

Name: Nguyễn Lê Đinh Vũ

ID: BI11-291

### Report for labwork svchost.exe

|                      |  |
|----------------------|--|
| Date:                | 23/10/2022   |
| Workstation:         | REM Vmware   |
| File Name:           | svchost.exe  |
| File Location:       | C:\Users\REM\Desktop\Malware\Day2\svchost.exe  |
| File Timestamps:     | Sat Aug 21 10:36:59 2010   |
| Notification Vector: |  |
| File Size (bytes):   | 104448 bytes   |
| Icon Graphic:        |  svchost   |
| Signed?:             |  |
| File Hash:           | Svchost.exe<br>md5: C63A537090D34F29DAADBEF221637435<br>sha1:BA17638BAC43E6E3B2FAF4BF3A22197B99D8A390<br>sha256:28046C14EA3325885EE1E731CD0BCF9F38445DF02675836B851CB2A<br>E94C050EB |
| Imp Hash:            | 31553623C43827D554AD9E1B7DFA6A5A   |
| PE Section Hashes:   |  |

We can see by click on ‘sections” part

pestudio 8.74 - Malware Initial Assessment - www.winitor.com

File Help

| property                    | value                   | value                  | value                   | value                   |
|-----------------------------|-------------------------|------------------------|-------------------------|-------------------------|
| name                        | .text                   | .rdata                 | .data                   | .reloc                  |
| md5                         | 7C04B5773D76E399D5AF... | 823AB78A72894FADD99... | 93DECF82026E326B7F9C... | 391A6C3F9E16B3AA2058... |
| file-ratio (99.02 %)        | 61.76 %                 | 25.00 %                | 3.43 %                  | 8.82 %                  |
| virtual-size (105907 bytes) | 64287 bytes             | 25624 bytes            | 7140 bytes              | 8856 bytes              |
| virtual-address             | 0x00001000              | 0x00011000             | 0x00018000              | 0x0001A000              |
| raw-size (103424 bytes)     | 64512 bytes             | 26112 bytes            | 3584 bytes              | 9216 bytes              |
| raw-address                 | 0x00000400              | 0x00010000             | 0x00016600              | 0x00017400              |
| cave (1073 bytes)           | 225 bytes               | 488 bytes              | 0 bytes                 | 360 bytes               |
| entropy                     | 6.569                   | 4.587                  | 2.883                   | 4.572                   |
| entry-point (0x0000AB74)    | x                       | -                      | -                       | -                       |
| blacklisted                 | -                       | -                      | -                       | -                       |
| writable                    | -                       | -                      | x                       | -                       |
| executable                  | x                       | -                      | -                       | -                       |
| shareable                   | -                       | -                      | -                       | -                       |
| discardable                 | -                       | -                      | -                       | x                       |
| cachable                    | x                       | x                      | x                       | x                       |
| pageable                    | x                       | x                      | x                       | x                       |
| initialized-data            | -                       | x                      | x                       | x                       |
| uninitialized-data          | -                       | -                      | -                       | -                       |
| readable                    | x                       | x                      | x                       | x                       |

#### Compile Time (pescanner, PEView):

The compile time is Sat Aug 21 10:36:59 in the year 2010

|                |                          |
|----------------|--------------------------|
| subsystem      | GUI                      |
| compiler-stamp | Sat Aug 21 10:36:59 2010 |
| debugger-stamp | n/a                      |

#### File Properties (PEStudio, PeView): Description, version, file header characteristics

Version: Aug.2010

#### File header characteristics:

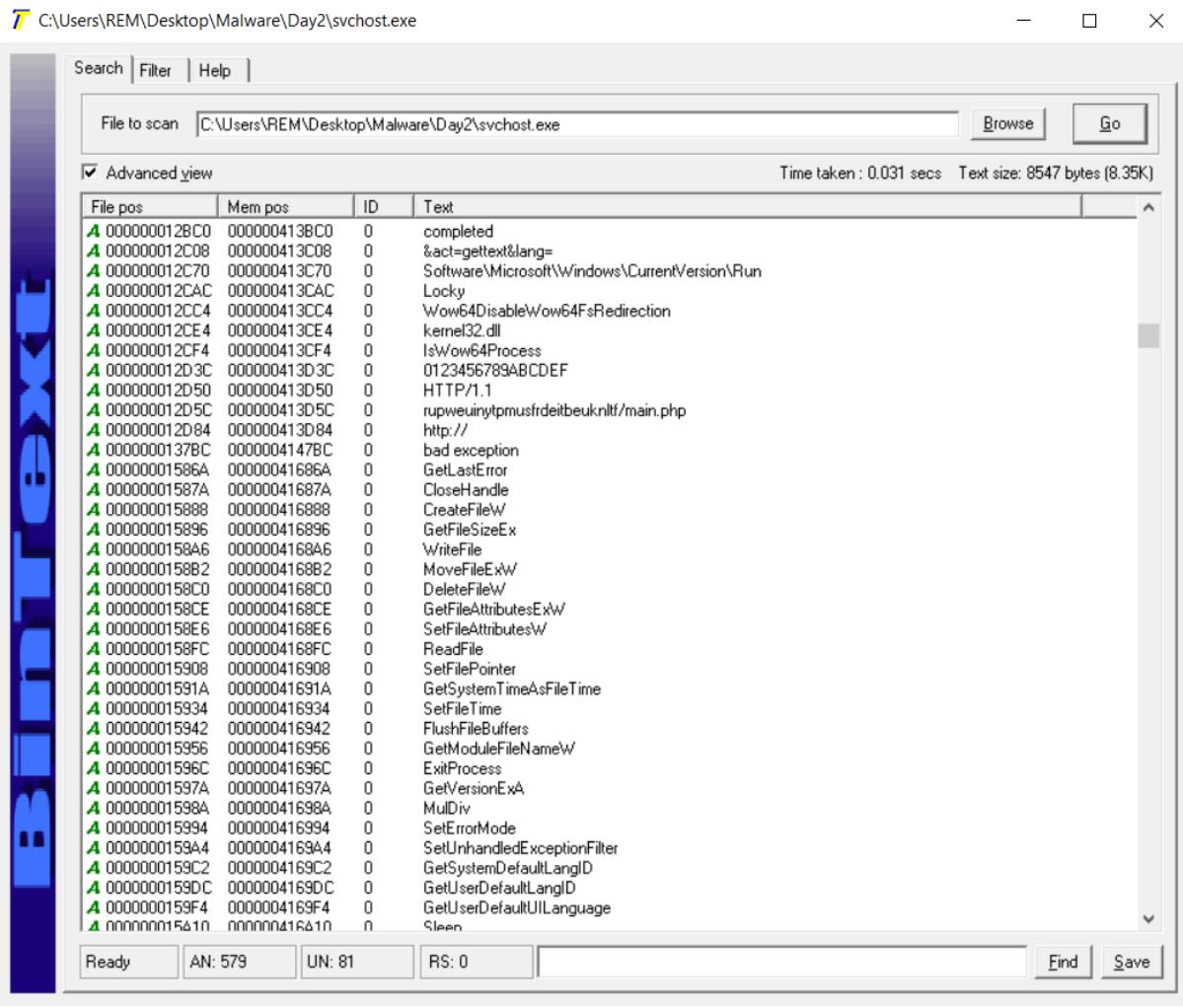
pestudio 8.74 - Malware Initial Assessment - www.winitor.com

File Help

| property  | value                                 |
|---|---------------------------------------|
| signature   | 0x00004550                            |
| machine   | Intel                                 |
| sections  | 4                                     |
| compiler-stamp                                      | 0x4C6FE48B (Sat Aug 21 10:36:59 2010) |
| pointer-symbol-table                                | 0x00000000                            |
| number-of-symbols                                   | 0                                     |
| size-of-optimal-header                              | 224 bytes                             |
| processor-32bit                                     | true                                  |
| relocation-stripped                                 | false                                 |
| large-address-aware                                 | true                                  |
| uniprocessor-only                                   | false                                 |
| system-image  | false                                 |
| dynamic-link-library                                | false                                 |
| executable  | true                                  |
| debug information stripped                          | false                                 |
| if on a removable media, copy and run from the swap | false                                 |
| if on a Network, copy and run from the swap         | false                                 |

#### Strings (strings, strings2, BinText): Functions, domains, IP addresses, commands, error msgs

- We can see some functions:



| File pos     | Mem pos      | ID | Text  |
|--------------|--------------|----|---|
| 000000012BC0 | 000000413BC0 | 0  | completed                                     |
| 000000012C08 | 000000413C08 | 0  | &act= gettext&lang=                           |
| 000000012C70 | 000000413C70 | 0  | Software\Microsoft\Windows\CurrentVersion\Run |
| 000000012CAC | 000000413CAC | 0  | Locky   |
| 000000012CC4 | 000000413CC4 | 0  | Wow64DisableWow64FsRedirection                |
| 000000012CE4 | 000000413CE4 | 0  | kernel32.dll                                  |
| 000000012CF4 | 000000413CF4 | 0  | IsWow64Process                                |
| 000000012D3C | 000000413D3C | 0  | 0123456789ABCDEF                              |
| 000000012D50 | 000000413D50 | 0  | HTTP/1.1                                      |
| 000000012D5C | 000000413D5C | 0  | rupweuinylpmusfrdeitbeuknlf/main.php          |
| 000000012D84 | 000000413D84 | 0  | http://                                       |
| 0000000137BC | 0000004147BC | 0  | bad exception                                 |
| 00000001586A | 00000041686A | 0  | GetLastError                                  |
| 00000001587A | 00000041687A | 0  | CloseHandle                                   |
| 000000015888 | 000000416888 | 0  | CreateFileW                                   |
| 000000015896 | 000000416896 | 0  | GetFileSizeEx                                 |
| 0000000158A6 | 0000004168A6 | 0  | WriteFile                                     |
| 0000000158B2 | 0000004168B2 | 0  | MoveFileExW                                   |
| 0000000158C0 | 0000004168C0 | 0  | DeleteFileW                                   |
| 0000000158CE | 0000004168CE | 0  | GetFileAttributesExW                          |
| 0000000158E6 | 0000004168E6 | 0  | SetFileAttributesW                            |
| 0000000158FC | 0000004168FC | 0  | ReadFile                                      |
| 000000015908 | 000000416908 | 0  | SetFilePointer                                |
| 00000001591A | 00000041691A | 0  | GetSystemTimeAsFileTime                       |
| 000000015934 | 000000416934 | 0  | SetFileTime                                   |
| 000000015942 | 000000416942 | 0  | FlushFileBuffers                              |
| 000000015956 | 000000416956 | 0  | GetModuleFileNameW                            |
| 00000001596C | 00000041696C | 0  | ExitProcess                                   |
| 00000001597A | 00000041697A | 0  | GetVersionExA                                 |
| 00000001598A | 00000041698A | 0  | MulDiv  |
| 000000015994 | 000000416994 | 0  | SetErrorMode                                  |
| 0000000159A4 | 0000004169A4 | 0  | SetUnhandledExceptionFilter                   |
| 0000000159C2 | 0000004169C2 | 0  | GetSystemDefaultLangID                        |
| 0000000159DC | 0000004169DC | 0  | GetUserDefaultLangID                          |
| 0000000159F4 | 0000004169F4 | 0  | GetUserDefaultUILanguage                      |
| nnnnnnn1541n | nnnnnn41641n | n  | Sleep   |

 C:\Users\REM\Desktop\Malware\Day2\svchost.exe

Search | Filter | Help |

File to scan: C:\Users\REM\Desktop\Malware\Day2\svchost.exe | Browse | Go |

Advanced view | Time taken : 0.031 secs | Text size: 8547 bytes (8.35K)

| File pos     | Mem pos      | ID | Text                              |
|--------------|--------------|----|-----------------------------------|
| 0000000159DC | 0000004169DC | 0  | GetUserDefaultLangID              |
| 0000000159F4 | 0000004169F4 | 0  | GetUserDefaultUILanguage          |
| 000000015A10 | 000000416A10 | 0  | Sleep                             |
| 000000015A18 | 000000416A18 | 0  | GetTempPathW                      |
| 000000015A28 | 000000416A28 | 0  | CopyFileW                         |
| 000000015A34 | 000000416A34 | 0  | CreateThread                      |
| 000000015A44 | 000000416A44 | 0  | WaitForSingleObject               |
| 000000015A5A | 000000416A5A | 0  | WideCharToMultiByte               |
| 000000015A70 | 000000416A70 | 0  | MultiByteToWideChar               |
| 000000015A86 | 000000416A86 | 0  | FindFirstFileW                    |
| 000000015A98 | 000000416A98 | 0  | FindClose                         |
| 000000015AA4 | 000000416AA4 | 0  | GetLocaleInfoA                    |
| 000000015AB6 | 000000416AB6 | 0  | GetWindowsDirectoryA              |
| 000000015ACE | 000000416ACE | 0  | GetVolumeNameForVolumeMountPointA |
| 000000015AF2 | 000000416AF2 | 0  | GetCurrentProcess                 |
| 000000015B06 | 000000416B06 | 0  | GetProcAddress                    |
| 000000015B18 | 000000416B18 | 0  | GetModuleHandleA                  |
| 000000015B2C | 000000416B2C | 0  | CreateProcessW                    |
| 000000015B3E | 000000416B3E | 0  | GetTempFileNameW                  |
| 000000015B52 | 000000416B52 | 0  | GetSystemTime                     |
| 000000015B62 | 000000416B62 | 0  | InitializeCriticalSection         |
| 000000015B7E | 000000416B7E | 0  | DeleteCriticalSection             |
| 000000015B96 | 000000416B96 | 0  | EnterCriticalSection              |
| 000000015BAE | 000000416BAE | 0  | LeaveCriticalSection              |
| 000000015BC6 | 000000416BC6 | 0  | GetCurrentThread                  |
| 000000015BD4 | 000000416BD4 | 0  | FindNextFileW                     |
| 000000015BEA | 000000416BEA | 0  | GetDiskFreeSpaceExW               |
| 000000015C00 | 000000416C00 | 0  | GetVolumeInformationW             |
| 000000015C18 | 000000416C18 | 0  | GetLogicalDrives                  |
| 000000015C2C | 000000416C2C | 0  | GetDriveTypeW                     |
| 000000015C3A | 000000416C3A | 0  | KERNEL32.dll                      |
| 000000015C4A | 000000416C4A | 0  | GetSystemMetrics                  |
| 000000015C5E | 000000416C5E | 0  | GetDC                             |
| 000000015C66 | 000000416C66 | 0  | ReleaseDC                         |
| 000000015C72 | 000000416C72 | 0  | DrawTextW                         |
| 000000015C7F | 000000416C7F | 0  | FillRect                          |

Ready | AN: 579 | UN: 81 | RS: 0 | Find | Save |

T C:\Users\REM\Desktop\Malware\Day2\svchost.exe

Search | Filter | Help |

File to scan C:\Users\REM\Desktop\Malware\Day2\svchost.exe

Advanced view Time taken : 0.031 secs Text size: 8547 bytes (8.35K)

| File pos        | Mem pos      | ID | Text                   |
|-----------------|--------------|----|------------------------|
| A 000000015C66  | 000000416C66 | 0  | ReleaseDC              |
| A 000000015C72  | 000000416C72 | 0  | DrawTextW              |
| A 000000015C7E  | 000000416C7E | 0  | FillRect               |
| A 000000015C8A  | 000000416C8A | 0  | FrameRect              |
| A 000000015C96  | 000000416C96 | 0  | SystemParametersInfoW  |
| A 000000015CAC  | 000000416CAC | 0  | USER32.dll             |
| A 000000015CBA  | 000000416CBA | 0  | DeleteDC               |
| A 000000015CC6  | 000000416CC6 | 0  | CreateCompatibleDC     |
| A 000000015CDC  | 000000416CDC | 0  | GetDeviceCaps          |
| A 000000015CEC  | 000000416CEC | 0  | DeleteObject           |
| A 000000015CF0  | 000000416CF0 | 0  | CreateFontA            |
| A 000000015D0A  | 000000416D0A | 0  | SelectObject           |
| A 000000015D1A  | 000000416D1A | 0  | CreateCompatibleBitmap |
| A 000000015D34  | 000000416D34 | 0  | CreateSolidBrush       |
| A 000000015D48  | 000000416D48 | 0  | SetTextColor           |
| A 000000015D58  | 000000416D58 | 0  | SetBkMode              |
| A 000000015D64  | 000000416D64 | 0  | GetObjectA             |
| A 000000015D72  | 000000416D72 | 0  | GetDIBits              |
| A 000000015D7C  | 000000416D7C | 0  | GDI32.dll              |
| A 000000015D88  | 000000416D88 | 0  | CryptDestroyKey        |
| A 000000015D9A  | 000000416D9A | 0  | CryptImportKey         |
| A 000000015DAC  | 000000416DAC | 0  | CryptSetKeyParam       |
| A 000000015DC0  | 000000416DC0 | 0  | CryptEncrypt           |
| A 000000015DD0  | 000000416DD0 | 0  | CryptReleaseContext    |
| A 000000015DE6  | 000000416DE6 | 0  | CryptGenRandom         |
| A 000000015DF8  | 000000416DF8 | 0  | CryptAcquireContextA   |
| A 000000015E10  | 000000416E10 | 0  | RegOpenKeyExA          |
| A 000000015E20  | 000000416E20 | 0  | RegCloseKey            |
| A 000000015E2E  | 000000416E2E | 0  | RegCreateKeyExA        |
| A 000000015E40  | 000000416E40 | 0  | RegSetValueExA         |
| A 000000015E52  | 000000416E52 | 0  | RegDeleteValueA        |
| A 000000015E64  | 000000416E64 | 0  | RegQueryValueExA       |
| A 000000015E78  | 000000416E78 | 0  | RegSetValueExW         |
| A 000000015E8A  | 000000416E8A | 0  | CryptGetHashParam      |
| A 000000015E9E  | 000000416E9E | 0  | CryptCreateHash        |
| A nnnnnnnn15FR0 | nnnnnn416FR0 | n  | CryptDestroyHash       |

Ready AN: 579 UN: 81 RS: 0

C:\Users\REM\Desktop\Malware\Day2\svchost.exe

Search | Filter | Help |

File to scan: C:\Users\REM\Desktop\Malware\Day2\svchost.exe | Browse | Go |

Advanced view | Time taken: 0.031 secs | Text size: 8547 bytes (8.35K)

| File pos        | Mem pos      | ID | Text                              |
|-----------------|--------------|----|-----------------------------------|
| A 0000000015EC4 | 000000416EC4 | 0  | OpenProcessToken                  |
| A 0000000015ED8 | 000000416ED8 | 0  | SetTokenInformation               |
| A 0000000015EEE | 000000416EEE | 0  | CryptHashData                     |
| A 0000000015EFE | 000000416EFE | 0  | GetFileSecurityW                  |
| A 0000000015F12 | 000000416F12 | 0  | OpenThreadToken                   |
| A 0000000015F24 | 000000416F24 | 0  | DuplicateToken                    |
| A 0000000015F36 | 000000416F36 | 0  | MapGenericMask                    |
| A 0000000015F48 | 000000416F48 | 0  | AccessCheck                       |
| A 0000000015F54 | 000000416F54 | 0  | ADVAPI32.dll                      |
| A 0000000015F64 | 000000416F64 | 0  | SHGetFolderPathW                  |
| A 0000000015F78 | 000000416F78 | 0  | ShellExecuteW                     |
| A 0000000015F86 | 000000416F86 | 0  | SHELL32.dll                       |
| A 0000000015F94 | 000000416F94 | 0  | InternetCloseHandle               |
| A 0000000015FAA | 000000416FAA | 0  | InternetCrackUrlA                 |
| A 0000000015FB8 | 000000416FB8 | 0  | InternetOpenA                     |
| A 0000000015FCE | 000000416FCE | 0  | InternetSetOptionA                |
| A 0000000015FE4 | 000000416FE4 | 0  | InternetConnectA                  |
| A 0000000015FF8 | 000000416FF8 | 0  | HttpOpenRequestA                  |
| A 000000001600C | 00000041700C | 0  | InternetQueryOptionA              |
| A 0000000016024 | 000000417024 | 0  | HttpSendRequestExA                |
| A 000000001603A | 00000041703A | 0  | InternetWriteFile                 |
| A 000000001604E | 00000041704E | 0  | HttpEndRequestA                   |
| A 0000000016060 | 000000417060 | 0  | HttpSendRequestA                  |
| A 0000000016074 | 000000417074 | 0  | HttpQueryInfoA                    |
| A 0000000016086 | 000000417086 | 0  | InternetReadFile                  |
| A 0000000016098 | 000000417098 | 0  | WININET.dll                       |
| A 00000000160A6 | 0000004170A6 | 0  | WNetOpenEnumW                     |
| A 00000000160B6 | 0000004170B6 | 0  | WNetEnumResourceW                 |
| A 00000000160CA | 0000004170CA | 0  | WNetAddConnection2W               |
| A 00000000160E0 | 0000004170E0 | 0  | WNetCloseEnum                     |
| A 00000000160EE | 0000004170EE | 0  | MPR.dll                           |
| A 00000000160F8 | 0000004170F8 | 0  | DsRoleGetPrimaryDomainInformation |
| A 000000001611C | 00000041711C | 0  | DsRoleFreeMemory                  |
| A 000000001612E | 00000041712E | 0  | NETAPI32.dll                      |
| A 000000001613E | 00000041713E | 0  | HeapAlloc                         |
| A nnnnnnnn1614A | nnnnnn41714A | 0  | HeapFree                          |

Ready | AN: 579 | UN: 81 | RS: 0 | Find | Save |

C:\Users\REM\Desktop\Malware\Day2\svchost.exe

Search | Filter | Help |

File to scan: C:\Users\REM\Desktop\Malware\Day2\svchost.exe | Browse | Go |

Advanced view | Time taken: 0.031 secs | Text size: 8547 bytes (8.35K)

| File pos       | Mem pos      | ID | Text                                  |
|----------------|--------------|----|---------------------------------------|
| A 000000016190 | 000000417190 | 0  | RaiseException                        |
| A 0000000161A2 | 0000004171A2 | 0  | GetStdHandle                          |
| A 0000000161B2 | 0000004171B2 | 0  | UnhandledExceptionFilter              |
| A 0000000161CE | 0000004171CE | 0  | IsDebuggerPresent                     |
| A 0000000161E2 | 0000004171E2 | 0  | TerminateProcess                      |
| A 0000000161F6 | 0000004171F6 | 0  | HeapSize                              |
| A 000000016202 | 000000417202 | 0  | HeapReAlloc                           |
| A 000000016210 | 000000417210 | 0  | IsProcessorFeaturePresent             |
| A 00000001622C | 00000041722C | 0  | GetModuleHandleW                      |
| A 000000016240 | 000000417240 | 0  | GetCPInfo                             |
| A 00000001624C | 00000041724C | 0  | InterlockedIncrement                  |
| A 000000016264 | 000000417264 | 0  | InterlockedDecrement                  |
| A 00000001627C | 00000041727C | 0  | GetACP                                |
| A 000000016286 | 000000417286 | 0  | GetOEMCP                              |
| A 000000016292 | 000000417292 | 0  | IsValidCodePage                       |
| A 0000000162A4 | 0000004172A4 | 0  | TlsAlloc                              |
| A 0000000162B0 | 0000004172B0 | 0  | TlsGetValue                           |
| A 0000000162BE | 0000004172BE | 0  | TlsSetValue                           |
| A 0000000162CC | 0000004172CC | 0  | TlsFree                               |
| A 0000000162D6 | 0000004172D6 | 0  | SetLastError                          |
| A 0000000162E6 | 0000004172E6 | 0  | GetCurrentThreadId                    |
| A 0000000162FC | 0000004172FC | 0  | HeapCreate                            |
| A 00000001630A | 00000041730A | 0  | LCMapStringW                          |
| A 00000001631A | 00000041731A | 0  | GetStringTypeW                        |
| A 00000001632C | 00000041732C | 0  | GetModuleFileNameA                    |
| A 000000016342 | 000000417342 | 0  | FreeEnvironmentStringsW               |
| A 00000001635C | 00000041735C | 0  | GetEnvironmentStringsW                |
| A 000000016376 | 000000417376 | 0  | SetHandleCount                        |
| A 000000016388 | 000000417388 | 0  | InitializeCriticalSectionAndSpinCount |
| A 0000000163B0 | 0000004173B0 | 0  | GetFileType                           |
| A 0000000163BE | 0000004173BE | 0  | QueryPerformanceCounter               |
| A 0000000163D8 | 0000004173D8 | 0  | GetTickCount                          |
| A 0000000163E8 | 0000004173E8 | 0  | GetCurrentProcessId                   |
| A 0000000163FE | 0000004173FE | 0  | RtlUnwind                             |
| A 00000001640A | 00000041740A | 0  | LoadLibraryW                          |
| A 000000016610 | 000000418010 | 0  | ?AvengelIronman@0                     |

Ready | AN: 579 | UN: 81 | RS: 0 | Find | Save |

- Some messages:

File to scan: C:\Users\REM\Desktop\Malware\Day2\svchost.exe

Time taken: 0.031 secs Text size: 8547 bytes (8.35K)

| File pos       | Mem pos      | ID | Text                          |
|----------------|--------------|----|-------------------------------|
| A 0000000178A9 | 00000041A7A9 | 0  | >'p>                          |
| A 0000000178CF | 00000041A7CF | 0  | 0%+04090H0e0                  |
| A 0000000178E1 | 00000041A7E1 | 0  | 01X1                          |
| A 000000017BED | 00000041A7ED | 0  | 2]3w3                         |
| A 000000017C01 | 00000041A801 | 0  | 4%4+444@4F4N4T4               |
| A 000000017C11 | 00000041A811 | 0  | 4f4s4)4                       |
| A 000000017C21 | 00000041A821 | 0  | 4*50525                       |
| A 000000017C29 | 00000041A829 | 0  | 5f5f5                         |
| A 000000017C31 | 00000041A831 | 0  | 546W6a6                       |
| A 000000017C47 | 00000041A847 | 0  | 7.7&7-737;7B7G707<7d7?n?7x?~7 |
| A 000000017C87 | 00000041A887 | 0  | 8*808H8                       |
| A 000000017C91 | 00000041A891 | 0  | 9L9x9                         |
| A 000000017C9B | 00000041A89B | 0  | 9!V_<                         |
| A 000000017CA9 | 00000041A8A9 | 0  | :4<?<Z<e<%>6>>>D>>>0>         |
| A 000000017CC7 | 00000041A8C7 | 0  | ?Q?)?w?                       |
| A 000000017CDF | 00000041A8DF | 0  | 0.0u0                         |
| A 000000017CED | 00000041A8ED | 0  | 141F1t1                       |
| A 000000017D01 | 00000041A901 | 0  | 2%222>2F2N2Z2                 |
| A 000000017D23 | 00000041A923 | 0  | 3.3@3F303b3                   |
| A 000000017D33 | 00000041A933 | 0  | 4:4e4q4l5                     |
| A 000000017D4B | 00000041A94B | 0  | 6N656                         |
| A 000000017D5F | 00000041A95F | 0  | 7'7 7                         |
| A 000000017D75 | 00000041A975 | 0  | 8'8@82888B8K8V8[8d8n8y8       |
| A 000000017D99 | 00000041A999 | 0  | :C,B<H<R<                     |
| A 000000017DA7 | 00000041A9A7 | 0  | <!=5=                         |
| A 000000017DE3 | 00000041A9E3 | 0  | 1=2(6.L6                      |
| A 000000017DFF | 00000041A9FF | 0  | 7&787J7<7n7                   |
| A 000000017E08 | 00000041AA08 | 0  | 7,8D8K8S8<8V8                 |
| A 000000017E2F | 00000041AA2F | 0  | 8.9@9D9H9L9                   |
| A 000000017E49 | 00000041AA49 | 0  | :7:ip:tx:                     |
| A 000000017E71 | 00000041AA71 | 0  | ={S=Y=_=e=k=q=x=              |
| A 000000017EA9 | 00000041AAA9 | 0  | >\$>?@>G>?P                   |
| A 000000017ECD | 00000041ACD  | 0  | 3R4s5g6                       |
| A 000000017E0B | 00000041AADB | 0  | <=4=?=V?                      |
| A 000000017EF5 | 00000041AAF5 | 0  | 101:1011v1                    |
| A 000000017F25 | 00000041AB25 | 0  | 3:RM3                         |

- Some IP addresses:

|                |              |   |   |
|----------------|--------------|---|---|
| A 000000012128 | 000000413128 | 0 | !"#\$%&'()*+,-./0123456789;:<=>?@ABCDEFGHIJKLMNPQRSTUVWXYZ[\n]                            |
| A 000000012169 | 000000413169 | 0 | ABCDEFHJKLMNOPQRSTUVWXYZ()  |
| A 0000000127EF | 0000004137EF | 0 | 91.195.12.187.195.64.154.114.149.202.109.205.51.254.181.122.78.40.108.39.188.127.231.116. |
| A 0000000128B4 | 0000004138B4 | 0 | bad allocation  |
| A 000000012904 | 000000413904 | 0 | vector<T> too long  |
| A 000000012918 | 000000413918 | 0 | string too long   |
| A 000000012928 | 000000413928 | 0 | invalid string position   |

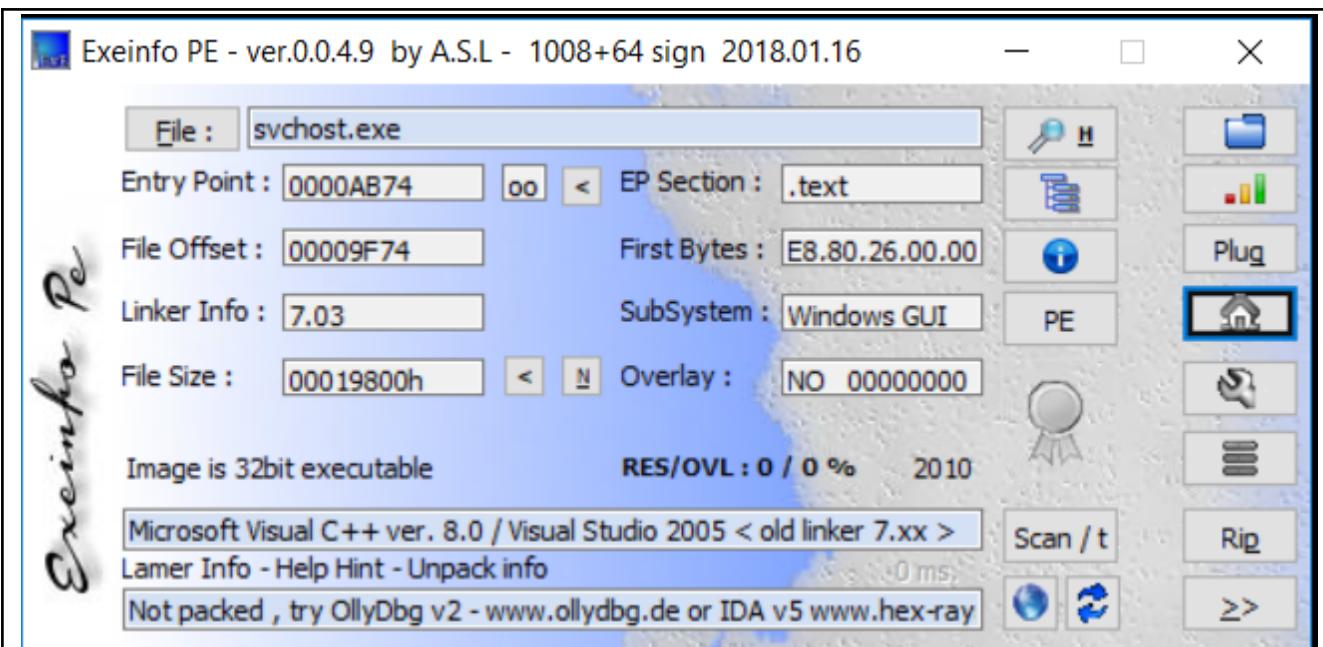
- We can see a list of IP addresses here:

- + 91.195.12.187
- + 195.64.154.114
- + 149.202.109.205
- + 51.254.181.122
- + 78.40.108.39
- + 188.127.231.116

### Packed (pscanner, PEiD, ExeInfo):

Not Packed

Testing using "ExeInfo"



### Entropy (ByteHist, pescanner): File, sections

pestudio 8.74 - Malware Initial Assessment - www.winitor.com

File Help

| property                    | value                   | value                  | value                   | value                   |
|-----------------------------|-------------------------|------------------------|-------------------------|-------------------------|
| name                        | .text                   | .rdata                 | .data                   | .reloc                  |
| md5                         | 7C04B5773D76E399D5AF... | 823AB78A72894FADD99... | 93DECF82026E326B7F9C... | 391A6C3F9E16B3AA2058... |
| file-ratio (99.02 %)        | 61.76 %                 | 25.00 %                | 3.43 %                  | 8.82 %                  |
| virtual-size (105907 bytes) | 64287 bytes             | 25624 bytes            | 7140 bytes              | 8856 bytes              |
| virtual-address             | 0x00001000              | 0x00011000             | 0x00018000              | 0x0001A000              |
| raw-size (103424 bytes)     | 64512 bytes             | 26112 bytes            | 3584 bytes              | 9216 bytes              |
| raw-address                 | 0x00000400              | 0x00010000             | 0x00016600              | 0x00017400              |
| cave (1073 bytes)           | 225 bytes               | 488 bytes              | 0 bytes                 | 360 bytes               |
| entropy                     | 6.569                   | 4.587                  | 2.883                   | 4.572                   |
| entry-point (0x0000AB74)    | x                       | -                      | -                       | -                       |
| blacklisted                 | -                       | -                      | -                       | -                       |
| writable                    | -                       | -                      | x                       | -                       |
| executable                  | x                       | -                      | -                       | -                       |
| shareable                   | -                       | -                      | -                       | -                       |
| discardable                 | -                       | -                      | -                       | x                       |
| cachable                    | x                       | x                      | x                       | x                       |
| pageable                    | x                       | x                      | x                       | x                       |
| initialized-data            | -                       | x                      | x                       | x                       |
| uninitialized-data          | -                       | -                      | -                       | -                       |
| readable                    | x                       | x                      | x                       | x                       |

In Sections, we can see the entropy of each section:

- + .text: 6569
- + .rdata: 4587
- + .data: 2883
- + .reloc: 4572

### Imported/Exported Functions (PEStudio, Dependency Walker):

Imported functions: wininet.dll, mpr.dll, netapi32.dll, kernel32.dll, user32.dll, gdi32.dll, advapi32.dll, shell32.dll

pestudio 8.74 - Malware Initial Assessment - www.winitor.com

File Help

| library (8)  | blacklist (3) | missing (0) | type (1) | imports (156) | file-description                       |
|--------------|---------------|-------------|----------|---------------|--|
| wininet.dll  | x             | -           | implicit | 13            | Internet Extensions for Win32          |
| mpr.dll      | x             | -           | implicit | 4             | Multiple Provider Router DLL           |
| netapi32.dll | x             | -           | implicit | 2             | Net Win32 API DLL                      |
| kernel32.dll | -             | -           | implicit | 91            | Windows NT BASE API Client DLL         |
| user32.dll   | -             | -           | implicit | 7             | Multi-User Windows USER API Client DLL |
| gdi32.dll    | -             | -           | implicit | 12            | GDI Client DLL                         |
| advapi32.dll | -             | -           | implicit | 25            | Advanced Windows 32 Base API           |
| shell32.dll  | -             | -           | implicit | 2             | Windows Shell Common DLL               |

c:\users\rem\Desktop\malwar  
 indicators (2/14)  
 virusTotal (n/a)  
 dos-stub (This program c  
 file-header (Aug.2010)  
 optional-header (GUI)  
 directories (3)  
 sections (99.02%)  
 libraries (3/8)  
 imports (156/20/0/1/67)  
 exports (0)  
 tls-callbacks (n/a)

## Open Source Research (VirusTotal, search engines, malware repositories):

Searching on VirusTotal, the “svchost.exe” is flagged as a malicious file with the score 65/72

The screenshot shows the VirusTotal analysis interface for the file 28046c14ea3325885ee1e731cd0bcf9f38445df02675836b851cb2ae94c050eb. The main summary indicates a score of 65/72, with 65 security vendors flagged it as malicious and no sandboxes flagged it as malicious. The file is a 102.00 KB EXE file from 2022-09-26 22:28:29 UTC, 28 days ago. Below the summary, there are tabs for DETECTION (selected), DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (4).

## File System Artifacts (Regshot, CaptureBAT, Process Monitor, Cuckoo):

**Triggers:** Browser, mail client, specific web pages (google, bank), time, reboot, user/admin privs

**Dependencies:** DNS, HTTP, IRC, ARP

- Regshot:

- On my machine, after comparing 2 shots, I got the result like this. "Svchost.exe" and other processes did a lot of changes ( maybe because I let it run for a longtime)

```

svhost.txt
1 Regshot 1.9.0 x64 ANSI
2 Comments:
3 Date/time: 2022/10/30 08:12:10 , 2022/10/30 08:16:42
4 Computer: DESKTOP-2C3IQHO , DESKTOP-2C3IQHO
5 Username: REM , REM
6
7 -----
8 Keys deleted: 38468
9 -----
10 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\{AppXwv0gcxhfzclwz3q5j596bfk9ths12een
11 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\Windows.protocol\pandora\{AppXwv0gcxhfzclwz3q5j596bfk9ths12een
12 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe
13 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe
14 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Microsoft.MSPaint
15 HKLM\SOFTWARE\Classes\Local

```

- Added 610 keys:

```

svhost.txt
38481 Keys added: 610
38482 -----
38483 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\ProgIDs\{AppXzjrn2jd058qcnbegk55rzemp770dxzn
38484 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Extensions\Windows.protocol\pandora\{AppXzjrn2jd058qcnbegk55rzemp770dxzn
38485 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe
38486 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.2203.1037.0_neutral_~_8wekyb3d8bbwe
38487 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.2203.1037.0_x64_8wekyb3d8bbwe
38488 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_4.2203.1037.0_x64_8wekyb3d8bbwe\Microsoft.MSPaint
38489 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_6.2203.1037.0_x64_8wekyb3d8bbwe\Microsoft.MSPaint
38490 HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\PackageRepository\Packages\Microsoft.MSPaint_6.2203.1037.0_x64_8wekyb3d8bbwe\Microsoft.MSPaint\Windows.fileTypeAssociation
38491 HKLM\SOFTWARE\Classes\Local

```

- Added 407 folders:

```

svhost.txt
184964 Folders added: 407
184965 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe\aa80b651-bccc-4d1c-b49e-0073f4790fdf
184966 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe\aa80b651-bccc-4d1c-b49e-0073f4790fdf\AppxMetadata
184967 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe\aa80b651-bccc-4d1c-b49e-0073f4790fdf\microsoft.system.package.metadata
184968 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa195ebfd-13cc-40fa-b6a7-adb235ad65
184969 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa195ebfd-13cc-40fa-b6a7-adb235ad65\appxMetadata
184970 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\appxMetadata
184971 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets
184972 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Assets
184973 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Fonts
184974 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Images
184975 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Images\HelpAndFeedback
184976 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\SmartSelect
184977 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Stickers
184978 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Images\Stickers\Thumbnails
184979 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Logos
184980 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\contrast-high
184981 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Logos\contrast-standard
184982 C:\Program Files\WindowsApps\Deleted\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\aa95ebfd-43cc-4f5a-b6a7-a5b933a03e54\Assets\Logos\contrast-white

```

- Deleted 119 folders:

```

svhost.txt
185375 Folders deleted: 119
185376 -----
185377 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe
185378 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe\AppxMetadata
185379 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_neutral_~_8wekyb3d8bbwe\microsoft.system.package.metadata
185380 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe
185381 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\AppxMetadata
185382 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets
185383 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Assets\Assets
185384 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Fonts
185385 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Images
185386 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Images\HelpAndFeedback
185387 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Images\SmartSelect
185388 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Images\Stickers
185389 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Images\Stickers\Thumbnails
185390 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Logs
185391 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Logs\contrast-high
185392 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Logs\contrast-standard
185393 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Logs\contrast-white
185394 C:\Program Files\WindowsApps\Microsoft.MSPaint_4.1804.13047.0_x64_8wekyb3d8bbwe\Assets\Logs\FileAssociation

```

- Total changes 154876:

```

svhost.txt
185481 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.NET.Native.Framework.1.6.1.6.24903.0_x86_8wekyb3d8bbwe
185482 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.Services.Store.Engagement_10.0.1610.0_x64_8wekyb3d8bbwe
185483 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.Services.Store.Engagement_10.0.1610.0_x86_8wekyb3d8bbwe
185484 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.VCLibs.140.0_14.0.24605.0_x64_8wekyb3d8bbwe
185485 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.VCLibs.140.0_14.0.24605.0_x86_8wekyb3d8bbwe
185486 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.VCLibs.140.0_14.0.25426.0_x64_8wekyb3d8bbwe
185487 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.VCLibs.140.0_14.0.25426.0_x86_8wekyb3d8bbwe
185488 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.XboxGameOverlay_1.24.5001.0_neutral_split.scale-100_8wekyb3d8bbwe
185489 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\Microsoft.XboxGameOverlay_1.24.5001.0_neutral_~_8wekyb3d8bbwe
185490 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\PandoraMediaInc.29680B314EFC2_13.0.39.0_neutral_split.scale-100_n619g4d5j0fnw
185491 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\PandoraMediaInc.29680B314EFC2_13.0.39.0_neutral_~_n619g4d5j0fnw
185492 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\PandoraMediaInc.29680B314EFC2_13.0.39.0_neutral_~_n619g4d5j0fnw
185493 C:\Users\All Users\Microsoft.Windows.AppRepository\Packages\PandoraMediaInc.29680B314EFC2_13.0.39.0_x64_n619g4d5j0fnw
185494 C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\{3ac98fze-d8dd-464e-84e5-ac09fa8e458a}
185495 C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\{5b2b3d12-e945-4eaa-9874-db47189b5fdb}
185496 -----
185497 -----
185498 Total changes: 154876
185499 -----

```

- Looking at the processes by using “Process Monitor”:

- Some registry actions:

|                         |  |                |                  |      |
|-------------------------|--|----------------|------------------|------|
| 4.33.1 svchost.exe 1748 | RegCreateKey HKCU\Software\Locky       | SUCCESS        | Desired Acces... | 5360 |
| 4.33.1 svchost.exe 1748 | RegSetInfoK_ HKCU\Software\Locky       | SUCCESS        | KeySetFormat...  | 5360 |
| 4.33.1 svchost.exe 1748 | RegQueryV_ HKCU\Software\Locky\id      | NAME NOT FOUND | Length: 144      | 5360 |
| 4.33.1 svchost.exe 1748 | RegQueryV_ HKCU\Software\Locky\pubkey  | NAME NOT FOUND | Length: 144      | 5360 |
| 4.33.1 svchost.exe 1748 | RegQueryV_ HKCU\Software\Locky\paytext | NAME NOT FOUND | Length: 144      | 5360 |

→ A new registry key named “Locky”

|                         |   |         |                  |      |
|-------------------------|---|---------|------------------|------|
| 4.33.1 svchost.exe 1076 | RegQueryV_ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings | SUCCESS | Type: REG_BI...  | 4144 |
| 4.33.1 svchost.exe 1076 | RegQueryV_ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings | SUCCESS | Type: REG_BI...  | 4144 |
| 4.33.1 svchost.exe 1076 | RegCloseKeyHKCU   | SUCCESS |                  | 4144 |
| 4.33.1 svchost.exe 1076 | RegCloseKeyHKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections                     | SUCCESS |                  | 4144 |
| 4.33.1 svchost.exe 1076 | RegOpenKeyHKLM  | SUCCESS | Desired Acces... | 4144 |
| 4.33.1 svchost.exe 1076 | RegOpenKey HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings                        | SUCCESS | Query Handle...  | 4144 |
| 4.33.1 svchost.exe 1076 | RegOpenKey HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings                        | SUCCESS | Desired Acces... | 4144 |

→ Registry key named “SavedLegacySettings”, type: REG\_BINARY

|                         |   |                |                |      |
|-------------------------|---|----------------|----------------|------|
| 4.33.1 svchost.exe 1748 | RegQueryV_ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable   | SUCCESS        | Type: REG_D... | 5384 |
| 4.33.1 svchost.exe 1076 | RegQueryV_ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer   | NAME NOT FOUND | Length: 144    | 5384 |
| 4.33.1 svchost.exe 1076 | RegQueryV_ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride | NAME NOT FOUND | Length: 144    | 5384 |
| 4.33.1 svchost.exe 1076 | RegQueryV_ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL | NAME NOT FOUND | Length: 144    | 5384 |
| 4.33.1 svchost.exe 1076 | RegQueryV_ HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect    | NAME NOT FOUND | Length: 144    | 5384 |
| 4.33.1 svchost.exe 1076 | RegCloseKeyHKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings               | SUCCESS        |                | 5384 |

→ Registry key named “ProxyEnable”, type: REG\_DWORD

Network Artifacts (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark): C2 domains/IP addresses, protocols, user-agent

Using Wireshark:

|              |                        |                   |      |   |
|--------------|------------------------|-------------------|------|---|
| 63 8. 538284 | 192.168.146.138        | 195.64.154.114    | TCP  | 66 [TCP Retransmission] 49840 → 80 [SYN] Seq=0 Win=655... |
| 64 8. 593134 | fe80::25de:8978:765... | ff02::c           | UDP  | 686 64629 → 3702 Len=624                                  |
| 65 9. 000413 | 00:50:56:c0:00:08      | ff:ff:ff:ff:ff:ff | ARP  | 60 Who has 192.168.146.2? Tell 192.168.146.1              |
| 66 9. 757497 | 192.168.146.138        | 239.255.255.250   | UDP  | 666 64628 → 3702 Len=624                                  |
| 67 9. 823020 | fe80::25de:8978:765... | ff02::c           | SSDP | 157 M-SEARCH * HTTP/1.1                                   |
| 68 9. 823606 | 192.168.146.138        | 239.255.255.250   | SSDP | 143 M-SEARCH * HTTP/1.1                                   |

Frame 63: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 ↓ Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be  
 ↓ Internet Protocol Version 4, Src: 192.168.146.138, Dst: 195.64.154.114  
 ↓ Transmission Control Protocol, Src Port: 49840 (49840), Dst Port: 80 (80), Seq: 0, Len: 0

→ IP address 195.64.154.114, TCP protocol, Src port 49840, Dst port 80.

|                |                 |                 |     |   |
|----------------|-----------------|-----------------|-----|---|
| 95 31. 502492  | 192.168.146.138 | 188.127.231.116 | TCP | 66 49845 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=... |
| 96 33. 010703  | 149.202.109.205 | 192.168.146.138 | TCP | 60 80 → 49843 [RST, ACK] Seq=3049457159 Ack=1 Win=6424... |
| 97 33. 525702  | 192.168.146.138 | 149.202.109.205 | TCP | 66 [TCP Spurious Retransmission] 49843 → 80 [SYN] Seq=... |
| 98 34. 275220  | 192.168.146.138 | 192.168.26.1    | TCP | 60 49839 → 52881 [RST, ACK] Seq=626 Ack=1 Win=0 Len=0     |
| 99 34. 507979  | 192.168.146.138 | 188.127.231.116 | TCP | 66 [TCP Retransmission] 49845 → 80 [SYN] Seq=0 Win=655... |
| 100 36. 484681 | 149.202.109.205 | 192.168.146.138 | TCP | 60 80 → 49843 [RST, ACK] Seq=3709077253 Ack=1 Win=6424... |

Frame 95: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 ↓ Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be  
 ↓ Internet Protocol Version 4, Src: 192.168.146.138, Dst: 188.127.231.116  
 ↓ Transmission Control Protocol, Src Port: 49845 (49845), Dst Port: 80 (80), Seq: 0, Len: 0

→ IP address 188.127.231.116, TCP protocol, Src port 49845, Dst Port 80

→ and IP address 149.202.109.205, TCP protocol, port 49843 (Dst) and port 80 (Src)

|                |                 |                 |     |   |
|----------------|-----------------|-----------------|-----|---|
| 115 45. 906659 | 192.168.146.138 | 91.195.12.187   | TCP | 66 [TCP Retransmission] 49847 → 80 [SYN] Seq=0 Win=655... |
| 116 52. 522202 | 188.127.231.116 | 192.168.146.138 | TCP | 60 80 → 49845 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0      |
| 117 52. 525265 | 192.168.146.138 | 149.202.109.205 | TCP | 66 49848 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=... |

Frame 115: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
 ↓ Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be  
 ↓ Internet Protocol Version 4, Src: 192.168.146.138, Dst: 91.195.12.187  
 ↓ Transmission Control Protocol, Src Port: 49847 (49847), Dst Port: 80 (80), Seq: 0, Len: 0

→ I got the same with IP address 91.195.12.187

|                |                 |                 |      |  |
|----------------|-----------------|-----------------|------|--|
| 106 36. 874495 | 51.254.181.122  | 192.168.146.138 | HTTP | 520 HTTP/1.1 404 Not Found (text/html)                     |
| 107 36. 874833 | 192.168.146.138 | 51.254.181.122  | TCP  | 60 49846 → 80 [ACK] Seq=220 Ack=468 Win=65535 Len=0        |
| 108 36. 875056 | 192.168.146.138 | 51.254.181.122  | TCP  | 60 49846 → 80 [FIN, ACK] Seq=220 Ack=468 Win=65535 Len=... |
| 109 36. 875240 | 51.254.181.122  | 192.168.146.138 | TCP  | 60 80 → 49846 [ACK] Seq=468 Ack=221 Win=64239 Len=0        |

Frame 106: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits)  
 ↓ Ethernet II, Src: 00:50:56:eb:59:be, Dst: 00:0c:29:7f:f8:4f  
 ↓ Internet Protocol Version 4, Src: 51.254.181.122, Dst: 192.168.146.138  
 ↓ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49846 (49846), Seq: 1, Ack: 220, Len: 466  
 ↓ Hypertext Transfer Protocol

→ IP address 51.254.181.122, HTTP protocol and TCP protocol, port 80 (Src), port 49846 (Dst).

We have an exciting file named “main.php”. Using follow TCP stream, I got this:

```

POST /main.php HTTP/1.1
Host: 51.254.181.122
Content-Length: 100
Connection: Keep-Alive
Cache-Control: no-cache

.T...4Kh.....r^..._.K.D.....}....L..MS...-G.x..G...{.e....+.ct.OJd.p.cd'.em.
3....Vbwz.9.LS.oa.pHTTP/1.1 404 Not Found
Date: Tue, 25 Oct 2022 10:41:43 GMT
Server: Apache/2.2.15 (CentOS)
Content-Length: 286
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /main.php was not found on this server.</p>
<hr>
<address>Apache/2.2.15 (CentOS) Server at 51.254.181.122 Port 80</address>
</body></html>

```

|   |                |                 |              |     |  |
|---|----------------|-----------------|--------------|-----|--|
| L   | 128.64.0.98705 | 192.168.146.138 | 78.40.108.39 | TCP | 60 49849 → 80 [RST, ACK] Seq=218 Ack=1 Win=0 Len=0 |
| Frame 128: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)                                |                |                 |              |     |  |
| Ethernet II, Src: 00:0c:29:7f:f8:4f, Dst: 00:50:56:eb:59:be   |                |                 |              |     |  |
| Internet Protocol Version 4, Src: 192.168.146.138, Dst: 78.40.108.39                                |                |                 |              |     |  |
| Transmission Control Protocol, Src Port: 49849 (49849), Dst Port: 80 (80), Seq: 218, Ack: 1, Len: 0 |                |                 |              |     |  |

→ IP address 78.40.108.39, we follow TCP stream and got this

```

POST /main.php HTTP/1.1
Host: 78.40.108.39
Content-Length: 100
Connection: Keep-Alive
Cache-Control: no-cache

.T...4Kh.....r^..._.K.D.....}....L..MS...-G.x..G...{.e....+.ct.OJd.p.cd'.em.
3....Vbwz.9.LS.oa.p

```

**Memory Analysis** (Volatility, Rekall, Redline, Process Hacker): rogue processes, code injection, rootkits, network artifacts

**Open Source Research** (centralops, robtex, urlvoid, ipvoid, TrustedSource):

**Static Analysis** (IDA Pro): Strings, CALLs, program flow, loops

- Using IDA pro:
- We disassemble svchost.exe using IDA, click on Imports, we observe numerous APIs associated with registry access, such as RegOpenKeyExA

### xrefs to RegOpenKeyExA

| Direction | Type | Address              | Text                  |
|-----------|------|----------------------|-----------------------|
| Up        | r    | sub_403D8A+F5        | call ds:RegOpenKeyExA |
| Up        | p    | sub_403D8A+F5        | call ds:RegOpenKeyExA |
| Up        | r    | WinMain(x,x,x,x)+7AC | call ds:RegOpenKeyExA |
| Up        | p    | WinMain(x,x,x,x)+7AC | call ds:RegOpenKeyExA |

- We press Alt+ T to search String RegOpenKeyExA, This will take you to address 004047F0, where you will see a CALL to RegOpenKeyExA
- At address 004047E2, we can see the link “Software\Microsoft\Windows\CurrentVersion\Run”. This is the path to the Run key and also the way this malware uses to keep the persistence.

```

.text:004047CA          mov    byte ptr [ebp+var_4], 15h
.text:004047CE          mov    al, ds:byte_4137ED
.text:004047D3          test   al, al
.text:004047D5          jz    short loc_404833
.text:004047D7          lea    eax, [ebp+var_50]
.text:004047DA          push   eax           ; phkResult
.text:004047DB          push   2000000h        ; samDesired
.text:004047E0          push   0              ; ulOptions
.text:004047E2          push   offset aSoftwareMicros ; "Software\Microsoft\Windows\CurrentVe...
.text:004047E7          push   80000001h       ; hKey
.text:004047E7 ; } // starts at 4047CA
.text:004047EC ; try {
.text:004047EC          mov    byte ptr [ebp+var_4], 16h
.text:004047F0          call   ds:RegOpenKeyExA
.text:004047F6          test   eax, eax
.text:004047F8          jz    short loc_404817
.text:004047FA          mov    [ebp+var_80], eax
.text:004047FD          mov    [ebp+var_84], offset ??_7livsx@06B@ ; const livsx::`vftable'
.text:00404807          push   offset __T1?AVlivsx@0 ; throw info for 'class livsx'
.text:0040480C          lea    eax, [ebp+var_84]
.text:00404812          jmp    loc_404209
.text:00404817

```

- At address 004047E7, there is a push “80000001h; hKey”. We can search this on the internet:

# Syntax

C++

Copy

```
LSTATUS RegOpenKeyExA(
    [in]          HKEY     hKey,
    [in, optional] LPCSTR  lpSubKey,
    [in]          DWORD    ulOptions,
    [in]          REGSAM   samDesired,
    [out]         PHKEY    phkResult
);
```

## Parameters

[in] hKey

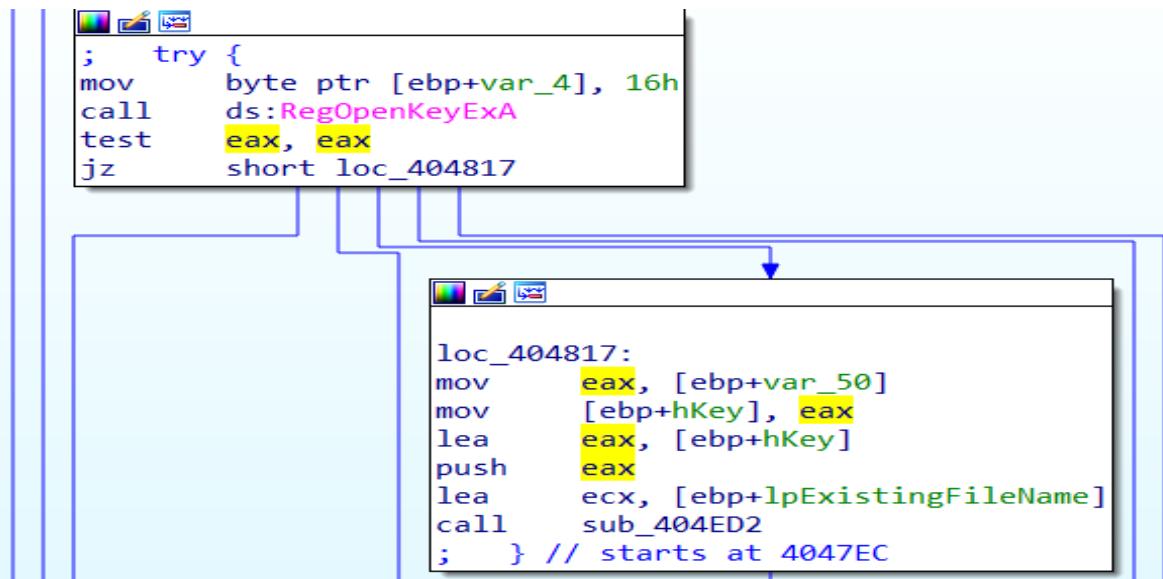
A handle to an open registry key. This handle is returned by the [RegCreateKeyEx](#) or [RegOpenKeyEx](#) function, or it can be one of the following [predefined keys](#):

[HKEY\\_CLASSES\\_ROOT](#) [HKEY\\_CURRENT\\_CONFIG](#) [HKEY\\_CURRENT\\_USER](#) [HKEY\\_LOCAL\\_MACHINE](#)  
[HKEY\\_USERS](#)

- We right-click on **80000001h** and select Use [Standard Symbolic Constant](#). We know that **RegOpenKeyExA** involves the registry. Reviewing the list of options, we see multiple references to **HKEY\_CURRENT\_USER**

|                             |                    |                    |
|-----------------------------|--------------------|--------------------|
| GDICOMMENT_WINDOWS_METAFILE | FFFFFFFFFF80000001 | MS SDK (Windows 7) |
| HKEY_CURRENT_USER           | FFFFFFFFFF80000001 | MS SDK (Windows 7) |
| KERB_WRAP_NO_ENCRYPT        | FFFFFFFFFF80000001 | MS SDK (Windows 7) |
| LINEERR_ALLOCATED           | FFFFFFFFFF80000001 | MS SDK (Windows 7) |
| MQCONN_PING_FAILURE         | FFFFFFFFFF80000001 | MS SDK (Windows 7) |

- The call to **RegOpenKeyExA** happens right before the “test” and “jz” instructions. If the test return 0 ( success ) -> jump to the address **loc\_404817**.

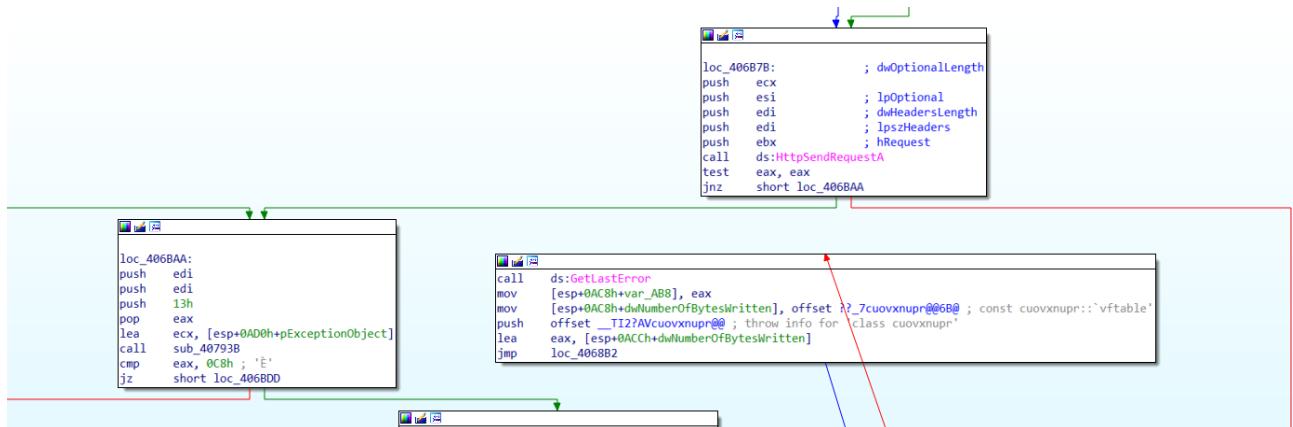


- If the call is not successful, execution will continue at 4047FA and then jump to loc\_404209.

```
.text:00404867      mov    byte ptr [ebp+var_4], 18h
.text:0040486B      push   offset ValueName ; "completed"
.text:00404870      push   [ebp+phkResult] ; hKey
.text:00404873      mov    dword ptr [ebp+var_5C], 1
.text:0040487A      call   ds:RegSetValueExA
.text:00404880      test   eax, eax
.text:00404882      jz    short loc_4048A4
.text:00404884      mov    [ebp+var_88], eax
.text:0040488A      mov    [ebp+var_8C], offset ??_7livesx@@6B@ ; const livesx::`vftable'
.text:00404894      push   offset __TI1?AVlivesx@@ ; throw info for 'class livesx'
.text:00404899      lea    eax, [ebp+var_8C]
.text:0040489F      jmp   loc_404209
```

- **HTTP C2 Analysis:**

- The address of the CALL to HttpSendRequestA is 406B80. The CALL to HttpSendRequestA occurs immediately before the “test” and “jnz” instructions, these instructions likely serve to evaluate the result. If “eax” is not 0, jump to loc\_406BAA otherwise jump to loc\_406B8A.



- The CALL to InternetOpenA occurs at 4068D0, at 4068D6 we can see MOV that places EAX into EBX and CMP that places EDI into EBX. We have CMP and JNZ, the CMP is comparing EBX with 0, if EBX = 0 => the result = 0, and If EBX ≠ 0 => the result ≠ 0. JNZ at 4068DA, If EBX ≠ 0 then jump to loc\_4068F9, the jump will occur if the call to InternetOpenA is successful. If the CALL to InternetOpenA is unsuccessful, execution will proceed linearly to 4068DC, where GetLastError will be called, and the JMP at 4068B2 will eventually be executed

```
.text:004068CF      push   edi      ; lpszAgent
.text:004068D0      call   ds:InternetOpenA
.text:004068D6      mov    ebx, eax
.text:004068D8      cmp    ebx, edi
.text:004068DA      jnz   short loc_4068F9
.text:004068DC      call   ds:GetLastError
.text:004068E2      mov    [esp+0AC8h+var_A8], eax
.text:004068E6      mov    [esp+0AC8h+pExceptionObject], offset ??_7cuovxnupr@@6B@ ; const cuovxnupr::`vftable'
.text:004068EE      push   offset __TI2?AVcuovxnupr@@ ; throw info for 'class cuovxnupr'
.text:004068F3      lea    eax, [esp+0ACCh+pExceptionObject]
.text:004068F7      jmp   short loc_4068B2
.text:004068F9 . . .
```

- In sub\_40684C, we can find the references to both InternetOpenA and HttpSendRequestA

- **Function components:**

- The address 4064E6 is the address of the CALL to GetTempFileNameW. the CALL to GetTempFileNameW is located in function sub\_4064C8

```

.text:004064DB      push    eax          ; lpTempFileName
.text:004064DC      push    0             ; uUnique
.text:004064DE      push    offset PrefixString ; "sys"
.text:004064E3      push    [ebp+lpPathName] ; lpPathName
.text:004064E6      call    ds:GetTempFileNameW
.text:004064EC      test   eax, eax
.text:004064EE      jnz    short loc_40650E
.text:004064F0      call    ds:GetLastError
.text:004064F6      mov     [ebp+var_4], eax
.text:004064F9      push    offset _T12AVLView::vftable
.text:004064FE      ; -----
.text:00406501      ; -----
.text:00406502      ; -----
.text:00406509      ; -----
.text:0040650E      ; -----
.text:0040650E loc_40650E:
.text:0040650E
.text:00406514      ; -----
.text:00406515      ; -----
.text:00406518      ; -----
.text:0040651D      ; -----
.text:004064C8      ; ===== S U B R O U T I N E =====
.text:004064C8      ; Attributes: bp-based frame
.text:004064C8      ; int __cdecl sub_4064C8(int, LPCWSTR lpPathName)
.text:004064C8      sub_4064C8      proc near             ; CODE XREF: sub_406196+67↑p
.text:004064C8
.text:004064C8      TempFileName    = word ptr -210h
.text:004064C8      pExceptionObject= dword ptr -8
.text:004064C8      var_4           = dword ptr -4
.text:004064C8      arg_0           = dword ptr 8
.text:004064C8      lpPathName     = dword ptr 0Ch
.text:004064C8
.text:004064C8      push    ebp
.text:004064C9      mov     ebp, esp
.text:004064CB      sub    esp, 210h
.text:004064D1      and    [ebp+var_4], 0
.text:004064D5      lea    eax, [ebp+TempFileName]
.text:004064DB      push    eax          ; lpTempFileName
.text:004064DC      push    0             ; uUnique
.text:004064DE      push    offset PrefixString ; "sys"
.text:004064E3      push    [ebp+lpPathName] ; lpPathName

```

**xrefs to GetTempFileNameW**

| Director | Ty            | Address                  | Text |
|----------|---------------|--------------------------|------|
| r        | sub_4064C8+1E | call ds:GetTempFileNameW |      |
| p        | sub_4064C8+1E | call ds:GetTempFileNameW |      |

Line 1 of 2

OK Cancel Search Help

→ Sub\_4064C8 has 2 arguments: lpPathName and arg\_0. We have some other variables named TempFileName, var\_8, and var\_4. In this function, the prologue includes addresses 4064C8-4064CB and the epilogue includes addresses 406520-406521. In this case, it includes the typical LEAVE and RETN instructions as well as POP instructions to restore registers that were saved in the prologue.

```

.text:00406520      leave
.text:00406521      retn
.text:00406521 sub_4064C8      endp

```

- We consider the call to CreateProcessW at the address 406166. This CALL is located in function sub\_40611C

```

|.text:00406158      push    ecx          ; lpProcessInformation
|.text:00406159      lea     ecx, [ebp+StartupInfo]
|.text:0040615C      push    ecx          ; lpStartupInfo
|.text:0040615D      push    ebx          ; lpCurrentDirectory
|.text:0040615E      push    ebx          ; lpEnvironment
|.text:0040615F      push    50h ; 'P'   ; dwCreationFlags
|.text:00406161      push    ebx          ; bInheritHandles
|.text:00406162      push    ebx          ; lpThreadAttributes
|.text:00406163      push    ebx          ; lpProcessAttributes
|.text:00406164      push    eax          ; lpCommandLine
|.text:00406165      push    ebx          ; lpApplicationName
|.text:00406166      call    ds:CreateProcessW
|.text:0040616C      test   eax, eax
|.text:0040616E      jnz    short loc_406182
|.text:00406170 loc_406170:      ; C:\Windows\system32\kernel32.dll!CreateProcessW+12
|.text:00406170      push    edi
|.text:00406171      xor    edi, edi
|.text:00406173      lea     esi, [ebp+lpCommand
|.text:00406176      call    sub_402D33
|.text:0040617B      pop    edi
|.text:0040617C      pop    esi
|.text:0040617D      .text:0040611C ; int __cdecl sub_40611C(LPWSTR lpCommandLine, int, int, int, int, int)
|.text:0040611C sub_40611C      proc near             ; CODE XREF: TopLevelExceptionFilter+12↑p
|.text:0040611C          ; WinMain(x,x,x,x)+4EA↑p ...
|.text:0040611C          StartupInfo      = _STARTUPINFOW ptr -54h
|.text:0040611C          ProcessInformation= _PROCESS_INFORMATION ptr -10h
|.text:0040611C          lpCommandLine    = dword ptr 8
|.text:0040611C          arg_14        = dword ptr 1Ch

```

xrefs to CreateProcessW

| Direction | Type          | Address                | Text |
|-----------|---------------|------------------------|------|
| r         | sub_40611C+4A | call ds:CreateProcessW |      |
| p         | sub_40611C+4A | call ds:CreateProcessW |      |

Line 1 of 2

OK Cancel Search Help

→ The sub\_40611C has 2 arguments: lpCommandLine and arg\_14. There are 2 variables named StartupInfo and hObject. Being the same as the previous function, in this one, the prologue includes addresses 40611C-406124 and the epilogue includes addresses 40617B-406181.

```

.text:0040617D          mov     al, bl
.text:0040617F          pop    ebx
.text:00406180          leave
.text:00406181          retn

```

- Loop components:
- A group of strings is located at 418CD8, we press G to jump to 418CD8, click on off\_418CD8, and press x to show the xrefs table, double click on the reference it leads to the address 407D84

```

.LCX.L:00407D82
.text:00407D82 loc_407D82:           ; CODE XREF: sub_407CA7+D0↑j
    xor    esi, esi
.text:00407D84 loc_407D84:           ; CODE XREF: sub_407CA7+FF↓j
    push   off_418CD8[esi] ; String2
    lea     eax, [ebp+FindFileData.cFileName]
    push   eax             ; String1
    call   __wcsicmp
    pop    ecx
    pop    ecx
    test  eax, eax
    jz    loc_407F22
    add   esi, 4
    cmp   esi, 38h ; '8'
    jb    short loc_407D84
    test  byte ptr [ebp+FindFileData.dwFileAttributes], 10h
    jz    short loc_407DF6
    mov   edi, [ebp+arg_4]
    lea   eax, [ebp+var_78]

```

- The loop is presented by the dotted line and the arrow. Before the loop, we have the instruction “xor esi, esi”, this zeroes esi and serves at the loop initiation. The CMP and JB instructions at 407DA3 and 407DA6, respectively, comprise the stopping condition. And our stopping condition is that check if “esi < 38h”, and we increase esi by 4 each loop run (add esi 4 at 407DA0).

- **Compound Expressions:**

- We consider the call to GetTempPathW at address 40526D

```

.text:00405267      mov    edi, 208h
.text:0040526C      push   edi          ; nBufferLength
.text:0040526D      call   ds:GetTempPathW
.text:00405273      test   eax, eax
.text:00405275      jz    short loc_4052A7
.text:00405277      cmp    eax, edi
.text:00405279      pop    edi
.text:0040527A      jnb   short loc_4052A7
.text:0040527C      push   [ebp+var_4]
.text:0040527F      and    dword ptr [esi+10h], 0
.text:00405283      xor    ecx, ecx
.text:00405285      lea    eax, [ebp+eax*2+Buffer]
.text:0040528C      mov    dword ptr [esi+14h], 7
.text:00405293      push   eax
.text:00405294      mov    [esi], cx
.text:00405297      push   esi
.text:00405298      lea    ecx, [ebp+Buffer]
.text:0040529E      call   sub_405904
.text:004052A3      mov    eax, esi
.text:004052A5      leave
.text:004052A6      retn
.text:004052A7 ;

```

- We have the test and jz instruction, which means jump to 4052A7 if eax is zero. We know that eax stored the value returned by the function CALL to GetTempPathW. Now, we can understand the checking condition is “jump to 4052A7 if the GetTempPathW fails”.

- Consider the jnb instruction at 405277, here we compare eax and edi. That means we “jump to 4052A7 if eax is not below edi”.
- In conclusion, this sub-function has the ability to check if the CALL to GetTempPath returns correctly and check if the buffer has enough space for the temporary path ( compare eax and edi - edi is considered as the specific size).
- At the address 406988, we can see a Call to HttpOpenRequestA, basically, we can get the version of the HTTP request is HTTP/1.1. And in this case, the HTTP verb is POST.

```

loc_406988:          ; lpszPassword
push    dword ptr [esp+124]
lea     eax, [esp+0ACCh+hConnect]
push    [esp+0ACCh+lpszUserName] ; lpszUserName
push    dword ptr [esp+0AD0h+nServerPort] ; nServerPort
push    [esp+0AD4h+lpszServerName] ; lpszServerName
push    eax           ; int
call    sub_4079F7
xor    eax, eax
mov     [esp+0AC8h+var_4], edi
cmp     [esp+0AC8h+var_A64], 4
mov     ecx, [esp+0AC8h+hConnect]
setz   al
push   edi           ; dwContext
mov    [esp+0ACCh+Buffer], ecx
dec    eax
and    eax, 0FF7F1000h
add    eax, 84CCF300h
push   eax           ; dwFlags
push   edi           ; lplpszAcceptTypes
push   edi           ; lpszReferrer
push   offset szVersion ; "HTTP/1.1"
push   [esp+0ADCh+lpszObjectName] ; lpszObjectName
push   offset szVerb   ; "POST"
push   ecx           ; hConnect
call   ds:HttpOpenRequestA
mov    ebx, eax
mov    [esp+0AC8h+pExceptionObject], edi
mov    [esp+0AC8h+var_AA8], edi
cmp    ebx, edi
jnz    short loc_406A10

```

**Debugging (OllyDbg):** Function breakpoints, monitor stack, memory map, plugins for unpacking, find OEP

#### ANALYSIS SUMMARY

#### Key Host and Network Indicators of Compromise (IOCs):

- These strange IP addresses:
  - + 91.195.12.187
  - + 195.64.154.114
  - + 149.202.109.205

|   |
|---|
| + 51.254.181.122  |
| + 78.40.108.39  |
| + 188.127.231.116   |
| - HKCU\Software\Locky   |
| - HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Connections\Save<br>dLegacySettings |
| - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable                        |

**Key Functionality:**

+RegOpenKeyExA, RegSetValueExA  
+ InternetOpenA, InternetConnectA, HttpOpenRequestA, HttpSendRequestA, InternetReadFile.  
+ GetTempFileNameW  
+ CreateProcessW  
+ GetTempPathW

**Purpose:**

**Persistence:**

Creates the persistence registry key in the path

- Software\Microsoft\Windows\CurrentVersion\Run

**Environment-specific Impact:**

**Root Cause:**

**Attribution:**