ID: 528071
Sample Name:
Rats4dIOmA.exe
Cookbook: default.jbs
Time: 18:22:21
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

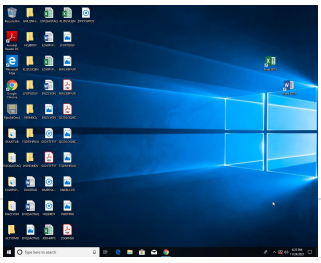
Windows Analysis Report Rats4dIOmA.exe

Overview

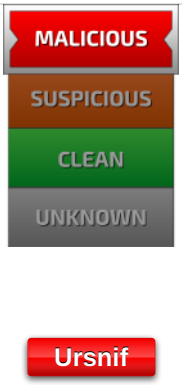
General Information

Sample Name:	Rats4dIOmA.exe
Analysis ID:	528071
MD5:	76a29095e02a15..
SHA1:	afd4593a0e709a1.
SHA256:	c26838865c4767..
Tags:	exe Gozi
Infos:	

Most interesting Screenshot:



Detection



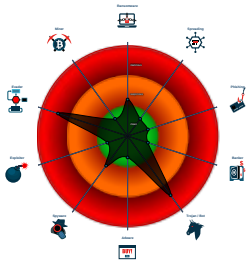
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected Ursnif
- Detected unpacking (changes PE se…
- Writes or reads registry keys via WMI
- Machine Learning detection for samp…
- Writes registry values via WMI
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- Rats4dIOmA.exe (PID: 6456 cmdline: "C:\Users\user\Desktop\Rats4dIOmA.exe" MD5: 76A29095E02A151ADC1F42EC844A65BD)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"dm+RfNkITE5FceWriGPYkZaFfoP/k2XQ2jeLd8rNgFw6gJ6fNWsHd0U6akxsQHth/SBWm4/eMI9Y1qgwNJteasgQsUC7Ht20y96mIxH1hvPh9uvLSH5z2CNo+fcP8K+V0yoOOQzDln/qE7mMJHLu+rmogHE7S6lb7FVy/7xxrRe3zMDt
5K9bDwOreWw0blGE",
  "c2_domain": [
    "yahoo.com",
    "soderunovos.website",
    "qoderunovos.website",
    "https://soderunovos.website",
    "https://qoderunovos.website"
  ],
  "botnet": "4482",
  "server": "12",
  "serpent_key": "10291029JSJUYNHG",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "dga_base_url": "constitution.org/usdeclar.txt",
  "dga_tld": "com ru org",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.310816150.0000000004758000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.310772228.0000000004758000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.310824742.0000000004758000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000002.518140305.00000000042B9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000002.518183803.0000000004758000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Rats4dIOmA.exe.42b94a0.3.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.Rats4dIOmA.exe.3c40000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.Rats4dIOmA.exe.42b94a0.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	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

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

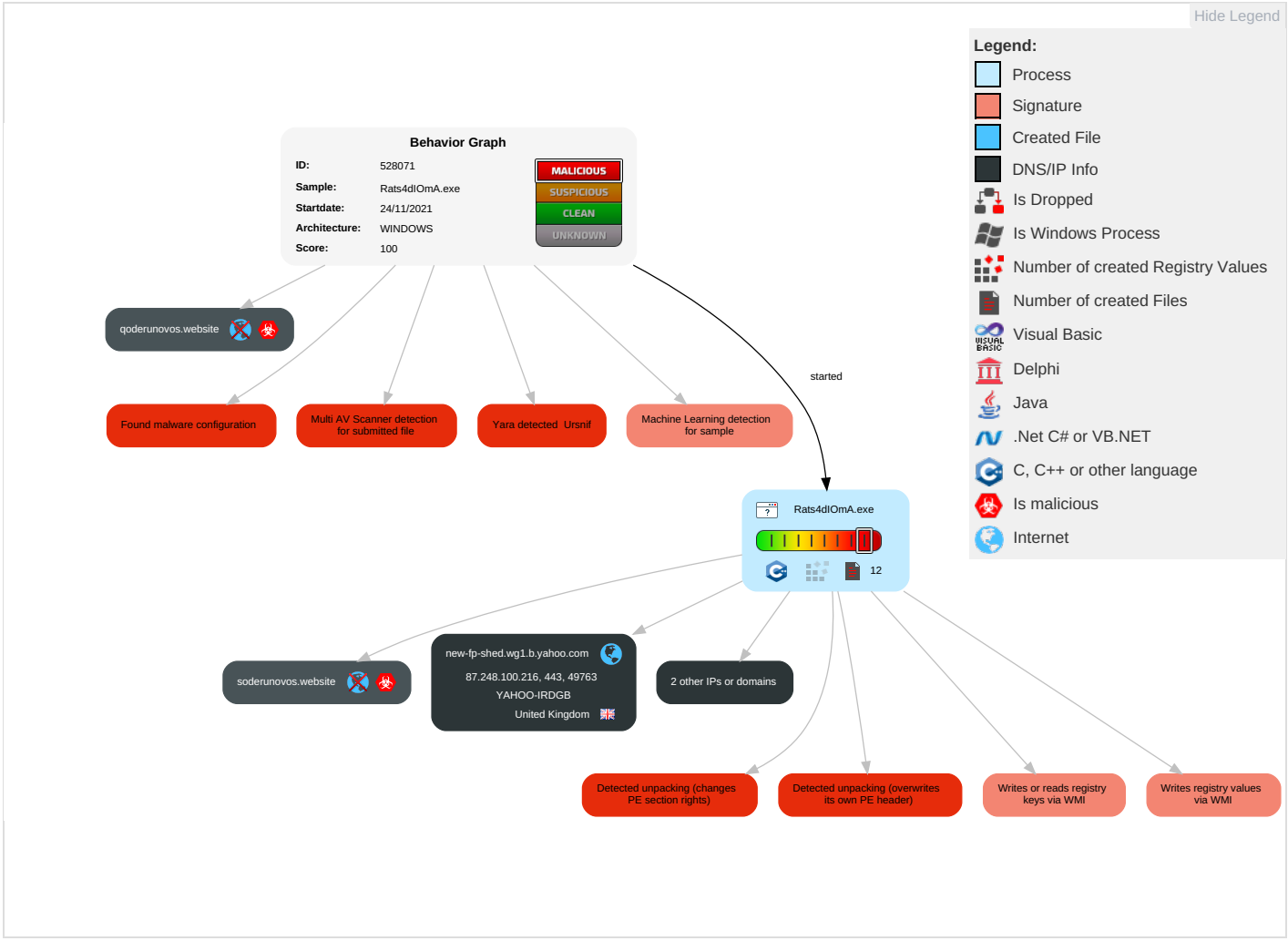
Remote Access Functionality:

Yara detected Ursnif

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 2	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 2	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin

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
Rats4dIOmA.exe	23%	Metadefender		Browse
Rats4dIOmA.exe	45%	ReversingLabs	Win32.Trojan.Chapak	
Rats4dIOmA.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Rats4dIOmA.exe.1fe0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.Rats4dIOmA.exe.3c40000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.Rats4dIOmA.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.Rats4dIOmA.exe.3bf0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://soderunovos.websitehttps://qoderunovos.websiten	0%	Avira URL Cloud	safe	
http://https://soderunovos.website	0%	Avira URL Cloud	safe	
http://https://qoderunovos.website	0%	Avira URL Cloud	safe	
http://https://soderunovos.website/jdraw/ldez60nkcypupl/Y8k6P2TKljJ3iNZCDUKjs/bDzAl0Dd4aRnqW1G/ctGW3CyINNEj	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
new-fp-shed.wg1.b.yahoo.com	87.248.100.216	true	false		high
yahoo.com	74.6.143.26	true	false		high
www.yahoo.com	unknown	unknown	false		high
qoderunovos.website	unknown	unknown	true		unknown
soderunovos.website	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.yahoo.com/jdraw/hz1bq3PmtqtDPcpAxd/_2FGYs9V_/2BcaIfj8lzbe6dwp1S50/qnf1CtPsO2EGsTOGBt0/TpQo4OHaLh1DZAzOHIElg2/LmJhngmT2kJ_2/FHuNwneH/Olki6SGkOhEdHnRV6_2B266/I71jLcWlaJ/WAM1n0wLbM0TzOock/J5o_2ByTSV9y/SAhEyWB5DMB/4lW4ok5N/nAsrN2WO_/2Fjc4.crw	false		high
http://https://yahoo.com/jdraw/hz1bq3PmtqtDPcpAxd/_2FGYs9V_/2BcaIfj8lzbe6dwp1S50/qnf1CtPsO2EGsTOGBt0/TpQo4OHaLh1DZAzOHIElg2/LmJhngmT2kJ_2/FHuNwneH/Olki6SGkOhEdHnRV6_2B266/I71jLcWlaJ/WAM1n0wLbM0TzOock/J5o_2ByTSV9y/SAhEyWB5DMB/4lW4ok5N/nAsrN2WO_/2Fjc4.crw	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.6.143.26	yahoo.com	United States		26101	YAHOO-3US	false
87.248.100.216	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528071
Start date:	24.11.2021
Start time:	18:22:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Rats4dIOmA.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:	25
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.evad.winEXE@1/0@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.5% (good quality ratio 27.8%) • Quality average: 82.4% • Quality standard deviation: 26%
HCA Information:	• Successful, ratio: 69% • 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
74.6.143.26	FpYf5EGDO9.exe	Get hash	malicious	Browse	
	Fuutbqvhmc.dll	Get hash	malicious	Browse	
	X4V4jFmFhO.dll	Get hash	malicious	Browse	
	bebys10.dll	Get hash	malicious	Browse	
	WGEcMZQA.dll	Get hash	malicious	Browse	
	vdbb9MZTVz.dll	Get hash	malicious	Browse	
	Information.xlsb	Get hash	malicious	Browse	
	V3HZtftyV5.xlsb	Get hash	malicious	Browse	
	t6i4DJb8qh.xlsb	Get hash	malicious	Browse	
	9lld0p2cVg.xlsb	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.26846.xlsb	Get hash	malicious	Browse	
	Attachment_97680.xlsb	Get hash	malicious	Browse	
	Attachment_96948.xlsb	Get hash	malicious	Browse	
	Document_89069.xlsb	Get hash	malicious	Browse	
	Attachment_777329.xlsb	Get hash	malicious	Browse	
	co-Payment.xlsb	Get hash	malicious	Browse	
	Presentation_812525.xlsb	Get hash	malicious	Browse	
	Document_7647.xlsb	Get hash	malicious	Browse	
	Document_7647.xlsb	Get hash	malicious	Browse	
	Invoice_52133.xls	Get hash	malicious	Browse	
87.248.100.216	FpYf5EGDO9.exe	Get hash	malicious	Browse	
	anIV2qJeLD.exe	Get hash	malicious	Browse	
	0MGLPJiSa5.dll	Get hash	malicious	Browse	
	Fuutbqvhmc.dll	Get hash	malicious	Browse	
	X4V4jFmFhO.dll	Get hash	malicious	Browse	
	GLpkbbRAp2.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bebys12.dll	Get hash	malicious	Browse	
	loveTubeLike.dll	Get hash	malicious	Browse	
	zuroq8.dll	Get hash	malicious	Browse	
	zuroq1.dll	Get hash	malicious	Browse	
	nextNextLike.dll	Get hash	malicious	Browse	
	gVuD2n1r5v.dll	Get hash	malicious	Browse	
	BQlyt2B7Im.dll	Get hash	malicious	Browse	
	52k0qe3yt3.dll	Get hash	malicious	Browse	
	BQlyt2B7Im.dll	Get hash	malicious	Browse	
	SayEjNMwtQ.dll	Get hash	malicious	Browse	
	uj8A47Ew7u.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.W64.Bzrloader.IEldorado.25041.dll	Get hash	malicious	Browse	
	powTubeDoor.dll	Get hash	malicious	Browse	
	WGEcMZQA.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
new-fp-shed.wg1.b.yahoo.com	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 87.248.100.216
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 87.248.100.216
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 87.248.100.216
	loveTubeLike.dll	Get hash	malicious	Browse	• 87.248.100.215
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 87.248.100.215
	Antic Cracked.exe	Get hash	malicious	Browse	• 87.248.100.215
	nesfooF2Q1.exe	Get hash	malicious	Browse	• 87.248.100.215
	X4V4jFmFhO.dll	Get hash	malicious	Browse	• 87.248.100.216
	GLpkbbRAp2.dll	Get hash	malicious	Browse	• 87.248.100.216
	youNextNext.dll	Get hash	malicious	Browse	• 87.248.100.215
	bebys10.dll	Get hash	malicious	Browse	• 87.248.100.215
	bebys12.dll	Get hash	malicious	Browse	• 87.248.100.216
	loveTubeLike.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq8.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq1.dll	Get hash	malicious	Browse	• 87.248.100.216
	nextNextLike.dll	Get hash	malicious	Browse	• 87.248.100.215
	TFlw2EliZh.exe	Get hash	malicious	Browse	• 87.248.100.215
	Solicitor Inquiry No. 001_4921 - UK.xls	Get hash	malicious	Browse	• 87.248.100.215
	kANwTlkiJp.dll	Get hash	malicious	Browse	• 87.248.100.215
	gVuD2n1r5v.dll	Get hash	malicious	Browse	• 87.248.100.215
yahoo.com	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 87.248.100.216
	X4V4jFmFhO.dll	Get hash	malicious	Browse	• 87.248.100.216
	GLpkbbRAp2.dll	Get hash	malicious	Browse	• 87.248.100.216
	bebys10.dll	Get hash	malicious	Browse	• 87.248.100.215
	bebys12.dll	Get hash	malicious	Browse	• 87.248.100.216
	loveTubeLike.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq8.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq1.dll	Get hash	malicious	Browse	• 87.248.100.216

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YAHOO-3US	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 74.6.143.26
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 74.6.143.25
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 74.6.143.26
	T8H5LF8GlO	Get hash	malicious	Browse	• 98.139.166.49
	TFEkbH3ag3	Get hash	malicious	Browse	• 98.139.166.22
	X4V4jFmFhO.dll	Get hash	malicious	Browse	• 74.6.143.26
	jew.x86	Get hash	malicious	Browse	• 98.139.166.15
	bebys10.dll	Get hash	malicious	Browse	• 74.6.143.26
	zD1jpTbFQq	Get hash	malicious	Browse	• 98.139.130.39
	zuroq8.dll	Get hash	malicious	Browse	• 74.6.143.25
	zuroq1.dll	Get hash	malicious	Browse	• 74.6.143.25
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 74.6.143.25
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 74.6.143.25
	uj8A47Ew7u.dll	Get hash	malicious	Browse	• 74.6.143.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	b3astmode.arm	Get hash	malicious	Browse	• 98.139.142.39
	WGEcMZQA.dll	Get hash	malicious	Browse	• 74.6.143.26
	mzfAM4jLfv.dll	Get hash	malicious	Browse	• 74.6.143.25
	vdbb9MZTVz.dll	Get hash	malicious	Browse	• 74.6.143.26
	Update-KB250-x86.exe	Get hash	malicious	Browse	• 67.195.204.72
	Update-KB2984-x86.exe	Get hash	malicious	Browse	• 67.195.204.74
YAHOO-IRDGB	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 212.82.100.140
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 212.82.100.140
	0MGLPJiSa5.dll	Get hash	malicious	Browse	• 87.248.100.216
	loveTubeLike.dll	Get hash	malicious	Browse	• 87.248.100.215
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 87.248.100.216
	X4V4jFmFhO.dll	Get hash	malicious	Browse	• 87.248.100.216
	GLpkbbRAp2.dll	Get hash	malicious	Browse	• 87.248.100.216
	iKuUJ0F8Du	Get hash	malicious	Browse	• 87.248.96.208
	youNextNext.dll	Get hash	malicious	Browse	• 87.248.100.215
	bebys10.dll	Get hash	malicious	Browse	• 87.248.100.215
	bebys12.dll	Get hash	malicious	Browse	• 87.248.100.216
	loveTubeLike.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq8.dll	Get hash	malicious	Browse	• 87.248.100.216
	zuroq1.dll	Get hash	malicious	Browse	• 87.248.100.216
	nextNextLike.dll	Get hash	malicious	Browse	• 87.248.100.216
	kANwTlkiJp.dll	Get hash	malicious	Browse	• 87.248.100.215
	gVuD2n1r5v.dll	Get hash	malicious	Browse	• 87.248.100.216
	#Ud83d#Udce0TetratecheFaxNOV03 xti.htm	Get hash	malicious	Browse	• 212.82.100.181
	BQlyt2B7Im.dll	Get hash	malicious	Browse	• 87.248.100.216
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 87.248.100.216

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	XP-SN-7843884.htm	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	XP-SN-8324655.htm	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	new-1834138397.xls	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	1.htm	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	FACTURAS.exe	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	new-1179494065.xls	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	TT-PRIME USD242,357,59.ppam	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	chase.xls	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	Statement from QNB.exe	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	private-1915056036.xls	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	private-1910485378.xls	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	doc201002124110300200.exe	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	t 2021.HtML	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	Justificante.exe	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	muhammadbad.html	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	MtCsSK9TK2.exe	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26
	0331C7BCA665F36513377FC301CBB32822FF35F9 25115.exe	Get hash	malicious	Browse	• 87.248.100.216 • 74.6.143.26

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.833285470480499
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:	Rats4dIOmA.exe
File size:	302080
MD5:	76a29095e02a151adc1f42ec844a65bd
SHA1:	afd4593a0e709a11296556d5b1fb1833bb394c4d
SHA256:	c26838865c476704101363c16c535dfae494dedadae972c0377c4f67669578b5
SHA512:	9574fecccc2b34b256025c391ee95fdac2e476e3533c753e44fc7fd218259327416b7eddbdc2ca6ba3956f0b7b65f633054f21ab08e562548353323ac3d8bc61
SSDEEP:	6144:mOcPU517+45GlCVKk8PVSXuZet0yyeuI3+9jbUm6nzKvPV:mOckd+RlqKkuVSXuZet0yyeroHUm6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.r"t..qt..qt..q...q]..q...qe..q...q...q}..q...qt..qq..q...qu..q...qu..q...qu..qRicht..q.....PE..L.....^.....

File Icon

Icon Hash:	a2e8e8e8a2a2a4a8

Static PE Info

General

Entrypoint:	0x417e90
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:	0x5EFCE5EA [Wed Jul 1 19:37:14 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:	227bb68f00c01d84de5b7cf57cce44af

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30b2a	0x30c00	False	0.60816806891	data	7.04444899707	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x32000	0x1b84ac0	0x1400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1bb7000	0x5f08	0x6000	False	0.53857421875	data	5.60832120978	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1bbd000	0x11610	0x11800	False	0.0746651785714	data	0.972136620896	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Panama	
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 24, 2021 18:23:50.497390985 CET	192.168.2.5	8.8.8.8	0x3e0d	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:51.244018078 CET	192.168.2.5	8.8.8.8	0xdb09	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)
Nov 24, 2021 18:24:11.737723112 CET	192.168.2.5	8.8.8.8	0xc17f	Standard query (0)	soderunovos.website	A (IP address)	IN (0x0001)
Nov 24, 2021 18:25:31.805324078 CET	192.168.2.5	8.8.8.8	0x2edb	Standard query (0)	qoderunovos.website	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 18:23:50.517024994 CET	8.8.8.8	192.168.2.5	0x3e0d	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:50.517024994 CET	8.8.8.8	192.168.2.5	0x3e0d	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:50.517024994 CET	8.8.8.8	192.168.2.5	0x3e0d	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:50.517024994 CET	8.8.8.8	192.168.2.5	0x3e0d	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:50.517024994 CET	8.8.8.8	192.168.2.5	0x3e0d	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:50.517024994 CET	8.8.8.8	192.168.2.5	0x3e0d	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:51.263613939 CET	8.8.8.8	192.168.2.5	0xdb09	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2021 18:23:51.263613939 CET	8.8.8.8	192.168.2.5	0xdb09	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)
Nov 24, 2021 18:23:51.263613939 CET	8.8.8.8	192.168.2.5	0xdb09	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)
Nov 24, 2021 18:24:11.760108948 CET	8.8.8.8	192.168.2.5	0xc17f	Name error (3)	soderunovos.website	none	none	A (IP address)	IN (0x0001)
Nov 24, 2021 18:25:31.825109005 CET	8.8.8.8	192.168.2.5	0x2edb	Name error (3)	qoderunovos.website	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- yahoo.com
- www.yahoo.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49762	74.6.143.26	443	C:\Users\user\Desktop\Rats4dIOmA.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 17:23:51 UTC	0	OUT	GET /jdraw/hz1bq3PmtqtDPcpAxd/_2FGYs9V_/2BcaIfj8lzbe6dwp1S50/qnf1CtPsO2EGsTOGBt0/TpQo4OHaLh1DZAzOHIElg2/LmJhngmT2kJ_2/FHuNwneH/Olki6SGkOhEdHnRV6_2B266/I71jLcWlaJ/WAM1n0wLbM0TzOock/J5o_2ByTSV9y/SAhEyWB5DMB/4lW4ok5N/nAsrN2WO_/2Fjc4.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: yahoo.com Connection: Keep-Alive Cache-Control: no-cache
2021-11-24 17:23:51 UTC	0	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 24 Nov 2021 17:23:51 GMT Connection: keep-alive Strict-Transport-Security: max-age=31536000 Server: ATS Cache-Control: no-store, no-cache Content-Type: text/html Content-Language: en X-Frame-Options: SAMEORIGIN Set-Cookie: B=b5jn619gpst97&b=3&s=c6; expires=Thu, 24-Nov-2022 17:23:51 GMT; path=/; domain=.yahoo.com Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only" Referrer-Policy: no-referrer-when-downgrade X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Location: https://www.yahoo.com/jdraw/hz1bq3PmtqtDPcpAxd/_2FGYs9V_/2BcaIfj8lzbe6dwp1S50/qnf1CtPsO2EGsTOGBt0/TpQo4OHaLh1DZAzOHIElg2/LmJhngmT2kJ_2/FHuNwneH/Olki6SGkOhEdHnRV6_2B266/I71jLcWlaJ/WAM1n0wLbM0TzOock/J5o_2ByTSV9y/SAhEyWB5DMB/4lW4ok5N/nAsrN2WO_/2Fjc4.crw Content-Length: 8
2021-11-24 17:23:51 UTC	1	IN	Data Raw: 72 65 64 69 72 65 63 74 Data Ascii: redirect

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49763	87.248.100.216	443	C:\Users\user\Desktop\Rats4dIOmA.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-24 17:23:51 UTC	1	OUT	GET /jdraw/hz1bq3PmtqtDPcpAxd/_2FGYs9V_/2BcaIfj8lzbe6dwp1S50/qnf1CtPsO2EGsTOGBt0/TpQo4OHaL h1DZAzOHIElg2/LmJhngmT2kJ_2/FHuNwneH/Olki6SGkOhEdHnRV6_2B266/I71jLcWlaJ/WAM1n0wLbM0TzOock/ J5o_2ByTSV9y/SAhEyWB5DMB/4lW4ok5N/nAsrN2WO_/2Fjc4.crw HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Connection: Keep-Alive Cache-Control: no-cache Host: www.yahoo.com Cookie: B=b5jn619gpst97&b=3&s=c6
2021-11-24 17:23:51 UTC	1	IN	HTTP/1.1 404 Not Found date: Wed, 24 Nov 2021 17:23:51 GMT p3p: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV" cache-control: private x-content-type-options: nosniff content-type: text/html; charset=UTF-8 x-envoy-upstream-service-time: 9 server: ATS Age: 0 Transfer-Encoding: chunked Connection: close Strict-Transport-Security: max-age=31536000 Content-Security-Policy: frame-ancestors 'self' https://*.builtbygirls.com https://*.rivals.com https://*.engadget.com https://*.intheknow.com https://*.autoblog.com https://*.techcrunch.com https://*.yahoo.com https://*.aol.com https://*.huffingtonpost.com https://*.oath.com https://*.search.yahoo.com https://*.search.aol.com https://*.search.huffpost.com https://*.verizonmedia.com https://*.publishing.oath.com https://*.autoblog.com; sandbox allow-forms allow-same-origin allow-scripts allow-popups allow-popups-to-escape-sandbox allow-presentation; report-uri https://csp.yahoo.com/beacon/csp?src=ats&site=frontpage&region=US&lang=en-US&device=desktop&yrid=cc01o4tgpst97&partner=; X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block
2021-11-24 17:23:51 UTC	2	IN	Data Raw: 53 65 74 2d 43 6f 6f 6b 69 65 3a 20 42 3d 62 35 6a 6e 36 31 39 67 70 73 74 39 37 26 62 3d 33 26 73 3d 63 36 3b 20 45 78 70 69 72 65 73 3d 54 68 75 2c 20 32 34 20 4e 6f 76 20 32 30 32 32 20 32 33 3a 32 33 3a 35 31 20 47 4d 54 3b 20 4d 61 78 2d 41 67 65 3d 33 31 35 35 37 36 30 30 3b 20 44 6f 6d 61 69 6e 3d 2e 79 61 68 6f 6f 2e 63 6f 6d 3b 20 50 61 74 68 3d 2f 0d 0a 45 78 70 65 63 74 2d 43 54 3a 20 6d 61 78 2d 61 67 65 3d 33 31 35 33 36 30 30 30 2c 20 72 65 70 6f 72 74 2d 75 72 69 3d 22 68 74 74 70 3a 2f 2f 63 73 70 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 62 65 61 63 6f 6e 2f 63 73 70 3f 73 72 63 3d 79 61 68 6f 6f 63 6f 6d 2d 65 78 70 65 63 74 2d 63 74 2d 72 65 70 6f 72 74 2d 6f 6e 6c 79 22 0d 0a 52 65 66 65 72 72 65 72 2d 50 6f 6c 69 63 79 3a 20 6e 6f 2d 72 65 66 Data Ascii: Set-Cookie: B=b5jn619gpst97&b=3&s=c6; Expires=Thu, 24 Nov 2022 23:23:51 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"Referrer-Policy: no-ref
2021-11-24 17:23:51 UTC	3	IN	Data Raw: 34 33 34 0d 0a Data Ascii: 434
2021-11-24 17:23:51 UTC	3	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 27 75 74 66 2d 38 27 3e 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 75 3d 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 2f 3f 65 72 72 3d 34 30 34 26 65 72 72 5f 75 72 6c 3d 68 74 74 70 73 25 33 61 25 32 66 25 32 66 77 77 77 2e 79 61 68 6f 6f 2e 63 6f 6d 25 32 66 6a 64 72 61 77 25 32 66 68 7a 31 62 71 33 50 6d 74 71 74 44 50 63 70 41 78 64 25 32 66 5f 32 46 47 59 73 39 56 5f 25 32 66 32 42 63 61 49 66 6a 38 6c 7a 62 65 36 64 77 70 31 53 35 30 25 32 66 71 6e 66 31 43 74 50 73 4f 32 45 47 73 54 4f 47 42 74 30 25 32 66 54 70 51 6f 34 4f 48 61 4c 68 31 44 5a 41 7a 4f 48 49 45 6c 67 32 25 32 66 4c 6d 4a 68 6e 67 6d 54 32 6b 4a 5f 32 25 32 66 46 48 75 4e 77 6e 65 48 25 32 66 4f 6c Data Ascii: <html><meta charset='utf-8'><script>var u='https://www.yahoo.com/?err=404&err_url=https%3a%2f%2fwww.yahoo.com%2fjdraw%2fhz1bq3PmtqtDPcpAxd%2f_2FGYs9V_%2f2BcaIfj8lzbe6dwp1S50%2fqnf1CtPsO2EGsTOGBt0%2fTpQo4OHaLh1DZAzOHIElg2%2fLmJhngmT2kJ_2%2fFHuNwneH%2fOl
2021-11-24 17:23:51 UTC	4	IN	Data Raw: 0d 0a Data Ascii:
2021-11-24 17:23:51 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

System Behavior

Analysis Process: Rats4dIOmA.exe PID: 6456 Parent PID: 5760

General

Start time:	18:23:19
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Rats4dIOmA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Rats4dIOmA.exe"
Imagebase:	0x400000
File size:	302080 bytes
MD5 hash:	76A29095E02A151ADC1F42EC844A65BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310816150.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310772228.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310824742.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.518140305.00000000042B9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.518183803.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310739841.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310804717.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310680440.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310789542.0000000004758000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.310712356.0000000004758000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis