

ID: 376398
Sample Name: YF4dF4w2Cr
Cookbook: default.jbs
Time: 13:31:05
Date: 26/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report YF4dF4w2Cr 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
E-Banking Fraud: 5
System Summary: 5
Persistence and Installation Behavior: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
Stealing of Sensitive Information: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 15
Data Directories 15
Sections 16
Resources 16

Copyright Joe Security LLC 2021

Imports 18
Exports 19
Possible Origin 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 20
Code Manipulations 20
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: YF4dF4w2Cr.exe PID: 6836 Parent PID: 5912 21
General 21
File Activities 21
Registry Activities 21
Key Created 21
Key Value Created 22
Analysis Process: YF4dF4w2Cr.exe PID: 6856 Parent PID: 6836 22
General 22
File Activities 22
File Deleted 22
Analysis Process: fwdrrebrand.exe PID: 6912 Parent PID: 568 23
General 23
Registry Activities 23
Key Value Modified 23
Analysis Process: fwdrrebrand.exe PID: 6928 Parent PID: 6912 23
General 23
File Activities 24
File Created 24
Disassembly 25
Code Analysis 25

Copyright Joe Security LLC 2021

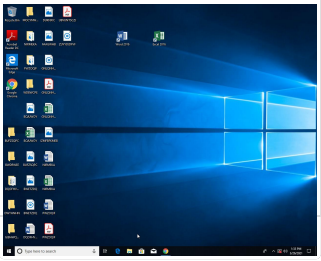
Analysis Report YF4dF4w2Cr

Overview

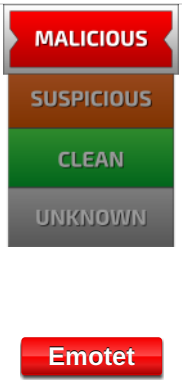
General Information

Sample Name:	YF4dF4w2Cr (renamed file extension from none to exe)
Analysis ID:	376398
MD5:	f4d1470af3a7d82..
SHA1:	0c45cf4e32116ea..
SHA256:	6fa0dd6002d4b4e..
Infos:	

Most interesting Screenshot:



Detection

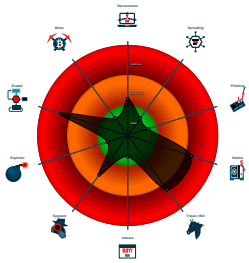


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Emotet e-Banking trojan
- 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…
- Antivirus or Machine Learning detec…
- Contains capabilities to detect virtua…
- Contains functionality to check if a d…
- Contains functionality to check if a w…

Classification



Startup

- **System is w10x64**
- YF4dF4w2Cr.exe (PID: 6836 cmdline: 'C:\Users\user\Desktop\YF4dF4w2Cr.exe' MD5: F4D1470AF3A7D82560B38558B132D468)
  - YF4dF4w2Cr.exe (PID: 6856 cmdline: --5c8d8ab7 MD5: F4D1470AF3A7D82560B38558B132D468)
- fwdrrebrand.exe (PID: 6912 cmdline: C:\Windows\SysWOW64\fwdrrebrand.exe MD5: F4D1470AF3A7D82560B38558B132D468)
  - fwdrrebrand.exe (PID: 6928 cmdline: --1cbc15eb MD5: F4D1470AF3A7D82560B38558B132D468)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.911351133.0000000000E71000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.911351133.0000000000E71000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0xfad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 07 E8 0 0 85 C0 • 0x50d4:$snippet6: 33 C0 21 05 FC 26 E8 00 A3 F8 26 E8 00 39 05 90 F3 E7 00 74 18 40 A3 F8 26 E8 00 83 3C C5 90 F3 ...
00000001.00000002.659738344.00000000023E1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.659738344.00000000023E1000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0xfad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 07 3F 0 2 85 C0 • 0x50d4:$snippet6: 33 C0 21 05 FC 26 3F 02 A3 F8 26 3F 02 39 05 90 F3 3E 02 74 18 40 A3 F8 26 3F 02 83 3C C5 90 F3 ...
00000001.00000002.659583488.00000000022F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 11 entries

Copyright Joe Security LLC 2021

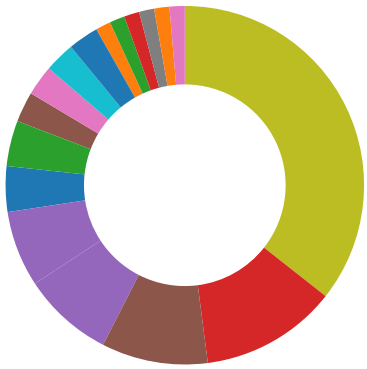
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.YF4dF4w2Cr.exe.22f053f.2.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x2577:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x255d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
1.2.YF4dF4w2Cr.exe.22f053f.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.YF4dF4w2Cr.exe.22f053f.2.unpack	Emotet	Emotet Payload	kevoreilly	• 0x7ad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 07 41 00 85 C0 • 0x48d4:$snippet6: 33 C0 21 05 FC 26 41 00 A3 F8 26 4 1 00 39 05 90 F3 40 00 74 18 40 A3 F8 26 41 00 83 3C C5 90 F3 ...
2.2.fwdrrebrand.exe.e4053f.2.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x2577:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x255d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
1.2.YF4dF4w2Cr.exe.22f053f.2.raw.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x3177:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x315d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
Click to see the 23 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

E-Banking Fraud:



Detected Emotet e-Banking trojan

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:

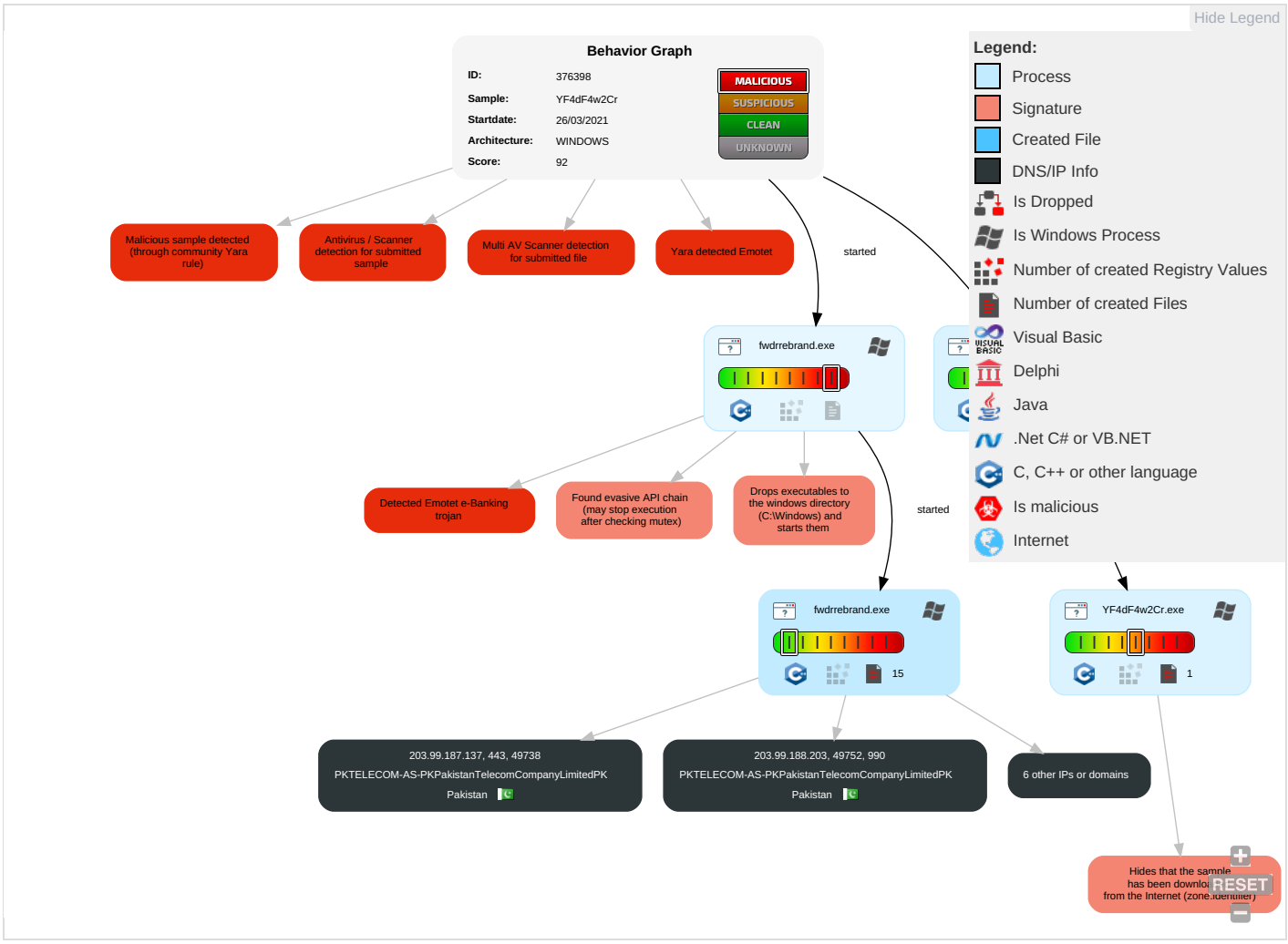


Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts 1	Native API 1 2 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	Input Capture 2	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Too Transfer 1
Default Accounts	Command and Scripting Interpreter 2	Windows Service 1 2	Access Token Manipulation 1	Obfuscated Files or Information 2	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Input Capture 2	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Service Execution 1 2	Logon Script (Windows)	Windows Service 1 2	Software Packing 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standa Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1	File Deletion 1	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 2	LSA Secrets	Security Software Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols

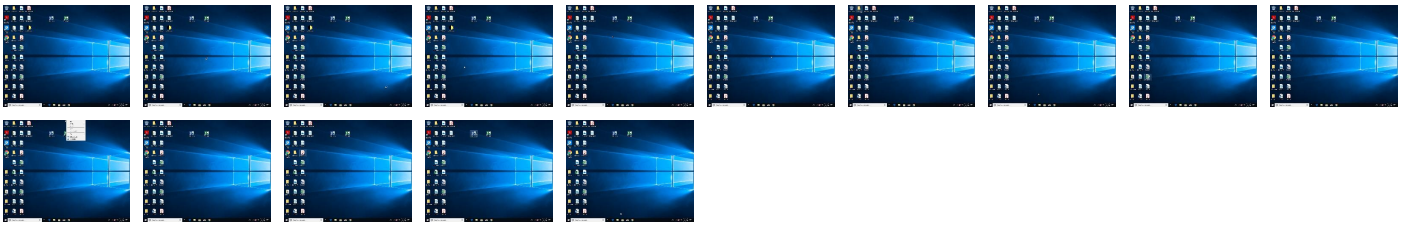
Behavior Graph



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
YF4dF4w2Cr.exe	41%	Metadefender		Browse
YF4dF4w2Cr.exe	86%	ReversingLabs	Win32.Trojan.Emotet	
YF4dF4w2Cr.exe	100%	Avira	TR/AD.Emotet.ddim	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.YF4dF4w2Cr.exe.22f053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.YF4dF4w2Cr.exe.22f053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.fwdrrebrand.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.ddim		Download File
0.2.YF4dF4w2Cr.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137917		Download File
0.0.YF4dF4w2Cr.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.ddim		Download File
3.2.fwdrrebrand.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137917		Download File
2.2.fwdrrebrand.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137917		Download File
2.2.fwdrrebrand.exe.e4053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.YF4dF4w2Cr.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.ddim		Download File
1.2.YF4dF4w2Cr.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137917		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
3.2.fwdrrebrand.exe.e4053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.fwdrrebrand.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.ddim		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://201.196.15.79/pnp/splash/loadan/merge/	0%	Avira URL Cloud	safe	

Domains and IPs

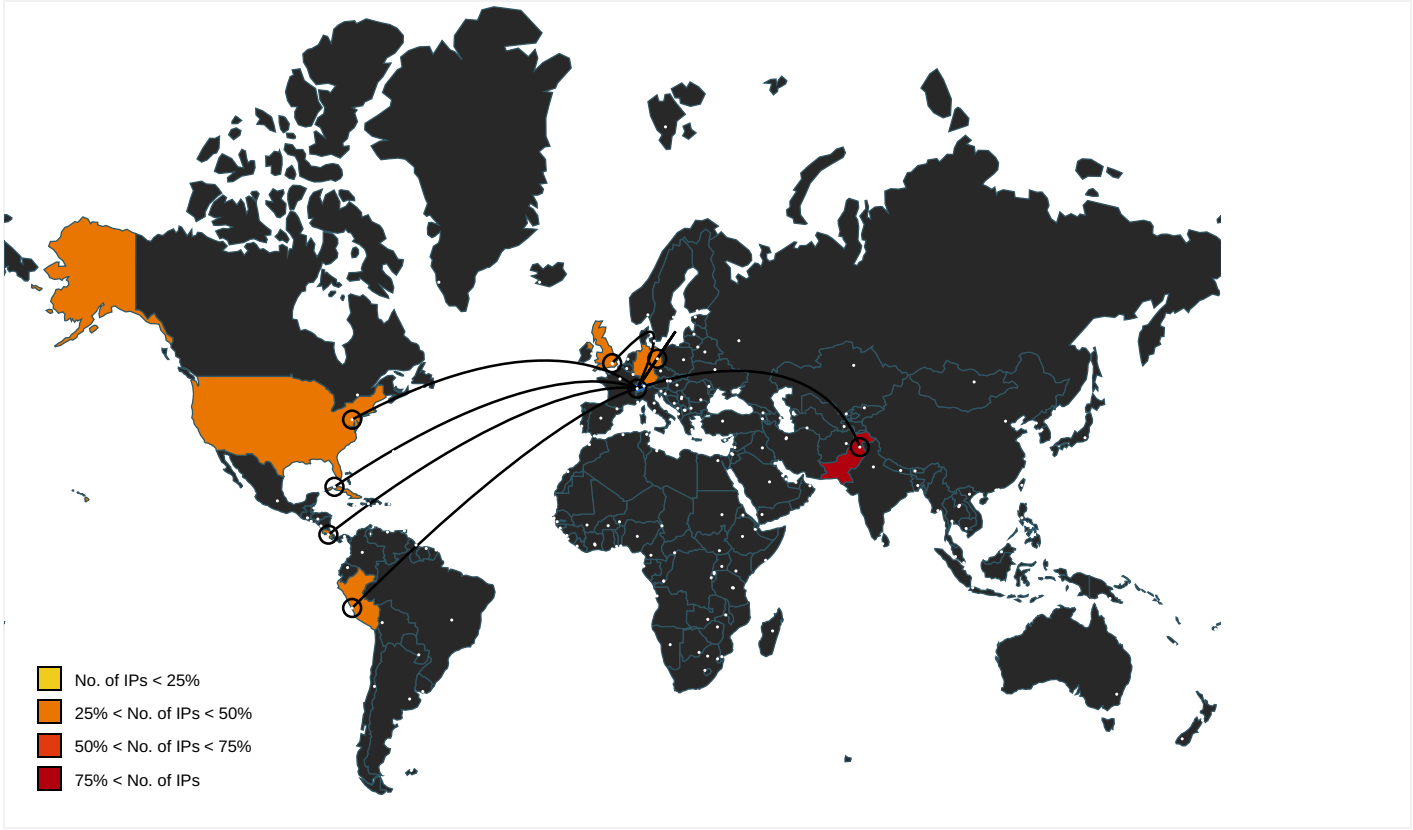
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://201.196.15.79/pnp/splash/loadan/merge/	fwdrrebrand.exe, 00000003.00000002.911061816.000000000019900.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.62.10	unknown	Germany		24940	HETZNER-ASDE	false
203.99.188.203	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
201.196.15.79	unknown	Costa Rica		11830	InstitutoCostarricensedeElectricidadyTelecomCR	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
200.55.168.82	unknown	Cuba		27725	EmpresadeTelecomunicacionesdeCubaSACU	false
213.138.100.98	unknown	United Kingdom		35425	BYTEMARK-ASGB	false
190.117.206.153	unknown	Peru		12252	AmericaMovilPeruSACPE	false
203.99.187.137	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
70.32.94.58	unknown	United States		398110	GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	376398
Start date:	26.03.2021
Start time:	13:31:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YF4dF4w2Cr (renamed file extension from none to 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:	10
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.bank.troj.evad.winEXE@6/0@0/8
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.2% (good quality ratio 59%) • Quality average: 84.1% • Quality standard deviation: 23.5%
HCA Information:	• Successful, ratio: 72% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/376398/sample/YF4dF4w2Cr.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
144.76.62.10	Payment+Summary+-+Ref+Id-+Q82.doc	Get hash	malicious	Browse	• 144.76.62.10:8080/codec/img/loadan/merge/
201.196.15.79	KjYa5KetGb.exe	Get hash	malicious	Browse	
200.55.168.82	Payment+Summary+-+Ref+Id-+Q82.doc	Get hash	malicious	Browse	
213.138.100.98	Payment+Summary+-+Ref+Id-+Q82.doc	Get hash	malicious	Browse	
190.117.206.153	Payment Summary - Ref Id- Q82.doc	Get hash	malicious	Browse	• 190.117.206.153:443/json/vermont/jit/
	description October 2019.doc	Get hash	malicious	Browse	• 190.117.206.153:443/walk/results/xian/merge/
	N.282 UPN 11.10.2019.doc	Get hash	malicious	Browse	• 190.117.206.153:443/enabled/
	20190918_90139353.doc	Get hash	malicious	Browse	• 190.117.206.153:443/pdf/stubs/loadan/
	20190918_90139353.doc	Get hash	malicious	Browse	• 190.117.206.153:443/odbc/usbccid/
	20190918_90139353.doc	Get hash	malicious	Browse	• 190.117.206.153:443/sess/
	548.exe	Get hash	malicious	Browse	• 190.117.206.153:443/add/
	20190918_90139353.doc	Get hash	malicious	Browse	• 190.117.206.153:443/stubs/
	20190918_90139353.doc	Get hash	malicious	Browse	• 190.117.206.153:443/codec/badge/
	20190918_90139353.doc	Get hash	malicious	Browse	• 190.117.206.153:443/child/mult/
	9003-09202019912.doc	Get hash	malicious	Browse	• 190.117.206.153:443/srvc/badge/jit/merge/
	9003-09202019912.doc	Get hash	malicious	Browse	• 190.117.206.153:443/sess/
	9003-09202019912.doc	Get hash	malicious	Browse	• 190.117.206.153:443/enabled/balloon/jit/merge/
	message_3392059.doc	Get hash	malicious	Browse	• 190.117.206.153:443/forced/arizona/loadan/
	message_3392059.doc	Get hash	malicious	Browse	• 190.117.206.153:443/splash/splash/pdf/
	message_3392059.doc	Get hash	malicious	Browse	• 190.117.206.153:443/nsip/jit/loadan/merge/

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documents-09_18_2019-Q212286.doc	Get hash	malicious	Browse	• 190.117.206.153:443/vermont/enable/
	Documents-09_18_2019-Q212286.doc	Get hash	malicious	Browse	• 190.117.206.153:443/nsip/free/jit/merge/
	Documents-09_18_2019-Q212286.doc	Get hash	malicious	Browse	• 190.117.206.153:443/sym/img/loadan/merge/
	Soumissions_19092019-5002924.doc	Get hash	malicious	Browse	• 190.117.206.153:443/publish/enable/jit/merge/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
InstitutoCostarricensedeElectricidadyTelecomCR	1.sh	Get hash	malicious	Browse	• 190.171.2.203
	7mB0FoVcSn.exe	Get hash	malicious	Browse	• 201.203.99.129
	rJz6SePuqu.dll	Get hash	malicious	Browse	• 201.203.96.60
	KjYa5KetGb.exe	Get hash	malicious	Browse	• 201.196.15.79
	68Faktura_VAT_8263562736.js	Get hash	malicious	Browse	• 200.91.115.40
	68Faktura_VAT_837478883422.js	Get hash	malicious	Browse	• 200.91.115.40
	INV-DK7408221-609.doc	Get hash	malicious	Browse	• 181.193.115.50
	http://nowley-rus.ru/administrator/cache/En_us/Black-Friday	Get hash	malicious	Browse	• 181.193.115.50
	Invoice_WCO5655_file.doc	Get hash	malicious	Browse	• 181.193.115.50
	INVOICE_NN6267_FILE.doc	Get hash	malicious	Browse	• 181.193.115.50
	dark.arm	Get hash	malicious	Browse	• 201.206.147.94
	vnc.exe	Get hash	malicious	Browse	• 201.197.138.2
	qwerty2.exe	Get hash	malicious	Browse	• 200.91.115.40
	9ZtszOkjm.exe	Get hash	malicious	Browse	• 201.237.32.61
	6520188910_891086.jpg.js	Get hash	malicious	Browse	• 200.91.115.40
	Phot.exe	Get hash	malicious	Browse	• 181.193.42.2
	INV_201901_FXJ47525663-991.doc	Get hash	malicious	Browse	• 201.194.127.211
	INV_201901_FXJ47525663-991.doc	Get hash	malicious	Browse	• 201.194.127.211
	adminsvcs.exe	Get hash	malicious	Browse	• 201.194.127.211
	FA_25012019_91386378.doc	Get hash	malicious	Browse	• 201.194.127.211
HETZNER-ASDE	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 144.76.242.196
	2sOfVsf40V.exe	Get hash	malicious	Browse	• 88.99.66.31
	mIkTGifBOr.exe	Get hash	malicious	Browse	• 195.201.225.248
	JJvkhWtyEm.exe	Get hash	malicious	Browse	• 195.201.225.248
	ajESKclz8f.exe	Get hash	malicious	Browse	• 88.99.66.31
	ed8a7ffec56f450a365e758012db092883bbd23565f3f.exe	Get hash	malicious	Browse	• 78.46.142.223
	KsNar1S9Ao.exe	Get hash	malicious	Browse	• 78.46.142.223
	81e32711095862add92b6628569a86fad212e146dc41b.exe	Get hash	malicious	Browse	• 78.46.142.223
	3688975dcd3f7829cfe55f7dd46166e0d6bd46c842c16.exe	Get hash	malicious	Browse	• 78.46.142.223
	uLVu6RlD4i.exe	Get hash	malicious	Browse	• 195.201.225.248
	hLOTlwUNup.exe	Get hash	malicious	Browse	• 88.99.66.31
	vZzN8hoqnD.exe	Get hash	malicious	Browse	• 88.99.66.31
	lm2LHApR75.exe	Get hash	malicious	Browse	• 195.201.225.248
	06607b04da0cd27e4a7abff3df7ee0be86df8226e81a5.exe	Get hash	malicious	Browse	• 78.46.142.223
	ZYKk8dtiEk.exe	Get hash	malicious	Browse	• 78.46.142.223
	FileZilla_3.53.0_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 49.12.121.47
	dUVOxpQFkT.exe	Get hash	malicious	Browse	• 78.46.142.223

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RsApxCz3YQ.exe	Get hash	malicious	Browse	• 195.201.225.248
	l59qWeKoK3.exe	Get hash	malicious	Browse	• 195.201.225.248
	83f723bc00bdf9847f4c2940332ef62253dd09d4b324b.exe	Get hash	malicious	Browse	• 78.46.142.223
PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	1.sh	Get hash	malicious	Browse	• 182.186.35.164
	Payment TT Copy. PDF.exe	Get hash	malicious	Browse	• 182.180.156.51
	PDFXCview.exe	Get hash	malicious	Browse	• 39.41.93.184
	mssecsvc.exe	Get hash	malicious	Browse	• 182.190.53.85
	iuE5dYsTLd.exe	Get hash	malicious	Browse	• 182.186.127.118
	i	Get hash	malicious	Browse	• 119.157.148.99
	JaQ0skAudI.exe	Get hash	malicious	Browse	• 182.186.89.232
	Y9UrMMIwN8.exe	Get hash	malicious	Browse	• 39.52.155.1
	SALES AND EXPENSES.xls	Get hash	malicious	Browse	• 182.186.224.209
	FhqpDjkst.exe	Get hash	malicious	Browse	• 182.180.143.39
	INV-XVH-O086312.doc	Get hash	malicious	Browse	• 182.180.77.215
	INV-XVH-O086312.doc	Get hash	malicious	Browse	• 182.180.77.215
	17Bill of lading Status_pdf.exe	Get hash	malicious	Browse	• 182.176.115.69
	mssecsvr.exe	Get hash	malicious	Browse	• 39.36.213.233
	zilla.exe	Get hash	malicious	Browse	• 182.182.230.248
	MP3Rocket.exe	Get hash	malicious	Browse	• 182.186.105.125
	a0UaSwRbSm.exe	Get hash	malicious	Browse	• 119.158.43.166
	41messag.exe	Get hash	malicious	Browse	• 39.58.46.97
	formneutral.exe	Get hash	malicious	Browse	• 182.180.170.72
	http://svai-nkt.ru/En/corporation/Invoice_number/jQxe-VGfy_PVswUKb-ZLx	Get hash	malicious	Browse	• 39.61.49.128

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):	6.584976742352093
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:	YF4dF4w2Cr.exe
File size:	502272
MD5:	f4d1470af3a7d82560b38558b132d468
SHA1:	0c45cf4e32116eae8d73b52c140f5d91a19ee8ea
SHA256:	6fa0dd6002d4b4e7ebabefc7f4f90f36fc53069e0cf4e845f683fb087d476e90
SHA512:	1f45093e1509d86ab03ee2c6f15a6dbc3ed4f41cac3c8faf5ae66445b787b58bf9e69d047d7ead3d1d22284d351fbb139a7a7eb73180f746f3d4f621859206c8

General

SSDEEP:	12288:x1n6BAlECcMIR4WlptZ2uOIR4bi6/Myw52BLhDG5Fq:x16SbcMMlpLLOS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8...V...V...V..s;...V..s-...V...W...V.....V.....V.....X.V.....V.....V.....V.Rich..V.....PE..L..

File Icon



Icon Hash:	64e4c4e4e4c4e4f0

Static PE Info

General

Entrypoint:	0x4316ec
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5D99FBDA [Sun Oct 6 14:36:10 2019 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:	9f251661407b9fa6502b6b65d148504e

Entrypoint Preview

Instruction
call 00007FBC6C9E301Dh
jmp 00007FBC6C9D8B5Dh
push 0000000Ch
push 0045DF00h
call 00007FBC6C9D8DFBh
mov esi, dword ptr [ebp+08h]
test esi, esi
je 00007FBC6C9D8D57h
cmp dword ptr [00468784h], 03h
jne 00007FBC6C9D8D25h
push 00000004h
call 00007FBC6C9E168Bh
pop ecx
and dword ptr [ebp-04h], 00000000h
push esi
call 00007FBC6C9E16B3h
pop ecx
mov dword ptr [ebp-1Ch], eax
test eax, eax
je 00007FBC6C9D8CEBh
push esi
push eax
call 00007FBC6C9E16D4h
pop ecx
pop ecx
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007FBC6C9D8CF0h
cmp dword ptr [ebp-1Ch], 00000000h

Instruction
jne 00007FBC6C9D8D19h
push dword ptr [ebp+08h]
jmp 00007FBC6C9D8CECh
push 00000004h
call 00007FBC6C9E1577h
pop ecx
ret
push esi
push 00000000h
push dword ptr [00466EACh]
call dword ptr [0044E22Ch]
test eax, eax
jne 00007FBC6C9D8CF8h
call 00007FBC6C9D92B6h
mov esi, eax
call dword ptr [0044E3ACh]
push eax
call 00007FBC6C9D9266h
mov dword ptr [esi], eax
pop ecx
call 00007FBC6C9D8DBFh
ret
mov edi, edi
push ebp
mov ebp, esp
push 00000000h
push dword ptr [ebp+14h]
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FBC6C9E3008h
add esp, 14h
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push ebx
xor ebx, ebx
push esi
push edi
cmp eax, ebx
je 00007FBC6C9D8CE9h
mov edi, dword ptr [ebp+00h]

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [C] VS2005 build 50727 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [EXP] VS2008 build 21022 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x61080	0x45	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5eb04	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x69000	0x182e2	.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	

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x57c60	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4e000	0x704	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x5ea54	0x40	.rdata
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	0x4c25b	0x4c400	False	0.565689036885	data	6.53895852223	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4e000	0x130c5	0x13200	False	0.320606107026	data	5.00400278699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x62000	0x67b8	0x2c00	False	0.302379261364	data	4.20689124117	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x69000	0x182e2	0x18400	False	0.639839722938	data	6.84520055945	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x6a6bc	0x134	data	English	United States
RT_CURSOR	0x6a7f0	0xb4	data	English	United States
RT_CURSOR	0x6a8a4	0x134	data	English	United States
RT_CURSOR	0x6a9d8	0xb4	data	English	United States
RT_CURSOR	0x6aa8c	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6abc0	0xb4	data	English	United States
RT_CURSOR	0x6ac74	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6ada8	0xb4	data	English	United States
RT_CURSOR	0x6ae5c	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6af90	0xb4	data	English	United States
RT_CURSOR	0x6b044	0x200	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6b244	0xb4	data	English	United States
RT_CURSOR	0x6b2f8	0x200	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6b4f8	0xb4	data	English	United States
RT_CURSOR	0x6b5ac	0x200	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6b7ac	0xb4	data	English	United States
RT_CURSOR	0x6b860	0x200	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6ba60	0xb4	data	English	United States
RT_CURSOR	0x6bb14	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6bc48	0xb4	data	English	United States
RT_CURSOR	0x6bcfc	0x134	data	English	United States
RT_CURSOR	0x6be30	0xb4	data	English	United States
RT_CURSOR	0x6bee4	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6c018	0x134	data	English	United States
RT_CURSOR	0x6c14c	0x134	data	English	United States
RT_CURSOR	0x6c280	0x134	data	English	United States
RT_CURSOR	0x6c3b4	0x134	data	English	United States
RT_CURSOR	0x6c4e8	0x134	data	English	United States
RT_CURSOR	0x6c61c	0x134	data	English	United States
RT_CURSOR	0x6c750	0x134	data	English	United States
RT_CURSOR	0x6c884	0x134	data	English	United States
RT_CURSOR	0x6c9b8	0x134	data	English	United States
RT_CURSOR	0x6caec	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x6cc20	0x134	data	English	United States
RT_CURSOR	0x6cd54	0x134	data	English	United States
RT_CURSOR	0x6ce88	0x134	data	English	United States
RT_CURSOR	0x6cfbc	0x134	data	English	United States
RT_CURSOR	0x6d0f0	0xb4	data	English	United States
RT_BITMAP	0x6d1a4	0x4a0	data	English	United States
RT_BITMAP	0x6d644	0xb8	data	English	United States

Copyright Joe Security LLC 2021

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x6d6fc	0x144	data	English	United States
RT_ICON	0x6d840	0x2e8	data		
RT_MENU	0x6db28	0x12c	data	English	United States
RT_MENU	0x6dc54	0x3ac	data	English	United States
RT_DIALOG	0x6e000	0x184	data	English	United States
RT_DIALOG	0x6e184	0x164	data	English	United States
RT_DIALOG	0x6e2e8	0xf2	data	English	United States
RT_DIALOG	0x6e3dc	0xdc	data	English	United States
RT_DIALOG	0x6e4b8	0xe8	data	English	United States
RT_DIALOG	0x6e5a0	0x1a2	data	English	United States
RT_DIALOG	0x6e744	0x15a	data	English	United States
RT_DIALOG	0x6e8a0	0x34	data	English	United States
RT_STRING	0x6e8d4	0x10e	data	English	United States
RT_STRING	0x6e9e4	0x204	data	English	United States
RT_STRING	0x6ebe8	0x60	data	English	United States
RT_STRING	0x6ec48	0x34	data	English	United States
RT_STRING	0x6ec7c	0x34	data	English	United States
RT_STRING	0x6ecb0	0x358	data	English	United States
RT_STRING	0x6f008	0x3a	data	English	United States
RT_STRING	0x6f044	0x208	data	English	United States
RT_STRING	0x6f24c	0xb0	data	English	United States
RT_STRING	0x6f2fc	0x298	data	English	United States
RT_STRING	0x6f594	0x1ea	data	English	United States
RT_STRING	0x6f780	0xf0	data	English	United States
RT_STRING	0x6f870	0xaa	data	English	United States
RT_STRING	0x6f91c	0x46	data	English	United States
RT_STRING	0x6f964	0x86	data	English	United States
RT_STRING	0x6f9ec	0x1f8	data	English	United States
RT_STRING	0x6fbe4	0xae	data	English	United States
RT_STRING	0x6fc94	0xb2	data	English	United States
RT_STRING	0x6fd48	0x2a	data	English	United States
RT_STRING	0x6fd74	0x184	data	English	United States
RT_STRING	0x6fef8	0x124	data	English	United States
RT_STRING	0x7001c	0x4a	data	English	United States
RT_STRING	0x70068	0x4e6	data	English	United States
RT_STRING	0x70550	0x264	data	English	United States
RT_STRING	0x707b4	0x2da	data	English	United States
RT_STRING	0x70a90	0x8a	data	English	United States
RT_STRING	0x70b1c	0x19a	data	English	United States
RT_STRING	0x70cb8	0xde	data	English	United States
RT_STRING	0x70d98	0x4a8	data	English	United States
RT_STRING	0x71240	0x228	data	English	United States
RT_STRING	0x71468	0x2c	data	English	United States
RT_STRING	0x71494	0x42	data	English	United States
RT_ACCELERATOR	0x714d8	0x78	data	English	United States
RT_ACCELERATOR	0x71550	0x18	data	English	United States
RT_RCDATA	0x71568	0xf944	data		
RT_GROUP_CURSOR	0x80eac	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80ed0	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80ef4	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80f18	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80f3c	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80f60	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80f84	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80fa8	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80fcc	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x80ff0	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x81014	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x81038	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x8105c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81070	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81084	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81098	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x810ac	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x810c0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x810d4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x810e8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x810fc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81110	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81124	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81138	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x8114c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81160	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0x81174	0x14	data		
RT_MANIFEST	0x81188	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetACP, IsValidCodePage, LCMapStringW, VirtualFree, HeapCreate, GetStdHandle, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetSystemTimeAsFileTime, InitializeCriticalSectionAndSpinCount, IsDebuggerPresent, GetConsoleCP, GetConsoleMode, LCMapStringA, GetStringTypeA, GetStringTypeW, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, GetLocaleInfoW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, CompareStringW, SetEnvironmentVariableA, SetUnhandledExceptionFilter, UnhandledExceptionFilter, SetEvent, TerminateProcess, HeapSize, CreateThread, ExitThread, ExitProcess, HeapReAlloc, VirtualAlloc, HeapFree, GetStartupInfoA, GetCommandLineA, HeapAlloc, RaiseException, RtlUnwind, GetTickCount, SetErrorMode, GetFileSizeEx, LocalFileTimeToFileTime, FileTimeToLocalFileTime, CreateFileA, GetShortPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, lstrcmpiA, GetStringTypeExA, DeleteFileA, MoveFileA, GetCurrentDirectoryA, GetPrivateProfileStringA, WritePrivateProfileStringA, GetPrivateProfileIntA, SystemTimeToFileTime, FileTimeToSystemTime, GetThreadLocale, GetOEMCP, GetCPInfo, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, GlobalHandle, GlobalReAlloc, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, LocalAlloc, InterlockedIncrement, GetModuleHandleW, GlobalFlags, InterlockedDecrement, GetModuleFileNameW, GetDiskFreeSpaceA, GetFullPathNameA, GetTempFileNameA, GetFileTime, SetFileTime, GetFileAttributesA, SuspendThread, ResumeThread, SetThreadPriority, CloseHandle, GetCurrentThread, ConvertDefaultLocale, EnumResourceLanguagesA, GetModuleFileNameA, GetLocaleInfoA, InterlockedExchange, lstrcmpA, GetCurrentThreadId, GlobalFindAtomA, GlobalDeleteAtom, FreeLibrary, CompareStringA, lstrcmpW, GetVersionExA, GetCurrentProcessId, GlobalGetAtomNameA, GlobalAddAtomA, GetProcAddress, GetModuleHandleA, LoadLibraryA, FreeResource, GlobalFree, GlobalAlloc, GlobalLock, GlobalUnlock, FormatMessageA, LocalFree, MultiByteToWideChar, MulDiv, lstrlenA, GetLastError, SetLastError, Sleep, GetExitCodeThread, CreateEventA, WideCharToMultiByte, FindResourceA, LoadResource, LockResource, SizeofResource, GetVersion, WaitForSingleObject, ResetEvent, GetTimeZoneInformation

DLL	Import
USER32.dll	RegisterClipboardFormatA, GetDCEx, EndPaint, BeginPaint, GetWindowDC, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, WindowFromPoint, GetSysColorBrush, GetMenuItemInfoA, InflateRect, DestroyCursor, SetRect, LoadCursorA, SetCapture, KillTimer, SetTimer, ClientToScreen, SetWindowRgn, DrawIcon, FillRect, CreateDialogIndirectParamA, GetNextDlgTabItem, EndDialog, ShowOwnedPopups, GetMessageA, TranslateMessage, GetCursorPos, ValidateRect, PostQuitMessage, SetParent, GetSystemMenu, DeleteMenu, IsRectEmpty, SetWindowTextA, IsDialogMessageA, SetDlgItemTextA, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, LoadBitmapA, ModifyMenuA, EnableMenuItem, CheckMenuItem, RegisterWindowMessageA, SendDlgItemMessageA, IsChild, SetWindowsHookExA, CallNextHookEx, GetClassLongA, SetPropA, GetPropA, RemovePropA, GetFocus, GetWindowTextA, GetForegroundWindow, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, DestroyWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, MapWindowPoints, ScrollWindow, TrackPopupMenu, SetScrollRange, GetScrollRange, SetScrollPos, GetScrollPos, SetForegroundWindow, ShowScrollBar, MessageBoxA, GetClassInfoExA, RegisterClassA, ScreenToClient, DeferWindowPos, GetScrollInfo, SetScrollInfo, DefWindowProcA, CallWindowProcA, SystemParametersInfoA, GetWindowPlacement, IsZoomed, GetClassNameA, UnpackDDElParam, ReuseDDElParam, LoadMenuA, DestroyMenu, WinHelpA, SetFocus, GetWindowThreadProcessId, IsWindowEnabled, EqualRect, GetDlgItem, GetDlgCtrlID, GetKeyState, LoadIconA, SetCursor, PeekMessageA, GetCapture, ReleaseCapture, LoadAcceleratorsA, SetActiveWindow, IsWindowVisible, IsIconic, InsertMenuItemA, CreatePopupMenu, GetClassInfoA, IntersectRect, OffsetRect, CopyRect, GetLastActivePopup, SetMenu, GetDesktopWindow, GetWindow, ShowWindow, GetSysColor, InvalidateRect, UnregisterClassA, GetTabbedTextExtentA, PostThreadMessageA, CreateMenu, CopyAcceleratorTableA, CharUpperA, DestroyIcon, GetWindowTextLengthA, LockWindowUpdate, GetWindowRect, SetRectEmpty, PtInRect, GetDC, GetSystemMetrics, ReleaseDC, GetMenuState, GetMenuStringA, AppendMenuA, InsertMenuA, RemoveMenu, AdjustWindowRectEx, RedrawWindow, SetWindowPos, GetClientRect, GetWindowLongA, SetWindowLongA, IsWindow, TranslateAcceleratorA, TranslateMDISysAccel, BringWindowToTop, GetActiveWindow, DrawMenuBar, CreateWindowExA, GetParent, GetMenuItemCount, GetSubMenu, GetMenuItemID, DefMDIChildProcA, GetMenu, DefFrameProcA, SendMessageA, LoadStringW, EnableWindow, UpdateWindow, PostMessageA, DispatchMessageA
GDI32.dll	SelectClipRgn, CreateRectRgn, GetViewportExtEx, GetWindowExtEx, GetPixel, PtVisible, RectVisible, SetPolyFillMode, TextOutA, Escape, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowOrgEx, SetWindowExtEx, ScaleWindowExtEx, GetCurrentPositionEx, CreatePatternBrush, CreateSolidBrush, CreateRectRgnIndirect, SetRectRgn, CombineRgn, GetNearestColor, GetBkMode, GetPolyFillMode, GetROP2, GetStretchBltMode, GetTextColor, GetTextAlign, GetTextFaceA, GetTextExtentPointA, GetWindowOrgEx, SetBkMode, RestoreDC, SaveDC, GetBkColor, ExtTextOutA, SetTextAlign, MoveToEx, LineTo, IntersectClipRect, ExcludeClipRect, SetMapMode, SetStretchBltMode, GetDeviceCaps, BitBlt, CreateFontIndirectA, GetStockObject, PatBlt, Rectangle, GetViewportOrgEx, CreatePen, EndDoc, AbortDoc, SetAbortProc, EndPage, StartPage, StartDocA, Ellipse, LPtoDP, DPtoLP, CreateEllipticRgn, CreateBitmap, SetBkColor, SetTextColor, GetClipBox, GetTextExtentPoint32A, GetTextMetricsA, CreateCompatibleBitmap, CreateCompatibleDC, StretchDIBits, DeleteDC, GetObjectA, CreateFontA, SelectObject, GetCharWidthA, DeleteObject, CreateDCA, SetROP2
COMDLG32.dll	GetFileTitleA
WINSPOOL.DRV	ClosePrinter, OpenPrinterA, GetJobA, DocumentPropertiesA
ADVAPI32.dll	RegSetValueExA, RegCreateKeyA, RegCreateKeyExA, GetFileSecurityA, SetFileSecurityA, RegQueryValueA, RegOpenKeyA, RegEnumKeyA, RegDeleteKeyA, RegOpenKeyExA, RegQueryValueExA, RegSetValueA, RegCloseKey, RegDeleteValueA
SHELL32.dll	DragFinish, DragQueryFileA, ExtractIconA, SHGetFileInfoA, DragAcceptFiles
SHLWAPI.dll	PathRemoveExtensionA, PathFindFileNameA, PathStripToRootA, PathIsUNCA, PathFindExtensionA, PathRemoveFileSpecW
ole32.dll	OleDestroyMenuDescriptor, OleCreateMenuDescriptor, IsAccelerator, OleTranslateAccelerator, CoInitializeEx, CoUninitialize, CoCreateInstance, CoTaskMemFree
OLEAUT32.dll	SysAllocStringLen, VariantChangeType, VariantClear, VariantInit

Exports

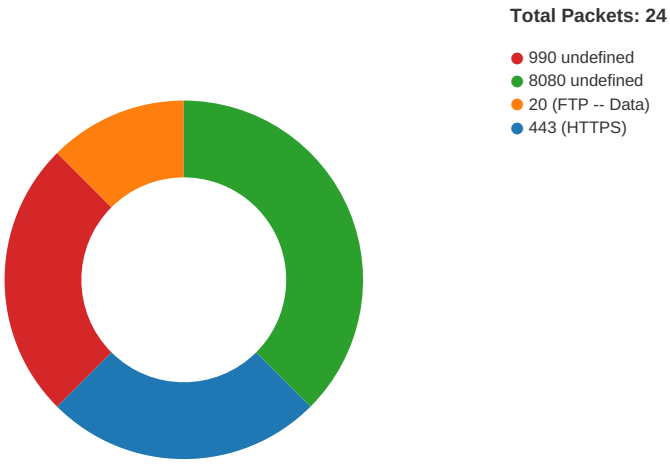
Name	Ordinal	Address
Run	1	0x4037c0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

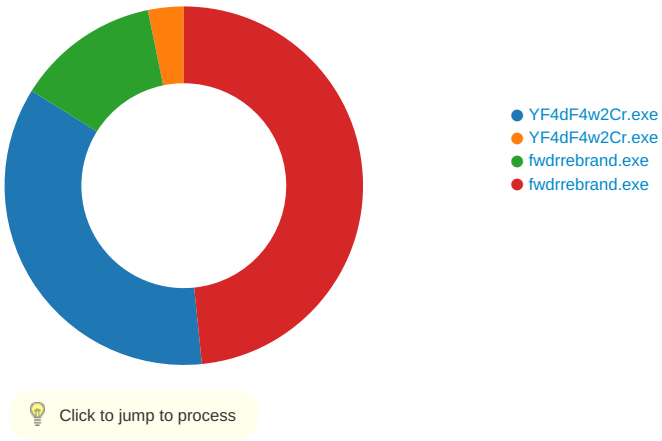
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 26, 2021 13:32:21.149575949 CET	49726	443	192.168.2.4	190.117.206.153
Mar 26, 2021 13:32:24.137447119 CET	49726	443	192.168.2.4	190.117.206.153
Mar 26, 2021 13:32:30.138016939 CET	49726	443	192.168.2.4	190.117.206.153
Mar 26, 2021 13:32:46.299501896 CET	49738	443	192.168.2.4	203.99.187.137
Mar 26, 2021 13:32:46.539707899 CET	443	49738	203.99.187.137	192.168.2.4
Mar 26, 2021 13:32:47.045715094 CET	49738	443	192.168.2.4	203.99.187.137
Mar 26, 2021 13:32:47.283056974 CET	443	49738	203.99.187.137	192.168.2.4
Mar 26, 2021 13:32:47.795870066 CET	49738	443	192.168.2.4	203.99.187.137
Mar 26, 2021 13:32:48.117441893 CET	443	49738	203.99.187.137	192.168.2.4
Mar 26, 2021 13:32:52.279159069 CET	49739	20	192.168.2.4	200.55.168.82
Mar 26, 2021 13:32:55.280688047 CET	49739	20	192.168.2.4	200.55.168.82
Mar 26, 2021 13:33:01.296782970 CET	49739	20	192.168.2.4	200.55.168.82
Mar 26, 2021 13:33:18.696319103 CET	49747	8080	192.168.2.4	70.32.94.58
Mar 26, 2021 13:33:18.809274912 CET	8080	49747	70.32.94.58	192.168.2.4
Mar 26, 2021 13:33:19.314100027 CET	49747	8080	192.168.2.4	70.32.94.58
Mar 26, 2021 13:33:19.425592899 CET	8080	49747	70.32.94.58	192.168.2.4
Mar 26, 2021 13:33:19.939344883 CET	49747	8080	192.168.2.4	70.32.94.58
Mar 26, 2021 13:33:20.051001072 CET	8080	49747	70.32.94.58	192.168.2.4
Mar 26, 2021 13:33:23.146354914 CET	49748	8080	192.168.2.4	213.138.100.98
Mar 26, 2021 13:33:23.184562922 CET	8080	49748	213.138.100.98	192.168.2.4
Mar 26, 2021 13:33:23.689268112 CET	49748	8080	192.168.2.4	213.138.100.98
Mar 26, 2021 13:33:23.727399111 CET	8080	49748	213.138.100.98	192.168.2.4
Mar 26, 2021 13:33:24.236388922 CET	49748	8080	192.168.2.4	213.138.100.98
Mar 26, 2021 13:33:24.274235964 CET	8080	49748	213.138.100.98	192.168.2.4
Mar 26, 2021 13:33:28.601304054 CET	49751	8080	192.168.2.4	144.76.62.10
Mar 26, 2021 13:33:28.625920057 CET	8080	49751	144.76.62.10	192.168.2.4
Mar 26, 2021 13:33:29.127257109 CET	49751	8080	192.168.2.4	144.76.62.10
Mar 26, 2021 13:33:29.152199984 CET	8080	49751	144.76.62.10	192.168.2.4
Mar 26, 2021 13:33:29.658544064 CET	49751	8080	192.168.2.4	144.76.62.10
Mar 26, 2021 13:33:29.680944920 CET	8080	49751	144.76.62.10	192.168.2.4
Mar 26, 2021 13:33:33.485486031 CET	49752	990	192.168.2.4	203.99.188.203
Mar 26, 2021 13:33:33.705632925 CET	990	49752	203.99.188.203	192.168.2.4
Mar 26, 2021 13:33:34.221575022 CET	49752	990	192.168.2.4	203.99.188.203
Mar 26, 2021 13:33:34.439589024 CET	990	49752	203.99.188.203	192.168.2.4
Mar 26, 2021 13:33:34.940423965 CET	49752	990	192.168.2.4	203.99.188.203
Mar 26, 2021 13:33:35.159921885 CET	990	49752	203.99.188.203	192.168.2.4
Mar 26, 2021 13:33:38.379935980 CET	49753	990	192.168.2.4	201.196.15.79
Mar 26, 2021 13:33:41.378377914 CET	49753	990	192.168.2.4	201.196.15.79
Mar 26, 2021 13:33:47.378798962 CET	49753	990	192.168.2.4	201.196.15.79

Code Manipulations

Copyright Joe Security LLC 2021

Statistics

Behavior



System Behavior

Analysis Process: YF4dF4w2Cr.exe PID: 6836 Parent PID: 5912

General

Start time:	13:31:52
Start date:	26/03/2021
Path:	C:\Users\user\Desktop\YF4dF4w2Cr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\YF4dF4w2Cr.exe'
Imagebase:	0x400000
File size:	502272 bytes
MD5 hash:	F4D1470AF3A7D82560B38558B132D468
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: 00000000.00000002.646512151.0000000002311000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.646512151.0000000002311000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.646499888.00000000022F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.646499888.00000000022F0000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.RCL\ShellNew	success or wait	1	420001	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1	NULL	unicode	Recalc Document	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\DefaultIcon	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE,0	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\open\ddeexec	NULL	unicode	[open("%1")]	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\print\ddeexec	NULL	unicode	[print("%1")]	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\printto\ddeexec	NULL	unicode	[printto("%1","%2","%3","%4")]	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\open\command	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE /dde	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\print\command	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE /dde	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\printto\command	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE /dde	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.RCL	NULL	unicode	Recalc.Document.1	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.RCL\ShellNew	NullFile	unicode		success or wait	1	427268	RegSetValueExA

Analysis Process: YF4dF4w2Cr.exe PID: 6856 Parent PID: 6836

General

Start time:	13:31:52
Start date:	26/03/2021
Path:	C:\Users\user\Desktop\YF4dF4w2Cr.exe
Wow64 process (32bit):	true
Commandline:	--5c8d8ab7
Imagebase:	0x400000
File size:	502272 bytes
MD5 hash:	F4D1470AF3A7D82560B38558B132D468
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: 00000001.00000002.659738344.00000000023E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.659738344.00000000023E1000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.659583488.00000000022F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.659583488.00000000022F0000.00000040.00000001.sdmp, Author: kevoreilly
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\fwdrrebrand.exe:Zone.Identifier	success or wait	1	23E1126	DeleteFileW

Copyright Joe Security LLC 2021

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: fwdrrebrand.exe PID: 6912 Parent PID: 568

General

Start time:	13:31:57
Start date:	26/03/2021
Path:	C:\Windows\SysWOW64\fwdrrebrand.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\fwdrrebrand.exe
Imagebase:	0x400000
File size:	502272 bytes
MD5 hash:	F4D1470AF3A7D82560B38558B132D468
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: 00000002.00000002.658516120.0000000000E51000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000002.00000002.658516120.0000000000E51000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.658502869.0000000000E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000002.00000002.658502869.0000000000E40000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	low

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\DefaultIcon	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE,0	C:\Windows\SysWOW64\FWDRRE~1.EXE,0	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\open\command	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE /dde	C:\Windows\SysWOW64\FWDRRE~1.EXE /dde	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\print\command	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE /dde	C:\Windows\SysWOW64\FWDRRE~1.EXE /dde	success or wait	1	42011A	RegSetValueA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Recalc.Document.1\shell\printto\command	NULL	unicode	C:\Users\user\Desktop\YF4DF4~1.EXE /dde	C:\Windows\SysWOW64\FWDRRE~1.EXE /dde	success or wait	1	42011A	RegSetValueA

Analysis Process: fwdrrebrand.exe PID: 6928 Parent PID: 6912

General

Start time:	13:31:58
Start date:	26/03/2021
Path:	C:\Windows\SysWOW64\fwdrrebrand.exe
Wow64 process (32bit):	true
Commandline:	--1cbc15eb
Imagebase:	0x400000

Copyright Joe Security LLC 2021

File size:	502272 bytes
MD5 hash:	F4D1470AF3A7D82560B38558B132D468
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: 00000003.00000002.911351133.0000000000E71000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000003.00000002.911351133.0000000000E71000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.911329225.0000000000E40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000003.00000002.911329225.0000000000E40000.00000040.00000001.sdmp, Author: kevoreilly
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	E714A5	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	E714A5	HttpSendRequestW
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	E714A5	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	E714A5	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	E714A5	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	E714A5	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	E714A5	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	E714A5	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	E714A5	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	E714A5	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	E714A5	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	E714A5	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	E714A5	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	E714A5	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	E714A5	HttpSendRequestW

Disassembly

Code Analysis