ID: 491718
Sample Name:
sFau6gAKEk.exe
Cookbook: default.jbs
Time: 20:35:32
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

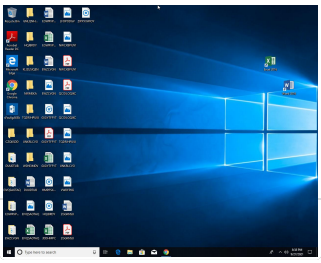
Windows Analysis Report sFau6gAKEk.exe

Overview

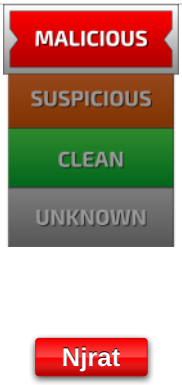
General Information

Sample Name:	sFau6gAKEk.exe
Analysis ID:	491718
MD5:	3441a429a71ac1..
SHA1:	d4f2ab9a718b2da.
SHA256:	d3763d5c2317a2..
Tags:	exe njrat RAT
Infos:	

Most interesting Screenshot:



Detection

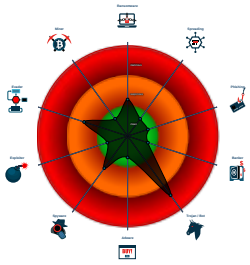


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected Njrat
- C2 URLs / IPs found in malware con…
- Uses dynamic DNS services
- Found a high number of Window / Us…
- PE file does not import any functions
- Queries the volume information (nam…
- Sample file is different than original …
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- sFau6gAKEk.exe (PID: 5200 cmdline: 'C:\Users\user\Desktop\sFau6gAKEk.exe' MD5: 3441A429A71AC1AD6E910EFDD06CACD3)
- **cleanup**

Malware Configuration

Threatname: Njrat


```
{
  "Host": "strigoo.duckdns.org",
  "Port": "9889",
  "Mutex Name": "aed1603e66c64f9fafe",
  "Network Seprator": "@!#&^%$",
  "Campaign ID": "NYAN CAT",
  "Version": "0.7NC"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: sFau6gAKEk.exe PID: 5200	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	

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

Yara detected Njrat

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Njrat

Stealing of Sensitive Information:

Yara detected Njrat

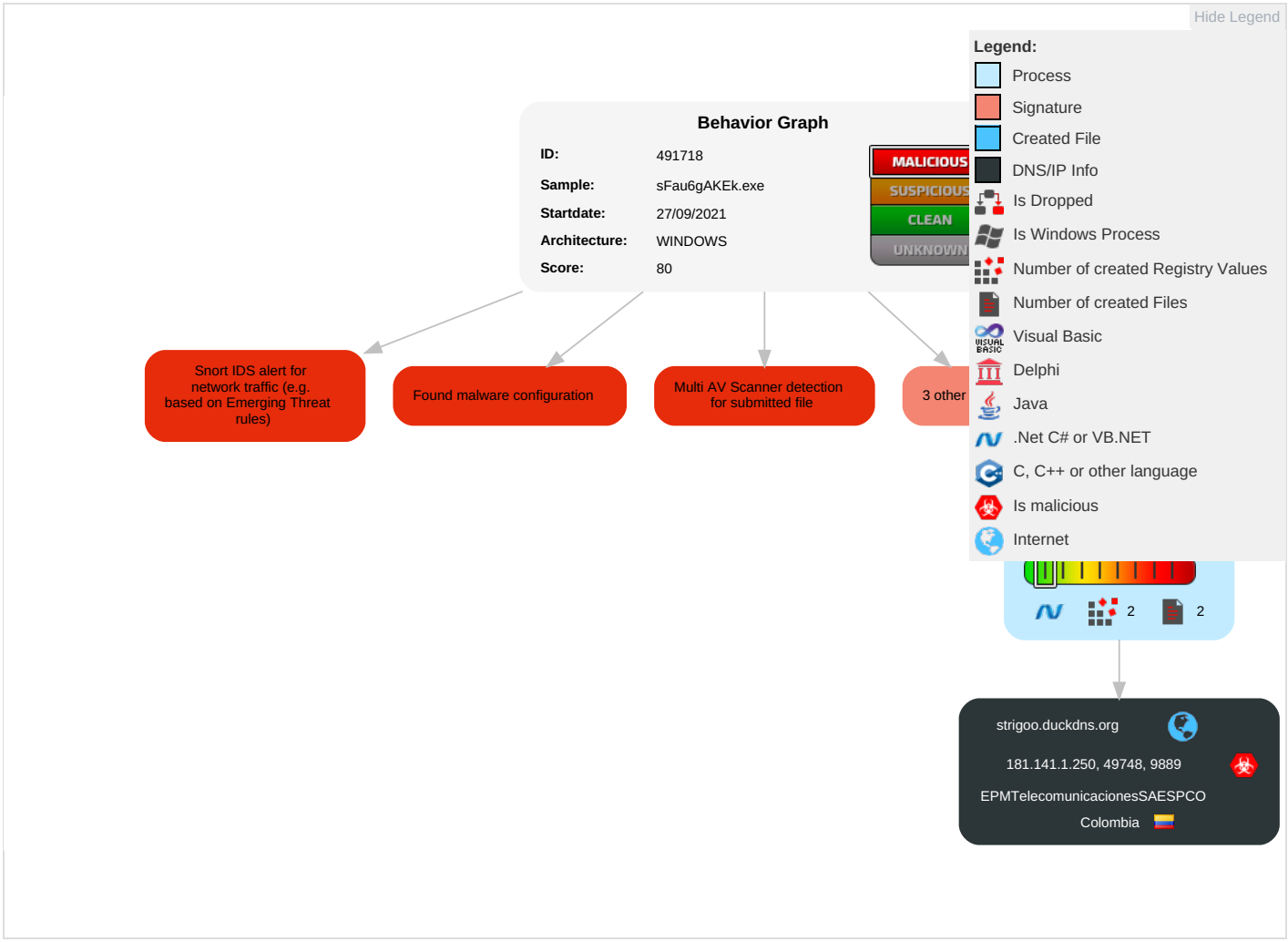
Remote Access Functionality:

Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1	Input Capture 1 1	Security Software Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

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
sFau6gAKEk.exe	50%	Virustotal		Browse
sFau6gAKEk.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
strigoo.duckdns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
strigoo.duckdns.org	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
strigoo.duckdns.org	0%	Avira URL Cloud	safe	
http://https://19a35f0c-6367-45ec-aec7-f047bc9f0ebe.com	0%	Virustotal		Browse
http://https://19a35f0c-6367-45ec-aec7-f047bc9f0ebe.com	0%	Avira URL Cloud	safe	
http://https://19a35f0c-6367-45ec-aec7-f047bc9f0ebe.com(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strigoo.duckdns.org	181.141.1.250	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
strigoo.duckdns.org	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
181.141.1.250	strigoo.duckdns.org	Colombia		13489	EPMTelecomunicacionesSA ESPCO	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491718
Start date:	27.09.2021
Start time:	20:35:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sFau6gAKEk.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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.winEXE@1/0@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.2%) • Quality average: 50% • Quality standard deviation: 50%
HCA Information:	• Successful, ratio: 97% • 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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EPMTelecomunicacionesSAESPCO	Du7uHwvCQC	Get hash	malicious	Browse	• 181.135.128.163
	2hrxC5NcX5	Get hash	malicious	Browse	• 190.151.230.115
	bfHSvjklSW	Get hash	malicious	Browse	• 201.184.41.14
	DetectSafeBrowsing.exe	Get hash	malicious	Browse	• 190.9.216.31
	XyMjGu74RX	Get hash	malicious	Browse	• 181.142.153.220
	FGLqhK6Zvk	Get hash	malicious	Browse	• 181.133.113.199
	b3astmode.x86	Get hash	malicious	Browse	• 181.135.96.142
	b3astmode.arm7	Get hash	malicious	Browse	• 190.28.71.143
	CPWpaRIC4Q.dll	Get hash	malicious	Browse	• 181.129.167.82
	StSCDEPGxM.exe	Get hash	malicious	Browse	• 181.141.7.190
	dark.arm7	Get hash	malicious	Browse	• 190.29.50.138
	x2HPpQ02mD	Get hash	malicious	Browse	• 190.128.61.51
	xzK3v4YYYx	Get hash	malicious	Browse	• 201.184.16.36
	gHQh80mu53	Get hash	malicious	Browse	• 181.133.113.195
	HoGxvkYZd5	Get hash	malicious	Browse	• 190.251.194.144
	qAwuBBElh2	Get hash	malicious	Browse	• 181.131.221.49
	k3dBuYbiCS	Get hash	malicious	Browse	• 181.131.221.53
	nogBoEEoTK	Get hash	malicious	Browse	• 181.131.49.107
	ChK3a1uHDf.exe	Get hash	malicious	Browse	• 181.140.202.66
	Documentacion.PDF.vbs	Get hash	malicious	Browse	• 181.140.202.66

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.689643149365699
TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	sFau6gAKEk.exe
File size:	322560
MD5:	3441a429a71ac1ad6e910efdd06cacd3
SHA1:	d4f2ab9a718b2da7c4b1d1863dbc6a83b3e29264
SHA256:	d3763d5c2317a279fc6ffce59700fb96f10570178d81c01a912db7b17811798c
SHA512:	e9564dd693fc9391aa6d121c714e807820f2dce50c4809a11914274adfeec1ce721caf72b4801916fa35a9abcb078e3242ac2e28b54aa558ca0f54bf8dee5b8a
SSDEEP:	3072:KX2p9qmX3OyGLKRB5jPCO3rv5Pc/qNnxRlWN2OD/a3/8HMN8/xo2eNeBiKzYdW0:9p9qK7/5PC2b5Pc/qVblPk/o/8HMF2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...3.Ka..... ....@.....@..... ....@...@.....@..... .....

File Icon

Icon Hash:	067179717179b10e

Static PE Info

General

Entrypoint:	0x140000000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614BB633 [Wed Sep 22 23:03:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x22de4	0x22e00	False	0.824344758065	data	7.61141443582	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x2bb1e	0x2bc00	False	0.166422991071	data	5.10147118742	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-20:36:41.157663	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54795	8.8.8.8	192.168.2.5
09/27/21-20:36:42.094591	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49748	9889	192.168.2.5	181.141.1.250

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:36:41.041933060 CEST	192.168.2.5	8.8.8.8	0xada8	Standard query (0)	strigoo.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:36:41.157663107 CEST	8.8.8.8	192.168.2.5	0xada8	No error (0)	strigoo.duckdns.org		181.141.1.250	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: sFau6gAKEk.exe PID: 5200 Parent PID: 5532

General

Start time:	20:36:29
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\sFau6gAKEk.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\sFau6gAKEk.exe'
Imagebase:	0xee0000
File size:	322560 bytes
MD5 hash:	3441A429A71AC1AD6E910EFDD06CACD3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis