**File Info**

File name:

* Sample\_5f6b5cda69480900164d7b49.bin

Other names:

* ееЕаАххВОеЕао.exe
* Office365.exe
* Sample\_5f6b5cda69480900164d7b49.exe
* 7UCRKL.exe
* VirusShare\_17492f7b9906b807cffd30e8a0edd993
* output.174365990.txt
* trickbot.exe
* 17492f7b9906b807cffd30e8a0edd993.virus
* ?????????????.exe
* 7e8c547fcc86e26b973e4c974da8ee2c4cfe84846e2cdfcd7f265929d27602f9.bin
* tugas.exe
* WindowsDefender.bin

File Type: Win32 EXE

Hashes: -

MD5

17492f7b9906b807cffd30e8a0edd993

SHA-1

ac0724c724f8d6e2a54b41b86d99aa189e40dc81

SHA-256 7e8c547fcc86e26b973e4c974da8ee2c4cfe84846e2cdfcd7f265929d27602f9

History (virus total)

* Creation Time 2019-07-18 08:09:43 UTC
* First Seen In The Wild 2020-06-11 13:11:23 UTC
* First Submission 2019-07-19 22:40:27 UTC
* Last Submission 2023-02-16 09:04:34 UTC
* Last Analysis 2023-01-06 11:19:15 UTC

Sections:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Virtual Address | Virtual Size | MD5 |
| .text | 4096 | 59744 | 8a3e635bbd00713fa9c78e66d692609e |
| .rdata | 65536 | 19648 | 20525fba755e17e594a8d4d3d7f66a85 |
| .data | 86016 | 12348 | 6f9be19e094ef8ae00e441b605289fc9 |
| .rsrc | 102400 | 308574 | 48cdcdc474523bf1cfa85ff149a3311e |

Imports:

* KERNEL32.dll
* OLEAUT32.dll
* SHELL32.dll
* ole32.dll
* USER32.dll
* GDI32.dll

Strings:

* 0000000127B4 0000004127B4 delete[]
* 0000000127C0 0000004127C0 new[]
* 000000062508 000000464508 <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
* 000000062553 000000464553 </assembly>
* 00000001492A 00000041492A DeleteCriticalSection
* 000000014942 000000414942 LeaveCriticalSection
* 00000001495A 00000041495A EnterCriticalSection
* 000000014C6A 000000414C6A WriteConsoleA
* 000000014C7A 000000414C7A GetConsoleOutputCP
* 000000014C90 000000414C90 WriteConsoleW
* 000000014CA0 000000414CA0 CreateFileA

Behavour:-

Registry actions:

Added:

* HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows Defender\Real-Time Protection Added Value DisableBehaviorMonitoring REG\_DWORD
* HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store Added Value C:\Users\NV\Desktop\Sample\_5f6b5cda69480900164d7b49.exe REG\_BINARY
* HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows Defender Added Value DisableAntiSpyware REG\_DWORD
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\TelemetryNamespaces Added Value P-ARIA-7005b72804a64fa4b2138faab88f877b-14cf798a-05a4-4b7b-9d02-4d99259ebd4a-7553 REG\_QWORD
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Ms Net 14.0 libraries Added Value Id REG\_SZ
* HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched Added Value Microsoft.Windows.Explorer REG\_DWORD
* HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows Defender\Real-Time Protection Added Value DisableOnAccessProtection REG\_DWORD

Dropped files:

* ееЕаАххВОеЕао.exe

C:\ProgramData\ееЕаАххВОеЕао.exe

* SAMPLE\_5F6B5CDA69480900164D7B-80859062.pf C:\Windows\Prefetch\SAMPLE\_5F6B5CDA69480900164D7B-80859062.pf
* ЕЕЕААХХВОЕЕАО.EXE-26B74893.pf

C:\Windows\Prefetch\ЕЕЕААХХВОЕЕАО.EXE-26B74893.pf

* NetLibs14 C:\Users\NV\AppData\Roaming\NetLibs14
* ееЕаАххВОеЕао.exe C:\Users\NV\AppData\Roaming\NetLibs14\ееЕаАххВОеЕао.exe
* SVCHOST.EXE-2823DB96.pf C:\Windows\Prefetch\SVCHOST.EXE-2823DB96.pf
* POWERSHELL.EXE-CA1AE517.pf C:\Windows\Prefetch\POWERSHELL.EXE-CA1AE517.pf
* SC.EXE-6C4D4413.pf C:\Windows\Prefetch\SC.EXE-6C4D4413.pf
* Ms Net 14.0 libraries C:\Windows\System32\Tasks\Ms Net 14.0 libraries