ID: 349662
Sample Name: eUTopTYPuc
Cookbook: default.jbs
Time: 15:10:11
Date: 07/02/2021
Version: 31.0.0 Emerald

Table of Contents

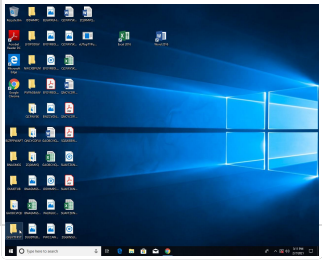
Analysis Report eUTopTYPuc

Overview

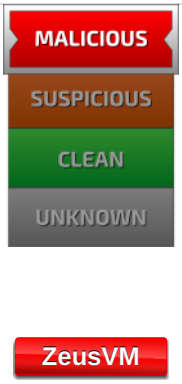
General Information

Sample Name:	eUTopTYPuc (renamed file extension from none to exe)
Analysis ID:	349662
MD5:	09580ec10df3398.
SHA1:	d86cc8b0439b75..
SHA256:	06a0b2c3fc76350..
Tags:	uncategorized

Most interesting Screenshot:



Detection

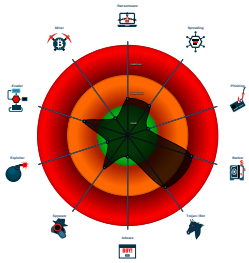


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected ZeusVM e-Banking Trojan
- Multi AV Scanner detection for subm…
- Contains VNC / remote desktop func…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to dynamically…
- Contains functionality to enumerate …
- Contains functionality to launch a pr…
- Contains functionality to open a port…
- Contains functionality to read the PEB
- Contains functionality to read the cli…

Classification



Startup

- **System is w10x64**
- eUTopTYPuc.exe (PID: 632 cmdline: 'C:\Users\user\Desktop\eUTopTYPuc.exe' MD5: 09580EC10DF3398CE68C176121FBBA66)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

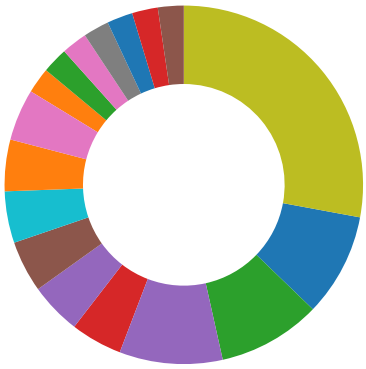
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Protection of GUI



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

E-Banking Fraud:

Detected ZeusVM e-Banking Trojan

Remote Access Functionality:

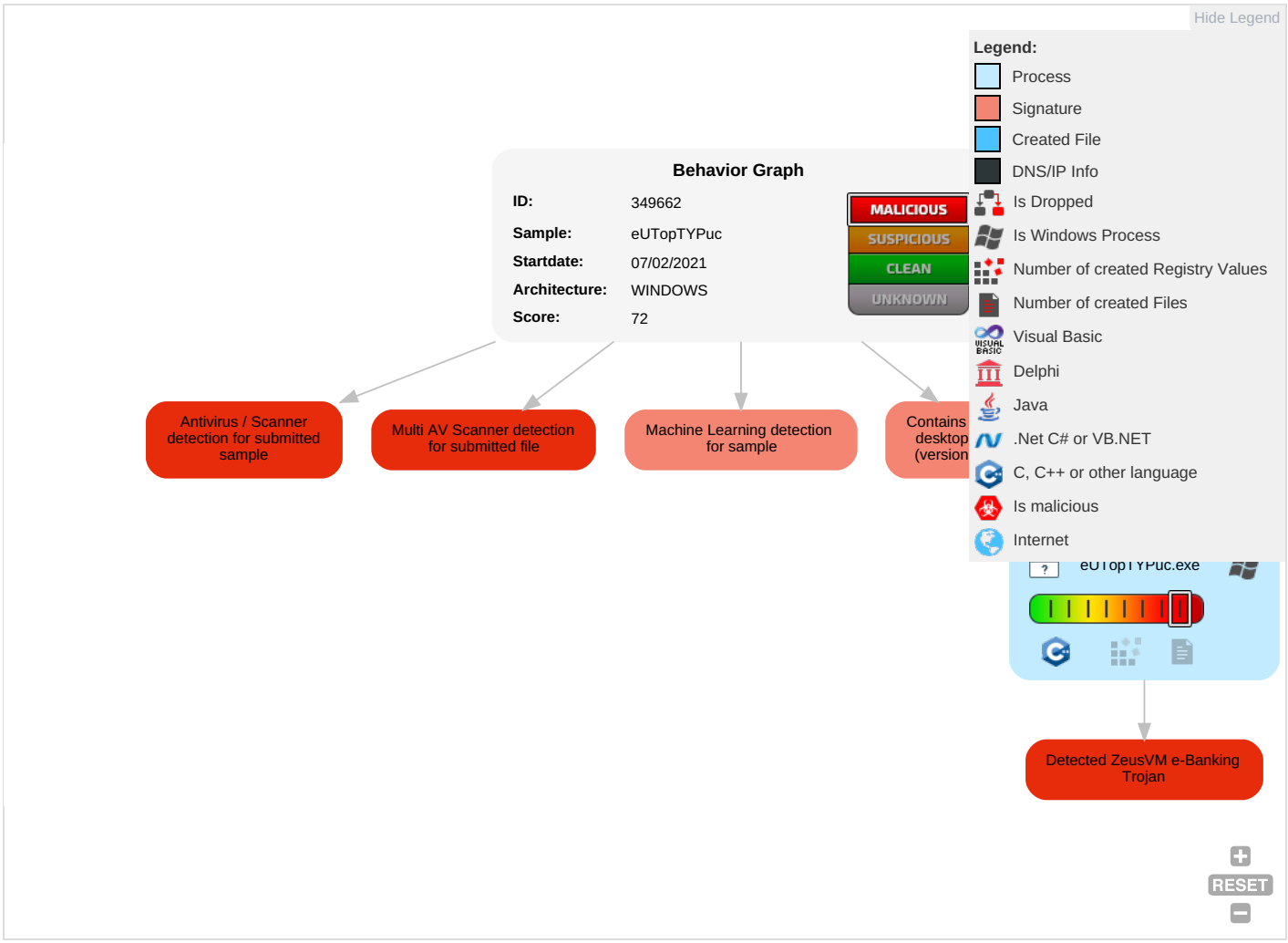
Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts 1	Native API 1	Create Account 1	Valid Accounts 1	Valid Accounts 1	Input Capture 1 1	Network Share Discovery 1	Remote Desktop Protocol 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Valid Accounts 1	Access Token Manipulation 1 1	Access Token Manipulation 1 1	LSASS Memory	System Time Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 1	Security Account Manager	Security Software Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Install Root Certificate 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols	

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.


Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
eUTopTYPuc.exe	92%	Virustotal		Browse
eUTopTYPuc.exe	83%	Metadefender		Browse
eUTopTYPuc.exe	96%	ReversingLabs	Win32.Trojan.Zeus	
eUTopTYPuc.exe	100%	Avira	TR/Spy.Zbot.aoqb.5	
eUTopTYPuc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.eUTopTYPuc.exe.400000.0.unpack	100%	Avira	TR/Spy.Zbot.aoqb.5		Download File
0.2.eUTopTYPuc.exe.400000.0.unpack	100%	Avira	TR/Spy.Zbot.aoqb.5		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	349662
Start date:	07.02.2021
Start time:	15:10:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eUTopTYPuc (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	1
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.bank.troj.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 91%) • Quality average: 80% • Quality standard deviation: 31.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS-DOS executable
Entropy (8bit):	6.695252019797953
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • DOS Executable Borland Pascal 7.0x (2037/25) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	eUTopTYPuc.exe
File size:	141824
MD5:	09580ec10df3398ce68c176121fbba66
SHA1:	d86cc8b0439b75ffecf6df985161c81f028a6fe2
SHA256:	06a0b2c3fc763506f6340dc4f582f7980378f7ededfb807541afeeca0499d8cd
SHA512:	f5c48d2393ed7663016c09dc0f4549cddc1f9fe9f243db74e89de7f14f745ab836657e2f224ac4d70c0c23587a736c508a43c16f4cb4a394d6722844bf047330
SSDEEP:	3072:/SV0AxFxYlFZR3v4iNGMHRHaFtC7qQZkGUGTVpAXhS5qsFwDFox63KruM:/Y0AKlFZR3v4icKHaFGxUsAXhSYsupUb
File Content Preview:	MZ..... ....PE..L...V..N.....:.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4139f2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x4EAF1E56 [Mon Oct 31 22:16:54 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	0b998d2a10b9f3bb78c6703e634f1aff

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 10h
push ebx
push 00000000h
xor bl, bl
call 00007FB00CDDF4A0h
test al, al
je 00007FB00CDE04FAh
push 00008007h
mov byte ptr [ebp-10h], bl
mov byte ptr [ebp-0Ch], 00000001h
mov byte ptr [ebp-01h], bl
call dword ptr [00401178h]
lea eax, dword ptr [ebp-08h]
push eax
call dword ptr [00401174h]
push eax
call dword ptr [004012CCh]
test eax, eax
je 00007FB00CDE04A7h
xor edx, edx
cmp dword ptr [ebp-08h], edx
jle 00007FB00CDE0461h
mov ecx, dword ptr [eax+edx*4]
test ecx, ecx
je 00007FB00CDE0454h
cmp word ptr [ecx], 002Dh
jne 00007FB00CDE044Eh
movzx ecx, word ptr [ecx+02h]
cmp ecx, 66h
je 00007FB00CDE0441h
cmp ecx, 69h
je 00007FB00CDE0438h
cmp ecx, 6Eh
je 00007FB00CDE042Dh
cmp ecx, 76h
jne 00007FB00CDE0436h
mov byte ptr [ebp-01h], 00000001h
jmp 00007FB00CDE0430h
mov byte ptr [ebp-0Ch], 00000000h

Instruction
jmp 00007FB00CDE042Ah
mov bl, 01h
jmp 00007FB00CDE0426h
mov byte ptr [ebp-10h], 00000001h
inc edx
cmp edx, dword ptr [ebp-08h]
jl 00007FB00CDE03E3h
push eax
call dword ptr [00401130h]
test bl, bl
je 00007FB00CDE0429h
call 00007FB00CDDFE55h
jmp 00007FB00CDE0456h
cmp byte ptr [ebp-01h], 00000000h
je 00007FB00CDE0445h
call 00007FB00CDDA34Bh
call 00007FB00CDD2176h
test byte ptr [00423968h], 00000004h
mov bl, al
je 00007FB00CDE043Dh
push 00000000h
mov eax, 004231B8h
call 00007FB00CDDA1A8h
jmp 00007FB00CDE042Fh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1f754	0x118	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x25000	0x11a4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x5a0	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20634	0x20800	False	0.640144230769	data	6.71836960756	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x204c	0x400	False	0.2099609375	data	1.62977361771	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x25000	0x1664	0x1800	False	0.626302083333	data	5.62270089865	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import

DLL	Import
KERNEL32.dll	FlushFileBuffers, GetTempPathW, GetFileSizeEx, OpenMutexW, GetLastError, SetLastError, VirtualAlloc, VirtualProtectEx, VirtualAllocEx, FindClose, LoadLibraryA, RemoveDirectoryW, WaitForMultipleObjects, FindNextFileW, VirtualProtect, GetFileTime, ReleaseMutex, FileTimeToLocalFileTime, GetVolumeNameForVolumeMountPointW, DeleteFileW, GetFileInformationByHandle, LocalFree, GetSystemTime, WriteProcessMemory, SetFileAttributesW, CreateThread, ExpandEnvironmentStringsW, SystemTimeToFileTime, UnmapViewOfFile, MultiByteToWideChar, CreateEventW, GetCurrentThreadId, TlsAlloc, TlsFree, MoveFileExW, GetModuleFileNameW, GetUserDefaultUILanguage, ExitProcess, GetCommandLineW, SetErrorMode, GetComputerNameW, GetVersionExW, OpenEventW, DuplicateHandle, GetCurrentProcessId, GetNativeSystemInfo, GetThreadContext, SetThreadContext, GetProcessId, GetPrivateProfileStringW, GetPrivateProfileIntW, lstrcmpiA, WTSGetActiveConsoleSessionId, GetLocalTime, HeapAlloc, CreateProcessW, CreateFileW, GetTimeZoneInformation, ReadFile, Thread32Next, GetFileAttributesW, HeapCreate, HeapDestroy, FreeLibrary, SetEndOfFile, ReadProcessMemory, Sleep, LoadLibraryW, WideCharToMultiByte, Thread32First, WriteFile, VirtualQueryEx, SetFileTime, IsBadReadPtr, GetProcessHeap, VirtualFree, CreateDirectoryW, HeapFree, CreateFileMappingW, SetFilePointerEx, FindFirstFileW, CreateMutexW, HeapReAlloc, GetTempFileNameW, FileTimeToDosDateTime, GetEnvironmentVariableW, CloseHandle, CreateToolhelp32Snapshot, Process32NextW, Process32FirstW, VirtualFreeEx, OpenProcess, CreateRemoteThread, EnterCriticalSection, GlobalUnlock, LeaveCriticalSection, InitializeCriticalSection, GetTickCount, GlobalLock, ResetEvent, SetThreadPriority, TerminateProcess, TlsSetValue, GetCurrentThread, SetEvent, WaitForSingleObject, TlsGetValue, GetFileAttributesExW, lstrcmpiW, GetProcAddress, MapViewOfFile, GetModuleHandleW
USER32.dll	LoadImageW, MsgWaitForMultipleObjects, WindowFromPoint, CharToOemW, GetWindowLongW, CharLowerA, CharUpperW, SetWindowLongW, SendMessageTimeoutW, GetWindow, DispatchMessageW, GetKeyboardState, ToUnicode, FillRect, PostMessageW, GetWindowInfo, GetTopWindow, IntersectRect, PostThreadMessageW, EqualRect, PrintWindow, SendMessageW, IsRectEmpty, EndPaint, GetMenuItemID, GetUpdateRgn, GetMessageW, RegisterClassExA, GetWindowDC, SetCapture, CharLowerBuffA, CharLowerW, GetThreadDesktop, MapVirtualKeyW, DrawIcon, GetIconInfo, GetSystemMetrics, GetWindowRect, GetParent, GetClassLongW, GetAncestor, SetWindowPos, IsWindow, MapWindowPoints, ExitWindowsEx, CreateDesktopW, SetProcessWindowStation, CloseWindowStation, CreateWindowStationW, GetProcessWindowStation, CloseDesktop, SetThreadDesktop, OpenWindowStationW, SetKeyboardState, GetSubMenu, GetShellWindow, OpenDesktopW, RegisterWindowMessageW, DrawEdge, MenuItemFromPoint, GetMenuItemRect, TrackPopupMenuEx, RegisterClassA, DefFrameProcW, SystemParametersInfoW, GetClassNameW, GetMenuState, GetMenuItemCount, DefDlgProcW, DefFrameProcA, OpenInputDesktop, BeginPaint, GetUpdateRect, GetDC, GetCapture, TranslateMessage, RegisterClassExW, SetCursorPos, GetClipboardData, PeekMessageW, GetDCEx, PeekMessageA, ReleaseDC, DefWindowProcA, GetCursorPos, DefMDIChildProcW, HiliteMenuItem, GetUserObjectInformationW, EndMenu, GetWindowThreadProcessId, GetMessageA, GetMessagePos, DefWindowProcW, CallWindowProcW, CallWindowProcA, RegisterClassW, ReleaseCapture, DefMDIChildProcA, DefDlgProcA, SwitchDesktop, GetMenu
ADVAPI32.dll	GetLengthSid, CryptGetHashParam, OpenProcessToken, GetSidSubAuthority, CryptAcquireContextW, OpenThreadToken, GetSidSubAuthorityCount, GetTokenInformation, RegCreateKeyExW, CryptReleaseContext, RegQueryValueExW, CreateProcessAsUserW, InitializeSecurityDescriptor, SetSecurityDescriptorDacl, SetNamedSecurityInfoW, LookupPrivilegeValueW, CryptCreateHash, ConvertStringSecurityDescriptorToSecurityDescriptorW, RegOpenKeyExW, GetSecurityDescriptorSacl, SetSecurityDescriptorSacl, CryptDestroyHash, AdjustTokenPrivileges, RegCloseKey, RegSetValueExW, CryptHashData, InitiateSystemShutdownExW, IsWellKnownSid, ConvertSidToStringSidW, EqualSid, RegEnumKeyExW
SHLWAPI.dll	wvnsprintfW, StrStrIW, StrStrIA, StrCmpNIW, PathQuoteSpacesW, PathIsURLW, PathRenameExtensionW, wvnsprintfA, StrCmpNIA, PathMatchSpecW, PathRemoveBackslashW, PathUnquoteSpacesW, PathAddExtensionW, PathCombineW, SHDeleteKeyW, PathSkipRootW, SHDeleteValueW, PathAddBackslashW, PathRemoveFileSpecW, PathFindFileNameW, PathIsDirectoryW, UrlUnescapeA
SHELL32.dll	ShellExecuteW, SHGetFolderPathW, CommandLineToArgvW
Secur32.dll	GetUserNameExW
ole32.dll	StringFromGUID2, CLSIDFromString, CoUninitialize, CoCreateInstance, CoInitializeEx
GDI32.dll	CreateCompatibleBitmap, GetDIBits, CreateDIBSection, SetViewportOrgEx, DeleteDC, GdiFlush, DeleteObject, SelectObject, SetRectRgn, CreateCompatibleDC, GetDeviceCaps, RestoreDC, SaveDC
WS2_32.dll	sendto, getsockname, select, getaddrinfo, recvfrom, getpeername, accept, listen, WSAEventSelect, WSAIoctl, connect, WSAAddressToStringW, WSAStartup, WSAGetLastError, shutdown, setsockopt, bind, socket, recv, freeaddrinfo, WSASend, closesocket, send, WSASetLastError
CRYPT32.dll	CertDuplicateCertificateContext, CertEnumCertificatesInStore, CertCloseStore, CertOpenSystemStoreW, CertDeleteCertificateFromStore, CryptUnprotectData, PFXImportCertStore, PFXExportCertStoreEx
WININET.dll	HttpAddRequestHeadersW, InternetSetStatusCallbackW, GetUrlCacheEntryInfoW, HttpAddRequestHeadersA, InternetQueryOptionA, InternetOpenA, HttpOpenRequestA, InternetSetOptionA, InternetCrackUrlA, InternetQueryOptionW, InternetConnectA, InternetCloseHandle, HttpSendRequestA, HttpSendRequestW, InternetReadFile, InternetReadFileExA, InternetQueryDataAvailable, HttpSendRequestExW, HttpQueryInfoA, HttpSendRequestExA
OLEAUT32.dll	VariantInit, SysAllocString, VariantClear, SysFreeString
NETAPI32.dll	NetApiBufferFree, NetUserEnum, NetUserGetInfo

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: eUTopTYPuc.exe PID: 632 Parent PID: 5732

General

Start time:	15:10:58
Start date:	07/02/2021
Path:	C:\Users\user\Desktop\eUTopTYPuc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\eUTopTYPuc.exe'
Imagebase:	0x400000
File size:	141824 bytes
MD5 hash:	09580EC10DF3398CE68C176121FBBA66
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis