ID: 387710
Sample Name: vEjGZyD0iN.exe
Cookbook: default.jbs
Time: 14:42:24
Date: 15/04/2021
Version: 31.0.0 Emerald

Table of Contents

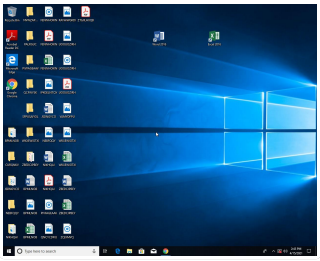
Analysis Report vEjGZyD0iN.exe

Overview

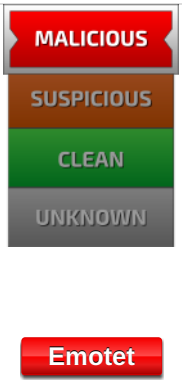
General Information

Sample Name:	vEjGZyD0iN.exe
Analysis ID:	387710
MD5:	ecbc4b40dcfec4e..
SHA1:	e08eb07c69d8fc8..
SHA256:	878d5137e0c9a0..
Infos:	

Most interesting Screenshot:



Detection

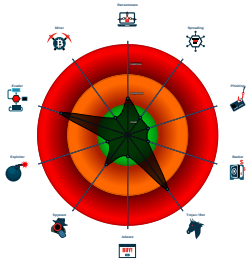


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Drops executables to the windows d…
- Found evasive API chain (may stop…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Contains capabilities to detect virtua…
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates files inside the system direc…

Classification



Startup

- **System is w10x64**
- vEjGZyD0iN.exe (PID: 7056 cmdline: 'C:\Users\user\Desktop\vEjGZyD0iN.exe' MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - vEjGZyD0iN.exe (PID: 7084 cmdline: C:\Users\user\Desktop\vEjGZyD0iN.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- lookupcart.exe (PID: 3832 cmdline: C:\Windows\SysWOW64\lookupcart.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - lookupcart.exe (PID: 644 cmdline: C:\Windows\SysWOW64\lookupcart.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- svchost.exe (PID: 4792 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6564 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
vEjGZyD0iN.exe	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
vEjGZyD0iN.exe	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 40 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 40 00 85 C0

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.326121826.0000000000981000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.404026613.0000000000981000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.334582341.0000000000981000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.327566145.0000000000981000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000002.00000000.327122709.0000000000981000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

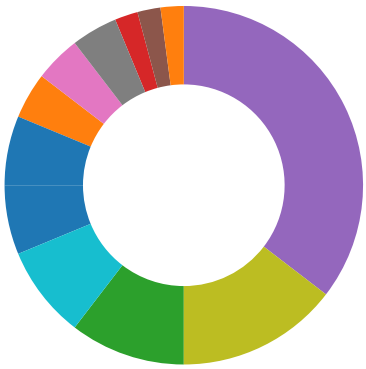
Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.vEjGZyD0iN.exe.980000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.0.vEjGZyD0iN.exe.980000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 98 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 98 00 85 C0
1.0.vEjGZyD0iN.exe.980000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.0.vEjGZyD0iN.exe.980000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 98 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 98 00 85 C0
6.0.lookupcart.exe.980000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Emotet

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

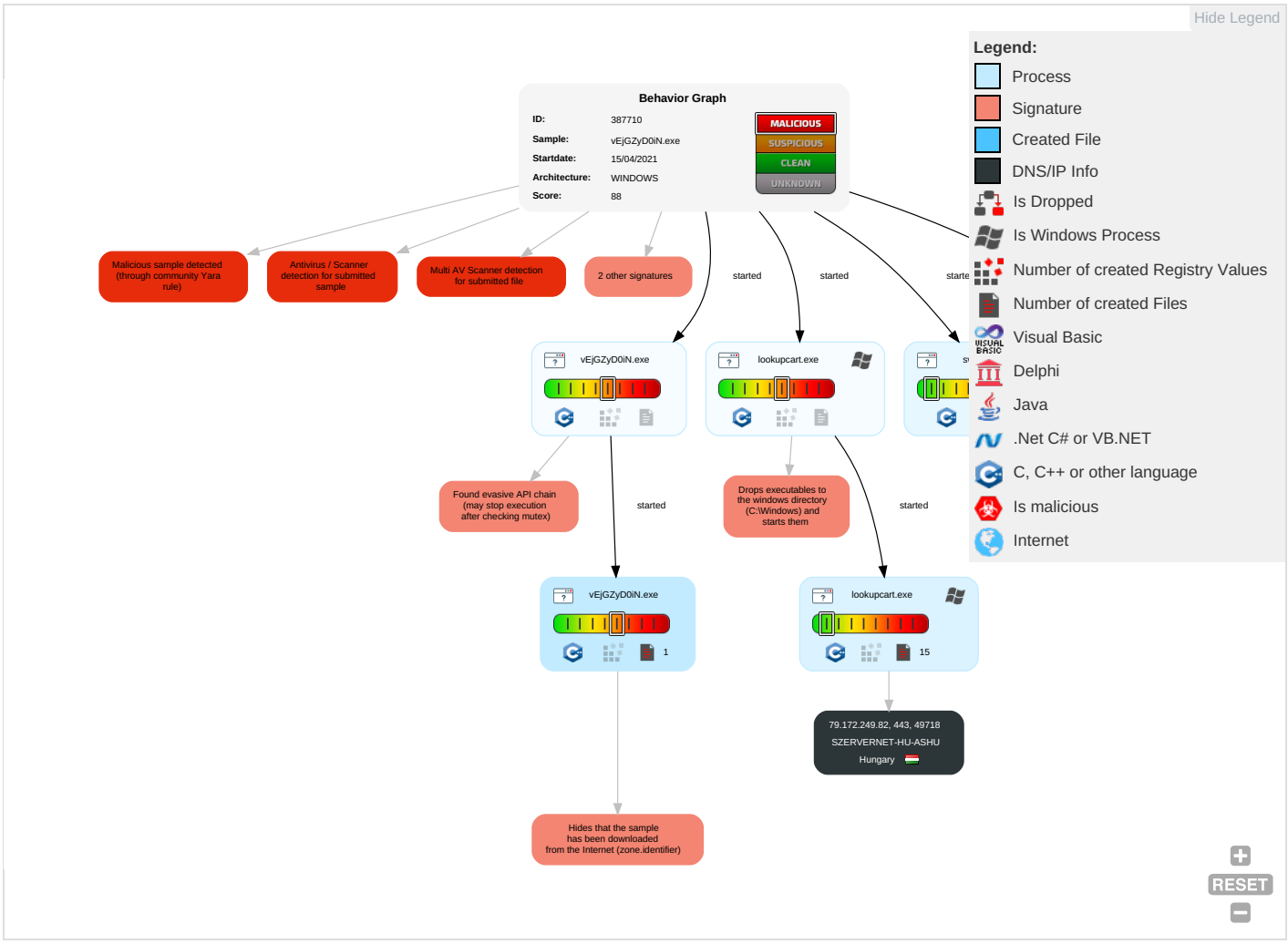
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remot Servic Effects
Valid Accounts	Native API 1 1	Path Interception	Process Injection 1	Masquerading 1 2	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remote Track D Without Authori
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe D Without Authori
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

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
vEjGZyD0iN.exe	87%	Virustotal		Browse
vEjGZyD0iN.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
vEjGZyD0iN.exe	100%	Avira	TR/Crypt.XPACK.Gen	
vEjGZyD0iN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.vEjGZyD0iN.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.lookupcart.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.lookupcart.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.vEjGZyD0iN.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.vEjGZyD0iN.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.lookupcart.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.lookupcart.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.vEjGZyD0iN.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://79.172.249.82:443/	3%	Virustotal		Browse
http://https://79.172.249.82:443/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://79.172.249.82:443/	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.172.249.82	unknown	Hungary		43711	SZERVERNET-HU-ASHU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	387710
Start date:	15.04.2021
Start time:	14:42:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vEjGZyD0iN.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:	13
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:	mal88.troj.evad.winEXE@8/0@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 41.1% (good quality ratio 37.4%) • Quality average: 79.1% • Quality standard deviation: 31%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.172.249.82	malware.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	zeD11Fztx8.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	9fdUNaHzLv.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	sample.exe.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	yxghUyIGb4.exe	Get hash	malicious	Browse	• 79.172.249.82:443/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0HvIGwMmBV.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	pitEBNziGR.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	RDuYHvb2jQ.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 79.172.249.82:443/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 79.172.249.82:443/
	http://okomekai.symphonic-net.com/Invoice-69070770/	Get hash	malicious	Browse	• 79.172.249.82:443/
	Outstanding invoice.doc	Get hash	malicious	Browse	• 79.172.249.82:443/
	Outstanding invoice.doc	Get hash	malicious	Browse	• 79.172.249.82:443/
	Informationen #018612525.doc	Get hash	malicious	Browse	• 79.172.249.82:443/
	Informationen #018612525.doc	Get hash	malicious	Browse	• 79.172.249.82:443/
	http://www.nzbodytalk.org.nz/INCORRECT-INVOICE/	Get hash	malicious	Browse	• 79.172.249.82:443/
	mail.rodolfogvalencia.com/Invoice/	Get hash	malicious	Browse	• 79.172.249.82:443/
	74039.exe	Get hash	malicious	Browse	• 79.172.249.82:443/
	Dokumente.doc	Get hash	malicious	Browse	• 79.172.249.82:443/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SZERVERNET-HU-ASHU	vEjGZyD0iN.exe	Get hash	malicious	Browse	• 79.172.249.82
	malware.exe	Get hash	malicious	Browse	• 79.172.249.82
	zeD11Fztx8.exe	Get hash	malicious	Browse	• 79.172.249.82
	9fdUNaHzLv.exe	Get hash	malicious	Browse	• 79.172.249.82
	sample.exe.exe	Get hash	malicious	Browse	• 79.172.249.82
	yxghUyIGb4.exe	Get hash	malicious	Browse	• 79.172.249.82
	0HvIGwMmBV.exe	Get hash	malicious	Browse	• 79.172.249.82
	pitEBNziGR.exe	Get hash	malicious	Browse	• 79.172.249.82
	http://https://kaliconsultancy.com/wp-content/uploads/2020/09/wflnfkqajn.php	Get hash	malicious	Browse	• 79.172.193.55
	http://https://delina.hu/praktikak/2016/02/01/csinalj-te-is-kreativ-mozaikkoveket	Get hash	malicious	Browse	• 95.140.36.82
	762002910000000.exe	Get hash	malicious	Browse	• 79.172.193.32
	1Wire_Copy.exe	Get hash	malicious	Browse	• 79.172.242.87
	430#U0437.js	Get hash	malicious	Browse	• 79.172.193.32
	59Transfer-copy.exe	Get hash	malicious	Browse	• 79.172.242.92
	25wire_slip.exe	Get hash	malicious	Browse	• 79.172.242.89
	BK.485799485.jse	Get hash	malicious	Browse	• 79.172.193.32
	PO 2312 CBD- 1302 S18.doc	Get hash	malicious	Browse	• 79.172.242.87
	RDuYHvb2jQ.exe	Get hash	malicious	Browse	• 79.172.249.82
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 79.172.249.82
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 79.172.249.82

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):	6.436116781781946
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:	vEjGZyD0iN.exe
File size:	45568
MD5:	ecbc4b40dcfec4ed1b2647b217da0441
SHA1:	e08eb07c69d8fc8e75927597767288a21d6ed7f6
SHA256:	878d5137e0c9a072c83c596b4e80f2aa52a8580ef214e5b a0d59daa5036a92f8
SHA512:	3ec4de3f35e10c874916a6402004e3b9fc60b5a026d2010 0ede992b592fe396db2bee0b225ab5f2fb85561f687a8abf 0c9e7c8b3cf0344c384c80297278be7b5
SSDEEP:	768:uhBY2Tumxi0mv/LWT3uBoGMUslwORSSrUBqvW zNQRC1s:ABxT6jW7uBgyOvWS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R..h...h...h.....h...i...h.....h.....h.Rich..h.....PE..L...7.]Z.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x409ee0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5A5DA737 [Tue Jan 16 07:18:15 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	4cfe8bbfb0ca5b84bbad08b043ea0c87

Entrypoint Preview

Instruction
push esi
push 0040C1F0h
push 3966646Ch
push 00000009h

Instruction
mov ecx, D22E2014h
call 00007FB5D48CA8FEh
mov edx, 004011F0h
mov ecx, eax
call 00007FB5D48CA822h
add esp, 0Ch
mov ecx, 8F7EE672h
push 0040C0D0h
push 6677A1D2h
push 00000048h
call 00007FB5D48CA8D9h
mov edx, 004010D0h
mov ecx, eax
call 00007FB5D48CA7FDh
add esp, 0Ch
push 08000000h
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C10Ch]
mov esi, eax
test esi, esi
je 00007FB5D48D2C38h
push 08000000h
push 00000000h
push esi
call dword ptr [0040C1F8h]
add esp, 0Ch
push esi
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C1E8h]
call 00007FB5D48CA25Ah
push 00000000h
call dword ptr [0040C1ACh]
pop esi
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
sub esp, 0Ch
push ebx
push esi
push edi
mov edi, edx
mov dword ptr [ebp-0Ch], ecx
mov esi, 00000001h
mov dword ptr [ebp-08h], esi
mov eax, dword ptr [edi]
cmp eax, 7Fh
jbe 00007FB5D48D2C21h
lea ecx, dword ptr [ecx+00h]
shr eax, 07h

Instruction
inc esi
cmp eax, 7Fh

Rich Headers

Programming Language:	• [LNK] VS2013 UPD4 build 31101 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbad0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd000	0x5cc	.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	0xb000	0x8	.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	0x9883	0x9a00	False	0.503297483766	data	6.45508103349	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb000	0xb2e	0xc00	False	0.160807291667	data	4.23495809712	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0xbd8	0x200	False	0.123046875	data	0.91267432928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xd000	0x5cc	0x600	False	0.8671875	data	6.49434732961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	WTSGetActiveConsoleSessionId

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/15/21-14:43:14.538617	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:14.574356	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/15/21-14:43:14.575191	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:14.612247	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
04/15/21-14:43:14.612715	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/15/21-14:43:14.647830	ICMP	449	ICMP Time-To-Live Exceeded in Transit			91.206.52.152	192.168.2.6
04/15/21-14:43:14.648162	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:18.221307	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:22.221249	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:26.221777	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:30.222209	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:34.222706	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:38.222816	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:42.222746	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:46.223375	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:50.223913	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/15/21-14:43:54.223872	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 15, 2021 14:43:24.645726919 CEST	49718	443	192.168.2.6	79.172.249.82
Apr 15, 2021 14:43:24.700354099 CEST	443	49718	79.172.249.82	192.168.2.6
Apr 15, 2021 14:43:24.700769901 CEST	49718	443	192.168.2.6	79.172.249.82
Apr 15, 2021 14:43:24.701332092 CEST	49718	443	192.168.2.6	79.172.249.82
Apr 15, 2021 14:43:24.754362106 CEST	443	49718	79.172.249.82	192.168.2.6
Apr 15, 2021 14:43:24.754797935 CEST	443	49718	79.172.249.82	192.168.2.6
Apr 15, 2021 14:43:24.754858017 CEST	443	49718	79.172.249.82	192.168.2.6
Apr 15, 2021 14:43:24.754869938 CEST	49718	443	192.168.2.6	79.172.249.82
Apr 15, 2021 14:43:24.754903078 CEST	49718	443	192.168.2.6	79.172.249.82
Apr 15, 2021 14:43:24.755285978 CEST	49718	443	192.168.2.6	79.172.249.82
Apr 15, 2021 14:43:24.808232069 CEST	443	49718	79.172.249.82	192.168.2.6

HTTP Request Dependency Graph

- 79.172.249.82:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49718	79.172.249.82	443	C:\Windows\SysWOW64\lookupcart.exe

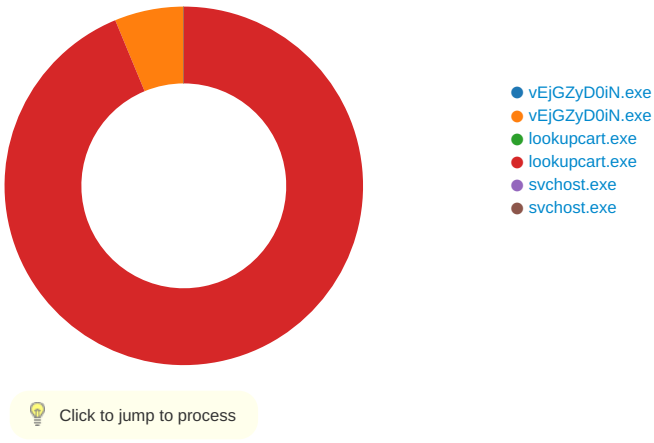
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 15, 2021 14:43:24.701332092 CEST	1068	OUT	POST / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.172.249.82:443 Content-Length: 436 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 23 69 5d 58 20 f6 64 09 28 5b a9 4c 38 7e b6 f2 94 d0 14 cf 6f 25 39 c5 a1 11 49 f8 4c 0d 98 ca 13 46 0d 2d 27 fa 14 33 7a 63 0e 6f d0 51 e6 17 e5 2d 70 05 3d 55 4b 0a 09 0e 1b 99 f1 26 2c a5 bd af 4f f5 8a 78 af 49 3d e1 ee bf 07 04 ca 18 6c 44 b3 ad 3b 56 c3 20 0f 48 39 79 89 3b 23 32 65 79 9d 05 16 45 e6 8b 45 3d f9 21 58 a5 da 47 cc 17 fc 26 70 77 3e 04 b4 40 07 01 8a f5 e3 27 a6 78 4d 7e e9 96 86 c7 6e 1a 55 40 cd f4 62 6a 3e 68 57 70 ae c5 ec f7 12 67 ba ab 40 8e 94 d6 3f 19 f6 61 a2 06 93 f4 15 0f 17 00 05 5a fe 5d c1 b8 e3 26 4c 93 7e 4b 11 10 f2 8f 24 6c 38 41 39 76 ec 1a 38 2c 43 90 fa 66 a8 a0 f4 a1 69 a6 ad 1e 28 fa 89 07 3e da ed 3a 85 27 2c 72 0e c2 34 23 1c 68 87 cc f5 be 42 31 c9 20 dd 6b 3c 89 4c f2 43 a4 41 b7 5c 96 99 29 bb 9d 86 72 5e 86 c7 c5 a3 b1 fb 10 4f 0c 26 54 18 16 2c 68 f7 57 65 21 6a 38 46 34 6d c9 06 4b 2a ae b4 cd 83 59 e1 52 7f a4 bc ec 3e 24 5b 75 02 7e eb 7d b2 e6 a2 af e4 19 36 e2 e2 6f f1 03 3d 1b 34 2e ad 99 c8 0d 8d e5 19 d5 a7 52 f4 e7 54 48 ed dd 91 d4 20 72 1a 59 94 6c b7 df 9d d8 47 9d 49 6c 94 2a d4 a5 70 87 5d 7c 2e 63 b8 3e c9 48 52 3b 04 30 03 56 d2 91 4c 8d e1 96 a3 9a 39 a5 ba 45 25 49 4f 64 9f 6d 78 3e 71 95 92 af e5 f9 55 21 d7 e5 89 3d e7 f6 53 01 a0 c6 4e 24 e3 68 d7 a8 73 80 21 7d 87 07 0a f1 3f f2 a0 e5 e0 a4 a4 34 c9 ec 43 4a 12 ac Data Ascii: #i]X d([L8~o%9ILF-'3zcoQ-p=UK&,OxI=lD;V H9y;#2eyEE=!XG&pw>@'xM~nU@bj>hWpg@?aZ]&L~K$l8A9v 8,Cfi(>:',r4#hB1 k<LCA\)r^O&T,hWeIj8F4mK*YR>$[u~}6o=4.RTH rYlGll*p]|.c>HR;0VL9E%lOdmx>qU!=SN$hs!}?4CJ
Apr 15, 2021 14:43:24.754797935 CEST	1069	IN	HTTP/1.1 400 Bad Request Date: Thu, 15 Apr 2021 12:43:24 GMT Server: Apache/2.4.25 (Debian) Content-Length: 362 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 20 72 65 71 75 65 73 74 20 74 68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20 63 6f 75 6c 64 20 6e 6f 74 20 75 6e 64 65 72 73 74 61 6e 64 2e 3c 62 72 20 2f 3e 0a 52 65 61 73 6f 6e 3a 20 59 6f 75 27 72 65 20 73 70 65 61 6b 69 6e 67 20 70 6c 61 69 6e 20 48 54 54 50 20 74 6f 20 61 6e 20 53 53 4c 2d 65 6e 61 62 6c 65 64 20 73 65 72 76 65 72 20 70 6f 72 74 2e 3c 62 72 20 2f 3e 0a 20 49 6e 73 74 65 61 64 20 75 73 65 20 74 68 65 20 48 54 54 50 53 20 73 63 68 65 6d 65 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 55 52 4c 2c 20 70 6c 65 61 73 65 2e 3c 62 72 20 2f 3e 0a 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>400 Bad Request</title> </head><body> Bad Request Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port. Instead use the HTTPS scheme to access this URL, please. </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: vEjGZyD0iN.exe PID: 7056 Parent PID: 6084

General

Start time:	14:43:14
Start date:	15/04/2021
Path:	C:\Users\user\Desktop\vEjGZyD0iN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vEjGZyD0iN.exe'
Imagebase:	0x980000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.326121826.0000000000981000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.327566145.0000000000981000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: vEjGZyD0iN.exe PID: 7084 Parent PID: 7056

General

Start time:	14:43:15
Start date:	15/04/2021
Path:	C:\Users\user\Desktop\vEjGZyD0iN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\vEjGZyD0iN.exe
Imagebase:	0x980000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000000.327122709.0000000000981000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.335148697.0000000000981000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\lookupcart.exe:Zone.Identifier	success or wait	1	9819CE	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: lookupcart.exe PID: 3832 Parent PID: 560

General

Start time:	14:43:18
Start date:	15/04/2021
Path:	C:\Windows\SysWOW64\lookupcart.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\lookupcart.exe
Imagebase:	0x980000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.334582341.0000000000981000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000000.333230150.0000000000981000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: lookupcart.exe PID: 644 Parent PID: 3832

General

Start time:	14:43:18
Start date:	15/04/2021
Path:	C:\Windows\SysWOW64\lookupcart.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\lookupcart.exe
Imagebase:	0x980000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.404026613.0000000000981000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000000.334160361.0000000000981000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	981E04	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\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	success or wait	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	success or wait	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\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	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	981E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	981E04	HttpSendRequestW

Analysis Process: svchost.exe PID: 4792 Parent PID: 560

General

Start time:	14:43:24
Start date:	15/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6564 Parent PID: 560

General

Start time:	14:43:42
Start date:	15/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis