ID: 800679
Sample Name:
promiscdetect.exe
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 18:03:39
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

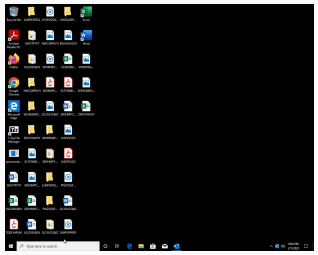
Windows Analysis Report

promiscdetect.exe

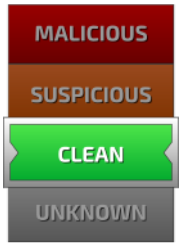
Overview

General Information

Sample Name:	promiscdetect.exe
Analysis ID:	800679
MD5:	70ebb2dee3c5…
SHA1:	7fab635c38960..
SHA256:	6684d2613ad5…



Detection

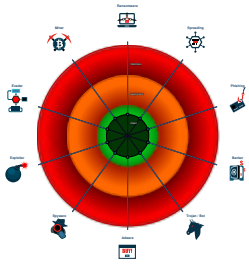


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Uses 32bit PE files
- Program does not show much activi…

Classification



Process Tree

- **System is w10x64_ra**
- promiscdetect.exe (PID: 6596 cmdline: C:\Users\alfredo\Desktop\promiscdetect.exe MD5: 70EBB2DEE3C5F7296E877CA515B61C57)
  - conhost.exe (PID: 6604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

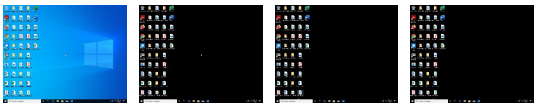
Mitre Att&ck Matrix

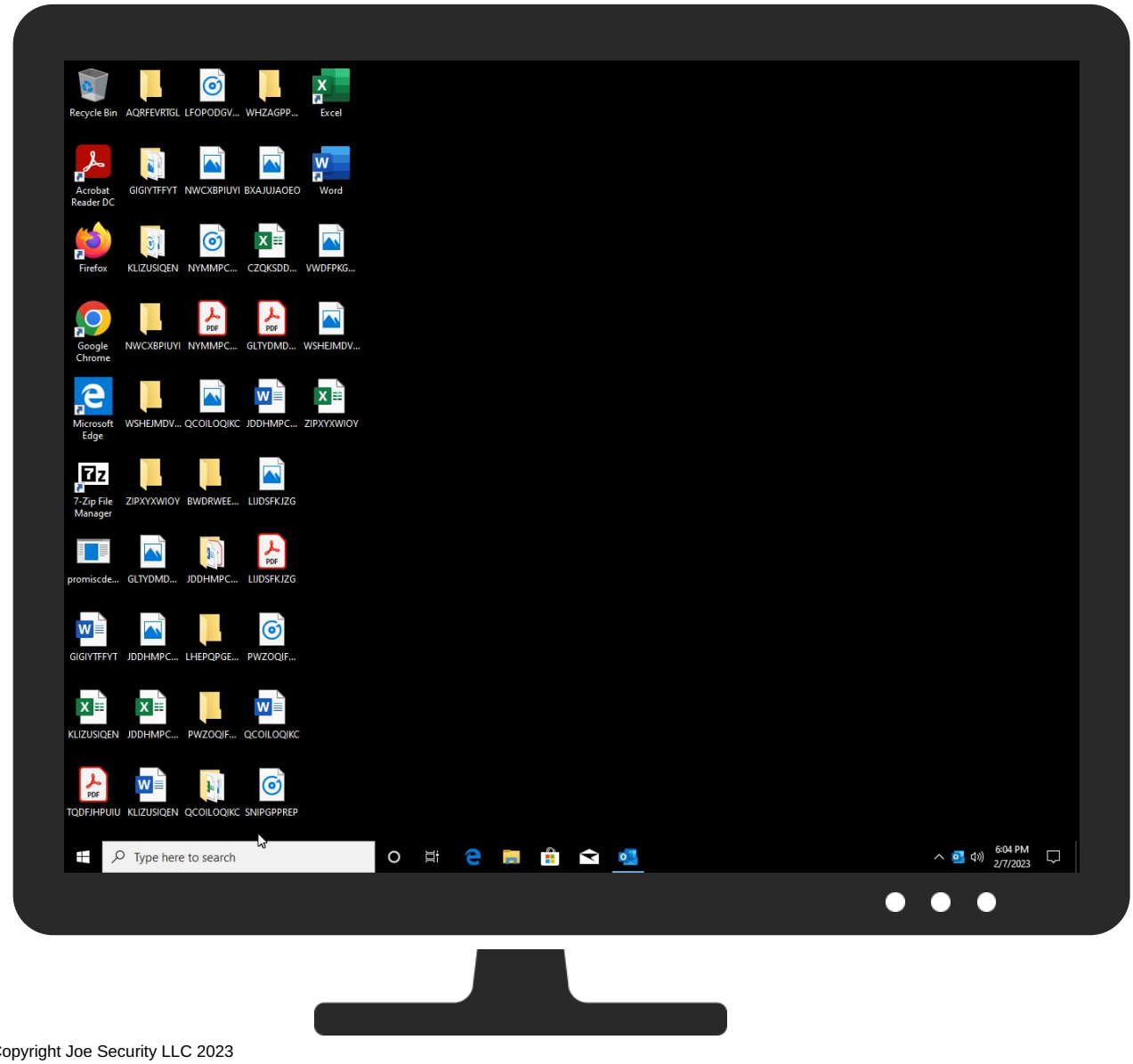
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	1 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

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
promiscdetect.exe	0%	ReversingLabs		
promiscdetect.exe	4%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800679
Start date and time:	2023-02-07 18:03:39 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	6
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample file name:	promiscdetect.exe

Detection:	CLEAN
Classification:	clean1.winEXE@2/1@0/0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, SIHClient.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.68, 20.190.159.2, 20.190.159.75, 40.126.31.69, 40.126.31.71, 20.190.159.64, 20.190.159.0, 20.190.159.23
- Excluded domains from analysis (whitelisted): prda.aadg.msidentity.com, slscr.update.microsoft.com, login.live.com, www.tm.lg.prod.aadmsa.akadns.net, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

\Device\ConDrv

Process:	C:\Users\alfredo\Desktop\promiscdetect.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.780157612175779
Encrypted:	false
SSDEEP:	
MD5:	D519C7983BC73F34F43A0E827C7AD0BF
SHA1:	8FF0F83652B9A22552B891CE61E403ADFCBFB67D
SHA-256:	76DE34994B86055464EB74F4E813B5C0FBC47BCDC4CF3BACAB235DD7680A84BA
SHA-512:	C3682CF3521C5E7EED067CF25BF0D9E20478F39F9CDC87644AA718D0AFDA5A24C75AF77C8E8CF68D1EE837565B03093317025ABFBD1F36F897FBB899646983B
Malicious:	false
Reputation:	low
Preview:	..PromiscDetect 1.1 - Copyright (c) 2019, Arne Vidstrom.. - https://vidstromlabs.com/freetools/promiscdetect/....Adapter name:.... - Intel(R) PRO/1000 MT Network Connection....Warning: Cannot open the adapter....Adapter name:.... - vmxnet3 Ethernet Adapter....Warning: Cannot open the adapter....Adapter name:.... - Intel(R) 82574L Gigabit Network Connection....Active filter for the adapter:.... - Directed (capture packets directed to this computer).. - Multicast (capture multicast packets for groups the computer is a member of).. - Broadcast (capture broadcast packets)....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.602306051800529
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	promiscdetect.exe
File size:	305152
MD5:	70ebb2dee3c5f7296e877ca515b61c57
SHA1:	7fab635c38960d4bfcd457243547cb8b57fcf62b
SHA256:	6684d2613ad59b6abaaff5972b2e6cdebece1e0f31c118cff96c7a2c18edfd97
SHA512:	aeb77a807f889cd35a69e4b7f1e3fdd27d9a9b6ed8cb98150c48f0243002723d7ea401929a77bb6c7a527cd70debf7a21efccd43d874ced5336a1720e47e145e
SSDEEP:	6144:2xC/66rPEmzw+sZmKAu864AESDca6od6iN5782cdiKG:2K66rPEmzw+sZmKAu864AESDca6oi2OM
TLSH:	AA546D10B981C032C67338310779E2B24DADB9312D645B9FA39C1A795F74591EA3AF2F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ...d.fLd.fLd.fL..eMn.fL..cM..fL..bMv.fL..cMA.fL..bMu.fL..eMu.fL..gMa.fLd.gL2.fL..bMe.fL...Le.fL..dMe.fLRichd.fL.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4018fb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x5CD92A01 [Mon May 13 08:25:37 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	63873711b7f8f1e20490708a4de6fb02

Entrypoint Preview

Instruction
call 00007F86DC66E71Dh
jmp 00007F86DC66DDECh
push ebp
mov ebp, esp
push 00000000h
call dword ptr [00440024h]
push dword ptr [ebp+08h]
call dword ptr [00440020h]
push C0000409h
call dword ptr [00440028h]
push eax
call dword ptr [0044002Ch]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call 00007F86DC6A9399h
test eax, eax
je 00007F86DC66DFD7h
push 00000002h
pop ecx
int 29h
mov dword ptr [00449AD0h], eax
mov dword ptr [00449ACCh], ecx
mov dword ptr [00449AC8h], edx
mov dword ptr [00449AC4h], ebx
mov dword ptr [00449AC0h], esi
mov dword ptr [00449ABCh], edi
mov word ptr [00449AE8h], ss
mov word ptr [00449ADCh], cs
mov word ptr [00449AB8h], ds
mov word ptr [00449AB4h], es
mov word ptr [00449AB0h], fs
mov word ptr [00449AACh], gs

Instruction
pushfd
pop dword ptr [00449AE0h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [00449AD4h], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [00449AD8h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [00449AE4h], eax
mov eax, dword ptr [ebp-00000324h]
mov dword ptr [00449A20h], 00010001h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x48494	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4b000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4c000	0x215c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x47520	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x47578	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x40000	0x160	.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	0x3e6b8	0x3e800	False	0.43704296875	COM executable for DOS	6.611142808606846	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x40000	0x8c86	0x8e00	False	0.4478708186619718	DOS executable (COM, 0x8C-variant)	5.106579823501425	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x49000	0x1c7c	0xa00	False	0.180859375	data	2.5187772506764334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x4b000	0x1e0	0x200	False	0.53125	data	4.7137725829467545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4c000	0x215c	0x2200	False	0.7933134191176471	data	6.662687903150661	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x4b060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	WriteConsoleW, DeviceIoControl, CreateFileA, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, InterlockedPushEntrySList, InterlockedFlushSList, RtlUnwind, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, EncodePointer, RaiseException, ExitProcess, GetModuleHandleExW, GetStdHandle, WriteFile, GetModuleFileNameW, GetCommandLineA, GetCommandLineW, HeapAlloc, HeapFree, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetFileType, GetCurrentThread, OutputDebugStringW, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, SetStdHandle, GetStringTypeW, GetProcessHeap, SetConsoleCtrlHandler, FlushFileBuffers, GetConsoleCP, GetConsoleMode, GetFileSizeEx, SetFilePointerEx, HeapSize, HeapReAlloc, CloseHandle, ReadFile, ReadConsoleW, CreateFileW, DecodePointer
ADVAPI32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey, RegEnumKeyExA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States