Acronis

Report
2020

安克諾斯Acronis網路威脅報告2020

2021年勒索之年的網路安全趨勢

Acronis 安克諾斯
網路威脅報告2020

目錄

介紹和摘要 3

Part 1. 2020主要網路威脅和趨勢 4

1.以COVID-19為主的攻擊 5

2.受到攻擊的遠端工作者 7

3.網路犯罪聚焦在管理服務提供者 9

4.Ransomware仍是最主要的威脅 10

5.簡易的備份和安全措施不再足夠 12

Part 2. 一般的惡意程式威脅 14

勒索軟體威脅 18

Part 3. 在Windows作業系統和其軟體的弱點 23

第三方應用程式容易受到攻擊，並且也易被不肖人士使用 25

全球最常被利用的應用程式 25

Part 4. 2021所需的關注 26

安克諾斯Acronis建議在當前和將來的威脅環境中保持安全 28

作者

Alexander Ivanyuk

Senior Director, Product and Technology Positioning, Acronis

Candid Wuest

Vice President of Cyber Protection Research, Acronis

介紹和摘要

安克諾斯Acronis是第一家實施完整的集成網路保護以保護所有資料、應用程式和系統的公司。網路保護要求威脅的研究和監控，並遵守網路保護的五個方向 - 安全性，可存取性，隱私性，真實性和可靠性（SAPAS）。 作為該策略的一部分，我們在全球範圍內建立了三個網路保護營運中心（CPOC），以監控和研究全年無休的網路威脅。

我們還升級了當前的旗艦產品：安克諾斯Acronis Cyber Protect Cloud（安克諾斯Acronis Cyber Cloud平台的一部分，用於服務供應商）和安克諾斯Acronis Cyber Protect 15（本地解決方案）。在發布這些版本之前，隨著勒索軟體技術不斷的發展，安克諾斯Acronis憑藉其創新的安克諾斯Acronis Active Protection 技術，證明了安克諾斯Acronis在阻止針對資訊的威脅方面的獨特專業知識。而且，更重要的是，安克諾斯Acronis在2016年開發的基於AI和行為的檢測技術已得到擴展，可以應對各種形式的惡意軟體和其他潛在威脅。

此報告涵蓋了根據我們在2020年遇到的情況而產生的威脅形勢。

該報告中提供的一般惡意軟體資料是在2020年5月安克諾斯Acronis Cyber Protect啟動後，於2020年6月至10月收集的，反應了我們在過去幾個月中檢測到的針對終端的威脅。

該報告代表了全球前景，其依據是分佈在世界各地的100,000多個獨立的端點。此報告僅反應Windows作業系統的威脅，因為它們比針對macOS的威脅要普遍得多。我們將繼續觀察局勢的發展，並可能在明年的報告中納入有關macOS威脅的資料。

2020年的前五項數據：

- 全球約有31%的公司行號每天至少被網路犯罪組織攻擊一次。
- 已知的ransomware案件約有50%是Maze ransomware。
- 在ransomware攻擊後，超過1000家的公司行號的資料被洩露。
- 微軟在短短9個月內修補了近1000個產品漏洞。
- 惡意軟體的平均生命週期為3.4天。

2021年的網路安全的主要趨勢:

- 對遠端工作者的攻擊只會增加。
- 資料洩露的比例將會遠大於資料加密。
- 會有更多在管理服務供應商、小型企業和雲端平台遭受網路攻擊。
- Ransomware將被視為新趨勢。
- 網路安全事件將會驅向於更自動化，惡意軟體案例的數量也將更多。

您可以在這份報告看到

- 在2020年觀察到的網路安全/威脅趨勢。
- 常規惡意軟體及其主要家族的統計數據檢視。
- 對Ransomware統計資料最危險的威脅深入分析。
- 為何機密資料洩露是Ransomware成功攻擊的第二階段。
- 哪些弱點是惡意程式攻擊成功的要素。
- 為什麼MSP受到越來越多的威脅。
- 2021年的網路安全/威脅預測和建議。

Part 1

2020主要的網路威脅和趨勢

1. 以COVID-19為主的攻擊
2. 受到攻擊的遠端工作者
3. 網路犯罪聚焦在管理服務供應商
4. 勒索軟體仍是最主要的威脅
5. 簡易的備份和安全措施不再足夠

從2019年底開始的COVID-19大流行對我們全球的生活產生了巨大影響。 但是這種流行病除了對人類健康帶來明顯的危險和巨大的經濟影響之外，還改變了數位世界、工作方式以及我們的網路生活。

隨著旅行的停止，大多數企業和服務不得不轉向線上營運。已經在線上的人必須增加，而其他人必須引入全新的過程。 政府、醫療和服務組織必須採用新的方式來滿足日常需求。

商務會議移轉到遠端視訊會議軟體上使用，像是Zoom、Webex和Microsoft Teams，這些趨勢成為了商務會議的新準則。辦公室工作人員常常匆忙地在沒有適當支持的情況下被送回家中，而後依靠自己的設備執行工作。

這種情況成為了網路犯罪者的機會，並對那些遠端工作者加強了攻擊。

1. 以COVID-19為主的攻擊

正如預期的那樣，人們急忙上網獲取有關新流行病的信息：如何保護自己，最新消息是什麼，可以依靠的援助等等。這種興趣導致大量騙局和其他形式的利用。

網路罪犯持續使用傳統網路攻擊中的技倆，利用COVID-19做為主題，誘騙受害者在網路釣魚網頁上輸入其憑證或個人資訊，或將惡意有效封包加載到偽裝包含與流行病資訊有關的的檔案中。還有其他值得注意的方法，下面的示例是我們遇到的一些以COVID-19為主題的釣魚手法

假的免費測試

最新版本的Trickbot / Qakbot / Qbot惡意軟體散佈在大量提供免費COVID-19測試的網路釣魚電子郵件中。要求受害者填寫附件表格，結果證明該表格是嵌入了惡意腳本的假檔案。為避免在惡意軟體沙箱中顯示其有效封包，該腳本要等一段時間後才能開始下載其有效封包。

誘餌檔案使用標準的後門程式誘騙使用者點擊“啟用內容”，從而允許執行嵌入的惡意VBA腳本。

假的財務支援

在許多情況下，網路攻擊根據該國受COVID-19影響的情況來制訂。 例如，德國的北萊茵-威斯特法倫州（NRW）成為網路釣魚活動的受害者。攻擊者在北威州經濟事務部網站上創建了流氓副本，以請求獲得COVID-19財政援助。

詐欺者收集了受害者提交的個人資料，然後使用受害者的資訊改成犯罪分子的銀行帳戶向合法網站提交了自己的請求。NRW官員報告說，已經批准了多達4,000個假請求，導致向詐騙者發送了高達1.09億美元的款項。

遠端教育的詐騙

罪犯也把重點放在遠端教育的利用。以流行病為主題的網路釣魚電子郵件發送了Formbook Trojan，該木馬嵌入學校教師的假評分應用程式中。Formbook是一種Infostealer惡意軟體，能夠從網路瀏覽器中竊取登入憑證。自2016年2月以來，它已在駭客論壇上受到了許多推廣。

有趣的是，攻擊者採用了多種反分析和反檢測技術，例如沙箱檢測和虛擬機檢測，隱寫術和XOR加密來隱藏有效封包，從而有效地逃避了Windows Defender。
眾所周知，Formbook的罪犯會攻擊生物醫學公司，以竊取財務資源、敏感的個人資料和智慧財產權。

假的病歷文件

Trickbot也利用了COVID-19流行病的恐懼來傳播了一個惡意文件，標題為：“第22.04.doc號法案的家庭和醫療假”（SHA256：875d0b66ab7252cf8fe6ab23e31926b43c1af6dfad6d196f311e64ed65e7c0ce）。真實的《家庭醫療假法》（FMLA）賦予僱員享有醫療福利的權利。但是，一旦使用者啟用了這些假的文件檔巨集，惡意指令便開始將其他惡意軟體下載到電腦上。

新型態的勒索

我們遇到了一個新型態的勒索詐騙。網絡犯罪分子仍然使用先前洩露的密碼作為令人信服的要素，但他們是威脅使用者的生命，而不是威脅要發布錄製的影片。網絡犯罪分子聲稱知道受害者的確切位置和日常工作。他們甚至可能用“冠狀病毒感染整個家庭”。為了要阻止他們這樣做，他們要求支付相當於4,000美元的比特幣。
詐騙份子已經不是第一次用這種方式威脅使用者的生命了。過去我們曾看到一些例子，他們威脅要派流氓毆打人們，但現在COVID-19將其威脅提升到一個新的水平。

這些電子郵件大多數是從隨機假的電子郵件地址或真實的電子郵件帳戶發送的。 當然，該訊息可明確看出是假的信件，您可以將其刪除。

追捕政府和私人公司的COVID-19秘密

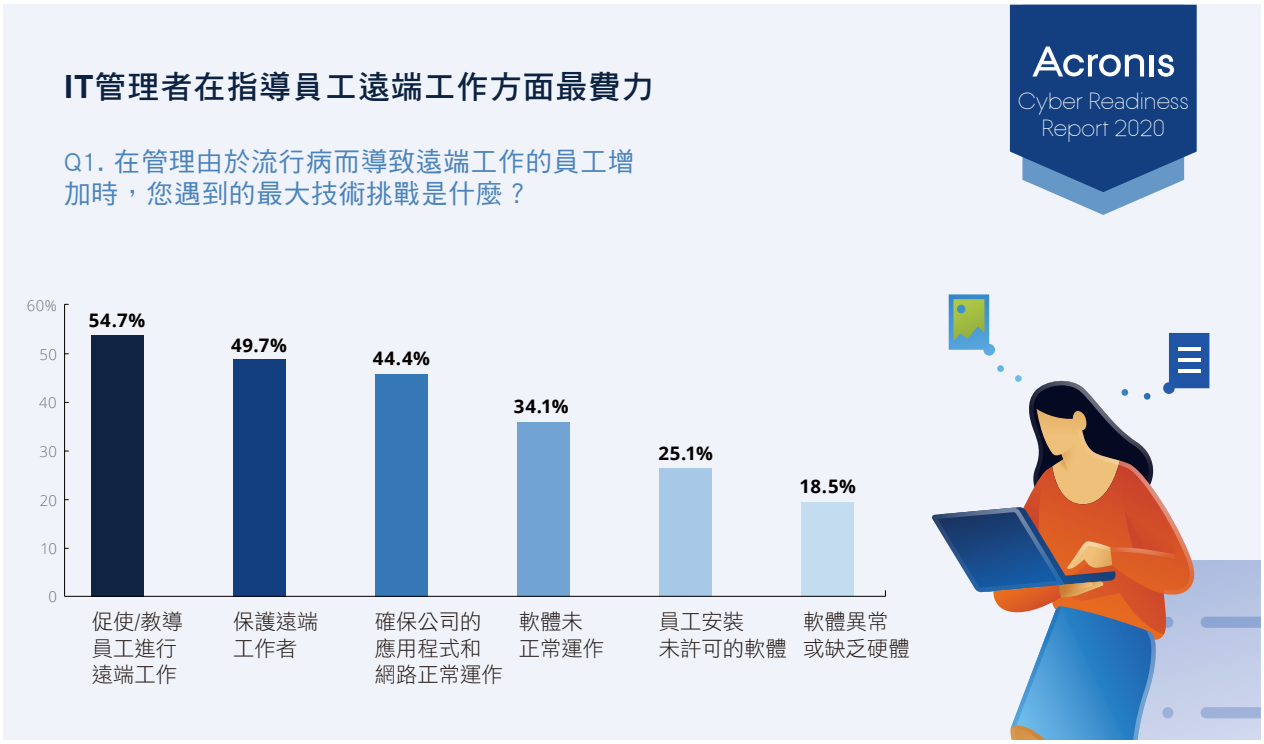
一些分析家認為某些與COVID-19流行病有關且有價值的資料被中國政府所隱瞞，此舉措引起世界各地駭客的注意。例如，據報導，越南政府贊助的駭客組織APT32（稱為OceanLotus Group）攻擊中國國家機構希望竊取病毒控制措施、醫學研究和統計數據，以揭示中國據稱尚未披露的感染數量。據稱，中國匯影醫療公司已開發出可基於AI電腦斷層掃描（CT）掃描圖像診斷COVID-19的96%準確性。根據網路安全公司Cyble的說法，被稱為“ THE0TIME”的駭客在暗網上以四比特幣的要價（當時約為30,000美元）出售了匯影醫療的資料，其中可能包含用戶資訊、原始碼和實驗報告。其他ATP團體則攻擊了製藥公司和疫苗接種實驗室，以竊取相關數據。

2. 受到攻擊的遠端工作者

COVID-19流行病已極大地改變了威脅格局，突出了與遠端工作操作相關的眾多安全和隱私風險，包括對內部公司伺服器的遠端訪問，虛擬會議以及員工之間的安全培訓。

為了評估IT團隊如何面對這種以最佳能力轉換到遠端環境-我們開發了首份安克諾斯Acronis網路就緒報告。在這份報告中，我們對2020年6月和2020年7月來自世界各地的3400家公司和遠端工作者進行了調查，以了解遠端工作所面臨的威脅、挑戰和趨勢。結果令人震驚：

- 近有一半的IT管理者都在努力指導和支援遠端工作者。
- 全球有31%的公司每天至少被網路攻擊一次。最常見的攻擊形式是釣魚附件、DDoS攻擊和視訊會議攻擊。
- 92%的全球組織必須採用新技術才能完成對遠端工作的轉換。結果，全球72%的組織在流行病期間發現IT成本的增加。
- 儘管技術費用支出的增加，成功的攻擊仍然很頻繁，原因在於組織沒有適當優先考慮防禦功能。
- 39%的公司在流行病期間遭受到視訊會議攻擊。



新冠肺炎增加Zoom的攻擊

COVID-19流行病的爆發使Zoom虛擬會議平台吸引了網絡犯罪分子的關注。隨著使用者的增加，越來越多的人開始分析Zoom程式碼中的弱點並引發隱私問題。

例如，Vice.com報告說，暗網市場上存在兩個零時差攻擊（供應商不知道的安全漏洞，因此沒有修補程序）：一個針對Windows，另一個針對macOS。 Zoom Windows RCE（遠端程式執行）漏洞的售價為500,000美元。

Zoom也成為被竊取服務憑證網路釣魚活動的目標。網路釣魚電子郵件已發送到50,000多個郵箱，針對Microsoft 365的用戶，他們以假的電子郵件邀請與人力資源部門進行即將到來的Zoom會議，以討論績效評估（該主題旨在引起受害者的焦慮，並讓受害者認為是封重要的電子郵件進而忽略了驗證信件的真實性）。

此類網路釣魚攻擊與憑證填充攻擊（攻擊者檢查用戶是否在多個服務上共享相同的密碼）相結合，導致在地下論壇上流傳了超過500,000個Zoom用戶憑證。
許多Zoom視訊會議都沒有設置密碼這一事實也吸引了網路犯罪分子。人們開始嘗試所有可能的會議ID號，直到找到正在進行的會議。然後，他們加入了通話，並通過播放影片，吵雜的音樂或其他不適當的素材打擾了參與者，這些爆炸式襲擊導致許多學校停止了遠端教學計劃。

Microsoft 365的使用者也遭受到攻擊

當然，Zoom不是攻擊者的唯一目標。Microsoft Teams和Webex也發生了類似的攻擊。例如一周之內，多達50,000個Microsoft 365用戶被包含偽造的Microsoft Teams通知的網路釣魚電子郵件攻擊，這些電子郵件將受害者導向到偽造的Microsoft 365登入頁面。

微軟的檔案共享服務（如Sway，SharePoint和OneNote）遭到了一些針對金融服務公司、律師事務所和房地產集團的小型網路釣魚活動攻擊。一項名為PerSwaysion的攻擊因濫用Sway服務而分三個步驟執行。它首先發送包含惡意PDF附件的網路釣魚電子郵件，該電子郵件看起來是含有“立即閱讀”超連結的Microsoft 365檔案共享通知。點擊該連結可在Microsoft檔案共享服務中打開另一個誘餌檔（特別是Sway），並帶有另一個“立即閱讀”連結，該連結將受害者帶到偽造的Microsoft登入頁面，從而竊取了其憑證。

在家工作的員工缺乏安全性

現在，有些人不得不在自己家中的電腦上工作，安全威脅的問題更加突顯。 這些家用電腦不僅常常缺乏有效的網路保護，而且許多使用者也沒有定期為其作業系統和常用的第三方軟體套用最新的安全更新，從而使他們的電腦容易受到攻擊。

許多這些私人公司的電腦不是被IT部門所管控，因此沒有公司政策適用於這些電腦。覆蓋這些漏洞和更新管理問題的急迫使管理員和技術人員感到頭疼，他們為緊急情況提供IT支持以幫助小型企業生存。
除此之外，家庭網路通常還受到其他不受保護的設備攻擊，這些設備通常來自孩子和家庭其他成員。此外，頻寬路由器通常已經過時，攻擊者可以劫持路由器並可能地重新導向特定流量。

3. 網路犯罪聚焦在管理服務提供者

由於許多中小型企業使用託管服務供應商（MSP）的服務，因此許多MSP成為網路攻擊的受害者。邏輯很簡單：犯罪分子無需破壞100個不同的公司，而只需入侵一個MSP即可訪問100個客戶。2020年的攻擊表明，MSP可以通過多種技術來破壞，其中配置不佳的遠端訪問軟體是最主要的攻擊媒介之一。網路罪犯利用缺乏多重因素驗證（2FA）漏洞，並用網路釣魚來訪問MSP管理工具來訪問其客戶的電腦。

例如，全球IT服務和解決方案提供商DXC Technology宣布有勒索軟體對其Xchanging子公司的系統進行攻擊。Xchanging主要為保險業的服務業提供服務，但其客戶列表包括來自其他領域的公司：金融服務、航空、國防、汽車、教育、消費包裝產品、醫療保健和製造業。

另一個例子是加拿大MSP Pivot技術解決方案公司，該公司披露了對其IT基礎架構的網路攻擊。勒索軟體攻擊後，Pivot Technology遭受了資料洩露，該事件可能已經影響了客戶的個人資訊。這種情況是2020年的典型情況，我們預計會有更多此類情況出現。

4. Ransomware仍是最主要的威脅

顯然，2020年是勒索軟體的一年，攻擊者越來越多，損失更大，網路犯罪分子正在執行新的勒索技術。大案件已成為家常便飯。Coalition是北美最大的網路保險服務提供商之一，根據Coalition發布的一份報告，勒索軟體案件佔2020年上半年提出的網路保險索賠的41%。“勒索軟體不受行業歧視，我們在每個行業中看到了勒索攻擊的增加。”Coalition報告。我們在安克諾斯Acronis可以證實這一事實。

請參閱本報告其他部分中來自網路保護營運中心的詳細統計資訊，此處我們概述了嚴峻的趨勢。

大目標帶來大的贖金

7月18日，阿根廷最大的電信營運商遭到了勒索軟體攻擊（很可能是Sodinokibi集團的攻擊），要求提供750萬美元的贖金。正如許多想要強迫受害者做出快速決定的攻擊者一樣，如果不在48小時內支付，則要求將增加一倍。據稱該勒索軟體感染了超過18,000個工作站，包括帶有高度敏感資料的端點。

全球最大的可穿戴設備公司之一Garmin證實，7月24日開始的主要停機是由於WastedLocker勒索軟體攻擊所致。這次襲擊迫使Garmin停止了聯絡中心營運，甚至是在台灣的生產線。

Garmin的年收入估計為40億美元，這無疑成為一個高價值目標。其所要求的贖金被認為高達1000萬美元。最近的其他WastedLocker攻擊要求的金額從50萬美元到數百萬美元不等。

高贖金受害者的名單仍持續增加。 FBI在2月發布了一些勒索軟體組織的利潤估算。該名單表明，Ryuk等組織在2019年的月收入約為300萬美元因此這些威脅只會持續增加。

更重要的是，現代勒索軟體不僅要求贖金解密資料，而且還向公眾披露被盜的機密資料，從而增加了他們獲得付款的機會。

要求不公開贖金

REvil / Sodinokibi勒索軟體組織於8月14日宣布，他們已經損害了位於肯塔基州的Brown-Forman總部的分公司， Jack Daniels、Old Forester、Glendronach以及其他各種葡萄酒和烈酒的分公司。2020年年度報告顯示，毛利潤超過20億美元，淨收入為8.72億美元，對於勒索軟體營運商來說，Brown-Forman無疑是高價值目標。

該REvil聲稱竊取了1TB資料，包括機密的員工資訊、財務資料、內部通信和公司協議。洩漏站點上發布的圖像表明，它們擁有的資料至少可以追溯到2009年。

專門從事光學和影像產品的跨國公司佳能（Canon）遭受了一次Maze勒索軟體攻擊，該攻擊影響了他們的電子郵件系統、Microsoft Teams、他們的美國網站以及其他內部應用程式。Maze勒索軟體營運商表示，他們從佳能那裡竊取了超過10TB的資料，包括私有資料庫，佳能則在發給員工的內部消息中確認了這次攻擊。

CWT是全球最大的旅遊和活動管理公司之一，遭到了Ragnar Locker勒索軟體的破壞。據稱攻擊者竊取了2TB的敏感公司資料，並聲稱已破壞了30,000多個系統。儘管攻擊者最初要求1000萬美元以安全返回被盜資料，但CWT進入談判並最終同意支付414比特幣的贖金，金額超過400萬美元。

Conti是一種新的勒索軟體（RaaS），是臭名昭著的Ryuk變種的後繼者，它發布了一個資料洩漏網站，作為其勒索策略的一部分，以迫使受害者支付贖金。儘管Conti活躍了幾個月，但直到最近，網路罪犯才公開發布了一個資料洩漏站點，他們威脅說，如果不支付所要求的贖金，他們就會發布受害者的被盜資料，目前，Conti.New列出了112名受害者，其中包括大型知名公司。

總共約20個不同的勒索軟體組創建了專門的頁面，用於託管在Tor地下網路上的資料洩漏。已有700多家公司發布了37%的資料洩漏來自Maze勒索軟體感染，其次是Conti（佔15%）和Sodinokibi（佔12%）。

這些資料洩露可能會導致聲譽損失，後續攻擊和各種罰款。此外，根據隱私法規（例如GDPR或CCPA），客戶資料的洩漏可能會受到懲罰，而根據美國OFAC法規，支付贖金可能是違法的。

5. 簡單的備份及安全性已不再足夠

自 2016 年以來，我們一直在預測勒索軟體將攻擊備份解決方案，之所以做出此預測，是因為諸如No More Ransom之類的組織（自2017年以來，安克諾斯Acronis一直是該組織引以為傲的成員），勸導人們和公司不要支付贖金，而是妥善保護裝置免受勒索軟體的侵害。如果您有備份，因為您可以從中恢復，則無需支付贖金。自 2017 年以來，幾乎每個勒索軟體都開始刪除或禁用 Windows 磁碟區陰影複製，並嘗試禁用傳統的備份解決方案。由於許多備份解決方案僅具有非常基本的自我保護功能甚至根本沒有。而由AMTSO member laboratory NioGuard進行的測試，很好地反映了這種嚴峻的形勢。

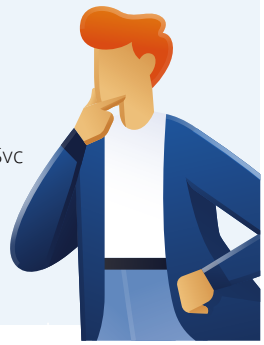
讓我們來看一些最近的勒索軟體示例。

CONTI 勒索軟體:

- 該勒索軟體的平均需求在$100,000美元以下
- 使用Windows Restart Manager在加密之前關閉任何打開或未儲存的檔案
- 包含 250 多個字串解密例行程式和大約 150 個要終止的服務
- 最多同時使用32個 CPU 執行緒及Windows I/O Completion Ports進行快速的檔案加密
- 順應趨勢，最近推出了“Conti.News”數據洩漏網站

此外，勒索軟體會刪除檔案的陰影複製副本，並將磁碟區的陰影複製儲存體由C：更改為H：，這也可能導致陰影複製副本消失。它還會停止屬於SQL、防毒軟體、網路安全和備份解決方案的服務，例如BackupExec和Veeam，它還嘗試終止安克諾斯Acronis Cyber Protect解決方案，但由於我們的自我保護功能而宣告失敗。
該列表包含約150個服務，包括:

Acronis VSS Provider	BackupExecRPCService	VeeamDeploySvc
Veeam Backup Catalog Data Service	BackupExecVSSProvider	VeeamEnterpriseManagerSvc
AcronisAgent	EPSecurityService	VeeamMountSvc
AcrSch2Svc	EPUpdateService	VeeamNFSSvc
Antivirus	mozyprobackup	VeeamRESTSvc
BackupExecAgentAccelerator	VeeamBackupSvc	VeeamTransportSvc
BackupExecAgentBrowser	VeeamBrokerSvc	VeeamHvIntegrationSvc
BackupExecDeviceMediaService	VeeamCatalogSvc	Zoolz 2 Service
BackupExecJobEngine	VeeamCloudSvc	AVP
BackupExecManagementService	VeeamDeploymentService	



NETWALKER 勒索軟體:

另一個例子是 Netwalker 勒索軟體，它於 2019 年 8 月在自然情況下發現的。它面對組織以及個別使用者實現了 RaaS Model。自2020年3月以來，他們成功勒索了約$2500萬美元。最新版本的 Netwalker 的顯著特徵是使用嚴重混淆的 PowerShell Loader在受侵害的系統上發動勒索軟體。使用 PowerShell 腳本，或者一般來說，在「離地攻擊」的策略下濫用任何預先安裝的工具，在網路罪犯中仍然很受歡迎。與其他許多的勒索軟體類似，Netwalker 會刪除檔案的 Windows陰影複製副本。

```
Get-Wmiobject Win32_Shadowcopy | ForEach-Object { $_.Delete();} | Out-Null
```

Netwalker 還嘗試停止以以下字串開始的備份服務 ， 以防止復原:

veeam*	ShadowProtectSvc	StorageCraft ImageManager
backup*	AcronisAgent	acrsch2svc*
backup	AcrSch2Svc	

Part 2

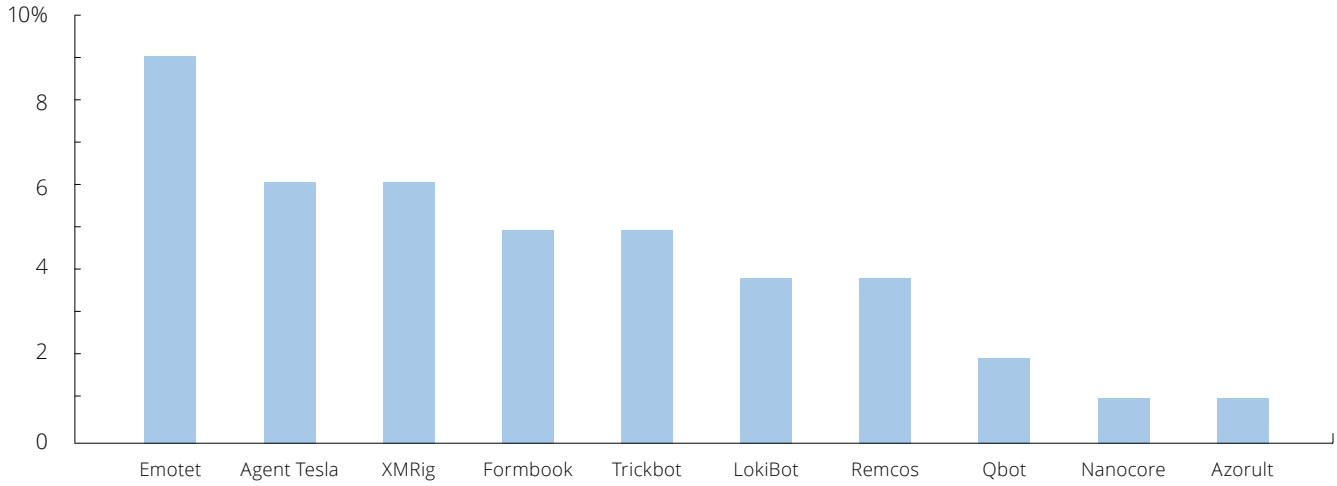
一般的惡意軟體威脅

在 2020 年第 3 季，平均有 11% 的客戶，成功阻止了至少一次的惡意軟體攻擊。自大規模的蔓延開始以來，這一數字略有下降，回到正常的水準。7月份仍為14.7%，8月份為10.1%，9月份為8.9%，10月份為6.7%。

2020 年第 3 季，客戶檢測出惡意軟體最多的國家是美國的27.9% 、德國的 16.7% 以及英國的 6.1%。

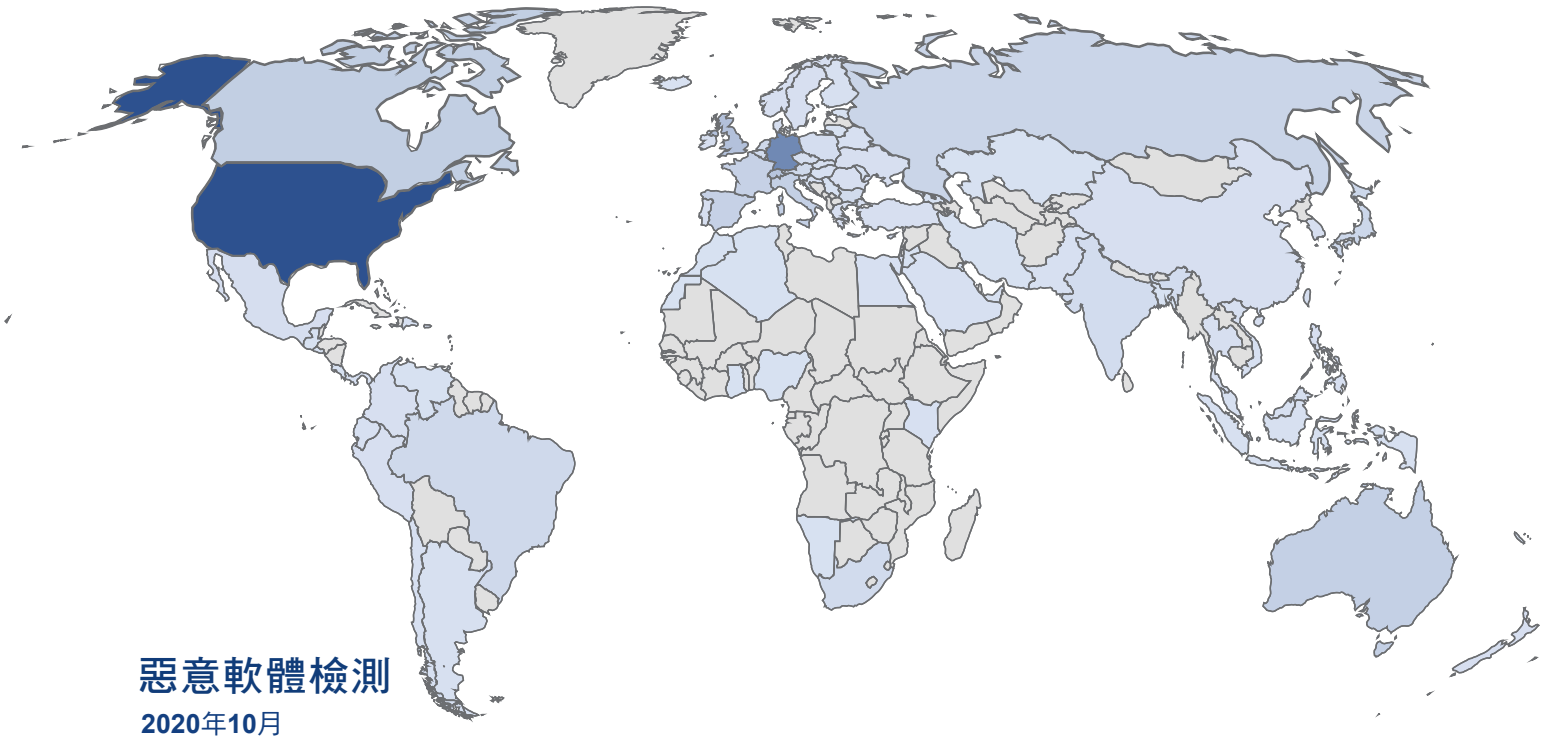
獨立的惡意軟體測試實驗室 AV-Test 在 2020 年第 3 季每天記錄 400,000 個新的惡意軟體樣本，這清楚的表示網路罪犯正在自動化其流程並產生大量新的惡意軟體威脅。但是這大多數的威脅僅在很短的時間內用於少數攻擊。在我們遇到的樣品中，19%只見過一次。惡意樣本的平均存留期為3.4天，然後就消失了且再也沒出現過。

以下是我們在 2020 年觀察和追蹤的十大惡意軟體家族:



全球檢測每個國家/地區每月的百分比

國家	2020年10月	2020年9月	2020年8月	2020年7月
美國	27.5%	27.9%	29.3%	16.4%
德國	18.4%	16.7%	16.8%	4.3%
瑞士	7.2%	5.4%	3.6%	3.2%
英國	5.9%	6.1%	6.4%	4.5%
加拿大	3.0%	3.6%	3.6%	1.5%
法國	3.0%	2.9%	3.3%	2.3%
義大利	3.0%	3.2%	3.3%	1.7%
澳大利亞	3.0%	3.3%	3.1%	2.0%
西班牙	2.6%	3.0%	2.8%	4.2%
日本	2.0%	2.3%	3.2%	15.7%



惡意軟體檢測

2020年10月

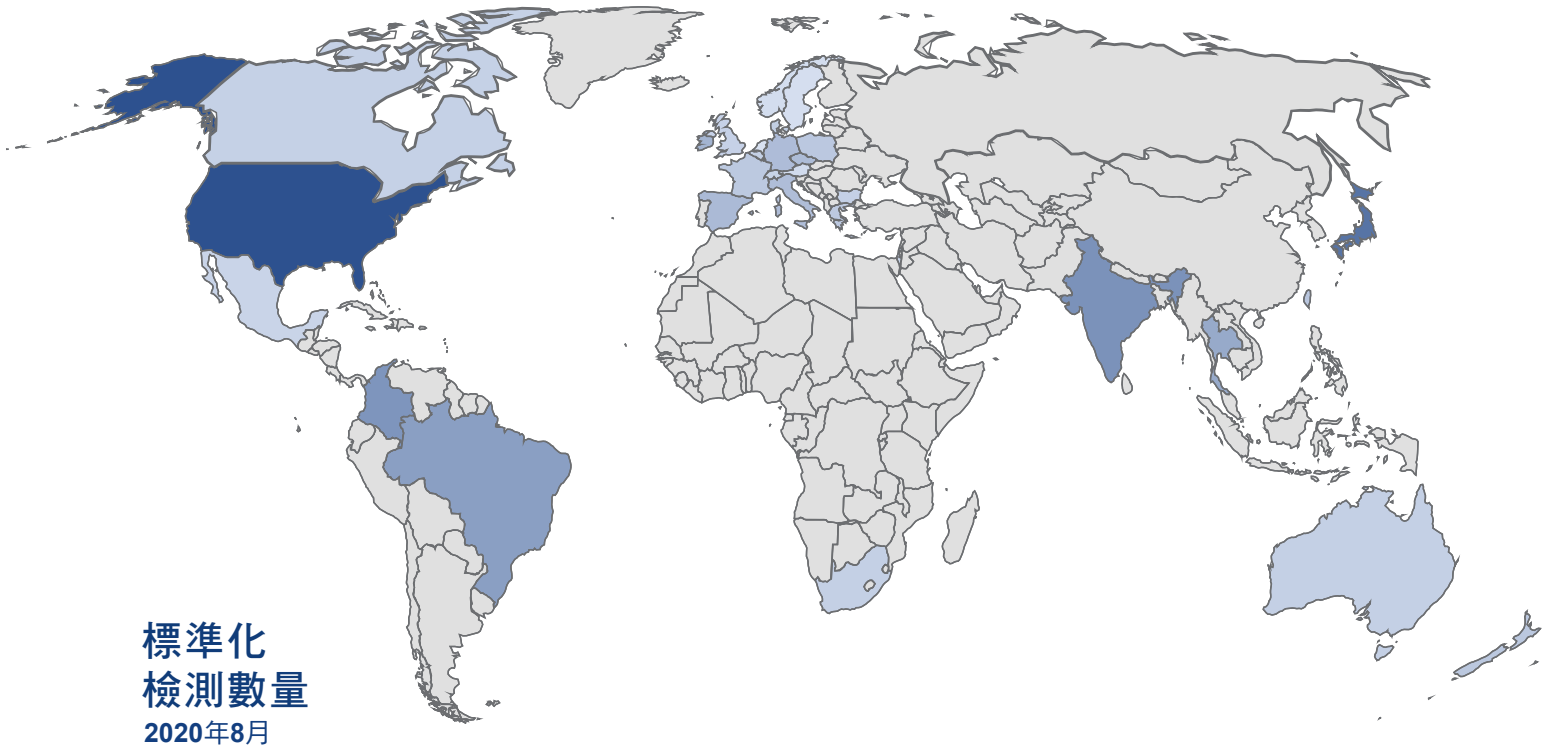
百分比

0% 0,27%

如果我們對每個國家/地區及每個活動客戶的檢測進行標準化，得到的分佈略有不同。下列表格標示了每個國家/地區，每1,000個用戶遇到的檢測數量。這清楚地顯示，網路威脅是一種全球化現象。

排名	國家	惡意軟體檢測 8月份每千名客戶
1	美國	2,059
2	日本	1,571
3	印度	1,168
4	哥倫比亞	1,123
5	巴西	994
6	泰國	856
7	愛爾蘭	729
8	西班牙	634
9	捷克共和國	611
10	德國	601
11	義大利	589

排名	國家	惡意軟體檢測 8月份每千名客戶
12	香港	518
13	台灣	480
14	新西蘭	462
15	波蘭	453
16	法國	444
17	希臘	437
18	丹麥	375
19	澳大利亞	361
20	比利時	358
21	南非	351
22	保加利亞	351
23	加拿大	347
24	英國	329
25	瑞士	311



標準化檢測數量
2020年8月

每 1,000個客戶端的檢測數量

131 2,059

勒索軟體威脅

正如我們在稍早章節已經提到的，勒索軟體仍然是企業的頭號網路威脅。雖然我們在2017年開發的安克諾斯Acronis Active Protection就觀察到了勒索軟體，但本節中我們介紹的重點是2020年1月1日至10月31日的數據。

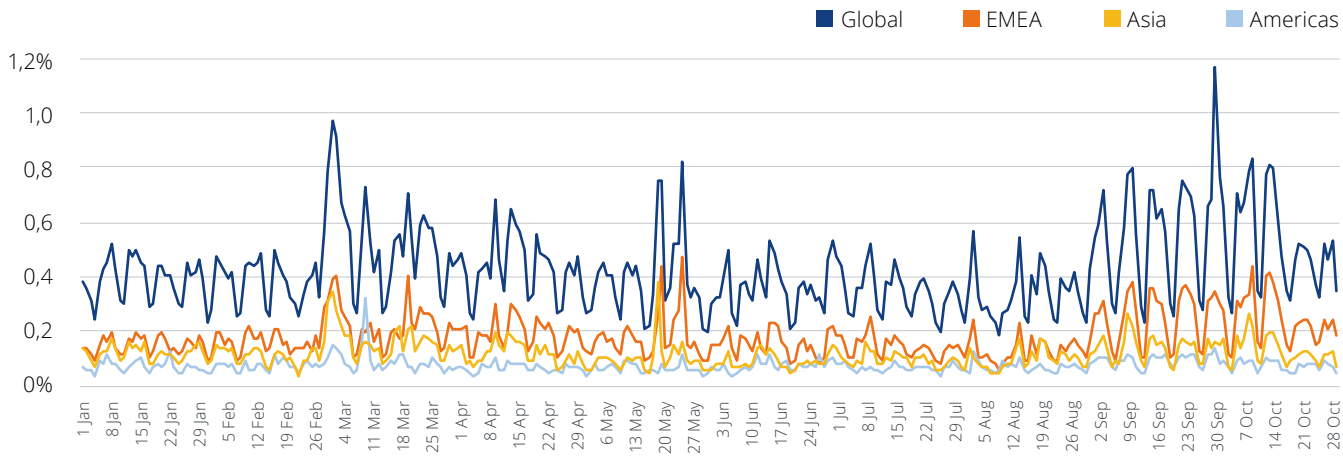
這些是我們在2020年觀察和追蹤的十大勒索家族。請注意，有些組織試圖用廣泛的方法盡可能的侵害更多的使用者，而另一些組織則專注於具有高價值的目標，他們嘗試以少量的侵害，取得更高的回報。因此，僅靠威脅檢測的數量並不能表示威脅的危險性高或低。

1. Maze
2. REvil/Sodinokibi
3. SNAKE (EKANS)
4. Nemty
5. NetWalker (aka Mailto)
6. Ragnar Locker
7. MegaCortex
8. CLOP
9. DoppelPaymer
10. Thanos

過去的九個月來，我們看到約有50個新的勒索軟體家族出現。有些關注的群體較小像是消費者這類，但如Avaddon,Mount Locker和Suncrypt這樣的新家族則關注高價值及利潤更高的公司。越來越多的這類組織活躍在勒索軟體服務的領域中，擔任再發佈者。這導致已知的勒索軟體威脅其蔓延及分佈率更快甚至更高。

勒索軟體的每日檢測

今年3月，我們在COVID-19開始時觀察到明顯的全球峰值。自那時起，勒索活動一直高於正常水準。關於受到攻擊的部門或區域，我們看到並沒有例外的——所有的部門都是攻擊的目標。在9月份，我們開始看到另一波勒索軟體的攻擊，尤其是針對北美的教育機構及製造公司。



前10個國家：勒索軟體的檢測(依地區)

亞洲：

國家	勒索軟體檢測區域 2020 年第 3 季的百分比
日本	17.7%
菲律賓	13.3%
台灣	9.6%
中國	8.6%
印度	7.8%
土耳其	5.4%
伊朗	5.3%
韓國	3.9%
印尼	3.7%
泰國	3.6%

歐洲、中東和非洲：

國家	勒索軟體檢測區域 2020 年第 3 季的百分比
德國	17.7%
法國	13.3%
義大利	9.6%
英國	8.6%
瑞士	7.8%
西班牙	5.4%
奧地利	5.3%
荷蘭	3.9%
比利時	3.7%
捷克共和國	3.6%

美洲：

國家	勒索軟體檢測區域 2020 年第 3 季的百分比
美國	67.3%
加拿大	15.9%
智利	4.7%
巴西	3.0%
墨西哥	2.7%
哥倫比亞	1.7%
祕魯	1.0%
阿根廷	0.8%
玻利維亞	0.4%
厄瓜多	0.3%

聚光燈下的勒索軟體組織

Evasive Maze勒索軟體在攻擊的目標中加密並竊取數 TB 的個人/私有資料

自 2019 年 5 月以來，Maze 勒索軟體在受攻擊的目標中一直出現，據知它應對Canon於 2020 年 7 月 30 日所受的最新攻擊負責，其導致image.canon雲端儲存服務的作業中斷。此外，Maze 勒索軟體組織聲稱其針對Canon的部分攻擊竊取了 10TB 的個人/私有資料。因為拒絕支付贖金，Maze組織已經公佈在2020年6月攻擊Xerox與LG時竊盜的數據資料。

- 不僅進行加密且會竊取資料，如果未支付贖金則將公佈資料
- 採用**anti-disassembly and anti-debugging**反偵測技術
- 預設為俄羅斯的區域不使用加密系統
- 混淆**wmic.exe**刪除陰影複製副本的調用
- 向位於俄羅斯莫斯科**'91.218.114.0'**網路中的**C&C**伺服器發送**HTTP check-in**需求
- 使用**Mimikatz**，**Procdump**和**Cobalt Strike**駭客工具進行擴散

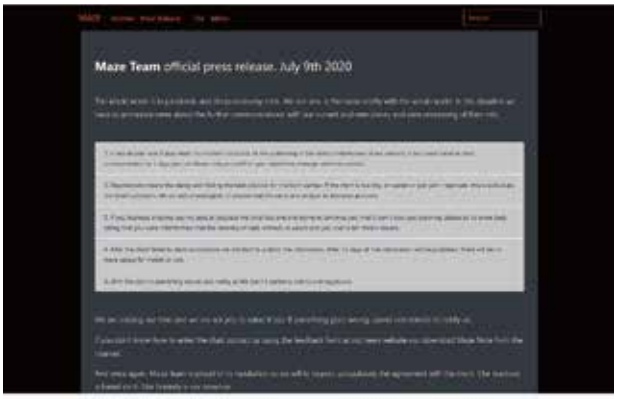
Maze的勒索軟體針對受攻擊的目標組織，通常是由spear-phishing email(釣魚郵件)開始、通過受侵害的 RDP 或 VDI（通常在Dark Web上購買憑證）以及利用 VPN 中的漏洞取得訪問的許可權限。

當Maze組織取得受侵害的組織內部網路的訪問許可權限，它將運行 Mimikatz 和 Procdump 來獲取儲存在記憶體中的密碼，並使用Cobalt Strike red-teaming工具切換到偵察。

Maze使用anti-disassembly (反偵測)技術來強化反組譯器中的編碼分析。
混淆技術包括:

1. 重新指向到同一位置的條件跳轉，替換絕對值
2. 呼叫後，將傳回位址送到堆疊中並跳至所呼叫的位址。

此外，Maze可以檢測其編碼是否正在呼叫。如果程序在除錯器下運行，它將檢查PEB 結構中的'BeingDebugged'。 如果編碼將進入無限迴圈不加密。此外，Maze通過程序的hash值，結束惡意軟體分析工具和office工具的程式。



Maze勒索軟體類似於最近的勒索軟體家族，如WastedLocker、Netwalker及REvil，因為它不僅加密，也竊取資料。它使用 7zip 工具及 WinSCP並向攻擊者的

FTP 伺服器傳送檔案。據報導，在一些案件中，洩漏出的資料也是 Base64 的編碼。總之，這使得Maze勒索軟體家族成為2020年所知最危險的家族之一。

DarkSide勒索軟體不會攻擊醫院、學校和政府

DarkSide是一個新的勒索軟體家族。攻擊開始於 2020 年 8 月初，據推測是由其他勒索軟體事件的前成員所發起的，這些勒索軟體活動在敲詐勒索活動中賺錢，並決定開發自己的編碼。根據已知事件，支付的贖金在$200,000美元至$2,000,000美元之間，就像其他受勒索軟體攻擊的目標一樣，DarkSide不僅對用戶的資料進行加密，而且還從受侵害的伺服器中洩漏出資料。

與成功攻擊Newhall學區和Fairfax County學校的Maze勒索軟體不同，DarkSide的行為準則禁止攻擊醫院，學校和政府組織。

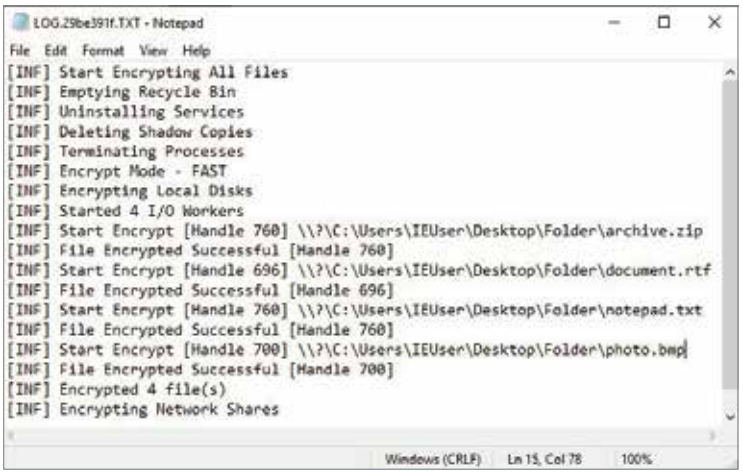
- **2020 年 8 月發現**
- **僅針對英語語系國家，避開前蘇聯國家**
- **不攻擊醫院、療養院、學校、大學、非營利組織、政府部門**
- **將 Salsa20 與自定義矩陣和 RSA-1024 加密演算法一起使用**
- **勒索的支付贖金從 $200,000到 $2,000,000**

勒索軟體會清空資源回收筒，而不需使用'SHEmptyRecycleBinA() function'其更隱秘。相反地，它會一個一個刪除扔到資源回收筒的檔案和資料夾。

Darkside 會移除以下與安全及備份解決方案相關的服務：

移除磁碟區陰影複製服務（VSS）後，勒索軟體通過啟動已混淆的 PowerShell 腳本刪除陰影複製副本。Darkside 還指定一個密鑰，該密鑰需要在第一個網站上輸入。不是每個使用者的密鑰都一樣，而是每個樣本一樣，因為該值在可執行檔中是經hardcoded處理且加密的。

結論是一樣的：很不幸的這是一個新準則，新的勒索軟體家族，即使不是太複雜的勒索軟體，預設情況下會攻擊備份。



惡意網站

在蔓延擴大期間，我們目睹了網路釣魚攻擊的增加，尤其是針對協作工具和檔案共享服務的攻擊，隨著員工在家工作，該工具和檔案共享服務越來越受歡迎。我們觀察到在三月份首次的高峰後，網路釣魚的攻擊已恢復正常。

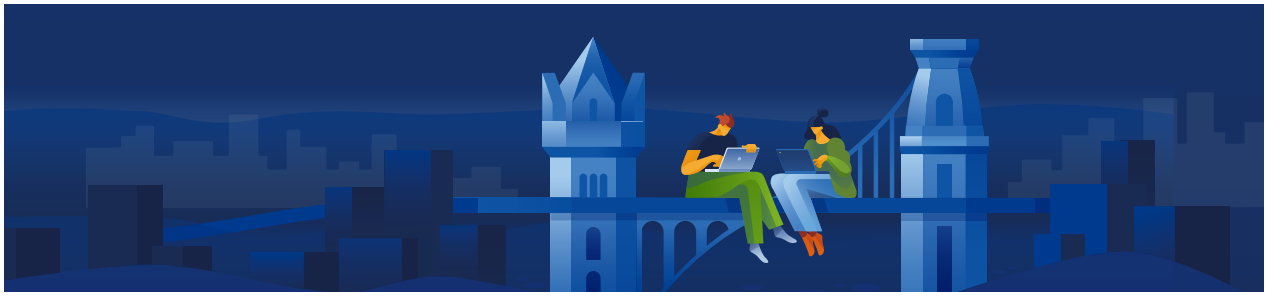
一些網路犯罪集團似乎已轉回由惡意附件的方式進行。 即使是臭名昭彰的Emotet組織，在缺席了五個月後，也於7月回歸，再次進行惡意的0ffice檔案發送動作。

月份	使用者百分比 惡意網站點擊
June	5.5%
July	5.1%
August	2.3%
September	2.7%
October	3.4%

在2020 年第 3 季，惡意網址被阻止的最大百分比是美國，為 16.4%。其次是德國，占 14.1%，捷克共和國佔10.4%。但是，有51%被阻止的網址是已加密的HTTPS，這使得在網路上進行過濾/篩選變得更加困難。我們還觀察到更多的網路釣魚仿冒2FA權杖，然後立即將其與腳本一起使用進行登錄。為了使這些網路釣魚頁面更難以檢測，通常將它們託管在受信任的雲端服務供應商（例如Azure或Google）上。某些攻擊者甚至增加CAPTCHA頁面，使用者須完成CAPTCHA的互動才可進入網路釣魚的頁面。該策略可以防止自動掃描解決方案的分析及阻止網路釣魚的網站。

第 3 季網址受阻最多的前 20 個國家

排名	國家	2020 年第 3 季 被阻止的網址百分比
1	美國	16.4%
2	德國	14.1%
3	捷克共和國	10.4%
4	西班牙	8.3%
5	英國	6.7%
6	中國	5.8%
7	南非	5.2%
8	香港	3.6%
9	義大利	3.4%
10	澳大利亞	2.4%
11	法國	2.1%
12	加拿大	2.0%
13	祕魯	1.9%
14	挪威	1.9%
15	荷蘭	1.8%
16	日本	1.6%
17	瑞士	1.6%
18	保加利亞	0.9%
19	新加坡	0.8%
20	奧地利	0.7%



Part 3

Windows作業系統和軟體中的漏洞

1 第三方應用程式容易受到攻擊，並且被惡意利用

2 全球最常用的應用程式

到2020年，已發現的漏洞和已發布的修補程式的數量劇增。RiskBased Security的VulnDB團隊匯總了2020年上半年披露的11,121個漏洞。

在9月份的最新Microsoft修補中，該公司報告了129個已關閉的安全漏洞，其中23個可利用透過惡意軟體來獲得對Windows電腦的完全控制，而對用戶幾乎沒有解決方式。這是微軟連續第七個月發布產品中100多個缺陷的修復程式，也是連續第四個月修復120多個缺陷。

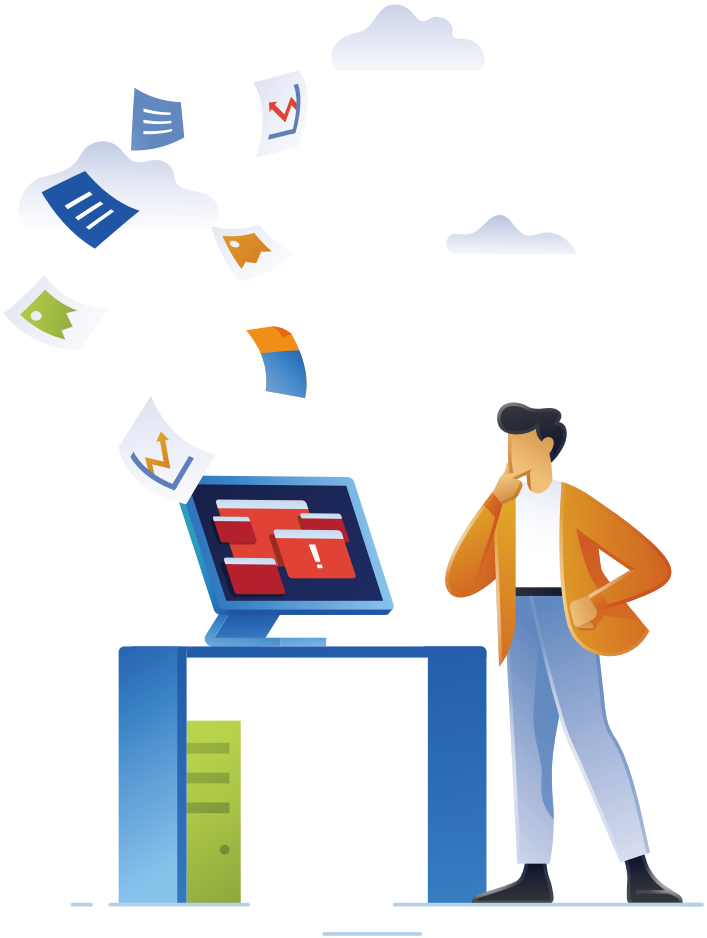
舊的問題還在：即使供應商迅速發布了修補，也不表示它每處都有修補。例如CVE-2020-0796，
如今它被人們稱為SMBGhost，它被認為具有危險，如果被武器化，它會獲得最罕見的常見漏洞評分系統（CVSS）等級：“完美”的10分。Microsoft在幾天之內發布了緊急更新修復程式。但是全球的網路安全公司包括安克諾斯Acronis，仍然可以看到該漏洞被惡意使用。

同樣，索引為CVE-2020-1425和CVE-2020-1457的漏洞（兩個遠端代碼執行（RCE）漏洞）的嚴重程度分別為“嚴重”和“重要”。 兩者都與Microsoft Windows編解碼器庫有關，後者處理記憶體中的對象。微軟表示，可以利用CVE-2020-1425的攻擊者“可以獲得訊息，從而進一步危害用戶的系統”。 同時，成功利用第二個漏洞可能使攻擊者能夠在目標電腦上執行任意代碼。在Microsoft的Exploitability Index中，每個漏洞都被評為“不太可能利用”。

正如我們在資料中看到的那樣，其中一些漏洞已被積極利用：CVE-2020-1020和CVE-2020-0938。正如我們所報導的。

3月23日，Microsoft確認了這些Windows漏洞，但沒有修復程序，攻擊者正在積極利用這些漏洞。當Microsoft發布修補程式時，未更新修補的Windows 10用戶面臨攻擊者能夠自行安裝程式，查看或更改資料以及建立新帳戶的風險。

Windows詐騙漏洞CVE-2020-1464也受到廣泛攻擊，Windows錯誤地驗證檔案簽章時，存在一個缺陷。
成功利用此漏洞的攻擊者可以使用附加到惡意可執行檔案的偽裝簽章來加載任何檔案，並誘使作業系統認為其合法。此漏洞影響所有受支援的Windows版本，如果尚未更新該修補，則會帶來嚴重問題。



第三方應用程式容易受到攻擊，並且也被惡意使用

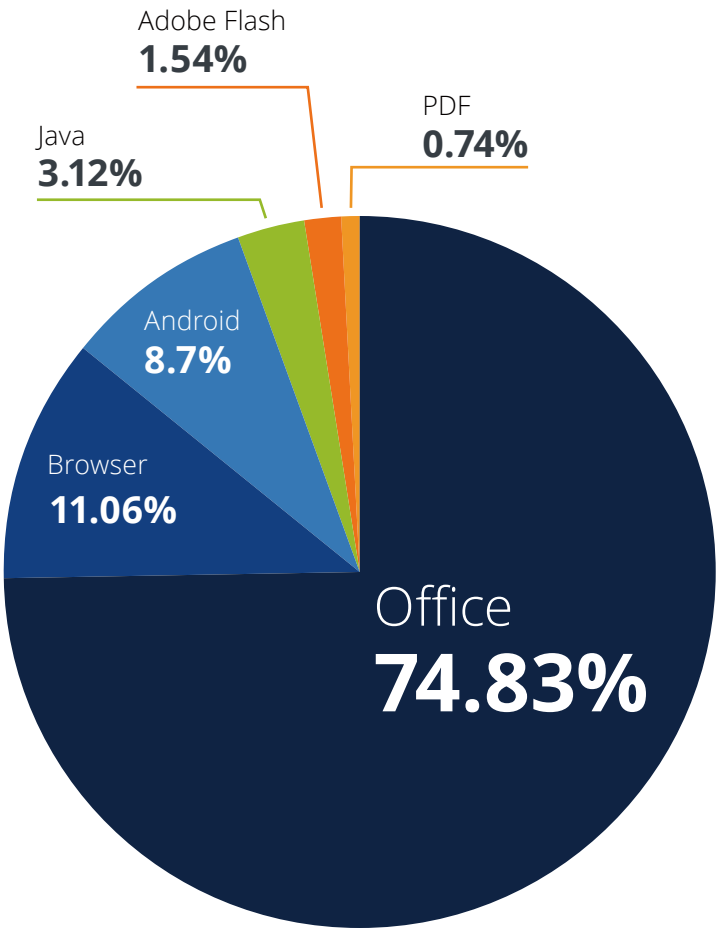
當然，微軟並不是唯一一家軟體中存在漏洞的公司， 在2020年我們還看到了以下漏洞遭惡意利用。

Adobe已在7月發布了針對其產品的定期安全修補，其中包括針對Photoshop，Prelude和Bridge的額外緊急安全更新。在發佈公司標準的每月安全更新一周後，Adobe發布了安全公告，揭露了總共13個漏洞，其中12個被視為嚴重漏洞。如果被利用，它們可能導致任意代碼執行。

8月，Adobe發布了修補程式來解決Adobe Acrobat和Adobe中的26個漏洞Reader，包括11個被評為嚴重的漏洞。可以利用關鍵漏洞繞過安全控制，其中9個關鍵漏洞允許遠端執行任意代碼。

Windows軟體不是唯一的漏洞類型。網路犯罪分子越來越多針對未修補的虛擬專用網（VPN）漏洞。Citrix VPN設備中的任意代碼執行漏洞（稱為CVE-2019-19781）已在野外攻擊中被檢測到。Pulse Secure VPN伺服器中的任意檔案讀取漏洞（稱為CVE-2019-11510）仍然是惡意行為者的誘人目標。

全球最常用的應用程式



Part 4

2021年關注的重點

安克諾斯Acronis建議在當前和未來的
威脅環境中保持安全

對遠端工作者的攻擊只會增加

隨著COVID-19感染人數迅速增加，很難想像大流行會在近期結束。疫苗可能甚至在2022年才能在全球施打，時間還很遙遠，欠缺保護的工作者仍停留在原地。2020年，網路罪犯意識到網路釣魚仍然非常有效，員工是企業資料的門戶，我們預測，將會有越來越多的網路罪犯努力獲取位於空蕩辦公室和資料中心的業務資料和系統，對遠端工作者的攻擊將會越來越多，而且越來越複雜。

資料滲透將大於資料加密

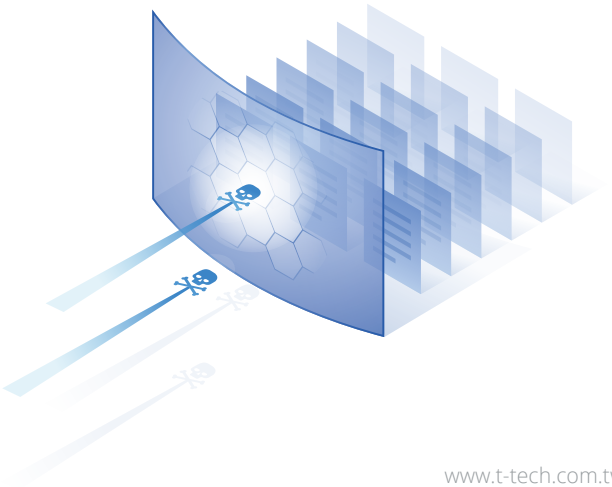
最近的勒索軟體案例顯示出，網路犯罪分子希望透過每次攻擊獲利。不僅如此，他們還發現，對於竊取的機密資料的勒索非常有效，甚至可能比僅對相同資料進行加密更好。這就是為什麼我們期望每種勒索軟體攻擊的主要目標都是資料洩露。資料保護以及防止資料丟失和洩漏的解決方案在未來將非常重要，因為即使我們發現新的勒索軟體系列的數量減少了，活躍的勒索軟體系列將造成巨大的損失，並且會非常成功。這意味著明年，我們判斷勒索軟體仍將是企業面臨的第一大威脅。

對服務供應商(MSP)和小型企業的攻擊更多

隨著越來越多的中小型企業使用服務供應商的雲端時，越來越多的網路犯罪分子將針對此發動攻擊。在2019-2020年，網路犯罪分子意識到攻擊MSP非常有效，尤其是可能沒有準備的較小MSP。透過攻擊MSP服務的數十家公司，並且可以透過勒索軟體感染或銀行木馬來獲得更多收益，此外，攻擊者可以利用完善的工具，例如遠端連線和軟體傳輸工具。由於小型企業和MSP都未做好應對嚴重攻擊的準備，儘能夠支付適度的贖金，因此這類攻擊的數量和受害者將大幅增加。

受到攻擊的雲

在封鎖期間，許多公司將其服務移至雲端。不幸的是，該配置通常匆忙完成，因此十分不安全，因為雲端應用程式和資料服務暴露給網路上的每個人。這種情況為攻擊者提供了訪問和暴露資料的機會，正如我們已經看到的S3資料儲存庫和彈性搜尋資料庫中的資料洩露事件一樣。此外ID和訪問管理正成為新的領域，但訪問管理仍然經常被忽略。這種情況將導致用戶實體行為監控和動態訪問控制的增加。



勒索軟體正在尋找新的目標

勒索軟體攻擊正在擴展到Windows和Mac電腦之外。攻擊者試圖在雲端環境中站穩腳步，因為雲端資料庫和儲存庫是他們有利可圖的目標。在組織內部，OT端日益暴露的工業控制系統（ICS）是勒索的另一個目標。對於家庭用戶而言，物聯網（IoT）的採用日益增加，尤其是與5G相關的物聯網，可能會產生新的感染問題--即使只是產生DDoS攻擊，也會讓受害者支付贖金。

攻擊者更高的自動化，惡意軟體樣本數量增加

網路犯罪分子正在嘗試盡可能地自動化攻擊過程，犯罪軟體入侵和自動化更加快傳播速度，大數據分析工具和機器學習使他們能夠找到新的受害者並生成個人化的垃圾郵件。

但是，在初始訪問和執行階段之後，大多數組織仍然使用手動方法在公司網路內部傳播惡意軟體。

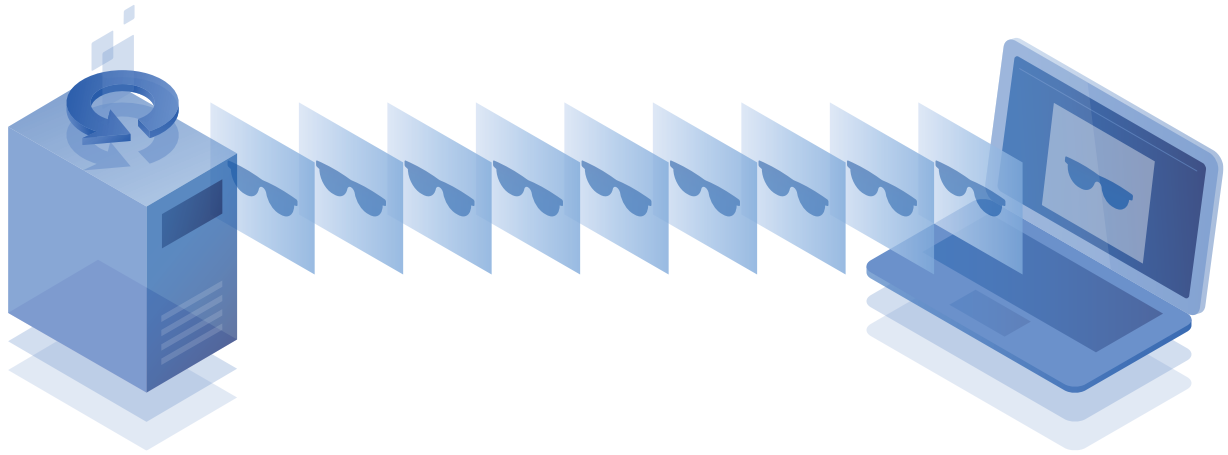
安克諾斯Acronis建議在當前和未來的威脅環境中保持安全

現代網路攻擊，資料洩漏和勒索軟體爆發都顯示了同一件事：網路安全正在失效。失效的原因是聰明的社會工程技術導致的技術薄弱和人為失誤。如果備份解決方案執行良好且不受損害，通常需要數小時和數天的時間才能將系統（包含資料）恢復到執行狀態。備份對於網路安全解決方案出現故障時至關重要，但是備份解決方案可能會受到影響、中斷、並且執行緩慢，這些將導致企業因停機而蒙受大量損失。為解決這些問題，我們建議使用整合的網路保護解決方案，例如安克諾斯Acronis Cyber Protect，該解決方案結合了反惡意軟體、漏洞評估、修補程式管理、RMM和備份功能整合在一系列Windows作業系統執行的單個代理中。通過此整合，您可以保持最佳性能，消除兼容性問題並確保快速恢復。

如果在更改資料時丟失或檢測到威脅，則代理將立即從備份中還原未更改的資料。反惡意軟體代理無法實現這種自動恢復。您的反惡意軟體解決方案可能會阻止威脅，但是某些資料可能已經丟失。備份代理將不會自動辨識，並且將資料緩慢還原（如果有的話）。

當然，安克諾斯Acronis Cyber Protect Cloud會透過在威脅破壞環境之前檢測並消除威脅，避免您要復原系統的這一步，這種防禦水準是透過增強的多層網路安全功能達到的。

也就是說，即使公司和家庭用戶使用這種防禦水準Acronis Cyber Protect 等現代解決方案，也不應忘記基本的安全守則。



修補您的作業系統與APPS

修補漏洞至關重要，因為許多漏洞都是由於未修補的漏洞而得逞的。借助具有內建的漏洞評估和修補管理功能的安克諾斯Acronis Cyber Protect 的解決方案，您將獲得保護。我們追蹤所有發現的漏洞和已發布的修補程式，並允許管理員或技術人員透過靈活的設定輕鬆修補所有端點和詳細的報告。

安克諾斯Acronis Cyber Protect不僅支援所有內建的Windows應用程式，而且還支援100多種流行的第三方應用程式，包括諸如Zoom和Slack之類的通訊工具，以及在遠端工作中使用的VPN工具等。 確保優先修補高嚴重性漏洞，然後按照成功報告檢查是否正確應用了修補程式。

如果您未使用安克諾斯 Acronis Cyber Protect 或未用任何修補程式管理軟體，您需要確保Windows獲得了它所需的所有更新，並且這些更新已及時安裝。

用戶往往忽略系統通知訊息，尤其是在Windows要求重新啟動時，這是一個很大的錯誤觀念。確保啟用了軟體供應商（如Adobe）的自動更新，並且及時更新了Acrobat Reader等應用程式。

為網路釣魚做準備，不要點擊可疑連結

現在，COVID-19被廣泛用於網路釣魚陷阱，但是這些惡意活動的數量只會增加，因此，每個遠端工作人員都需要為此做好準備。每天都有大量有關網路釣魚和惡意網站出現，這些通常會在瀏覽器保護功能被過濾掉，但使用安克諾斯Acronis Cyber Protect的網路保護解決方案，您還將獲得專用的URL過濾功能。端點保護解決方案提供了相同的功能，儘管安克諾斯Acronis Cyber Protect 具有與公共衛生主題相關的特殊類別的優先更新，但惡意連結可能來自任何地方，包括電子郵件、論壇文章、即時訊息和應用程式，千萬不要點擊不需要或收到的不明連結。

網路釣魚或惡意附件可以透過電子郵件發送與上述相同的惡意連結。關於附件：請每次檢查附件的真正來源，並詢問自己是否在等待這封信。無論如何，在打開附件之前，應先使用反惡意軟體解決方案對其進行掃描。

在處理公司資訊時使用VPN服務

無論您是連接到遠端公司的資源和服務，還是您的工作都不需要進行這些活動，而只是瀏覽一些網路資源並使用通訊工具，請使用虛擬私人網路（VPN）。VPN會加密您的所有流量，以確保安全，以防駭客試圖在傳輸過程中竊取您的資料。
如果您的公司中有VPN程式，則可從管理員或MSP技術人員那裡得到協助。 如果您必須自己保護工作場所的安全，請使用在軟體市場中或直接從供應商取得有信譽、推薦的知名VPN程式和服務。

確保您的網路安全解決方案運行正常

在安克諾斯Acronis Cyber Protect中，我們使用了許多平衡良好且經過微調的安全技術，其中包括建議使用多個檢測引擎，而不是嵌入式Windows解決方案。

但是僅使用反惡意軟體防禦是不夠的，應該對其進行正確設定。這意味著：

- 至少每天進行一次全面掃描
- 產品需要每天或每小時獲取更新，具體取決於更新的頻率
- 在安克諾斯Acronis Cyber Protect的情況下，產品應連接到其雲端檢測機制–在安克諾斯Acronis Cloud Brain上。默認情況下是打開的，但是您需要確保網路連線可用並且不會被反惡意軟體阻止
- 啟用按需和按存取(實時)掃描，並對所有已安裝或執行的新軟體做此動作

此外，請不要忽略來自反惡意軟體解決方案的郵件。請仔細閱讀，如果您使用的是安全廠商提供的付費版本，則請確保是合法的授權。

將密碼和工作空間留給自己

最後的安全提醒：確保您和員工的密碼都是安全的私人密碼，並切勿與任何人共享密碼，同時為您使用每項不同的服務使用較複雜的密碼。為了幫助您記住它們，請使用密碼管理器軟體。另外，因為現在8位數密碼已經很容易被破解了，建立高強度密碼的最簡單方法則是建立一組您可以記住的長字元。

安克諾斯Acronis Cyber Cloud或安克諾斯Acronis Cyber Backup的解決方案，我們永遠不會儲存密碼在任何地方以防止對您的資料進行任何不必要的訪問。

最後，在許多情況下，人們甚至可以從一台未鎖定的電腦上竊取敏感資訊，甚至可以從遠端竊取，所以即使在家中工作，也不要忘記鎖定筆電或桌電並限制對它的存取。

Acronis 安克諾斯

關於安克諾斯Acronis

安克諾斯Acronis結合了資料保護和網路安全功能，提供整合的自動化網路保護功能，以解決現代數位世界面臨的安全性、可存取性、隱私、真實性和可靠性（SAPAS）挑戰。 藉此可滿足服務供應商和IT專業人員需求的靈活部署模式，安克諾斯Acronis利用創新的新一代防毒、備份、災難復原和端點保護管理解決方案，為資料、應用程式和系統提供了卓越的網路保護。藉由屢獲殊榮的AI反惡意軟體和區塊鏈的資料身份驗證技術，安克諾斯Acronis 從雲端到混合環境再到本地的任何環境，提供彈性且低成本的保護。
安克諾斯Acronis於2003年在新加坡成立，並於2008年在瑞士成立，目前在18個國家的33個地區擁有1,500多名員工。我們的解決方案受到超過550萬家庭用戶和50萬間公司的信任，其中包括全球財富1000強的公司和專業運動團隊。安克諾斯Acronis產品可透過150多個國家/地區的50,000個合作夥伴和服務供應商以40多種語言提供。欲了解更多訊息，請前往www.t-tech.com.tw

湛揚科技 Acronis 總代理
www.t-tech.com.tw
台北：(02)2735-3512 技服電話：(02)7718-5588
高雄：(07)972-7388 技服信箱：support@t-tech.com.tw