ID: 524302
Sample Name:
1RMZ62tUAl.exe
Cookbook: default.jbs
Time: 10:42:48
Date: 18/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

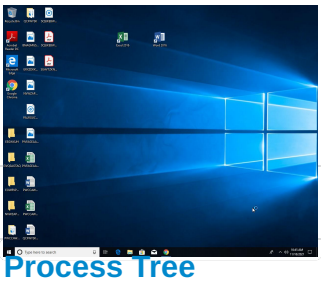
Windows Analysis Report 1RMZ62tUAl.exe

Overview

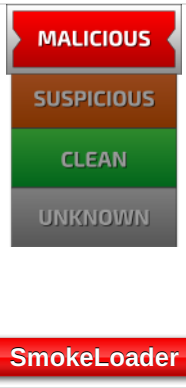
General Information

Sample Name:	1RMZ62tUAl.exe
Analysis ID:	524302
MD5:	8696a4269e30dd..
SHA1:	125198e1f636ef1..
SHA256:	47ec411eab0aa1..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

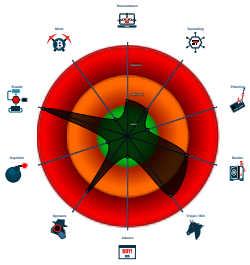


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Maps a DLL or memory area into an…
- Tries to harvest and steal Putty / Wi…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- 1RMZ62tUAl.exe (PID: 316 cmdline: "C:\Users\user\Desktop\1RMZ62tUAl.exe" MD5: 8696A4269E30DDB34A7E0E84629EDE03)
  - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 5732 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 2892 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 4424 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5056 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 3532 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 6052 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 6908 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 4760 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 6008 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 6528 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 6184 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5824 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 6264 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- favdejf (PID: 6992 cmdline: C:\Users\user\AppData\Roaming\favdejf MD5: 8696A4269E30DDB34A7E0E84629EDE03)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://rsuehfidvdkfvk.top/",
    "http://rsuehfidvdkfvk.top/"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.559721619.00000000027D1000.00000040.00020000.sdmp	JoeSecurity_SmokeLoader	Yara detected SmokeLoader	Joe Security	
00000016.00000002.555611191.000000000011000.00000040.00020000.sdmp	JoeSecurity_SmokeLoader	Yara detected SmokeLoader	Joe Security	
0000000A.00000002.424469148.0000000003C21000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000017.00000002.555126531.000000000031000.00000040.00020000.sdmp	JoeSecurity_SmokeLoader	Yara detected SmokeLoader	Joe Security	
00000019.00000002.555346763.0000000000E91000.00000040.00020000.sdmp	JoeSecurity_SmokeLoader	Yara detected SmokeLoader	Joe Security	
Click to see the 8 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Checks if browser processes are running

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Contains functionality to compare user and computer (likely to detect sandboxes)
- Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging:

- Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

- Benign windows process drops PE files
- System process connects to network (likely due to code injection or exploit)
- Maps a DLL or memory area into another process
- Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

- Yara detected SmokeLoader
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

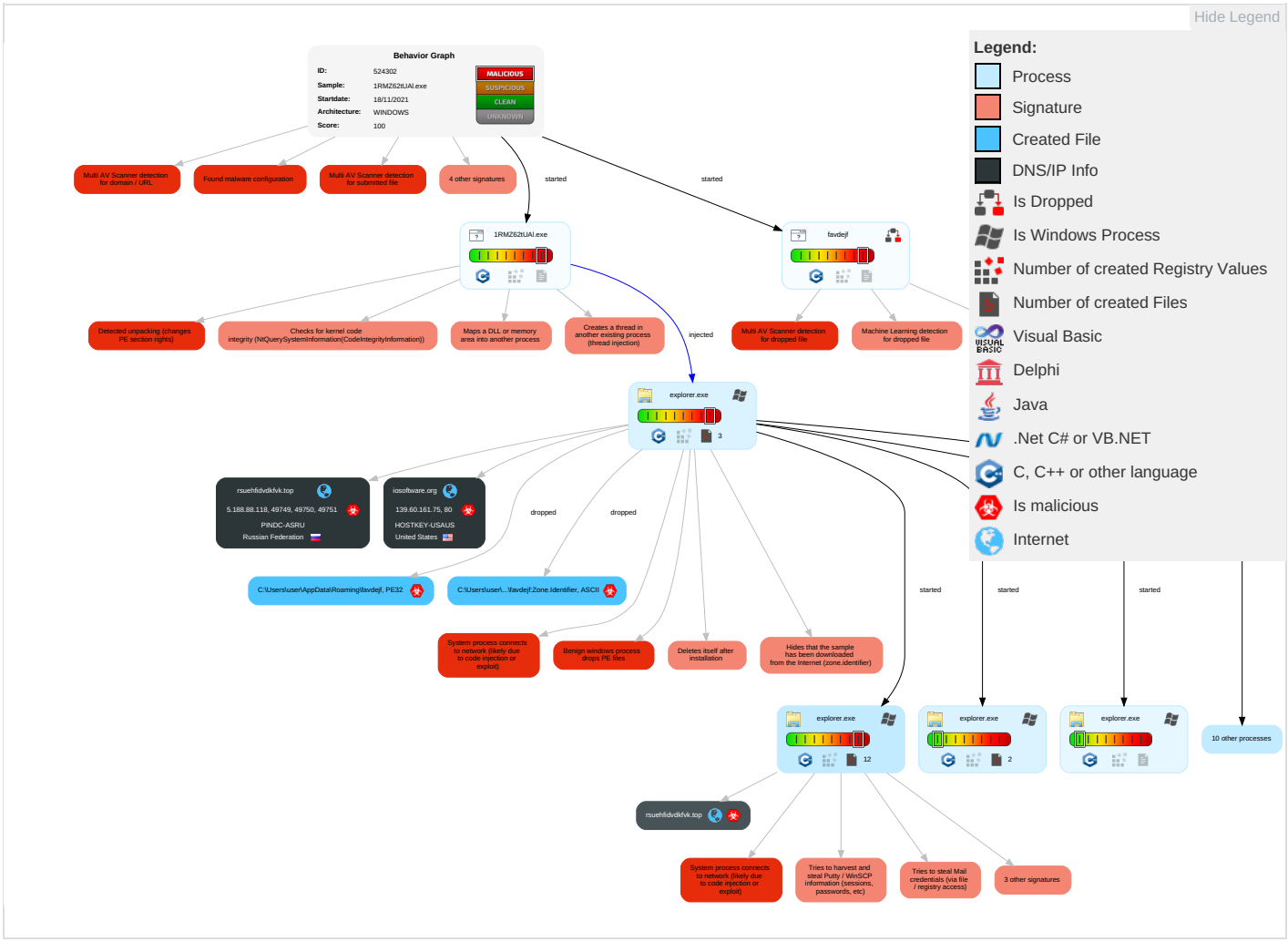
- Yara detected SmokeLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Ea Ins Ne Co
Default Accounts	Exploitation for Client Execution 1	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 3	Input Capture 2 1	File and Directory Discovery 4	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Ex Re Ca
Domain Accounts	Command and Scripting Interpreter 2	Create Account 1	Process Injection 3 1 3	Software Packing 1 1	Credentials in Registry 1	System Information Discovery 1 7	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 3	Ex Tr Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Security Software Discovery 5 5 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Application Layer Protocol 1 1 3	Sl Sv
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Virtualization/Sandbox Evasion 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Process Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 3	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rc Ba

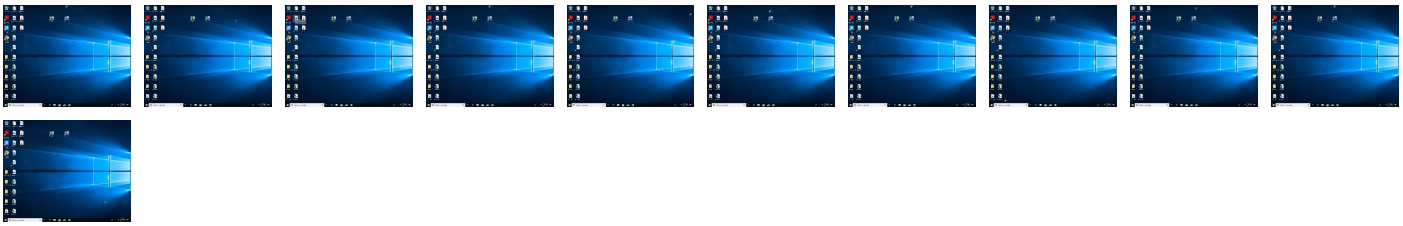
Behavior Graph



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
1RMZ62tUAl.exe	47%	Virustotal		Browse
1RMZ62tUAl.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\favdejf	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\favdejf	56%	ReversingLabs	Win32.Trojan.Babar	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.1RMZ62tUAl.exe.2150000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.favdejf.2000e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.1RMZ62tUAl.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.3.favdejf.3c00000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.1RMZ62tUAl.exe.2140e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.favdejf.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
rsuehfidvdkfvk.top	2%	Virustotal		Browse
iosoftware.org	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://rsuehfidvdkfvk.top/Mozilla/5.0	0%	Avira URL Cloud	safe	
http://rsuehfidvdkfvk.top/application/x-www-form-urlencodedMozilla/5.0	0%	Avira URL Cloud	safe	
http://rsuehfidvdkfvk.top/	0%	Avira URL Cloud	safe	
http://rsuehfidvdkfvk.top/:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rsuehfidvdkfvk.top	5.188.88.118	true	true	• 2%, Virustotal, Browse	unknown
iosoftware.org	139.60.161.75	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://rsuehfidvdkfvk.top/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.188.88.118	rsuehfidvdkfvk.top	Russian Federation		34665	PINDC-ASRU	true
139.60.161.75	iosoftware.org	United States		395839	HOSTKEY-USAUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	524302
Start date:	18.11.2021
Start time:	10:42:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1RMZ62tUAl.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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winEXE@15/6@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.5% (good quality ratio 7.9%) • Quality average: 29.9% • Quality standard deviation: 36.6%
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:44:30	Task Scheduler	Run new task: Firefox Default Browser Agent 2E48D3EE74E86FF4 path: C:\Users\user\AppData\Roaming\favdejf
10:45:15	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
5.188.88.118	4B32N61SUN.exe	Get hash	malicious	Browse	• rsuehfidvdkfvk.top/
	umpa0fYSwl.exe	Get hash	malicious	Browse	• rsuehfidvdkfvk.top/
139.60.161.75	4B32N61SUN.exe	Get hash	malicious	Browse	• iosoftware.org/system86.exe
	umpa0fYSwl.exe	Get hash	malicious	Browse	• iosoftware.org/system86.exe
	v0VaFGKpQR.exe	Get hash	malicious	Browse	• iosoftware.org/system86.exe
	Yob73TQCPI.exe	Get hash	malicious	Browse	• iosoftware.org/system86.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
rsuehfidvdkfvk.top	4B32N61SUN.exe	Get hash	malicious	Browse	• 5.188.88.118
	umpa0fYSwl.exe	Get hash	malicious	Browse	• 5.188.88.118

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	v0VaFGKpQR.exe	Get hash	malicious	Browse	• 8.209.67.58
	Yob73TQCPI.exe	Get hash	malicious	Browse	• 8.209.67.58
iosoftware.org	4B32N61SUN.exe	Get hash	malicious	Browse	• 139.60.161.75
	umpa0fYSwl.exe	Get hash	malicious	Browse	• 139.60.161.75
	v0VaFGKpQR.exe	Get hash	malicious	Browse	• 139.60.161.75
	Yob73TQCPI.exe	Get hash	malicious	Browse	• 139.60.161.75
	GwGRsPZJO7.exe	Get hash	malicious	Browse	• 139.60.161.75
	GhlYvtlwHA.exe	Get hash	malicious	Browse	• 139.60.161.75
	WSWw3rqaqL.exe	Get hash	malicious	Browse	• 139.60.161.75

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PINDC-ASRU	4B32N61SUN.exe	Get hash	malicious	Browse	• 5.188.88.118
	umpa0fYSwl.exe	Get hash	malicious	Browse	• 5.188.88.118
	Nov_SOA_MT103.xlsx	Get hash	malicious	Browse	• 91.240.242.111
	triage_dropped_file.exe	Get hash	malicious	Browse	• 91.240.242.111
	Gno6CluFsB.exe	Get hash	malicious	Browse	• 91.240.242.111
	QUOTATION REQUEST document file 465.exe	Get hash	malicious	Browse	• 91.240.242.111
	Zo7DiD3qYT.exe	Get hash	malicious	Browse	• 91.240.242.111
	s20KNIIaif.exe	Get hash	malicious	Browse	• 91.240.242.111
	fXvJwoVvee.exe	Get hash	malicious	Browse	• 91.240.242.111
	DVv7dqTcMg.exe	Get hash	malicious	Browse	• 91.240.242.111
	Quotation Forms_MV YU FENG4 TRADER.xlsx	Get hash	malicious	Browse	• 91.240.242.111
	Quotation form MV YU FENG4 TRADER.xlsx	Get hash	malicious	Browse	• 91.240.242.111
	MV Glorious Sea.xlsx	Get hash	malicious	Browse	• 91.240.242.111
	Requisition for spare parts1.xlsx	Get hash	malicious	Browse	• 91.240.242.111
	AWsh7ps5RC.exe	Get hash	malicious	Browse	• 91.240.242.111
	IxG7d9No5Q.exe	Get hash	malicious	Browse	• 5.188.88.190
	AyAj5GJqIg.exe	Get hash	malicious	Browse	• 5.188.88.203
	Md0q201V1D.exe	Get hash	malicious	Browse	• 5.188.88.203
	yj2Lz2zdxp.exe	Get hash	malicious	Browse	• 5.188.88.203
	y1JBw0eea5.exe	Get hash	malicious	Browse	• 5.188.88.203
HOSTKEY-USAUS	4B32N61SUN.exe	Get hash	malicious	Browse	• 139.60.161.75
	umpa0fYSwl.exe	Get hash	malicious	Browse	• 139.60.161.75
	v0VaFGKpQR.exe	Get hash	malicious	Browse	• 139.60.161.75
	Yob73TQCPI.exe	Get hash	malicious	Browse	• 139.60.161.75
	rMVpcZ73UK.exe	Get hash	malicious	Browse	• 139.60.160.200
	8Jem3WHfr1.exe	Get hash	malicious	Browse	• 139.60.160.200
	3Pmz7pGNI6.exe	Get hash	malicious	Browse	• 139.60.160.200
	2kozcBdouI.exe	Get hash	malicious	Browse	• 139.60.160.200
	j8Ng2Kt6YP.exe	Get hash	malicious	Browse	• 139.60.160.200
	trz51D4.exe	Get hash	malicious	Browse	• 139.60.161.68
	trz51D4.exe	Get hash	malicious	Browse	• 139.60.161.68
	mixazed.exe	Get hash	malicious	Browse	• 139.60.161.63
	service4.exe	Get hash	malicious	Browse	• 139.60.161.68
	service4.exe	Get hash	malicious	Browse	• 139.60.161.68
	file.dll	Get hash	malicious	Browse	• 139.60.161.99
	o7w2HSi17V.exe	Get hash	malicious	Browse	• 139.60.163.56
	trz51D4.exe	Get hash	malicious	Browse	• 139.60.161.68
	trz51D4.exe	Get hash	malicious	Browse	• 139.60.161.68
	evil.doc	Get hash	malicious	Browse	• 139.60.161.74
	evil.doc	Get hash	malicious	Browse	• 139.60.161.74

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\6128.tmp	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\6476.tmp	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\6708.tmp	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.5110032006906435
Encrypted:	false
SSDEEP:	12:TL1t4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwa5q0S93BPZ75fOS:TLLJLbXaFpEO5bNmISHn06UwcQPx5fB
MD5:	3219CA933D97DF8F5931EF68B7EEDF04
SHA1:	D79FEE14CBDE4E92447996C9FB37ADCB673B6138
SHA-256:	21DE8DD11459659421BA1DBC554C15A3756FF1A38CC797A139D407F1F94092B4
SHA-512:	A3CFCC17612975C5630B49736F4B535555D06B23E3523E46495020B8B55B2361C4B5EF39FE649273F2D323BE0EC138707E67DC59EB719BA8EF676439491662AC
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\cveiudv	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	modified
Size (bytes):	422174
Entropy (8bit):	**7.9995511013879135**
Encrypted:	**true**
SSDEEP:	12288:TCpGNN3qZTiF2HBupddNvuYke2ECsmcsKL6zzS1iyE/:GSN3qZT+2opdrvtksCsnsc18
MD5:	B13B4E1CB91F37EC7EB8E449AF7BAD81

C:\Users\user\AppData\Roaming\cveiudv	
SHA1:	7AF7D20E70B230670A90F14C5C8AC7B222A0411A
SHA-256:	F8352AC185B423B72C0F8D64C4E4AC80B6D56419CE27501DC2B5D7D26DDCEC64
SHA-512:	0E520B75F8ABA7F52B5295CDC6BD969B191A70B232B94CF9976F3A34983F5E6045A2E531FFAA03A006F8F62A9642E3E1FB84E73D47AC492C4A156F0B52078272
Malicious:	false
Preview:	.s..d...T6aK[.%B6.i..._5.".....e...7E..*C...5.4.....J.c...v.....+.Q.y.....>...G.n.2(...'..v...1./...~-.'.iE.Dc.n.....O[Q.}.....5.....|WT..4.".pa(...uF..R..^.%..>.....b.lP.%...g.y..) ..d.=..1..p.u....4.q..^k....B...n..9.M\.U-R....I.7?/.....<V...Y..3.....Y.q.....C..D.:...^2.Zy...)....x...p{.....w.=.X..i..{?$CV.<..;.....b.v..'...8....Hc<.l/..c...).^f.....(#...U..p..g;.P...].H..'.b.... ....G....M.....vAj..z .^+.....n..qg.s..K..3L.....n?.d.3b.....].....du7.E....SNi.D1NA...+..*2.[^...b.....&..h\|rP.=....VR..y.....3n..0.....U..n%A2....~.$W.W+..u...M.7;.X.....".._...}..Xn.-6\?L.4.R..%..B...A...$+..R8>....D....pc.h....K9u..i...A4k.*}d.EjF...`.&..M>.X..f...$F...C*?.a:....f....7.....ri9.o.#U..F..<~....C..Sj.T..M.....g.z5w.2.j....._..[[..V..KA.....cZ.0S..Z... .....1N.....<...%Y..&0`p8hSz,...W.#t...V....?.zQ..}.....B..e.F...#xW.rA.k..s....s.....WF..O_u.N.(?..J.....7.....w...o..|B3s

C:\Users\user\AppData\Roaming\favdejf	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	285184
Entropy (8bit):	5.909368896887488
Encrypted:	false
SSDEEP:	3072:80Zpf7ywrLoWHdAucQoHnSzG+dWpvgne52lPxsBvBPoeg8MRkY34R3R8UJPb9wy:RIUJcQk3+WvgnJla7oe0RdIdRzYy
MD5:	8696A4269E30DDB34A7E0E84629EDE03
SHA1:	125198E1F636EF118E468145D02E801A3FFE2A97
SHA-256:	47EC411EAB0AA15619F24CAA6256ED4CA5CFC695A26F5B71830B53B07C22B05B
SHA-512:	481AE35EC056DE3C08AE167E7B2FEA9352C82A7CD47EBBC46047270E1A0F518B3FEECE8AD6900D0A5AC5CA1B44C80DA0E916504809E93E176933931D940CAD 96
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..'t..tt..tt..t..Wt]..t..bte..t..Vt...t}.ot...tt..t...t..Stu..t..ftu..t..atu..tRi cht..t.....PE..L.... I_.....z.....@.....x....`...D.....`.....x..@..... .....text..... ..`.data....J.....@....rsrc....D...`...F.....@..@.reloc.....P.....@..B..... ....

C:\Users\user\AppData\Roaming\favdejf:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.909368896887488
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:	1RMZ62tUAl.exe
File size:	285184
MD5:	8696a4269e30ddb34a7e0e84629ede03
SHA1:	125198e1f636ef118e468145d02e801a3ffe2a97

General

SHA256:	47ec411eab0aa15619f24caa6256ed4ca5cfc695a26f5b71830b53b07c22b05b
SHA512:	481ae35ec056de3c08ae167e7b2fea9352c82a7cd47ebbc46047270e1a0f518b3feece8ad6900d0a5ac5ca1b44c80da0e916504809e93e176933931d940cad96
SSDEEP:	3072:80Zpf7ywrLoWHdAucQoHnSzG+dWpvgne52lPxsBvBPoeg8MRkY34R3R8UJPb9wy:RIUJcQk3+WvgnJla7oe0RdIdRzYy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..'t..tt..tt..t..Wt]..t..bte..t..Vt...t}.ot...tt..t...t..Stu..t..ftu..t..atu..tRicht..t.....PE..L.... I_.....

File Icon

Icon Hash:	aecaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x417ad0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F6C20F2 [Thu Sep 24 04:30:42 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	ff6439958bc7d1b926a3ea41188420fe

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2f18a	0x2f200	False	0.615742083886	data	7.06143863939	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x31000	0x1b84ac0	0x1400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1bb6000	0x44c0	0x4600	False	0.707645089286	data	6.19981176683	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1bbb000	0x10818	0x10a00	False	0.0732935855263	data	0.963621944631	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
Spanish	Paraguay	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 18, 2021 10:44:29.788239002 CET	192.168.2.3	8.8.8.8	0xeda6	Standard query (0)	rsuehfidvd kfvk.top	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:31.239069939 CET	192.168.2.3	8.8.8.8	0x3738	Standard query (0)	rsuehfidvd kfvk.top	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:31.753774881 CET	192.168.2.3	8.8.8.8	0x883d	Standard query (0)	rsuehfidvd kfvk.top	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:32.049560070 CET	192.168.2.3	8.8.8.8	0x7b89	Standard query (0)	iosoftware.org	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:49.812151909 CET	192.168.2.3	8.8.8.8	0xbc17	Standard query (0)	rsuehfidvd kfvk.top	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:50.679728985 CET	192.168.2.3	8.8.8.8	0x96a8	Standard query (0)	iosoftware.org	A (IP address)	IN (0x0001)
Nov 18, 2021 10:45:15.733613968 CET	192.168.2.3	8.8.8.8	0x1536	Standard query (0)	rsuehfidvd kfvk.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 18, 2021 10:44:30.080061913 CET	8.8.8.8	192.168.2.3	0xeda6	No error (0)	rsuehfidvd kfvk.top		5.188.88.118	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:31.259133101 CET	8.8.8.8	192.168.2.3	0x3738	No error (0)	rsuehfidvd kfvk.top		5.188.88.118	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:31.775317907 CET	8.8.8.8	192.168.2.3	0x883d	No error (0)	rsuehfidvd kfvk.top		5.188.88.118	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:32.075397015 CET	8.8.8.8	192.168.2.3	0x7b89	No error (0)	iosoftware.org		139.60.161.75	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:50.187908888 CET	8.8.8.8	192.168.2.3	0xbc17	No error (0)	rsuehfidvd kfvk.top		5.188.88.118	A (IP address)	IN (0x0001)
Nov 18, 2021 10:44:50.704993963 CET	8.8.8.8	192.168.2.3	0x96a8	No error (0)	iosoftware.org		139.60.161.75	A (IP address)	IN (0x0001)
Nov 18, 2021 10:45:15.753202915 CET	8.8.8.8	192.168.2.3	0x1536	No error (0)	rsuehfidvd kfvk.top		5.188.88.118	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- oidhj.com
  - rsuehfidvdkfvk.top
- wjigjxv.com
- mrirybsj.net
- tmmykkqa.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49749	5.188.88.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2021 10:44:30.158356905 CET	1005	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://oidhj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 338 Host: rsuehfidvdkfvk.top
Nov 18, 2021 10:44:30.514741898 CET	1007	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Thu, 18 Nov 2021 09:44:30 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 66 36 36 0d 0a 2c 01 00 00 0d ea ca f4 a9 bc c2 d2 42 81 8e 85 72 87 9b 58 60 8c d3 6c ea b8 55 27 e0 a1 b4 5e b6 34 5e b5 2b 44 fb 30 3b bc 67 5c ce fe b0 25 96 55 51 79 63 d7 60 70 55 2b e3 ef 22 79 35 f6 af 06 12 95 2f 9a 3d 93 4d 37 5a 42 f1 ab b5 95 90 bc f3 c3 36 8c 23 18 ba 54 73 c3 a9 20 6c 2f b2 93 54 fd bf db 73 3f 84 fb f5 e7 00 5e cd 13 22 cd 51 c2 19 3a c0 a2 1b 66 bc 39 14 d0 06 ed a7 6a 57 9d 82 73 7b 99 f4 a1 cf 5e 8d 37 3c bb 78 c7 58 00 b4 b7 52 a3 a1 4a 49 d1 4b 32 99 24 13 48 b6 ea ec 50 f3 a7 cc ce f2 57 ff 4b 29 f0 04 36 62 69 16 61 bb af 08 44 e6 69 bb 3c c3 ea f3 8c 5a 35 b2 fb 1a 3e 11 a4 de 25 42 ea 4b e6 60 89 13 26 de c6 22 17 42 32 ea 7b 8f 78 6e e5 2b ae 19 b3 76 5a 44 4f bb de 21 98 19 01 2f 49 a4 df 10 37 c1 f7 b6 b9 06 b8 50 96 3c 5c 81 9c 7b ee 15 3c f3 52 6c 24 12 fa e8 fe 72 b1 7f 94 17 ef 5d 66 a8 43 f3 b6 0c 51 0d 30 1b 6f a5 59 b4 d8 f8 d1 af 4b 7f f2 2d ad 31 aa eb 9e e5 cf 00 1e 71 06 00 b8 d3 34 d5 03 0f 06 00 0d 00 9c 03 00 00 c9 a6 6d fb 75 e6 cb 32 fd 66 8b 8e 41 26 0b 00 e5 c4 0d 6d 04 5e 5c e7 10 19 f4 25 09 91 e2 11 1d 20 4d 5a 26 d2 b8 dd 32 27 a3 25 c3 34 44 f1 af 41 59 5f 25 4d 9d 3c 3e 34 a2 81 d2 ca d1 51 64 d7 e5 5e 5e 84 51 60 e4 02 3b 29 c7 b1 b2 8f 87 03 6c 8f 65 32 08 3d c1 d2 8b 5b df 28 2c d3 f1 6c 90 9d e7 31 0d 81 8d ef f6 7d 15 a4 5a be 82 97 68 3b 5a 2c 32 cf 42 6b 9b 68 03 76 8b ce 62 87 63 a2 90 83 3d c1 c8 4a 9e d2 2b 50 82 9a 7a 43 69 8e 2d b6 35 4c 79 f6 f9 87 2e 92 c6 68 28 ad 22 17 5b 7a bc a2 04 1f 80 eb cd 89 67 b6 29 35 f2 db b0 f3 01 c1 5d 88 62 d6 3a 43 c4 ea 38 dd 76 40 32 7f 02 83 9d 3d ad c0 ec c8 af 83 82 42 e3 d5 7e 0f 5e 78 42 ff 89 eb 43 dc 87 39 c1 36 23 12 c7 42 2c 69 fc bf 45 d4 4c c2 12 09 5b 97 57 97 46 e3 49 da e1 0a c1 03 f1 ff 65 20 8d 3f 80 d7 45 b8 0f 83 ef 72 31 3a 85 33 e8 47 1e 4c 71 7b 8d db 39 e5 d8 86 94 2c 34 66 51 ad ca 8e ba 45 cd b5 7b f5 12 9b a0 da 2b ed 70 b9 69 f4 93 6d e6 c6 b1 44 d8 34 5e c2 e6 cb f4 e6 48 4f 8e 48 b8 66 56 c0 8a aa 26 e5 de 88 d1 77 10 49 9f 33 b5 35 d9 8d 63 2d c5 39 ea eb 6e c3 26 f9 01 ff 8c 29 4c 14 3e 59 82 64 63 17 bb 76 69 a9 27 3c 0b 0c c1 7b 0c f6 8f 76 b5 1f a3 90 4b 14 1e 92 34 24 7b fe 50 b8 45 c7 88 ff 2d 7e 60 f9 c4 c2 a6 4c 55 30 de 0e 46 76 50 8c 22 e3 5b 72 21 32 24 ee e3 34 65 ab 7c 3e 91 9c 3f 76 e5 77 3c 50 46 9f 59 46 e7 2d c3 cc 7e 32 6c e5 1d 70 61 c2 2b 7b 3c dd 0e c7 55 06 e7 4f 20 40 5a 4f dc 3d c9 23 e3 b0 e6 b7 76 fc 1c 76 46 c6 e8 12 a1 c2 98 ea 86 6e 16 8d b0 67 b5 80 af 65 61 61 5d 7b 82 7c 11 70 32 6d 59 af c0 d8 b6 14 e4 87 fe 1f 14 2d 1b 36 40 c9 53 d0 01 48 c0 c0 18 d0 d2 d4 40 ba a6 f0 e0 65 8a 35 00 fb 16 1c ea 16 43 ff ff da 9e a4 0e 39 cc 8f cc cf 3c 5b e8 e9 f2 7e 9a 1d 89 4e 09 a9 e7 77 b1 1c 33 e7 cc d4 55 79 09 b3 92 6a 6a 7b ef 8c 49 d0 ef 3e af 77 c2 29 c3 61 bf a8 77 6e 8b 9f c4 5a d4 ef 5b 16 ae 08 63 c3 62 4f ba 80 cd 6e f3 56 25 c0 f7 65 c1 94 5c 33 d8 3c e3 64 3c 17 9a 05 56 99 a2 71 ea af 4c cd 45 af 12 22 b8 7a 93 32 e0 07 d0 0e 68 36 7a 94 fb fd 54 f4 72 90 96 65 ad 67 d0 f1 65 30 23 05 d3 61 15 2f b7 a5 f3 65 a4 ae 56 12 8c c7 60 5a 4e 41 ea 2f 7c 0d ea 73 e7 88 2e 6c 56 5c 7a 79 7e 21 5b b9 99 23 a8 74 b2 d0 6e f9 51 92 c9 41 e9 b3 d3 a9 29 b0 7c ff ef b5 7c 8b de 40 a7 aa 05 4f 02 d5 04 f9 d3 60 a3 c6 7a 2f e1 5a 70 c5 3b 84 81 5e e6 83 f2 57 37 e0 19 b5 a8 fe ba cf 5e e4 b1 25 54 ec e5 5b 1a 0c 27 b2 84 9c 18 05 43 ff 6b ae d5 49 25 f3 d8 94 c3 33 9f 11 37 a6 c0 b2 42 70 b4 c7 5d de 69 a2 84 f9 c1 23 bc fa ee e5 e4 ae 9b 96 Data Ascii: 1f66,BrX`lU'^4^+D0;g\%UQyc`pU+"y5/=M7ZB6#Ts l/Ts?^"Q:f9jWs{^7<xXRJIK2$HPWK)6biaDi<Z5>%BK `&"B2{xn+vZDO!/l7P<\{<Rl$r]fCQ0oYK-1q4mu2fA&m^\% MZ&2'%4DAY_%M<>4Qd^^Q`;)le2=[(,l1}Zh;Z,2Bkhvbc=J+PzCi-5Ly.h("[zg)5]b:C8v@2=B~^xBC96#B,iEL[WFIe ?Er1:3GLq{9,4fQE{+pimD4^HOHfV&wl35c-9n&)L>Ydcvi'<{vK4${PE-~`LU0FvP"[r!2$4e|>?vw<PFYF-~2lpa+{<UO @ZO=#vvFngeaa]{|p2mY-6@SH@e5C9<[~Nw3Uyjj{I>w)awnZ[cbOnV%e\3<d<VqLE"z2h6zTrege0#a/eV`ZNA/|s.lV\zy~![#tnQA)||@O`z/Zp;^W7^%T['CkI%37Bp]i#

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49750	5.188.88.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2021 10:44:31.329138041 CET	1445	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wjigjxv.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 247 Host: rsuehfidvdkfvk.top
Nov 18, 2021 10:44:31.741991043 CET	1446	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Thu, 18 Nov 2021 09:44:31 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49751	5.188.88.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2021 10:44:31.842526913 CET	1447	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mrirybsj.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 362 Host: rsuehfidvdkfvk.top
Nov 18, 2021 10:44:32.039333105 CET	1447	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Thu, 18 Nov 2021 09:44:31 GMT Content-Type: text/html; charset=utf-8 Content-Length: 43 Connection: close Data Raw: 00 00 a5 82 9a e9 e7 a9 cb d5 14 c4 95 94 67 85 c2 1f 10 97 c9 73 e0 ad 1c 27 e0 bf bd 15 ad 68 5d fb 0c 2c 85 07 1f d1 2c 50 d3 Data Ascii: gs'h],,P

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49789	5.188.88.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2021 10:44:50.264198065 CET	2299	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tmmykkqa.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 205 Host: rsuehfidvdkfvk.top
Nov 18, 2021 10:44:50.649455070 CET	2301	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Thu, 18 Nov 2021 09:44:50 GMT Content-Type: text/html; charset=utf-8 Content-Length: 46 Connection: close Data Raw: 00 00 a5 82 9a e9 e7 a9 cb d5 14 c4 95 94 67 85 c2 1f 10 97 c9 73 e0 ad 1c 27 e0 bf bd 15 ad 68 5d fb 2c 30 82 06 0a 92 71 1e 98 ef c5 4a Data Ascii: gs'h],0qJ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49819	5.188.88.118	80	C:\Windows\explorer.exe

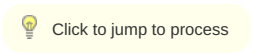
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 18, 2021 10:45:15.836029053 CET	8493	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rsuehfidvdkfvk.top/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 423 Host: rsuehfidvdkfvk.top
Nov 18, 2021 10:45:16.057694912 CET	8494	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Thu, 18 Nov 2021 09:45:16 GMT Content-Type: text/html; charset=utf-8 Content-Length: 406 Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 72 73 75 65 68 66 69 64 76 64 6b 66 76 6b 2e 74 6f 70 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.41 (Ubuntu) Server at rsuehfidvdkfvk.top Port 80</address></body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 1RMZ62tUAI.exe PID: 316 Parent PID: 760

General

Start time:	10:43:42
Start date:	18/11/2021
Path:	C:\Users\user\Desktop\1RMZ62tUAI.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1RMZ62tUAI.exe"
Imagebase:	0x400000
File size:	285184 bytes
MD5 hash:	8696A4269E30DDB34A7E0E84629EDE03
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.357733391.0000000002160000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.357762865.0000000002181000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3352 Parent PID: 316

General

Start time:	10:43:55
Start date:	18/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000006.00000000.345433901.0000000004DE1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: favdejf PID: 6992 Parent PID: 664

General

Start time:	10:44:30
Start date:	18/11/2021
Path:	C:\Users\user\AppData\Roaming\favdejf
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\favdejf
Imagebase:	0x400000
File size:	285184 bytes
MD5 hash:	8696A4269E30DDB34A7E0E84629EDE03
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000A.00000002.424469148.0000000003C21000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000A.00000002.424450951.0000000003C00000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 56%, ReversingLabs
Reputation:	low

Analysis Process: explorer.exe PID: 5732 Parent PID: 3352

General

Start time:	10:45:11
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Analysis Process: explorer.exe PID: 2892 Parent PID: 3352

General

Start time:	10:45:13
Start date:	18/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Key Created

Analysis Process: explorer.exe PID: 4424 Parent PID: 3352

General

Start time:	10:45:15
Start date:	18/11/2021

Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 5056 Parent PID: 3352

General

Start time:	10:45:18
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000016.00000002.555611191.0000000000111000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: explorer.exe PID: 3532 Parent PID: 3352

General

Start time:	10:45:20
Start date:	18/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000017.00000002.555126531.0000000000311000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: explorer.exe PID: 6052 Parent PID: 3352

General

Start time:	10:45:22
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000018.00000002.559721619.00000000027D1000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: explorer.exe PID: 6908 Parent PID: 3352

General

Start time:	10:45:24
Start date:	18/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000019.00000002.555346763.0000000000E91000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: explorer.exe PID: 4760 Parent PID: 3352

General

Start time:	10:45:26
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 6008 Parent PID: 3352

General

Start time:	10:45:29
Start date:	18/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff720ea0000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 6528 Parent PID: 3352

General

Start time:	10:45:32
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

Analysis Process: explorer.exe PID: 6184 Parent PID: 3352

General

Start time:	10:45:34
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 5824 Parent PID: 3352

General

Start time:	10:45:36
Start date:	18/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 6264 Parent PID: 3352

General

Start time:	10:45:38
Start date:	18/11/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x360000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis