

**MALWARE ANALYSIS**

**REPORT**

File Name: Installer.exe

By – Ashok Singh

**SUMMARY**

The precise file behavior could not be analyzed because the DLL file was not successfully executed. The DLL was executed using the “**userdll32.exe**” file in command prompt and with different export functions of DLL but all of them returned an error. Analyzing the export functions of the DLL we can assume the file supported ANSI and Unicode character and using extended library by this DLL file. The behavior of this DLL is suspicious and give the window session, token, read write memory, file operation, connection listening and processes list. This DLL file behavior similar to a Remote Access Terminal (RAT) or a Password stealer. In this file we did not get the any IP or domain connections.

**BASIC PROPERTIES**

|  |
| --- |
| Names JGA0TLK.dll or BA2C403A.dll |
| MD5 7ade3c1d254e2b256cf6281a8d88d286 |
| SHA-1 6209405a872079fae4485c32a9edc1688ed33900 |
| SHA-256 4eaffde337c87e447ad674b279c5a5b3805b1556af3563a12d85e0d57  5ac856e |
| Authentihash 4a793394522279029b5afde9550eac3033fb6257dc3e2e1662092e06b  741560f |
| Imp hash 4b64da26f47500511ae98abd5079c002 |
| SSDEEP 6144:z1OJ4J5PXGZ8A210j/EeTwfDCtFZeGSxFe8YmHec30atxmXh/g54P+  QcL:z1TsuAhr90mtFsGSDeC33NtxmXBg5rZ |
| File type Win32 DLL |
| Magic PE32+ executable for MS Windows (DLL) (console) Mono/.Net assembly |
| File size 940 KB (962560 bytes) |
| Target M/C x64 |
| Time Stamp 2018-12-17 12:44:18 |

**VERSION INFOS**

|  |
| --- |
| Legal Copyright Copyright © 1997 America Online, Inc. |
| File Version 072 |
| Product Name JG ART DLL |
| File Description JG ART DLL |
| Original Filename JGA0TLK.dll |

**STATIC ANTIVIRUS ANALYSIS**

File has been identified by 35/70 Antivirus engines on Virus Total as malicious

|  |  |
| --- | --- |
| ANTIVIRUS | SIGNATURE |
| eScan | Trojan.Agent.DMAB |
| QuickHeal | Bundler.PrepscramRI.S4971798 |
| Zillya | Trojan.Emotet.Win64.76 |
| Alibaba | Trojan:Application/Kryptik.e18a6544 |
| K7GW | Trojan ( 005484d81 ) |
| K7AntiVirus | Trojan ( 005484d81 ) |
| Arcabit | Trojan.Agent.DMAB |
| Invincea | heuristic |
| F-Prot | W64/S-9f9e6594!Eldorado |
| APEX | Malicious |
| ClamAV | Win.Malware.Tspy-6803833-0 |
| BitDefender | Trojan.Agent.DMAB |
| Rising | Trojan.Win64/Kryptik!1.B555 (CLASSIC) |
| Endgame | malicious (high confidence) |
| Emsisoft | Trojan.Agent.DMAB (B) |
| F-Secure | Heuristic.HEUR/AGEN.1037295 |
| TrendMicro | TSPY64\_HPDRIDEX.SM1 |
| FireEye | Generic.mg.7ade3c1d254e2b25 |
| Cyren | W64/S-9f9e6594!Eldorado |
| MAX | malware (ai score=82) |
| Antiy-AVL | Trojan[Banker]/Win64.Emotet |
| GData | Trojan.Agent.DMAB |
| AhnLab-V3 | Trojan/Win64.Dridex.R268869 |
| ALYac | Trojan.Agent.DMAB |
| TACHYON | Trojan/W64.Agent.962560.C |
| Ad-Aware | Trojan.Agent.DMAB |
| ESET-NOD32 | a variant of Win64/Kryptik.BNN |
| TrendMicro-HouseCall | TSPY64\_HPDRIDEX.SM1 |
| Ikarus | Trojan.Win64.Crypt |
| MaxSecure | Banker.Win64.Emotet.sb |
| Fortinet | W64/Kryptik.BNW!tr |
| AVG | Win64:Malware-gen |
| Avast | Win64:Malware-gen |
| CrowdStrike | win/malicious\_confidence\_100% (D) |
| Sophos | Troj/Dridex-AAY |

**File Metadata**

|  |  |
| --- | --- |
| Name | Detail |
| Character Set | Windows, Latin1 |
| Code Size | 761856 |
| Company Name | America Online |
| Entry Point | 0x1290 |
| File Description | JG ART DLL |
| File Flags Mask | 0x003f |
| File OS | Windows 16-bit |
| File Subtype | 0 |
| File Type | Win64 DLL |
| File Type Extension | dll |
| File Version | 072 |
| File Version Number | 72.0.0.0 |
| Image File Characteristics | Executable, Large address aware, DLL |
| Image Version | 0.0 |
| Initialized Data Size | 946176 |
| Internal Name | JGA0TLK.dll |
| Language Code | English (U.S.) |
| Legal Copyright | Copyright 1997 America Online, Inc. |
| Linker Version | 7.1 |
| MIME Type | application/octet-stream |
| Machine Type | AMD AMD64 |
| OS Version | 5.0 |
| Object File Type | Dynamic link library |
| Original File Name | JGA0TLK.dll |
| PE Type | PE32+ |
| Product Version Number | 0.0.0.0 |
| Subsystem | Windows command line |
| Subsystem Version | 5.0 |
| Time Stamp | 2018:12:17 13:44:18+01:00 |

**File Section**

DLL file section Detail.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Virtual Address | Virtual Size | Raw Size |
| .text | 4096 | 11251 | 12288 |
| .rdata | 16384 | 3178 | 4096 |
| .data | 20480 | 12102 | 12288 |
| .pdata | 32768 | 336 | 4096 |
| .rsrc | 622592 | 2431 | 4096 |
| .reloc | 626688 | 192 | 4096 |

**Import Function**

The malware Import dynamic link library

|  |  |
| --- | --- |
| Import DLL | Import function name |
| KERNEL32.dll | TransmitCommChar, GetEnvironmentStrings |
| USER32.dl | IsWindowEnabled , GetProcessWindowStation , CheckDlgButton, GetWindowRect |

**Export Function Name**

Export function by BA2C403A.dll.

 IsInteractiveUserSession

 QueryActiveSession

 QueryUserToken

 RegisterUsertokenForNoWinlogon

 WTSCloseServer

 WTSConnectSessionA

 WTSConnectSessionW

 WTSCreateListenerA

 WTSCreateListenerW

 WTSDisconnectSession

 WTSEnableChildSessions

 WTSEnumerateListenersA

 WTSEnumerateListenersW

 WTSEnumerateProcessesA

 WTSEnumerateProcessesExA

 WTSEnumerateProcessesExW

 WTSEnumerateProcessesW

 WTSEnumerateServersA

 WTSEnumerateServersW

 WTSEnumerateSessionsA

 WTSEnumerateSessionsExA

 WTSEnumerateSessionsExW

 WTSEnumerateSessionsW

 WTSFreeMemory

 WTSFreeMemoryExA

 WTSFreeMemoryExW

 WTSGetChildSessionId

 WTSGetListenerSecurityA

 WTSGetListenerSecurityW

 WTSIsChildSessionsEnabled

 WTSLogoffSession

 WTSOpenServerA

 WTSOpenServerExA

 WTSOpenServerExW

 WTSOpenServerW

 WTSQueryListenerConfigA

 WTSQueryListenerConfigW

 WTSQuerySessionInformationA

 WTSQuerySessionInformationW

 WTSQueryUserConfigA

 WTSQueryUserConfigW

 WTSQueryUserToken

 WTSRegisterSessionNotification

 WTSRegisterSessionNotificationEx

 WTSSendMessageA

 WTSSendMessageW

 WTSSetListenerSecurityA

 WTSSetListenerSecurityW

 WTSSetRenderHint

 WTSSetSessionInformationA

 WTSSetSessionInformationW

 WTSSetUserConfigA

 WTSSetUserConfigW

 WTSShutdownSystem

 WTSStartRemoteControlSessionA

 WTSStartRemoteControlSessionW

 WTSStopRemoteControlSession

 WTSTerminateProcess

 WTSUnRegisterSessionNotification

 WTSUnRegisterSessionNotificationEx

 WTSVirtualChannelClose

 WTSVirtualChannelOpen

 WTSVirtualChannelOpenEx

 WTSVirtualChannelPurgeInput

 WTSVirtualChannelPurgeOutput

 WTSVirtualChannelQuery

 WTSVirtualChannelRead

 WTSVirtualChannelWrite

 WTSWaitSystemEvent