

JOeSandbox Cloud BASIC



ID: 433188

Sample Name: 5a#U0435.exe

Cookbook: default.jbs

Time: 12:34:24

Date: 11/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 5a#U0435.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	4
Sigma Overview	5
Signature Overview	5
AV Detection:	5
System Summary:	5
Data Obfuscation:	5
Hooking and other Techniques for Hiding and Protection:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	5
Stealing of Sensitive Information:	5
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
Contacted IPs	10
General Information	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	11
General	11
File Icon	12
Static PE Info	12
General	12
Entrypoint Preview	12
Data Directories	12
Sections	12
Resources	12
Imports	13
Version Infos	13
Network Behavior	13
Code Manipulations	13
Statistics	13
Behavior	13
System Behavior	13
Analysis Process: 5a#U0435.exe PID: 7092 Parent PID: 6028	13
General	13
File Activities	13
File Created	13
File Written	13
File Read	13
Analysis Process: 5a#U0435.exe PID: 6960 Parent PID: 7092	14
General	14
File Activities	14
File Created	14
File Read	14
Disassembly	14

Analysis Report 5a#U0435.exe

Overview

General Information

Sample Name:

5a#U0435.exe

Analysis ID:

433188

MD5:

840880750b20f76..

SHA1:

f34240bbc4cd3f2..

SHA256:

05791cd943319c..

Tags:

exe

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

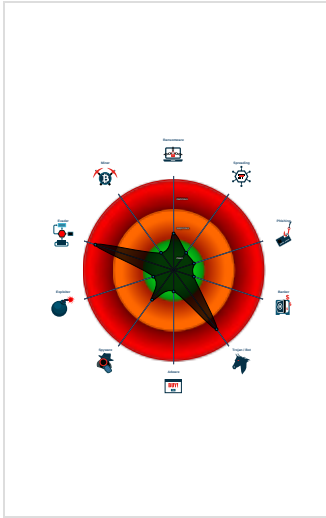
AgentTesla

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 method ...
- .NET source code contains very larg...
- .NET source code contains very larg...
- Injects a PE file into a foreign proce...
- Moves itself to temp directory
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...

Classification



Process Tree

- System is w10x64
- 5a#U0435.exe (PID: 7092 cmdline: 'C:\Users\user\Desktop\5a#U0435.exe' MD5: 840880750B20F76B946071CDB03ACB04)
 - 5a#U0435.exe (PID: 6960 cmdline: {path} MD5: 840880750B20F76B946071CDB03ACB04)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "leticia@inh.edu.mxInstitutohmh71mail.inh.edu.mx"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.720814161.0000000003E09000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.720814161.0000000003E09000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000000.716723139.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.716723139.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.718826690.0000000002E55000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 8 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.5a#U0435.exe.3ed40f8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.5a#U0435.exe.3ed40f8.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.2.5a#U0435.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.5a#U0435.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.5a#U0435.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

System Summary:



.NET source code contains very large array initializations

.NET source code contains very large strings

Data Obfuscation:



.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:



Moves itself to temp directory

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)

HIPS / PFW / Operating System Protection Evasion:



Injects a PE file into a foreign processes

Stealing of Sensitive Information:



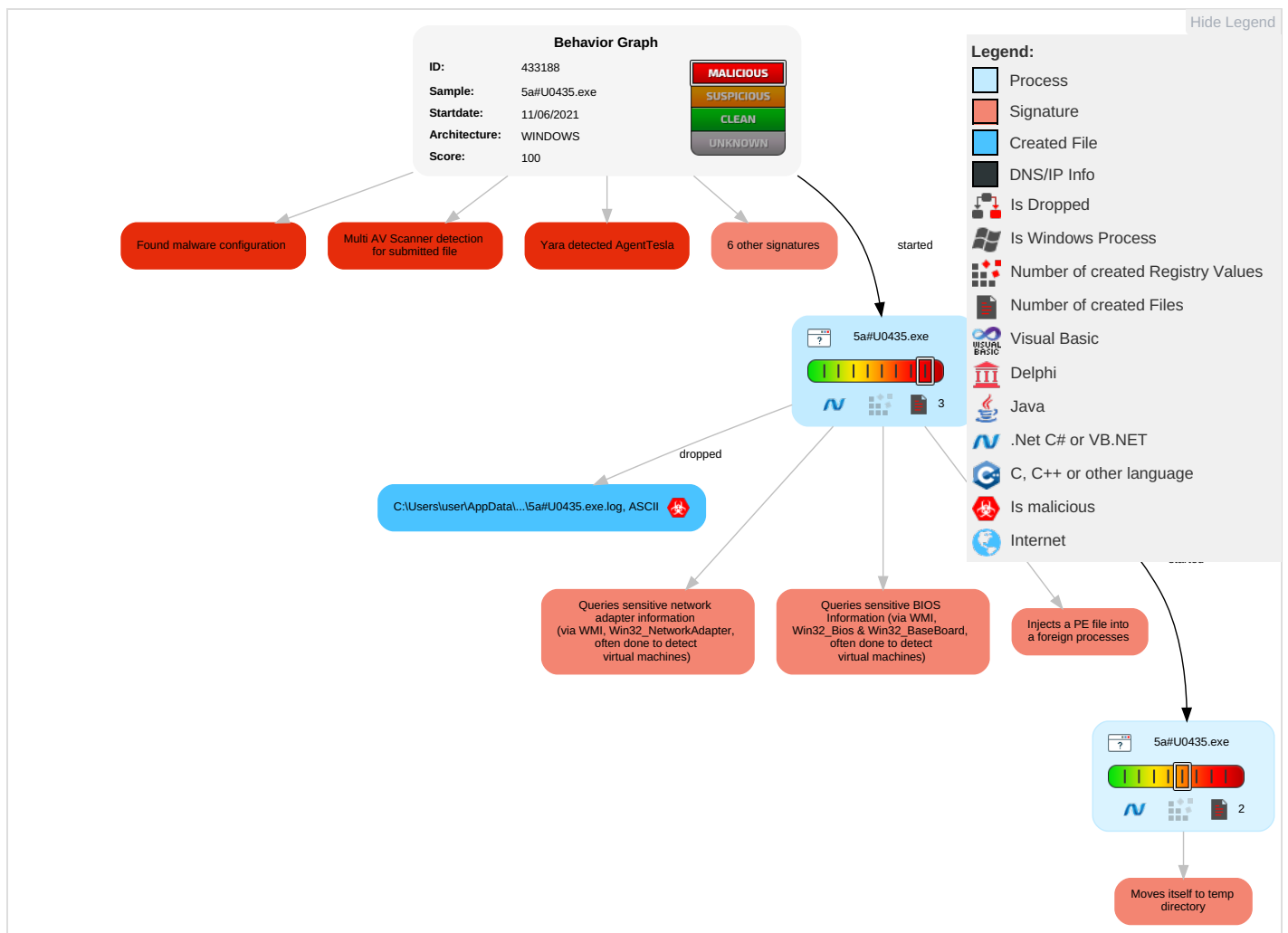
Remote Access Functionality:



Mitre Att&ck Matrix

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

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
5a#U0435.exe	43%	Virustotal		Browse
5a#U0435.exe	28%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.5a#U0435.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.5a#U0435.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.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://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.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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://aMMkIB.com	0%	Avira URL Cloud	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:	32.0.0 Black Diamond
Analysis ID:	433188
Start date:	11.06.2021
Start time:	12:34:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5a#U0435.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:	14
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@3/1@0/0
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
12:35:58	API Interceptor	530x Sleep call for process: 5a#U0435.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

C:\Users\luser\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5a#U0435.exe.log		
Process:	C:\Users\luser\Desktop\5a#U0435.exe	
File Type:	ASCII text, with CRLF line terminators	
Category:	dropped	
Size (bytes):	1216	
Entropy (8bit):	5.355304211458859	
Encrypted:	false	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr	
MD5:	FED34146BF2F2FA59DCF8702FCC8232E	
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C	
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6	
Malicious:	true	
Reputation:	high, very likely benign file	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089";C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a";C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089";C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21	

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.66213714438686

General

TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.80% - Win32 Executable (generic) a (10002005/4) 49.75% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Windows Screen Saver (13104/52) 0.07% - Generic Win/DOS Executable (2004/3) 0.01%
File name:	5a#U0435.exe
File size:	498176
MD5:	840880750b20f76b946071cdb03acb04
SHA1:	f34240bbc4cd3f2b50aeab05967404d5eff1518c
SHA256:	05791cd943319c72fc571ddd042d9c15545816977141d95d1ede6e4f7576c213
SHA512:	ba04f75818e97d1a3323a13eda8becc55ad094db8e102514810ae1f79da92559997af3b0cdc82e1d507db3dfd721b22f21e02c1af106bcee798a37440d5b5630
SSDEEP:	6144:3BU/xITe0C1y7cGUfEnYKvQbsuZCCOb5jx/VFFFH9+DAFHUYExIR/1KaJA1:36/X9ocCj+OVjxvFb+DhYqIR1fJk
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......PE..L.....0.....b.....@.....@.....

File Icon

	
Icon Hash:	18da1abcb2d2d2b0

Static PE Info

General

Entrypoint:	0x47a262
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:	0x60C2EEA8 [Fri Jun 11 05:03:36 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	0x78268	0x78400	False	0.86692762474	data	7.69530252682	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x105c	0x1200	False	0.271050347222	data	2.85405726059	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7e000	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

Behavior

 Click to jump to process

System Behavior

Analysis Process: 5a#U0435.exe PID: 7092 Parent PID: 6028

General

Start time:	12:35:06
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\5a#U0435.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\5a#U0435.exe'
Imagebase:	0x8b0000
File size:	498176 bytes
MD5 hash:	840880750B20F76B946071CDB03ACB04
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: 00000000.00000002.720814161.0000000003E09000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.720814161.0000000003E09000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.718826690.0000000002E55000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

General

Start time:	12:35:44
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\5a#U0435.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7e0000
File size:	498176 bytes
MD5 hash:	840880750B20F76B946071CDB03ACB04
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: 00000008.00000000.716723139.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.716723139.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.902344270.0000000002CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.902344270.0000000002CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.901262278.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.901262278.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis