ID: 338152
Sample Name: BL FOR SHIPMENT_doc.gz.exe
Cookbook: default.jbs
Time: 18:12:09
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

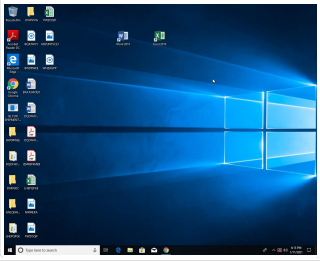
Analysis Report BL FOR SHIPMENT_doc.gz.exe

Overview

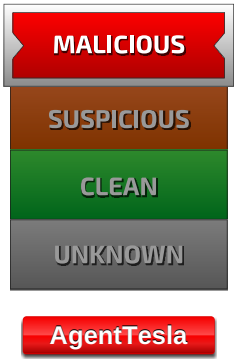
General Information

Sample Name:	BL FOR SHIPMENT_doc.gz.exe
Analysis ID:	338152
MD5:	04e43f3aee65c1d.
SHA1:	1bce09b3a5c827..
SHA256:	9fecb65659cb47a..
Tags:	exe

Most interesting Screenshot:



Detection

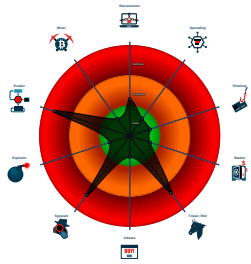


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- 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…

Classification



Startup

- **System is w10x64**
- BL FOR SHIPMENT_doc.gz.exe (PID: 6440 cmdline: 'C:\Users\user\Desktop\BL FOR SHIPMENT_doc.gz.exe' MD5: 04E43F3AEE65C1D03B8C7ADFA6D9FCE9)
  - BL FOR SHIPMENT_doc.gz.exe (PID: 3976 cmdline: {path} MD5: 04E43F3AEE65C1D03B8C7ADFA6D9FCE9)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "kyqjbOqsGP2YKsV",
  "URL: ": "https://M2zxRmp3kpObpEIzJWTy.com",
  "To: ": "sydney@dicon.md",
  "ByHost: ": "mail.dicon.md:587",
  "Password: ": "Hoq8zXmvKJ",
  "From: ": "sydney@dicon.md"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.665888158.00000000045C4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.1009653360.0000000002E81000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.1009653360.0000000002E81000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.1008577891.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: BL FOR SHIPMENT_doc.gz.exe PID: 6440	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 3 entries				

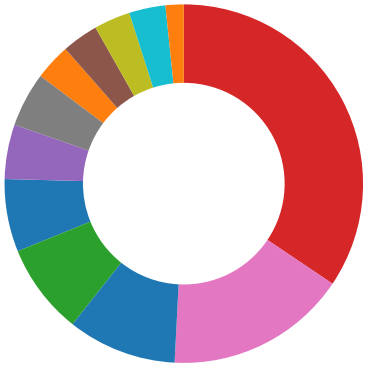
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.BL FOR SHIPMENT_doc.gz.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

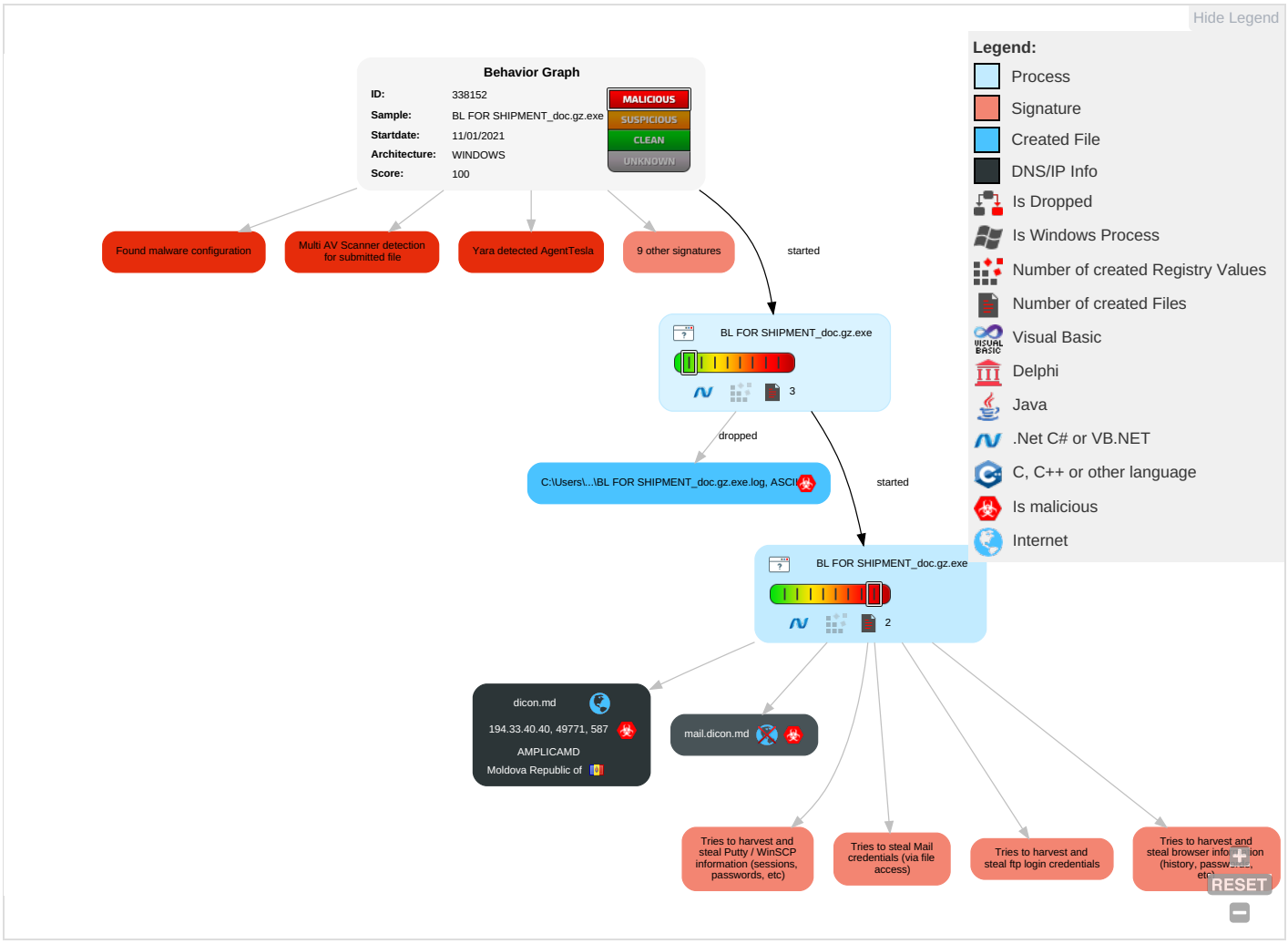
Remote Access Functionality:

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	Virtualization/Sandbox Evasion 1 3	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)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3	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	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 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 2	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 1 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

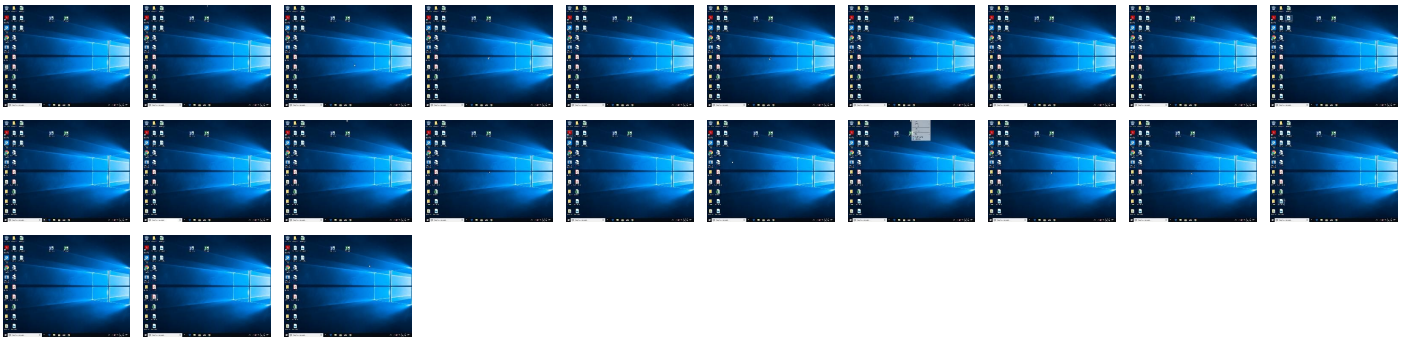
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
BL FOR SHIPMENT_doc.gz.exe	28%	Virustotal		Browse
BL FOR SHIPMENT_doc.gz.exe	17%	ReversingLabs	Win32.Trojan.Pwsx	
BL FOR SHIPMENT_doc.gz.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.BL FOR SHIPMENT_doc.gz.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
dicon.md	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://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://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://dicon.md	0%	Virustotal		Browse
http://dicon.md	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://M2zxRmp3kpObpElzJWTy.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://fwuwEZ.com	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/05	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://mail.dicon.md	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dicon.md	194.33.40.40	true	true	• 0%, Virustotal, Browse	unknown
mail.dicon.md	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://M2zxRmp3kpObpEIzJWTy.com	true	• Avira URL Cloud: safe	unknown

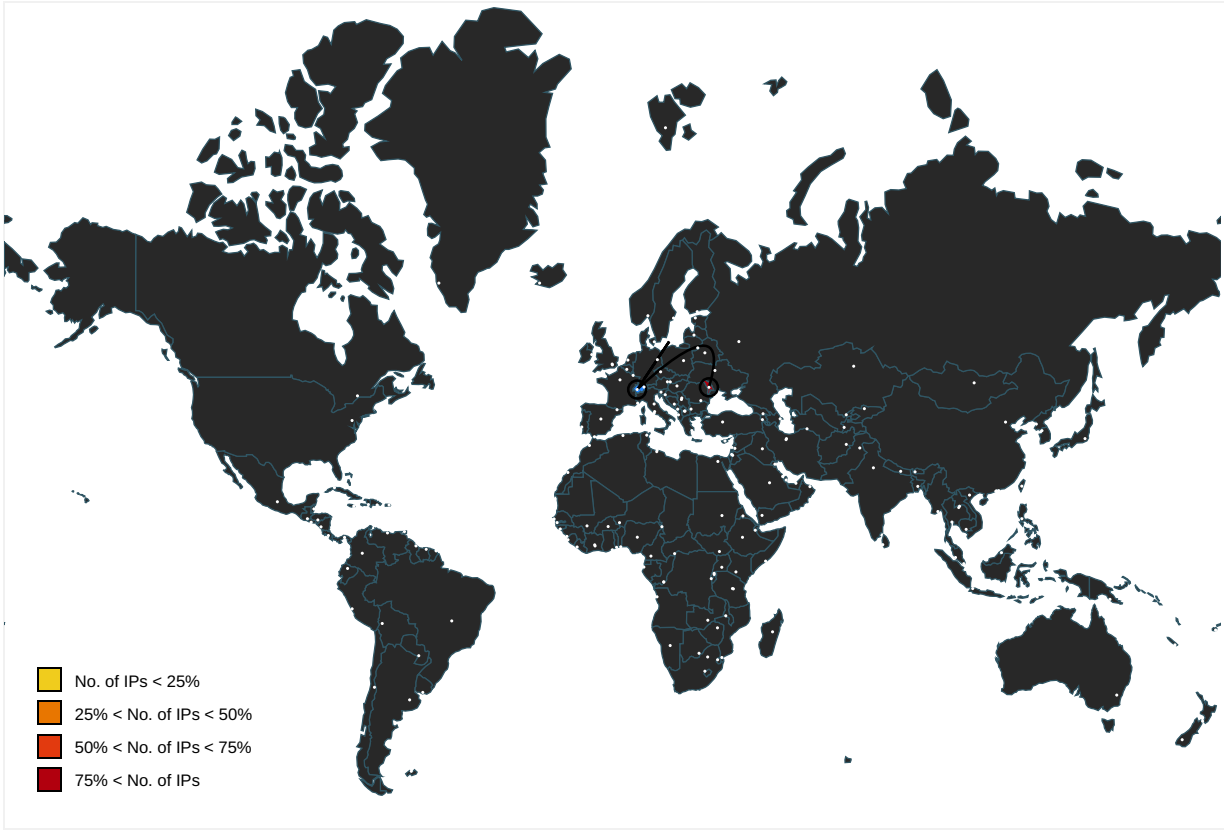
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1009653360.0000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1009653360.0000002E81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1010094051.00000000031DD000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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%tordir%%ha	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1009653360.00000002E81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.tiro.com	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://dicon.md	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1010094051.00000000031DD000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fwuwEZ.com	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1009653360.0000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.i.lencr.org/05	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1010094051.00000000031DD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://r3.o.lencr.org0	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1010094051.00000031DD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.dicon.md	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1010094051.00000031DD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.fonts.com	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.667695107.000006160000.00000002.00000001.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	BL FOR SHIPMENT_doc.gz.exe, 00000000.00000002.665888158.00000000045C4000.00000004.00000001.sdmp, BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1008577891.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	BL FOR SHIPMENT_doc.gz.exe, 00000001.00000002.1010094051.00000031DD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.33.40.40	unknown	Moldova Republic of		206698	AMPLICAMD	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338152
Start date:	11.01.2021
Start time:	18:12:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BL FOR SHIPMENT_doc.gz.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:	17
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:	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 • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.255.188.83, 51.104.139.180, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 8.248.133.254, 8.248.149.254, 67.26.137.254, 8.248.131.254, 67.27.233.254, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.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
18:13:00	API Interceptor	1100x Sleep call for process: BL FOR SHIPMENT_doc.gz.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMPLICAMD	15#U043e #U0437#U0430#U043a#U0430#U0437#U0435.js	Get hash	malicious	Browse	• 185.165.242.5

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BL FOR SHIPMENT_doc.gz.exe.log	
Process:	C:\Users\user\Desktop\BL FOR SHIPMENT_doc.gz.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	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):	7.672462819594914
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	BL FOR SHIPMENT_doc.gz.exe
File size:	868352
MD5:	04e43f3aee65c1d03b8c7adfa6d9fce9
SHA1:	1bce09b3a5c827d412feea47a86619fa9a7ac94f
SHA256:	9fecb65659cb47a10afab901b14904f54384f5481e0ef0331e009bfc580cfe29
SHA512:	0150f88de48b441f8280a57afa2da62db8d96030aa7d76216ea27a2ebec2077aba2bd6944940fb2241f26e8f45d996d7d49760a205e12f9797aaff2549d6dcd9
SSDEEP:	12288:8+YIt10emnVKrlQksJo6DIDn5WT54ETEE5VJAoWEaDr/HZiB41ab5qMp9meTH:NYq1bmn4rjsywT3YE5VJAxvD08op9/T
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p._.....4.....^R... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d525e
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:	0x5FFC7099 [Mon Jan 11 15:36:57 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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	0xd5208	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x800	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0xd3264	0xd3400	False	0.813755085059	data	7.68132853589	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x800	0x800	False	0.3330078125	data	3.49311095127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	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	0xd6090	0x388	data		
RT_MANIFEST	0xd6428	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

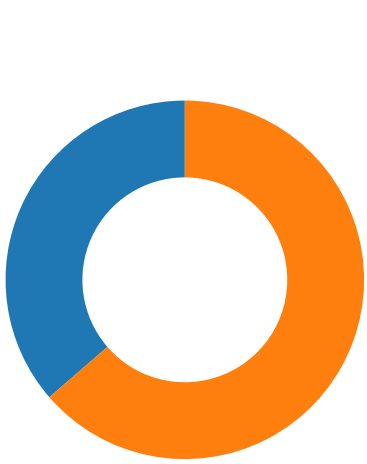
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2011 - 2020
Assembly Version	2.159.0.0
InternalName	n.exe
FileVersion	2.159.0.0
CompanyName	Overwolf Ltd.
LegalTrademarks	
Comments	Overwolf Launcher
ProductName	OverwolfLauncher
ProductVersion	2.159.0.0
FileDescription	OverwolfLauncher
OriginalFilename	n.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:14:42.559436083 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:42.637659073 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:42.637816906 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:42.861222029 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:42.861852884 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:42.945286036 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:42.945712090 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.030203104 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.074209929 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.118367910 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.236181974 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.239213943 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.239265919 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.239305019 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.239357948 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.248747110 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.327022076 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.327749014 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.371118069 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.613140106 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.693869114 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.695502043 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.774070024 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.775563002 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.869687080 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.871118069 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:43.949812889 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:43.950710058 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:44.029705048 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:44.030528069 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:44.108799934 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:44.111227036 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:44.111510038 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:44.112556934 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:44.112760067 CET	49771	587	192.168.2.4	194.33.40.40
Jan 11, 2021 18:14:44.189486027 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:44.189588070 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:44.190604925 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:44.190726995 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:44.427582026 CET	587	49771	194.33.40.40	192.168.2.4
Jan 11, 2021 18:14:44.468312979 CET	49771	587	192.168.2.4	194.33.40.40

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:12:49.464170933 CET	64549	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:49.512180090 CET	53	64549	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:50.583703995 CET	63153	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:50.631527901 CET	53	63153	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:52.270781040 CET	52991	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:52.318659067 CET	53	52991	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:53.491065979 CET	53700	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:53.540293932 CET	53	53700	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:54.771020889 CET	51726	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:54.819034100 CET	53	51726	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:55.708014965 CET	56794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:55.755938053 CET	53	56794	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:56.842890978 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:56.902055025 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:58.026612997 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:58.077466011 CET	53	56627	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:58.837728977 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:58.888622046 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 18:12:59.635940075 CET	63116	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:12:59.683841944 CET	53	63116	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:00.618387938 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:00.669015884 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:01.396958113 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:01.444984913 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:02.156285048 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:02.204107046 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:02.917515039 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:02.968255043 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:14.248281002 CET	61522	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:14.299212933 CET	53	61522	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:17.927120924 CET	52337	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:17.985075951 CET	53	52337	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:31.205475092 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:31.309273958 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:31.873848915 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:31.985476017 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:32.586378098 CET	49285	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:32.642829895 CET	53	49285	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:33.081886053 CET	50601	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:33.140909910 CET	53	50601	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:33.206767082 CET	60875	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:33.265825033 CET	53	60875	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:33.604794025 CET	56448	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:33.661056995 CET	53	56448	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:34.221616030 CET	59172	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:34.280769110 CET	53	59172	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:34.867137909 CET	62420	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:34.926578045 CET	53	62420	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:35.735361099 CET	60579	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:35.794492006 CET	53	60579	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:36.685787916 CET	50183	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:36.733956099 CET	53	50183	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:37.153882027 CET	61531	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:37.213567972 CET	53	61531	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:39.725151062 CET	49228	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:39.776146889 CET	53	49228	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:49.024144888 CET	59794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:49.072282076 CET	53	59794	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:49.217411041 CET	55916	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:49.289505005 CET	53	55916	8.8.8.8	192.168.2.4
Jan 11, 2021 18:13:51.394382000 CET	52752	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:13:51.454652071 CET	53	52752	8.8.8.8	192.168.2.4
Jan 11, 2021 18:14:24.312299013 CET	60542	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:14:24.363344908 CET	53	60542	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:14:26.142430067 CET	60689	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:14:26.208874941 CET	53	60689	8.8.8.8	192.168.2.4
Jan 11, 2021 18:14:42.143096924 CET	64206	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:14:42.242369890 CET	53	64206	8.8.8.8	192.168.2.4
Jan 11, 2021 18:14:42.278589010 CET	50904	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:14:42.466648102 CET	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 18:14:42.143096924 CET	192.168.2.4	8.8.8.8	0x1c8e	Standard query (0)	mail.dicon.md	A (IP address)	IN (0x0001)
Jan 11, 2021 18:14:42.278589010 CET	192.168.2.4	8.8.8.8	0x83e6	Standard query (0)	mail.dicon.md	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:14:42.242369890 CET	8.8.8.8	192.168.2.4	0x1c8e	No error (0)	mail.dicon.md	dicon.md		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:14:42.242369890 CET	8.8.8.8	192.168.2.4	0x1c8e	No error (0)	dicon.md		194.33.40.40	A (IP address)	IN (0x0001)
Jan 11, 2021 18:14:42.466648102 CET	8.8.8.8	192.168.2.4	0x83e6	No error (0)	mail.dicon.md	dicon.md		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 18:14:42.466648102 CET	8.8.8.8	192.168.2.4	0x83e6	No error (0)	dicon.md		194.33.40.40	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 11, 2021 18:14:42.861222029 CET	587	49771	194.33.40.40	192.168.2.4	220-web2.amplica.net ESMTP Exim 4.93 #2 Mon, 11 Jan 2021 19:14:42 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 11, 2021 18:14:42.861852884 CET	49771	587	192.168.2.4	194.33.40.40	EHLO 830021
Jan 11, 2021 18:14:42.945286036 CET	587	49771	194.33.40.40	192.168.2.4	250-web2.amplica.net Hello 830021 [84.17.52.74] 250-SIZE 83886080 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 11, 2021 18:14:42.945712090 CET	49771	587	192.168.2.4	194.33.40.40	STARTTLS
Jan 11, 2021 18:14:43.030203104 CET	587	49771	194.33.40.40	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior

● BL FOR SHIPMENT_doc.gz.exe
● BL FOR SHIPMENT_doc.gz.exe

Click to jump to process

System Behavior

Analysis Process: BL FOR SHIPMENT_doc.gz.exe PID: 6440 Parent PID: 5904

General

Start time:	18:12:54
Start date:	11/01/2021
Path:	C:\Users\user\Desktop\BL FOR SHIPMENT_doc.gz.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BL FOR SHIPMENT_doc.gz.exe'
Imagebase:	0xce0000
File size:	868352 bytes
MD5 hash:	04E43F3AEE65C1D03B8C7ADFA6D9FCE9
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: 00000000.00000002.665888158.00000000045C4000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BL FOR SHIPMENT_doc.gz.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	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\BL FOR SHIPMENT_doc.gz.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	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: BL FOR SHIPMENT_doc.gz.exe PID: 3976 Parent PID: 6440

General

Start time:	18:13:03
Start date:	11/01/2021
Path:	C:\Users\user\Desktop\BL FOR SHIPMENT_doc.gz.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb40000
File size:	868352 bytes
MD5 hash:	04E43F3AEE65C1D03B8C7ADFA6D9FCE9
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: 00000001.00000002.1009653360.0000000002E81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.1009653360.0000000002E81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.1008577891.0000000000402000.00000040.00000001.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	6D1CCF06	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	6D1CCF06	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\324146fd-dc8f-4c05-93a8-e37158c61d65	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C011B4F	ReadFile

Disassembly

Code Analysis