I'm not a bot

All screenshots are available in the full report All screenshots are available in the full report All screenshots are available in the full report You can’t perform that action at this time. You can’t perform that action at this time. Proactive Protection This file passed all security checks, but stay vigilant. New malware variants appear daily that can evade detection. Always verify files come from official sources and check digital signatures when available. Anti-Detection/Stealthyness Cryptographic Related Environment Awareness General An application crash occurred details Report process "WerFault.exe" was created by "keymaker.exe" source Monitored Target Calls an API typically used to load libraries details "keymaker.exe" called "LoadLibrary" with a parameter api-ms-win-core-synch-l1-2-0 (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter api-ms-win-core-fibers-l1-1-1 (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter api-ms-win-core-localization-l1-2-1 (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter kernel32 (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter NTDLL.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter KERNEL32.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter COMCTL32.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter USER32.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter SHLWAPI.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter SHELL32.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter GDI32.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter OLE32.DLL (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter api-ms-win-core-com-l1-1-0 (UID: 00000000-00005616) "keymaker.exe" called "LoadLibrary" with a parameter OLEAUT32.DLL (UID: 00000000-00005616) source API Call relevance 1/10 ATT&CK ID T1129 (Show technique in the MITRE ATT&CK™ matrix) Calls an API typically used to retrieve function addresses details "keymaker.exe" called "GetProcAddress" with a parameter InitializeCriticalSectionEx (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter FlsAlloc (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter FlsSetValue (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter FlsGetValue (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter LCMapStringEx (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter FlsFree (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter InitOnceExecuteOnce (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateEventExW (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateSemaphoreW (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateSemaphoreExW (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateThreadpoolTimer (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter SetThreadpoolTimer (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter WaitForThreadpoolTimerCallbacks (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CloseThreadpoolTimer (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateThreadpoolWait (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter SetThreadpoolWait (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CloseThreadpoolWait (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter FlushProcessWriteBuffers (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter FreeLibraryWhenCallbackReturns (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter GetCurrentProcessorNumber (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateSymbolicLinkW (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter GetCurrentPackageId (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter GetTickCount64 (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter GetFileInformationByHandleEx (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter SetFileInformationByHandle (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter GetSystemTimePreciseAsFileTime (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter InitializeConditionVariable (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter WakeConditionVariable (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter WakeAllConditionVariable (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter SleepConditionVariableCS (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter InitializeSRWLock (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter AcquireSRWLockExclusive (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter TryAcquireSRWLockExclusive (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter ReleaseSRWLockExclusive (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter SleepConditionVariableSRW (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateThreadpoolWork (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter SubmitThreadpoolWork (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CloseThreadpoolWork (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CompareStringEx (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter GetLocaleInfoEx (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter AreFileApisANSI (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CoTaskMemFree (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CoUninitialize (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CoTaskMemAlloc (UID: 00000000-00005616) "keymaker.exe" called "GetProcAddress" with a parameter CreateStreamOnHGlobal (UID: 00000000-00005616) source API Call relevance 1/10 ATT&CK ID T1106 (Show technique in the MITRE ATT&CK™ matrix) Contains ability to dynamically determine API calls Contains ability to execute Windows APIs details Found reference to API (Indicator: "MessageBoxA"; File: "keymaker.exe") Found reference to API (Indicator: "LoadLibraryA"; File: "keymaker.exe") Found reference to API (Indicator: "GetProcAddress"; File: "keymaker.exe") source File/Memory relevance 1/10 ATT&CK ID T1106 (Show technique in the MITRE ATT&CK™ matrix) Contains registry location strings details "SOFTWARE\BANDISOFT\BANDICAM" in Source: 00000000-00005616.00000000.66765.00400000.00000040.mdmp "SOFTWARE\BANDISOFT\BANDICAM\OPTION" in Source: 00000000-00005616.00000000.66765.00400000.00000040.mdmp source File/Memory relevance 1/10 ATT&CK ID T1012 (Show technique in the MITRE ATT&CK™ matrix) Creates mutants details "Bandicam v2.1.2.740" source Created Mutant relevance 3/10 Loads modules at runtime details "keymaker.exe" loaded module "API-MS-WIN-CORE-SYNCH-L1-2-0" at base 76f90000 "keymaker.exe" loaded module "API-MS-WIN-CORE-FIBERS-L1-1-1" at base 76f90000 "keymaker.exe" loaded module "API-MS-WIN-CORE-LOCALIZATION-L1-2-1" at base 76f90000 "keymaker.exe" loaded module "KERNEL32" at base 76870000 "keymaker.exe" loaded module "%WINDIR%\TEMP\VXOLE32.DLL" at base 72670000 "keymaker.exe" loaded module "NTDLL.DLL" at base 772b0000 "keymaker.exe" loaded module "KERNEL32.DLL" at base 76870000 "keymaker.exe" loaded module "COMCTL32.DLL" at base 74d50000 "keymaker.exe" loaded module "USER32.DLL" at base 76390000 "keymaker.exe" loaded module "SHLWAPI.DLL" at base 76700000 "keymaker.exe" loaded module "SHELL32.DLL" at base 75290000 "keymaker.exe" loaded module "GDI32.DLL" at base 76df0000 "keymaker.exe" loaded module "OLE32.DLL" at base 75960000 "keymaker.exe" loaded module "API-MS-WIN-CORE-COM-L1-1-0" at base 75ef0000 "keymaker.exe" loaded module "OLEAUT32.DLL" at base 76170000 "keymaker.exe" loaded module "%WINDIR%\SYSTEM32\UXTHEME.DLL" at base 74c20000 "keymaker.exe" loaded module "%WINDIR%\SYSTEM32\ASYCFILT.DLL" at base 71f80000 "keymaker.exe" loaded module "EXT-MS-WIN-KERNEL32-ERRORHANDLING-L1-1-0.DLL" at base 76870000 source API Call relevance 1/10 ATT&CK ID T1129 (Show technique in the MITRE ATT&CK™ matrix) Loads the Bcrypt module DLL Loads the RPC (Remote Procedure Call) module DLL Matched Compiler/Packer signature (DIE) details "keymaker.exe" was detected as "PESpin" and name: "Protector" "keymaker.exe" was detected as "Microsoft Linker" and name: "Linker" source Static Parser ATT&CK ID T1027 (Show technique in the MITRE ATT&CK™ matrix) PE file contains executable sections details "keymaker.exe" has an executable section named ".wkt0" "keymaker.exe" has an executable section named ".rsrc" source Static Parser relevance 1/10 PE file contains writable sections details "keymaker.exe" has an writable section named ".wkt0" "keymaker.exe" has an writable section named ".rsrc" source Static Parser PE file entrypoint instructions details "keymaker.exe" file has an entrypoint instructions - "jmp 0x4100d7,push 0xe860,add byte ptr [eax], al,mov ebx, dword ptr [esp],add ebx, 0x12,sub dword ptr [ebx], 0x6b1e8,dec byte ptr [ebx - 3],sub byte ptr [esp], 0x77,out 0x46, eax,add byte ptr [ebx], cl,in al, 0x74,sahf ,jne 0x4100fa,mov dword ptr [ecx + 0x7ad70473], 0x73812ff7,sbb dword ptr [edi], esi,inc ebx,mov bh, 0xf6,ret ,imul esi, dword ptr [edi - 0x70000], -0x1d,leave ,ret 8,mov dword ptr [0xff017268], eax,pop ebp,xor ecx, ecx,inc ecx,loop 0x410137,jmp 0x410129,ljmp 0xff0d:0xebeb01eb,call 0x41012f,ljmp 0xe2ff:0xbea835a,jmp 0x41013b," source Static Parser Reads information about supported languages details "keymaker.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE"; Key: "EMPTY") "keymaker.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE"; Key: "EN-US") "keymaker.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\EXTENDEDLOCALE"; Key: "EN-US") source Registry Access relevance 3/10 ATT&CK ID T1082 (Show technique in the MITRE ATT&CK™ matrix) Spawns new processes Spawns new processes that are not known child processes Uses 32 bit executable PE details "keymaker.exe" has flags like IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE source Static Parser Installation/Persistence Contains ability to load modules (API string) Opens registry keys details "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\CODEPAGE"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER\SEGMENT HEAP"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SOFTWARE\MICROSOFT\WOW64\X86"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\STATESEPARATION\REDIRECTIONMAP\KEYS"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\SAFEBOOT\OPTION"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\SRP\GP\DLL"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKLM\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\CODEIDENTIFIERS"; Key: ""; Value: "") "keymaker.exe" (Access type: "OPEN"; Path: "HKCU\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\CODEIDENTIFIERS"; Key: ""; Value: "") source Registry Access relevance 1/10 ATT&CK ID T1012 (Show technique in the MITRE ATT&CK™ matrix) Queries basic information of the specified process Queries registry keys details "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\CODEPAGE"; Key: "ACP"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\CODEPAGE"; Key: "OEMCP"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER"; Key: "RAISEEXCEPTIONONPOSSIBLEDEADLOCK"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER"; Key: "RESOURCEPOLICIES"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY"; Key: "57A6ED1A-79F7-5011-B242-4784E5620CF7"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WOW64\X86"; Key: "KEYMAKER.EXE"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WOW64\X86"; Key: ""; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY"; Key: "3C74AFB9-8D82-44E3-B52C-365DBF48382A"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY"; Key: "B749553B-D950-5E03-6282-3145A61B1002"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY"; Key: "05F95EFE-7F75-49C7-A994-60A55CC09571"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSAPPCOMPAT"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSUSERENABLED"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\CODEIDENTIFIERS"; Key: "TRANSPARENTENABLED"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\FILESYSTEM"; Key: "LONGPATHSENABLED"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY"; Key: "8CCCA27D-F1D8-4DDA-B5DD-339AEE937731"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\APPCOMPATFLAGS"; Key: "LOGFLAGS"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\WMI\SECURITY"; Key: "18608E62-A628-49D9-8C02-55972E097D24"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\APPCOMPATFLAGS"; Key: "SHOWDEBUGINFO"; Value: "") "keymaker.exe" (Access type: "QUERYVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\APPCOMPATFLAGS\SDBUPDATES"; Key: "SYSMAIN.SDB"; Value: "") source Registry Access relevance 1/10 ATT&CK ID T1012 (Show technique in the MITRE ATT&CK™ matrix) Reads files Touches files details "keymaker.exe" trying to touch file "%WINDIR%\SysWOW64\apphelp.dll" "keymaker.exe" trying to touch file "C:\keymaker.exe" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64tdll.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\kernel32.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\KernelBase.dll" "keymaker.exe" trying to touch file "C:\Windows\apppatch\sysmain.sdb" "keymaker.exe" trying to touch file "C:\Windows\apppatch\MergeSdbFilesSource\sysMerge.sdb" "keymaker.exe" trying to touch file "C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.22621.1635_none_6ebca75c88023f94\comctl32.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\win32u.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\ucrtbase.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\msvcp_win.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\gdi32full.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\gdi32.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\user32.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\msvcrt.dll" "keymaker.exe" trying to touch file "C:\Windows\SysWOW64\imm32.dll" source API Call relevance 1/10 ATT&CK ID T1083 (Show technique in the MITRE ATT&CK™ matrix) Tries to access non-existent files (executable) Network Related Found potential URL in binary/memory GETs files from a webserver (HTTPS) details GET /exp017/a5766fee-9478-488b-9fc0-64d1ad72c290-WindowsServices_Evoke/api/v1/tas HTTP/1.1Host: default.exp-tas.com Cache-Control: no-store no-cache X-PHOTOS-CALLERID: 9NMPJ99VJBWV X-EVOKE-RING: X-WINNEXT-RING: Public X-WINNEXT-TELEMETRYLEVEL: Basic X-WINNEXT-OSVERSION: 10.0.22621.0 X-WINNEXT-APPVERSION: 1.23092.158.0 X-WINNEXT-PLATFORM: Desktop X-WINNEXT-CANTAILOR: False X-MSEDGE-CLIENTID: {fe4289f0-6a0d-44ad-a249-527db813dcb0} X-WINNEXT-PUBDEVICEID: 36UTaMR5Mra1jEiOuip2QXJy2Ns7hzfP7l3bgBCDSdI= Accept-Encoding: gzip deflate br GET /v9.0/oemdiscovery?oemId=&scmId=&phoneManufacturerName=&smBiosManufacturerName=1iyvfQL9i&phoneDeviceModel=&smBiosDm=2MtRP8vo HTTP/1.1Accept-Encoding: gzip deflate Accept: */* TASIGNORE: YES MS-PreciseDeviceFamilyVersion: 281475124959811 8 User-Agen%WINDIR%\tore/22310.1401.8.0 MS-CV: KuaTBitsWUS6bmd6SaEQxA.1 Accept-Language: en-US Host: storeedgefd.dsx.mp.microsoft.com Connection: Keep-Alive source Network Traffic relevance 3/10 ATT&CK ID T1071.001 (Show technique in the MITRE ATT&CK™ matrix) Sends GET/POST requests (HTTPS) details Found HTTPS GET request to Found HTTPS GET request to source Network Traffic relevance 1/10 ATT&CK ID T1071.001 (Show technique in the MITRE ATT&CK™ matrix) Spyware/Information Retrieval System Security Contains ability to access device drivers details Found string "DriverData=%WINDIR%\System32\Drivers\DriverData" (Indicator: "\drivers\"; Source: "00000000-00005616.00000000.66765.004D0000.00000004.mdmp, 00000000-00005616.00000000.66765.02190000.00000004.mdmp") Found string "DriverData=C:\Windows\System32\Drivers\DriverData" (Indicator: "system32\drivers"; Source: "00000000-00005616.00000000.66765.004D0000.00000004.mdmp, 00000000-00005616.00000000.66765.02190000.00000004.mdmp") Found string "32\Drivers\Z" (Indicator: "\drivers\"; Source: "00000000-00005616.00000000.66765.004D0000.00000004.mdmp") Found string "DriverData=C:\Windows\System32\Drivers\DrivtPk" (Indicator: "\drivers\"; Source: "00000000-00005616.00000000.66765.004D0000.00000004.mdmp") Found string "DriverData=C:\Windows\System32\Drivers\DrivtPk" (Indicator: "system32\drivers"; Source: "00000000-00005616.00000000.66765.004D0000.00000004.mdmp") Found string "qvverData=C:\Windows\System32\Drivers\DriverData" (Indicator: "\drivers\"; Source: "00000000-00005616.00000000.66765.02190000.00000004.mdmp") Found string "qvverData=C:\Windows\System32\Drivers\DriverData" (Indicator: "system32\drivers"; Source: "00000000-00005616.00000000.66765.02190000.00000004.mdmp") source File/Memory relevance 1/10 ATT&CK ID T1543.003 (Show technique in the MITRE ATT&CK™ matrix) Unusual Characteristics Loading content, please wait... No relevant DNS requests were made. No relevant HTTP requests were made. No significant files were extracted. A process crash was detected during the runtime analysis Not all sources for indicator ID "registry-177" are available in the report Not all sources for indicator ID "registry-172" are available in the report Not all sources for indicator ID "api-263" are available in the report Enforcing malicious verdict, as a reliable source indicates high confidence