ID: 1459120
Sample Name:
Wo0CkmOz64.exe
Cookbook: default.jbs
Time: 21:17:12
Date: 18/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

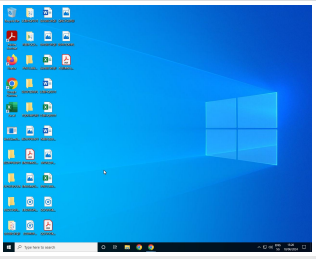
Windows Analysis Report

Wo0CkmOz64.exe

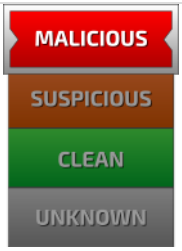
Overview

General Information

Sample name:	Wo0CkmOz64.exerenamed because original name is a hash value
Original sample name:	06b81c8edd7f6..
Analysis ID:	1459120
MD5:	06b81c8edd7f6..
SHA1:	af4ffbf3510bb2...
SHA256:	65082d1a97a4...
Tags:	32 exe trojan
Infos:	



Detection



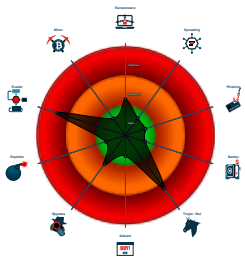
PureLog Stealer

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected PureLog Stealer
- .NET source code contains method …
- .NET source code contains potentia…
- .NET source code contains very larg…
- AI detected suspicious sample
- Machine Learning detection for sam…
- Tries to detect sandboxes and other…
- Yara detected Costura Assembly Lo…
- Allocates memory with a write watch…
- Binary contains a suspicious time s…

Classification



Process Tree

- **System is w10x64**
- Wo0CkmOz64.exe (PID: 2752 cmdline: "C:\Users\user\Desktop\Wo0CkmOz64.exe" MD5: 06B81C8EDD7F620513A06E3A5CC11483)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.3380383003.000000001BBA0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.3379202075.000000001B690000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
00000000.00000002.3376338658.0000000012F41000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Wo0CkmOz64.exe.1bba0000.7.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.Wo0CkmOz64.exe.1b690000.6.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
0.2.Wo0CkmOz64.exe.1b690000.6.raw.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
0.2.Wo0CkmOz64.exe.130312b8.5.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
0.2.Wo0CkmOz64.exe.130312b8.5.raw.unpack	JoeSecurity_PureLogStealer	Yara detected PureLog Stealer	Joe Security	
Click to see the 6 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- AI detected suspicious sample
- Machine Learning detection for sample

System Summary

- .NET source code contains very large array initializations

Data Obfuscation

- .NET source code contains method to dynamically call methods (often used by packers)
- .NET source code contains potential unpacker
- Yara detected Costura Assembly Loader

Malware Analysis System Evasion

- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information

Yara detected PureLog Stealer

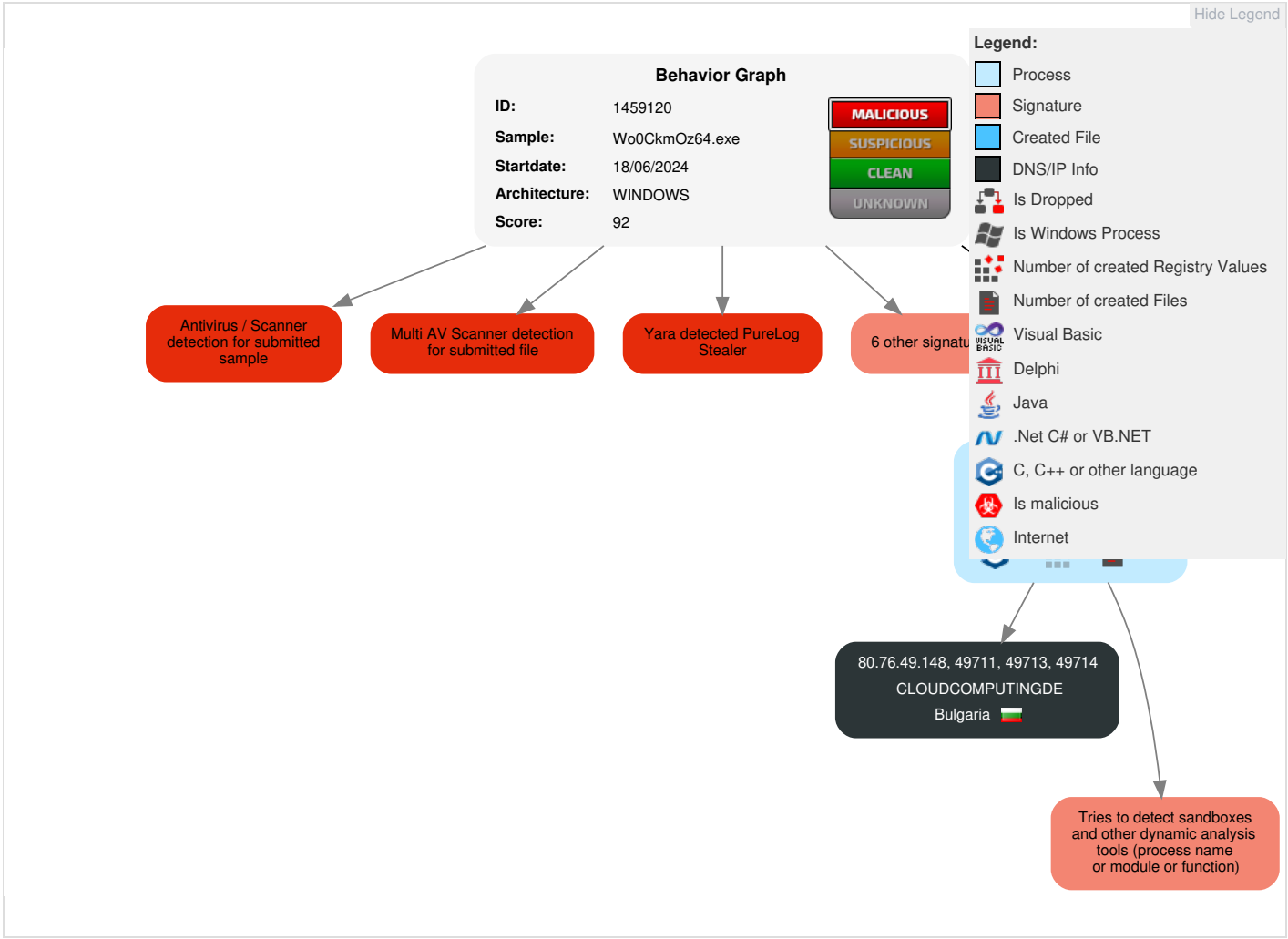
Remote Access Functionality

Yara detected PureLog Stealer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	3 1 Virtualization/Sandbox Evasion	LSASS Memory	3 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Steganography	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	2 Obfuscated Files or Information	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	2 2 Software Packing	LSA Secrets	Internet Connection Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Timestomp	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Remote System Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery

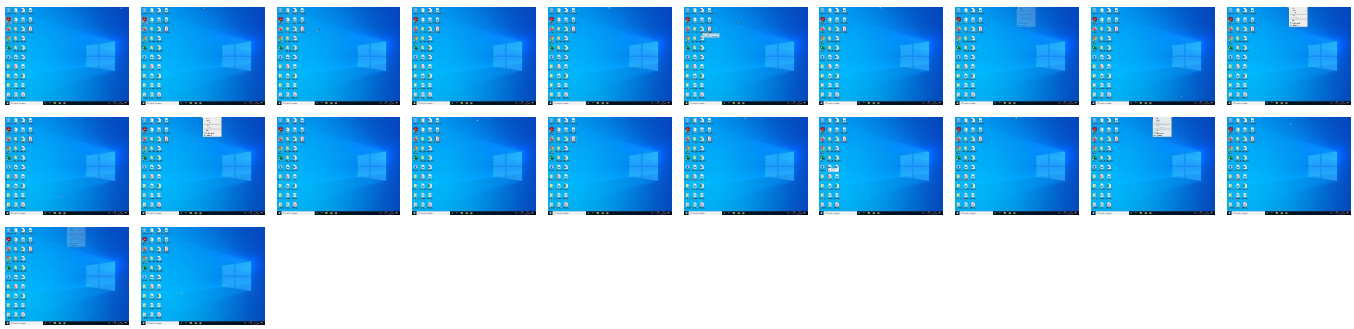
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Wo0CkmOz64.exe	71%	ReversingLabs	ByteCode-MSIL.Trojan.PureLogStealer	
Wo0CkmOz64.exe	100%	Avira	TR/Dropper.Gen	
Wo0CkmOz64.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://github.com/mgravell/protobuf-netJ	0%	Avira URL Cloud	safe	
http://https://github.com/mgravell/protobuf-neti	0%	Avira URL Cloud	safe	
http://https://github.com/mgravell/protobuf-net	0%	Avira URL Cloud	safe	
http://https://stackoverflow.com/q/14436606/23354	0%	Avira URL Cloud	safe	
http://https://stackoverflow.com/q/2152978/23354	0%	Avira URL Cloud	safe	
http://https://stackoverflow.com/q/11564914/23354;	0%	Avira URL Cloud	safe	

Domains and IPs

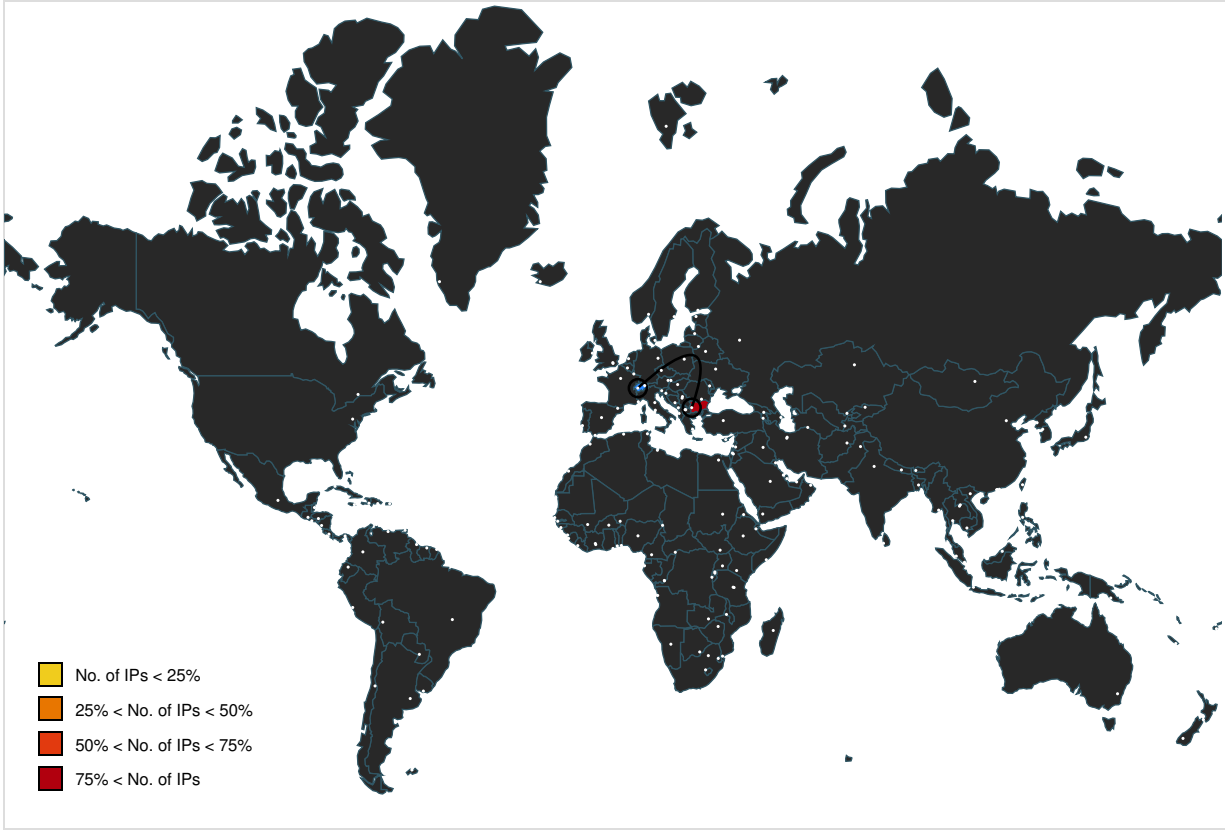
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-net	Wo0CkmOz64.exe, 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3371838921.0000000002BB0000.00000004.08000000.00040000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3376338658.000000001336B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/mgravell/protobuf-neti	Wo0CkmOz64.exe, 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3371838921.0000000002BB0000.00000004.08000000.00040000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3376338658.000000001336B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackoverflow.com/q/14436606/23354	Wo0CkmOz64.exe, 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3371838921.0000000002BB0000.00000004.08000000.00040000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3371913837.0000000002C11000.00000004.00000800.00020000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3376338658.000000001336B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/mgravell/protobuf-netJ	Wo0CkmOz64.exe, 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3371838921.0000000002BB0000.00000004.08000000.00040000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3376338658.000000001336B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackoverflow.com/q/11564914/23354;	Wo0CkmOz64.exe, 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3371838921.0000000002BB0000.00000004.08000000.00040000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3376338658.000000001336B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackoverflow.com/q/2152978/23354	Wo0CkmOz64.exe, 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3371838921.0000000002BB0000.00000004.08000000.00040000.00000000.sdmp, Wo0CkmOz64.exe, 00000000.00000002.3376338658.000000001336B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.76.49.148	unknown	Bulgaria		43659	CLOUDCOMPUTINGDE	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1459120
Start date and time:	2024-06-18 21:17:12 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	8
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	Wo0CkmOz64.exerenamed because original name is a hash value
Original Sample Name:	06b81c8edd7f620513a06e3a5cc11483.exe
Detection:	MAL
Classification:	mal92.troj.evad.winEXE@1/0@0/1
EGA Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target Wo0CkmOz64.exe, PID 2752 because it is empty
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: Wo0CkmOz64.exe

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) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.998288715406636
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Wo0CkmOz64.exe
File size:	856'064 bytes

MD5:	06b81c8edd7f620513a06e3a5cc11483
SHA1:	af4ffbf3510bb2e86387d26a6de309736548b340
SHA256:	65082d1a97a4636a529d3a52248ec1eed728fa78c1a3b3e34986e0378b393f1c
SHA512:	9d80d9208d778779538cf5075b4018dc8b8d037a9d07c961ce2389580290df050929876d1adc2489f7dc5f6c1466cde7d21b9152185e88ba0601e4dd2da4aec7
SSDEEP:	24576:fI0eDXhXsbQSa0t2xiewR2rpXN/L+9+dClWdD9:AVebQzxieHpXNL+jWdD
TLSH:	8E05336341660B90EC3B31B91B5CBB85D3B4F45DB278AB7184FD3745D6C2D4C8A2A8E8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0.....&/... ...@....@.. .....@.....

File Icon

Icon Hash:	00928e8e8686b000

Static PE Info

General

Entrypoint:	0x402f26
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xC8E3E1A2 [Tue Oct 20 00:00:34 2076 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
popfd
mov ah, 28h
xor edi, dword ptr [ebx+1A3F4A74h]
add dword ptr [ebp-2Ah], edx
mov ah, FBh
mov ebp, 50AC891Eh
push ecx
int D0h
popfd
mov eax, dword ptr [E5F0278Dh]
inc ebp
or dword ptr [eax], ecx
fld tbyte ptr [edi+125D0849h]
cmp al, C9h
add ecx, dword ptr [ebx-16h]
xchg eax, esi
push cs
retn FD36h
insd

Instruction
mov edi, ebp
xchg eax, edx
sbb dl, byte ptr [eax]
inc eax
salc
scasd
add dword ptr [ecx+ecx*8], 11CB4B64h
cmp eax, C89BE90Dh
out dx, eax
scasd
add byte ptr [edx-346D90F2h], ch

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2ed4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x56c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2eb8	0x1c	.text
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd05a0	0xd0600	770641f1a98083bf31fa95fdbdd86bf1	False	0.9987686056538693	data	7.999487700871465	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x56c	0x600	8a873b0a97c1a8a85796cbb4935c6f9c	False	0.3997395833333333	data	3.9339981650904186	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	0xc	0x200	34aa1c7f786d5445ac690bf61d2e9e0f	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_VERSION	0xd4090	0x2dc	data			0.43306010928961747
RT_MANIFEST	0xd437c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.5489795918367347

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2024 21:18:09.141510963 CEST	49711	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:09.146845102 CEST	7702	49711	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:09.146953106 CEST	49711	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:10.540179014 CEST	7702	49711	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:10.540246010 CEST	49711	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:10.549874067 CEST	49711	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:10.554729939 CEST	7702	49711	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:10.560682058 CEST	49713	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:10.566210032 CEST	7702	49713	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:10.566281080 CEST	49713	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:11.982278109 CEST	7702	49713	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:11.982376099 CEST	49713	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:11.982599974 CEST	49713	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:11.983155012 CEST	49714	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:11.987298012 CEST	7702	49713	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:11.987919092 CEST	7702	49714	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:11.987993956 CEST	49714	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.382674932 CEST	7702	49714	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.382740021 CEST	49714	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.382854939 CEST	49714	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.383271933 CEST	49715	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.388106108 CEST	7702	49714	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.388565063 CEST	7702	49715	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.388863087 CEST	49715	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.396214008 CEST	7702	49715	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.396260977 CEST	49715	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.396333933 CEST	49715	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.396646976 CEST	49716	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.401057005 CEST	7702	49715	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.401371002 CEST	7702	49716	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.401473045 CEST	49716	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.409975052 CEST	7702	49716	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.410023928 CEST	49716	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.991096973 CEST	49716	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.991787910 CEST	49717	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:13.996259928 CEST	7702	49716	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.996879101 CEST	7702	49717	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:13.997111082 CEST	49717	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:14.323818922 CEST	49717	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:14.329365015 CEST	7702	49717	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:14.329411983 CEST	49717	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:14.334270000 CEST	7702	49717	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:15.399308920 CEST	7702	49717	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:15.399378061 CEST	49717	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:15.399513006 CEST	49717	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:15.399935961 CEST	49718	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:15.405038118 CEST	7702	49717	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:15.405102968 CEST	7702	49718	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:15.405189991 CEST	49718	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:15.581182003 CEST	49718	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:15.586077929 CEST	7702	49718	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:15.586124897 CEST	49718	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:15.593799114 CEST	7702	49718	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:16.790262938 CEST	7702	49718	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:16.790333986 CEST	49718	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:16.790457964 CEST	49718	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:16.790992022 CEST	49719	7702	192.168.2.6	80.76.49.148

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 18, 2024 21:18:16.800076962 CEST	7702	49718	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:16.801033020 CEST	7702	49719	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:16.801131964 CEST	49719	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:17.002578020 CEST	49719	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:17.009890079 CEST	7702	49719	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:17.009975910 CEST	49719	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:17.019483089 CEST	7702	49719	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:18.194920063 CEST	7702	49719	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:18.195035934 CEST	49719	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.195199013 CEST	49719	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.195784092 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.200634956 CEST	7702	49719	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:18.200651884 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:18.200747013 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.393647909 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.398709059 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:18.398766994 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.403701067 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:18.408972025 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.413930893 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:18.413995028 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:18.418946981 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.002813101 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.007709980 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.007766962 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.013520956 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.652283907 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.652350903 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.652503014 CEST	49721	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.652857065 CEST	49722	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.666204929 CEST	7702	49721	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.666533947 CEST	7702	49722	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.666600943 CEST	49722	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.697191954 CEST	7702	49722	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.697257996 CEST	49722	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.697381973 CEST	49722	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.697760105 CEST	49723	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.705105066 CEST	7702	49722	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.705118895 CEST	7702	49723	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.705209970 CEST	49723	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.719852924 CEST	7702	49723	80.76.49.148	192.168.2.6
Jun 18, 2024 21:18:19.719932079 CEST	49723	7702	192.168.2.6	80.76.49.148
Jun 18, 2024 21:18:19.720067978 CEST	49723	7702	192.168.2.6	80.76.49.148

Statistics

No statistics

System Behavior

Analysis Process: Wo0CkmOz64.exe PID: 2752, Parent PID: 4004

General

Target ID:	0

Start time:	15:18:06
Start date:	18/06/2024
Path:	C:\Users\user\Desktop\Wo0CkmOz64.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Wo0CkmOz64.exe"
Imagebase:	0x980000
File size:	856'064 bytes
MD5 hash:	06B81C8EDD7F620513A06E3A5CC11483
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.3380383003.000000001BBA0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.3379202075.000000001B690000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.3376338658.0000000012F41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_PureLogStealer, Description: Yara detected PureLog Stealer, Source: 00000000.00000002.3376338658.0000000013171000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.3371913837.0000000002C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD93C9797B	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFD93C9797B	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFD93C76FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFD93C76FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFD93C45F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFD93C6F056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFD93C6F056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFD93C45F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFD93C76FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFD93C76FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFD93C76FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFD93C45F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\567ff6b0de7f9dcd8111001e94ab7cf6\System.Drawing.ni.dll.aux	0	584	success or wait	1	7FFD93C45F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFD93C45F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFD93C45F36	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFD923CC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFD923CC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFD923CC9C8	ReadFile

Disassembly

No disassembly