xcitium

PUA
Xcitium Final Verdict

File Name: Instalar.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 6ff269608201a97017590f0b7cc0081ad286ba3e
MD5: eb2906a84808343685b26df16297d100
First Seen Date: 2023-06-27 17:03:10 UTC
Number of Clients Seen: 4
Last Analysis Date: 2023-06-29 16:16:47 UTC
Human Expert Analysis Date: 2023-06-28 07:21:26 UTC
Human Expert Analysis Result: PUA
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-06-27 19:09:45 UTC	PUA
Static Analysis Overall Verdict	2023-06-29 16:16:47 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-06-29 16:16:47 UTC	No Match
Human Expert Analysis Overall Verdict	2023-06-28 07:21:26 UTC	PUA
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Suspicious
Timestamp value suspicious	Clean
Header Checksum is zero!	Suspicious
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Clean
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Packer detection on signature database

UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Modifies Windows policies	
Has no visible windows	

Behavioral Information

QueryFilePath

C:\Instalar.exe
C:\Windows\system32\RICHED20.dll
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\system32\PROPSYS.dll

LowerChar

.EXE
.exe
program
file

CreateMutex

<NULL>
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

OpenMutex

Local\MSCTF.Asm.MutexDefault1

ReadFile

C:\
C:\Users\desktop.ini
C:\Users
C:\Users\win7
C:\Users\win7\Videos\desktop.ini
C:\Users\win7\Favorites\desktop.ini
C:\Users\win7\Downloads\desktop.ini
C:\Users\win7\Links\desktop.ini

LoadLibrary

API-MS-Win-Core-LocalRegistry-L1-1-0.dll
KERNEL32.DLL
ADVAPI32.DLL
COMCTL32.DLL
COMDLG32.DLL
GDI32.DLL
OLE32.DLL
SHELL32.DLL
USER32.DLL

riched32.dll
riched20.dll
comctl32.dll
UxTheme.dll
IMM32.dll
ole32.dll
C:\Windows\system32\ole32.dll
ADVAPI32.dll
propsys.dll
SHELL32.dll
ntmarta.dll
C:\Windows\System32\shdocvw.dll
PROPSYS.dll
OLEAUT32.dll
Secur32.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
api-ms-win-downlevel-advapi32-l2-1-0.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{724EF170-A42D-4FEF-9F26-B60E846FBA4F}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions
\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{76765B11-3F95-4AF2-AC9D-EA55D8994F1A}\InProcServer32
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{289A9A43-BE44-4057-A41B-587A76D7E7F9}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}
\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{905E63B6-C1BF-494E-B29C-65B732D3D21A}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{82A74AEB-AEB4-465C-A014-D097EE346D63}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{054FAE61-4DD8-4787-80B6-090220C4B700}
\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Keyboard Layout\Toggle
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{374DE290-123F-4565-9164-39C4925E467B}
\REGISTRY\MACHINE\SOFTWARE\Classes\exefile
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{52528A6B-B9E3-4ADD-B60D-588C2DBA842D}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{491E922F-5643-4AF4-A7EB-4E7A138D8174}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{915221FB-9EFE-4BDA-8FD7-F78DCA774F87}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A990AE9F-A03B-4E80-94BC-9912D7504104}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}
\REGISTRY\MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{E555AB60-153B-4D17-9F04-A5FE99FC15EC}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B7534046-3ECB-4C18-BE4E-64CD4CB7D6AC}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{C870044B-F49E-4126-A9C3-B52A1FF411E8}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{D9DC8A3B-B784-432E-A781-5A1130A75963}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B6EBFB86-6907-413C-9AF7-4FC2ABF07CC5}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{3D644C9B-1FB8-4F30-9B45-F670235F79C0}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{859EAD94-2E85-48AD-A71A-0969CB56A6CD}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4BD8D571-6D19-48D3-BE97-422220080E43}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2112AB0A-C86A-4FFE-A368-0DE96E47012E}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{33E28130-4E1E-4676-835A-98395C3BC3BB}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{DE61D971-5EBC-4F02-A3A9-6C82895E5C04}
\REGISTRY\MACHINE\SOFTWARE\Microsoft\CTF\TIP

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{9274BD8D-CFD1-41C3-B35E-B13F55A758F4}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4BD8D571-6D19-48D3-BE97-422220080E43}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{D0384E7D-BAC3-4797-8F14-CBA229B392B5}

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVers

\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{0E5AAE11-A475-4C5B-AB00-C66DE400274E}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{FD228CB7-AE11-4AE3-864C-16F3910AB8FE}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F1B32785-6FBA-4FCF-9D55-7B8E7F157091}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{AE50C081-EBD2-438A-8655-8A092E34987A}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A305CE99-F527-492B-8B1A-7E76FA98D6E4}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{62AB5D82-FDC1-4DC3-A9DD-070D1D495D97}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A990AE9F-A03B-4E80-94BC-9912D7504104}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{FD228CB7-AE11-4AE3-864C-16F3910AB8FE}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2112AB0A-C86A-4FFE-A368-0DE96E47012E}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{98EC0E18-2098-4D44-8644-66979315A281}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{82A5EA35-D9CD-47C5-9629-E15D2F714E6E}

\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2B0F765D-C0E9-4171-908E-08A611B84FF6}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{56784854-C6CB-462B-8169-88E350ACB882}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{0762D272-C50A-4BB0-A382-697DCD729B80}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{15CA69B3-30EE-49C1-ACE1-6B5EC372AFB5}

\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\N

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{0F214138-B1D3-4A90-BBA9-27CBC0C5389A}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{9E52AB10-F80D-49DF-ACB8-4330F5687855}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7B0DB17D-9CD2-4A93-9733-46CC89022E7C}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{33E28130-4E1E-4676-835A

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{BCB5256F-79F6-4CEE-B725-DC34E402FD46}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{DE92C1C7-837F-4F69-A3BB-86E631204A23}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{C4900540-2379-4C75-844B-64E6FAF8716B}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2A00375E-224C-49DE-B8D1-440DF7EF3DDC}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{52528A6B-B9E3-4ADD-B60D-588C2DBA842D}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2400183A-6185-49FB-A2D8-4A392A602BA3}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{48DAF80B-E6CF-4F4E-B800-0E69D84EE384}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{3214FAB5-9757-4298-BB61-92A9DEAA44FF}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5CD7AEE2-2219-4A67-B85D-6C9CE15660CB}

\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{babe9b14-0f98-11e5-b301-806e6f6e6963}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{BCBD3057-CA5C-4622-B42D-BC56DB0AE516}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}

\REGISTRY\MACHINE\SOFTWARE\Microsoft\CTF\TIP\{3697C5FA-60DD-4B56-92D4-74A569205C16}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{8AD10C31-2ADB-4296-A8F7-E4701232C972}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B6EBFB86-6907-413C-9AF7-4FC2ABF07CC5}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A4115719-D62E-491D-AA7C-E74B8BE3B067}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{C1BAE2D0-10DF-4334-BEDD-7AA20B227A9D}

\REGISTRY\MACHINE\SOFTWARE\Classes\Directory

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{DEBF2536-E1A8-4C59-B6A2-414586476AEA}

\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{babe9b10-0f98-11e5-b301-806e6f6e6963}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B250C668-F57D-4EE1-A63C-290EE7D1AA1F}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A302545D-DEFF-464B-ABE8-61C8648D939B}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{D20BEEC4-5CA8-4905-AE3B-BF251EA09B53}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{69D2CF90-FC33-4FB7-9A0C-EBB0F0FCB43C}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\W

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7B0DB17D-9CD2-4A93-9733-46CC89022E7C}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4BFEFB45-347D-4006-A5BE-AC0CB0567192}

\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{babe9b11-0f98-11e5-b301-806e6f6e6963}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B94237E7-57AC-4347-9151-B08C6C32D1F7}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{0AC0837C-BBF8-452A-850D-79D08E667CA7}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{EE32E446-31CA-4ABA-814F-A5EBD2FD6D5E}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A302545D-DEFF-464B-ABE8-61C8648D939B}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{FDD39AD0-238F-46AF-ADB4-6C85480369C7}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2C36C0AA-5812-4B87-BFD0-4CD0DFB19B39}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{DF7266AC-9274-4867-8D55-3BD661DE872D}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2400183A-6185-49FB-A2D8-4A392A602BA3}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}

\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1F486A52-3CB1-48FD-8F50-B8DC300D9F9D}\InProcServer32

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{905E63B6-C1BF-494E-B29C-65B732D3D21A}

\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\CTF\DirectSwitchHotkeys

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{C5ABBF53-E17F-4121-8900-86626FC2C973}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{3214FAB5-9757-4298-BB61-92A9DEAA44FF}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{5CE4A5E9-E4EB-479D-B89F-130C02886155}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{CAC52C1A-B53D-4EDC-92D7-6B2E8AC19434}

\REGISTRY\MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{0E5AAE11-A475-4C5B-AB00-C66DE400274E}\InProcServer32

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{352481E8-33BE-4251-BA85-6007CAEDCF9D}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4D9F7874-4E0C-4904-967B-40B0D20C3E4B}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{DFDF76A2-C82A-4D63-906A-5644AC457385}

\REGISTRY\MACHINE\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4FCC-854C-77E8F3D1AA80}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{C4AA340D-F20F-4863-AFEF-F87EF2E6BA25}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\PropertyBag

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{54EED2E0-E7CA-4FDB-9148-0F4247291CFA}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{A63293E8-664E-48DB-A079-DF759E0509F7}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{56784854-C6CB-462B-8169-88E350ACB882}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{10C07CD0-EF91-4567-B850-448B77CB37F9}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7B396E54-9EC5-4300-BE0A-2482EBAE1A26}

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{FDD39AD0-238F-46AF-ADB4-

6C85480369C7}
\REGISTRY\USER\S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Internet Explorer\Security
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1A6FDBA2-F42D-4358-A798-B74D745926C5}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{9E3995AB-1F9C-4F13-B827-48B24B6C7174}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{190337D1-B8CA-4121-A639-6D472D16972A}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{ED4824AF-DCE4-45A8-81E2-FC7965083634}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{18989B1D-99B5-455B-841C-AB7C74E4DDFC}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{1777F761-68AD-4D8A-87BD-30B759FA33DD}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{ED4824AF-DCE4-45A8-81E2-FC7965083634}\PropertyBag
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{8983036C-27C0-404B-8F08-102D10DCFD74}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{43668BF8-C14E-49B2-97C9-747784D784B7}
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{4C5C32FF-BB9D-43B0-B5B4
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B88F4DAA-E7BD-49A9-B74D-02885A5DC765}

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise NI Detector 3	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2023-06-29 16:16:44 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2023-06-29 16:16:44 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-06-28 06:27:51 UTC
Analysis End Date: 2023-06-28 07:21:26 UTC
File Upload Date: 2023-06-27 17:02:42 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family:
Malware Type: Pua

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x413F0E68 [Wed Sep 8 13:51:36 2004 UTC]
Debug Artifacts	
Entry Point	0x421bd0 (UPX1)
Exifinfo	
File Size	3248109
File Type Enum	6
Imphash	
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	050849679304b4de8f0ea9e3af46b33ff7d4168c29abd405bcd54c8f7419fe0d
Ssdeep	
Trid	

File Paths

FILE PATH ON CLIENT	SEEN COUNT
E:\utilirarios 2006 (per 9.5)\Antivirus 2006\The Hacker Antivirus 5.9\Instalar.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x16000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x17000	0xb000	0xae00	7.89941387	f76adac890590d78dae0bcf4520cc48d
.rsrc	0x22000	0x2000	0x1c00	2.87689799924	7fe8f62cbeee9826b9f629e4529c61a0