

Summary

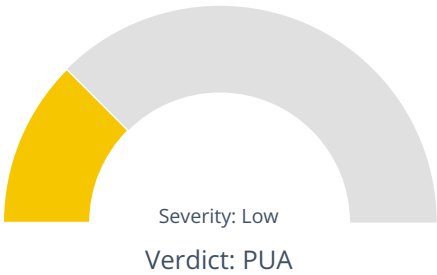
File Name: 972631C1A59F7256B984C3878296797B7607D0B8.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 972631c1a59f7256b984c3878296797b7607d0b8
MD5: e26f7a876b6c2ae91a3165b4d82171c8



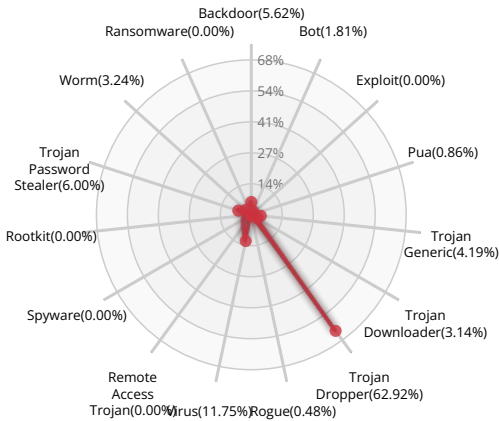
PUA

Xcitium Verdict Cloud Final Verdict

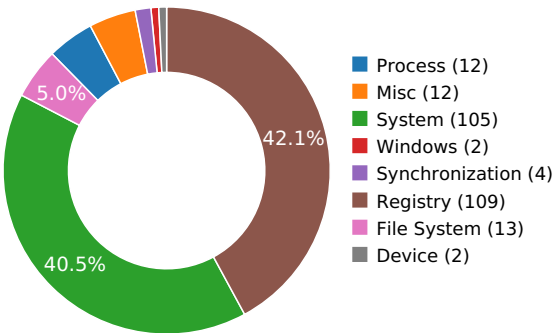
DETECTION SECTION



CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



PACKER

[Show sources](#)

STATIC ANOMALY

[Show sources](#)

Behavior Graph

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\ERROR

C:\Program Files (x86)\Internet Download Manager\IDMan.exe

C:\Users\user\AppData\Local\Temp\IDMan.exe

C:\Windows\Fonts\staticcache.dat

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Users\user\AppData\Local\Temp\imageres.dll

C:\Windows\System32\imageres.dll

\Device\KsecDD

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\chrome.exe\Default

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

RESOLVED APIS

gdi32.dll.GetLayout

gdi32.dll.GdiRealizationInfo

gdi32.dll.FontIsLinked

advapi32.dll.RegOpenKeyExW

advapi32.dll.RegQueryInfoKeyW

gdi32.dll.GetTextFaceAliasW

advapi32.dll.RegEnumValueW

advapi32.dll.RegCloseKey

advapi32.dll.RegQueryValueExW

gdi32.dll.GetFontAssocStatus

advapi32.dll.RegQueryValueExA

advapi32.dll.RegEnumKeyExW

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware

dwmapi.dll.DwmIsCompositionEnabled

comctl32.dll.RegisterClassNameW

kernel32.dll.SortGetHandle

kernel32.dll.SortCloseHandle

uxtheme.dll.EnableThemeDialogTexture

uxtheme.dll.OpenThemeData

uxtheme.dll.GetThemeBool

gdi32.dll.GdiIsMetaPrintDC

ole32.dll.CoInitializeEx

ole32.dll.CoUninitialize

cryptbase.dll.SystemFunction036

ole32.dll.CoRegisterInitializeSpy

ole32.dll.CoRevokeInitializeSpy

uxtheme.dll.BufferedPaintInit

uxtheme.dll.BufferedPaintRenderAnimation

uxtheme.dll.BeginBufferedAnimation
uxtheme.dll.IsThemeBackgroundPartiallyTransparent
uxtheme.dll.DrawThemeParentBackground
uxtheme.dll.DrawThemeBackground
uxtheme.dll.GetThemeBackgroundContentRect
uxtheme.dll.DrawThemeText
uxtheme.dll.EndBufferedAnimation
oleaut32.dll.#500
uxtheme.dll.CloseThemeData
uxtheme.dll.BufferedPaintStopAllAnimations
uxtheme.dll.BufferedPaintUnInit

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\chrome.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\chrome.exe\Default
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Internet Download Manager
HKEY_CURRENT_USER\SOFTWARE\DownloadManager
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\972631c1a59f7256b984c3878296797b7607d0b8.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

READ FILES

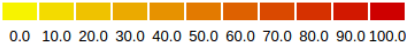
C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\imageres.dll
\Device\KsecDD

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

Network Behavior

CONTACTED IPS

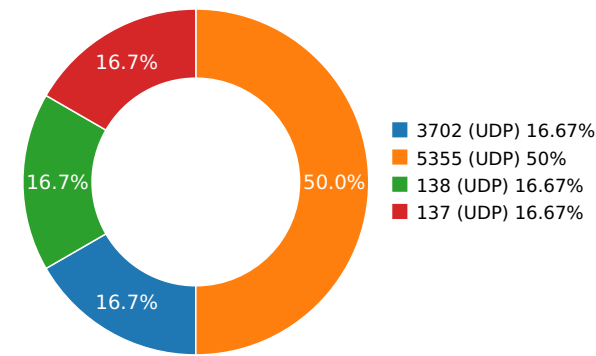


Name	IP	Country	ASN	ASN Name	Trigger Process Type
------	----	---------	-----	----------	----------------------

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.19310307503	Sandbox	224.0.0.252	5355
7.22319507599	Sandbox	224.0.0.252	5355
7.23019003868	Sandbox	239.255.255.250	3702
7.24928307533	Sandbox	192.168.56.255	137
9.78062319756	Sandbox	224.0.0.252	5355
13.2485191822	Sandbox	192.168.56.255	138

NETWORK PORT DISTRIBUTION



DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
-----------	-----------------

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	972631C1A59F7256B984C3878296797B7607D0B8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	972631c1a59f7256b984c3878296797b7607d0b8
MD5:	e26f7a876b6c2ae91a3165b4d82171c8
First Seen Date:	2017-11-06 01:49:37.786336 (9 years ago)
Number Of Clients Seen:	0
Last Analysis Date:	2017-11-06 01:49:37.786336 (9 years ago)
Human Expert Analysis Date:	2017-11-06 13:49:53.514955 (9 years ago)
Human Expert Analysis Result:	PUA

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

 PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	8
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Entry Point	0x408cec (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	77312
Sha256	a2af2a6a4729b7fd4b91418c33e35b0d66bc16ea76ec1771cbbf4d6e311743cf
Mime Type	application/x-dosexec

 PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x7f28	0x8000	6.38129627033	885dd6af7664efc487c1e3ff036fb7ed
DATA	0x9000	0x53c	0x600	2.73838426797	997a08644bec37f07efa621ba12c8264
BSS	0xa000	0x691	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xb000	0xa14	0xc00	4.13684649355	f8a2c2f2fe9d4b7c8c2821cfc75b1035
.tls	0xc000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xd000	0x18	0x200	0.20448815744	d61303205e73ca096826f93772cb8a34
.reloc	0xe000	0x738	0x800	6.36757598905	5c9027af6b185664b106f3dc54b6c4f9
.rsrc	0xf000	0x8e00	0x8e00	7.41477311937	16e7109991581ae67c79edd8321e414e

 PE Imports

- kernel32.dll
 - DeleteCriticalSection
 - LeaveCriticalSection
 - EnterCriticalSection
 - InitializeCriticalSection
 - VirtualFree
 - VirtualAlloc
 - LocalFree
 - LocalAlloc
 - GetVersion
 - GetCurrentThreadId
 - WideCharToMultiByte
 - MultiByteToWideChar
 - GetThreadLocale
 - GetStartupInfoA
 - GetModuleFileNameA
 - GetLocaleInfoA
 - GetCommandLineA
 - FreeLibrary
 - ExitProcess
 - CreateThread

- WriteFile
 - UnhandledExceptionFilter
 - RtlUnwind
 - RaiseException
 - GetStdHandle
- user32.dll
 - GetKeyboardType
 - MessageBoxA
 - CharNextA
- advapi32.dll
 - RegQueryValueExA
 - RegOpenKeyExA
 - RegCloseKey
- oleaut32.dll
 - SysFreeString
 - SysReAllocStringLen
 - SysAllocStringLen
- kernel32.dll
 - TlsSetValue
 - TlsGetValue
 - LocalAlloc
 - GetModuleHandleA
- advapi32.dll
 - RegSetValueExW
 - RegQueryValueExW
 - RegQueryValueExA
 - RegOpenKeyExW
 - RegOpenKeyExA
 - RegCloseKey
- kernel32.dll
 - WriteFile
 - WinExec
 - WaitForSingleObject
 - UnmapViewOfFile
 - Sleep
 - SizeofResource
 - SetLastError
 - SetFilePointer
 - OutputDebugStringA
 - MapViewOfFile
 - LockResource
 - LoadResource
 - GetTickCount
 - GetTempPathW
 - GetLastError
 - GetFileSize
 - GetFileAttributesW
 - FreeResource
 - FormatMessageA
 - FindResourceA
 - ExitProcess
 - CreateProcessW
 - CreateFileMappingW
 - CreateFileW
 - CreateFileA
 - CloseHandle
- gdi32.dll
 - SetTextColor
 - SetBkColor
- user32.dll
 - wvsprintfA
 - WaitForInputIdle
 - TrackPopupMenu
 - ShowWindow
 - SetWindowTextA
 - SetForegroundWindow
 - SetFocus
 - SetDlgItemTextW
 - SetDlgItemTextA
 - SetCursor
 - SendMessageA
 - PostQuitMessage
 - MessageBoxA
 - LoadCursorA
 - IsDlgButtonChecked

- GetDlgItem
 - GetCursorPos
 - FindWindowExA
 - FindWindowA
 - EndDialog
 - EnableWindow
 - DialogBoxParamA
 - DestroyMenu
 - CreatePopupMenu
 - CheckDlgButton
 - AppendMenuA
- shell32.dll
 - ShellExecuteExA
- shell32.dll
 - IsUserAnAdmin
 - ShellExecuteW
 - ShellExecuteA
 - SHGetSpecialFolderPathW

 PE Resources

-  RT_ICON
-  RT_DIALOG
-  RT_RCDATA
-  RT_GROUP_ICON
-  RT_MANIFEST

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS