ID: 385394
Sample Name: xVvAobZvWU
Cookbook: default.jbs
Time: 12:44:14
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

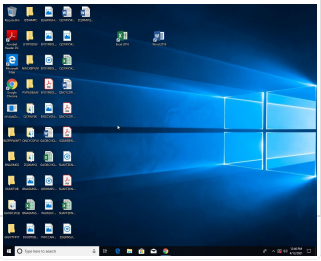
Analysis Report xVvAobZvWU

Overview

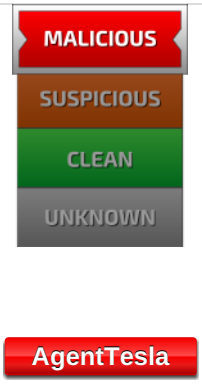
General Information

Sample Name:	xVvAobZvWU (renamed file extension from none to exe)
Analysis ID:	385394
MD5:	b415645d1b8039..
SHA1:	cfcc4ee2d2e00ae..
SHA256:	806bf1c6fa71332..
Infos:	

Most interesting Screenshot:



Detection



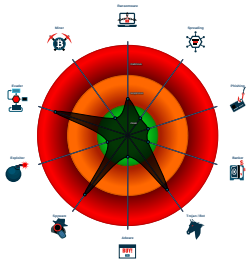
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…

Classification



Startup

- **System is w10x64**
- xVvAobZvWU.exe (PID: 5504 cmdline: 'C:\Users\user\Desktop\xVvAobZvWU.exe' MD5: B415645D1B8039996726B424CD53A81C)
  - xVvAobZvWU.exe (PID: 2584 cmdline: {path} MD5: B415645D1B8039996726B424CD53A81C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "jaen@brimaq.combrimaQ2012mail.brimaq.commetoyou2411@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.460161679.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.200144937.000000000389000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: xVvAobZvWU.exe PID: 2584	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 3 entries

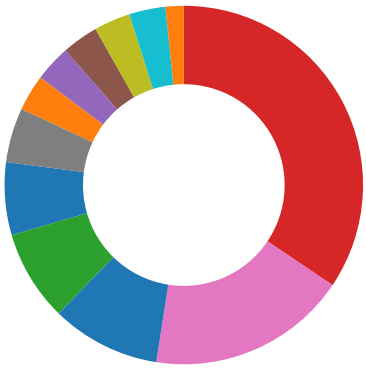
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.xVvAobZvWU.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.xVvAobZvWU.exe.39b33b0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.xVvAobZvWU.exe.39b33b0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

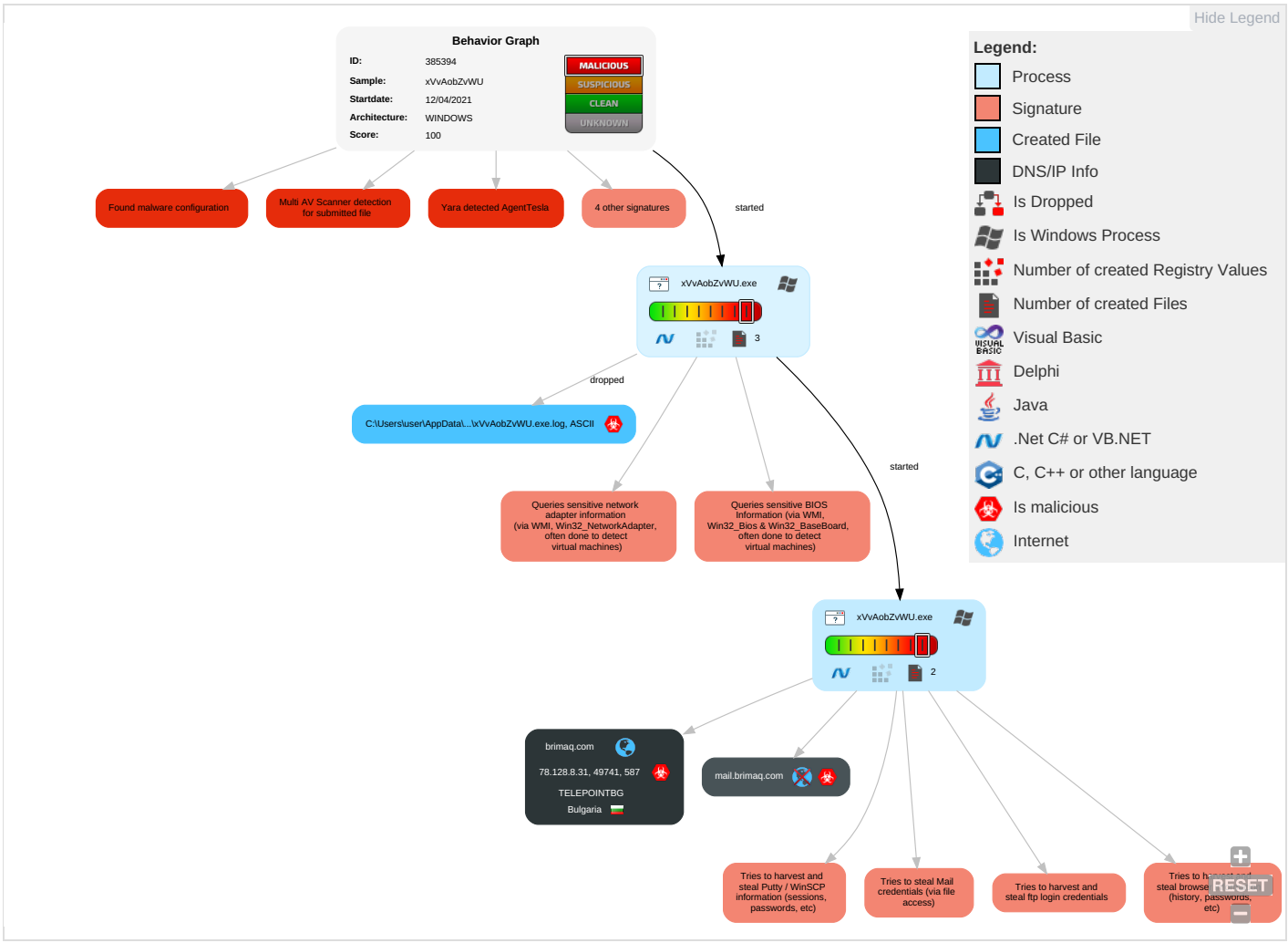
Remote Access Functionality:

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	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 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	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 4	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	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

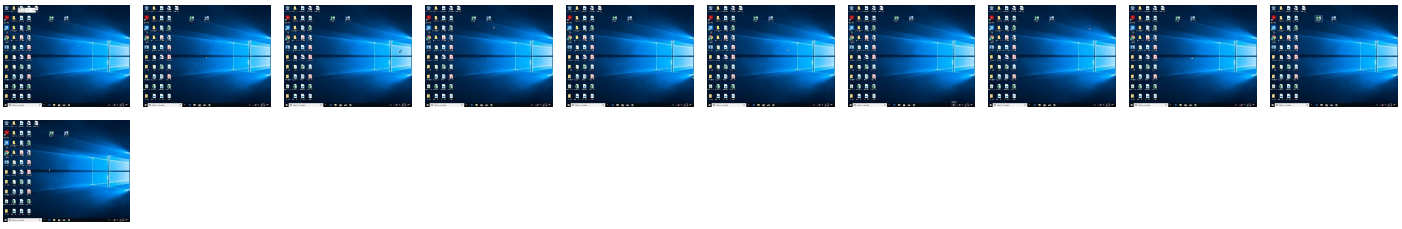
Behavior Graph



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
xVvAobZvWU.exe	30%	Virustotal		Browse
xVvAobZvWU.exe	10%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
xVvAobZvWU.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.xVvAobZvWU.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
brimaq.com	0%	Virustotal		Browse
mail.brimaq.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://UfeDnz.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://Bavw5lBQkDhG9.net1-5-21-3853321935-2125563209-4053062332-1002_Classes	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://Bavw5lBQkDhG9.net	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	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://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://brimaq.com	0%	Avira URL Cloud	safe	
http://mail.brimaq.com	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	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://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

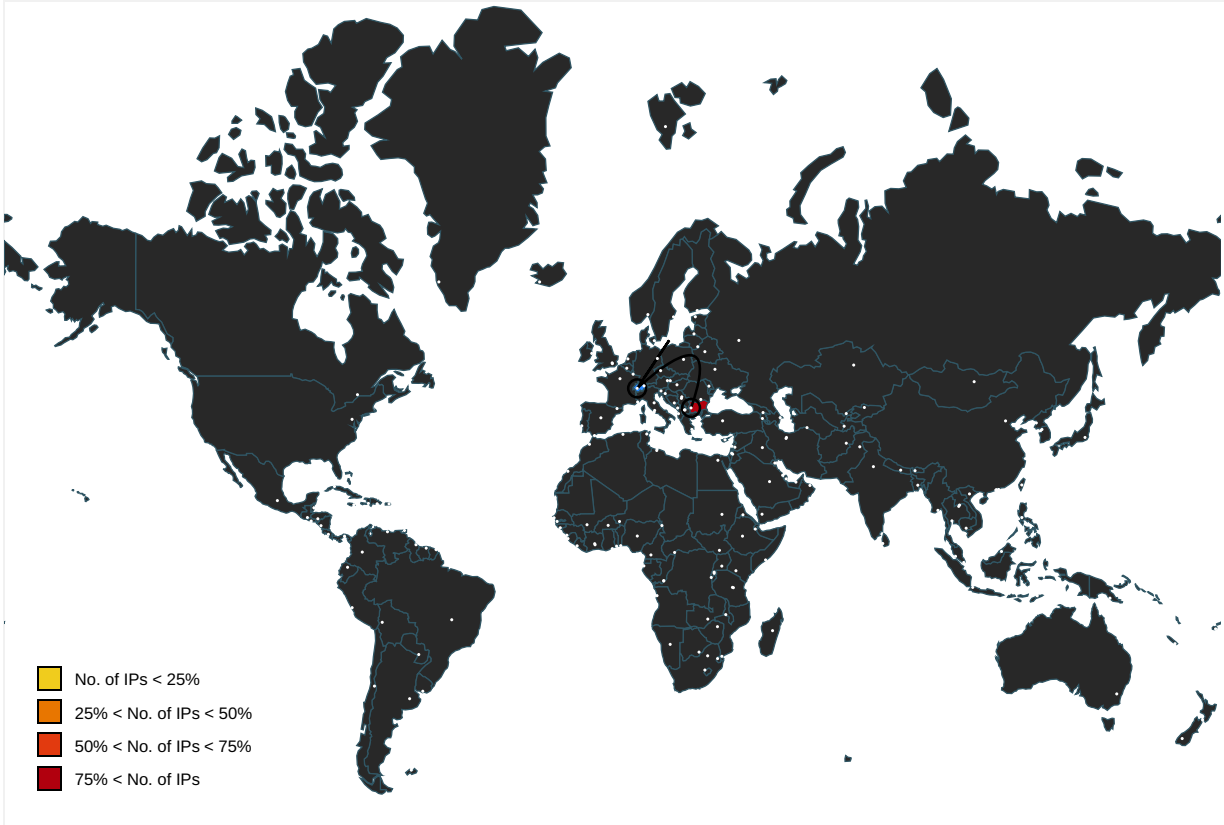
Name	IP	Active	Malicious	Antivirus Detection	Reputation
brimaq.com	78.128.8.31	true	true	• 0%, Virustotal, Browse	unknown
mail.brimaq.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://UfeDnz.com	xVvAobZvWU.exe, 00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	xVvAobZvWU.exe, 00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://Bavw5lBQkDhG9.net1-5-21-3853321935-2125563209-4053062332-1002_Classes	xVvAobZvWU.exe, 00000002.00000003.401682628.0000000001094000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	xVvAobZvWU.exe, 00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Bavw5lBQkDhG9.net	xVvAobZvWU.exe, 00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	xVvAobZvWU.exe, 00000002.00000003.413844373.00000000012C7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	xVvAobZvWU.exe, 00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://brimaq.com	xVvAobZvWU.exe, 00000002.00000002.466430906.0000000003101000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.brimaq.com	xVvAobZvWU.exe, 00000002.00000002.466430906.0000000003101000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	xVvAobZvWU.exe, 00000002.00000003.413844373.00000000012C7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	xVvAobZvWU.exe, 00000000.00000002.200144937.0000000003809000.00000004.00000001.sdmp, xVvAobZvWU.exe, 00000002.00000002.460161679.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	xVvAobZvWU.exe, 00000002.00000003.413844373.00000000012C7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	xVvAobZvWU.exe, 00000002.00000003.413844373.00000000012C7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.128.8.31	brimaq.com	Bulgaria		31083	TELEPOINTBG	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385394
Start date:	12.04.2021

Start time:	12:44:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xVvAobZvWU (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:	25
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@3/1@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 45% • Quality standard deviation: 39.5%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 13.64.90.137, 104.43.139.144, 52.147.198.201, 20.82.210.154, 52.255.188.83, 92.122.144.200, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): www.bing.com, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:44:57	API Interceptor	838x Sleep call for process: xVvAobZvWU.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
78.128.8.31	FAKTURA I RACHUNKI.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEPOINTBG	FAKTURA I RACHUNKI.exe	Get hash	malicious	Browse	• 78.128.8.31
	0AX4532QWSA.xlsx	Get hash	malicious	Browse	• 217.174.152.38
	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 217.174.149.3
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 79.124.76.20
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 79.124.76.20
	document-1932597637.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1932597637.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1961450761.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909441643.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1961450761.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909441643.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1942925331.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1942925331.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1892683183.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1892683183.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909894964.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909894964.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1965918496.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1965918496.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1901557343.xls	Get hash	malicious	Browse	• 217.174.152.52

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\xVvAobZvWU.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xVvAobZvWU.exe.log	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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\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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.881411013396599
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:	xVvAobZvWU.exe
File size:	678400
MD5:	b415645d1b8039996726b424cd53a81c
SHA1:	cfcc4ee2d2e00ae4deb8591e7b8682d6946db5f5
SHA256:	806bf1c6fa713325b45642893ede4dcb76dbf6044aea80a5315da1075cc25b9a
SHA512:	a3d6f1444a13842e56e7aada5fcaf323058718fc564b9699956316afc1563f2b426e13b7f556fd4cd6de1ac6eef98e7fdebd05bdaecf986291bde742cb939c37
SSDEEP:	12288:j0yZ00LCYKcGRcbLtD7TJrQrfVpo67st01Q5WMMe1zr6FEg848vDEpW:JZpCYKcGabvWXuoMMedr6F1zU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....,q.....0..P.....n.. .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a6ed2
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:	0x94712C9A [Tue Dec 1 14:15:54 2048 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General	
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa6e80	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x5f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa6e64	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa4ed8	0xa5000	False	0.90078272964	data	7.8881862753	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x5f8	0x600	False	0.438802083333	data	4.24177120131	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa8090	0x366	data		
RT_MANIFEST	0xa8408	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

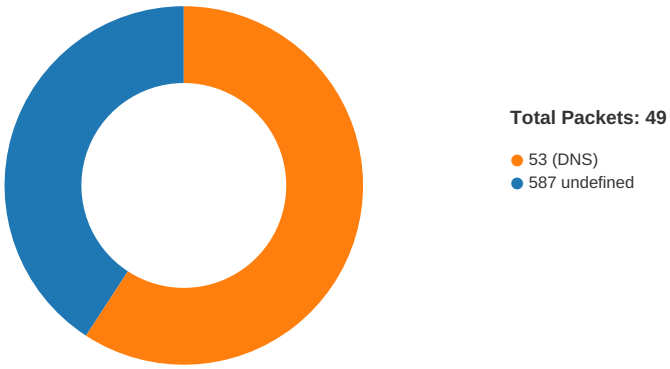
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Integra Wealth
Assembly Version	1.8.9.10
InternalName	2i.exe
FileVersion	1.9.1.0
CompanyName	Integra Wealth
LegalTrademarks	
Comments	
ProductName	ReplacementFallback
ProductVersion	1.9.1.0
FileDescription	ReplacementFallback
OriginalFilename	2i.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:46:38.869477987 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:38.946281910 CEST	587	49741	78.128.8.31	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:46:38.946373940 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.163911104 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.164525986 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.243127108 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.243381023 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.323828936 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.378572941 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.385159016 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.473922014 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.473978996 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.474025965 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.474138021 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.485213995 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.564122915 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.613044977 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.850397110 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:39.928841114 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:39.932363033 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.011511087 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.016185045 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.115988970 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.117352962 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.194215059 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.194924116 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.311352968 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.351804972 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.352585077 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.429482937 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.435127974 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.435487032 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.435702085 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.435915947 CEST	49741	587	192.168.2.3	78.128.8.31
Apr 12, 2021 12:46:40.512160063 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.512242079 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.512346983 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.512382984 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.543119907 CEST	587	49741	78.128.8.31	192.168.2.3
Apr 12, 2021 12:46:40.597439051 CEST	49741	587	192.168.2.3	78.128.8.31

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:44:50.612360954 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:44:50.669533014 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 12:44:51.245843887 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:44:51.297452927 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 12:44:52.431533098 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:44:52.481501102 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 12:44:53.900589943 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:44:53.949954987 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 12:44:57.193084955 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:44:57.241938114 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 12:44:58.087940931 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:44:58.141357899 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 12:44:59.118503094 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:44:59.175698042 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:00.035691023 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:00.086199045 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:01.092727900 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:01.141478062 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:01.867960930 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:01.916639090 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:03.007688046 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:03.059261084 CEST	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 12:45:03.925549984 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:03.974323988 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:06.181027889 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:06.234987974 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:07.642683983 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:07.691351891 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:24.676044941 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:24.728600979 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:26.453423977 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:26.505266905 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:27.536922932 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:27.585517883 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:31.249435902 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:31.322732925 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:36.898156881 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:36.956593990 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:45.408162117 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:45.474838018 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:47.998008013 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:48.047997952 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:52.693586111 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:52.742301941 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:56.675220966 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:56.726906061 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 12:45:59.935096025 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:45:59.986671925 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 12:46:02.939059019 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:46:03.000535965 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 12:46:34.890126944 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:46:34.941271067 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 12:46:37.076522112 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:46:37.137068987 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 12:46:38.585671902 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:46:38.683134079 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 12:46:38.718928099 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 12:46:38.780081034 CEST	53	56579	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 12:46:38.585671902 CEST	192.168.2.3	8.8.8.8	0xd703	Standard query (0)	mail.brimaq.com	A (IP address)	IN (0x0001)
Apr 12, 2021 12:46:38.718928099 CEST	192.168.2.3	8.8.8.8	0xae83	Standard query (0)	mail.brimaq.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 12:46:38.683134079 CEST	8.8.8.8	192.168.2.3	0xd703	No error (0)	mail.brimaq.com	brimaq.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 12:46:38.683134079 CEST	8.8.8.8	192.168.2.3	0xd703	No error (0)	brimaq.com		78.128.8.31	A (IP address)	IN (0x0001)
Apr 12, 2021 12:46:38.780081034 CEST	8.8.8.8	192.168.2.3	0xae83	No error (0)	mail.brimaq.com	brimaq.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 12:46:38.780081034 CEST	8.8.8.8	192.168.2.3	0xae83	No error (0)	brimaq.com		78.128.8.31	A (IP address)	IN (0x0001)

SMTP Packets

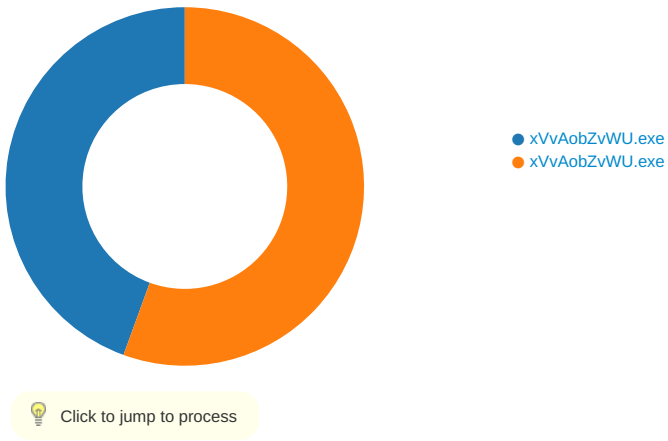
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 12:46:39.163911104 CEST	587	49741	78.128.8.31	192.168.2.3	220-srvr.laprimeracloud08.com ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 12:46:39 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 12:46:39.164525986 CEST	49741	587	192.168.2.3	78.128.8.31	EHLO 818225
Apr 12, 2021 12:46:39.243127108 CEST	587	49741	78.128.8.31	192.168.2.3	250-srvr.laprimeracloud08.com Hello 818225 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 12:46:39.243381023 CEST	49741	587	192.168.2.3	78.128.8.31	STARTTLS
Apr 12, 2021 12:46:39.323828936 CEST	587	49741	78.128.8.31	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: xVvAobZvWU.exe PID: 5504 Parent PID: 5772

General

Start time:	12:44:56
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\xVvAobZvWU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\xVvAobZvWU.exe'
Imagebase:	0x3a0000
File size:	678400 bytes
MD5 hash:	B415645D1B8039996726B424CD53A81C
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: 00000000.00000002.200144937.0000000003809000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF0CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xVvAobZvWU.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E21C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xVvAobZvWU.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E21C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile

Analysis Process: xVvAobZvWU.exe PID: 2584 Parent PID: 5504

General

Start time:	12:44:59
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\xVvAobZvWU.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa50000
File size:	678400 bytes
MD5 hash:	B415645D1B8039996726B424CD53A81C
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: 00000002.00000002.460161679.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.464571382.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF0CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF0CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\48e3e404-5b02-47f0-9a95-ff982dff7eb9	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CD51B4F	ReadFile

Disassembly

Code Analysis