA 強式驗證、及時的弱點修補以及整個基礎架構的可見性非常重要。

在 2022 年保持安全

不幸的是，企業仍在努力跨雲端、辦公室和家庭辦公室的複雜生態系統高效地保護它們的整個工作負載。做到這一點需要高效的解決方案，此方案將網路安全性與資料防護以及端點的管理和監控整合在一起。此全方位網路防護方法允許對大量網路威脅進行自動回應。

Copyright © 2002-2021 Acronis International GmbH.

Acronis 關於在目前和未來威脅環境中保持安全的建議

第 5 部分

現代網路攻擊、資料洩漏和勒索軟體爆發都表明了同一件事：網路安全是失敗的。出現此失敗狀況的原因是，技術薄弱和聰明的社交工程導致人爲錯誤。在備份解決方案運作良好且未被盜用的情況下，通常需要幾小時和幾天的時間來將系統（含資料）還原至運作狀態。網路安全解決方案失敗時，備份是必要；但同時備份解決方案可能會被盜用、停用，緩慢地執行，導致企業因停機時間而損失大量的資金。

爲了解決這些問題，我們建議使用整合式網路防護解決方案，例如 Acronis Cyber Protect，它將防惡意軟體、EDR、DLP、電子郵件安全性、弱點評估、修補程式管理、RMM 及備份功能結合在一系列 Windows 作業系統下執行的單一代理程式。此整合可讓您維持最佳的效能、消除相容性問題，及確保快速地復原。如果在資料改動期間未發現或偵測到一個威脅，則該資料將立即從備份中還原，因爲它的一個代理程式知道資料已遺失且需要還原。

當防惡意軟體代理程式與擁有自己的代理程式的備份產品分開時，這一點無法實現。您的防惡意軟體解決方案可能會停止威脅，但部分資料可能已經遺失。備份代理程式不會自動知道它，最好的情況下資料會被緩慢地還原 (如果有的話)。

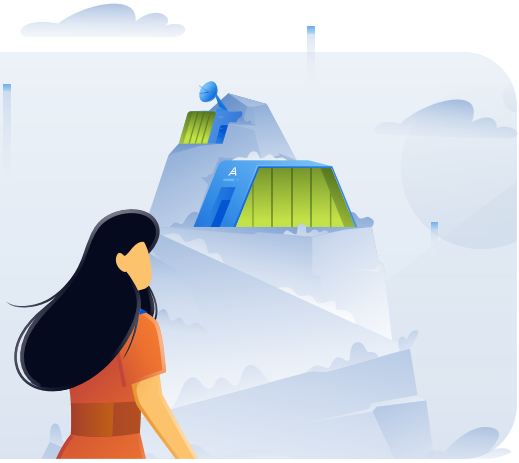
當然，Acronis Cyber Protect Cloud 會在威脅危害環境之前偵測並消除它們，努力讓資料復原不需要進行。這會透過我們增强的多層網路安全性功能實現。

Copyright © 2002-2021 Acronis International GmbH.

修補您的作業系統和應用程式

修補非常關鍵，因爲很多攻擊因未修補的弱點而成功進行。藉由 Acronis Cyber Protect 之類的解決方案，您就被內嵌式弱點評估和修補程式管理功能所覆蓋。我們會追蹤所有已發現的弱點和已發行的修補程式，並允許管理員或技術人員使用靈活的組態和詳細的報告來輕鬆地修補所有端點。Acronis Cyber Protect 支援所有內嵌式 Windows 應用程式以及 230 個以上的熱門第三方應用程式，其中包括 Zoom 和 Slack 之類的電信工具，及遠端工作中使用的熱門 VPN 用戶端。請確保先修補高嚴重性的弱點，並遵循成功報告來檢查修補程式是否已正確套用。

若您沒有 Acronis Cyber Protect 且/或未使用任何修補程式管理軟體，事情就會困難很多。 至少，您將需要確定 Windows 獲取它需要的所有更新，并且這些更新已及時安裝。使用者常常會忽略系統郵件，尤其在 Windows 要求重新啟動時。這是一個很嚴重的錯誤。確保 Adobe 之類的熱門軟體廠商的自動更新已啟用，且 PDF Reader 之類的應用程式也及時進行了更新。



準備好隨時應對網路釣魚嘗試，不要按下可疑的連結

主題型網路釣魚和惡意網站每天都會大量地出現，且通常在瀏覽器層級被篩選出來，但是有了 Acronis Cyber Protect 之類的網路防護解決方案后，您還會獲得專屬的 URL 篩選功能。雖然在 Acronis Cyber Protect 中我們擁有與公開健康主題有關的特殊類別，端點防護解決方案中也提供了這個功能，它會以更高的優先順序進行更新。請記住，惡意連結通常來自：您的即時訊息、電子郵件、論壇貼文等。請勿按下您不需要或您不希望收到的連結。

與上面提到的惡意連結一樣，網路釣魚或惡意主題的附件可透過電子郵件傳送。關於附件：始終檢查它的真實出處，並問您自己是否希望收到它。無論如何，在開啓附件之前，須由您的防惡意軟體解決方案進行察看。

處理業務資料時使用 VPN

無論您是連接至遠端公司來源和服務，還是您的工作不需要這些活動，您僅僅是瀏覽部分網路資源和使用電信工具，請始終使用虛擬私人網路 (VPN)。如果您的公司有一個 VPN 程序，您將很可能獲得來自管理員或 MSP 技術人員的指導。如果您必須親自保護自己的工作場所，請使用推薦的知名 VPN 應用程式和服務，這些應用程式和服務是軟體市場廣泛提供的，或直接從廠商處購買。VPN 會將您所有的流量加密，使其安全以防駭客試圖擷取您正在傳輸的資料。

Copyright © 2002-2021 Acronis International GmbH.

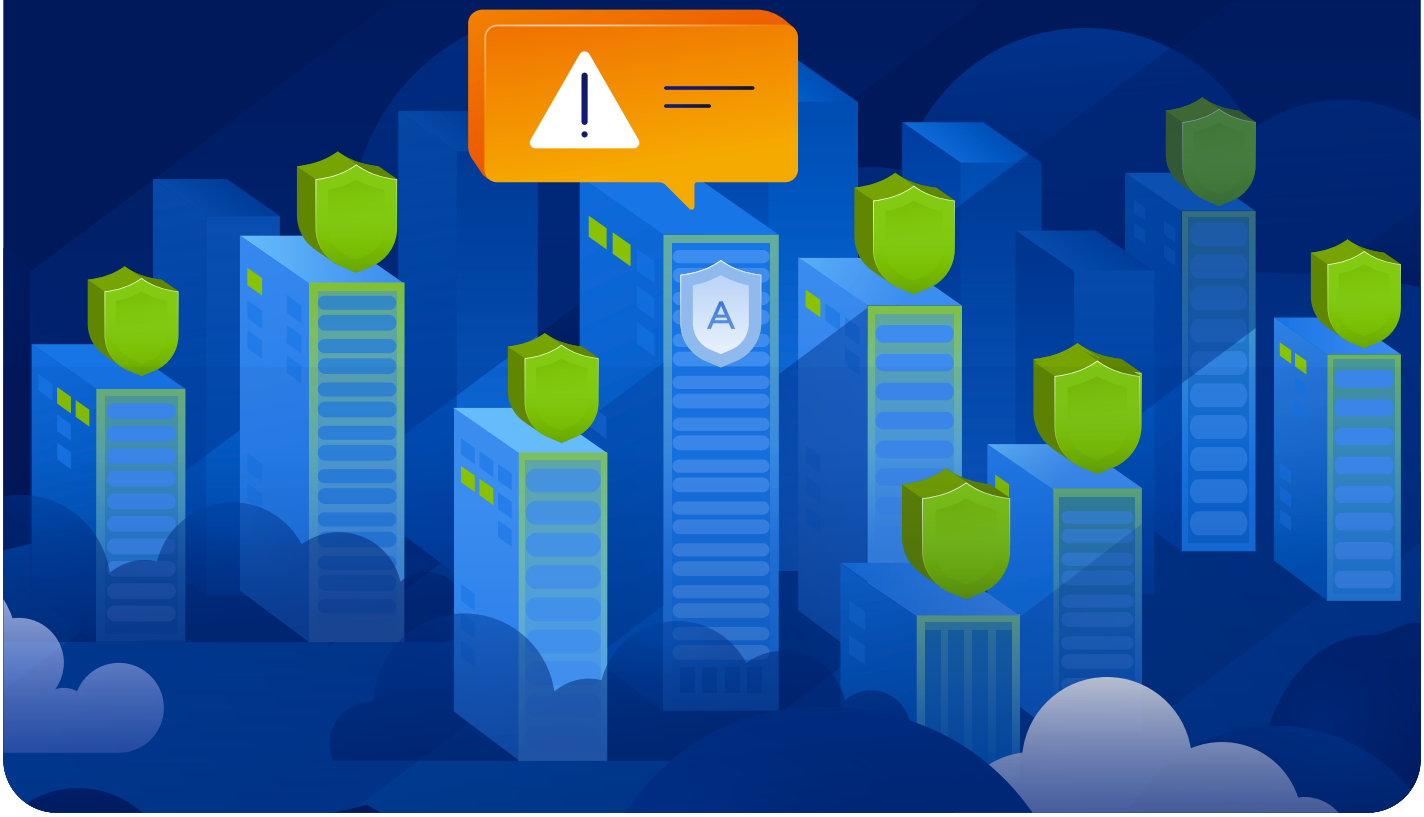
確保您的網路安全性正常地執行

在 **Acronis Cyber Protect** 中，我們使用很多平衡良好且精確調整的安全性技術，包括若干偵測引擎。我們建議用它取代嵌入式 Windows 解決方案。

但僅擁有一種防惡意軟體防禦能力是不夠；它應正確地設定。這意味著：

- 每天應至少執行一次全面的掃描。
- 產品需要每日或每小時獲得更新，視它們可用的頻率而定。
- 產品應連接到其雲端偵測機制，如果是 Acronis Cyber Protect，則連接至 Acronis Cloud Brain。它依預設是開啓的，但您需要確定網際網路可用且不會意外被防惡意軟體阻止。
- 隨需和即時監視 (即時) 掃描應啟用，並對每個已安裝或已執行的新軟體進行應變。

此外，不要忽略來自防惡意軟體解決方案中的訊息。如果您正在使用安全廠商提供的付費版本，請仔細地閱讀這些訊息，確保授權是合法的。



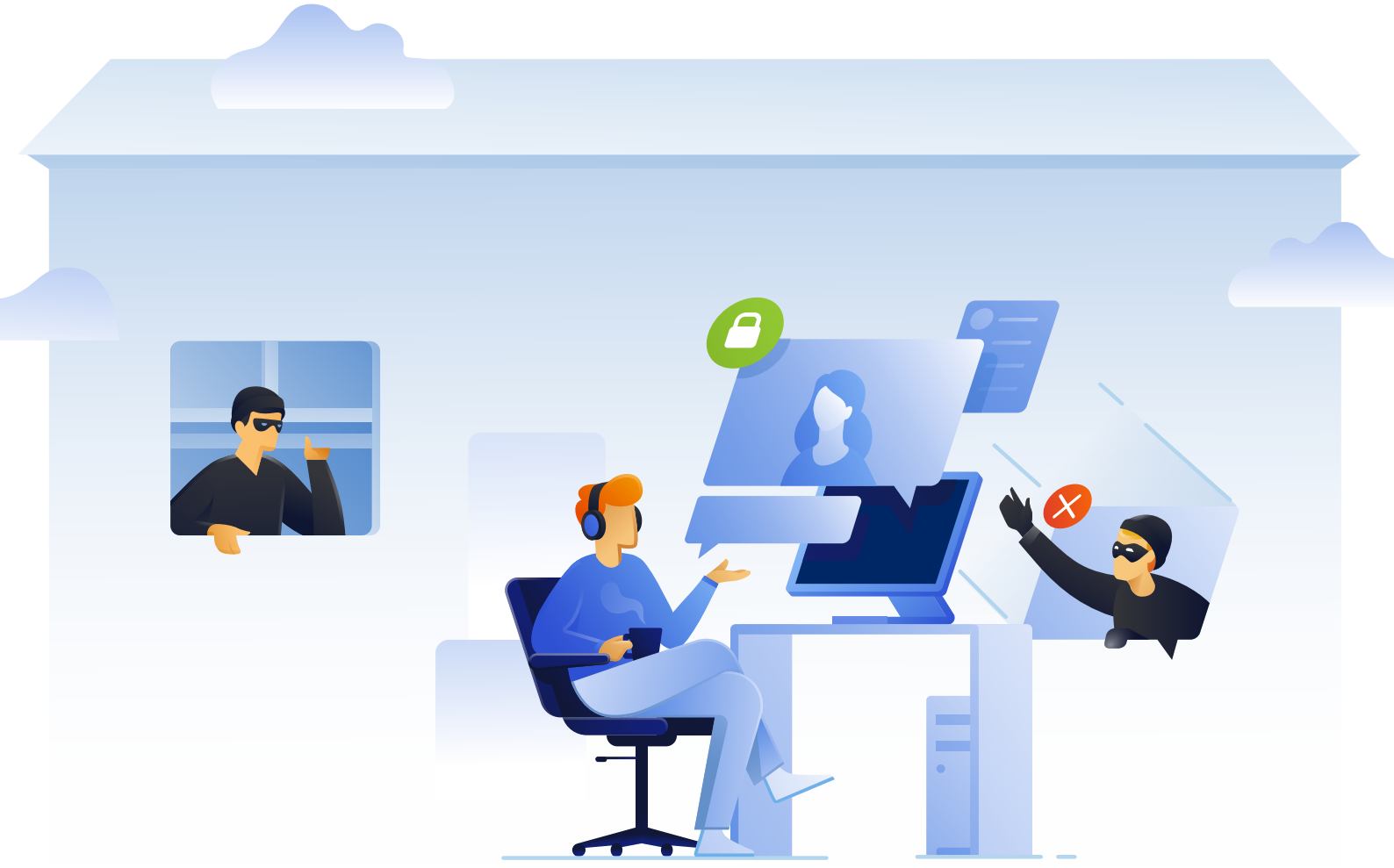
Copyright © 2002-2021 Acronis International GmbH.

只讓您自己知道密碼保持工作隱私權

安全性秘訣 1：確定您的密碼和您員工的密碼為強式且私密。永遠不要與任何人分享密碼，並針對您所使用的每個服務使用不同的長密碼。爲了幫助您記住它們，請使用密碼管理軟體。或者，建立強式密碼最簡單的方法是建立一組您可以記住的長片語。現在，8 個字元的密碼可輕鬆地暴力破解。

在 Acronis Cyber Cloud 或 Acronis Cyber Backup 之類的安全產品中，我們從不將密碼儲存在任何位置，因爲一旦忘記，將會終止對您資料的存取。

此外，即使在家工作，也要記得將您的筆記型電腦或桌上型電腦鎖定並限制它的存取。在很多情況下，人們可輕易地從未上鎖的電腦中竊取機密資訊，即使隔著很遠也不例外。



Copyright © 2002-2021 Acronis International GmbH.

Acronis 簡介

Acronis 結合資料保護與網路安全，提供整合式的自動化網路防護，解決現代數位世界在安全、易用性、隱私權、真實性與安全性（SAPAS）幾方面的挑戰。Acronis 的靈活部署模型符合服務供應商與 IT 專業人員的需求，藉由創新的新世代防毒、備份、災難復原以及 AI 提供的端點防護管理解決方案，為資料、應用程式和系統提供優越的網路防護。依靠進階防惡意軟體（由先進的機器智慧和區塊鏈資料驗證技術提供支援的），Acronis 可在任何環境（包括雲端、混合和內部部署）提供防護，且價格實惠。

Acronis 於 2003 年在新加坡創立，並於 2008 年在瑞士註冊成立有限公司，目前於 19 個國家/地區設有 34 個據點，擁有超過 1,700 名員工。Acronis 的解決方案廣獲超過 550 萬名居家使用者及 500,000 家公司，以及頂級的職業運動隊伍信賴。Acronis 的服務範圍遍及全球超過 150 個國家/地區，共有 50,000 多個合作夥伴及服務供應商提供 Acronis 的產品，服務語言超過 25 種。如需詳細資訊，請造訪 www.acronis.com