ID: 465749
Sample Name: emo.exe
Cookbook: default.jbs
Time: 08:31:56
Date: 16/08/2021
Version: 33.0.0 White Diamond

Table of Contents

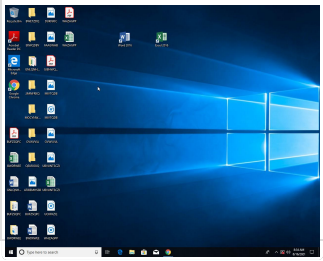
Windows Analysis Report emo.exe

Overview

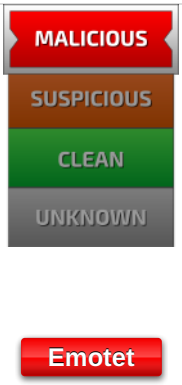
General Information

Sample Name:	emo.exe
Analysis ID:	465749
MD5:	1d314c60cf2ab83..
SHA1:	a076655c3e4b48..
SHA256:	459f8d96d0c2130.
Infos:	

Most interesting Screenshot:



Detection



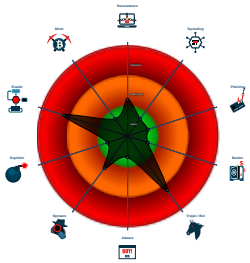
Emotet

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

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Drops executables to the windows d…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to open a port…

Classification



Process Tree

- **System is w10x64**
- emo.exe (PID: 6700 cmdline: 'C:\Users\user\Desktop\emo.exe' MD5: 1D314C60CF2AB83672F258033F1C9FDB)
  - emo.exe (PID: 6728 cmdline: C:\Users\user\Desktop\emo.exe MD5: 1D314C60CF2AB83672F258033F1C9FDB)
- aspcolorer.exe (PID: 7008 cmdline: C:\Windows\SysWOW64\aspcolorer.exe MD5: 1D314C60CF2AB83672F258033F1C9FDB)
  - aspcolorer.exe (PID: 7032 cmdline: C:\Windows\SysWOW64\aspcolorer.exe MD5: 1D314C60CF2AB83672F258033F1C9FDB)
- svchost.exe (PID: 7092 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6240 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4864 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6452 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.655519273.00000000041D1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.655519273.00000000041D1000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x5b80:$snippet4: 33 C0 C7 05 10 72 1E 04 20 2A 1E 04 C7 05 14 72 1E 04 20 2A 1E 04 A3 18 72 1E 04 A3 1C 72 1E 04 ...
00000001.00000002.670974631.00000000026F1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.670974631.00000000026F1000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x5b80:$snippet4: 33 C0 C7 05 10 72 70 02 20 2A 70 02 C7 05 14 72 70 02 20 2A 70 02 A3 18 72 70 02 A3 1C 72 70 02 ...
00000005.00000002.668324043.0000000002D61000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 3 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.emo.exe.41d0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.emo.exe.41d0000.3.unpack	Emotet	Emotet Payload	kevoreilly	• 0x5f80:$snippet4: 33 C0 C7 05 10 72 1E 04 20 2A 1E 04 C7 05 14 72 1E 04 20 2A 1E 04 A3 18 72 1E 04 A3 1C 72 1E 04 ...
1.2.emo.exe.26f0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.emo.exe.26f0000.3.unpack	Emotet	Emotet Payload	kevoreilly	• 0x5f80:$snippet4: 33 C0 C7 05 10 72 70 02 20 2A 70 02 C7 05 14 72 70 02 20 2A 70 02 A3 18 72 70 02 A3 1C 72 70 02 ...
5.2.aspcolorer.exe.2d60000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

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)

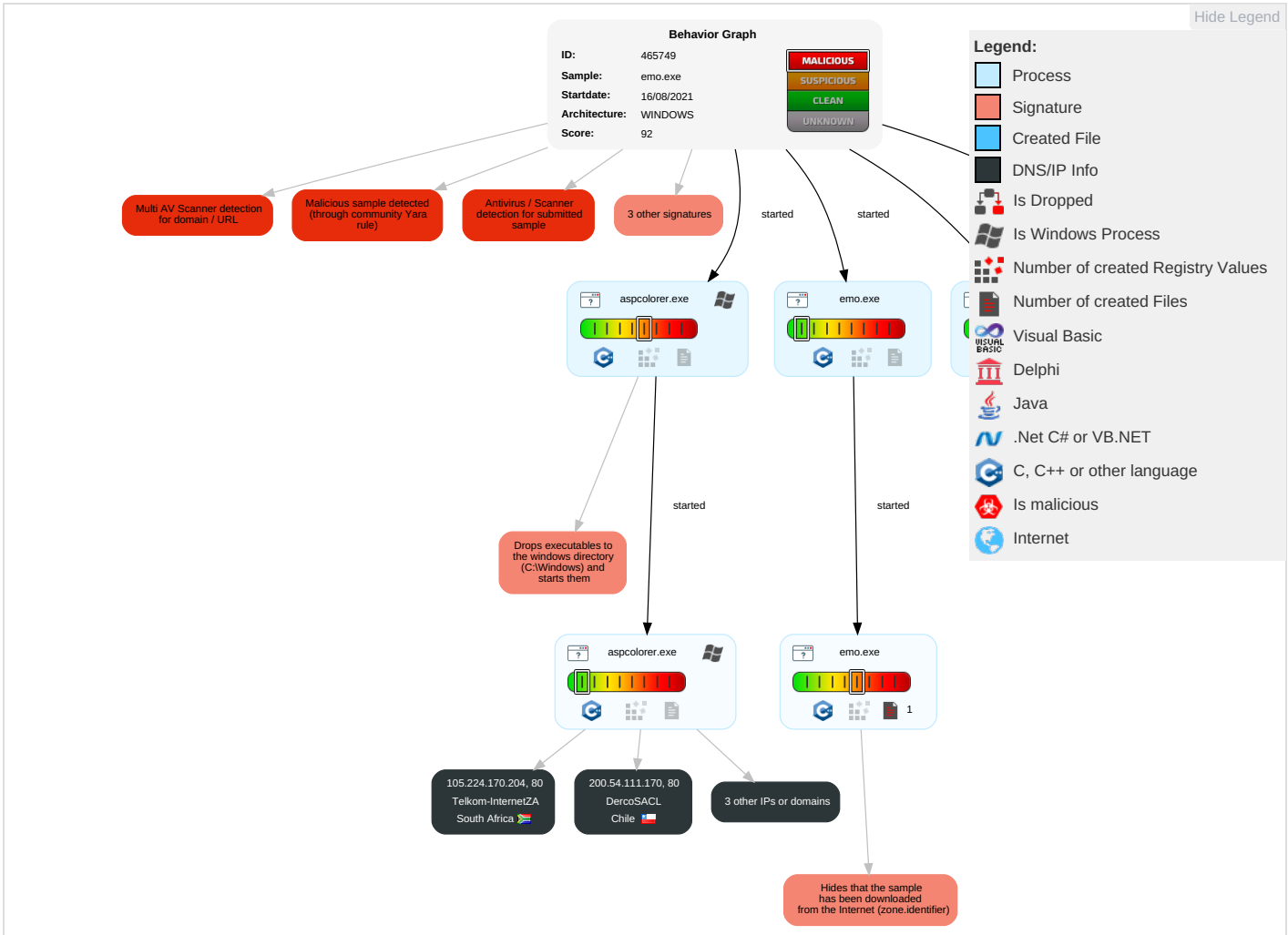
Stealing of Sensitive Information:

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	Ren Ser Effe
Valid Accounts	Native API 1	Path Interception	Process Injection 1	Masquerading 1 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Ren Trac Witl Autl
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Ren Wip Witl Autl
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obt Dev Clou Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	System Information Discovery 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

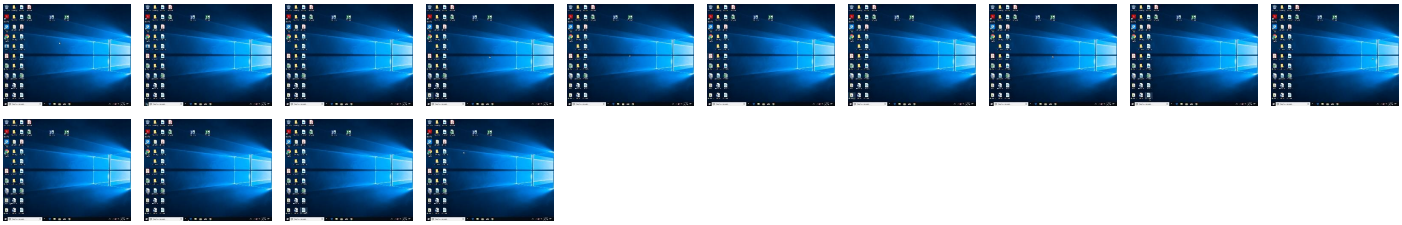
Behavior Graph



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
emo.exe	92%	Virustotal		Browse
emo.exe	70%	Metadefender		Browse
emo.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
emo.exe	100%	Avira	TR/Crypt.ZPACK.awz	
emo.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.aspcolorer.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.awz		Download File
6.1.aspcolorer.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
0.2.emo.exe.26f03af.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.aspcolorer.exe.2d40000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.emo.exe.26f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.emo.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111422		Download File
0.2.emo.exe.41d0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.aspcolorer.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111422		Download File
5.2.aspcolorer.exe.25c03af.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.emo.exe.26d0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.emo.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111422		Download File
5.1.aspcolorer.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
5.2.aspcolorer.exe.2d60000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.aspcolorer.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111422		Download File
6.2.aspcolorer.exe.2520000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.emo.exe.26b03af.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.emo.exe.41b0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.emo.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
1.0.emo.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.awz		Download File
6.0.aspcolorer.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.awz		Download File
6.2.aspcolorer.exe.2500000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.aspcolorer.exe.24d03af.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.emo.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.awz		Download File
0.1.emo.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://105.224.170.204/	7%	Virustotal		Browse
http://105.224.170.204/	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.136.151.73	unknown	United States		33363	BHN-33363US	false
186.159.186.156	unknown	Costa Rica		52228	CableTicaCR	false
66.112.88.78	unknown	United States		22561	CENTURYLINK-LEGACY-LIGHTCOREUS	false
105.224.170.204	unknown	South Africa		37457	Telkom-InternetZA	false
200.54.111.170	unknown	Chile		52310	DercoSACL	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	465749
Start date:	16.08.2021
Start time:	08:31:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	emo.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:	19
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:	mal92.troj.evad.winEXE@10/0@0/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.2% (good quality ratio 23%) • Quality average: 60.2% • Quality standard deviation: 40.2%
HCA Information:	• Successful, ratio: 78% • 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

Simulations

Behavior and APIs

Time	Type	Description
08:33:32	API Interceptor	10x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.136.151.73	oBftD9JG5h.exe	Get hash	malicious	Browse	
	cVEAJou1VVpN.exe	Get hash	malicious	Browse	
186.159.186.156	oBftD9JG5h.exe	Get hash	malicious	Browse	
	knownconf.exe	Get hash	malicious	Browse	
	Thanksgiving-Card.doc	Get hash	malicious	Browse	
	Thanksgiving-Day-eCard.doc	Get hash	malicious	Browse	
	cVEAJou1VVpN.exe	Get hash	malicious	Browse	
66.112.88.78	oBftD9JG5h.exe	Get hash	malicious	Browse	
	cVEAJou1VVpN.exe	Get hash	malicious	Browse	
105.224.170.204	oBftD9JG5h.exe	Get hash	malicious	Browse	
200.54.111.170	knownconf.exe	Get hash	malicious	Browse	• 200.54.111.170/
	Thanksgiving-Card.doc	Get hash	malicious	Browse	• 200.54.111.170/
	cVEAJou1VVpN.exe	Get hash	malicious	Browse	• 200.54.111.170/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BHN-33363US	PbttSF5mXT	Get hash	malicious	Browse	• 97.79.100.11
	ylq3OWuGzx	Get hash	malicious	Browse	• 97.102.236.200
	gP6rht35si	Get hash	malicious	Browse	• 96.58.97.59
	rq4MIQFAmU	Get hash	malicious	Browse	• 68.205.124.183
	gaxq7wN4q8	Get hash	malicious	Browse	• 97.69.18.33
	1isequal9.arm	Get hash	malicious	Browse	• 72.238.255.130
	B7S4YwiJLF	Get hash	malicious	Browse	• 72.188.139.200
	vHVNRpNhIs	Get hash	malicious	Browse	• 65.35.98.22
	aWhBGJrwWz	Get hash	malicious	Browse	• 97.79.50.21
	cxvJueYLS4	Get hash	malicious	Browse	• 68.204.233.85
	PaVUnU0r3p	Get hash	malicious	Browse	• 173.170.188.138
	0tJClm2RJX	Get hash	malicious	Browse	• 97.96.159.101
	I1lRHeFtqX	Get hash	malicious	Browse	• 173.168.235.70
	PHvqpLRfRl.exe	Get hash	malicious	Browse	• 50.91.114.38
	FD6qpyHOPI	Get hash	malicious	Browse	• 184.89.14.255
	oaG6jOntjL	Get hash	malicious	Browse	• 71.43.252.117
	X7AvBM4NoO	Get hash	malicious	Browse	• 97.102.236.236
	lhAgWM449Y	Get hash	malicious	Browse	• 97.68.238.145
	tMA66IeqHu	Get hash	malicious	Browse	• 107.144.164.77
	en2hmUmzUR	Get hash	malicious	Browse	• 67.9.44.166
CableTicaCR	N3pBzXZZne	Get hash	malicious	Browse	• 186.15.24.113
	oBftD9JG5h.exe	Get hash	malicious	Browse	• 186.159.186.156
	knownconf.exe	Get hash	malicious	Browse	• 186.159.186.156
	Thanksgiving-Card.doc	Get hash	malicious	Browse	• 186.159.186.156
	Thanksgiving-Day-eCard.doc	Get hash	malicious	Browse	• 186.159.186.156
	cVEAJou1VVpN.exe	Get hash	malicious	Browse	• 186.159.186.156
CENTURYLINK-LEGACY-LIGHTCOREUS	bf2Xd5XNqv	Get hash	malicious	Browse	• 173.202.160.130
	uMxlFgugKt	Get hash	malicious	Browse	• 99.195.171.130
	Pm96d6X1Y8	Get hash	malicious	Browse	• 184.159.108.177
	VfNmYKR1b7	Get hash	malicious	Browse	• 207.119.166.119
	uiInKzkLQx	Get hash	malicious	Browse	• 64.238.249.90
	UcEBQV1ZS7	Get hash	malicious	Browse	• 184.159.53.109
	jSZ8nD73MZ	Get hash	malicious	Browse	• 99.195.15.255
	TCMKnazFHf	Get hash	malicious	Browse	• 69.179.220.20

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	lLc1G9C259	Get hash	malicious	Browse	• 209.102.144.97
	4Fkt5QAGt1	Get hash	malicious	Browse	• 72.161.226.83
	qgQgEjl283	Get hash	malicious	Browse	• 99.195.171.120
	JRyLnlTR1O	Get hash	malicious	Browse	• 209.102.21 0.148
	4JQil8gLKd	Get hash	malicious	Browse	• 209.102.181.23
	RB1NsQ9LQf.exe	Get hash	malicious	Browse	• 209.102.187.47
	oBftD9JG5h.exe	Get hash	malicious	Browse	• 66.112.88.78

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):	6.111194457335321
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:	emo.exe
File size:	180224
MD5:	1d314c60cf2ab83672f258033f1c9fdb
SHA1:	a076655c3e4b48b2a074a7d37210adaea0e22f92
SHA256:	459f8d96d0c21300199c87ee798b594216732a27da6c31 90f36b483df9faaabf
SHA512:	82f5b8d8b4eec5dac2220a9cef857be499e0a5c6ac6b4e0 95633bcdfeb7892dabfd5a3ae4b19833c2e635494855a5 559c032f60eae0de7aba1eceec5592efee
SSDEEP:	3072:6XzE6a+Y65AsnY2H9cWkxSASTWHVST7n+5oo uZ5M:uzbY65fR9cWkMASTWHgnEoou
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....P... P...Pl..QR..PL..Q..tP..zPRich...P.....PE..L..... .....0.....@....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401919
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	GUARD_CF
Time Stamp:	0x2EF7B716 [Wed Dec 21 05:03:18 1994 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:	054b7d2027518d923046c03a250703b0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x24cc	0x3000	False	0.498453776042	data	5.69610691174	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4000	0x838	0x1000	False	0.3046875	data	3.02034569562	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5000	0x1f08	0x1000	False	0.109375	data	1.53583714414	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
DATA	0x7000	0x9861	0xa000	False	0.617065429688	data	6.59989433749	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
CONST	0x11000	0x6401	0x7000	False	0.696463448661	data	6.43333519721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
Data	0x18000	0xef26	0xf000	False	0.755501302083	data	6.96026063595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x27000	0x4140	0x5000	False	0.1634765625	data	3.52467749328	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2c000	0x154	0x1000	False	0.0869140625	data	0.832521456064	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Language of compilation system	Country where language is spoken	Map
Korean	North Korea	
Korean	South Korea	
Chinese	China	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/16/21-08:34:22.920882	ICMP	401	ICMP Destination Unreachable Network Unreachable			208.110.249.249	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: emo.exe PID: 6700 Parent PID: 5860

General

Start time:	08:32:47
Start date:	16/08/2021
Path:	C:\Users\user\Desktop\emo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\emo.exe'
Imagebase:	0x400000
File size:	180224 bytes
MD5 hash:	1D314C60CF2AB83672F258033F1C9FDB
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: 00000000.00000002.655519273.00000000041D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.655519273.00000000041D1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

Analysis Process: emo.exe PID: 6728 Parent PID: 6700

General

Start time:	08:32:47
Start date:	16/08/2021
Path:	C:\Users\user\Desktop\emo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\emo.exe
Imagebase:	0x400000
File size:	180224 bytes
MD5 hash:	1D314C60CF2AB83672F258033F1C9FDB
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: 00000001.00000002.670974631.00000000026F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.670974631.00000000026F1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: aspcolorer.exe PID: 7008 Parent PID: 568

General

Start time:	08:32:53
Start date:	16/08/2021
Path:	C:\Windows\SysWOW64\aspcolorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\aspcolorer.exe
Imagebase:	0x400000
File size:	180224 bytes
MD5 hash:	1D314C60CF2AB83672F258033F1C9FDB
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: 00000005.00000002.668324043.0000000002D61000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000005.00000002.668324043.0000000002D61000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

Analysis Process: aspcolorer.exe PID: 7032 Parent PID: 7008

General

Start time:	08:32:54
Start date:	16/08/2021
Path:	C:\Windows\SysWOW64\aspcolorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\aspcolorer.exe
Imagebase:	0x400000
File size:	180224 bytes
MD5 hash:	1D314C60CF2AB83672F258033F1C9FDB
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: 00000006.00000002.917142816.0000000002521000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000006.00000002.917142816.0000000002521000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

Analysis Process: svchost.exe PID: 7092 Parent PID: 568

General

Start time:	08:32:56
Start date:	16/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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

Show Windows behavior

Analysis Process: svchost.exe PID: 6240 Parent PID: 568

General

Start time:	08:33:14
Start date:	16/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000

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 Show Windows behavior

Analysis Process: svchost.exe PID: 4864 Parent PID: 568

General

Start time:	08:33:23
Start date:	16/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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 Show Windows behavior

Analysis Process: svchost.exe PID: 6452 Parent PID: 568

General

Start time:	08:33:30
Start date:	16/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
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 Show Windows behavior

Disassembly

Code Analysis