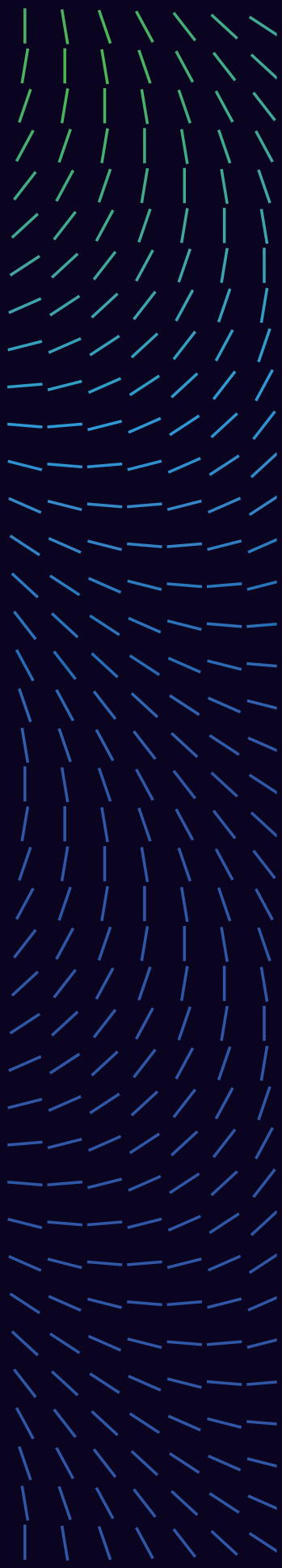
Trellix

TRELLIX 資安威脅研究室 研究報告 REPORT APRIL 2022

REPORT

目錄



2021年第四季，全世界已經歷了兩年的疫情肆虐，在此期間網路攻擊者也趁機作亂，Log4Shell就是惡名昭彰的亂源之一。

到了2022年第一季，資安威脅的焦點轉移到歐亞地區的衝突，尤其是針對烏克蘭基礎設施的網路威脅特別引人注目。

我們最新的Trellix資安威脅研究室研究報告中，包含了我們在 2021年第四季的調查結果，其中有我們對政府高官的多階段間諜攻擊的識別、第一季對烏克蘭的網路攻擊、以及新發現的HermeticWiper分析。

首席科學家致詞

歡迎閱讀我們最新的資安威脅報告。

新的一年已經過了一季，這段時間對所有人而言一點也不輕鬆。我們正在逐漸擺脫疫情的影響，但圍繞歐亞地區衝突的不確定性，正持續影響著我們的日常生活。

首先，Trellix站在和平這一方。無論任一方捲入衝突，我們的使命都是保護我們的客戶並遵守國際法條規範。在我們準備這份報告時，我們正持續進行研究和保持警惕。如Lapsus$ 組織攻擊了世界各地的大公司，最初的攻擊對象是在南美洲，原始碼和認證資料等敏感數據都被洩漏出來。

我們觀察到這些認證資料被濫用於簽署惡意軟體，以繞過作業系統和安全信任，進行惡意的行為。您可以在此讀取這個組織的詳細資訊，了解他們當前的違規作為，以及我們的對策。

在我們公司成立以來的第二份威脅報告中，您可以了解到目前主導全球頭條新聞的資安事件。從對烏克蘭基礎設施的攻擊，到能夠破壞啟動磁區的 HermeticWiper 惡意軟體，網路安全對許多人而言，在新的一年裡仍然是被高度關心的話題。

同時，我們回顧了2021年第四季Log4shell 漏洞，影響了數億台設備，許多設備現在正面臨全新威脅的到來。

多年來，身為分析和研究勒索軟體的先鋒，Trellix 研究室團隊與公部門合作，對於在2021 年12月關閉勒索軟體、並逮捕首腦的成就感到自豪。從Conti勒索軟體和Trickbot惡意軟體群組最近洩露的聊天記錄，顯示了這些團體運作的高超專業程度。這在在證明，我們需要公私部門的一致共識與行動，以阻止這些網路攻擊所造成的破壞。

此外，歡迎造訪我們的 Trellix 資安威脅研究室部落格，其中包含我們最新的資安威脅內容、影片和安全公告鏈接。

在這份報告中，我們還介紹了近來所觀察到的其他普遍威脅和攻擊。

— Christiaan Beek
首席科學家

Twitter @ChristiaanBeek

首席科學家致詞

TRELLIX 資安威脅研究室分析針對烏克蘭的網路攻擊，以及 HERMETICWIPER

Trellix Labs 研究團隊對在烏克蘭部署的活動分析，令我們相信 Whispergate 和新發現的 HermeticWiper 之間可能存在某種關聯。

以下繼續介紹我們對烏克蘭地區威脅活動的情報和分析。

避免初期入侵的建議步驟

組織需事先審查與俄羅斯民族國家活動相關的初期入侵策略、技術和程式 (TTP)，藉以主動保護作業環境，以免遭受滲透

- 利用惡意的URL短網址，進行釣魚式/魚叉式網路釣魚攻擊。
- 監控網路暴力攻擊，以識別有效的帳戶憑證和 Microsoft 365 帳戶。
- 為所有用戶啟用多重要素身份驗證（MFA）功能。
- 濫用大眾服務系統－CISA 可提供已被濫用的 CVE 的完整表單。
- 禁止使用所有不必要的連接埠和協議，與遠程服務相關的也在禁止之列。
- 尋找並阻擋在先前攻擊中出現的無關開源工具，如UltraVNC、AdvancedRun、wget 和 impacket。

針對烏克蘭進行資安威脅的主要活動和團體包括：

ACTINIUM APT	IsaacWiper
Agent Tesla	NOBELIUM APT
CaddyWiper	OutSteel
CERT-AU 4109	RURansom Wiper
DDoS Attacks	SaintBot
Gamaredon APT	Shuckworm APT
Gamaredon APT	UAC-0056

歡迎造訪我們的 Trellix 資安威脅中心，瀏覽近期所發現包括 HermeticWiper在內的威脅。

TRELLIX 資安研究室發現可疑的 DARKHOTEL APT 活動更新

3月時，我們的團隊發現了自 2021 年 11 月下半月以來，針對澳門多家豪華飯店的第一階段惡意活動。攻擊開始於一封寄給飯店管理階層的魚叉式網路釣魚電子郵件，這些收件者的職位包括人力資源副總裁、副理、和櫃台經理。根據這些職位，我們可以假設網路攻擊者擁有充足的飯店網路使用權限，如房務預定系統等。讓我們來看這種攻擊是如何進行的：

- 在魚叉式網路釣魚攻擊的電子郵件裡，包含了個一開啟就會將惡意巨集嵌入作業系統的 Excel 檔案附件。
- 惡意巨集所啟動的攻擊機制，在下方的資安攻擊流程圖中說明。
- 巨集一開始會在受害者電腦裡，建立一個工作排程來執行資料辨識、列表、和洩漏動作。
- 接下來，為了讓攻擊者的伺服器與受害者電腦之間建立連線，巨集使用 lolbas（Living Off the Land Binaries and Scripts）技術來執行 PowerShell 命令列，作為被信任的執行腳本。

歡迎造訪我們的部落格，以了解更多 DarkHotel APT 背景、歸因、活動和技術分析。

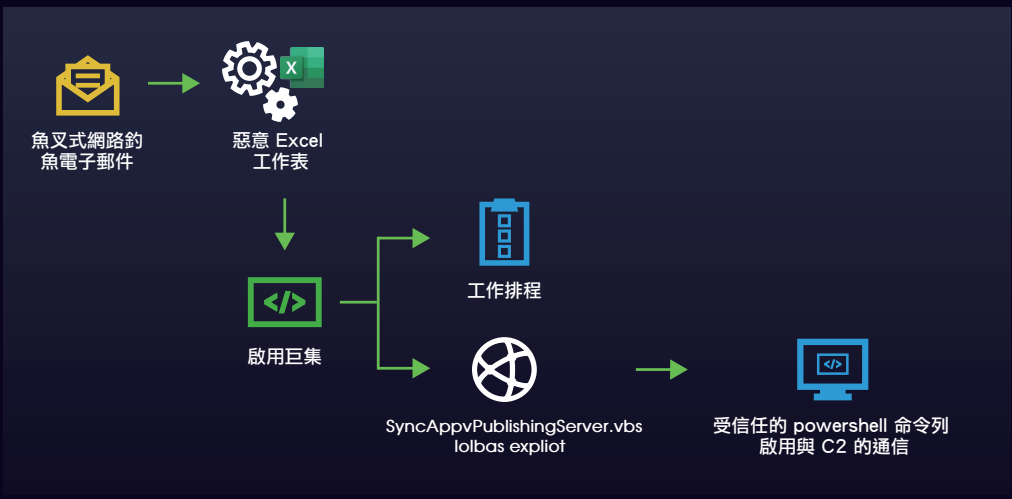


圖 1. 資安攻擊流程圖

TRELLIX 資安研究室發現政府高官遭到網路攻擊

1月時，我們的團隊宣布發現一項多階段間諜活動，目標包含負責國家安全政策的高階政府官員、以及亞洲西部各國防工業的成員。Trellix向受害者披露此間諜活動，並提供了所需的工具，將所有已知的攻擊元件，從其電腦環境中刪除。

對此攻擊的分析，是從執行一個包含 MSHTML 遠程代碼執行漏洞 (CVE-2021-40444) 的 Excel 檔案開始。開啟了這個檔案，就會執行其中的惡意DLL ，作為我們稱為 Graphite 的第三階段惡意軟體下載器。Graphite 是一個新發現的惡意軟體樣板，它是以 One-Drive Empire Stager為基礎所開發，藉由Microsoft Graph API將OneDrive帳號作為指令和控制伺服器之用。
這種多階段攻擊的最後階段，我們認為這與APT作業有關聯，包括執行不同的Empire stager，最後會在受害者的電腦中下載一個Empire代理程式，讓攻擊者伺服器得以遠端控制受害者的電腦。

下圖說明攻擊的流程。

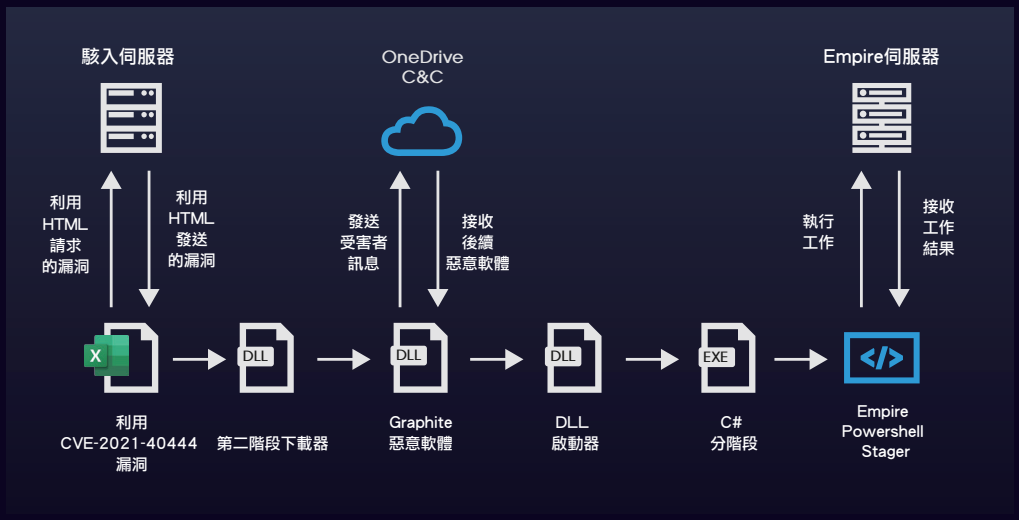
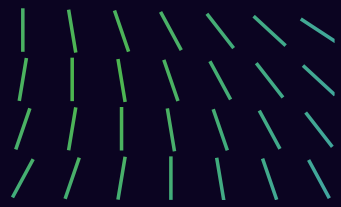


圖 2. 攻擊流程圖

歡迎造訪我們的部落格，以進一步探討其攻擊階段、內部攻擊架構、和歸因分析。



我們的研究方法

我們將Trellix後端系統所提供的遙測數據，用於季度資安威脅報告的資料來源。在這份報告裡，結合了我們的遙測資料、資安威脅相關的開源情報，以及我們對勒索軟體、各個國家的資安威脅的調查。

我們所討論的遙測，著重的是事前的預防偵測，而不是被攻擊後的補救。當我們的產品偵測到檔案、URL、IP 地址或其他指標等，具有特定特性的資料時，我們就會收到回報。

維護客戶隱私至關重要，尤其是遙測資料涉及到客戶的產業和國家地區。我們在每個國家／地區的客戶樣貌都有所不同，當我們更深入地研究這些數據時，要分析的資料量就相對大幅增加。

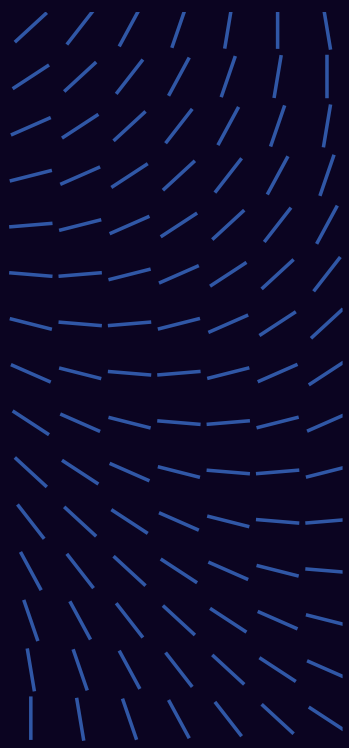
舉例說明：電信業者在我們的遙測資料數量中名列前茅，但這並不一定代表電信業被當作主要的攻擊目標。電信部門也包含 ISP 供應商角色，它們擁有可供出售或出租的 IP 位址空間。這意味著來自 ISP 的 IP 位址被標示為電信用途，然而這些IP位址可能已經被客戶承租，應用於其他行業。因此在實際的行業數據研究時，還是會有些許的落差。

勒索軟體

在 2021 年最後一季，勒索軟體的格局繼續發生變化，它已經不是先前的報告中所描述的龐大規模攻擊，勒索軟體攻擊者如今必須找到一個新基地重起爐灶。執法部門已經成功打擊了幾個倍受矚目的勒索軟體組織，其中之一是 REvil/Sodinokibi，它在第三季仍然在勒索軟體排行榜名列前茅。然而，REvil 在經歷了拆除基礎設施、幾起內部糾紛、和成員被捕後銷聲匿跡。Trellix 很自豪能夠藉由提供惡意軟體分析、定位關鍵基礎設施、和識別多個嫌疑犯的身分，瓦解了Revil組織。

2021年第四季的前三名勒索軟體，分別是Lockbit、Cuba和Conti。我們懷疑 REvil 的殘餘成員很可能已經在這些勒索軟體家族當中，找到了新的棲身之地。

在這份報告發稿前夕，情況再次發生變化。Conti已經成長為最大的家族之一，並在網路上洩漏了數千條內部聊天記錄，暴露了他們內部的秘密。我們將此洩漏稱為勒索軟體的巴拿馬文件，在下一季的報告中會報導出來。



為了幫助企業更完善了解、和抵禦勒索軟體攻擊，我們的資安威脅研究團隊從2021年第四季開始，就各種勒索軟體威脅的蔓延情況，對於勒索軟體家族、技術、國家、部門和媒介等方面，展示我們的研究和發現。

289%

媒體和通信類別
從 2021 年第三季到第四季
增加了289%。

▼61%

從 2021 年第三季到第四季，美國客戶的勒索軟體數量下降了61%。

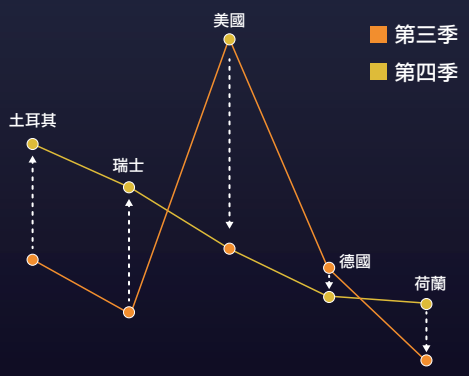
勒索軟體主要攻擊對象

- 商業服務
- 非營利組織
- 政府
- 媒體和通訊
- 運輸和航運

MITRE ATT&CK 報告中最常用的勒索軟體技術

1. 為惡意目的加密數據
2. 洩漏檔案和目錄
3. 竄改檔案或訊息
4. 洩漏執行中程式
5. 程式中注入惡意執行碼

勒索軟體主要攻擊的國家



被偵測到的主要勒索軟體家族

	Lockbit	Cuba	Conti	Ryuk	BlackMatter
Q3	4%	8%	6.7%	7%	N/A
Q4	23%	19%	17%	11%	7%

各國資安狀態

我們的團隊追踪和監看各國資安狀態，以及相關的指標和資安威脅技術。我們的研究包含了威脅行為者、工具、國家、行業、和MITRE ATT&CK資料庫。
2021 年第四季的資安威脅技術。以及這些事件的所有相關數據，包括指標、YARA 規則和偵測邏輯，都可以在 MVISION Insights 中取得。

MITRE ATT&CK 報告中最常用的勒索軟體技術

1. PowerShell
2. 工作排程
3. 竄改檔案或訊息
4. Windows
5. 網路協議

▲95%

Cobalt Strike 在 2021 年第四季的 Nation-State Threat Tool 觀察中排名最高。

▲30%

APT 29 在 2021 年第四季度的所有國家觀察中排名最高，比第三季增加 35%。

26%

土耳其的資安威脅活動，佔2021年第四季全球總偵測量的 26%。

企業客戶排行

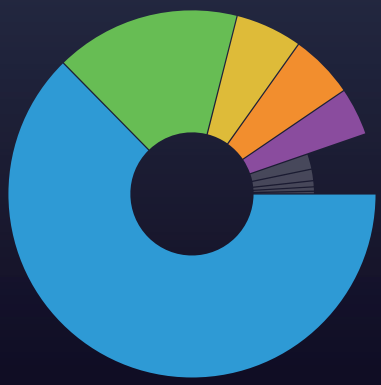
- 電信業
- 運輸和航運業
- 商業服務
- 政府
- 非營利組織

流行資安威脅統計

我們的團隊在2021年第四季追踪了威脅類別。此研究反映了在觀察到的流行惡意軟體系列、相關客戶國家、企業客戶部門和 MITRE ATT&CK 技術類型中的檢測百分比。

企業客戶排行

- 運輸業
- 電信業
- 消費者
- 商業服務
- 科技業



75%

RedLine Stealer (20%)、Raccoon Stealer (17%)、Remcos RAT (12%)、LokiBot (12%) 和 Formbook (12%) 佔2021年第四季所觀察到惡意軟體家族工具威脅的75%。

62%

交通運輸業客戶在 2021 年第四季，是被攻擊最嚴重的行業（62%），超過了其餘前10名行業的總和。

80%

從 2021 年第三季開始，觀察到美國客戶被影響程度增加 80%。

被通報最多的 MITRE ATT&CK 技術

1. 竄改檔案或訊息
2. 來自 Web 瀏覽器的憑證
3. 洩漏檔案和目錄
4. 登錄檔執行碼／啟動檔案夾
5. 洩漏系統資訊

最常被運用的惡意軟件家族

	RedLine Stealer	Raccoon Stealer	Remcos RAT	LokiBot	Formbook
Q3	1.2%	N/A	24%	19%	36%
Q4	20%	17%	12%	12%	12%

世界各地區、行業、攻擊方式分析

2021 年第四季開源公開報告的事件中，顯著增加的地區、行業、方式如下：

攻擊方式

- 惡意軟體 (46%)
- 未知 (19%)
- 帳戶接管 (16%)
- 安全漏洞 (10%)
- 針對性攻擊 (8%)

150%

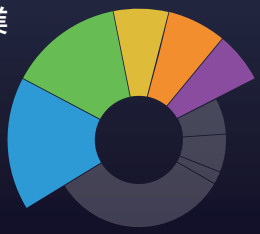
德國在 2021 年第四季通報事件的增幅最高（150%）。

38%

美國在 2021 年第四季通報的事件最多，佔通報事件總數的 38%。

最多被攻擊的行業

- 個人
- 衛生保健業
- 科技業
- 公部門
- 教育業



就地取材式攻擊

網路犯罪分子持續開發攻擊工具，但近來開始轉向以就地取材 (LotL, Living off the Land) 的技術，藉由濫用合法二進位檔案和管理程式，將惡意負載傳送到目標系統。根據 2021 年第四季的統計，Trellix 發現攻擊者使用工具的趨勢略有變化，目的在於要更不容易被偵測到。

隨著防禦技術的加強，以及同行之間的資訊分享，以致戰術、攻擊技術和程式也發生變化。在我們的第三季報告中，我們重點介紹了一些常見於 Windows、以及管理人員用於執行日常任務的一些二進制檔案。並建議部署必要的軟體，以監控異常情況並保持系統效率。從第三季報告開始，我們報導了惡意駭客已經利用這些程式進行威脅活動，在第四季被惡意駭客濫用的程式，已經發現使用的情況略有變化。不變的是：惡意駭客試圖保持隱身，並濫用系統上已經存在的內容來傳遞訊息與負載，如勒索軟體、信標、竊取資料、和偵察工具等。

為了在偵察階段就能識別出這些二進制檔案或管理工具，攻擊者可能會以職缺公告、使用者見證廣告信、公司同事查詢資料之類的假郵件來收集訊息。

原生作業系統二進制檔案		說明
Windows Command Shell (CMD) (53.44%)	T1059.003	Windows Command Shell 是 Windows 的主要 CLI 公用程式，通常用於在備用資料流中執行檔案和命令。
Powershell (43.92%)	T1059.001	PowerShell 通常用於執行腳本和 PowerShell 命令。
WMI/WMIC (33.86%)	T1218, T1564.004	WMIC 是 WMI 的命令列界面，攻擊者可以使用它在本地、備用資料流中或遠端系統上執行命令。
Rundll32 (24.34%)	T1218.011, T1564.004	Rundll32 可執行本地、他人共享、或是透過備用資料流從網路所得到的DLL檔案。
Regsvr32 (14.29%)	T1218.010	攻擊者可能會使用 Regsvr32 註冊 dll 檔案、執行惡意代碼，和繞過應用程式白名單。
Schtasks (12.70%)	T1053.005	攻擊者可能會安排長時間的惡意軟體執行、或自動化工作。

MSHTA (10.05%)	T1218.005	攻擊者可能會使用MSHTA 來執行 JavaScript、JScript 和 VBScript檔案，這些檔案可能隱藏在本地 HTA 檔案和備用資料流中、或從遠端位置傳送過來。
Excel (8.99%)	T1105	許多系統縱使並未安裝，但還是包含了這套試算表軟體，攻擊者可能會向用戶發送包含惡意代碼或腳本的附件，這些惡意代碼或腳本在執行時，就可用從遠端位置進行操控。
Net.exe (7.94%)	T1087 & Sub-techniques	Windows 的命令列公用程式，它容許攻擊者執行偵察任務，如辨識別受害者電腦的用戶名稱、網路和服務等功能。
Certutil (4.23%)	T1105, 1564.004 T1027	Windows 命令列公用程式，用於取得認證頒發機構資訊，和認證配置服務。攻擊者可以使用 Certutil 來收集遠端工具及其內容、對檔案進行編碼和解碼，以及使用備用資料流。
Reg.exe (3.70%)	1003.002, 1564.004	攻擊者可能會使用 Reg.exe 增加、修改、刪除和輸出登錄表數值，這些數值可能經由備用資料流外洩。此外，Reg.exe 可從SAM檔案中傾印憑證資料。

管理工具			說明
Remote Services (35.98%)	T1021.001, T1021.004, T1021.005	AnyDesk ConnectWise Control RDP UltraVNC PuTTY WinSCP	攻擊者可能會使用 Windows 和第三方軟體以及有效帳戶，對遠端設備執行惡意軟體、以及洩漏資料。
Archive Utilities (6.35%)	T1560.001	7-Zip WinRAR WinZip	攻擊者可以使用此備份應用程式，將要竊取的檔案或執行檔進行壓縮或解壓縮。
BITSAdmin (3.70%)	T1105, T1218, T1564.004		BiTSAdmin 通常用於軟體維護及清理，並在完成設定標準後，呼叫其他程式作業。
ADFind (2.65%)	T1016, T1018 T1069, & Sub-Techniques, T1087 & Sub-techniques, T1482		攻擊者可以使用命令列應用程式取得Active Directory的資訊，如網域信任、權限組、遠端系統和網路配置等。
PsExec (2.12%)	T1569.002		PsExec 為可在遠端系統上執行命令和程式的工具。
fodhelper.exe (0.05%)	T1548.002		Fodhelper.exe 是一個 Windows 公用程式，攻擊者可使用它在受害者的電腦上，以調升的權限執行惡意程式。

資源

要追踪最新的資安威脅和研究，請參閱以下 Trellix 資源：資安威脅中心－我們團隊所發現最具影響力的威脅。

TWITTER

Trellix Threat Labs

Christiaan Beek

John Fokker

Douglas McKee

Steve Povolny

下載PDF

瀏覽資安威脅報告檔案

關於 Trellix

Trellix 是一家重新定義網路安全未來的全球性公司。該公司的開放式原生擴展偵測和回應 (XDR) 平台，可幫助企業面對當今最先進的威脅，對資料保護和作業彈性具備高度信心。Trellix 的資安專家與眾多夥伴生態系統通力合作，透過機器學習和自動化加速技術創新，為 40,000 多家企業和政府客戶提供支援。更多訊息請造訪 www.trellix.com。

Trellix資安威脅研究室

訂閱我們的資安威脅資訊

台灣區代理商 | 創泓科技股份有限公司
台北市內湖區洲子街77號10樓 | 電話：886 2 2658 3077 | 傳真：886 2 2658 3097
郵件：sales@uniforce.com.tw | www.uniforce.com.tw

UNIFORCE 創泓科技

Trellix
6220 American Center Drive,
San Jose, CA 95002

研究與撰述

Christiaan Beek
Tim Hux
John Fokker
Douglas McKee
Tim Polzer
Steve Povolny
Leandro Velasco
Max Kersten
Alfred Alvarado
Thibault Seret