

**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 similar to a Remote Access Terminal, Password stealer and Access File Manager. In this file we did not get the any IP or domain connections.

.

**BASIC PROPERTIES**

|  |
| --- |
| Names JGA0TLK.dll or E79EA438.dll |
| MD5 d8f133ee840bfc4667838997cb353041 |
| SHA-1 e98712a429d0aa4e3dcb72347ec30a65df06ae20 |
| SHA-256 0349722cab1f39346254f63c9e33e79d6c4c145d2d78780f8ea246abb30fecf1 |
| Authentihash a7d346ebd478a5d2b49fc251d36485fcbe026c5f90a62cb32de9  2890a837ced5 |
| Imp hash 4b64da26f47500511ae98abd5079c002 |
| SSDEEP 6144:vOJ4J5PXGZ8A210j/EeTwfDCtFZeGSxFe8YmHec30atxmXh/g54P+Qc  L:vTsuAhr90mtFsGSDeC33NtxmXBg5rZ |
| File type Win32 DLL |
| Magic PE32+ executable for MS Windows (DLL) (console) Mono/.Net assembly |
| File size 944 KB (966656 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 33/70 Antivirus engines on Virus Total as malicious

|  |  |
| --- | --- |
| ANTIVIRUS | SIGNATURE |
| K7AntiVirus | Trojan ( 005484d81 ) |
| MicroWorld-eScan | Trojan.Agent.DMAB |
| QuickHeal | Bundler.PrepscramRI.S4971798 |
| BitDefender | Trojan.Agent.DMAB |
| K7GW | Trojan ( 005484d81 ) |
| Arcabit | Trojan.Agent.DMAB |
| Invincea | heuristic |
| F-Prot | W64/S-9f9e6594!Eldorado |
| TrendMicro-HouseCall | TSPY64\_HPDRIDEX.SM1 |
| ClamAV | Win.Malware.Tspy-6803833-0 |
| Ad-Aware | Trojan.Agent.DMAB |
| Emsisoft | Trojan.Agent.DMAB (B) |
| F-Secure | Heuristic.HEUR/AGEN.1037295 |
| TrendMicro | TSPY64\_HPDRIDEX.SM1 |
| FireEye | Generic.mg.2e3d7019ac3a281e |
| Sophos | Troj/Dridex-AAY |
| Ikarus | Trojan.Win64.Crypt |
| Cyren | W64/S-9f9e6594!Eldorado |
| Webroot | Infostealer.Dridex.Gen |
| Avira | HEUR/AGEN.1037295 |
| Fortinet | W64/Kryptik.BNW!tr |
| Antiy-AVL | Trojan[Banker]/Win64.Emotet |
| Endgame | malicious (high confidence) |
| Acronis | suspicious |
| ALYac | Trojan.Agent.DMAB |
| MAX | malware (ai score=82) |
| ESET-NOD32 | a variant of Win64/Kryptik.BNN |
| Rising | Trojan.Win64/Kryptik!1.B555 (CLASSIC) |
| GData | Trojan.Agent.DMAB |
| MaxSecure | Banker.Win64.Emotet.sb |
| AVG | Win64:Malware-gen |
| Avast | Win64:Malware-gen |
| CrowdStrike | win/malicious\_confidence\_100% (D) |

**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.

* GetFileVersionInfoA
* GetFileVersionInfoByHandle
* GetFileVersionInfoExA
* GetFileVersionInfoExW
* GetFileVersionInfoSizeA
* GetFileVersionInfoSizeExA
* GetFileVersionInfoSizeExW
* GetFileVersionInfoSizeW
* GetFileVersionInfoW
* VerFindFileA
* VerFindFileW
* VerInstallFileA
* VerInstallFileW
* VerLanguageNameA
* VerLanguageNameW
* VerQueryValueA
* VerQueryValueW