ID: 357249
Sample Name: payment.exe
Cookbook: default.jbs
Time: 10:43:28
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

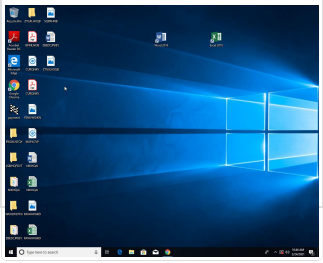
Analysis Report payment.exe

Overview

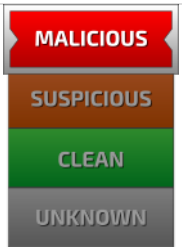
General Information

Sample Name:	payment.exe
Analysis ID:	357249
MD5:	0780e01f6ac683c..
SHA1:	d2c1ef0cab63992..
SHA256:	0fc71d13ed4108b.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



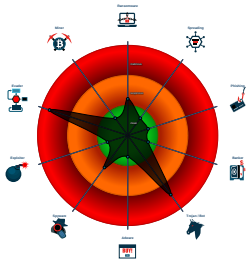
AgentTesla GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- payment.exe (PID: 6976 cmdline: 'C:\Users\user\Desktop\payment.exe' MD5: 0780E01F6AC683C0529FB1D40AACA8B4)
  - RegAsm.exe (PID: 4660 cmdline: 'C:\Users\user\Desktop\payment.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 4688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

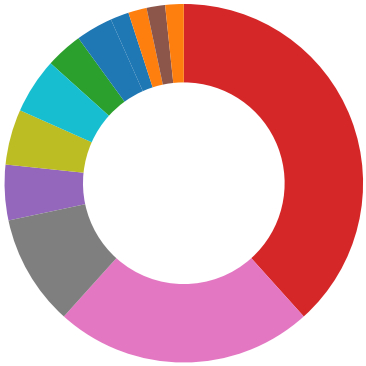
Source	Rule	Description	Author	Strings
0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000F.00000002.592476347.000000000564000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 4660	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 4660	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

System Summary:

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

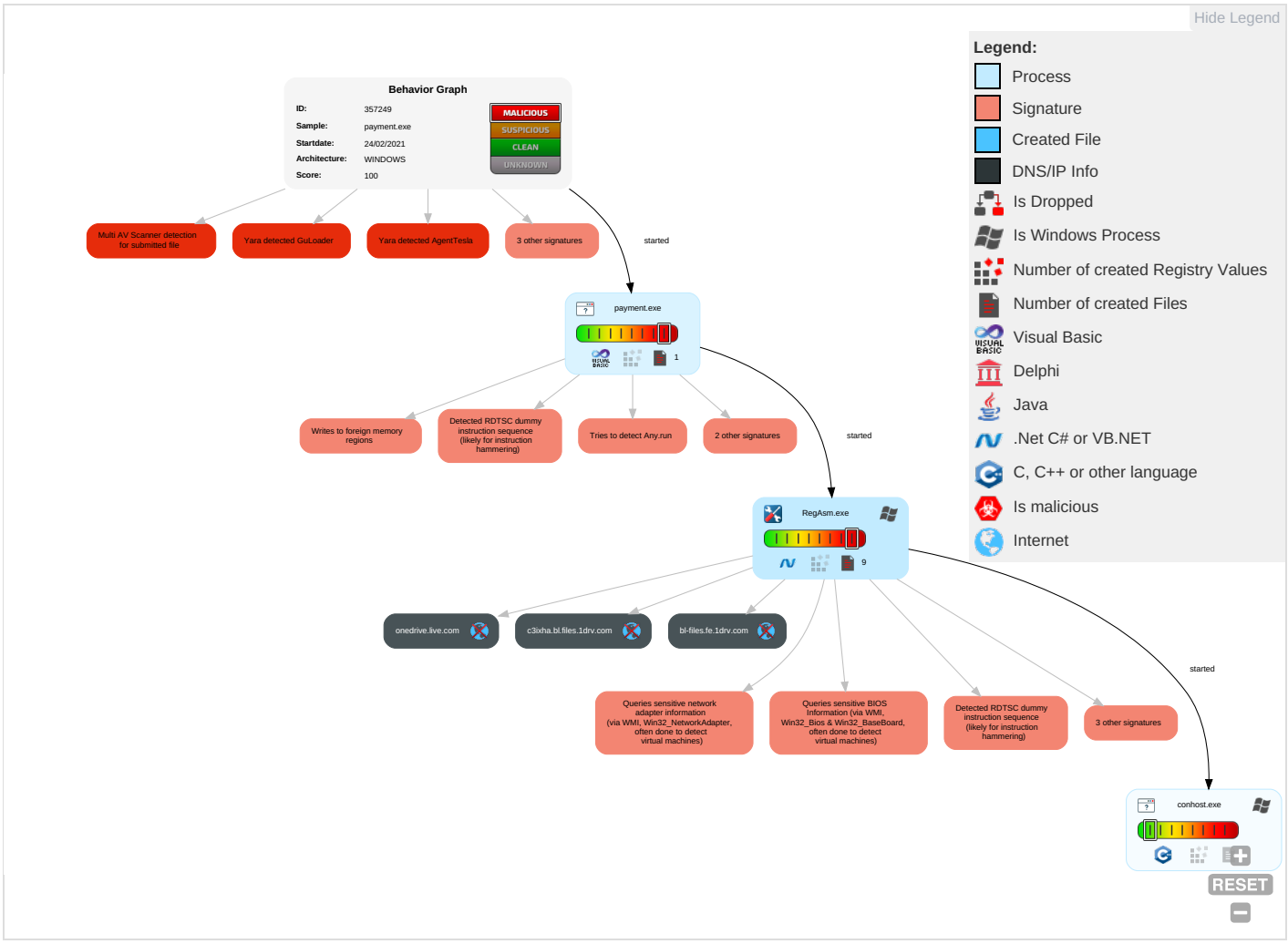
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 4	OS Credential Dumping	Security Software Discovery 6 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	I I I (
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	I I (
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	I I
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	I I (
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 3 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J I S

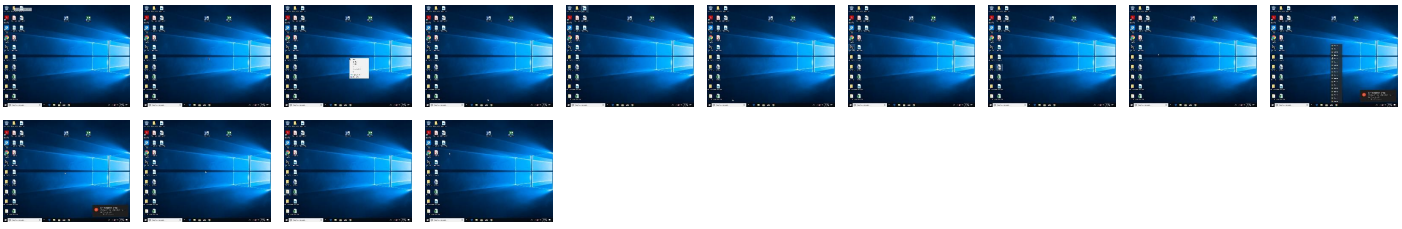
Behavior Graph



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
payment.exe	57%	Virustotal		Browse
payment.exe	46%	ReversingLabs	Win32.Backdoor.Remcos	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://kBTuTq.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
c3ixha.bl.files.1drv.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://kBTuTq.com	RegAsm.exe, 0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://onedrive.live.com/download?cid=876616565B0E44B1&resid=876616565B0E44B1%213215&authkey=AC2zGE	RegAsm.exe	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357249
Start date:	24.02.2021
Start time:	10:43:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@4/0@2/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.5% (good quality ratio 21.9%) • Quality average: 54.7% • Quality standard deviation: 11.1%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.193.48, 92.122.145.220, 104.42.151.234, 51.11.168.160, 2.20.142.209, 2.20.142.210, 51.103.5.159, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 13.107.42.13, 13.107.42.12, 184.30.24.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, odc-web-brs.onedrive.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, l-0004.l-msedge.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, audownload.windowsupdate.nsatc.net, odc-bl-files-brs.onedrive.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, odc-bl-files-geo.onedrive.akadns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, bl-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:44:19	API Interceptor	1x Sleep call for process: payment.exe modified
10:46:00	API Interceptor	191x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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, for MS Windows
Entropy (8bit):	6.584972265863127
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	payment.exe
File size:	225280
MD5:	0780e01f6ac683c0529fb1d40aaca8b4
SHA1:	d2c1ef0cab63992d4bea95fdf7838047997c46a7
SHA256:	0fc71d13ed4108b3afb81d9347063f9ef6ed9c3528a9c6e67a892c8a8db5fada

General

SHA512:	d7c0ede50d907e9374d3dc6ccaf18dedb1984b0d54a8bd50ba9fac9405c9f4acb7994e182b7a9e49d7d9c95f1135015e1d5cb61d8838536cc7edbfa12724bd8d
SSDEEP:	1536:ai24BsvhHpVmqBu755CxBa/t3UWoF6Jp6GeSlm3WdtHV1BsjlwoEffyW053iYk:SxZTGb9F3UWoFWpNgZUfh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L...M..H.....0...@.....0.....@....@.....

File Icon

Icon Hash:	0634b8d4c8c4c0ce

Static PE Info

General

Entrypoint:	0x401630
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48A5FC4D [Fri Aug 15 21:59:41 2008 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:	c495ca9196b04f3a1871ecbfcbd50911

Entrypoint Preview

Instruction
push 00402BD8h
call 00007FF4A8EA6DC5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], dl
pop edx
out dx, eax
or eax, 4E4BFD93h
xchg eax, edx
or dh, ah
das
push ebx
clc
jnc 00007FF4A8EA6DD2h
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+72h], dl
outsd
push 00000065h
arpl word ptr [ecx+esi+00h], si
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
sub byte ptr [edx], ch
call far 42B0h : F9A52BC6h
mov edi, DA7EB6B7h
lds eax, fword ptr [edx+edi*2+3Fh]
dec edi
faddp st(6), st(0)
aaa
leave
cdq
inc esp
mov bh, byte ptr [ecx]
xor ebp, ebp
xchg dword ptr [eax], edi
adc byte ptr [eax+3Ah], bl
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
mov esp, B4000014h
push cs
add byte ptr [eax], al
add byte ptr [ebx], dl
add byte ptr [ecx+eax*2+54h], al
inc ecx
push esp
push edx

Instruction
inc ecx
dec esi
push ebx
dec ebp
dec ecx
push ebx
push ebx
dec ecx
dec edi
dec esi
inc ebp
push edx
push ebx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x33364	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x36000	0x1252	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x124	.text
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	0x32870	0x33000	False	0.263604856005	data	6.80293275288	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x34000	0x1280	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x36000	0x1252	0x2000	False	0.168090820312	data	2.29185489566	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x369aa	0x8a8	data		
RT_ICON	0x36442	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x36420	0x22	data		
RT_VERSION	0x36120	0x300	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaLateMemSt, __vbaObjSet, __vbaCyAdd, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaCyI2, __vbaStrCmp, __vbaVarTstEq, __vbaObjVar, __vbaI2I4, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaFpCmpCy, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaI2Var, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarDup, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0404 0x04b0
LegalCopyright	Coldest
InternalName	Ancistrocladaceous5
FileVersion	1.00
CompanyName	SummerDream Company
LegalTrademarks	Coldest
Comments	SummerDream Company
ProductName	Project1
ProductVersion	1.00
OriginalFilename	Ancistrocladaceous5.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 10:44:10.911381006 CET	55074	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:10.960200071 CET	53	55074	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:11.780896902 CET	54513	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:11.834822893 CET	53	54513	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:12.757447004 CET	62044	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:12.806353092 CET	53	62044	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:13.411082983 CET	63791	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:13.477824926 CET	53	63791	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:13.569865942 CET	64267	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:13.618797064 CET	53	64267	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:14.516139984 CET	49448	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:14.568125010 CET	53	49448	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:15.470302105 CET	60342	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:15.522371054 CET	53	60342	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:16.690913916 CET	61346	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:16.740000963 CET	53	61346	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:18.376986980 CET	51774	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:18.428474903 CET	53	51774	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:19.211590052 CET	56023	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:19.264411926 CET	53	56023	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:20.427401066 CET	58384	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:20.480751991 CET	53	58384	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:23.716433048 CET	60261	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:23.768256903 CET	53	60261	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:25.128577948 CET	56061	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:25.177556038 CET	53	56061	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:29.631326914 CET	58336	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:29.683278084 CET	53	58336	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:31.132128954 CET	53781	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:31.183218002 CET	53	53781	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:32.073699951 CET	54064	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:32.127625942 CET	53	54064	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:32.960329056 CET	52811	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:33.009255886 CET	53	52811	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:37.799596071 CET	55299	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:37.851288080 CET	53	55299	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:38.644771099 CET	63745	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 10:44:38.693814993 CET	53	63745	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:44.368793964 CET	50055	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:44.420629025 CET	53	50055	8.8.8.8	192.168.2.6
Feb 24, 2021 10:44:49.696610928 CET	61374	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:44:49.748292923 CET	53	61374	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:05.888565063 CET	50339	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:05.954570055 CET	53	50339	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:07.742175102 CET	63307	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:07.792047024 CET	53	63307	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:22.955830097 CET	49694	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:23.017445087 CET	53	49694	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:29.490305901 CET	54982	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:29.541260958 CET	53	54982	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:30.131491899 CET	50010	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:30.181240082 CET	53	50010	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:30.849584103 CET	63718	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:30.950206041 CET	53	63718	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:31.368204117 CET	62116	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:31.433454990 CET	53	62116	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:31.986391068 CET	63816	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:32.055495024 CET	53	63816	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:32.674719095 CET	55014	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:32.732131958 CET	53	55014	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:33.386050940 CET	62208	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:33.443485022 CET	53	62208	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:34.287131071 CET	57574	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:34.347367048 CET	53	57574	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:35.530936956 CET	51818	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:35.588417053 CET	53	51818	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:36.095642090 CET	56628	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:36.156138897 CET	53	56628	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:36.366750956 CET	60778	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:36.416053057 CET	53	60778	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:49.429064035 CET	53799	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:49.478157043 CET	53	53799	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:50.202363014 CET	54683	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:50.230230093 CET	59329	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:45:50.281210899 CET	53	54683	8.8.8.8	192.168.2.6
Feb 24, 2021 10:45:50.289444923 CET	53	59329	8.8.8.8	192.168.2.6
Feb 24, 2021 10:46:11.232192039 CET	64021	53	192.168.2.6	8.8.8.8
Feb 24, 2021 10:46:11.283066988 CET	53	64021	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 10:45:49.429064035 CET	192.168.2.6	8.8.8.8	0xd2a9	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 24, 2021 10:45:50.202363014 CET	192.168.2.6	8.8.8.8	0x8cbf	Standard query (0)	c3ixha.bl.files.1drv.com	A (IP address)	IN (0x0001)

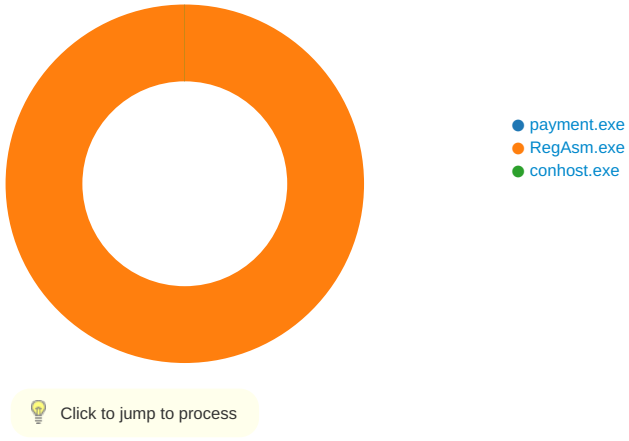
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 10:45:49.478157043 CET	8.8.8.8	192.168.2.6	0xd2a9	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 10:45:50.281210899 CET	8.8.8.8	192.168.2.6	0x8cbf	No error (0)	c3ixha.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 10:45:50.281210899 CET	8.8.8.8	192.168.2.6	0x8cbf	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: payment.exe PID: 6976 Parent PID: 5912

General

Start time:	10:44:18
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\payment.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\payment.exe'
Imagebase:	0x400000
File size:	225280 bytes
MD5 hash:	0780E01F6AC683C0529FB1D40AACA8B4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 4660 Parent PID: 6976

General

Start time:	10:45:35
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\payment.exe'
Imagebase:	0x10000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.597115330.000000001D081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000F.00000002.592476347.0000000000564000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

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	567C79	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	567C79	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	567C79	InternetOpenUrlA
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	567C79	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	567C79	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	567C79	InternetOpenUrlA
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	6D7DCF06	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	6D7DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D7B5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D7BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D7BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C621B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C621B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D7B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D7B5705	unknown

Analysis Process: conhost.exe PID: 4688 Parent PID: 4660

General

Start time:	10:45:36
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis