Summary

File Name: d191af7816640acd232d85dff54294cf0890d15d6d5d2c0fdfaa95babccf9a6c.exe

File Type: PE32+ executable (GUI) x86-64, for MS Windows

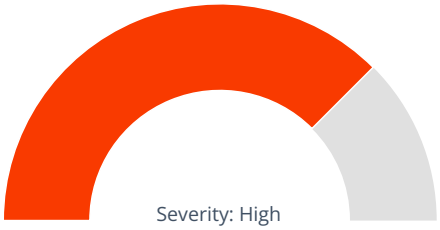
SHA1: 45b63e00c568632d21828d652ee538085ad64e11

MD5: 3affbe6f0688c8a598fef9d8bcef1c6b

MALWARE

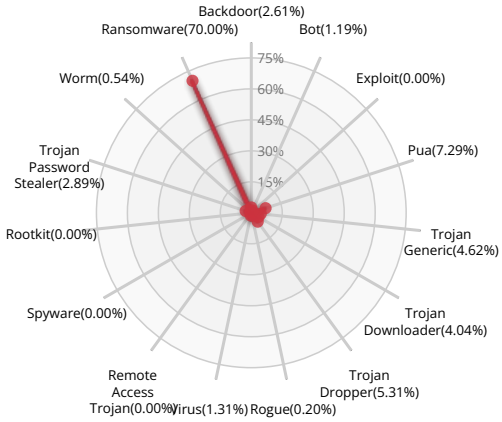
Xcitium Verdict Cloud Final Verdict

DETECTION SECTION

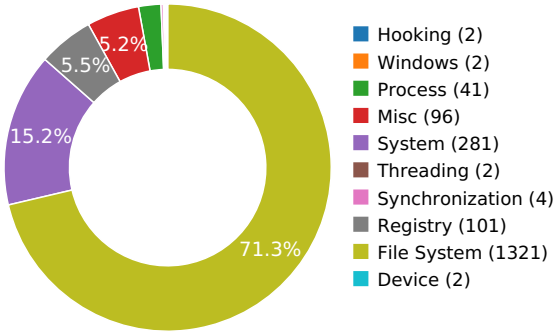


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Activity Details

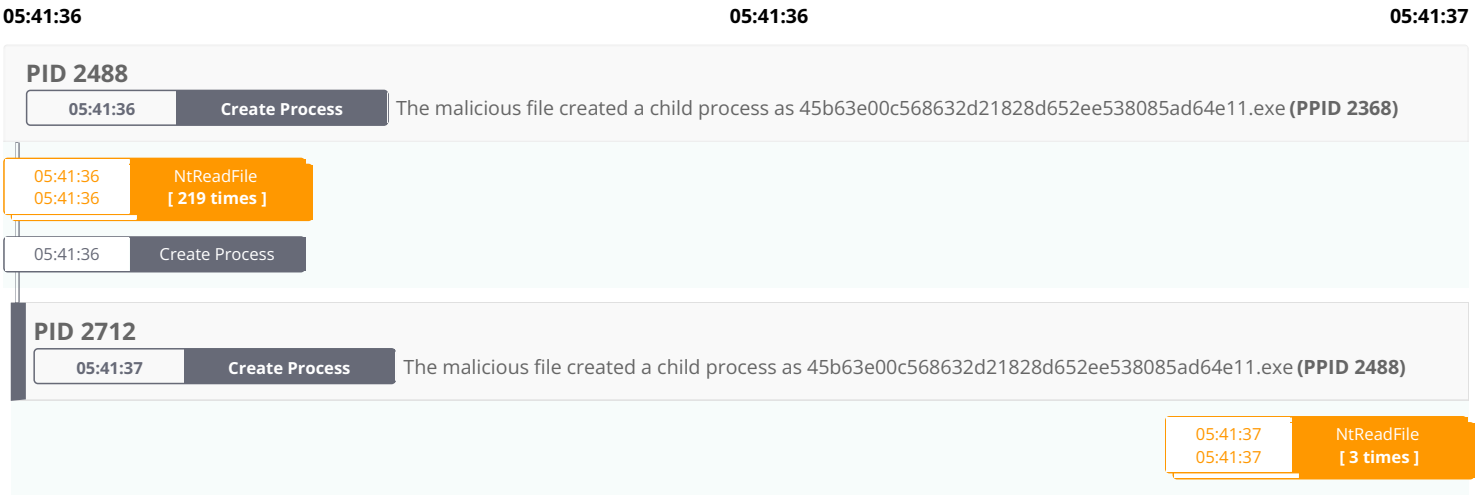
INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Writes a potential ransom message to disk — Show sources

Behavior Graph



Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\45b63e00c568632d21828d652ee538085ad64e11.exe
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp_MEI22722
C:\Users\user\AppData\Local\Temp_MEI22722\VCRUNTIME140.dll
C:\Users\user\AppData\Local\Temp_MEI22722_bz2.pyd
C:\Users\user\AppData\Local\Temp_MEI22722_cffi_backend.cp310-win_amd64.pyd
C:\Users\user\AppData\Local\Temp_MEI22722_decimal.pyd
C:\Users\user\AppData\Local\Temp_MEI22722_hashlib.pyd
C:\Users\user\AppData\Local\Temp_MEI22722_lzma.pyd
C:\Users\user\AppData\Local\Temp_MEI22722_queue.pyd
C:\Users\user\AppData\Local\Temp_MEI22722_socket.pyd
C:\Users\user\AppData\Local\Temp_MEI22722_ssl.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\bcrypt
C:\Users\user\AppData\Local\Temp_MEI22722\bcrypt_bcrypt.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\brotli
C:\Users\user\AppData\Local\Temp_MEI22722\brotli_brotli.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat\bindings
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat\bindings_rust.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\libcrypto-1_1.dll
C:\Users\user\AppData\Local\Temp_MEI22722\libssl-1_1.dll
C:\Users\user\AppData\Local\Temp_MEI22722\python3.dll
C:\Users\user\AppData\Local\Temp_MEI22722\python310.dll
C:\Users\user\AppData\Local\Temp_MEI22722\select.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\unicodedata.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\zstandard
C:\Users\user\AppData\Local\Temp_MEI22722\zstandard_cffi.cp310-win_amd64.pyd
C:\Windows\sysnative\tzres.dll
C:\Users\user\AppData\Local\Temp_MEI22722\zstandard\backend_c.cp310-win_amd64.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\base_library.zip
C:\Users\user\AppData\Local\Temp_MEI22722\certifi

C:\Users\user\AppData\Local\Temp_MEI22722\certifi\cacert.pem

C:\Users\user\AppData\Local\Temp_MEI22722\certifi\py.typed

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\INSTALLER

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE.APACHE

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE.BSD

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\METADATA

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\RECORD

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\WHEEL

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\top_level.txt

C:\Users\user\AppData\Local\Temp_MEI22722*

C:\Users\user\AppData\Local\Temp_MEI22722\bcrypt*

C:\Users\user\AppData\Local\Temp_MEI22722\brotli*

C:\Users\user\AppData\Local\Temp_MEI22722\certifi*

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography*

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat*

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat\bindings*

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info*

C:\Users\user\AppData\Local\Temp_MEI22722\zstandard*

C:\Users\user\AppData\Local\Temp_MEI22722\ucrtbase.dll

C:\Users\user\AppData\Local\Temp_MEI22722\VERSION.dll

C:\Windows\sysnative\version.dll

C:\Users\user\AppData\Local\Temp_MEI22722\api-ms-win-core-path-l1-1-0.dll

C:\Windows\sysnative\api-ms-win-core-path-l1-1-0.dll

C:\Windows\system\api-ms-win-core-path-l1-1-0.dll

C:\Windows\api-ms-win-core-path-l1-1-0.dll

C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-path-l1-1-0.dll

C:\Windows\sysnative\wbem\api-ms-win-core-path-l1-1-0.dll

C:\Windows\sysnative\WindowsPowerShell\v1.0\api-ms-win-core-path-l1-1-0.dll

C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-path-l1-1-0.dll

C:\Program Files (x86)\Universal Extractor\api-ms-win-core-path-l1-1-0.dll

C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-path-l1-1-0.dll

C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-path-l1-1-0.dll

C:\Python27\api-ms-win-core-path-l1-1-0.dll

C:\Python27\Scripts\api-ms-win-core-path-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-core-path-l1-1-0.dll
C:\tools\api-ms-win-core-path-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-core-path-l1-1-0.dll
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\imageres.dll
C:\Users\user\AppData\Local\Temp_MEI22722\imageres.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
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\Microsoft\CTF\EnableAnchorContext

MODIFIED FILES

C:\Users\user\AppData\Local\Temp_MEI22722\VCRUNTIME140.dll

C:\Users\user\AppData\Local\Temp_MEI22722_bz2.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_cffi_backend.cp310-win_amd64.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_decimal.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_hashlib.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_lzma.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_queue.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_socket.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_ssl.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\bcrypt_bcrypt.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\brotli_brotli.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat\bindings_rust.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\libcrypto-1_1.dll

C:\Users\user\AppData\Local\Temp_MEI22722\libssl-1_1.dll

C:\Users\user\AppData\Local\Temp_MEI22722\python3.dll

C:\Users\user\AppData\Local\Temp_MEI22722\python310.dll

C:\Users\user\AppData\Local\Temp_MEI22722\select.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\unicodedata.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\zstandard_cffi.cp310-win_amd64.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\zstandard\backend_c.cp310-win_amd64.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\base_library.zip

C:\Users\user\AppData\Local\Temp_MEI22722\certifi\cacert.pem

C:\Users\user\AppData\Local\Temp_MEI22722\certifi\py.typed

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\INSTALLER

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE.APACHE

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE.BSD

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\METADATA

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\RECORD

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\WHEEL

C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\top_level.txt

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.LCMapStringEx
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
uxtheme.dll.CloseThemeData
uxtheme.dll.BufferedPaintStopAllAnimations
uxtheme.dll.BufferedPaintUnInit

DELETED FILES

C:\Users\user\AppData\Local\Temp_MEI22722\base_library.zip
C:\Users\user\AppData\Local\Temp_MEI22722\bcrypt_bcrypt.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\bcrypt
C:\Users\user\AppData\Local\Temp_MEI22722\brotli_brotli.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\brotli
C:\Users\user\AppData\Local\Temp_MEI22722\certifi\cacert.pem
C:\Users\user\AppData\Local\Temp_MEI22722\certifi\py.typed
C:\Users\user\AppData\Local\Temp_MEI22722\certifi
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat\bindings_rust.pyd
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat\bindings
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography\hazmat
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\INSTALLER
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE.APACHE
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\LICENSE.BSD
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\METADATA
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\RECORD
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\top_level.txt
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info\WHEEL
C:\Users\user\AppData\Local\Temp_MEI22722\cryptography-41.0.1.dist-info
C:\Users\user\AppData\Local\Temp_MEI22722\libcrypto-1_1.dll

C:\Users\user\AppData\Local\Temp_MEI22722\libssl-1_1.dll

C:\Users\user\AppData\Local\Temp_MEI22722\python3.dll

C:\Users\user\AppData\Local\Temp_MEI22722\python310.dll

C:\Users\user\AppData\Local\Temp_MEI22722\select.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\unicodedata.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\VCRUNTIME140.dll

C:\Users\user\AppData\Local\Temp_MEI22722\zstandard\backend_c.cp310-win_amd64.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\zstandard_cffi.cp310-win_amd64.pyd

C:\Users\user\AppData\Local\Temp_MEI22722\zstandard

C:\Users\user\AppData\Local\Temp_MEI22722_bz2.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_cffi_backend.cp310-win_amd64.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_decimal.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_hashlib.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_lzma.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_queue.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_socket.pyd

C:\Users\user\AppData\Local\Temp_MEI22722_ssl.pyd

C:\Users\user\AppData\Local\Temp_MEI22722

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR

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

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

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

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

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\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\45b63e00c568632d21828d652ee538085ad64e11.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\Microsoft\CTF\EnableAnchorContext

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses

READ FILES

C:\Users\user\AppData\Local\Temp\45b63e00c568632d21828d652ee538085ad64e11.exe

C:\Windows\sysnative\tzres.dll

C:\Users\user\AppData\Local\Temp_MEI22722\python310.dll

C:\Windows\sysnative\version.dll

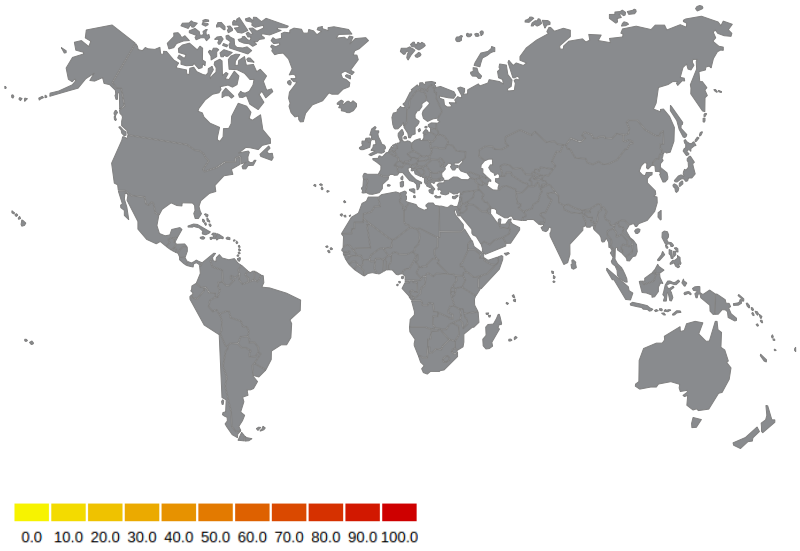
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\sysnative\imageres.dll
\Device\KsecDD

MUTEXES

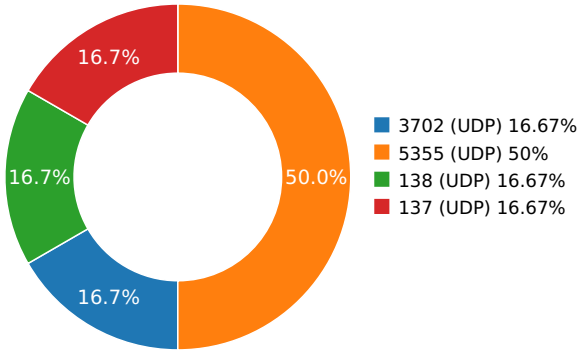
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.03070306778	Sandbox	224.0.0.252	5355
7.08414793015	Sandbox	192.168.56.255	137
7.17128109932	Sandbox	224.0.0.252	5355
7.593075037	Sandbox	239.255.255.250	3702
9.73562097549	Sandbox	224.0.0.252	5355
13.1710700989	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp_MEI22722\Zstandard\Backend_c.Cp310-Win_amd64.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 4ec296c5608d46afdb37048b920a676b **SHA-1 :** c94c21c9e9621940f59bcec2f6a576a991b42a03 **SHA-256 :** a0f31c62e0c1b25857330afa3d8c23b68d2e2b1d **SHA-512 :** 7c49668bc1e9cca2b07533ae7e1dfac27a6c660d **Size :** 525.312 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\LICENSE.APACHE	**Type :** ASCII text **MD5 :** 4e168cce331e5c827d4c2b68a6200e1b **SHA-1 :** de33ead2bee64352544ce0aa9e410c0c44fdf7d9 **SHA-256 :** aac73b3148f6d1d7111dbca32099f68d26c644c6 **SHA-512 :** f451048e81a49fbfa11b49de16ff46c52a8e3042d **Size :** 11.36 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_cffi_backend.Cp310-Win_amd64.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 6f1b90884343f717c5dc14f94ef5acea **SHA-1 :** cca1a4dcf7a32bf698e75d58c5f130fb3572e423 **SHA-256 :** 2093e7e4f5359b38f0819bdef8314fda332a1427f **SHA-512 :** e2c673b75162d3432bab497bad3f5f15a957191C **Size :** 181.248 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_hashlib.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** d856a545a960bf2dca1e2d9be32e5369 **SHA-1 :** 67a15ecf763cdc2c2aa458a521db8a48d816d91e **SHA-256 :** cd33f823e608d3bda759ad441f583a20fc019811 **SHA-512 :** 34a074025c8b28f54c01a7fd44700fdedb391f55b **Size :** 61.824 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_ssl.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 9ddb64354ef0b91c6999a4b244a0a011 **SHA-1 :** 86a9dc5ea931638699eb6d8d03355ad7992d2fee **SHA-256 :** e33b7a4aa5cdd5462ee66830636fdd38048575a4 **SHA-512 :** 4c86478861fa4220680a94699e7d55fbdc90d278 **Size :** 159.096 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_bz2.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** bbe89cf70b64f38c67b7bf23c0ea8a48 **SHA-1 :** 44577016e9c7b463a79b966b67c3ecc868957470 **SHA-256 :** 775fbc6e9a4c7e9710205157350f3d6141b5a9e8 **SHA-512 :** 3ee72ba60541116bbca1a62db64074276d40ad8 **Size :** 83.32 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Brotli_brotli.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 5cd8cbde51c687b96a732c6cab46b016 **SHA-1 :** 9584be1465af75937f9cff3c6609ce2f6228498f **SHA-256 :** 9d007f4dd7e138404aa849eb1afa8637b8d28606 **SHA-512 :** 1f9681c65f8f803d7e150c03a126ccee715e68003 **Size :** 838.144 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp_MEI22722\Python3.Dll	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** c17b7a4b853827f538576f4c3521c653 **SHA-1 :** 6115047d02fbbad4ff32afb4ebd439f5d529485a **SHA-256 :** d21e60f3dfbf2bab0cc8a06656721fa3347f026df **SHA-512 :** 8e08e702d69df6840781d174c4565e14a28022b **Size :** 64.896 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Certifi\Cacert.Pem	**Type :** ASCII text **MD5 :** 8d0619bfe30deadf6f21196f0f8d53d3 **SHA-1 :** e7abd65a8ccafeff6caf6a2ff98d27d24d87c9ad **SHA-256 :** b301535dca491d9814ea28faa320ac7a19d0f5d9 **SHA-512 :** 5a88e4a06b98832aaa9bbb89e382f6c7e9b65c5e **Size :** 278.952 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\Top_level.Txt	**Type :** ASCII text **MD5 :** e7274bd06ff93210298e7117d11ea631 **SHA-1 :** 7132c9ec1fd99924d658cc672f3afe98afefab8a **SHA-256 :** 28d693f929f62b8bb135a11b7ba9987439f7a960 **SHA-512 :** aa6021c4e60a6382630bebc1e16944f9b312359c **Size :** 0.013 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Unicodedata.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 4c8af8a30813e9380f5f54309325d6b8 **SHA-1 :** 169a80d8923fb28f89bc26ebf89ffe37f8545c88 **SHA-256 :** 4b6e3ba734c15ec789b5d7469a5097bd082bdfd **SHA-512 :** ea127779901b10953a2bf9233e20a4fab2fba6f97 **Size :** 1122.176 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\INSTALLER	**Type :** ASCII text **MD5 :** 365c9bfeb7d89244f2ce01c1de44cb85 **SHA-1 :** d7a03141d5d6b1e88b6b59ef08b6681df212c599 **SHA-256 :** ceebae7b8927a3227e5303cf5e0f1f7b34bb542a **SHA-512 :** d220d322a4053d84130567d626a9f7bb2fb8f0b8 **Size :** 0.004 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Bcrypt_bcrypt.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 03ef5e8da65667751e1fd3fa0c182d3e **SHA-1 :** 4608d1efca23143006c1338deda144a2f3bb8a16 **SHA-256 :** 3d1c66bdcb4fa0b8e917895e1b4d62ee14260ea **SHA-512 :** c094a3dfbd863726524c56dab2592b3513a3a8c4 **Size :** 301.568 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\WHEEL	**Type :** ASCII text **MD5 :** c20f485ec06558eb04b2edce8362fd4f **SHA-1 :** d621f40b4522e88fd3e56ebeaa6332c7bdf40bed **SHA-256 :** 005f333e44a4700866383a4bb757adf739b24782 **SHA-512 :** c701255a1793c5478f8b8ff7cbd86adb4fe232080 **Size :** 0.1 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\LICENSE.BSD	**Type :** ASCII text **MD5 :** 5ae30ba4123bc4f2fa49aa0b0dce887b **SHA-1 :** ea5b412c09f3b29ba1d81a61b878c5c16ffe69d8 **SHA-256 :** 602c4c7482de6479dd2e9793cda275e5e63d773 **SHA-512 :** ddbb20c80adbc8f4118c10d3e116a5cd6536f720 **Size :** 1.532 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp_MEI22722\Libssl-1_1.Dll	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 8769adafca3a6fc6ef26f01fd31afa84 **SHA-1 :** 38baef74bdd2e941ccd321f91bfd49dacc6a3cb6 **SHA-256 :** 2aebb73530d21a2273692a5a3d57235b770daf1 **SHA-512 :** fac22f1a2ffbfb4789bdeed476c8daf42547d40efe **Size :** 702.816 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Select.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** c119811a40667dca93dfe6faa418f47a **SHA-1 :** 113e792b7dcec4366fc273e80b1fc404c309074c **SHA-256 :** 8f27cd8c5071cb740a2191b3c599e99595b121f4 **SHA-512 :** 107257dbd8cf2607e4a1c7bef928a6f61ebdfc21b **Size :** 29.048 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_lzma.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 0a94c9f3d7728cf96326db3ab3646d40 **SHA-1 :** 8081df1dca4a8520604e134672c4be79eb202d14 **SHA-256 :** 0a70e8546fa6038029f2a3764e721ceebea41581 **SHA-512 :** 6f047f3bdaead121018623f52a35f7e8b38c58d3a **Size :** 157.56 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Base_library.Zip	**Type :** Zip archive data, at least v2.0 to extract **MD5 :** 524a85217dc9edc8c9efc73159ca955d **SHA-1 :** a4238cbde50443262d00a843ffe814435fb0f4e2 **SHA-256 :** 808549964adb09afafb410cdc030df4813c5c2a72 **SHA-512 :** f5a929b35a63f073bdc7600155ba2f0f262e6f60c **Size :** 831.92 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\LICENSE	**Type :** ASCII text **MD5 :** 8c3617db4fb6fae01f1d253ab91511e4 **SHA-1 :** e442040c26cd76d1b946822caf29011a51f75d6d **SHA-256 :** 3e0c7c091a948b82533ba98fd7cbb40432d6f1a9 **SHA-512 :** 77a1919e380730bcce5b55d76fbffba2f95874254 **Size :** 0.197 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Python310.Dll	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** deaf0c0cc3369363b800d2e8e756a402 **SHA-1 :** 3085778735dd8badad4e39df688139f4eed5f954 **SHA-256 :** 156cf2b64dd0f4d9bdb346b654a11300d6e9e15a **SHA-512 :** 5cac1d92af7ee18425b5ee8e7cd4e941a9ddffb4b **Size :** 4492.664 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_decimal.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 6339fa92584252c3b24e4cce9d73ef50 **SHA-1 :** dccda9b641125b16e56c5b1530f3d04e302325cd **SHA-256 :** 4ae6f6fb3992bb878416211221b3d62515e994d7 **SHA-512 :** 428b62591d4eba3a4e12f7088c990c48e30b6423 **Size :** 248.704 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_socket.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 0f5e64e33f4d328ef11357635707d154 **SHA-1 :** 8b6dcb4b9952b362f739a3f16ae96c44bea94a0e **SHA-256 :** 8af6d70d44bb9398733f88bcfb6d2085dd1a193c **SHA-512 :** 4be9febb583364da75b6fb3a43a8b50ee29ca8fc **Size :** 77.696 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp_MEI22722\Zstandard_cffi.Cp310-Win_amd64.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 117e86f2144e337b04c04949df435e8f **SHA-1 :** fffb49bd8a50368f25c014ed725f060eae6ff3d3 **SHA-256 :** 3ae3f79f0fa25e5978937c83fa77650a6ce2ae650 **SHA-512 :** 2e4fc563a11805add9eda9cc68f9d3f988d970d4(**Size :** 655.36 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Libcrypto-1_1.Dll	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 6f4b8eb45a965372156086201207c81f **SHA-1 :** 8278f9539463f0a45009287f0516098cb7a15406 **SHA-256 :** 976ce72efd0a8aeeb6e21ad441aa9138434314ea **SHA-512 :** 2c5c54842aba9c82fb9e7594ae9e264ac3cbdc2cc **Size :** 3441.504 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\VCRUNTIME140.Dll	**Type :** PE32+ executable (DLL) (console) x86-64, for MS Windows **MD5 :** 870fea4e961e2fbd00110d3783e529be **SHA-1 :** a948e65c6f73d7da4ffde4e8533c098a00cc7311 **SHA-256 :** 76fdb83fde238226b5bebaf3392ee562e2cb7ca8 **SHA-512 :** 0b636a3cdefa343eb4cb228b391bb657b5b4c20c **Size :** 109.392 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722_queue.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** 52d0a6009d3de40f4fa6ec61db98c45c **SHA-1 :** 5083a2aff5bcce07c80409646347c63d2a87bd25 **SHA-256 :** 007bcf19d9b036a7e73f5ef31f39bfb1910f72c9c1 **SHA-512 :** cd552a38efaa8720a342b60318f62320ce20c038 **Size :** 30.592 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography\Hazmat\Bindings_rust.Pyd	**Type :** PE32+ executable (DLL) (GUI) x86-64, for MS Windows **MD5 :** c43b06ff74532d3f019ec49b305b6691 **SHA-1 :** 536dbd74295e2de0fab50ae763d32e04e8dee4e4 **SHA-256 :** 66b292e36fdb53a3b827bb23959551d4772942d **SHA-512 :** 1f6af3f6abc231221c2dc708a6a838b5dbec5ee8e **Size :** 6596.608 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\METADATA	**Type :** ASCII text, with CRLF line terminators **MD5 :** 4e5169613d93ec27ee0b3a0e80db6640 **SHA-1 :** 7d721c24ead56b9cd623ed9b5e0811de9a71b85b **SHA-256 :** 855ed42caab9fbdcc6a95c098a02bc58c9035757 **SHA-512 :** 14179fca4596cbdf4201ed38e8c0866bcc67f334b **Size :** 5.308 Kilobytes.
C:\Users\User\AppData\Local\Temp_MEI22722\Cryptography-41.0.1.Dist-Info\RECORD	**Type :** ASCII text, with CRLF line terminators **MD5 :** e37c1ab144452fdb2ed9f66c119ae9c0 **SHA-1 :** d4a3c94df3fdcbe9eff8011123537db160f334a7 **SHA-256 :** 201644eed53b9ab5e903a8a9269d1e6f4eff6b4f2 **SHA-512 :** 0f94409ef84cb2fad2b4a45d0c42ed5a484444b4(**Size :** 15.24 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	d191af7816640acd232d85dff54294cf0890d15d6d5d2c0fdfaa95babccf9a6c.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
SHA1:	45b63e00c568632d21828d652ee538085ad64e11
MD5:	3affbe6f0688c8a598fef9d8bcef1c6b
First Seen Date:	2023-07-29 09:40:16.947451 (4 days ago)
Number Of Clients Seen:	4
Last Analysis Date:	2023-07-29 09:53:25.973789 (4 days ago)
Human Expert Analysis Date:	2023-07-30 11:36:23.817092 (3 days ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	4
File Type Enum	7
Debug Artifacts	[]
Number Of Sections	7
Trid	[]
Compilation Time Stamp	0x64C3AC48 [Fri Jul 28 11:53:44 2023 UTC]
Entry Point	0x14000afa0 (.text)
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
File Size	10348611
Ssdeep	
Sha256	d191af7816640acd232d85dff54294cf0890d15d6d5d2c0fdfaa95babccf9a6c
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x28710	0x28800	6.48667752666	e4f89af1ba6511882cb4cd14d9f6eca0
.rdata	0x2a000	0x1282e	0x12a00	5.81299986053	5caf5ab57d3fed70c8b6793b4ca01772
.data	0x3d000	0x103e8	0xe00	1.80114268406	8197d15b5af8fff7ec6022f8809b64c8
.pdata	0x4e000	0x20a0	0x2200	5.32574879678	77e2f2d72516a8aa1832e8298e54381f
_RDATA	0x51000	0x15c	0x200	2.7579156834	0ed86077474ad8a4a0621ecbc29cb84c
.rsrc	0x52000	0xf49c	0xf600	7.5555827686	2a561f84ac4c20f82b09919c46bf97cc
.reloc	0x62000	0x754	0x800	5.23933364424	7fed9a3addc55d51107d5af5a380ab8e

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 336392, u'sha256': u'7cccfafd00332ac9c9f6ac0112cc0653991eb169943919e55d05f3fa15929821', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 340144, u'sha256': u'd73c1848a067a0fd094423213dc1e855b5b29b0b441f0bcb315feb90d662972e', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 342360, u'sha256': u'5a008270f7254f5ca861e9936f4b5b7a23c04d63165895234fd1782bc03ec0e5', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 343744, u'sha256': u'3919b11194f130d310dfe08bdce2891c5b64f2703107f53a5a1cbc016fdb609f', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 38188}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 381932, u'sha256':

u'7ef5a24efde1748c0eb12c5817b14cfe1397ae968489a7824a269d02c8223cee', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 391572, u'sha256': u'c5536b396be6dcfc96f4e4f77cc7007b2a56730ee57598a6979cc1c1c71c920a', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 395836, u'sha256': u'ac2e25dc4a4f7bd96a0bcf3ea63cd1bcf26a6f6a05835e32f96ef99cb4323f30', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

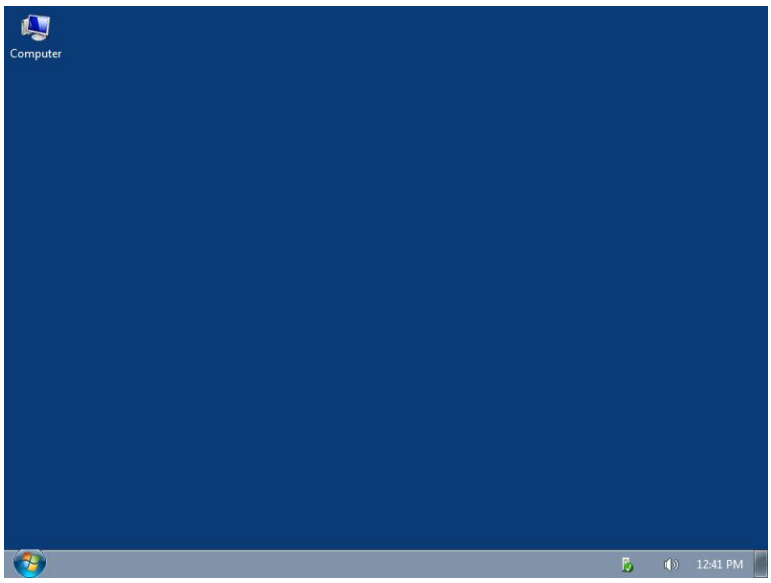
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 396964, u'sha256': u'f5b94a42f1c77c9eef858a0dfd656419fea900b00318c2c0bf49c2fce345d838', u'type': u'MS Windows icon resource - 7 icons, 48x48', u'size': 104}

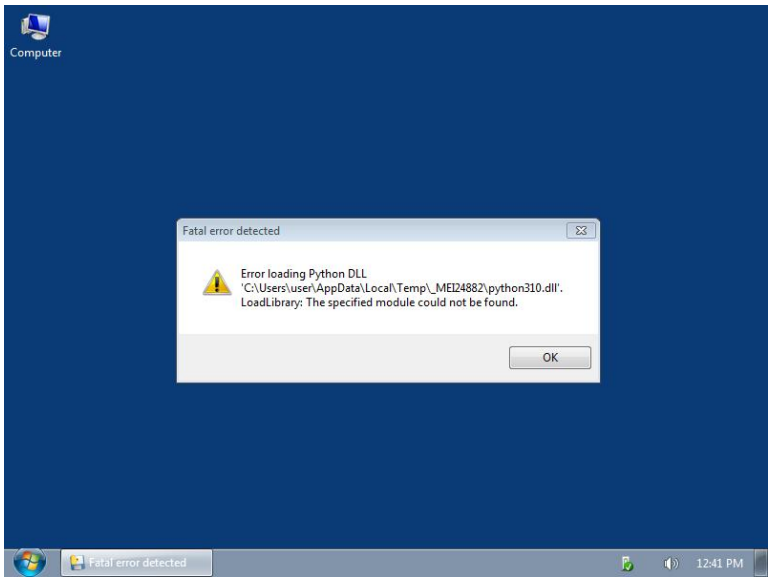
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 397068, u'sha256': u'94146f7cbbb2a5a4662325321c6d5d057c50f06308fbbb6f2c5a3bdaf0adbaac', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 1422}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS






Computer
12:41 PM