

**MALWARE ANALYSIS**

**REPORT**

File Name: Installer.exe

By – Ashok Singh

**SUMMARY**

The respective file is a Remote Access Terminal (RAT). Once the file is executed, a loading window is displayed which is the time the Malware extracts the required malicious DLL files in the Temp Folder. The next step is when the Malware checks for a working Internet Connection. If the connection is not available, the Malware pauses at its current state, whereas If a connection is detected, a new window is detected titled as "Agree and Install". On finding a “Agree and Install”. On clicking the Agree button, a loading screen is displayed upon which it presents a window masking as and Update Process. The Malware then makes the connection with domain “setuporder.com” and IP “165.227.255.218” in the background executes the Service “RasMan” which sends a Remote Access session to the Malicious Server.

**BASIC PROPERTIES**

|  |
| --- |
| Names Installer.exe or 6888690E.exe |
| MD5 14e2efc71475939f2bb00efc31a6345f |
| SHA-1 87d493a04ca0392c77e1ddd027d48e1a63128ffa |
| SHA-256 f9bb95c1d5f23580f3ed9f2e31dfb9687ce94af7033c084da42eabc155ea84f6 |
| Authentihash 0a62e489c0bb9ced8c41e31e475ed26fb8d7612956f215365031  e7c3bbcea5e5 |
| Imp hash dd27e28f78a76c1bac253438b42dca85 |
| SSDEEP 49152:T1qxy1h7IPd/nIKSIrH6K0jmAZn5LQisuOCzidaXzxM5zl9IIm9PwK  YWJLNafn0:bh7IPd/nI0jNGpLBtOCzidaXukIKF5a0 |
| File type Win32 EXE |
| Magic PE32 executable for MS Windows (GUI) Intel 80386 32-bit |
| File size 3.22 MB (3379496 bytes) |
| F-PROT Aspack |
| PEiD ASProtect v1.23 RC1 |

**VERSION INFOS**

|  |
| --- |
| Legal Copyright Copyright.(C) 2018 Ragunathan Limited |
| File Version 0.1.8.3 |
| Legal Trademarks Prime Quinta Update Software - Ragunathan Limited |
| Product Name Prime Quinta Update Software |
| File Description Prime Quinta Update Software - Ragunathan Limited |
| Original Filename Installer.exe |
| Translation 0x0000 0x04e4 |

**STATIC ANTIVIRUS ANALYSIS**

File has been identified by 23/72 Antivirus engines on Virus Total as malicious

|  |  |
| --- | --- |
| ANTIVIRUS | SIGNATURE |
| Qihoo-360 | HEUR/QVM19.1.7D07.Malware.Gen |
| K7GW | Trojan ( 0053fece1 ) |
| K7AntiVirus | Trojan ( 0053fece1 ) |
| Symantec | ML.Attribute.HighConfidence |
| Paloalto | generic.ml |
| Alibaba | Trojan:Win32/Kryptik.60f1887b |
| Rising | Trojan.Kryptik!8.8 (CLOUD) |
| Sophos | Generic PUA IH (PUA) |
| F-Secure | Heuristic.HEUR/AGEN.1040333 |
| DrWeb | Adware.Downware.19231 |
| McAfee-GW-Edition | Artemis!Trojan |
| Fortinet | W32/Kryptik.GMAT!tr |
| Emsisoft | Application.FusionCore (A) |
| Ikarus | Trojan.Win32.Crypt |
| Webroot | W32.Adware.Gen |
| Avira | HEUR/AGEN.1040333 |
| Microsoft | PUA:Win32/FusionCore |
| McAfee | Artemis!14E2EFC71475 |
| VBA32 | TScope.Malware-Cryptor.SB |
| ESET-NOD32 | a variant of Win32/Kryptik.GMAT |
| TrendMicro-HouseCall | TROJ\_GEN.R002H0CET19 |
| AVG | Win32:Adware-gen [Adw] |
| Avast | Win32:Adware-gen [Adw] |

**CONTACTED URLs**

The file contacts/makes connection the following URLs.

* https://setuporder.com/installer.php?code=putgq&uid=&action=2142
* https://setuporder.com/postdata3.php
* https://setuporder.com/ipb.php?id=d3a483c58c3f&id2=c2a613049b4b&icount=21&rcount=49&ucount=1&m=40f3ef570df14b0ba1191650f7bc9c2f
* http://stp-1014845532.us-east-1.elb.amazonaws.com/p.gif?rs=i&h=&av=&aver=&osver=5.1&ossp=3&err=0&64=0&adm=1&quant=8923
* https://setuporder.com/pixel.php?rs=i&h=&av=&aver=&osver=5.1&ossp=3&err=0&64=0&adm=1&quant=8923&cpu=intel(r)+core(tm)+i7-4790+cpu+%40+3.60ghz&gpu=virtualbox+graphics+adapter
* https://setuporder.com/postdata4.php?data=v10+av%3d%26aver%3d%26osver%3d5%2e1%2664%3d0
* https://setuporder.com/addr.php
* https://setuporder.com/fuse.php
* https://setuporder.com/find.php
* https://setuporder.com/posttest.php

**CONTACTED IPs**

The file contacts/makes connection the following IPs

* 165.227.255.218

**CONTACTED DOMAINS**

The file contacts/makes connection the following Domains

* setuporder.com
* stp-1014845532.us-east-1.elb.amazonaws.com

**FILES WRITTEN**

The malware writes the following files.

* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\ INetC2.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\System.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Banner.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\nsProcess.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Trillium.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Nuntius.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\md5dll.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Image.bmp
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Image2.bmp
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\LCLogo.bmp
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\accept.ico
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\decline.ico
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\nsDialogs.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\eula3.rtf

**FILES OPENED**

The malware opens the following files.

* C:\WINDOWS\system32\winime32.dll
* C:\WINDOWS\system32\ws2\_32.dll
* C:\WINDOWS\system32\ws2help.dll
* C:\WINDOWS\system32\psapi.dll
* C:\WINDOWS\system32\imm32.dll
* C:\WINDOWS\system32\lpk.dll
* C:\WINDOWS\system32\usp10.dll
* C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_6.0.2600.5512\_x-ww\_35d4ce83\comctl32.dll
* C:\WINDOWS\system32\shell32.dll
* C:\WINDOWS\WindowsShell.Manifest
* C:\WINDOWS\system32\wsock32.dll
* C:\WINDOWS\system32\rpcss.dll
* C:\WINDOWS\system32\MSCTF.dll
* C:\WINDOWS\system32\shfolder.dll
* C:\WINDOWS\system32\setupapi.dll
* C:\DiskD
* C:\User\Root\AppData\Local\Temp\nsf2.tmp
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp \nsq3.tmp\INetC2.dll
* C:\WINDOWS\system32\wininet.dll
* C:\WINDOWS\Fonts\sserife.fon
* C:\WINDOWS\system32\MSCTFIME.IME
* C:\WINDOWS\system32\uxtheme.dll
* C:\User\Root\AppData\Local\Temporary Internet Files
* C:\User\Root\AppData\Local\History
* C:\User\Root\AppData\Local\Temporary Internet Files\Content.IE5
* C:\User\Root\AppData\Local \Temporary Internet Files\Content.IE5\index.dat
* C:\User\Root\Cookies
* C:\User\Root\AppData\ Cookies\index.dat
* C:\User\Root\AppData\Local\History\History.IE5
* C:\User\Root\AppData\Local\History\History.IE5\index.dat
* C:\WINDOWS\system32\userenv.dll
* C:\AUTOEXEC.BAT
* C:\WINDOWS\system32\schannel.dll
* C:\WINDOWS\system32\rasapi32.dll
* C:\WINDOWS\system32\rasman.dll
* C:\WINDOWS\system32\tapi32.dll
* C:\WINDOWS\system32\rtutils.dll
* C:\WINDOWS\system32\winmm.dll
* C:\WINDOWS\system32\sensapi.dll
* C:\WINDOWS\system32\urlmon.dll
* C:\WINDOWS\system32\mswsock.dll
* C:\WINDOWS\system32\hnetcfg.dll
* C:\WINDOWS\system32\wshtcpip.dll
* C:\WINDOWS\system32\update.exe
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\System.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Banner.dll
* C:\WINDOWS\system32\MSIMTF.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\nsProcess.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Trillium.dll
* C:\WINDOWS\system32\winspool.drv
* C:\WINDOWS\system32\clbcatq.dll
* C:\WINDOWS\system32\comres.dll
* C:\WINDOWS\Registration\R000000000007.clb
* C:\WINDOWS\system32\shdocvw.dll
* C:\WINDOWS\system32\riched20.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Nuntius.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\md5dll.dll
* C:\User\Root\AppData\Local\Temporary Internet Files\Content.IE5\C1OS62RY\p[1].gif
* C:\WINDOWS\system32\rsaenh.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\Image.bmp
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\nsDialogs.dll
* C:\WINDOWS\system32\msftedit.dll
* C:\WINDOWS\win.ini
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\eula3.rtf

**FILES DELETED**

The malware deletes the following files.

* C:\User\Root\AppData\Local\Temp\nsaF067.tmp
* C:\User\Root\AppData\Local\Temp\nsaF068.tmp
* C:\User\Root\AppData\Local\Temporary Internet Files\Content.IE5\C1OS62RY\p[1].gif

**PROCESS AND SERVICE ACTIONS**

Permissions Requested

* SE\_LOAD\_DRIVER\_PRIVILEGE
* SE\_DEBUG\_PRIVILEGE

Services opened

* RASMAN

**MUTEXES CREATED**

Mutexes Created

* RasPbFile

Mutexes Opened

* updpriGro748
* RasPbFile

**MODULES LOADED**

The malware loads the following runtime modules.

* wsock32.dll
* ntdll.dll
* advapi32.dll
* kernel32.dll
* user32.dll
* gdi32.dll
* shell32.dll
* comctl32.dll
* ole32.dll
* version.dll
* setupapi.dll
* rpcrt4.dll
* crypt32.dll
* ws2\_32.dll
* wldap32.dll
* psapi.dll
* wininet.dll
* winspool.drv
* oleaut32.dll
* shlwapi.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\trilliumenu.dll
* C:\User\Root\AppData\Local\Temp\nsaF067.tmp\trilliumloc.dll
* secur32.dll
* wsock32
* ws2\_32
* userenv.dll
* netapi32.dll
* wintrust.dll
* rasapi32.dll
* rtutils.dll
* rasman.dll
* c:\windows\system32\msv1\_0.dll
* sensapi.dll
* urlmon.dll
* c:\windows\system32\mswsock.dll
* dnsapi.dll
* rasadhlp.dll
* hnetcfg.dll
* c:\windows\system32\wshtcpip.dll
* clbcatq.dll
* riched20.dll
* rsaenh.dll
* riched20
* wevtapi.dll

**DROPPED FILES**

The malware drops the following files

|  |  |
| --- | --- |
| Name | system.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF067.tmp\System.dll |
| Size | 10.5KB |
| Processes | 780 (6888690E.exe) |
| Type | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| MD5 | 56a321bd011112ec5d8a32b2f6fd3231 |
| SHA1 | df20e3a35a1636de64df5290ae5e4e7572447f78 |
| SHA256 | bb6df93369b498eaa638b0bcdc4bb89f45e9b02ca12d28bcedf4629ea7f5e0f1 |
| CRC32 | 6998BB0F |
| ssdeep | 192:uv+cJZE61KRWJQO6tFiUdK7ckK4k7l1XRBm0w+NiHi1GSJ:uf6rtFRduQ1W+fG8 |

|  |  |
| --- | --- |
| Name | banner.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF067.tmp\Banner.dll |
| Size | 4.0KB |
| Processes | 780 (6888690E.exe) |
| Type | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| MD5 | a748a0a7a7eb56ad356cce710968a380 |
| SHA1 | a8cd1e978a4b481f410fc5205ca5a29cdb2c22e7 |
| SHA256 | 33409ceab861b0164a9ec3a0395934cade72e2ef1f14a9468a604892b2bbcbd9 |
| CRC32 | 21580C6D |
| ssdeep | 48:6dQCailyzzBhsNDt/fsg2T1lBzlBcHEvRugYy/sQBSz7as:HHiFkgoPBpBcHGRuRQa |

|  |  |
| --- | --- |
| Name | nsprocess.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF067.tmp\nsProcess.dll |
| Size | 4.5KB |
| Processes | 780 (6888690E.exe) |
| Type | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| MD5 | faa7f034b38e729a983965c04cc70fc1 |
| SHA1 | df8bda55b498976ea47d25d8a77539b049dab55e |
| SHA256 | 579a034ff5ab9b732a318b1636c2902840f604e8e664f5b93c07a99253b3c9cf |
| CRC32 | 3CD28811 |
| ssdeep | 48:iYXzAm8HGJLvwM8GJFd6I7W4JtT2bxNNAa4GsNf+CJ8aYqmtlKdgAtgma1QvtCSJ:lz2mJkpGR6GY74GQ1YqmstgGCtR |

|  |  |
| --- | --- |
| Name | trillium.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF067.tmp\Trillium.dll |
| Size | 1.2MB |
| Processes | 780 (6888690E.exe) |
| Type | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| MD5 | 2c1699ee8599af8f4c96d22c6a94b3c6 |
| SHA1 | 1440a08b37dada4446c5475aaa55c29bad500b54 |
| SHA256 | 3f76bb9ab0e9eba016eb4fc9625dc8866030599e0cc71068d4d0aee45d3ab5be |
| CRC32 | 77D757A8 |
| ssdeep | 24576:BfRaakDRbOAezeNWf/sCOMMTQsG0i/nugTubZGGZMzkEaHNYK3F0u+Uw+Q:hjkDRCAebHsPZTQj0i/nuL0GcNaT0uRM |

|  |  |
| --- | --- |
| Name | inetc2.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF067.tmp\INetC2.dll |
| Size | 21.5KB |
| Processes | 780 (6888690E.exe) |
| Type | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| MD5 | 92ec4dd8c0ddd8c4305ae1684ab65fb0 |
| SHA1 | d850013d582a62e502942f0dd282cc0c29c4310e |
| SHA256 | 5520208a33e6409c129b4ea1270771f741d95afe5b048c2a1e6a2cc2ad829934 |
| CRC32 | C495AF3E |
| ssdeep | 384:VpOSdCjDyyvBwRlX+ODbswYM2s74NS0v0Ac9khYLMkIX0+Gzyekx:rdCjW/lX1PfYM2X1 |
| Yara | * network\_http - Communications over HTTP * network\_ftp - Communications over FTP * win\_files\_operation - Affect private profile * Str\_Win32\_Wininet\_Library - Match Windows Inet API library declaration * Str\_Win32\_Internet\_API - Match Windows Inet API call * Str\_Win32\_Http\_API - Match Windows Http API call |

|  |  |
| --- | --- |
| Name | md5dll.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF067.tmp\md5dll.dll |
| Size | 6.5 KB |
| Processes | 780 (6888690E.exe) |
| Type | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| MD5 | 0745ff646f5af1f1cdd784c06f40fce9 |
| SHA1 | bf7eba06020d7154ce4e35f696bec6e6c966287f |
| SHA256 | fbed2f1160469f42ce97c33ad558201b2b43e3020257f9b2259e3ce295317a70 |
| ssdeep | 96:GL2PcvGn5olZMTZxEp8agTsflVwn4GogZcko5N1ub:U2Pxn5UZMTZipyaw4ZkKP2 |

|  |  |
| --- | --- |
| Name | nuntius.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF067.tmp\nuntius.dll |
| Size | 83.5 KB |
| Processes | 780 (6888690E.exe) |
| Type | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| MD5 | a0856301a39378e1da94a697b8e650e8 |
| SHA1 | 9e121677d296d30a4e013a01ed4bd8b7760e44ed |
| SHA256 | 2516b2dd9ff286275049647d2e0824d79beb01209e62ef081004fba293be9e5c |
| ssdeep | 1536:cJAooeFk8mEScnAV5Cxe/KaDvIML1GwMqqJ5d6:4Arv8pAJjqJ54 |