

JoeSandbox Cloud BASIC



ID: 458935

Sample Name: 29.7.2021.exe

Cookbook: default.jbs

Time: 22:09:17

Date: 03/08/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report 29.7.2021.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: Agenttesla	3
Yara Overview	3
Memory Dumps	3
Unpacked PEs	4
Sigma Overview	4
Jbx Signature Overview	4
AV Detection:	4
System Summary:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Stealing of Sensitive Information:	4
Remote Access Functionality:	4
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	5
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
Contacted IPs	7
General Information	7
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	9
Static File Info	9
General	9
File Icon	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	10
Imports	10
Version Infos	10
Network Behavior	10
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: 29.7.2021.exe PID: 1004 Parent PID: 5480	10
General	10
File Activities	11
File Created	11
File Read	11
Disassembly	11
Code Analysis	11

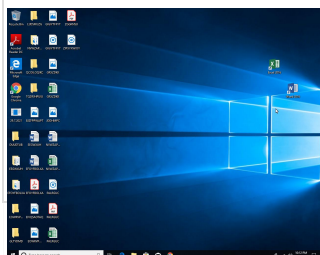
Windows Analysis Report 29.7.2021.exe

Overview

General Information

Sample Name:	29.7.2021.exe
Analysis ID:	458935
MD5:	1aae6bb425f9754.
SHA1:	0fd447e79c9e9d9.
SHA256:	61b5c977dcd06c...
Tags:	exe null
Infos:	

Most interesting Screenshot:



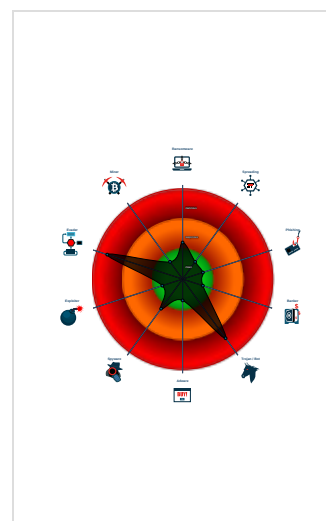
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
AgentTesla	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Yara detected AgentTesla
Yara detected AgentTesla
Yara detected AntiVM3
.NET source code contains potentia...
.NET source code contains very larg...
Machine Learning detection for samp...
Queries sensitive BIOS Information ...
Queries sensitive network adapter in...
Tries to detect sandboxes and other...
Contains long sleeps (>= 3 min)

Classification



Process Tree

- System is w10x64
-  29.7.2021.exe (PID: 1004 cmdline: 'C:\Users\user\Desktop\29.7.2021.exe' MD5: 1AAE6BB425F9754D217037E354DB1F3B)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "kintkinty@vivaldi.net",
  "Password": "pmoneyboy994",
  "Host": "smtp.vivaldi.net"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.491962978.0000000000D7 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.491962978.0000000000D7 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.496151220.00000000037A 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.496151220.00000000037A 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.492722077.00000000027A 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.29.7.2021.exe.d70000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.29.7.2021.exe.d70000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.29.7.2021.exe.d70000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.29.7.2021.exe.d70000.1.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.29.7.2021.exe.37df960.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 3 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 submitted file

Machine Learning detection for sample

System Summary:



.NET source code contains very large strings

Data Obfuscation:



.NET source code contains potential unpacker

Malware Analysis System Evasion:



Yara detected AntiVM3

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

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

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

Stealing of Sensitive Information:



Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:



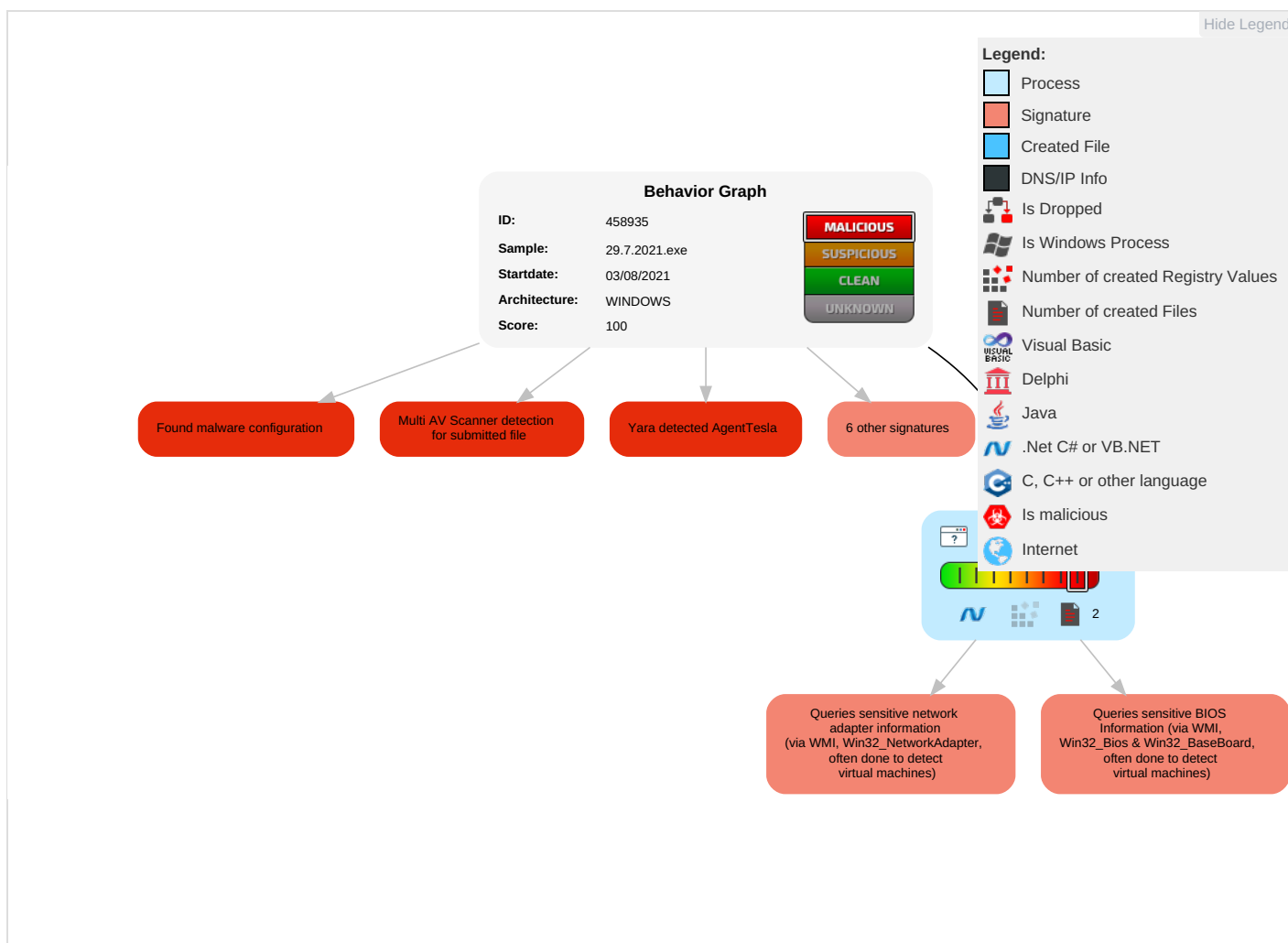
Yara detected AgentTesla

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	Network Effects
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1	Disable or Modify Tools 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdropping, Insecure Network Communications
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploitation of Sensitive Information, Redirecting Ports, Spoofing, Denial of Service
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploitation of Sensitive Information, Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 1 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulation of Device Communications

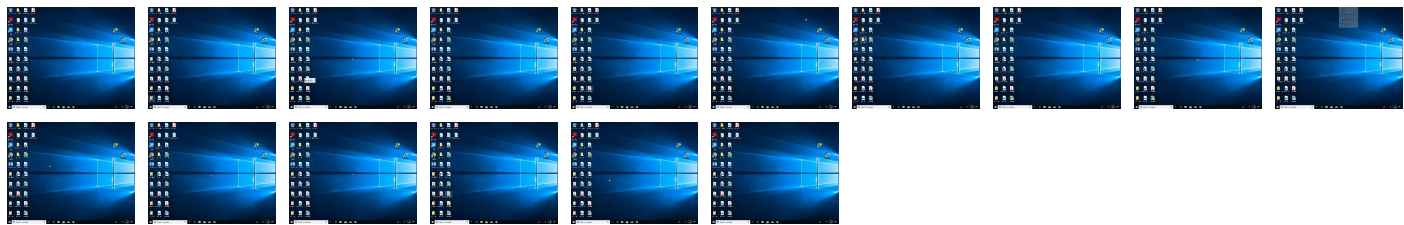
Behavior Graph



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
29.7.2021.exe	65%	Virustotal		Browse
29.7.2021.exe	46%	Metadefender		Browse
29.7.2021.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
29.7.2021.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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.founder.com.cn/cn/bThe	0%	URL Reputation	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://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://QgZlYk.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comldF	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comictoV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	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	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458935
Start date:	03.08.2021
Start time:	22:09:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	29.7.2021.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 47.9% • Quality standard deviation: 30%
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
22:10:58	API Interceptor	535x Sleep call for process: 29.7.2021.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:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.243271261799799
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:	29.7.2021.exe
File size:	557056
MD5:	1aae6bb425f9754d217037e354db1f3b
SHA1:	0fd447e79c9e9d9e50f268474a5a187b77c524dd
SHA256:	61b5c977dcd06cf5ecc11af4dc0190c189f55a644a771675812c0d65f27d1ae6
SHA512:	c78f838a1594f91d9222c2f88f0db5849d825bd9cc78fe78eb02a2b491e71ec7d2562dcfd36f3890fe4ddee5988b2d2cd70e912408ba5a3c29225877ce87e942
SSDEEP:	12288:9l3p+gczyhNSvRbBQHR4qz91hl0zSaNsvz+yuW DVid21Nal+E8tyvX4KLg69jfUx:HTKzpn2E+vFBI8H
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.PE..L... @G.a.....0..V.....B.....@.....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x489442
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:	0x61024740 [Thu Jul 29 06:14:24 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	0x87448	0x87600	False	0.737038680171	data	7.25332165725	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x5fc	0x600	False	0.446614583333	data	4.22227882843	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	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

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: 29.7.2021.exe PID: 1004 Parent PID: 5480

General

Start time:	22:10:06
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\29.7.2021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\29.7.2021.exe'
Imagebase:	0x360000
File size:	557056 bytes
MD5 hash:	1AAE6BB425F9754D217037E354DB1F3B
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: 00000000.00000002.491962978.0000000000D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.491962978.0000000000D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.496151220.00000000037A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.496151220.00000000037A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.492722077.00000000027A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.492722077.00000000027A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

[File Activities](#)

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis