

**MALWARE ANALYSIS**

**REPORT**

File Name: Installer.exe

By – Ashok Singh

**SUMMARY**

The respective file behavior like is a Remote Access Terminal (RAT). Once the file is executed, a loading window is displayed and malware checks for a working Internet Connection. If the connection is available, the Malware extracts the required malicious DLL files in the Temp Folder and a new window is displayed titled as "Agree and Install". On clicking the Agree button, a loading screen is displayed which masks as an Update Process. The Malware then makes a connection with the domain “[poolapplication.com](https://www.virustotal.com/gui/domain/poolapplication.com)” and IP “[174.138.109.81](https://www.virustotal.com/gui/ip-address/174.138.109.81)” in the background and executes the Service “RasMan” which sends a Remote Access session to the Malicious Server and downloads a set of malicious DLLs. If the Internet is disconnected at an initial stage, the malware can’t download the DLL files. Irrespective to the fact if the internet connection was lost initially or latter, the malware deletes all the DLL files from temp folder and terminate itself and connected processes.

**BASIC PROPERTIES**

|  |
| --- |
| Names Installer.exe or D75FFEB1.exe |
| MD5 7063c2510efba3271021e4264484e67d |
| SHA-1 cd5a2604c90a3a74cdccf9b333c2e15ff06d99b4 |
| SHA-256 1650d5967b35f2584bd41493987756b6de4aed08a9a445e3194c19  e3a528ff96 |
| Authentihash 0ecdbb6a19c6854ba3f4463ebaf251196ba28f867aecee564f33  a1195cb270b0 |
| Imp hash 23e90ed6c47bb343ef9b5e32ad7e4c39 |
| SSDEEP 98304:T/mAz9YC5bEikX8g+An9yaKLSig0B0qgzPj7:BxJQMg++9yaKGmJgzPj |
| File type Win32 EXE |
| Magic PE32 executable for MS Windows (GUI) Intel 80386 32-bit |
| File size 3.25 MB (3410232 bytes) |
| F-PROT Aspack |
| PEiD ASProtect v1.23 RC1 |

**VERSION INFOS**

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

**STATIC ANTIVIRUS ANALYSIS**

File has been identified by 18/72 Antivirus engines on Virus Total as malicious

|  |  |
| --- | --- |
| ANTIVIRUS | SIGNATURE |
| Alibaba | Trojan:Win32/Kryptik.140fa9fc |
| AVG | Win32:Adware-gen [Adw] |
| DrWeb | Adware.Downware.19253 |
| F-Secure | Heuristic.HEUR/AGEN.1040333 |
| Ikarus | Trojan.Win32.Crypt |
| K7GW | Trojan ( 0053fece1 ) |
| McAfee-GW-Edition | Artemis!Trojan |
| Sophos AV | Mal/Generic-S |
| TrendMicro-HouseCall | TROJ\_GEN.R002H0CET19 |
| Avast | Win32:Adware-gen [Adw] |
| Avira (no cloud) | HEUR/AGEN.1040333 |
| ESET-NOD32 | A Variant Of Win32/Kryptik.GMAT |
| Fortinet | W32/Kryptik.GMAT!tr |
| K7AntiVirus | Trojan ( 0053fece1 ) |
| McAfee | Artemis!7063C2510EFB |
| Rising | Trojan.Kryptik!8.8 (CLOUD) |
| Symantec | ML.Attribute.HighConfidence |
| VBA32 | BScope.Trojan.Delpem |

**CONTACTED URLs**

The file contacts/makes connection the following URLs.

* [https://poolapplication.com/installer.php?code=putgq&uid=&action=2142](https://www.virustotal.com/gui/url/d1fb729613d00b9d0b366dce7c4f9ca4b95ffdae6ca10bc8d4d04be7d7c08569)
* [https://poolapplication.com/postdata3.php](https://www.virustotal.com/gui/url/e1b5b0fe27174e61bbef4dcf6051ecb606791e7b2f7b363c2f8028079c933cb1)
* [https://poolapplication.com/ipb.php?id=be0879faa803&id2=8b1158f3615b&icount=21&rcount=49&ucount=1&m=bef05a9bb0eb41b7b315ac35de73aa37](https://www.virustotal.com/gui/url/0657febf0cdada4044c415bbceb90fa2676a3369d501cdcc62369289574ed8e4)
* [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://www.virustotal.com/gui/url/985bab33fe641588241246780a9cd1d5d870308b780d68b9f500181f9fcd69f9)
* [https://poolapplication.com/pixel.php?rs=i&h=&av=&aver=&osver=5.1&ossp=3&ostype=&err=0&64=0&adm=1&quant=8923&cpu=intel(r)+core(tm)+i7-4790+cpu+%40+3.60ghz&gpu=virtualbox+graphics+adapter](https://www.virustotal.com/gui/url/4bde561d1bcf113c23520706098ed8768d310ac30693bbe1671daf3f981b66f4)
* [https://poolapplication.com/postdata4.php?data=v10+av%3d%26aver%3d%26osver%3d5%2e1%2664%3d0](https://www.virustotal.com/gui/url/21e89eca2b6b80ba42fa6bc8e4f387cefad56f9dc83fff21fca77836a25f049b)
* [https://poolapplication.com/addr.php](https://www.virustotal.com/gui/url/8049e53deb40b4860c86428435808755b85128111fa4a0f2aed3a06eb67959ee)
* [https://poolapplication.com/fuse.php](https://www.virustotal.com/gui/url/69835239d78ec9512c922a452bbc57eb96cd48c9b64760e18b5075de6ec93642)
* [https://poolapplication.com/find.php](https://www.virustotal.com/gui/url/d9cc94f3cb179246ed334305bdd7ac9220fff0a7c95bf5ad294294046d1633e1)
* [https://poolapplication.com/posttest.php](https://www.virustotal.com/gui/url/0bea3623b4e4e4245676fa20f930dca388fcc181530edcfd5418b844751182fb)

**CONTACTED IPs**

The file contacts/makes connection the following IPs

* [174.138.109.81](https://www.virustotal.com/gui/ip-address/174.138.109.81)

**CONTACTED DOMAINS**

The file contacts/makes connection the following Domains

* [poolapplication.com](https://www.virustotal.com/gui/domain/poolapplication.com)
* stp-1014845532.us-east-1.elb.amazonaws.com

**FILES WRITTEN**

The malware writes the following files.

* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\
* C:\Users\Root\AppData\Local\Temp\nsaFEBD.tmp\
* C:\Users\Root\AppData\Local\Temp\nsgF60.tmp\nsgF60.tmp
* C:\Users\Root\AppData\Local\Temp\nsgF60.tmp\nsgF61.tmp
* C:\Users\Root\AppData\Local\Temp\nsgF60.tmp\nso4B76.tmp
* C:\Users\Root\AppData\Local\Temp\nsgF60.tmp\nso4B77.tmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\ INetC2.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\System.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Banner.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\nsProcess.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Trillium.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Nuntius.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\md5dll.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Image.bmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Image2.bmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\LCLogo.bmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\accept.ico
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\decline.ico
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\nsDialogs.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.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:\Users\Root\AppData\Local\Temp\nsf2.tmp
* C:\Users\Root\AppData\Local\Temp\nsaF067.tmp
* C:\Users\Root\AppData\Local\Temp\nsaF067.tmp \nsaF183.tmp\INetC2.dll
* C:\WINDOWS\system32\wininet.dll
* C:\WINDOWS\Fonts\sserife.fon
* C:\WINDOWS\system32\MSCTFIME.IME
* C:\WINDOWS\system32\uxtheme.dll
* C:\Users\Root\AppData\Local\Temporary Internet Files
* C:\Users\Root\AppData\Local\History
* C:\Users\Root\AppData\Local\Temporary Internet Files\Content.IE5
* C:\Users\Root\AppData\Local \Temporary Internet Files\Content.IE5\index.dat
* C:\Users\Root\Cookies
* C:\Users\Root\AppData\ Cookies\index.dat
* C:\Users\Root\AppData\Local\History\History.IE5
* C:\Users\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\nsaF183.tmp\System.dll
* C:\User\Root\AppData\Local\Temp\nsaF183.tmp\Banner.dll
* C:\WINDOWS\system32\MSIMTF.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\nsProcess.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.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:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Nuntius.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\md5dll.dll
* C:\Users\Root\AppData\Local\Temporary Internet Files\Content.IE5\C1OS62RY\p[1].gif
* C:\WINDOWS\system32\rsaenh.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Image.bmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\nsDialogs.dll
* C:\WINDOWS\system32\msftedit.dll
* C:\WINDOWS\win.ini
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp \eula3.rtf

**FILES DELETED**

The malware deletes the following files.

* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\
* C:\Users\Root\AppData\Local\Temp\nsaFEBD.tmp\
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\ INetC2.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\System.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Banner.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\nsProcess.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Trillium.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Nuntius.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\md5dll.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Image.bmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\Image2.bmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\LCLogo.bmp
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\accept.ico
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\decline.ico
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\nsDialogs.dll
* C:\Users\Root\AppData\Local\Temp\nsaF183.tmp\eula3.rtf
* C:\Users\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
* ZonesCounterMutex
* ZonesCacheCounterMutex
* ZonesLockedCacheCounterMutex

Mutexes Opened

* RasPbFile
* updpriGro748
* WininetStartupMutex
* WininetConnectionMutex
* WininetProxyRegistryMutex

**MODULES LOADED**

The malware loads the following runtime modules.

* comctl32.dll
* NTDLL.DLL
* ADVAPI32.DLL
* KERNEL32.dll
* USER32.dll
* GDI32.dll
* SHELL32.dll
* ADVAPI32.dll
* COMCTL32.dll
* ole32.dll
* OLEACCRC.DLL
* RPCRT4.dll
* KERNEL32.DLL
* C:\WINDOWS\system32\MSCTF.dll
* C:\WINDOWS\system32\SHELL32.dll
* rpcrt4.dll
* shell32.dll
* advapi32.dll
* kernel32.dll
* KERNEL32
* C:\WINDOWS\system32\msctfime.ime
* C:\WINDOWS\system32\ole32.dll
* Secur32.dll
* ws2\_32
* userenv.dll
* secur32.dll
* netapi32.dll
* C:\WINDOWS\system32\wintrust.dll
* RASAPI32.DLL
* RasPbFile
* RTUTILS.DLL
* ntdll.dll
* DisableImprovedZoneCheck
* WS2HELP.dll
* hnetcfg.dll
* C:\WINDOWS\System32\wshtcpip.dll
* C:\WINDOWS\system32\schannel.dll
* C:\WINDOWS\system32\Msctf.dll
* WS2\_32.dll
* PSAPI.DLL
* SHLWAPI.dll
* OLEAUT32.dll
* Ole32.dll
* Comctl32.dll
* C:\WINDOWS\system32\shdocvw.dll
* Kernel32.dll
* Advapi32.dll
* C:\WINDOWS\system32\rsaenh.dll

**DROPPED FILES**

The malware drops the following files

|  |  |
| --- | --- |
| Name | system.dll |
| File Path | C:\Users\Root\AppData\Local\Temp\nsaF183.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\nsaF183.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\nsaF183.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\nsaF183.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\nsaF183.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\nsaF183.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\nsaF183.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 |