ID: 540821
Sample Name: fiHY95Y1CZ.exe
Cookbook: default.jbs
Time: 09:45:31
Date: 16/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report fiHY95Y1CZ.exe

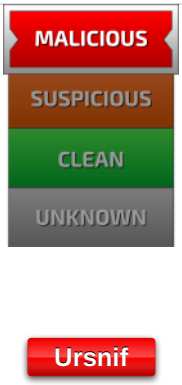
Overview

General Information

Sample Name:	fiHY95Y1CZ.exe (renamed file extension from exe to dll)
Analysis ID:	540821
MD5:	3b7d8109b37e99..
SHA1:	9ee1957c39834e..
SHA256:	53f09461a48f10c..
Tags:	exe geo Gozi ISFB ITA Ursnif
Infos:	

Most interesting Screenshot:

Detection

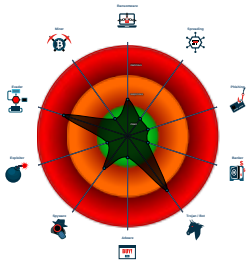


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- PE file has a writeable .text section
- Writes or reads registry keys via WMI
- Machine Learning detection for samp…
- Sigma detected: Suspicious Call by …
- Writes registry values via WMI
- Uses 32bit PE files

Classification



- **System is w10x64**
- loaddll32.exe (PID: 6620 cmdline: loaddll32.exe "C:\Users\user\Desktop\fiHY95Y1CZ.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6664 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\fiHY95Y1CZ.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6712 cmdline: rundll32.exe "C:\Users\user\Desktop\fiHY95Y1CZ.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6700 cmdline: regsvr32.exe /s C:\Users\user\Desktop\fiHY95Y1CZ.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6728 cmdline: rundll32.exe C:\Users\user\Desktop\fiHY95Y1CZ.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"B+xl4hUTn5rXiL0afazu2ddSc/ECZk5wqODKe0fS2KdIXHYzLOi+LPPP1HVzyCQFE2ZPog7imXfWyeJPGgVZO8mmh7g0OCbF0hBgHX6wj0qY1fBDcQxYjLnhuuJTPFt0voqEKHGGIgbiz86prZpdJls6h0dECkyqCOUP77xD4bHwJFYwmMp7govarzlBsbdorQ4qNFnd4O2rK1GEuQisAwdMkb4j9MqHf7vkHewrh1BGBeNcr85NjoxXAnfZDuX+M7b1dWoszYHJF1rgWzk4yz7fc+7Q4leAIr2PkWbTRuRpOe4P6Ok01hKGTLORQhRgWw6Mv2aRFMimHgiQWhhaHetICEhMcBl5C0yxhZCOhu4=",
  "c2_domain": [
    "microsoft.com/windowsdisabler",
    "windows.update3.com",
    "berukoneru.website",
    "gerukoneru.website",
    "fortunarah.com"
  ],
  "botnet": "8899",
  "server": "12",
  "serpent_key": "56473871MNTYAIDA",
  "sleep_time": "10",
  "CONF_TIMEOUT": "10",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.414360466.0000000002DFF000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000002.781134724.0000000004F98000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.418282417.0000000004BDF000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.346775098.0000000004F58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.370009221.0000000002FFB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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

System Summary:

PE file has a writeable .text section

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

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

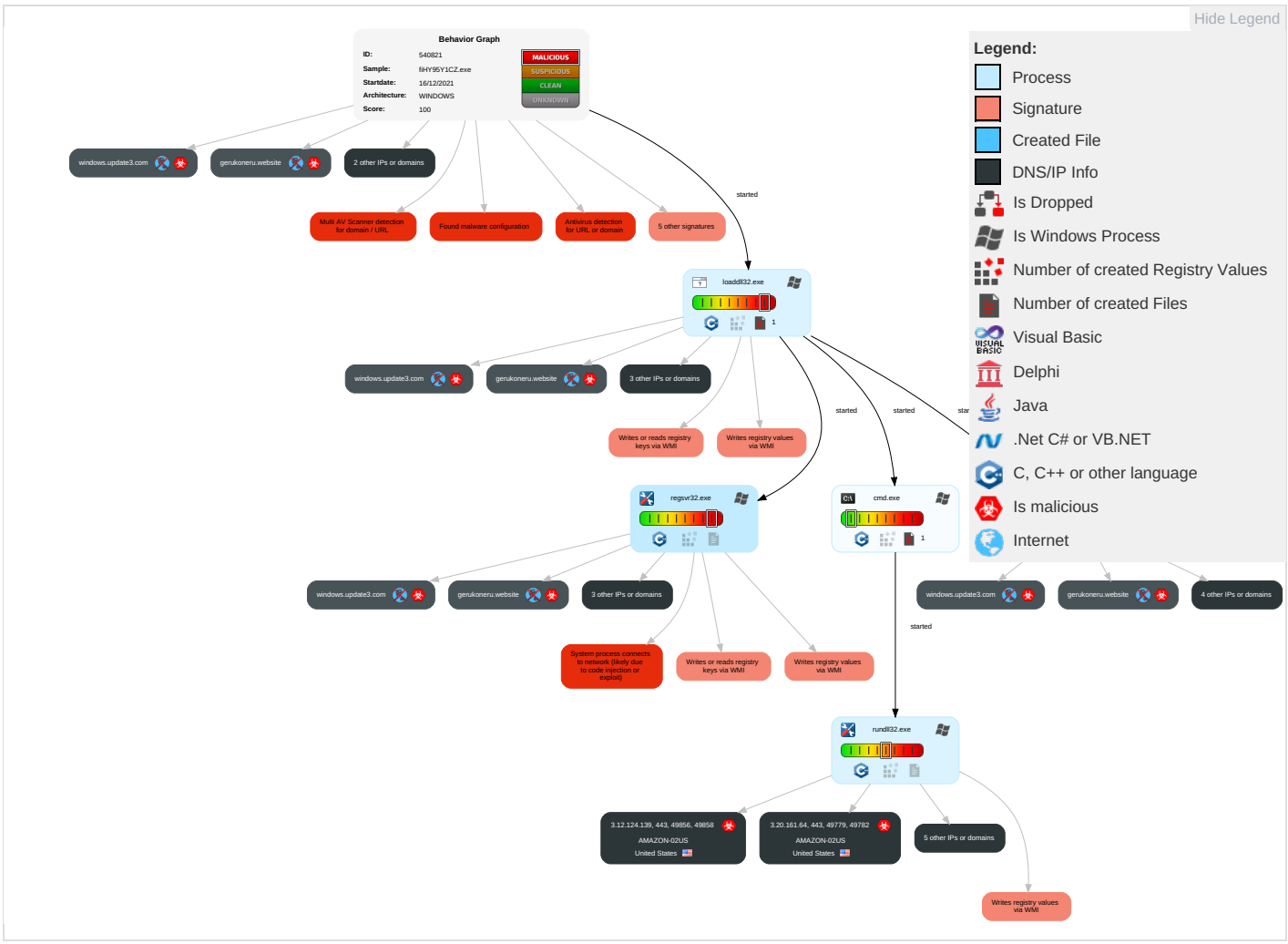
Remote Access Functionality:

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	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eave Insec Netw Comr
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	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	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Explo Track Local
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Regsvr32 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Account 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	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

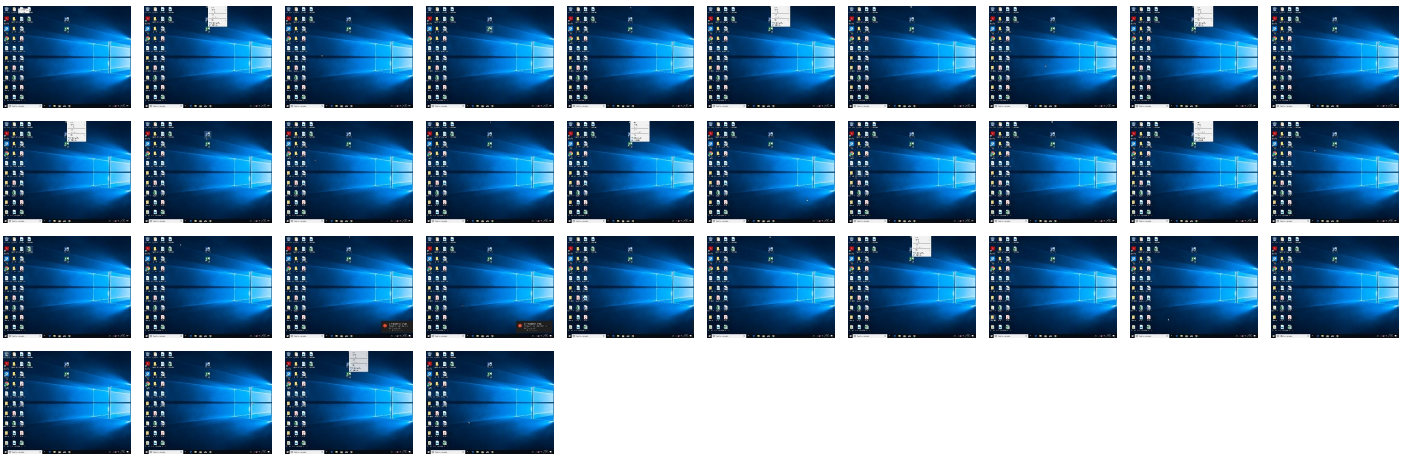
Behavior Graph



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
fiHY95Y1CZ.dll	24%	Virustotal		Browse
fiHY95Y1CZ.dll	38%	ReversingLabs	Win32.Infostealer.Gozi	
fiHY95Y1CZ.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.regsvr32.exe.3460000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
5.2.rundll32.exe.6e0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.2.loaddll32.exe.780000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.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
6.2.rundll32.exe.540000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Domains

Source	Detection	Scanner	Label	Link
berukoneru.website	10%	Virustotal		Browse
windows.update3.com	0%	Virustotal		Browse
gerukoneru.website	9%	Virustotal		Browse
fortunarah.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://gerukoneru.website:443	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/2	0%	Avira URL Cloud	safe	
http://https://berukoneru.website:4434	100%	Avira URL Cloud	malware	
http://https://berukoneru.website:443	100%	Avira URL Cloud	malware	
http://https://gerukoneru.website/7	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/pwsRZXEKCNadKEKqX1o9/b2Zj7hHedRFWAjDTz7_/2FOi9hvcPIf92jE5HHyv1B/OfZF	100%	Avira URL Cloud	malware	
http://https://windows.update3.com/	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/llU	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/tire/Wt7VtJWXxvCxj/q8Hicv2m/rYOqGahqW2aY_2BSfNZT5kT/9hHx0IzQpe/vlCX_2Bqh	0%	Avira URL Cloud	safe	
http://https://assets.onestore.ms/cdnfiles/onestorerolling-1605-16000/shell/common/respond-proxy.html	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/tire/fPNeZGvZ_2FjPtgP/S4ORv62WOG6CqCc/RpObjfG9eDuBR7sVqh/4jcyxlUAH/kr39Z	0%	Avira URL Cloud	safe	
http://https://fortunarah.com/	0%	Avira URL Cloud	safe	
http://https://gerukoneru.website/g	0%	Avira URL Cloud	safe	
http://https://gerukoneru.website/f	0%	Avira URL Cloud	safe	
http://https://assets.onestore.ms/cdnfiles/onestorerolling-1605-16000/shell/common/respo	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/	100%	Avira URL Cloud	malware	
http://https://windows.update3.com/tire/e5hjYNeWetXz_2B/Th5RGlAc56d_2FCUbi/NUhZqTgpn/_2FHcnisafGQJWYV9uWj/n	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/tire/za2qkobGG8hjnBcNlK5rpy/DM0ZTFZcdObn9/heBYxiqA/288tZtaDdhUDDHi0oDe4mT	100%	Avira URL Cloud	malware	
http://https://gerukoneru.website/o	0%	Avira URL Cloud	safe	
http://https://gerukoneru.website/	0%	Avira URL Cloud	safe	
http://https://gerukoneru.website/tire/2BC_2BBRBNFJ1PmozxxmKVd/gm6Dkla7K7/8u9w5b_2FXO_2FnQt/BMclQSrzXXf4/Rq	0%	Avira URL Cloud	safe	
http://https://windows.update3.com/Z	0%	Avira URL Cloud	safe	
http://https://c.s	0%	Avira URL Cloud	safe	
http://https://gerukoneru.website/V	0%	Avira URL Cloud	safe	
http://https://nodejs.org0	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/n	100%	Avira URL Cloud	malware	
http://https://berukoneru.website/tire/r5QiHxjTySmGYdSO5D/jcUwjLzfU/E7ReP6jBdZthorydDqCp/VP_2FtRTEArd2s1OvU	100%	Avira URL Cloud	malware	
http://https://gerukoneru.website/_	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/_	100%	Avira URL Cloud	malware	
http://https://fortunarah.com/g	0%	Avira URL Cloud	safe	
http://https://berukoneru.website/f	100%	Avira URL Cloud	malware	
http://https://windows.update3.com/tire/NBe6wGJmUc0TyUzeyP/5Njlm_2FV/AnUx9J_2FMkoEzFmIRim/7MsjKW4RRjAKub2A8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	18.219.227.107	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
berukoneru.website	unknown	unknown	true	• 10%, Virustotal, Browse	unknown
windows.update3.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
gerukoneru.website	unknown	unknown	true	• 9%, Virustotal, Browse	unknown
fortunarah.com	unknown	unknown	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.20.161.64	unknown	United States		16509	AMAZON-02US	true
18.219.227.107	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
3.12.124.139	unknown	United States		16509	AMAZON-02US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	540821
Start date:	16.12.2021
Start time:	09:45:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fiHY95Y1CZ.exe (renamed file extension from exe to 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:	28
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@91/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64% (good quality ratio 60.7%) • Quality average: 78% • Quality standard deviation: 29.5%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:47:02	API Interceptor	36x Sleep call for process: rundll32.exe modified
09:47:03	API Interceptor	18x Sleep call for process: regsvr32.exe modified
09:47:03	API Interceptor	19x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

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):	5.256885449705882
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:	fiHY95Y1CZ.dll
File size:	1776800
MD5:	3b7d8109b37e996e06ae68144f37a73c
SHA1:	9ee1957c39834e9ea87cd72d7f09e9f08e1712d3
SHA256:	53f09461a48f10c95f426cd179106cbe94fba81c498fb7414d6a849470ee777e
SHA512:	549f93153ae0659dfc4876cb5e7dd3b65316fe5293912bcde2828f014039e7528b854db608653296f277be6bcd1b7a725f846fdf9698390baea2b2636a7d19cc

General

SSDEEP:	49152:4W58UQw8MT8UQw8MT8UQw8MT8UQw8MT8UQw8MT8UQw8MO:4O8UQw8MT8UQw8MT8UQw8MT8UQw8MT8L
File Content Preview:	MZ.....!..L.!This .ro.ra. cannot be run in DOS m.de....$.....PE..L.....a..... .....!.....f6..... .....P..

File Icon

Icon Hash:	82b0f4c6d2c66cb1

Static PE Info

General

Entrypoint:	0x1001c09b
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61B6D28E [Mon Dec 13 04:56:46 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:	05e4e1045777d757fa17eaf53eecd299

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/1/2020 5:00:00 PM 12/18/2023 4:00:00 AM
Subject Chain	• CN=OpenJS Foundation, O=OpenJS Foundation, L=San Francisco, S=California, C=US
Version:	3
Thumbprint MD5:	8E8056A2284F0304445ED325353454BF
Thumbprint SHA-1:	E16BB6EE4ED3935C46C356D147E811286BA4BBFE
Thumbprint SHA-256:	968F9536C18A4475095B37792855AA62306275DEC05BD72F21653C98026CFC4E
Serial:	038EDB2FC6E405731A760F1516144C85

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x28613	0x22000	False	0.518655215993	data	5.42328856771	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2a000	0x237af	0x1d200	False	0.0684012875536	data	6.13260963822	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4e000	0x16f8e8	0x16fa00	False	0.2185235411	data	4.81723301086	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x1be000	0x670	0x800	False	0.69384765625	data	5.74685750781	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/16/21-09:48:04.909243	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:48:06.443354	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:48:07.457320	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:48:08.496291	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:48:10.177155	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:01.472370	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:02.539281	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:06.405672	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:07.484648	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:08.675917	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:11.266525	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:57.574727	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:49:59.580242	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:50:00.602049	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:50:05.088933	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:50:06.169872	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:50:08.187515	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
12/16/21-09:50:08.812572	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 16, 2021 09:47:26.971112967 CET	192.168.2.7	8.8.8.8	0xdee2	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.025146961 CET	192.168.2.7	8.8.8.8	0xa486	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.116242886 CET	192.168.2.7	8.8.8.8	0x1b94	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:29.785082102 CET	192.168.2.7	8.8.8.8	0x17cd	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:38.298553944 CET	192.168.2.7	8.8.8.8	0xd69e	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:39.982805967 CET	192.168.2.7	8.8.8.8	0x33e	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:40.068403006 CET	192.168.2.7	8.8.8.8	0x556b	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:40.651721001 CET	192.168.2.7	8.8.8.8	0xf460	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:48.375288963 CET	192.168.2.7	8.8.8.8	0xd5c1	Standard query (0)	gerukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:50.203558922 CET	192.168.2.7	8.8.8.8	0xf9d6	Standard query (0)	gerukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:50.295247078 CET	192.168.2.7	8.8.8.8	0x5d1a	Standard query (0)	gerukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:50.872693062 CET	192.168.2.7	8.8.8.8	0x1d10	Standard query (0)	gerukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:58.879478931 CET	192.168.2.7	8.8.8.8	0x549	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:59.893799067 CET	192.168.2.7	8.8.8.8	0x549	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:00.414546013 CET	192.168.2.7	8.8.8.8	0xab7	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:00.504049063 CET	192.168.2.7	8.8.8.8	0x66c	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:00.940325975 CET	192.168.2.7	8.8.8.8	0x549	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:01.073736906 CET	192.168.2.7	8.8.8.8	0x21ce	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:01.426948071 CET	192.168.2.7	8.8.8.8	0xab7	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:01.519082069 CET	192.168.2.7	8.8.8.8	0x66c	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:02.081192017 CET	192.168.2.7	8.8.8.8	0x21ce	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:02.440943003 CET	192.168.2.7	8.8.8.8	0xab7	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:02.549933910 CET	192.168.2.7	8.8.8.8	0x66c	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:03.003319979 CET	192.168.2.7	8.8.8.8	0x549	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:03.112885952 CET	192.168.2.7	8.8.8.8	0x21ce	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:04.471956968 CET	192.168.2.7	8.8.8.8	0xab7	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:04.566345930 CET	192.168.2.7	8.8.8.8	0x66c	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:05.159606934 CET	192.168.2.7	8.8.8.8	0x21ce	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:25.470429897 CET	192.168.2.7	8.8.8.8	0x982b	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.107110977 CET	192.168.2.7	8.8.8.8	0xc765	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.184900999 CET	192.168.2.7	8.8.8.8	0x89a2	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:30.256908894 CET	192.168.2.7	8.8.8.8	0xe5ed	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 16, 2021 09:48:36.246262074 CET	192.168.2.7	8.8.8.8	0xe4c8	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:39.935625076 CET	192.168.2.7	8.8.8.8	0x9240	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:40.069211006 CET	192.168.2.7	8.8.8.8	0x76c9	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:41.136293888 CET	192.168.2.7	8.8.8.8	0x19af	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:46.405317068 CET	192.168.2.7	8.8.8.8	0xc45d	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:50.170628071 CET	192.168.2.7	8.8.8.8	0xebe7	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:50.291120052 CET	192.168.2.7	8.8.8.8	0x4c5b	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:51.356180906 CET	192.168.2.7	8.8.8.8	0x34d	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:56.451184988 CET	192.168.2.7	8.8.8.8	0x3fa2	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:57.445242882 CET	192.168.2.7	8.8.8.8	0x3fa2	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:58.507932901 CET	192.168.2.7	8.8.8.8	0x3fa2	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:00.340672970 CET	192.168.2.7	8.8.8.8	0x2fa4	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:00.439784050 CET	192.168.2.7	8.8.8.8	0x417	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:01.382004023 CET	192.168.2.7	8.8.8.8	0x2fa4	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:01.458255053 CET	192.168.2.7	8.8.8.8	0x417	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:02.081366062 CET	192.168.2.7	8.8.8.8	0x9171	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:02.381783962 CET	192.168.2.7	8.8.8.8	0x2fa4	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:02.460206985 CET	192.168.2.7	8.8.8.8	0x417	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:03.095551014 CET	192.168.2.7	8.8.8.8	0x9171	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:04.153434038 CET	192.168.2.7	8.8.8.8	0x9171	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:04.385709047 CET	192.168.2.7	8.8.8.8	0x2fa4	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:04.515564919 CET	192.168.2.7	8.8.8.8	0x417	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:06.249155998 CET	192.168.2.7	8.8.8.8	0x9171	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:21.756612062 CET	192.168.2.7	8.8.8.8	0xdbc6	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:27.348459005 CET	192.168.2.7	8.8.8.8	0x6ccd	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:27.611932039 CET	192.168.2.7	8.8.8.8	0x2241	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:29.548809052 CET	192.168.2.7	8.8.8.8	0xea0d	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:32.417371988 CET	192.168.2.7	8.8.8.8	0x502c	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:38.161843061 CET	192.168.2.7	8.8.8.8	0x1aa0	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:38.606929064 CET	192.168.2.7	8.8.8.8	0x4afa	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:40.319984913 CET	192.168.2.7	8.8.8.8	0x4e94	Standard query (0)	berukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:42.488115072 CET	192.168.2.7	8.8.8.8	0xc53d	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:48.380752087 CET	192.168.2.7	8.8.8.8	0x21af	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:48.800364017 CET	192.168.2.7	8.8.8.8	0x22d5	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:50.501629114 CET	192.168.2.7	8.8.8.8	0x7772	Standard query (0)	gerukoneru .website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:52.549086094 CET	192.168.2.7	8.8.8.8	0x209a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:53.546605110 CET	192.168.2.7	8.8.8.8	0x209a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 16, 2021 09:49:54.562756062 CET	192.168.2.7	8.8.8.8	0x209a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:56.563133955 CET	192.168.2.7	8.8.8.8	0x209a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:00.069917917 CET	192.168.2.7	8.8.8.8	0xf718	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:00.135617018 CET	192.168.2.7	8.8.8.8	0xbe5a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:00.643827915 CET	192.168.2.7	8.8.8.8	0xc354	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:01.063044071 CET	192.168.2.7	8.8.8.8	0xf718	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:01.125665903 CET	192.168.2.7	8.8.8.8	0xbe5a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:01.642425060 CET	192.168.2.7	8.8.8.8	0xc354	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:02.125401020 CET	192.168.2.7	8.8.8.8	0xf718	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:02.141103983 CET	192.168.2.7	8.8.8.8	0xbe5a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:02.656879902 CET	192.168.2.7	8.8.8.8	0xc354	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:04.156891108 CET	192.168.2.7	8.8.8.8	0xbe5a	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:04.657082081 CET	192.168.2.7	8.8.8.8	0xc354	Standard query (0)	fortunarah.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:18.062139988 CET	192.168.2.7	8.8.8.8	0xc34	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:25.743124962 CET	192.168.2.7	8.8.8.8	0xb203	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:25.761929035 CET	192.168.2.7	8.8.8.8	0x5b02	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:26.500143051 CET	192.168.2.7	8.8.8.8	0x8bce	Standard query (0)	windows.update3.com	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:28.723965883 CET	192.168.2.7	8.8.8.8	0x2d41	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:36.390099049 CET	192.168.2.7	8.8.8.8	0x72db	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:36.496087074 CET	192.168.2.7	8.8.8.8	0xdc47	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:37.139866114 CET	192.168.2.7	8.8.8.8	0x7816	Standard query (0)	berukoneru.website	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:38.758304119 CET	192.168.2.7	8.8.8.8	0xcec3	Standard query (0)	gerukoneru.website	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:47:27.097388029 CET	8.8.8.8	192.168.2.7	0xdee2	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:47:27.097388029 CET	8.8.8.8	192.168.2.7	0xdee2	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.097388029 CET	8.8.8.8	192.168.2.7	0xdee2	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.097388029 CET	8.8.8.8	192.168.2.7	0xdee2	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.145597935 CET	8.8.8.8	192.168.2.7	0xa486	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:47:27.145597935 CET	8.8.8.8	192.168.2.7	0xa486	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.145597935 CET	8.8.8.8	192.168.2.7	0xa486	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.145597935 CET	8.8.8.8	192.168.2.7	0xa486	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.244956970 CET	8.8.8.8	192.168.2.7	0x1b94	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:47:27.244956970 CET	8.8.8.8	192.168.2.7	0x1b94	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.244956970 CET	8.8.8.8	192.168.2.7	0x1b94	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:27.244956970 CET	8.8.8.8	192.168.2.7	0x1b94	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:29.904055119 CET	8.8.8.8	192.168.2.7	0x17cd	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:47:29.904055119 CET	8.8.8.8	192.168.2.7	0x17cd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:29.904055119 CET	8.8.8.8	192.168.2.7	0x17cd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:29.904055119 CET	8.8.8.8	192.168.2.7	0x17cd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:38.320662022 CET	8.8.8.8	192.168.2.7	0xd69e	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:40.004465103 CET	8.8.8.8	192.168.2.7	0x33e	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:40.085695982 CET	8.8.8.8	192.168.2.7	0x556b	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:40.673250914 CET	8.8.8.8	192.168.2.7	0xf460	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:48.396979094 CET	8.8.8.8	192.168.2.7	0xd5c1	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:50.224988937 CET	8.8.8.8	192.168.2.7	0xf9d6	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:47:50.316543102 CET	8.8.8.8	192.168.2.7	0x5d1a	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:47:50.893662930 CET	8.8.8.8	192.168.2.7	0x1d10	Name error (3)	gerukoneru .website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:03.895652056 CET	8.8.8.8	192.168.2.7	0x549	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:04.909097910 CET	8.8.8.8	192.168.2.7	0x549	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:04.976258993 CET	8.8.8.8	192.168.2.7	0x549	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:05.430758953 CET	8.8.8.8	192.168.2.7	0xab7	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:05.521769047 CET	8.8.8.8	192.168.2.7	0x66c	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:06.091595888 CET	8.8.8.8	192.168.2.7	0x21ce	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:06.443227053 CET	8.8.8.8	192.168.2.7	0xab7	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:06.536413908 CET	8.8.8.8	192.168.2.7	0x66c	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:07.100347042 CET	8.8.8.8	192.168.2.7	0x21ce	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:07.457132101 CET	8.8.8.8	192.168.2.7	0xab7	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:07.567496061 CET	8.8.8.8	192.168.2.7	0x66c	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:08.018371105 CET	8.8.8.8	192.168.2.7	0x549	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:08.130769968 CET	8.8.8.8	192.168.2.7	0x21ce	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:08.496167898 CET	8.8.8.8	192.168.2.7	0xab7	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:08.603629112 CET	8.8.8.8	192.168.2.7	0x66c	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:10.177064896 CET	8.8.8.8	192.168.2.7	0x21ce	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:25.599142075 CET	8.8.8.8	192.168.2.7	0x982b	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:48:25.599142075 CET	8.8.8.8	192.168.2.7	0x982b	No error (0)	prod-sav-park-lb01-1 919960993.us-east-2. elb.amazon aws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:25.599142075 CET	8.8.8.8	192.168.2.7	0x982b	No error (0)	prod-sav-park-lb01-1 919960993.us-east-2. elb.amazon aws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:25.599142075 CET	8.8.8.8	192.168.2.7	0x982b	No error (0)	prod-sav-park-lb01-1 919960993.us-east-2. elb.amazon aws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.128571987 CET	8.8.8.8	192.168.2.7	0xc765	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:48:29.128571987 CET	8.8.8.8	192.168.2.7	0xc765	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.128571987 CET	8.8.8.8	192.168.2.7	0xc765	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.128571987 CET	8.8.8.8	192.168.2.7	0xc765	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.203954935 CET	8.8.8.8	192.168.2.7	0x89a2	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:48:29.203954935 CET	8.8.8.8	192.168.2.7	0x89a2	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.203954935 CET	8.8.8.8	192.168.2.7	0x89a2	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:29.203954935 CET	8.8.8.8	192.168.2.7	0x89a2	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:30.273638964 CET	8.8.8.8	192.168.2.7	0xe5ed	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:48:30.273638964 CET	8.8.8.8	192.168.2.7	0xe5ed	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:30.273638964 CET	8.8.8.8	192.168.2.7	0xe5ed	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:30.273638964 CET	8.8.8.8	192.168.2.7	0xe5ed	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:36.262774944 CET	8.8.8.8	192.168.2.7	0xe4c8	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:39.954916954 CET	8.8.8.8	192.168.2.7	0x9240	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:40.087718010 CET	8.8.8.8	192.168.2.7	0x76c9	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:41.154951096 CET	8.8.8.8	192.168.2.7	0x19af	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:46.421927929 CET	8.8.8.8	192.168.2.7	0xc45d	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:50.187510967 CET	8.8.8.8	192.168.2.7	0xebe7	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:48:50.311907053 CET	8.8.8.8	192.168.2.7	0x4c5b	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:48:51.377249002 CET	8.8.8.8	192.168.2.7	0x34d	Name error (3)	gerukoneru .website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:00.475156069 CET	8.8.8.8	192.168.2.7	0x3fa2	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:01.470026970 CET	8.8.8.8	192.168.2.7	0x3fa2	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:02.532615900 CET	8.8.8.8	192.168.2.7	0x3fa2	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:05.361011982 CET	8.8.8.8	192.168.2.7	0x2fa4	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:05.444638014 CET	8.8.8.8	192.168.2.7	0x417	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:06.399498940 CET	8.8.8.8	192.168.2.7	0x2fa4	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:06.476315022 CET	8.8.8.8	192.168.2.7	0x417	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:06.533787966 CET	8.8.8.8	192.168.2.7	0x2fa4	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:07.102721930 CET	8.8.8.8	192.168.2.7	0x9171	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:07.477535963 CET	8.8.8.8	192.168.2.7	0x417	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:08.113522053 CET	8.8.8.8	192.168.2.7	0x9171	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:08.675761938 CET	8.8.8.8	192.168.2.7	0x417	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:08.724967003 CET	8.8.8.8	192.168.2.7	0x2fa4	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:09.171401978 CET	8.8.8.8	192.168.2.7	0x9171	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:11.266437054 CET	8.8.8.8	192.168.2.7	0x9171	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:21.775130033 CET	8.8.8.8	192.168.2.7	0xdbc6	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:49:21.775130033 CET	8.8.8.8	192.168.2.7	0xdbc6	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:21.775130033 CET	8.8.8.8	192.168.2.7	0xdbc6	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:21.775130033 CET	8.8.8.8	192.168.2.7	0xdbc6	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:27.365381002 CET	8.8.8.8	192.168.2.7	0x6ccd	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:49:27.365381002 CET	8.8.8.8	192.168.2.7	0x6ccd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:49:27.365381002 CET	8.8.8.8	192.168.2.7	0x6ccd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:27.365381002 CET	8.8.8.8	192.168.2.7	0x6ccd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:27.630573988 CET	8.8.8.8	192.168.2.7	0x2241	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:49:27.630573988 CET	8.8.8.8	192.168.2.7	0x2241	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:27.630573988 CET	8.8.8.8	192.168.2.7	0x2241	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:27.630573988 CET	8.8.8.8	192.168.2.7	0x2241	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:29.565855026 CET	8.8.8.8	192.168.2.7	0xea0d	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:49:29.565855026 CET	8.8.8.8	192.168.2.7	0xea0d	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:29.565855026 CET	8.8.8.8	192.168.2.7	0xea0d	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:29.565855026 CET	8.8.8.8	192.168.2.7	0xea0d	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:32.438484907 CET	8.8.8.8	192.168.2.7	0x502c	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:38.184230089 CET	8.8.8.8	192.168.2.7	0x1aa0	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:38.625797987 CET	8.8.8.8	192.168.2.7	0x4afa	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:40.340465069 CET	8.8.8.8	192.168.2.7	0x4e94	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:42.505004883 CET	8.8.8.8	192.168.2.7	0xc53d	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:48.399806023 CET	8.8.8.8	192.168.2.7	0x21af	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:48.817127943 CET	8.8.8.8	192.168.2.7	0x22d5	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:50.523742914 CET	8.8.8.8	192.168.2.7	0x7772	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:56.711815119 CET	8.8.8.8	192.168.2.7	0x209a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)

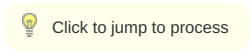
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:49:57.574570894 CET	8.8.8.8	192.168.2.7	0x209a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:49:59.580099106 CET	8.8.8.8	192.168.2.7	0x209a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:00.601974010 CET	8.8.8.8	192.168.2.7	0x209a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:04.095603943 CET	8.8.8.8	192.168.2.7	0xf718	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:04.167093039 CET	8.8.8.8	192.168.2.7	0xbe5a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:04.671138048 CET	8.8.8.8	192.168.2.7	0xc354	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:05.088732958 CET	8.8.8.8	192.168.2.7	0xf718	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:05.149595022 CET	8.8.8.8	192.168.2.7	0xbe5a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:05.668211937 CET	8.8.8.8	192.168.2.7	0xc354	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:06.166713953 CET	8.8.8.8	192.168.2.7	0xbe5a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:06.672385931 CET	8.8.8.8	192.168.2.7	0xf718	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:06.683897972 CET	8.8.8.8	192.168.2.7	0xc354	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:08.187335968 CET	8.8.8.8	192.168.2.7	0xbe5a	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:08.812439919 CET	8.8.8.8	192.168.2.7	0xc354	Server failure (2)	fortunarah.com	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:18.082094908 CET	8.8.8.8	192.168.2.7	0xc34	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:50:18.082094908 CET	8.8.8.8	192.168.2.7	0xc34	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:18.082094908 CET	8.8.8.8	192.168.2.7	0xc34	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:18.082094908 CET	8.8.8.8	192.168.2.7	0xc34	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:25.759835958 CET	8.8.8.8	192.168.2.7	0xb203	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:50:25.759835958 CET	8.8.8.8	192.168.2.7	0xb203	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:25.759835958 CET	8.8.8.8	192.168.2.7	0xb203	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2021 09:50:25.759835958 CET	8.8.8.8	192.168.2.7	0xb203	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:25.877816916 CET	8.8.8.8	192.168.2.7	0x5b02	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:50:25.877816916 CET	8.8.8.8	192.168.2.7	0x5b02	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:25.877816916 CET	8.8.8.8	192.168.2.7	0x5b02	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:25.877816916 CET	8.8.8.8	192.168.2.7	0x5b02	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:26.517128944 CET	8.8.8.8	192.168.2.7	0x8bce	No error (0)	windows.update3.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 16, 2021 09:50:26.517128944 CET	8.8.8.8	192.168.2.7	0x8bce	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.20.161.64	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:26.517128944 CET	8.8.8.8	192.168.2.7	0x8bce	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.219.227.107	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:26.517128944 CET	8.8.8.8	192.168.2.7	0x8bce	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.124.139	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:28.742445946 CET	8.8.8.8	192.168.2.7	0x2d41	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:36.409636021 CET	8.8.8.8	192.168.2.7	0x72db	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:36.514867067 CET	8.8.8.8	192.168.2.7	0xdc47	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:37.158690929 CET	8.8.8.8	192.168.2.7	0x7816	Name error (3)	berukoneru.website	none	none	A (IP address)	IN (0x0001)
Dec 16, 2021 09:50:38.777276039 CET	8.8.8.8	192.168.2.7	0xcec3	Name error (3)	gerukoneru.website	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6620 Parent PID: 3592

General

Start time:	09:46:29
Start date:	16/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\fiHY95Y1CZ.dll"
Imagebase:	0xae0000
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: 00000001.00000003.414360466.0000000002DFF000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.370009221.0000000002FFB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.779225699.0000000003178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346831969.0000000003178000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.392772677.0000000002EFD000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6664 Parent PID: 6620

General

Start time:	09:46:30
Start date:	16/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\fiHY95Y1CZ.dll",#1
Imagebase:	0x870000
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: 6700 Parent PID: 6620

General

Start time:	09:46:30
Start date:	16/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\fiHY95Y1CZ.dll
Imagebase:	0xe80000
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: 00000004.00000003.418476955.000000000581F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.370329481.0000000005A1B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.780149501.0000000005B98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.346931198.0000000005B98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.396552270.000000000591D000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6712 Parent PID: 6664

General

Start time:	09:46:30
Start date:	16/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\fiHY95Y1CZ.dll",#1
Imagebase:	0x1190000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000005.00000003.418282417.0000000004BDF000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.346775098.0000000004F58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.370118981.0000000004DDB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.396516562.0000000004CDD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.780908469.0000000004F58000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6728 Parent PID: 6620

General

Start time:	09:46:30
Start date:	16/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\fiHY95Y1CZ.dll,DllRegisterServer
Imagebase:	0x1190000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000006.00000002.781134724.0000000004F98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.397818170.0000000004D1D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.376015691.0000000004E1B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.352281996.0000000004F98000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.419719832.0000000004C1F000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis