ID: 552911
Sample Name: MSC INVOICE.exe
Cookbook: default.jbs
Time: 22:17:32
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

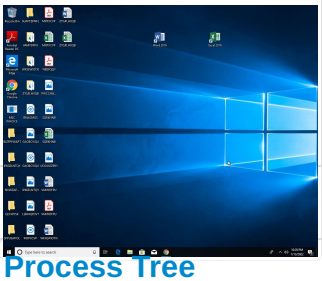
Windows Analysis Report MSC INVOICE.exe

Overview

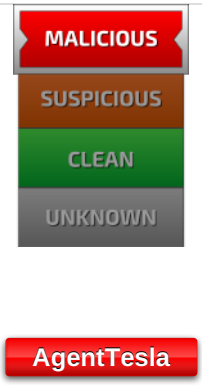
General Information

Sample Name:	MSC INVOICE.exe
Analysis ID:	552911
MD5:	fecd0c876664920..
SHA1:	ea9c3588a0eea1..
SHA256:	94b190ce6f9544e.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

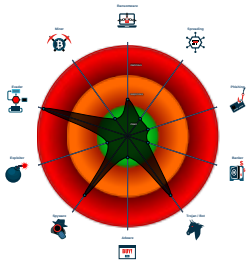


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- MSC INVOICE.exe (PID: 6372 cmdline: "C:\Users\user\Desktop\MSC INVOICE.exe" MD5: FECD0C876664920359CB84EA32BED1C2)
  - MSC INVOICE.exe (PID: 6900 cmdline: C:\Users\user\Desktop\MSC INVOICE.exe MD5: FECD0C876664920359CB84EA32BED1C2)
  - MSC INVOICE.exe (PID: 6884 cmdline: C:\Users\user\Desktop\MSC INVOICE.exe MD5: FECD0C876664920359CB84EA32BED1C2)
  - MSC INVOICE.exe (PID: 6988 cmdline: C:\Users\user\Desktop\MSC INVOICE.exe MD5: FECD0C876664920359CB84EA32BED1C2)
  - MSC INVOICE.exe (PID: 7004 cmdline: C:\Users\user\Desktop\MSC INVOICE.exe MD5: FECD0C876664920359CB84EA32BED1C2)
- xWBWc.exe (PID: 5428 cmdline: "C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe" MD5: FECD0C876664920359CB84EA32BED1C2)
  - xWBWc.exe (PID: 4588 cmdline: C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe MD5: FECD0C876664920359CB84EA32BED1C2)
- xWBWc.exe (PID: 4660 cmdline: "C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe" MD5: FECD0C876664920359CB84EA32BED1C2)
  - xWBWc.exe (PID: 2520 cmdline: C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe MD5: FECD0C876664920359CB84EA32BED1C2)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "mariel.lalu@jeteix.com",
  "Password": "qlRYaFn8",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.481335564.00000000023F1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000013.00000000.476442523.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000013.00000000.476442523.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000002.616612673.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.616612673.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 40 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.xWBWc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.2.xWBWc.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.2.xWBWc.exe.241f82c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
19.0.xWBWc.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.0.xWBWc.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 51 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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

.NET source code contains potential unpacker

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- 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 ftp login credentials
- Tries to harvest and steal browser information (history, passwords, etc)

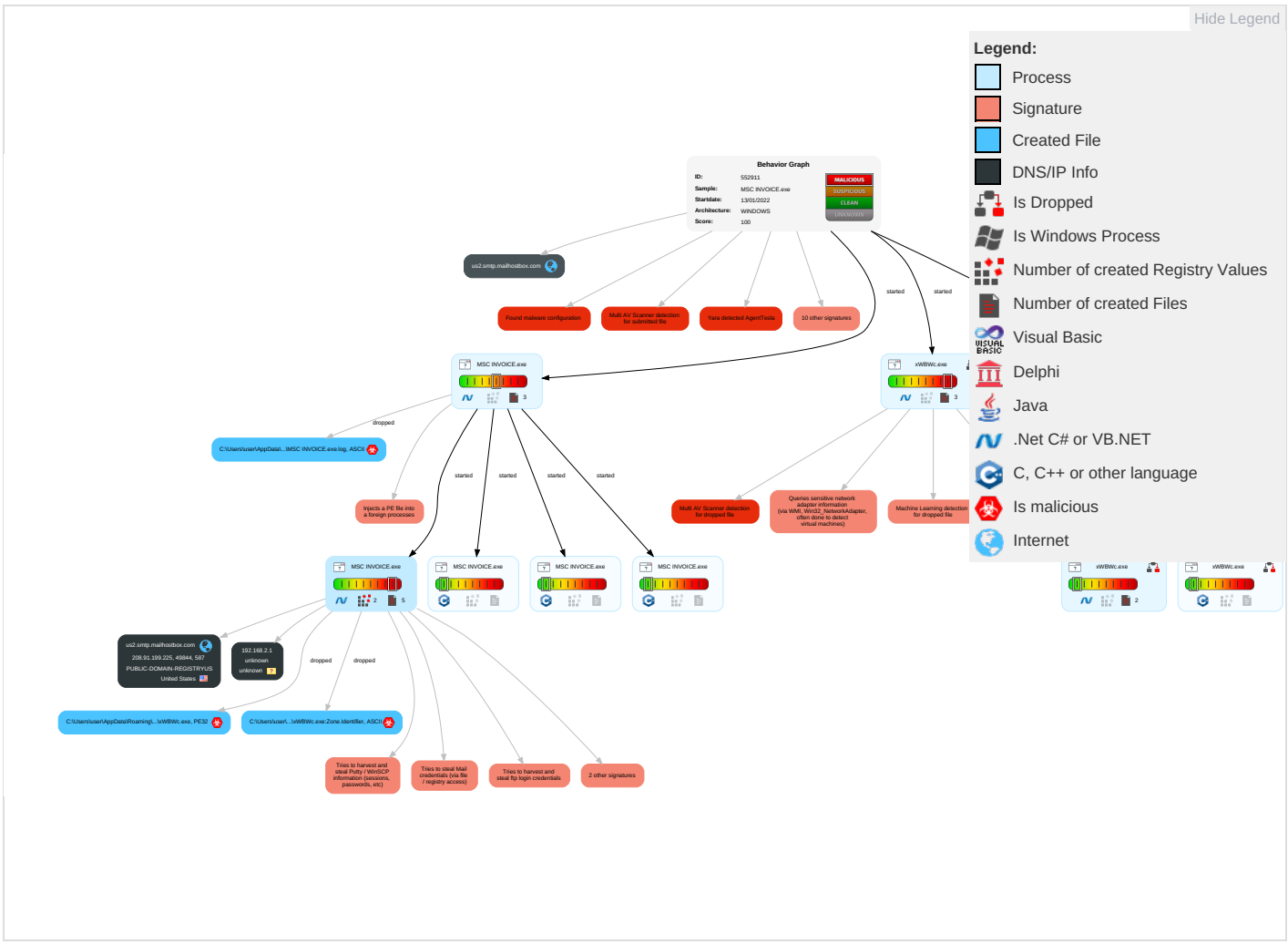
Remote Access Functionality:

- 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
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	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	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

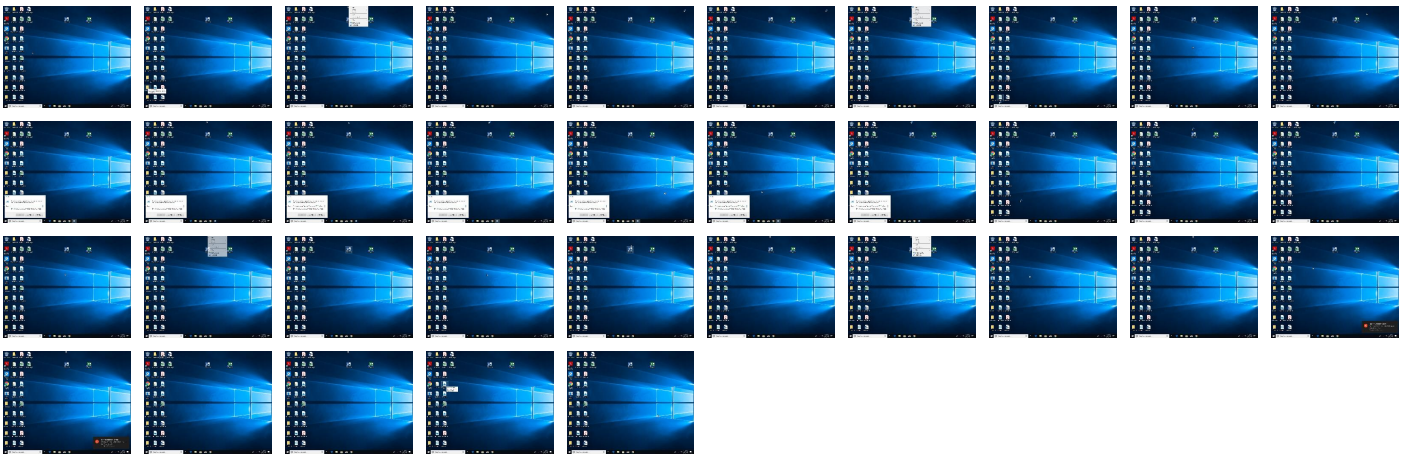
Behavior Graph



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
MSC INVOICE.exe	33%	Virustotal		Browse
MSC INVOICE.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
MSC INVOICE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe	33%	Virustotal		Browse
C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe	46%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.0.xWBWc.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSC INVOICE.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.2.xWBWc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.xWBWc.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSC INVOICE.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
8.2.MSC INVOICE.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSC INVOICE.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.xWBWc.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSC INVOICE.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.xWBWc.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.xWBWc.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.MSC INVOICE.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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.fontbureau.comO	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	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.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	
http://EkYSne.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.225	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552911
Start date:	13.01.2022
Start time:	22:17:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MSC INVOICE.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:	29
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.spyw.evad.winEXE@15/4@2/2
EGA Information:	• Successful, ratio: 60%
HDC Information:	• Successful, ratio: 6.5% (good quality ratio 2.7%) • Quality average: 25% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 97% • 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
22:18:41	API Interceptor	681x Sleep call for process: MSC INVOICE.exe modified
22:19:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run xWBWc C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
22:19:23	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run xWBWc C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
22:19:29	API Interceptor	344x Sleep call for process: xWBWc.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\MSC INVOICE.exe.log	
Process:	C:\Users\user\Desktop\MSC INVOICE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
Reputation:	moderate, 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\f1d8480152e0da9a60ad49c6d16a3b6d\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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xWBWc.exe.log	
Process:	C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xWBWc.exe.log	
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\f1d8480152e0da9a60ad49c6d16a3b6d\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

C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe	
Process:	C:\Users\user\Desktop\MSC INVOICE.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	476672
Entropy (8bit):	7.7772829570710025
Encrypted:	false
SSDEEP:	12288:qK7777777777778Oo2TGcfyZ2lQ7Nbb+miID2qAwmaVQ7d6P:qK777777777777BoDcfyZxZ+miID/Awn
MD5:	FECD0C876664920359CB84EA32BED1C2
SHA1:	EA9C3588A0EEA1D9816A3097617901ABFCCEE2E6
SHA-256:	94B190CE6F9544E1717B7DA29B2B5ACDFA10BC554D88B1FC541CEAF9500A7A28
SHA-512:	86C88827E0FA1B5AE8043141672A746212CD1ACD02A2707CD2DDE47A8C0BC1DDC1925EFB0243D3147E4A4ED90E557514B94F6A38373ED2296228E533A935DF0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 33%, Browse • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....w.a.....0..<.....Z... ...`....@.. ..... ..@.....hZ..O....`..... ....H.....text....:... ...<..... ..`.rsrc.....`.....>.....@..@.rel oc.....D.....@..B.....Z.....H.....D..0/.....5....t..`.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*....0.....(.....(....-#.(.....(....-..(.....(....9....r...p.(.....(....-.~....+..(.....(.....(.....(.....(....-.~....+..(.....(.....(.....(.....(....-.~....+..(.....(.....(....(....+.~.....(.....,.r...p.(.....(.....E..... .../...>...M...\...k...+rr1..p.(.....+iri..p.(...

C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\MSC INVOICE.exe
File Type:	ASCII text, with CRLF line terminators
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:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.7772829570710025
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:	MSC INVOICE.exe
File size:	476672
MD5:	fecd0c876664920359cb84ea32bed1c2
SHA1:	ea9c3588a0eea1d9816a3097617901abfccee2e6

General

SHA256:	94b190ce6f9544e1717b7da29b2b5acdfa10bc554d88b1fc541ceaf9500a7a28
SHA512:	86c88827e0fa1b5ae8043141672a746212cd1acd02a2707cd2dde47a8c0bc1ddc1925efb0243d3147e4a4ed90e557514b94f6a38373ed2296228e533a935df00
SSDEEP:	12288:qK7777777777778Oo2TGcfyZ2lQ7Nbb+miID2qAwmaVQ7d6P:qK777777777777BoDcfyZxZ+miID/Awn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....w.a.....0..<.....Z... ..`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x475aba
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:	0x61E077B2 [Thu Jan 13 19:04:18 2022 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	0x73ac0	0x73c00	False	0.897534759719	data	7.78929926116	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x5dc	0x600	False	0.427083333333	data	4.14224885105	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 22:20:34.913722038 CET	192.168.2.6	8.8.8.8	0xe9ec	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:38.713813066 CET	192.168.2.6	8.8.8.8	0x337c	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 22:20:34.938357115 CET	8.8.8.8	192.168.2.6	0xe9ec	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:34.938357115 CET	8.8.8.8	192.168.2.6	0xe9ec	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:34.938357115 CET	8.8.8.8	192.168.2.6	0xe9ec	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:34.938357115 CET	8.8.8.8	192.168.2.6	0xe9ec	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:38.731316090 CET	8.8.8.8	192.168.2.6	0x337c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:38.731316090 CET	8.8.8.8	192.168.2.6	0x337c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:38.731316090 CET	8.8.8.8	192.168.2.6	0x337c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 13, 2022 22:20:38.731316090 CET	8.8.8.8	192.168.2.6	0x337c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2022 22:20:35.455670118 CET	587	49844	208.91.199.225	192.168.2.6	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 13, 2022 22:20:35.457639933 CET	49844	587	192.168.2.6	208.91.199.225	EHLO 980108
Jan 13, 2022 22:20:35.607841015 CET	587	49844	208.91.199.225	192.168.2.6	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 13, 2022 22:20:35.608146906 CET	49844	587	192.168.2.6	208.91.199.225	STARTTLS
Jan 13, 2022 22:20:35.758307934 CET	587	49844	208.91.199.225	192.168.2.6	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: MSC INVOICE.exe PID: 6372 Parent PID: 5932

General

Start time:	22:18:32
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\MSC INVOICE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\MSC INVOICE.exe"
Imagebase:	0x920000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
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: 00000000.00000002.386022562.0000000002E41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.386566208.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.386566208.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: MSC INVOICE.exe PID: 6900 Parent PID: 6372

General

Start time:	22:18:42
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\MSC INVOICE.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\MSC INVOICE.exe
Imagebase:	0x310000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: MSC INVOICE.exe PID: 6884 Parent PID: 6372

General

Start time:	22:18:43
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\MSC INVOICE.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\MSC INVOICE.exe
Imagebase:	0x3f0000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: MSC INVOICE.exe PID: 6988 Parent PID: 6372

General

Start time:	22:18:44
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\MSC INVOICE.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\MSC INVOICE.exe
Imagebase:	0x3f0000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: MSC INVOICE.exe PID: 7004 Parent PID: 6372

General

Start time:	22:18:45
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\MSC INVOICE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\MSC INVOICE.exe
Imagebase:	0x4a0000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
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: 00000008.00000002.616612673.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.616612673.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.380080063.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.380080063.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.377790173.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.377790173.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.382962108.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.382962108.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.379130922.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.379130922.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.624664599.00000000027E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.624664599.00000000027E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: xWBWc.exe PID: 5428 Parent PID: 3440

General

Start time:	22:19:23
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe"
Imagebase:	0x10000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
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: 0000000E.00000002.481335564.00000000023F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.481487768.000000000243A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.483144084.00000000033F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.483144084.00000000033F9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 33%, Virustotal, Browse • Detection: 46%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: xWBWc.exe PID: 4588 Parent PID: 5428

General

Start time:	22:19:30
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
Imagebase:	0xc30000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
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: 00000013.00000000.476442523.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.476442523.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000000.475465445.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.475465445.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.616556442.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.616556442.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000000.477003369.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.477003369.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000000.474471833.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.474471833.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.623944283.00000000030A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.623944283.00000000030A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: xWBWc.exe PID: 4660 Parent PID: 3440

General

Start time:	22:19:31
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe"
Imagebase:	0x310000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
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: 00000014.00000002.488588582.0000000002651000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.488637453.0000000002698000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.488979150.0000000003659000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.488979150.0000000003659000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: xWBWc.exe PID: 2520 Parent PID: 4660

General

Start time:	22:19:37
Start date:	13/01/2022
Path:	C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\xWBWc\xWBWc.exe
Imagebase:	0xe60000
File size:	476672 bytes
MD5 hash:	FECD0C876664920359CB84EA32BED1C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis