ID: 497240
Sample Name: tcpmdmaus.exe
Cookbook: default.jbs
Time: 15:41:07
Date: 05/10/2021
Version: 33.0.0 White Diamond

Table of Contents

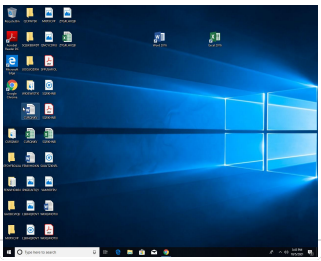
Windows Analysis Report tcpmdmaus.exe

Overview

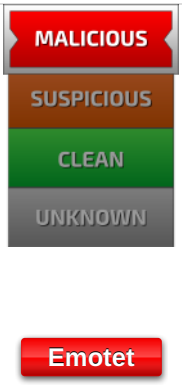
General Information

Sample Name:	tcpmdmaus.exe
Analysis ID:	497240
MD5:	abe13ddc14525c..
SHA1:	01b8022edd4ef8e.
SHA256:	8524e558dded96..
Infos:	

Most interesting Screenshot:



Detection

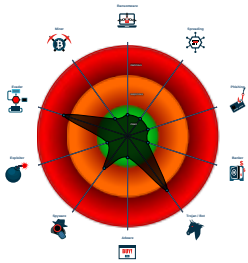


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- Machine Learning detection for samp…
- Hides that the sample has been dow…
- Drops executables to the windows d…
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match
- Deletes files inside the Windows fold…
- May sleep (evasive loops) to hinder …

Classification



Process Tree

- **System is w10x64**
- tcpmdmaus.exe (PID: 5368 cmdline: 'C:\Users\user\Desktop\tcpmdmaus.exe' MD5: ABE13DDC14525C4C35A85224689BFB27)
  - tcpmdmaus.exe (PID: 3200 cmdline: C:\Users\user\Desktop\tcpmdmaus.exe MD5: ABE13DDC14525C4C35A85224689BFB27)
- svchost.exe (PID: 6160 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- sharedconnect.exe (PID: 2932 cmdline: C:\Windows\SysWOW64\sharedconnect.exe MD5: ABE13DDC14525C4C35A85224689BFB27)
  - sharedconnect.exe (PID: 6128 cmdline: C:\Windows\SysWOW64\sharedconnect.exe MD5: ABE13DDC14525C4C35A85224689BFB27)
- svchost.exe (PID: 2940 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2440 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5752 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4368 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.742507592.0000000001481000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.742507592.0000000001481000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x5990:$snippet4: 33 C0 C7 05 80 A8 48 01 00 A0 48 01 C7 05 84 A8 48 01 00 A0 48 01 A3 88 A8 48 01 A3 8C A8 48 01 A3 90 A8 48 01 39 05 00 A0 48 01 74 1D 8D 49 00 40 A3 88 A8 48 01 83 3C C5 00 A0 48 01 00 75 F0 ...
00000000.00000002.372046233.0000000000951000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.372046233.0000000000951000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x5990:$snippet4: 33 C0 C7 05 80 A8 95 00 00 A0 95 00 C7 05 84 A8 95 00 00 A0 95 00 A3 88 A8 95 00 A3 8C A8 95 00 A3 90 A8 95 00 39 05 00 A0 95 00 74 1D 8D 49 00 40 A3 88 A8 95 00 83 3C C5 00 A0 95 00 00 75 F0 ...

Source	Rule	Description	Author	Strings
00000006.00000002.402858488.0000000000861000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.sharedconnect.exe.860000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
6.2.sharedconnect.exe.860000.2.unpack	Emotet	Emotet Payload	kevoreilly	• 0x5d90:$snippet4: 33 C0 C7 05 80 A8 86 00 00 A0 86 00 C7 05 84 A8 86 00 00 A0 86 00 A3 88 A8 86 00 A3 8C A8 86 00 A3 90 A8 86 00 39 05 00 A0 86 00 74 1D 8D 49 00 40 A3 88 A8 86 00 83 3C C5 00 A0 86 00 00 75 F0 ...
7.2.sharedconnect.exe.1480000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
7.2.sharedconnect.exe.1480000.3.unpack	Emotet	Emotet Payload	kevoreilly	• 0x5d90:$snippet4: 33 C0 C7 05 80 A8 48 01 00 A0 48 01 C7 05 84 A8 48 01 00 A0 48 01 A3 88 A8 48 01 A3 8C A8 48 01 A3 90 A8 48 01 39 05 00 A0 48 01 74 1D 8D 49 00 40 A3 88 A8 48 01 83 3C C5 00 A0 48 01 00 75 F0 ...
5.2.tcpmdmaus.exe.cd0000.2.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:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

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)

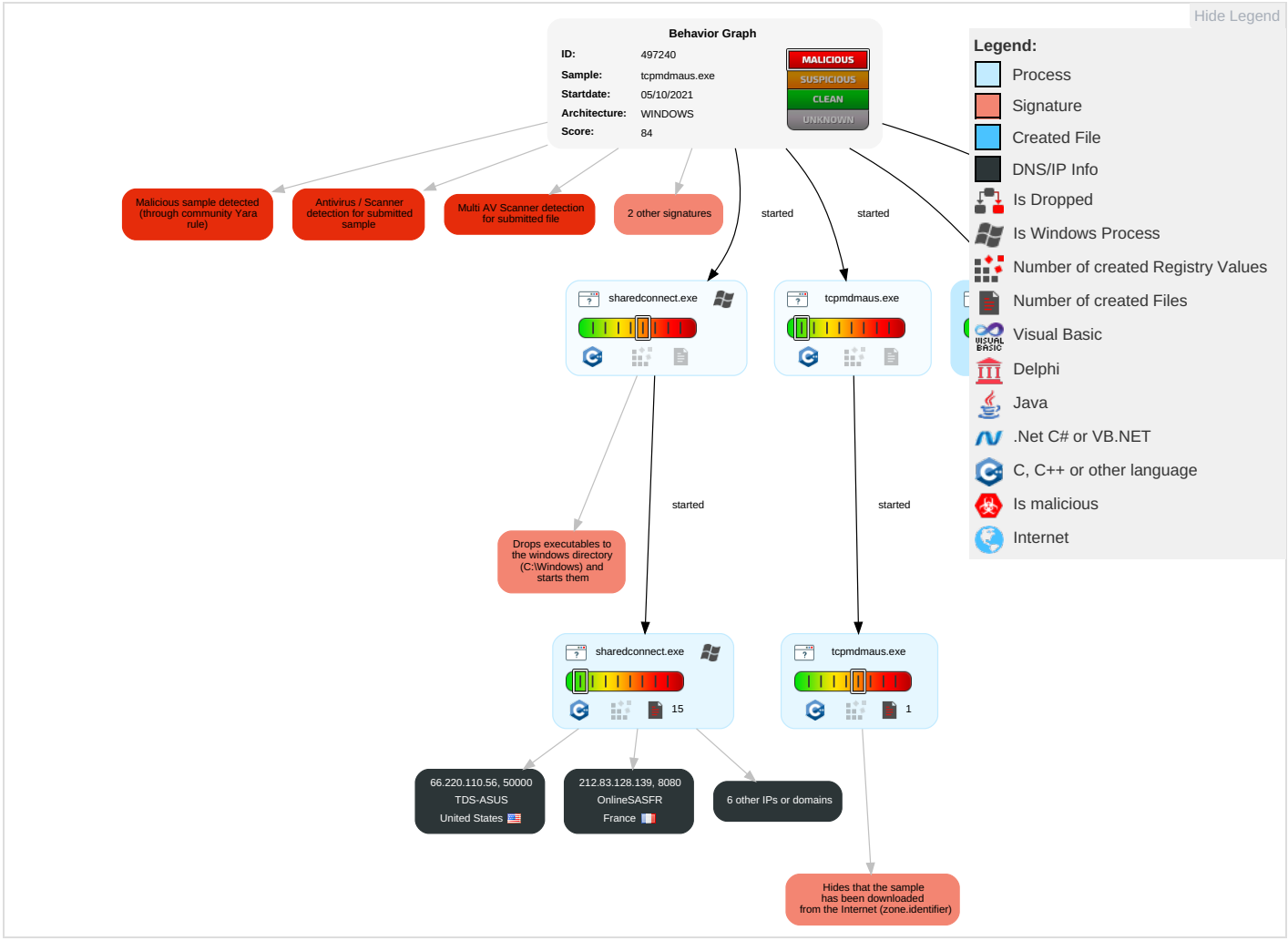
Stealing of Sensitive Information:

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
Valid Accounts 1	Service Execution 1 2	Valid Accounts 1	Valid Accounts 1	Masquerading 1 2	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrc Insecure Network Commun
Default Accounts	Native API 1	Windows Service 1 2	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Windows Service 1 2	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1	Access Token Manipulation 1	NTDS	System Service Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

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
tcpmdmaus.exe	85%	Virustotal		Browse
tcpmdmaus.exe	17%	Metadefender		Browse
tcpmdmaus.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
tcpmdmaus.exe	100%	Avira	HEUR/AGEN.1116174	
tcpmdmaus.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.tcpmdmaus.exe.2823d44.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.sharedconnect.exe.860000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.tcpmdmaus.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
0.2.tcpmdmaus.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
7.2.sharedconnect.exe.1480000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.sharedconnect.exe.1013d44.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.tcpmdmaus.exe.793d44.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.sharedconnect.exe.1470000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.tcpmdmaus.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
6.0.sharedconnect.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
5.2.tcpmdmaus.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
6.2.sharedconnect.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
6.2.sharedconnect.exe.770000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.tcpmdmaus.exe.7f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.tcpmdmaus.exe.940000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.tcpmdmaus.exe.cd0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.sharedconnect.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
7.2.sharedconnect.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1135375		Download File
0.2.tcpmdmaus.exe.950000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.sharedconnect.exe.1453d44.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	1%	Virustotal		Browse
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	1%	Virustotal		Browse
http://https://www.disneyplus.com/legal/privacy-policy	0%	Avira URL Cloud	safe	
http://https://77.157.40.119:443/	4%	Virustotal		Browse
http://https://77.157.40.119:443/	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://schemas.microsoft.co	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://77.157.40.119:443/	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.186.78.177	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
24.217.117.217	unknown	United States		20115	CHARTER-20115US	false
139.162.216.32	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	false
77.157.40.119	unknown	France		15557	LDCOMNETFR	false
110.143.116.201	unknown	Australia		1221	ASN-TELSTRATelstraCorporation LtdAU	false
66.220.110.56	unknown	United States		4181	TDS-ASUS	false
197.82.220.82	unknown	South Africa		10474	OPTINETZA	false
212.83.128.139	unknown	France		12876	OnlineSASFR	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	497240
Start date:	05.10.2021
Start time:	15:41:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tcpmdmaus.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
Run name:	Run with higher sleep bypass
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:	mal84.troj.evad.winEXE@11/4@0/9
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 40.8% (good quality ratio 33.1%) • Quality average: 64.5% • Quality standard deviation: 37.9%
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:43:26	API Interceptor	1x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.186.78.177	Emotet.doc	Get hash	malicious	Browse	
	Emotet.doc	Get hash	malicious	Browse	
24.217.117.217	http://suidi.com/IRS-Accounts-Transcipts-03/5/	Get hash	malicious	Browse	• 24.217.117.217/
	L9 2018 Payroll.doc	Get hash	malicious	Browse	• 24.217.117.217/
	L9 2018 Payroll.doc	Get hash	malicious	Browse	• 24.217.117.217/
	emotet.doc	Get hash	malicious	Browse	• 24.217.117.217/
	emotet.doc	Get hash	malicious	Browse	• 24.217.117.217/
	0521329 invoicing.doc	Get hash	malicious	Browse	• 24.217.117.217/
	0521329 invoicing.doc	Get hash	malicious	Browse	• 24.217.117.217/
	36784.exe	Get hash	malicious	Browse	• 24.217.117.217/
	0D73199318512570.doc	Get hash	malicious	Browse	• 24.217.117.217/
	[EXT] Payment status.doc	Get hash	malicious	Browse	• 24.217.117.217/
	[EXT] Payment status.doc	Get hash	malicious	Browse	• 24.217.117.217/
	emotet_43.doc	Get hash	malicious	Browse	• 24.217.117.217/
	emotet_43.doc	Get hash	malicious	Browse	• 24.217.117.217/
	INV042479428.doc	Get hash	malicious	Browse	• 24.217.117.217/
	INV042479428.doc	Get hash	malicious	Browse	• 24.217.117.217/
	9C0C7649.exe	Get hash	malicious	Browse	• 24.217.117.217/
	[EXT] Payment status.doc	Get hash	malicious	Browse	• 24.217.117.217/
	[EXT] Payment status.doc	Get hash	malicious	Browse	• 24.217.117.217/
	VPV-7014436651.doc	Get hash	malicious	Browse	• 24.217.117.217/
	VPV-7014436651.doc	Get hash	malicious	Browse	• 24.217.117.217/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-CXA-ALL-CCI-22773-RDCUS	tcpmdmaus.exe	Get hash	malicious	Browse	• 184.186.78.177
	arm7-20211004-1530	Get hash	malicious	Browse	• 209.34.217.143
	yir8ieZzXL	Get hash	malicious	Browse	• 70.163.133.117
	Zot0D0dD8J	Get hash	malicious	Browse	• 70.181.229.157
	cu8KB5if2T	Get hash	malicious	Browse	• 68.96.149.188
	8qv45JJrGQ	Get hash	malicious	Browse	• 68.111.25.31
	lessie.arm7	Get hash	malicious	Browse	• 184.178.190.23
	lessie.x86	Get hash	malicious	Browse	• 68.102.97.252
	834V8Sq5HQ	Get hash	malicious	Browse	• 72.200.138.26
	CdGi0KyPWX	Get hash	malicious	Browse	• 204.62.73.120
	dLM8lB4AQ7	Get hash	malicious	Browse	• 24.120.45.59
	SN3tZLChOJ	Get hash	malicious	Browse	• 98.171.80.191
	CDcUegnLSd	Get hash	malicious	Browse	• 68.101.118.225
	sora.arm7	Get hash	malicious	Browse	• 68.13.191.193
	sora.x86	Get hash	malicious	Browse	• 68.6.255.103
	index_2021-09-30-12_54	Get hash	malicious	Browse	• 68.7.243.91
	Wns7odRLbP	Get hash	malicious	Browse	• 70.175.218.163
	te2GttY5SP	Get hash	malicious	Browse	• 70.167.152.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6IT73F9Sr1	Get hash	malicious	Browse	• 68.109.156.159
	X3m77l2V5l	Get hash	malicious	Browse	• 184.181.23 6.242
CHARTER-20115US	FX8w3rI5cw	Get hash	malicious	Browse	• 47.42.193.254
	rf8Mq00YCl.dll	Get hash	malicious	Browse	• 97.84.78.80
	Zot0D0dD8J	Get hash	malicious	Browse	• 35.131.24.189
	nMftbNUfgt	Get hash	malicious	Browse	• 71.88.102.148
	lessie.arm	Get hash	malicious	Browse	• 71.90.182.89
	NazNIp21Xu	Get hash	malicious	Browse	• 47.238.133.75
	vojwi3a7DD	Get hash	malicious	Browse	• 68.185.115.38
	02uKvQqAqD	Get hash	malicious	Browse	• 66.227.190.152
	P2gQCIjHzq	Get hash	malicious	Browse	• 68.119.71.134
	djRl6t3Lqh	Get hash	malicious	Browse	• 68.118.113.151
	mirai.x86	Get hash	malicious	Browse	• 71.14.195.190
	sora.x86	Get hash	malicious	Browse	• 47.7.201.76
	Wns7odRLbP	Get hash	malicious	Browse	• 68.189.209.109
	hVLbKSQ0zq	Get hash	malicious	Browse	• 68.115.120.122
	arm7	Get hash	malicious	Browse	• 156.19.217.42
	b3astmode.arm	Get hash	malicious	Browse	• 66.168.5.54
	x86	Get hash	malicious	Browse	• 47.135.131.124
	whoareyou.x86	Get hash	malicious	Browse	• 150.181.23 7.235
	arm	Get hash	malicious	Browse	• 24.177.200.244
	x86_64	Get hash	malicious	Browse	• 24.207.175.171

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5903632458536222
Encrypted:	false
SSDEEP:	6:0FDtek1GaD0JOCEfMuaaD0JOCEfMKQmDaS/tAl/gz2cE0fMbhEZolrRSQ2hyYIIT:0dtNGaD0JcaaD0JwQQaS/tAg/0bjSQJ
MD5:	6A977DB879538ECF271A9B3B759DA94E
SHA1:	80A7358EBBC0824951A3D071A20B1BB581CC3C89
SHA-256:	6DD20771059479B00CFB42C57B224356999DC0E8B00D7130737FEC6F79ADFEF5
SHA-512:	6710EABC657B3FF199997F56238E4BFD632F21EA75B6CD018CF391976B3893BC60D21C62AA4E49654D07A567EB025EB4D7B9167A8806D7B2A938076225F08CBE
Malicious:	false
Reputation:	low
Preview:	......:{..(......+...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....+...y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0xfe58a2ca, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09347639506480135
Encrypted:	false
SSDEEP:	6:pAzwl/+yge1RIE11Y8TRXF4CmKzAzwl/+yge1RIE11Y8TRXF4CmK:C0+ygaO4bl+KM0+ygaO4bl+K

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
MD5:	C74A34D114B9EDD02FD41D7B4A8823D7
SHA1:	490E41D8B06C5A8CBBFB0BC6B4FF8C1AE65725CA
SHA-256:	8DEE8D47503401EE5003865E9059889341E7C43C27D929CC4B88C0F7DA36A302
SHA-512:	A7959F5F70FCB8CEE0E61463B67F49E166AA9EC9C2349E6B8E06D00395B46DB1AA92BC4575E109714CBC67EE843130C0CDCCC3B87D435E5F7EDE43970A893B2F
Malicious:	false
Preview:	.X..... .....e.f.3...w.....&.....w...+...y..h.(.....3...w.....B.....@..... ....3...w..... .....Vp...+...ygq.....+...yg..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.107829924515286
Encrypted:	false
SSDEEP:	3:Sr7Ev+OOAl/bJdAtioTall:Sri+OOAt4Zy
MD5:	EF667AACA01CCCCDFD2B92821334B044
SHA1:	B326E0849830C269A7D367AF92475FE62CB8688E
SHA-256:	5B1AC376D11254DBF817DC733980A0B12D32E5B866B471DBE311FCF4243D3596
SHA-512:	41351517A1E823A91B204DB86655AAD80CFCB86C97A1731FCC75AAEE93F299C753FFF9194CFC74508443BB72A54022CCF292C3ADA6FCC7328ECBFA5D904276A6
Malicious:	false
Preview:	...(.....3...w...+...yg.....w.....w.....w....:O....w.....+...yg..... ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.458919584976166
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:	tcpmdmaus.exe
File size:	280576
MD5:	abe13ddc14525c4c35a85224689bfb27
SHA1:	01b8022edd4ef8e9ab20807c032b7ce2849b3df3
SHA256:	8524e558dded9665e69541b332d556e43c007d0d4001fe5355ac4816c22e7a21

General

SHA512:	1592bd7a07aff9f04f44ecbdc049daef083e943cd2e930a9bd40ab1f7fbab71ae23c8229a3857b8917c7fc93427827fc0b9a02db2cb5a4a0351fc914eecee834
SSDEEP:	1536:y1dwtM1uD1drq12rh0PC4nRh87bEOYPyGy5oBu7WiKT:Y7uDDq8qHnRsbEjP/u7l
File Content Preview:	MZ.....@.....st.!.am.nL.7r....dern32.u....!..i...g!. .e!..$MZ.. mu.bThrL. un ....This pro W.....PE..L...`d.[.....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40100f
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:	0x5B1E6460 [Mon Jun 11 12:00:32 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	0b7b2a1ae1bd9f4631da141abed1aa7d

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x17898	0x17a00	False	0.0648044808201	data	0.983565645054	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x19000	0x46c	0x600	False	0.238932291667	data	1.7374447372	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bT	0x1a000	0x16eb	0x400	False	0.576171875	data	4.5070923188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x1c000	0x59a	0x600	False	0.257161458333	data	2.47810388592	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_READ
D	0x1d000	0x127ec	0x12800	False	0.308290223818	data	5.2061094126	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.crt0	0x30000	0xccbc	0xce00	False	0.561343294903	data	5.66222181743	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
cji8	0x3d000	0x5dd3	0x5e00	False	0.00835272606383	data	4.06889527583	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x43000	0x5e4c	0x6000	False	0.133138020833	data	3.29366479111	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x49000	0x472	0x600	False	0.209635416667	data	1.61290752237	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
Bulgarian	Bulgaria	
Chinese	Taiwan	
Czech	Czech Republic	
Danish	Denmark	
Greek	Greece	
English	United States	
Finnish	Finland	
Hebrew	Israel	
Hungarian	Hungary	
Japanese	Japan	

Language of compilation system	Country where language is spoken	Map
Korean	North Korea	
Korean	South Korea	
Polish	Poland	
Romanian	Romania	
Russian	Russia	
Croatian	Croatia	
Slovak	Slovakia	
Thai	Thailand	
Turkish	Turkey	
Slovenian	Slovenia	
Vietnamese	Vietnam	
Chinese	China	

Language of compilation system	Country where language is spoken	Map
Portuguese	Portugal	

Network Behavior

Network Port Distribution

TCP Packets

ICMP Packets

HTTP Request Dependency Graph

- 77.157.40.119:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49849	77.157.40.119	443	C:\Windows\SysWOW64\sharedconnect.exe

Timestamp	kBytes transferred	Direction	Data
Oct 5, 2021 15:44:16.475884914 CEST	6905	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: 77.157.40.119:443 Content-Length: 388 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2e f5 8d 30 20 97 63 af c8 5c 78 1d 1b 05 84 50 56 8e 19 5b d4 5e 84 69 7f 59 6c 87 46 e0 d0 59 8a f6 f3 38 80 a7 31 36 2a 41 93 7c 48 14 e8 94 4c f9 4b a4 47 e8 3f dd ae dc 2e 2b a6 0b 4e 9c 34 a8 33 bf b2 99 f0 55 30 50 57 c9 c7 08 84 57 c2 87 fe ef f4 fc 77 58 f0 6b 96 ac 8a dc 86 e9 20 3d c9 74 db ea 0a ab 88 74 c8 a2 da fc ca 06 27 02 7e a7 63 dd 3c 82 37 62 c3 a8 6a 68 12 a6 6c 70 b1 91 2e 31 24 27 9d ec 9e b1 3c 60 67 ed 52 57 23 21 97 d1 43 4b 2b f3 c0 e1 d7 82 bd 52 05 c3 43 20 17 61 0a dc ab cd c6 64 a6 a4 fe c2 c1 49 a3 e5 b5 c1 14 51 03 79 f0 cd 9d 37 2c 80 ec 86 6d 01 ab 1d 6e 2b af 18 4a 34 7e 89 f2 2d df ca f3 76 fb 2a 58 a0 da 6e 5b b3 e4 35 ff 79 1c 08 46 4f f8 f4 d1 97 26 3f 57 f1 fe 15 cb 39 c2 3f 9a 59 61 23 4a 83 97 0b 58 bb b3 e5 2d a3 fb 9e bd 22 dc 9e 9e e9 b1 bf 77 80 43 48 4f 42 61 24 17 ab 8b 56 2a d4 4c c4 56 1c 00 70 44 c3 81 65 e6 f8 8f 76 25 88 52 c6 8c 6e 33 f3 e4 0e 60 c1 63 0e 7a 7b 6f 50 ab 44 30 93 04 9f e4 a9 3a 73 17 af 84 fb 97 c1 dd 90 81 87 1b d4 f8 ce e1 a3 09 5c f0 44 44 8f 9c 35 7c bc 2a c5 93 40 4e 97 a2 d9 5b ed bd de 1b 90 8c 2a 61 27 49 13 6f 1a d4 55 91 07 0b ff b1 62 6e ec f2 b1 b2 df 1a d2 2d c8 Data Ascii: .0 c\xPV[^iYlFY816*A|HLKG?.+N43U0PWWwXk =tt'~c<7bjhlp.1$'<`gRW#!CK+RC adlQy7,mn+J4~-v*Xn [5yFO&?W9?Ya#JX-"wCHOBa$V*LVpDev%Rn3`cz{oPD0:s\DD5|*@N[*a'IoUbn-

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: tcpmdmaus.exe PID: 5368 Parent PID: 6096

General

Start time:	15:42:06
Start date:	05/10/2021
Path:	C:\Users\user\Desktop\tcpmdmaus.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\tcpmdmaus.exe'
Imagebase:	0x3b0000
File size:	280576 bytes
MD5 hash:	ABE13DDC14525C4C35A85224689BFB27
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: 00000000.00000002.372046233.0000000000951000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.372046233.0000000000951000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

Analysis Process: svchost.exe PID: 6160 Parent PID: 560

General

Start time:	15:42:18
Start date:	05/10/2021
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

Show Windows behavior

Analysis Process: tcpmdmaus.exe PID: 3200 Parent PID: 5368

General

Start time:	15:42:18
Start date:	05/10/2021
Path:	C:\Users\user\Desktop\tcpmdmaus.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\tcpmdmaus.exe
Imagebase:	0x3b0000
File size:	280576 bytes
MD5 hash:	ABE13DDC14525C4C35A85224689BFB27
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: 00000005.00000002.403460556.0000000000CD1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000005.00000002.403460556.0000000000CD1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities Show Windows behavior

File Deleted

Analysis Process: sharedconnect.exe PID: 2932 Parent PID: 560

General

Start time:	15:42:20
Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\sharedconnect.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sharedconnect.exe
Imagebase:	0x3b0000
File size:	280576 bytes
MD5 hash:	ABE13DDC14525C4C35A85224689BFB27
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: 00000006.00000002.402858488.0000000000861000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000006.00000002.402858488.0000000000861000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

Analysis Process: sharedconnect.exe PID: 6128 Parent PID: 2932

General

Start time:	15:42:32
Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\sharedconnect.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sharedconnect.exe
Imagebase:	0x3b0000
File size:	280576 bytes
MD5 hash:	ABE13DDC14525C4C35A85224689BFB27
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: 00000007.00000002.742507592.0000000001481000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000007.00000002.742507592.0000000001481000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities Show Windows behavior

File Created

Analysis Process: svchost.exe PID: 2940 Parent PID: 560

General

Start time:	15:42:35
Start date:	05/10/2021
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

Show Windows behavior

Analysis Process: svchost.exe PID: 2440 Parent PID: 560

General

Start time:	15:42:47
Start date:	05/10/2021
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

Show Windows behavior

Analysis Process: svchost.exe PID: 5752 Parent PID: 560

General

Start time:	15:42:56
Start date:	05/10/2021
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

Show Windows behavior

Analysis Process: svchost.exe PID: 4368 Parent PID: 560

General

Start time:	15:43:26
Start date:	05/10/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
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

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis