從 NetWalker 死灰復燃的 Alpha 勒索軟體

2024 年 2 月 16 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

Alpha 是 2023 年 2 月首次出現一種新型勒索軟體，最近幾週以來加強運作，它與早已不復存在的 NetWalker 勒索軟體非常相似，NetWalker 在一次全球性執法行動後已於 2021 年 1 月消失。

與 NetWalker 的關聯

經由對 Alpha 分析後顯示，它與之前的 NetWalker 勒索軟體非常相似。這兩種威脅都使用以 PowerShell 為基礎的載入器 (loader) 來傳遞有效載荷。除此之外，Alpha 和 NetWalker 的有效載荷程式碼之間有大量相同之處。包含：

- 兩者有效載荷其主要功能的執行流程大致相同。
- 在單一執行緒內處理兩項功能：終止處理程序和終止服務。
- 相似的 API 解析。然而在解析 API 雜湊值 (hash) 時，其使用的雜湊值並不相同。
- 兩者有效載荷有著相似的設定，包括跳過的資料夾、檔案和副檔名，以及要終止的處理程序和服務。
- 加密完成後，兩者有效載荷都會使用暫時性的批次檔刪除自己。
- 兩者都有相似的支付入口，包含相同的訊息：『For enter, please use user code』。

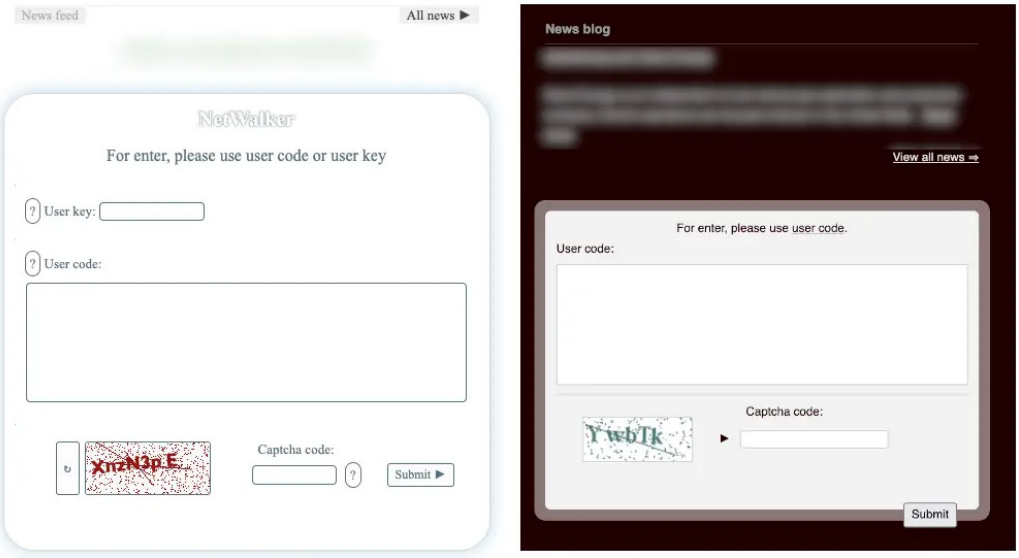

圖 1. NetWalker 支付入口 (左) 和 Alpha 支付入口(右)。兩者都包含相同的訊息：『For enter, please use user code』

NetWalker	Alpha
nslsvice.exe	nslsvice.exe
pg*	pg*
nservice.exe	nservice.exe
cbvscserv*	cbvscserv*
ntrtscan.exe	ntrtscan.exe
cbservi*	cbservi*
hMailServer*	hMailServer*
IBM*	IBM*
bes10*	bes10*
black*	black*
apach*	apach*
bd2*	bd2*
db*	db*
ba*	ba*
be*	be*
QB*	QB*
oracle*	oracle*
wbengine*	wbengine*
vee*	vee*
postg*	postg*
sage*	sage*
sap*	sap*
b1*	b1*
fdlaunch*	fdlaunch*
msmdsrv*	msmdsrv*
report*	report*
msdtssr*	msdtssr*
coldfus*	coldfus*
cfdot*	cfdot*
swag*	swag*
swstrtr*	swstrtr*
jetty.exe	jetty.exe
wrsa.exe	wrsa.exe
team*	team*

NetWalker	Alpha
agent*	agent*
store.exe	store.exe
sql*	sql*
sqbcoreservice.exe	sqbcoreservice.exe
thunderbird.exe	thunderbird.exe
ocssd.exe	ocssd.exe
encsvc.exe	encsvc.exe
excel.exe	excel.exe
synctime.exe	synctime.exe
mspub.exe	mspub.exe
ocautoupds.exe	ocautoupds.exe
thebat.exe	thebat.exe
dbeng50.exe	dbeng50.exe
sql	*sql*
mydesktopservice.exe	mydesktopservice.exe
onenote.exe	onenote.exe
outlook.exe	outlook.exe
powerpnt.exe	powerpnt.exe
msaccess.exe	msaccess.exe
tbirdconfig.exe	tbirdconfig.exe
wordpad.exe	wordpad.exe
ocomm.exe	ocomm.exe
dbsnmp.exe	dbsnmp.exe
thebat64.exe	thebat64.exe
winword.exe	winword.exe
oracle.exe	oracle.exe
xfssvccon.exe	xfssvccon.exe
firefoxconfig.exe	firefoxconfig.exe
visio.exe	visio.exe
mydesktopqos.exe	mydesktopqos.exe
infopath.exe	infopath.exe
agntsvc.exe	agntsvc.exe
	notepad.exe
	genshinimpact.exe

表 1. NetWalker 和 Alpha 要終止的處理程序清單幾乎完全相同。唯一不同的是，Alpha 列表中增加記事本 (Notepad)和『元神』遊戲 (Genshin Impact)。後者被列入的原因尚不清楚。

```
NTSTATUS __stdcall NtQuerySystemInformation_w(SYSTEM_INFORMATION_CLASS SystemInformationClass)
{
  int v1; // esi
  APIs *CustomIAT; // eax
  int v3; // eax
  NTSTATUS v5; // [esp+10h] [ebp-4h] BYREF

  v1 = 0x1024;
  v5 = 0;
  while ( RtlReAllocateHeap_w(&v5, v1) )
  {
    CustomIAT = (APIs *)GetCustomIAT();
    v3 = ((int (__stdcall *)(SYSTEM_INFORMATION_CLASS, NTSTATUS, int, _DWORD))CustomIAT->NtQuerySystemInformation)(
           SystemInformationClass,
           v5,
           v1,
           0);
    if ( v3 != 0xC0000004 )
    {
      if ( v3 >= 0 )
        return v5;
      break;
    }
    v1 += 0x1024;
  }
  RtlFreeHeap_w(v5);
  return 0;
```

圖 2. 在 NetWalker 中使用自訂的匯入位址表 (IAT)。當呼叫 NtQuerySystemInformation API 時，它會使用一個函數來解析自訂 IAT 的起始位址，並從該位址引用所需的 API 位置。

```
int __cdecl NtQuerySystemInformation_w(int a1, int a2)
{
  APIs *CustomIAT; // eax
  int v4; // [esp+0h] [ebp-10h]
  int v5; // [esp+4h] [ebp-Ch]
  int i; // [esp+8h] [ebp-8h]
  int Heap; // [esp+Ch] [ebp-4h]

  if ( !a2 )
    a2 = 0x1024;
  v4 = 0;
  Heap = 0;
  for ( i = a2; ; i += a2 )
  {
    Heap = RtlReAllocateHeap_w(Heap, i);
    if ( !Heap )
    {
      RtlFreeHeap(0);
      return 0;
    }
    CustomIAT = (APIs *)GetCustomIAT();
    v5 = ((int (__stdcall *)(int, int, int, _DWORD))CustomIAT->NtQuerySystemInformation)(a1, Heap, i, 0);
    if ( v5 != 0xC0000004 )
      break;
  }
  if ( v5 >= 0 )
    return Heap;
  return v4;
}
```

圖 3. 在 Alpha 中使用自訂匯入位址表 (IAT)。

Alpha 攻擊

雖然 Alpha 在 2023 年 2 月首次出現，但它一直保持低調，直到最近幾週，它似乎開始擴大行動規模，並推出一個資料洩漏 (data leak) 網站。

在最近涉及 Alpha 攻擊中，攻擊者大量使用一些就地取材工具 (living-off-the-land) ，包括：

- Taskkill：Windows 命令列工具，可用於終止一個或多個工作或處理程序。
- PsExec：微軟 Sysinternals 工具，用於在其他系統上執行程序。攻擊者主要使用該工具在受害者網路上橫向移動。
- Net.exe：微軟工具，可用於停止和啟動 IPv6 協定。
- Reg.exe：Windows 命令列工具，可用於編輯本地或遠端電腦的登錄表。

重塑品牌還是回歸？

NetWalker 是首波從針對性的勒索軟體攻擊中獲利的網路犯罪活動之一，在勒索軟體攻擊中，攻擊者試圖加密整個網路以勒索受害者。據稱，僅一名被監禁的犯罪組織成員就從攻擊中獲利超過 2760 萬美元。

經過全球執法行動之後的長期停止運作，人們一直以為 NetWalker 已經徹底消失。然而，Alpha 與 NetWalker 勒索軟體之間的相似之處表明，這兩種威脅之間存在著密切聯繫。Alpha 可能是一個或多個最初的 NetWalker 開發人員試圖恢復勒索軟體舊業。另外，Alpha 背後的攻擊者可能已經獲取並修改原始 NetWalker 有效載荷，以便啟動自己的勒索軟體運作。

防護方案／緩解措施

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)。

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。

46569bf23a2f00f6bac5de6101b8f771feb972d104633f84e13d9bc98b844520-PowerShell loader
6462b8825e02cf55dc905dd42f0b4777dfd5aa4ff777e3e8fe71d57b7d9934e7-PowerShell loader
6e204e39121109dafcb618b33191f8e977a433470a0c43af7f39724395f1343e-PowerShell loader
89bfcbf74607ad6d532495de081a1353fc3cf4cd4a00df7b1ba06c10c2de3972-PowerShell loader
e43b1e06304f39dfcc5e59cf42f7a17f3818439f435ceba9445c56fe607d59ea-PowerShell loader
e573d2fec8731580ab620430f55081ceb7153d0344f2094e28785950fb17f499-Alpha ransomware loader
e68dd7f20cd31309479ece3f1c8578c9f93c0a7154dcf21abce30e75b25da96b-Alpha ransomware loader
ab317c082c910cfe89214b31a0933eaab6c766158984f7aafb9943aef7ec6cbb-Alpha ransomware loader
df15266a9967320405b3771d0b7353dc5a4fb1cbf935010bc3c8c0e2fe17fb94-Alpha ransomware loader
b7ca6d401b051712cb5b1a388a2135921a4420db8fe41842d51d2ec27380b479-Alpha ransomware loader
5f3bf9c07eedde053f19ce134caa7587f8fb6c466e33256e1253f3a9450b7110-Alpha ransomware loader
c00fbf3fb992e7f237c396d69081246570cbd60d6c7a2262c01ae4d8e6f17ddd-Alpha ransomware loader
b2adf8ec7ab5193c7358f6acb30b003493466daee33ea416e3f703e744f73b7d-Alpha ransomware loader

a8d350bbe8d9ccfbb0c3e9c2dd9251c957d18ce13ae405ceb2f2d087c115db15-Alpha ransomware loader
2d07f0425dc465b3a1267a672c1293f9a3d0cd23106b7be490807fea490978ea-Alpha ransomware loader
f5d25777331ba55d80e064dea72240c1524ffcd3870555a8c34ff5377def3729-Alpha ransomware loader
9d6ed8396ee79ae92a5e6cef718add321226def3461711cf585e0fd302c961ae-Alpha ransomware loader
1c12ff296e7d9f90391e45f8a1d82d8140edf98d616a7da28741094d60d4779d-Alpha ransomware loader
9c71500a9472814f7bf97a462fe9822cf93dc41e2e34cc068734586d5e5146ef-Alpha ransomware loader
480cf54686bd50157701d93cc729ecf70c14cd1acd2cb622b38fc25e23dfbc26-Alpha ransomware loader
0bad18cb64b14a689965540126e0adbc952f090f1fb7b6447fe897a073860cdb-Alpha ransomware loader
c5f7492a3e763b4456afbb181248fdb8e652575cea286db7861e97ffcd1b72e4-Alpha ransomware loader
f3858d29073ae90f90c9bb284913752533fe1a6437edd6536e4b1775fc8f6db4-Alpha ransomware loader

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/alpha-netwalker-ransomware

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**。