

JoeSandbox Cloud BASIC



ID: 433772

Sample Name: payload.exe

Cookbook: default.jbs

Time: 19:38:09

Date: 13/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report payload.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
AV Detection:	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
Contacted IPs	6
Public	6
General Information	6
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	7
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Network Behavior	9
Network Port Distribution	9
TCP Packets	9
Code Manipulations	9
Statistics	10
Behavior	10
System Behavior	10
Analysis Process: payload.exe PID: 2596 Parent PID: 5812	10
General	10
File Activities	10
File Created	10
File Written	10
File Read	10
Analysis Process: conhost.exe PID: 5388 Parent PID: 2596	10
General	10
Disassembly	10
Code Analysis	11

Analysis Report payload.exe

Overview

General Information

Sample Name:	payload.exe
Analysis ID:	433772
MD5:	b06395f18df7aec..
SHA1:	83e8ebe8e706fe4.
SHA256:	1d9bcc9ec9ebb9...
Infos:	
Most interesting Screenshot:	

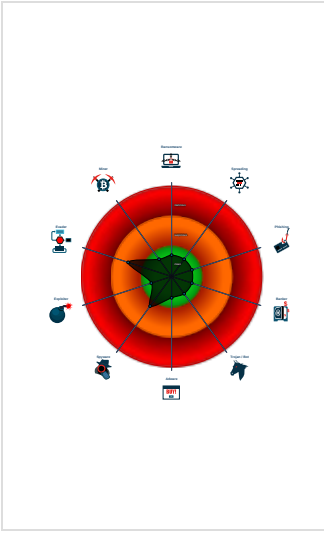
Detection

Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub...
Contains long sleeps (>= 3 min)
Found a high number of Window / Us...
May sleep (evasive loops) to hinder ...
Program does not show much activi...
Queries the volume information (nam...
Sample execution stops while proce...
Sample file is different than original ...
Uses 32bit PE files

Classification



Process Tree

System is w10x64
- payload.exe (PID: 2596 cmdline: 'C:\Users\user\Desktop\payload.exe' MD5: B06395F18DF7AEC3D7C00AA219594631) - conhost.exe (PID: 5388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496) - cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

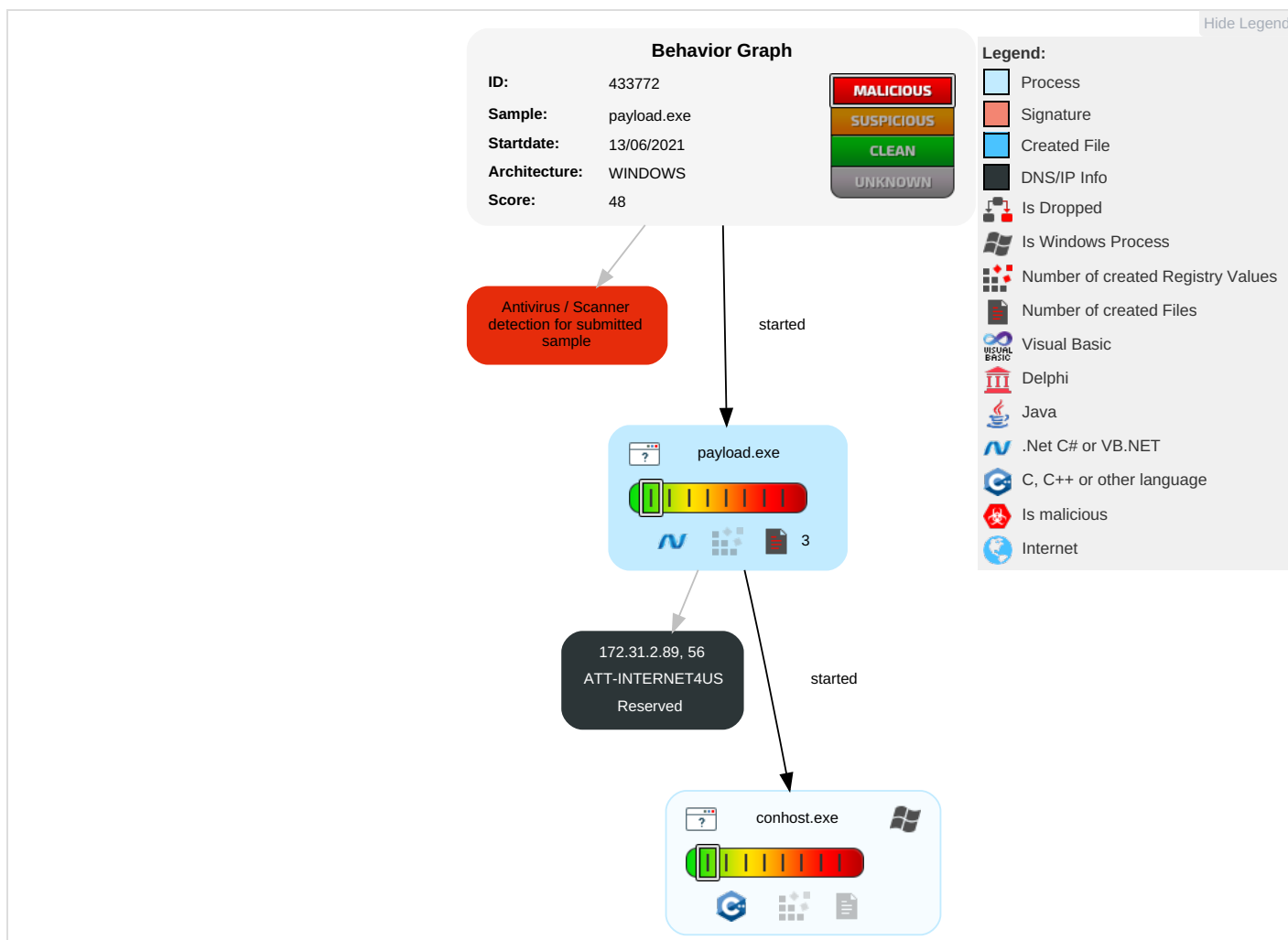
AV Detection:



Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Disable or Modify Tools 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	Recovery

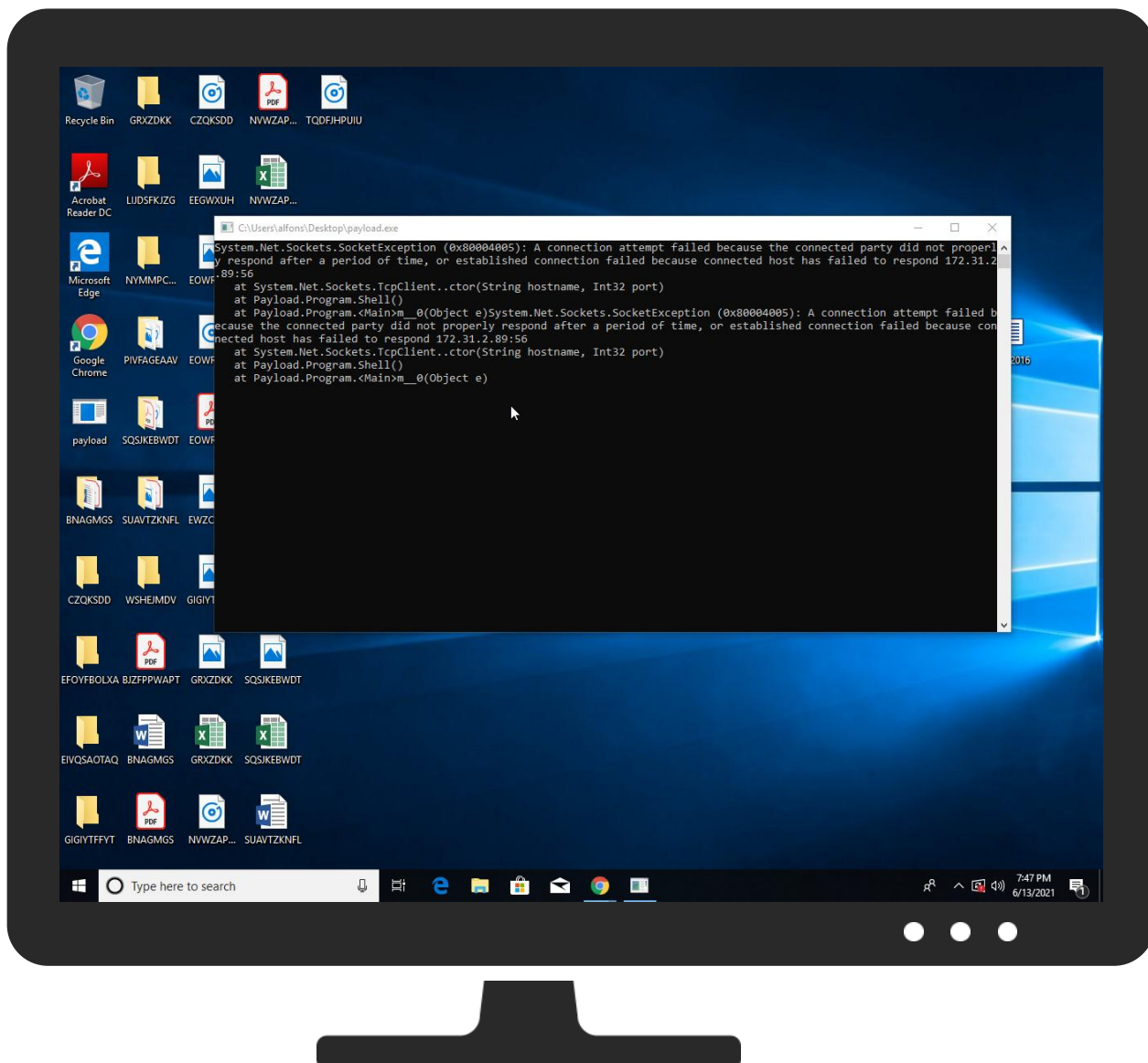
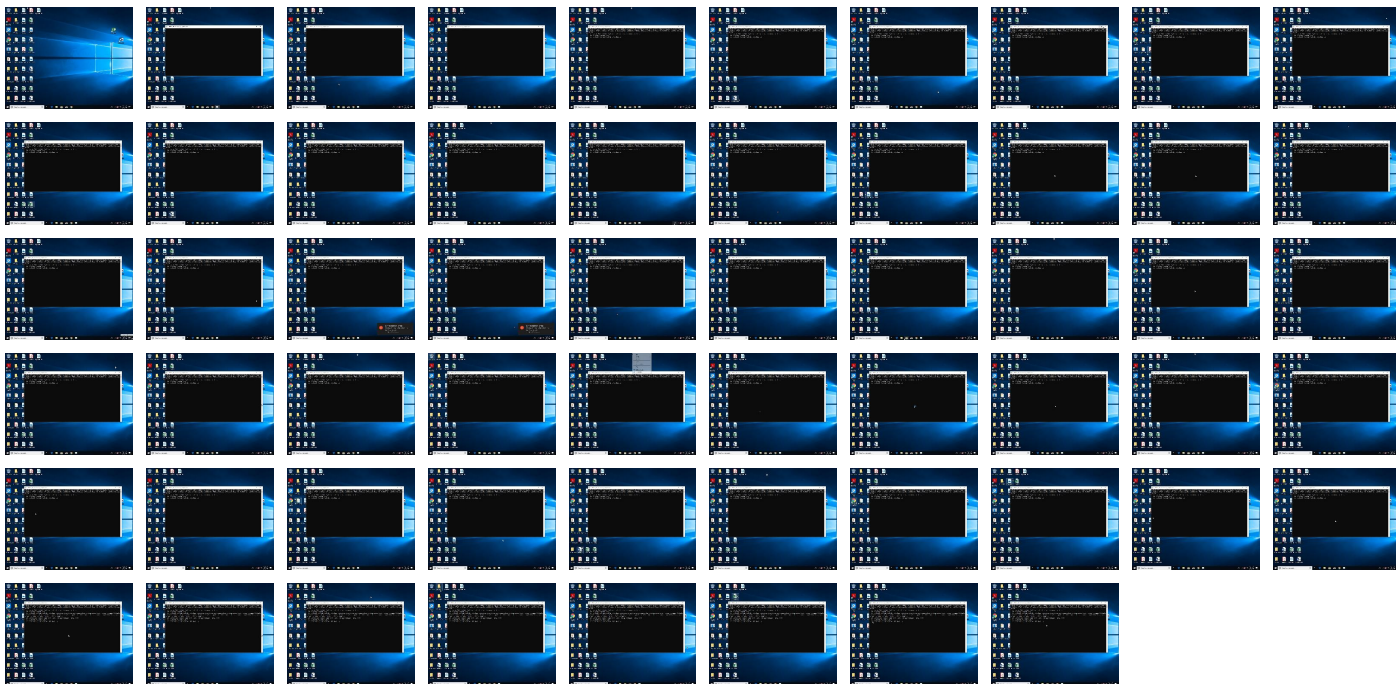
Behavior Graph



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
payload.exe	100%	Avira	HEUR/AGEN.1133230	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.payload.exe.100000.0.unpack	100%	Avira	HEUR/AGEN.1133230		Download File
1.0.payload.exe.100000.0.unpack	100%	Avira	HEUR/AGEN.1133230		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.31.2.89	unknown	Reserved		7018	ATT-INTERNET4US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433772
Start date:	13.06.2021
Start time:	19:38:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payload.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:	44
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:	mal48.winEXE@2/1@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
19:38:55	API Interceptor	3653x Sleep call for process: payload.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ATT-INTERNET4US	payload.exe	Get hash	malicious	Browse	• 172.31.2.56
	payload.exe	Get hash	malicious	Browse	• 172.31.2.71
	payload.exe	Get hash	malicious	Browse	• 172.31.2.100
	mssecsvr.exe	Get hash	malicious	Browse	• 71.149.37.79
	Docc.html	Get hash	malicious	Browse	• 13.36.218.177
	fl8BN6Qdsu.dll	Get hash	malicious	Browse	• 13.32.16.68
	#Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm	Get hash	malicious	Browse	• 13.36.218.177
	mjzvlwau	Get hash	malicious	Browse	• 13.171.225.162
	MedMooc.exe	Get hash	malicious	Browse	• 172.17.0.207
	FAX.HTML	Get hash	malicious	Browse	• 13.36.218.177
	K9pRfTme7J.exe	Get hash	malicious	Browse	• 172.18.60.217
	K9pRfTme7J.exe	Get hash	malicious	Browse	• 172.18.60.217
	project-a.exe	Get hash	malicious	Browse	• 172.129.11.3.237
	project-a.exe	Get hash	malicious	Browse	• 172.129.11.3.237
	OW73NJTujh.dll	Get hash	malicious	Browse	• 12.96.42.215
	S5.exe	Get hash	malicious	Browse	• 12.176.148.42
	_cro.exe	Get hash	malicious	Browse	• 172.16.2.1
	EKSkwdJJi7.exe	Get hash	malicious	Browse	• 172.19.255.48

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DA1wxOjE9C.exe	Get hash	malicious	Browse	13.36.178.139
	XPChvE6GQd	Get hash	malicious	Browse	45.30.40.164

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

I\Device\ConDrv	
Process:	C:\Users\user\Desktop\payload.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	784
Entropy (8bit):	4.821721066094882
Encrypted:	false
SSDEEP:	12:pqecNtxWwWIGxWVDroBitqecNtxWwWIGxWVDroBO:rcNtxHIG8VXTHcNtxHIG8VXv
MD5:	C147D87539490FCE026C828437C09B01
SHA1:	A921A72CCBED142579DE211DA005FB65AE713A07
SHA-256:	12AE6114710970B7297DD8C52A0874FA455E11F96235FC38DD863A6174213629
SHA-512:	D686D4EFA3C7D5CD152AB535B2EC95EEFE66D70A60A85C2E9A79202481879D67117B24254543E173BBA56461BD80098D49FABE0D107427D32D772903CF5080F
Malicious:	false
Reputation:	low
Preview:	System.Net.Sockets.SocketException (0x80004005): A connection attempt failed because the connected party did not properly respond after a period of time, or est ablished connection failed because connected host has failed to respond 172.31.2.89:56.. at System.Net.Sockets.TcpClient..ctor(String hostname, Int32 port).. at Paylo ad.Program.Shell().. at Payload.Program.<Main>m__0(Object e)System.Net.Sockets.SocketException (0x80004005): A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 172.31.2.89:56.. at System.Net.Soc kets.TcpClient..ctor(String hostname, Int32 port).. at Payload.Program.Shell().. at Payload.Program.<Main>m__0(Object e)

Static File Info

General	
File type:	PE32 executable (console) Intel 80386 Mono/.Net as sembly, for MS Windows
Entropy (8bit):	3.742190561091188
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:	payload.exe
File size:	5120
MD5:	b06395f18df7aec3d7c00aa219594631
SHA1:	83e8ebe8e706fe4fdb0220cac18094ca4caa0259
SHA256:	1d9bcc9e9ebbe9e1b0947bdbb0a80c09e7277b2af65a4d 25d64d99606d2a7b3a
SHA512:	76402a28a309311854efbd07589187a59bb90a696e9fdb6 62c921a7f98633c0e73f476c5e1d71404a7c0ad5d09edee 7e40d5ff8d1ac310a792c93faef5e89e2f
SSDEEP:	48:6HKfJGNa8766G8KH4duogo+bAcyMuPCU2Z+FK16 +k+IDUrinJmwJL0TQZtEOPulr:7Fj8G8KH49go+E1PCU UdTUrs7bsPOM
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$.....PE..L.....>*. ...@....@..... ..@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x402a3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 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	0xa44	0xc00	False	0.5068359375	data	4.66745426327	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x2d8	0x400	False	0.328125	data	2.32307159838	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: payload.exe PID: 2596 Parent PID: 5812

General

Start time:	19:38:54
Start date:	13/06/2021
Path:	C:\Users\user\Desktop\payload.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\payload.exe'
Imagebase:	0x100000
File size:	5120 bytes
MD5 hash:	B06395F18DF7AEC3D7C00AA219594631
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5388 Parent PID: 2596

General

Start time:	19:38:54
Start date:	13/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

