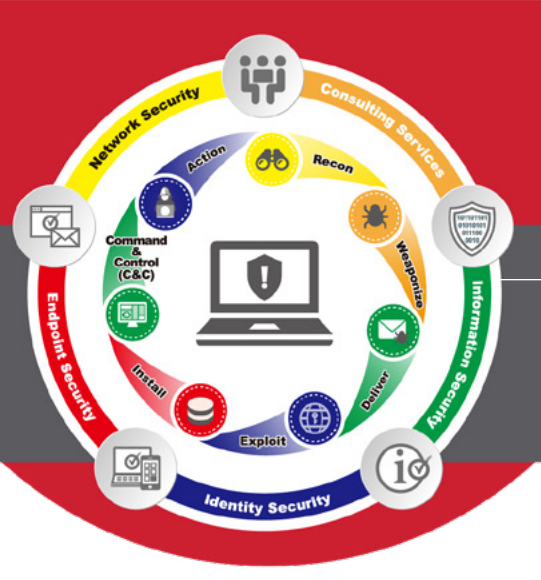


好工具淪為壞凶器又一起，AutoIt淪為駭客圈愛用的混淆器

2024 年 11 月 5 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

AutoIt 是一種免費的腳本語言，設計用來自動化 Windows 圖形化介面程式和常用的腳本。自 2004 年推出第一個公開可用的版本以來，只要花點時間就可以在黑帽駭客社群找出如何濫用它的知識與經驗分享。多年來，攻擊者在攻擊鏈中多利用它來逃避偵測。

以最近的實際案例來說，在 Snake Keylogger 這支惡意竊密程式所涉入的惡意活動中，AutoIt 就被用作混淆器。Snake Keylogger 內嵌於 AutoIt 腳本中，並由 AutoIt 腳本的編譯器 Aut2Exe 轉換為 Windows 可執行檔。

網路上的知識：混淆器是一種能將原始程式碼的功能完全保留並發揮，但令人難以閱讀與理解的工具。在特定情況，你需要提供程式給其他人，或公開在網站，例如：網頁內的 javascript code，基於保護個人智慧財產，你不希望別人了解你的程式邏輯與演算法，但是程式又可以必須可以正確執行。混淆器在網路攻擊中也扮演愈來越重要的角色，它能讓駭客利用現成的惡意軟體，經由混淆後，讓基於簽名檔的安全軟體，束手無策。

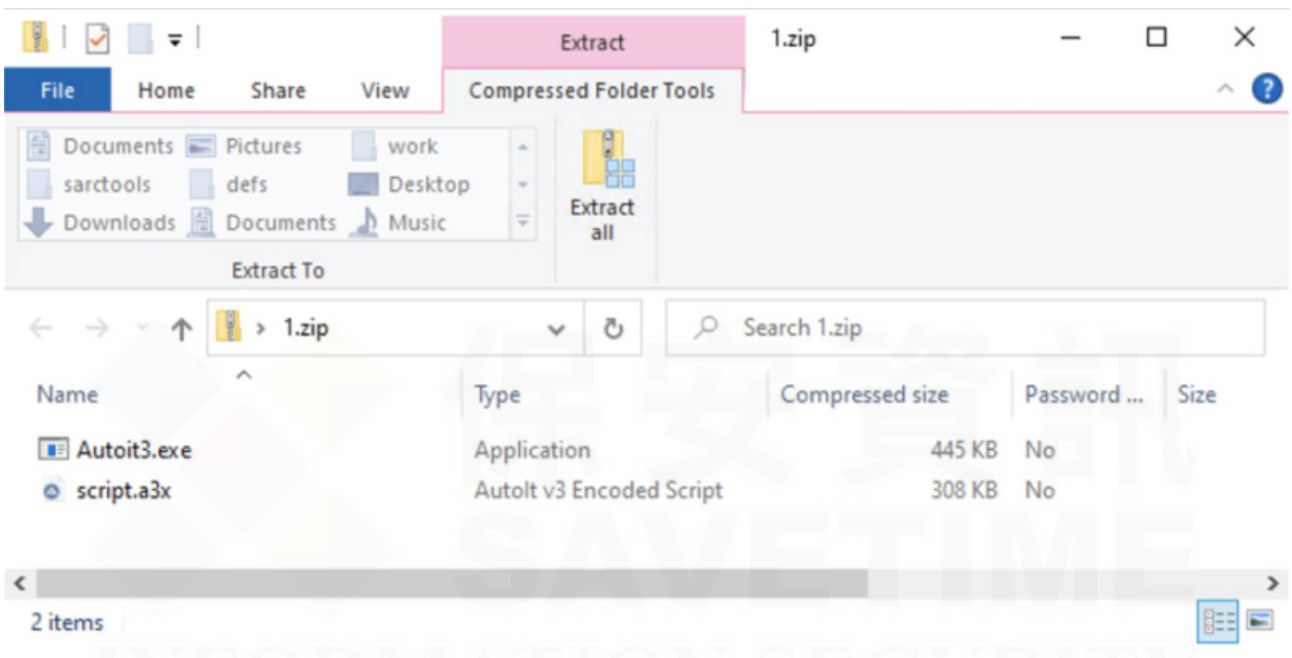
從 Windows 可執行檔中的 AutoIt 腳本編譯的二進位資料

```
A3 48 4B BE 98 6C 4A A9 99 4C 53 0A 86 D6 48 7D   .HK..lJ..LS...H}
41 55 33 21 45 41 30 36 FA E2 B0 E0 8F 64 BB AE   AU3!EA06.....d..
13 21 39 71 51 FF D6 12 6B 43 CA 52 AF AD 00 00   .!9qQ...kC.R....
E6 FB 25 78 C8 E2 13 F9 7D 1D ED DD 71 00 B0 55   ..%x....}...q..U
2D AC 9A D5 28 15 D4 F0 CF 25 E4 CF 11 8E 56 C2   -...(....%....V.
CE 3F 70 EF B9 68 12 F8 00 00 2E AC 66 00 E7 CE   .?p..h......f...
36 AE 6B 99 3D 58 92 51 E9 53 69 0C 1A 2E 52 00   6.k.=X.Q.Si...R.
5D C1 C8 FC 3A D8 F7 B6 0B 1E 6A 14 46 AE 55 80   ]...:.....j.F.U.
58 FF 58 DE AF 8B 98 A1 80 91 5A 52 F1 5D 9A 94   X.X.......ZR.]..
1F 01 A6 6B 1C 48 4E 8D E3 D3 64 DD 93 F0 08 85   ...k.HN...d.....
A8 52 5B E7 10 77 B8 98 5D 4A 40 46 C2 91 8A A3   .R[..w..]J@F....
B4 98 9D C5 9D 88 71 3D 17 F8 D0 33 67 A0 01 0E   ......q=...3g...
EF 09 00 65 D6 1C 00 FE 9A 21 50 96 0A DB 01 61   ...e.....!P....a
22 22 A0 96 0A DB 01 E3 AB 2B A0 6D FB FA 03 B3   "".......+.m....
97 6F 60 85 F2 38 8E 35 E6 DE 0C 78 D2 E3 F2 28   .o`..8.5...x...(
6E 55 8B 6A 84 F5 A4 00 30 36 A8 6E 22 B7 51 02   nU.j....06.n".Q.
```

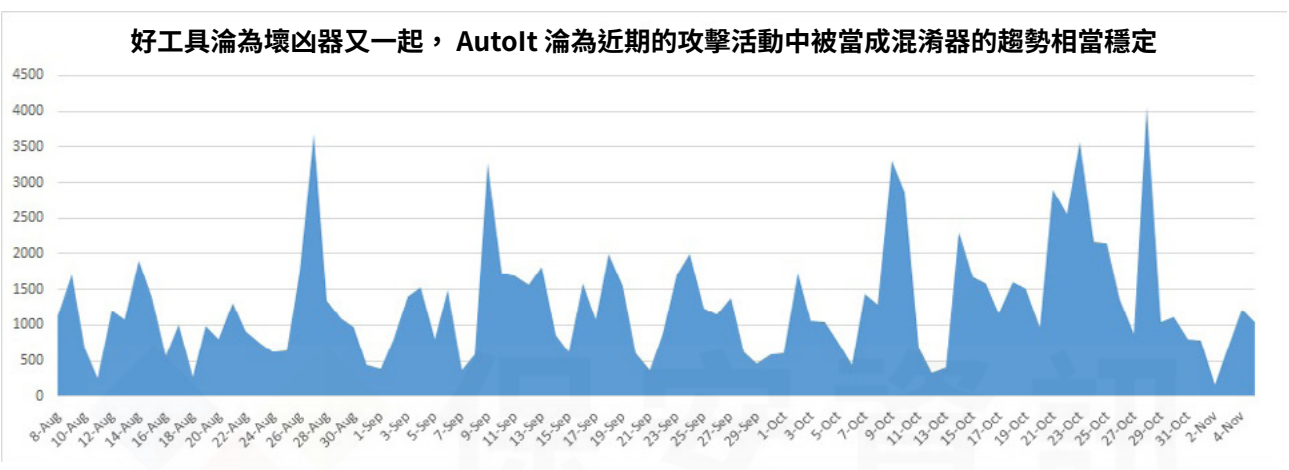
從編譯資料中提取的 (混淆) 腳本

```
Global $xvqmwba = "0x1b00d44951594f5842535249b0c64a41f75932584a5755560a4230524750565a444952594f58465352494f394a414f5932584a5755
$xvqmwba &= "932384e5759564a4230524750565a444952594f58465352494f394a414f5932584a5755564a4230524750565a444952594f58465352494f394a
$xvqmwba &= "20150565a0449452597858465377494f3927414f5916584a572b564a424e524750325a444920594f582753524908394a41205932582457555634
$xvqmwba &= "52623e55564c421a68472e4a5a444d5036a35846597463e13934064f59362602575552347b30524322c24444397a114f584c21c8574f496291
$xvqmwba &= "e65a444d7959657a44502ff94f394e6b695b49e94a57517d4a681250442de75a444d787f4d23f453524d643960634d5a4fea4a57517c6c404b
$xvqmwba &= "4220524750575a445852274e5846573d6e4f39404b64593472596754565a4230524550564b443750594f5c297b524945336141497321684b57
$xvqmwba &= "d43524b402667594f5252ad515a4a284f57b15acc496c256e564a3227df0750565b615f435d206d4653582679394a4bed711d584a5d46505b4
$xvqmwba &= "94a41435932494a296a564a48bc5a47504d4eba48595e63526e51524964b975414f534c674a575f5c614236784750456a46496e594f584b5352
$xvqmwba &= "5247565629014952536774465354493c7c4a4145711c584a5155250f4230586f60565a4249211c4f584c7b60494f3f4a320a593252626355564
$xvqmwba &= "055846597a104f394c69055932523810565 63a6a7a52475a24f947492271055846597a114f394c69055932523810565 63a6a7a52475a24e547
$xvqmwba &= "55640c209524754240340492227635846577a194f394cc17559325c38e451563a3c1c5247547e0a444954d97458465720ac4b393a3f6359325c
$xvqmwba &= "5f7e03423058c71b565a403b175e4f28c61e52494b4b21464f29b2004a57517c597232527350565a54495248 5ba640355249494a1a414f5338
$xvqmwba &= "7545d5d684e555f200a465358635c0948417b5932585a5755475ebc362c475050291449525345265453524d443e6646485f5d094a575f54ca5
$xvqmwba &= "9b34a41492a62584a5d5f285c4230564c577a5d434f3d084f584c51d25f4f394e3f5959325c415079514d445f0047505c70577950597b58465
$xvqmwba &= "59434020654a41454a38494e4650405b47be3b280e565a4e49435d5e52504258c726561441 4f53322a435e552650cf33524751734c40eb774e
$xvqmwba &= "de5946535c494f394a414f5930584a57f8574a422b5247509e5b44495c594f58465352494f394a414e5932589d5655569243305257505 65a01
$xvqmwba &= "74a301258472054721449525f45734655784 94f3959714d5923584a575f564a5330203b5a562a466102594f5e4c78524f65394a4154693758e
$xvqmwba &= "85a492b4c33885e322862025556406a7952475a5d5c2b395259452a4e5852393dec4d413f5e1a114a575f393b4230584756392844 49585b202
$xvqmwba &= "a575f221a4230534c2e2e5a44435e594837265352434239432e365932525953445262183052 4d232c5a4443415c5e5d292852494 51f94374f4
$xvqmwba &= "144f570353524854094f41c259325852575547 4a4243d547505c5137c1525945543409534 93f3454cc1059325959535d7ec342305843f0a5a
$xvqmwba &= "4a48429b4b5026720d4952535c5c575758624f3f60415c6931586c5755565042304347 78c05a44437ace4f584c2183454f4962d94f593870dd
$xvqmwba &= "9384b4e894573627630524d43515a6c2b525958646453434d3c9a4a41454a37494f382e564a482354565439fe444958595e5d29f6524945395
$xvqmwba &= "496945588e53524952394a504f5941ff4a575f5d38c23e523778005a444f7a124f584c5f555d3dfb44413f4ebf5b4a5754735c4a927754554 2
$xvqmwba &= "2d594f59634545d56a2a4c5667f1325840714450 5cd31d506c5a475f52d37a624f584c5f553bb5374a3120f03258405a270c4b424041435939
$xvqmwba &= "7422d9c52475a455e44585536e258465941405e30679a914e235f3f4255564b6e3d434025435a44483d584f584c538e584b3394536a7106584
$xvqmwba &= "4928397bd94f4e32584a5755564b4283e64742135a4448496945588e53524952394a504f5941ff4a575f5d38c23e523778005a444f7a124f58
```

在另一個案例中，DarkGate 涉入攻擊活動的攻擊鏈中使用 AutoIt。一個包含合法 AutoIt 解譯器 Autoit3.exe 和惡意編譯的 AutoIt 二進位檔 script.a3x 的 Zip 檔案被放置在受攻擊的網站上。攻擊鏈的前一階段會下載 Zip 檔案，解壓後並執行含有惡意二進位檔的 Autoit3.exe。



在這兩種情況下，攻擊者都會將惡意程式碼隱藏在 AutoIt 腳本中，以增加偵測的難度。我們長期對此攻擊手法與途徑的持續監控顯示其趨勢相當穩定。



賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- AUT.Heuristic!gen1
- AUT.Heuristic!gen3
- AUT.Heuristic!gen5
- AUT.Heuristic!gen6
- AUT.Heuristic!gen7
- AUT.Heuristic!gen10
- AUT.Heuristic!gen12
- AUT.Heuristic!gen13
- AUT.Heuristic!gen14
- AUT.Heuristic!gen15
- AUT.Heuristic!gen16
- AUT.Heuristic!gen18
- AUT.Heuristic!gen19
- AUT.Heuristic!gen20
- AUT.Heuristic!gen22
- AUT.VictoryGate!gen1
- Scr.Malscript!gen14
- Scr.Malcode!gen

賽門鐵克提供三種常見情境的端點安全解決方案：SEP／SESE／SESC，請點擊此處了解解決方案的全貌以及您的企業適合選用哪一種方案。

在重要的伺服主機，例如：AD、SQL、ERP、WEB、Exchenge……主機，賽門鐵克基於政策強制、最低資源、最少權限及網路入侵防禦技術……DCS：Data Center Security 是大型企業列為資料中心必要的解決方案，請點擊此處瀏覽 DCS 的完整資訊。

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 年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。