ID: 528524
Sample Name: Sipari#U015f
formu.exe
Cookbook: default.jbs
Time: 13:18:14
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

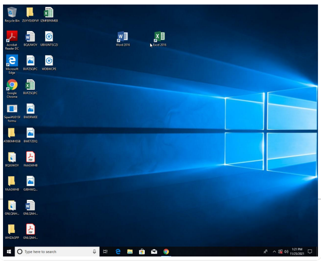
Windows Analysis Report Sipari#U015f formu.exe

Overview

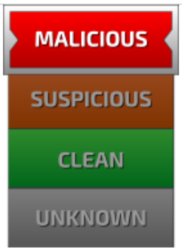
General Information

Sample Name:	Sipari#U015f formu.exe
Analysis ID:	528524
MD5:	032bbfd4181a7ce.
SHA1:	c99434f7f007f6f0..
SHA256:	9ae8f73164a7e81.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



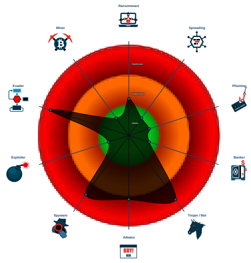
AgentTesla

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

Signatures

- Found malware configuration
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- .NET source code contains very larg…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- Sipari#U015f formu.exe (PID: 5356 cmdline: "C:\Users\user\Desktop\Sipari#U015f formu.exe" MD5: 032BBFD4181A7CEE029849DB610A318B)
  - Sipari#U015f formu.exe (PID: 5956 cmdline: C:\Users\user\Desktop\Sipari#U015f formu.exe MD5: 032BBFD4181A7CEE029849DB610A318B)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot2124462934:AAGr-L06waDdFGpnKJz3_DCOFcJpWDQ7WIM/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "-640017301",
  "Chat URL": "https://api.telegram.org/bot2124462934:AAGr-L06waDdFGpnKJz3_DCOFcJpWDQ7WIM/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.656174478.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.656174478.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.654836486.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.654836486.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.656667714.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Sipari#U015f formu.exe.2d971c8.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
3.0.Sipari#U015f formu.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.Sipari#U015f formu.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.Sipari#U015f formu.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.Sipari#U015f formu.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.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)

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected Telegram RAT

Yara detected AgentTesla

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Remote Access Functionality:

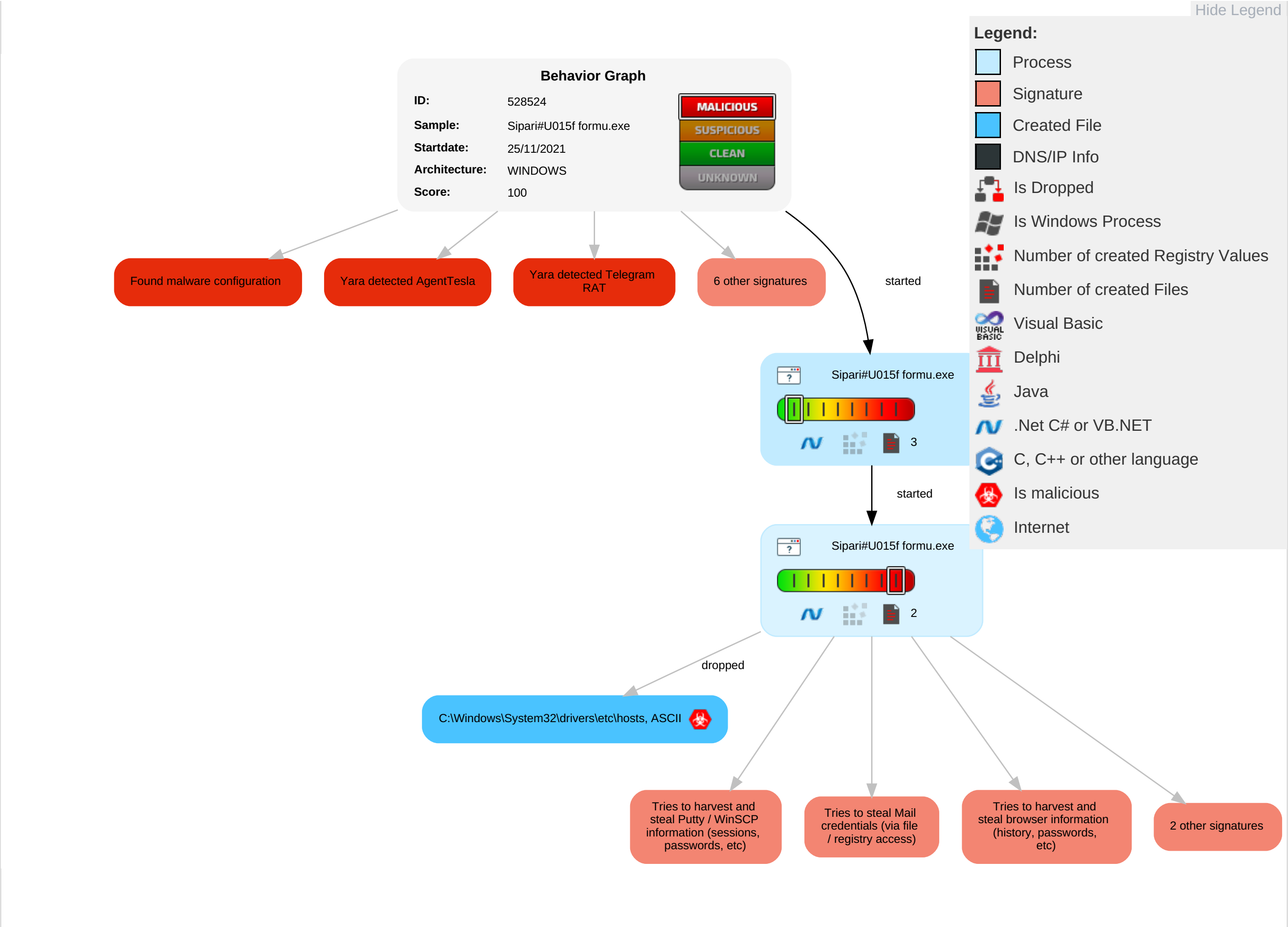
Yara detected Telegram RAT

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encryp Channe
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File and Directory Permissions Modification 1	Input Capture 1 1 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Junk D
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Stegan
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 3 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 1	Scheduled Transfer	Protocc Impers
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	System Information Discovery 1 1 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer P

Behavior Graph



Behavior Graph

ID: 528524

Sample: Sipari#U015f formu.exe

Startdate: 25/11/2021

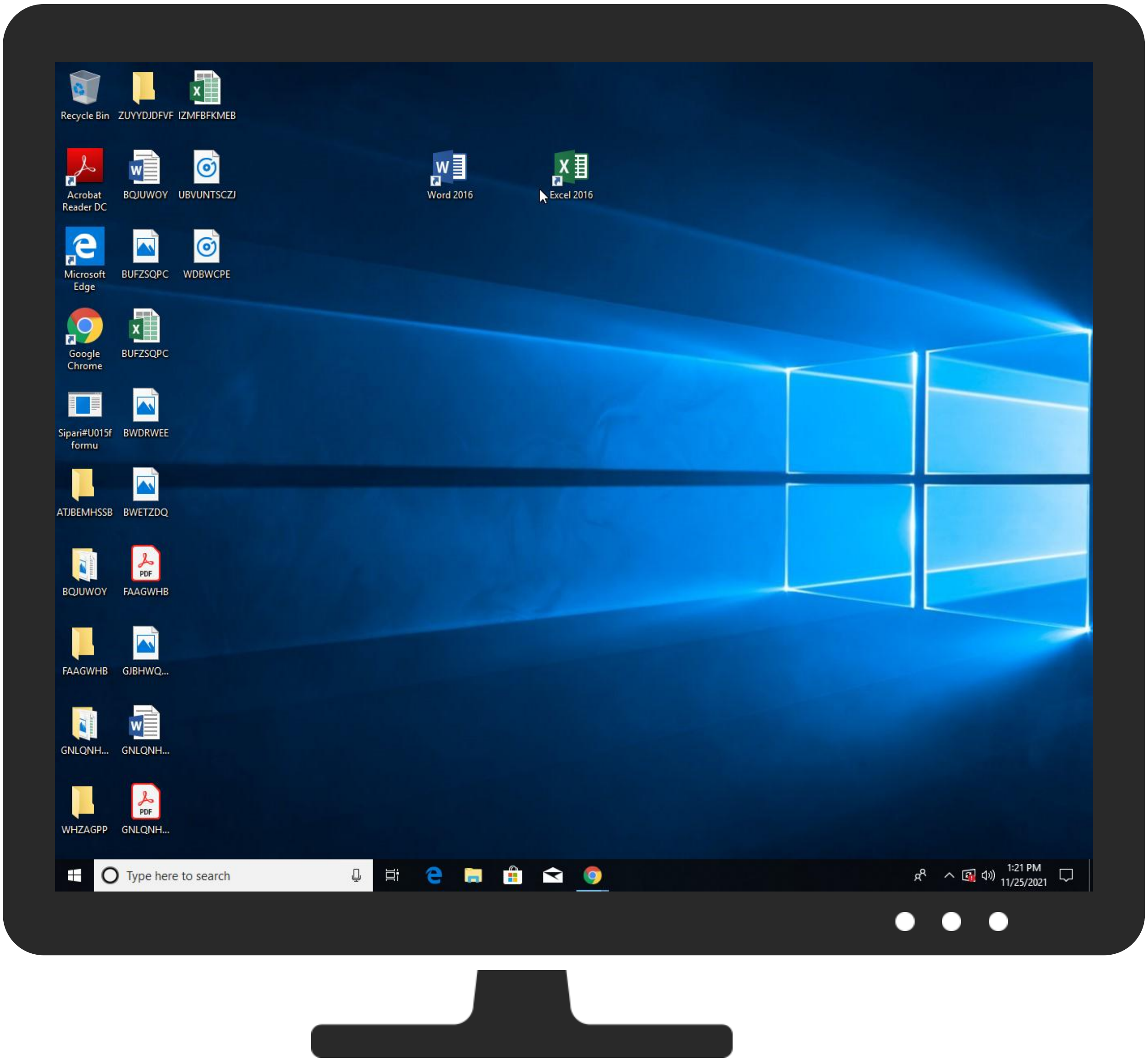
Architecture: WINDOWS

Score: 100

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
3.0.Sipari#U015f formu.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.Sipari#U015f formu.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Sipari#U015f formu.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Sipari#U015f formu.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Sipari#U015f formu.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Sipari#U015f formu.exe.400000.8.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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	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://nQZIDO.com	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	

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:	34.0.0 Boulder Opal
Analysis ID:	528524
Start date:	25.11.2021
Start time:	13:18:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sipari#U015f formu.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:	16
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.adwa.spyw.evad.winEXE@3/2@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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
13:19:03	API Interceptor	835x Sleep call for process: Sipari#U015f formu.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\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sipari#U015f formu.exe.log	
Process:	C:\Users\user\Desktop\Sipari#U015f formu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
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

C:\Windows\System32\drivers\etc\hosts ☣	
Process:	C:\Users\user\Desktop\Sipari#U015f formu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Windows\System32\drivers\etc\hosts	
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.871616213599999
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:	Sipari#U015f formu.exe
File size:	500736
MD5:	032bbfd4181a7cee029849db610a318b
SHA1:	c99434f7f007f6f0f1317839cc7129db813d0750
SHA256:	9ae8f73164a7e8159a942f5c304cb55560f975ca943f00c2ef4f6dd489ce0656
SHA512:	aa504d9d1235478c61bb0545cbef88e03bf2ab0a852ddbc ae1c65ba79511bf44ac43c023bcf5cf15c80aec4adf90a4 52a3d611cc32a6107c60f5c70fc13bf8e1
SSDEEP:	12288:xe1O0GEJPlAFHRv2wAtHcrhCaMI7oPLH8ixBFm:xkO0GkPlQRv2lt8rdVMPLH8i1
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....C.a.............0............^.... ....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47b95e
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:	0x619F43BA [Thu Nov 25 08:05:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319

General

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	0x79974	0x79a00	False	0.897995889003	data	7.88235938246	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x5ac	0x600	False	0.425130208333	data	4.10522833329	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: Sipari#U015f formu.exe PID: 5356 Parent PID: 1000

General

Start time:	13:19:02
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Sipari#U015f formu.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Sipari#U015f formu.exe"

Imagebase:	0xa80000
File size:	500736 bytes
MD5 hash:	032BBFD4181A7CEE029849DB610A318B
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: 00000000.00000002.658539650.0000000002D31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.658683577.0000000002DF5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.659041461.0000000003D3D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.659041461.0000000003D3D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Sipari#U015f formu.exe PID: 5956 Parent PID: 5356

General

Start time:	13:19:04
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Sipari#U015f formu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Sipari#U015f formu.exe
Imagebase:	0x590000
File size:	500736 bytes
MD5 hash:	032BBFD4181A7CEE029849DB610A318B
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: 00000003.00000000.656174478.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.656174478.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.654836486.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.654836486.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.656667714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.656667714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.916854824.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.916854824.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.655483675.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.655483675.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.918210853.0000000002A51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000002.918210853.0000000002A51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.918210853.0000000002A51000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis