ID: 632535
Sample Name: null.exe
Cookbook: default.jbs
Time: 18:50:25
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

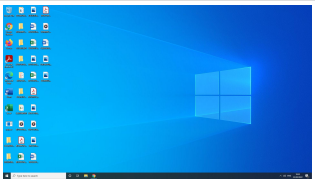
Windows Analysis Report

null.exe

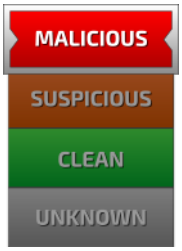
Overview

General Information

Sample Name:	null.exe
Analysis ID:	632535
MD5:	b4dd22013aefae..
SHA1:	177f953496b10a..
SHA256:	de14f22c88e552..
Infos:	



Detection

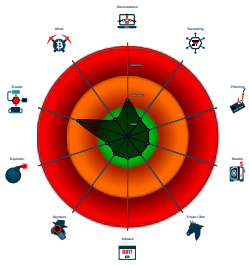


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Tries to load missing DLLs
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder…
- Detected potential crypto function
- Contains functionality to launch a pr…
- Sample execution stops while proce…
- Found evasive API chain (may stop…
- Launches processes in debugging m…
- Contains functionality to dynamicall…
- Found large amount of non-executed…

Classification



Process Tree

- **System is w10x64native**
- null.exe (PID: 6420 cmdline: "C:\Users\user\Desktop\null.exe" MD5: B4DD22013AEFAE6F721F0B67BE61DC91)
- null.exe (PID: 860 cmdline: C:\Users\user\Desktop\null.exe MD5: B4DD22013AEFAE6F721F0B67BE61DC91)
  - null.exe (PID: 4584 cmdline: -a MD5: B4DD22013AEFAE6F721F0B67BE61DC91)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

Copyright Joe Security LLC 2022

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

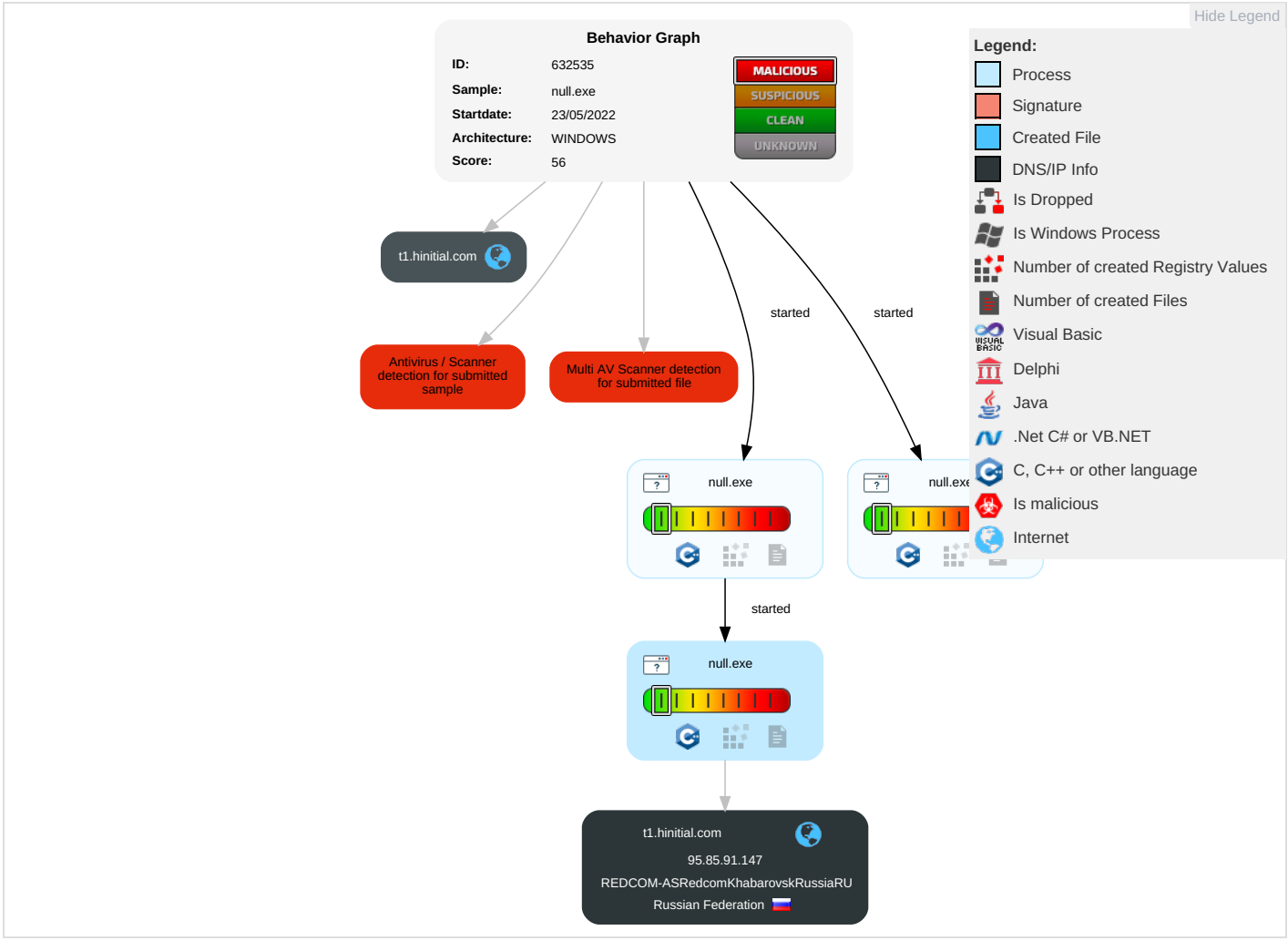
Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	2 Service Execution	1 Valid Accounts	1 Valid Accounts	1 Valid Accounts	OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	2 Native API	3 Windows Service	1 Access Token Manipulation	1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 DLL Side-Loading	3 Windows Service	1 Disable or Modify Tools	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Process Injection	1 Access Token Manipulation	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 DLL Side-Loading	1 Process Injection	LSA Secrets	4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

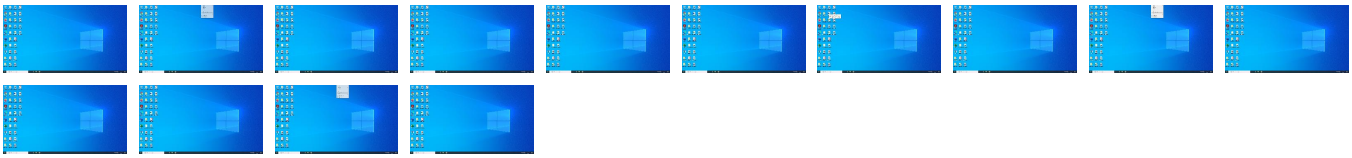
Behavior Graph



Screenshots

Thumbnails

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



Copyright Joe Security LLC 2022

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
null.exe	59%	Virustotal		Browse
null.exe	0%	Metadefender		Browse
null.exe	65%	ReversingLabs	Win64.Trojan.Lazy	
null.exe	100%	Avira	BDS/Redcap.gmumq	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
t1.hinitial.com	2%	Virustotal		Browse

URLs

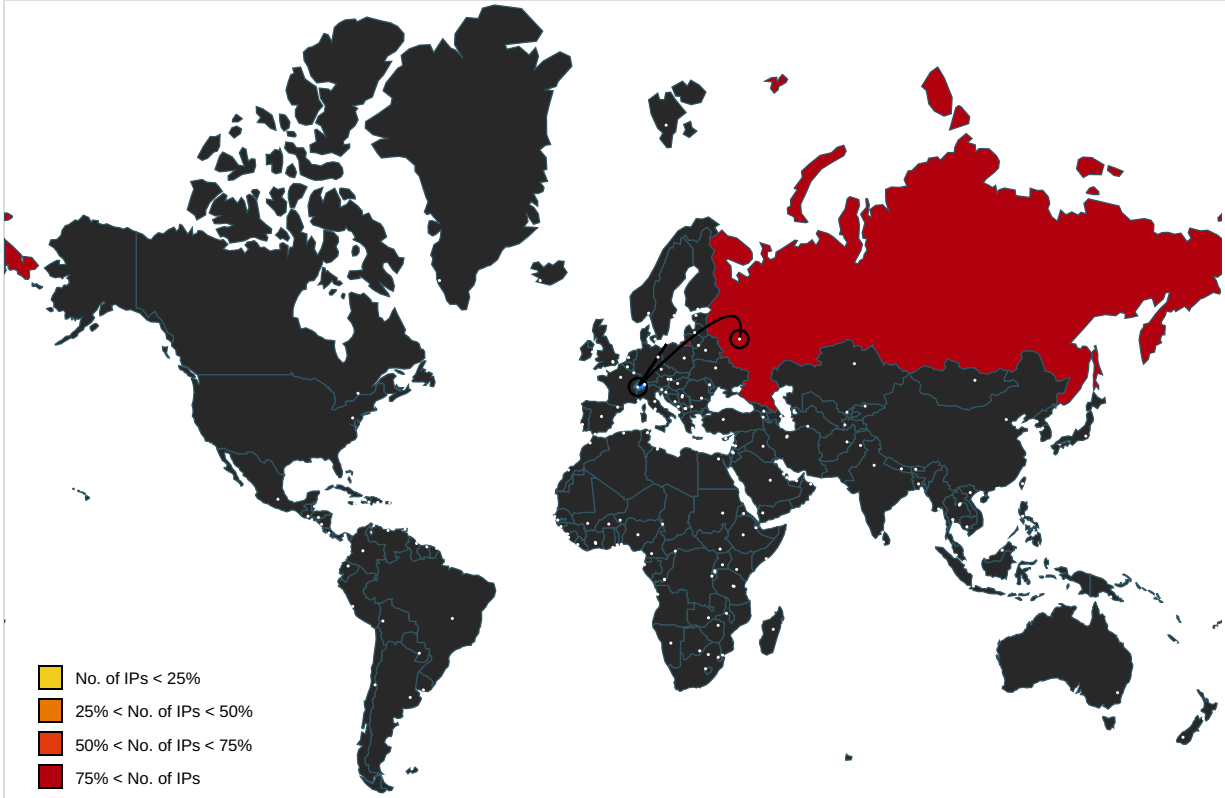
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t1.hinitial.com	95.85.91.147	true	false	• 2%, Virustotal, Browse	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.85.91.147	t1.hinitial.com	Russian Federation		8749	REDCOM-ASRedcomKhabarovskRussiaRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632535
Start date and time: 23/05/202218:50:25	2022-05-23 18:50:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	null.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	4
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

Copyright Joe Security LLC 2022

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.winEXE@4/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 86.7%) • Quality average: 67% • Quality standard deviation: 33.8%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 20.82.19.171
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, wd-prod-cp-eu-west-2-fe.westeurope.cloudapp.azure.com, wdcp.microsoft.com, wd-prod-cp.trafficmanager.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	6.044403199320442
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	null.exe
File size:	116224
MD5:	b4dd22013aefae6f721f0b67be61dc91
SHA1:	177f953496b10a4256431166c6247cc5a135e343
SHA256:	de14f22c88e552b61c62ab28d27a617fb8c0737350ca7c631de5680850282761
SHA512:	2141c4405f55921687dd7521d05bc26c0341ec7918fc578a61b0eded776b945365c2149829b6cb3b0d93c4d6334e47d15054dc50f99eea262ade9797fcf3f511
SSDEEP:	3072:V97LLBkDNOjkm0bDG8Y7FFiOTVsaJVYvL2H2nZQJ9A0:V97LLBymkmyNQ3TVsanYvk2I9n
TLSH:	6EB37C0B73B560F8D5A39238CCA65A0AD7B374760734878F07648A962F237A5AD3D731
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;x..Z...Z...Z...,...Z...,...Z...,...Z..."...Z...Z..VZ...,...Z...,...Z..Rich.Z.....PE..d...E.;a....."......6.

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x140007380
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x613B0045 [Fri Sep 10 06:50:45 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	61c1b6f838d2e5795c01ab4099a5158c

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
call 00007F8FC063D034h
dec eax
add esp, 28h
jmp 00007F8FC06364EBh
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax

Instruction
sub esp, 00000088h
dec eax
lea ecx, dword ptr [00015339h]
call dword ptr [0000DF03h]
dec eax
mov eax, dword ptr [00015424h]
dec eax
mov dword ptr [esp+58h], eax
inc ebp
xor eax, eax
dec eax
lea edx, dword ptr [esp+60h]
dec eax
mov ecx, dword ptr [esp+58h]
call 00007F8FC06409C0h
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007F8FC06366B3h
dec eax
mov dword ptr [esp+38h], 00000000h
dec eax
lea eax, dword ptr [esp+48h]
dec eax
mov dword ptr [esp+30h], eax
dec eax
lea eax, dword ptr [esp+40h]
dec eax
mov dword ptr [esp+28h], eax
dec eax
lea eax, dword ptr [000152E4h]
dec eax
mov dword ptr [esp+20h], eax
dec esp
mov ecx, dword ptr [esp+50h]
dec esp
mov eax, dword ptr [esp+58h]
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx
call 00007F8FC064096Eh
jmp 00007F8FC0636694h
dec eax
mov eax, dword ptr [esp+00000088h]
dec eax
mov dword ptr [000153B0h], eax
dec eax
lea eax, dword ptr [esp+00000088h]
dec eax
add eax, 08h
dec eax
mov dword ptr [0001533Dh], eax
dec eax
mov eax, dword ptr [00015396h]
dec eax
mov dword ptr [00015207h], eax

Rich Headers

Programming Language:	• [C++] VS2010 build 30319 • [LNK] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [ASM] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x19e5c	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x1f000	0xf60	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0x2b4	.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	0x15000	0x450	.rdata
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	0x1343a	0x13600	False	0.563936491935	data	6.35635961526	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x15000	0x5c38	0x5e00	False	0.361951462766	data	4.76231264876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1b000	0x3a98	0x1800	False	0.14501953125	data	2.15174800968	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x1f000	0xf60	0x1000	False	0.480712890625	data	4.91828664629	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x20000	0x4c4	0x600	False	0.330729166667	data	3.14527945205	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetExitCodeProcess, LocalReAlloc, CreateProcessA, TerminateProcess, FileTimeToSystemTime, ReadFile, GetModuleFileNameW, GetSystemDirectoryA, MultiByteToWideChar, GetFileSizeEx, GetStartupInfoA, FindFirstFileA, GetLastError, GetProcAddress, RemoveDirectoryA, CopyFileA, Sleep, LoadLibraryA, LocalAlloc, MoveFileA, CreateEventW, WaitForMultipleObjects, CreatePipe, GetModuleFileNameA, FindNextFileA, WTSGetActiveConsoleSessionId, CloseHandle, FileTimeToLocalFileTime, GetCurrentProcessId, LocalFree, DeleteFileA, LocalFileTimeToFileTime, WideCharToMultiByte, WriteFile, SetFileTime, FormatMessageA, GetTickCount, GetLogicalDrives, SetEvent, GetCurrentProcess, SystemTimeToFileTime, FreeLibrary, PeekNamedPipe, CreateFileA, GetComputerNameA, FindClose, GetSystemDefaultLangID, RaiseException, FlushFileBuffers, HeapSize, CreateFileW, LoadLibraryW, WriteConsoleW, SetFilePointer, RtlPcToFileHeader, GetStringTypeW, GetSystemTimeAsFileTime, QueryPerformanceCounter, DeleteCriticalSection, GetStartupInfoW, SetHandleCount, HeapFree, HeapAlloc, GetFileAttributesA, HeapReAlloc, GetCommandLineW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, EncodePointer, FlsGetValue, FlsSetValue, FlsFree, SetLastError, GetCurrentThreadId, FlsAlloc, DecodePointer, RtlUnwindEx, SetStdHandle, EnterCriticalSection, InitializeCriticalSectionAndSpinCount, LeaveCriticalSection, GetFileType, GetConsoleCP, GetConsoleMode, HeapSetInformation, GetVersion, HeapCreate, GetModuleHandleW, ExitProcess, GetStdHandle, LCMapStringW, FreeEnvironmentStringsW, GetEnvironmentStringsW
ADVAPI32.dll	CryptDestroyKey, CryptEncrypt, SetServiceStatus, CryptImportKey, DuplicateTokenEx, SetTokenInformation, CreateProcessAsUserW, CryptReleaseContext, RegisterServiceCtrlHandlerA, CryptSetKeyParam, CryptAcquireContextW, StartServiceCtrlDispatcherA, OpenProcessToken, CryptDecrypt
SHELL32.dll	SHCreateDirectoryExA
ole32.dll	CoInitialize
WS2_32.dll	recvfrom, inet_addr, htonl, WSAGetLastError, WSAStartup, setsockopt, sendto, WSACleanup, socket, closesocket, gethostbyname, htons, ntohs
USERENV.dll	CreateEnvironmentBlock, DestroyEnvironmentBlock

Copyright Joe Security LLC 2022

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:52:19.486927986 CEST	58910	53	192.168.11.20	1.1.1.1
May 23, 2022 18:52:19.500576973 CEST	53	58910	1.1.1.1	192.168.11.20

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 23, 2022 18:52:19.501262903 CEST	192.168.11.20	95.85.91.147	278e		Echo
May 23, 2022 18:52:19.722810030 CEST	95.85.91.147	192.168.11.20	2f8e		Echo Reply
May 23, 2022 18:52:20.734555960 CEST	192.168.11.20	95.85.91.147	278d		Echo
May 23, 2022 18:52:20.955913067 CEST	95.85.91.147	192.168.11.20	2f8d		Echo Reply
May 23, 2022 18:52:21.969005108 CEST	192.168.11.20	95.85.91.147	278c		Echo
May 23, 2022 18:52:22.190438986 CEST	95.85.91.147	192.168.11.20	2f8c		Echo Reply
May 23, 2022 18:52:23.205174923 CEST	192.168.11.20	95.85.91.147	278b		Echo
May 23, 2022 18:52:23.426640034 CEST	95.85.91.147	192.168.11.20	2f8b		Echo Reply
May 23, 2022 18:52:24.436856031 CEST	192.168.11.20	95.85.91.147	278a		Echo
May 23, 2022 18:52:24.658402920 CEST	95.85.91.147	192.168.11.20	2f8a		Echo Reply
May 23, 2022 18:52:25.671168089 CEST	192.168.11.20	95.85.91.147	2789		Echo
May 23, 2022 18:52:25.892827034 CEST	95.85.91.147	192.168.11.20	2f89		Echo Reply
May 23, 2022 18:52:26.905476093 CEST	192.168.11.20	95.85.91.147	2788		Echo
May 23, 2022 18:52:27.126847029 CEST	95.85.91.147	192.168.11.20	2f88		Echo Reply
May 23, 2022 18:52:28.139565945 CEST	192.168.11.20	95.85.91.147	2787		Echo
May 23, 2022 18:52:28.361217976 CEST	95.85.91.147	192.168.11.20	2f87		Echo Reply
May 23, 2022 18:52:29.373480082 CEST	192.168.11.20	95.85.91.147	2786		Echo
May 23, 2022 18:52:29.594908953 CEST	95.85.91.147	192.168.11.20	2f86		Echo Reply
May 23, 2022 18:52:30.607522011 CEST	192.168.11.20	95.85.91.147	2785		Echo
May 23, 2022 18:52:30.829972029 CEST	95.85.91.147	192.168.11.20	2f85		Echo Reply
May 23, 2022 18:52:31.843360901 CEST	192.168.11.20	95.85.91.147	2784		Echo
May 23, 2022 18:52:32.064838886 CEST	95.85.91.147	192.168.11.20	2f84		Echo Reply
May 23, 2022 18:52:33.075835943 CEST	192.168.11.20	95.85.91.147	2783		Echo
May 23, 2022 18:52:33.297228098 CEST	95.85.91.147	192.168.11.20	2f83		Echo Reply
May 23, 2022 18:52:34.309854031 CEST	192.168.11.20	95.85.91.147	2782		Echo
May 23, 2022 18:52:34.531219006 CEST	95.85.91.147	192.168.11.20	2f82		Echo Reply
May 23, 2022 18:52:35.544363976 CEST	192.168.11.20	95.85.91.147	2781		Echo
May 23, 2022 18:52:35.766043901 CEST	95.85.91.147	192.168.11.20	2f81		Echo Reply
May 23, 2022 18:52:36.777883053 CEST	192.168.11.20	95.85.91.147	2780		Echo
May 23, 2022 18:52:36.999372005 CEST	95.85.91.147	192.168.11.20	2f80		Echo Reply
May 23, 2022 18:52:38.012209892 CEST	192.168.11.20	95.85.91.147	277f		Echo
May 23, 2022 18:52:38.234091997 CEST	95.85.91.147	192.168.11.20	2f7f		Echo Reply
May 23, 2022 18:52:39.246475935 CEST	192.168.11.20	95.85.91.147	277e		Echo
May 23, 2022 18:52:39.467701912 CEST	95.85.91.147	192.168.11.20	2f7e		Echo Reply
May 23, 2022 18:52:40.481132030 CEST	192.168.11.20	95.85.91.147	277d		Echo
May 23, 2022 18:52:40.703804016 CEST	95.85.91.147	192.168.11.20	2f7d		Echo Reply
May 23, 2022 18:52:41.714379072 CEST	192.168.11.20	95.85.91.147	277c		Echo
May 23, 2022 18:52:41.936547995 CEST	95.85.91.147	192.168.11.20	2f7c		Echo Reply
May 23, 2022 18:52:42.948646069 CEST	192.168.11.20	95.85.91.147	277b		Echo
May 23, 2022 18:52:43.169866085 CEST	95.85.91.147	192.168.11.20	2f7b		Echo Reply
May 23, 2022 18:52:44.185075998 CEST	192.168.11.20	95.85.91.147	277a		Echo
May 23, 2022 18:52:44.406735897 CEST	95.85.91.147	192.168.11.20	2f7a		Echo Reply
May 23, 2022 18:52:45.416727066 CEST	192.168.11.20	95.85.91.147	2779		Echo
May 23, 2022 18:52:45.638020039 CEST	95.85.91.147	192.168.11.20	2f79		Echo Reply
May 23, 2022 18:52:46.651015997 CEST	192.168.11.20	95.85.91.147	2778		Echo
May 23, 2022 18:52:46.872421980 CEST	95.85.91.147	192.168.11.20	2f78		Echo Reply
May 23, 2022 18:52:47.885001898 CEST	192.168.11.20	95.85.91.147	2777		Echo

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 23, 2022 18:52:48.106790066 CEST	95.85.91.147	192.168.11.20	2f77		Echo Reply
May 23, 2022 18:52:49.119822979 CEST	192.168.11.20	95.85.91.147	2776		Echo
May 23, 2022 18:52:49.341362953 CEST	95.85.91.147	192.168.11.20	2f76		Echo Reply
May 23, 2022 18:52:50.369240046 CEST	192.168.11.20	95.85.91.147	2775		Echo
May 23, 2022 18:52:50.590873003 CEST	95.85.91.147	192.168.11.20	2f75		Echo Reply
May 23, 2022 18:52:51.603307962 CEST	192.168.11.20	95.85.91.147	2774		Echo
May 23, 2022 18:52:51.828000069 CEST	95.85.91.147	192.168.11.20	2f74		Echo Reply
May 23, 2022 18:52:52.837022066 CEST	192.168.11.20	95.85.91.147	2773		Echo
May 23, 2022 18:52:53.058506012 CEST	95.85.91.147	192.168.11.20	2f73		Echo Reply
May 23, 2022 18:52:54.071105003 CEST	192.168.11.20	95.85.91.147	2772		Echo
May 23, 2022 18:52:54.292603970 CEST	95.85.91.147	192.168.11.20	2f72		Echo Reply
May 23, 2022 18:52:55.305073977 CEST	192.168.11.20	95.85.91.147	2771		Echo
May 23, 2022 18:52:55.526648045 CEST	95.85.91.147	192.168.11.20	2f71		Echo Reply
May 23, 2022 18:52:56.540024042 CEST	192.168.11.20	95.85.91.147	2770		Echo
May 23, 2022 18:52:56.761620998 CEST	95.85.91.147	192.168.11.20	2f70		Echo Reply
May 23, 2022 18:52:57.779529095 CEST	192.168.11.20	95.85.91.147	276f		Echo
May 23, 2022 18:52:58.000955105 CEST	95.85.91.147	192.168.11.20	2f6f		Echo Reply
May 23, 2022 18:52:59.007271051 CEST	192.168.11.20	95.85.91.147	276e		Echo
May 23, 2022 18:52:59.228715897 CEST	95.85.91.147	192.168.11.20	2f6e		Echo Reply
May 23, 2022 18:53:00.241580009 CEST	192.168.11.20	95.85.91.147	276d		Echo
May 23, 2022 18:53:00.463193893 CEST	95.85.91.147	192.168.11.20	2f6d		Echo Reply
May 23, 2022 18:53:01.475564957 CEST	192.168.11.20	95.85.91.147	276c		Echo
May 23, 2022 18:53:01.696916103 CEST	95.85.91.147	192.168.11.20	2f6c		Echo Reply
May 23, 2022 18:53:02.709750891 CEST	192.168.11.20	95.85.91.147	276b		Echo
May 23, 2022 18:53:02.931293011 CEST	95.85.91.147	192.168.11.20	2f6b		Echo Reply
May 23, 2022 18:53:03.943738937 CEST	192.168.11.20	95.85.91.147	276a		Echo
May 23, 2022 18:53:04.165222883 CEST	95.85.91.147	192.168.11.20	2f6a		Echo Reply
May 23, 2022 18:53:05.178240061 CEST	192.168.11.20	95.85.91.147	2769		Echo
May 23, 2022 18:53:05.399604082 CEST	95.85.91.147	192.168.11.20	2f69		Echo Reply
May 23, 2022 18:53:06.412662983 CEST	192.168.11.20	95.85.91.147	2768		Echo
May 23, 2022 18:53:06.634666920 CEST	95.85.91.147	192.168.11.20	2f68		Echo Reply
May 23, 2022 18:53:07.646497011 CEST	192.168.11.20	95.85.91.147	2767		Echo
May 23, 2022 18:53:07.867818117 CEST	95.85.91.147	192.168.11.20	2f67		Echo Reply
May 23, 2022 18:53:08.880140066 CEST	192.168.11.20	95.85.91.147	2766		Echo
May 23, 2022 18:53:09.101727962 CEST	95.85.91.147	192.168.11.20	2f66		Echo Reply
May 23, 2022 18:53:10.114310026 CEST	192.168.11.20	95.85.91.147	2765		Echo
May 23, 2022 18:53:10.335840940 CEST	95.85.91.147	192.168.11.20	2f65		Echo Reply
May 23, 2022 18:53:11.348572969 CEST	192.168.11.20	95.85.91.147	2764		Echo
May 23, 2022 18:53:11.570347071 CEST	95.85.91.147	192.168.11.20	2f64		Echo Reply
May 23, 2022 18:53:12.582515001 CEST	192.168.11.20	95.85.91.147	2763		Echo
May 23, 2022 18:53:12.803739071 CEST	95.85.91.147	192.168.11.20	2f63		Echo Reply
May 23, 2022 18:53:13.817154884 CEST	192.168.11.20	95.85.91.147	2762		Echo
May 23, 2022 18:53:14.038719893 CEST	95.85.91.147	192.168.11.20	2f62		Echo Reply
May 23, 2022 18:53:15.050946951 CEST	192.168.11.20	95.85.91.147	2761		Echo
May 23, 2022 18:53:15.272712946 CEST	95.85.91.147	192.168.11.20	2f61		Echo Reply
May 23, 2022 18:53:16.284835100 CEST	192.168.11.20	95.85.91.147	2760		Echo
May 23, 2022 18:53:16.506175041 CEST	95.85.91.147	192.168.11.20	2f60		Echo Reply
May 23, 2022 18:53:17.519197941 CEST	192.168.11.20	95.85.91.147	275f		Echo
May 23, 2022 18:53:17.740711927 CEST	95.85.91.147	192.168.11.20	2f5f		Echo Reply
May 23, 2022 18:53:18.754992008 CEST	192.168.11.20	95.85.91.147	275e		Echo
May 23, 2022 18:53:18.976475954 CEST	95.85.91.147	192.168.11.20	2f5e		Echo Reply
May 23, 2022 18:53:19.987246037 CEST	192.168.11.20	95.85.91.147	275d		Echo
May 23, 2022 18:53:20.208791971 CEST	95.85.91.147	192.168.11.20	2f5d		Echo Reply
May 23, 2022 18:53:21.221251011 CEST	192.168.11.20	95.85.91.147	275c		Echo
May 23, 2022 18:53:21.442929029 CEST	95.85.91.147	192.168.11.20	2f5c		Echo Reply
May 23, 2022 18:53:22.455698967 CEST	192.168.11.20	95.85.91.147	275b		Echo
May 23, 2022 18:53:22.677161932 CEST	95.85.91.147	192.168.11.20	2f5b		Echo Reply
May 23, 2022 18:53:23.689799070 CEST	192.168.11.20	95.85.91.147	275a		Echo
May 23, 2022 18:53:23.911335945 CEST	95.85.91.147	192.168.11.20	2f5a		Echo Reply

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 23, 2022 18:53:24.923518896 CEST	192.168.11.20	95.85.91.147	2759		Echo
May 23, 2022 18:53:25.144808054 CEST	95.85.91.147	192.168.11.20	2f59		Echo Reply
May 23, 2022 18:53:26.157876015 CEST	192.168.11.20	95.85.91.147	2758		Echo
May 23, 2022 18:53:26.379144907 CEST	95.85.91.147	192.168.11.20	2f58		Echo Reply
May 23, 2022 18:53:27.391848087 CEST	192.168.11.20	95.85.91.147	2757		Echo
May 23, 2022 18:53:27.613234043 CEST	95.85.91.147	192.168.11.20	2f57		Echo Reply
May 23, 2022 18:53:28.625880003 CEST	192.168.11.20	95.85.91.147	2756		Echo
May 23, 2022 18:53:28.847733021 CEST	95.85.91.147	192.168.11.20	2f56		Echo Reply
May 23, 2022 18:53:29.860153913 CEST	192.168.11.20	95.85.91.147	2755		Echo
May 23, 2022 18:53:30.081793070 CEST	95.85.91.147	192.168.11.20	2f55		Echo Reply
May 23, 2022 18:53:31.094122887 CEST	192.168.11.20	95.85.91.147	2754		Echo
May 23, 2022 18:53:31.315434933 CEST	95.85.91.147	192.168.11.20	2f54		Echo Reply
May 23, 2022 18:53:32.328387022 CEST	192.168.11.20	95.85.91.147	2753		Echo
May 23, 2022 18:53:32.550025940 CEST	95.85.91.147	192.168.11.20	2f53		Echo Reply
May 23, 2022 18:53:33.562515020 CEST	192.168.11.20	95.85.91.147	2752		Echo
May 23, 2022 18:53:33.784257889 CEST	95.85.91.147	192.168.11.20	2f52		Echo Reply
May 23, 2022 18:53:34.796909094 CEST	192.168.11.20	95.85.91.147	2751		Echo
May 23, 2022 18:53:35.018826008 CEST	95.85.91.147	192.168.11.20	2f51		Echo Reply
May 23, 2022 18:53:36.030724049 CEST	192.168.11.20	95.85.91.147	2750		Echo
May 23, 2022 18:53:36.252176046 CEST	95.85.91.147	192.168.11.20	2f50		Echo Reply
May 23, 2022 18:53:37.264580965 CEST	192.168.11.20	95.85.91.147	274f		Echo
May 23, 2022 18:53:37.486119032 CEST	95.85.91.147	192.168.11.20	2f4f		Echo Reply
May 23, 2022 18:53:38.499068975 CEST	192.168.11.20	95.85.91.147	274e		Echo
May 23, 2022 18:53:38.720771074 CEST	95.85.91.147	192.168.11.20	2f4e		Echo Reply
May 23, 2022 18:53:39.732932091 CEST	192.168.11.20	95.85.91.147	274d		Echo
May 23, 2022 18:53:39.954252005 CEST	95.85.91.147	192.168.11.20	2f4d		Echo Reply
May 23, 2022 18:53:40.966793060 CEST	192.168.11.20	95.85.91.147	274c		Echo
May 23, 2022 18:53:41.188664913 CEST	95.85.91.147	192.168.11.20	2f4c		Echo Reply
May 23, 2022 18:53:42.201052904 CEST	192.168.11.20	95.85.91.147	274b		Echo
May 23, 2022 18:53:42.422633886 CEST	95.85.91.147	192.168.11.20	2f4b		Echo Reply
May 23, 2022 18:53:43.435338020 CEST	192.168.11.20	95.85.91.147	274a		Echo
May 23, 2022 18:53:43.657475948 CEST	95.85.91.147	192.168.11.20	2f4a		Echo Reply
May 23, 2022 18:53:44.669305086 CEST	192.168.11.20	95.85.91.147	2749		Echo
May 23, 2022 18:53:44.890914917 CEST	95.85.91.147	192.168.11.20	2f49		Echo Reply
May 23, 2022 18:53:45.903264999 CEST	192.168.11.20	95.85.91.147	2748		Echo
May 23, 2022 18:53:46.124619007 CEST	95.85.91.147	192.168.11.20	2f48		Echo Reply
May 23, 2022 18:53:47.137665987 CEST	192.168.11.20	95.85.91.147	2747		Echo
May 23, 2022 18:53:47.358968019 CEST	95.85.91.147	192.168.11.20	2f47		Echo Reply
May 23, 2022 18:53:48.371918917 CEST	192.168.11.20	95.85.91.147	2746		Echo
May 23, 2022 18:53:48.593400002 CEST	95.85.91.147	192.168.11.20	2f46		Echo Reply
May 23, 2022 18:53:49.606010914 CEST	192.168.11.20	95.85.91.147	2745		Echo
May 23, 2022 18:53:49.830382109 CEST	95.85.91.147	192.168.11.20	2f45		Echo Reply
May 23, 2022 18:53:50.839708090 CEST	192.168.11.20	95.85.91.147	2744		Echo
May 23, 2022 18:53:51.061114073 CEST	95.85.91.147	192.168.11.20	2f44		Echo Reply
May 23, 2022 18:53:52.073793888 CEST	192.168.11.20	95.85.91.147	2743		Echo
May 23, 2022 18:53:52.295233965 CEST	95.85.91.147	192.168.11.20	2f43		Echo Reply
May 23, 2022 18:53:53.308331013 CEST	192.168.11.20	95.85.91.147	2742		Echo
May 23, 2022 18:53:53.529952049 CEST	95.85.91.147	192.168.11.20	2f42		Echo Reply
May 23, 2022 18:53:54.542073011 CEST	192.168.11.20	95.85.91.147	2741		Echo
May 23, 2022 18:53:54.763437986 CEST	95.85.91.147	192.168.11.20	2f41		Echo Reply
May 23, 2022 18:53:55.776276112 CEST	192.168.11.20	95.85.91.147	2740		Echo
May 23, 2022 18:53:55.997728109 CEST	95.85.91.147	192.168.11.20	2f40		Echo Reply
May 23, 2022 18:53:57.010705948 CEST	192.168.11.20	95.85.91.147	273f		Echo
May 23, 2022 18:53:57.232147932 CEST	95.85.91.147	192.168.11.20	2f3f		Echo Reply
May 23, 2022 18:53:58.244329929 CEST	192.168.11.20	95.85.91.147	273e		Echo
May 23, 2022 18:53:58.466092110 CEST	95.85.91.147	192.168.11.20	2f3e		Echo Reply
May 23, 2022 18:53:59.478722095 CEST	192.168.11.20	95.85.91.147	273d		Echo
May 23, 2022 18:53:59.700299978 CEST	95.85.91.147	192.168.11.20	2f3d		Echo Reply
May 23, 2022 18:54:00.712460995 CEST	192.168.11.20	95.85.91.147	273c		Echo

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 23, 2022 18:54:00.933804989 CEST	95.85.91.147	192.168.11.20	2f3c		Echo Reply
May 23, 2022 18:54:01.947798967 CEST	192.168.11.20	95.85.91.147	273b		Echo
May 23, 2022 18:54:02.169105053 CEST	95.85.91.147	192.168.11.20	2f3b		Echo Reply
May 23, 2022 18:54:03.181072950 CEST	192.168.11.20	95.85.91.147	273a		Echo
May 23, 2022 18:54:03.402707100 CEST	95.85.91.147	192.168.11.20	2f3a		Echo Reply
May 23, 2022 18:54:04.414951086 CEST	192.168.11.20	95.85.91.147	2739		Echo
May 23, 2022 18:54:04.637978077 CEST	95.85.91.147	192.168.11.20	2f39		Echo Reply
May 23, 2022 18:54:05.649126053 CEST	192.168.11.20	95.85.91.147	2738		Echo
May 23, 2022 18:54:05.870557070 CEST	95.85.91.147	192.168.11.20	2f38		Echo Reply
May 23, 2022 18:54:06.883045912 CEST	192.168.11.20	95.85.91.147	2737		Echo
May 23, 2022 18:54:07.104404926 CEST	95.85.91.147	192.168.11.20	2f37		Echo Reply
May 23, 2022 18:54:08.117283106 CEST	192.168.11.20	95.85.91.147	2736		Echo
May 23, 2022 18:54:08.339112997 CEST	95.85.91.147	192.168.11.20	2f36		Echo Reply
May 23, 2022 18:54:09.351306915 CEST	192.168.11.20	95.85.91.147	2735		Echo
May 23, 2022 18:54:09.572669983 CEST	95.85.91.147	192.168.11.20	2f35		Echo Reply
May 23, 2022 18:54:10.585688114 CEST	192.168.11.20	95.85.91.147	2734		Echo
May 23, 2022 18:54:10.807246923 CEST	95.85.91.147	192.168.11.20	2f34		Echo Reply
May 23, 2022 18:54:11.819575071 CEST	192.168.11.20	95.85.91.147	2733		Echo
May 23, 2022 18:54:12.041218042 CEST	95.85.91.147	192.168.11.20	2f33		Echo Reply
May 23, 2022 18:54:13.053560019 CEST	192.168.11.20	95.85.91.147	2732		Echo
May 23, 2022 18:54:13.274827957 CEST	95.85.91.147	192.168.11.20	2f32		Echo Reply
May 23, 2022 18:54:14.297705889 CEST	192.168.11.20	95.85.91.147	2731		Echo
May 23, 2022 18:54:14.519192934 CEST	95.85.91.147	192.168.11.20	2f31		Echo Reply
May 23, 2022 18:54:15.521795034 CEST	192.168.11.20	95.85.91.147	2730		Echo
May 23, 2022 18:54:15.743238926 CEST	95.85.91.147	192.168.11.20	2f30		Echo Reply
May 23, 2022 18:54:16.755970955 CEST	192.168.11.20	95.85.91.147	272f		Echo
May 23, 2022 18:54:16.977569103 CEST	95.85.91.147	192.168.11.20	2f2f		Echo Reply
May 23, 2022 18:54:17.990052938 CEST	192.168.11.20	95.85.91.147	272e		Echo
May 23, 2022 18:54:18.211795092 CEST	95.85.91.147	192.168.11.20	2f2e		Echo Reply
May 23, 2022 18:54:19.224370003 CEST	192.168.11.20	95.85.91.147	272d		Echo
May 23, 2022 18:54:19.445794106 CEST	95.85.91.147	192.168.11.20	2f2d		Echo Reply
May 23, 2022 18:54:20.458304882 CEST	192.168.11.20	95.85.91.147	272c		Echo
May 23, 2022 18:54:20.679930925 CEST	95.85.91.147	192.168.11.20	2f2c		Echo Reply
May 23, 2022 18:54:21.692289114 CEST	192.168.11.20	95.85.91.147	272b		Echo
May 23, 2022 18:54:21.913667917 CEST	95.85.91.147	192.168.11.20	2f2b		Echo Reply
May 23, 2022 18:54:22.925997972 CEST	192.168.11.20	95.85.91.147	272a		Echo
May 23, 2022 18:54:23.147197008 CEST	95.85.91.147	192.168.11.20	2f2a		Echo Reply
May 23, 2022 18:54:24.160736084 CEST	192.168.11.20	95.85.91.147	2729		Echo
May 23, 2022 18:54:24.382256031 CEST	95.85.91.147	192.168.11.20	2f29		Echo Reply
May 23, 2022 18:54:25.395235062 CEST	192.168.11.20	95.85.91.147	2728		Echo
May 23, 2022 18:54:25.616441011 CEST	95.85.91.147	192.168.11.20	2f28		Echo Reply
May 23, 2022 18:54:26.628535032 CEST	192.168.11.20	95.85.91.147	2727		Echo

DNS Queries

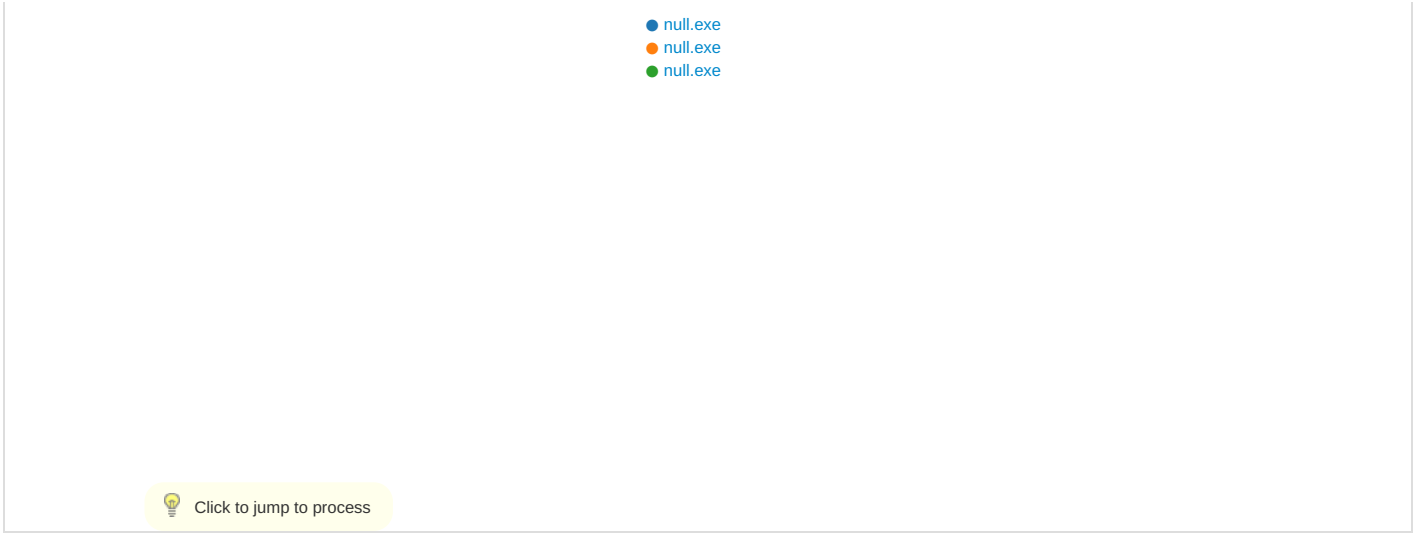
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 18:52:19.486927986 CEST	192.168.11.20	1.1.1.1	0x22a6	Standard query (0)	t1.hinitial.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 18:52:19.500576973 CEST	1.1.1.1	192.168.11.20	0x22a6	No error (0)	t1.hinitial.com		95.85.91.147	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: null.exe PID: **6420**, Parent PID: **5060**

General	
Target ID:	1
Start time:	18:52:17
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\null.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\null.exe"
Imagebase:	0x7ff7a43a0000
File size:	116224 bytes
MD5 hash:	B4DD22013AEFAE6F721F0B67BE61DC91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: null.exe PID: **860**, Parent PID: **916**

General	
Target ID:	2
Start time:	18:52:17
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\null.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\null.exe
Imagebase:	0x7ff7a43a0000
File size:	116224 bytes
MD5 hash:	B4DD22013AEFAE6F721F0B67BE61DC91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: null.exe PID: **4584**, Parent PID: **860**

General

Copyright Joe Security LLC 2022

Target ID:	3
Start time:	18:52:17
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\null.exe
Wow64 process (32bit):	false
Commandline:	-a
Imagebase:	0x7ff7a43a0000
File size:	116224 bytes
MD5 hash:	B4DD22013AEFAE6F721F0B67BE61DC91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly