ID: 412499
Sample Name: tLes2JdtRw.exe
Cookbook: default.jbs
Time: 18:30:34
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

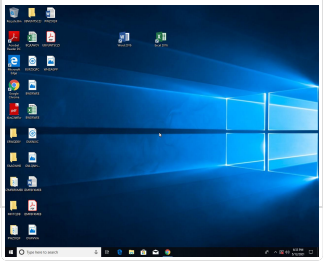
Analysis Report tLes2JdtRw.exe

Overview

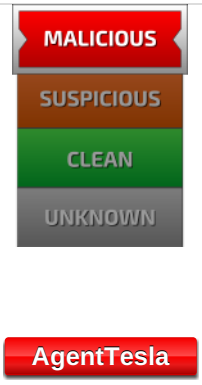
General Information

Sample Name:	tLes2JdtRw.exe
Analysis ID:	412499
MD5:	2edb5a087966f25.
SHA1:	ba38e69ebe87da..
SHA256:	1b80ed1165b46b..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



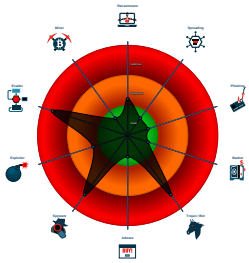
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- tLes2JdtRw.exe (PID: 6888 cmdline: 'C:\Users\user\Desktop\tLes2JdtRw.exe' MD5: 2EDB5A087966F25F972506500A48C9F3)
  - tLes2JdtRw.exe (PID: 7072 cmdline: C:\Users\user\Desktop\tLes2JdtRw.exe MD5: 2EDB5A087966F25F972506500A48C9F3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sergio.arroyo@kaeiser.comQIErWCn3smtp.kaeiser.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.906500988.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.906500988.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.908393469.000000000311000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.656178946.0000000002C25000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.657948952.0000000003BE9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 5 entries

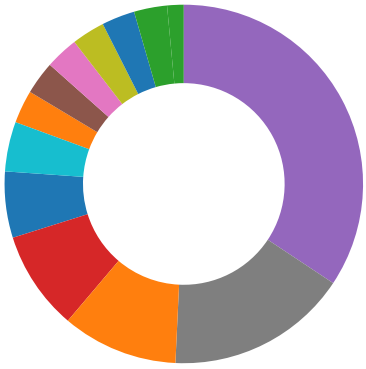
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.tLes2JdtRw.exe.3c9b718.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.tLes2JdtRw.exe.3c9b718.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.tLes2JdtRw.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.tLes2JdtRw.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.tLes2JdtRw.exe.3c9b718.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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:

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

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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:

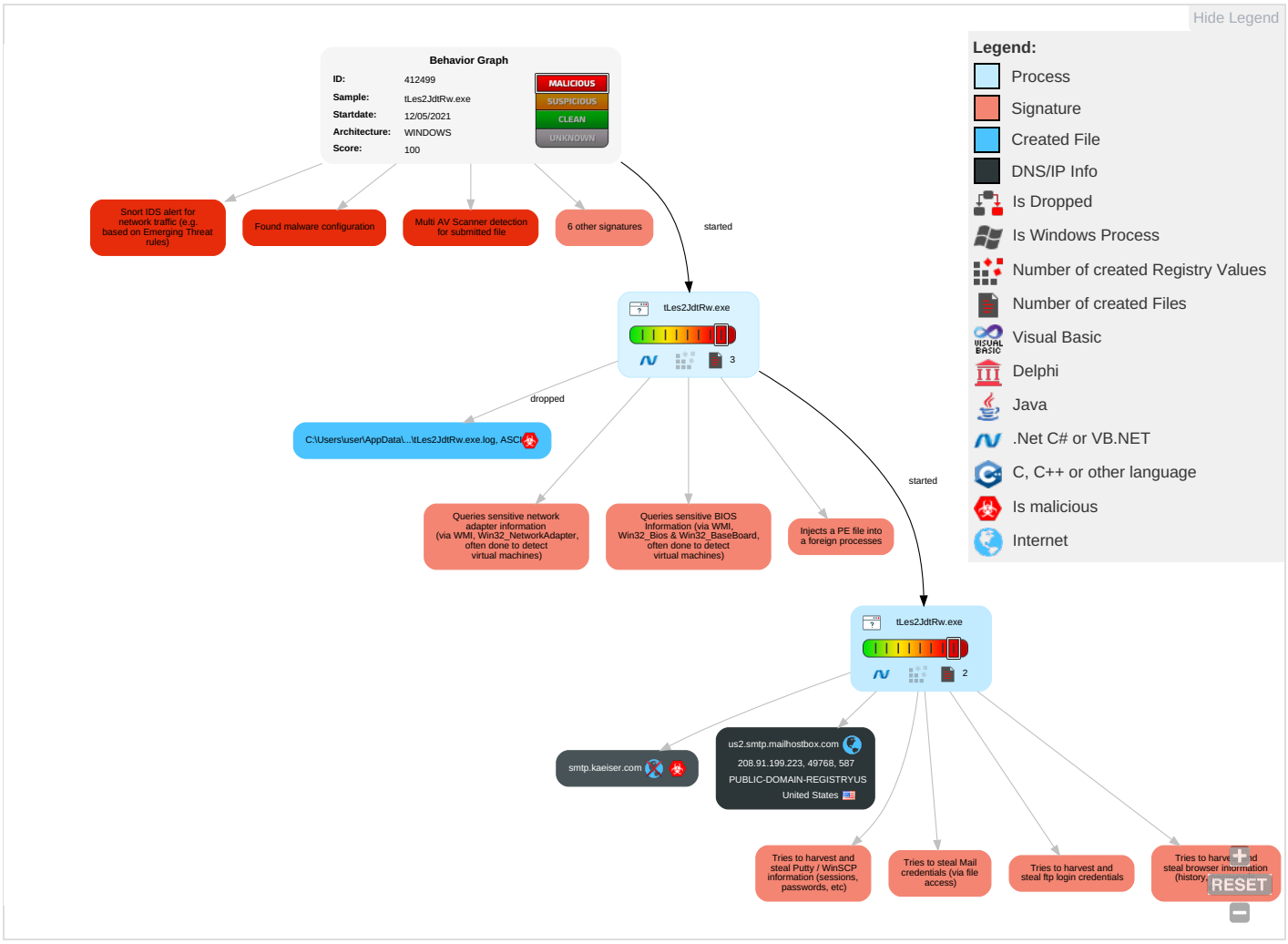
Yara detected AgentTesla

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 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	Command and Scripting Interpreter 2	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 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 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
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

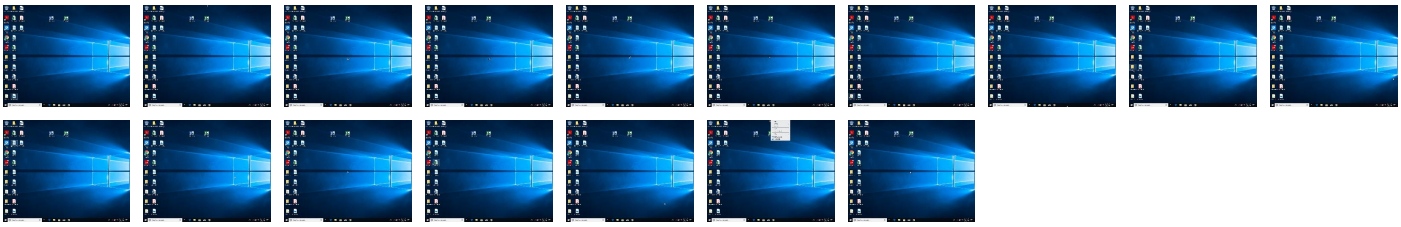
Behavior Graph



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
tLes2JdtRw.exe	26%	Virustotal		Browse
tLes2JdtRw.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	
tLes2JdtRw.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.tLes2JdtRw.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://vn95dHBD7e.net4	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://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://vn95dHBD7e.net	0%	Avira URL Cloud	safe	
http://qdovFN.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://smtp.kaeiser.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
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	

Domains and IPs

Contacted Domains

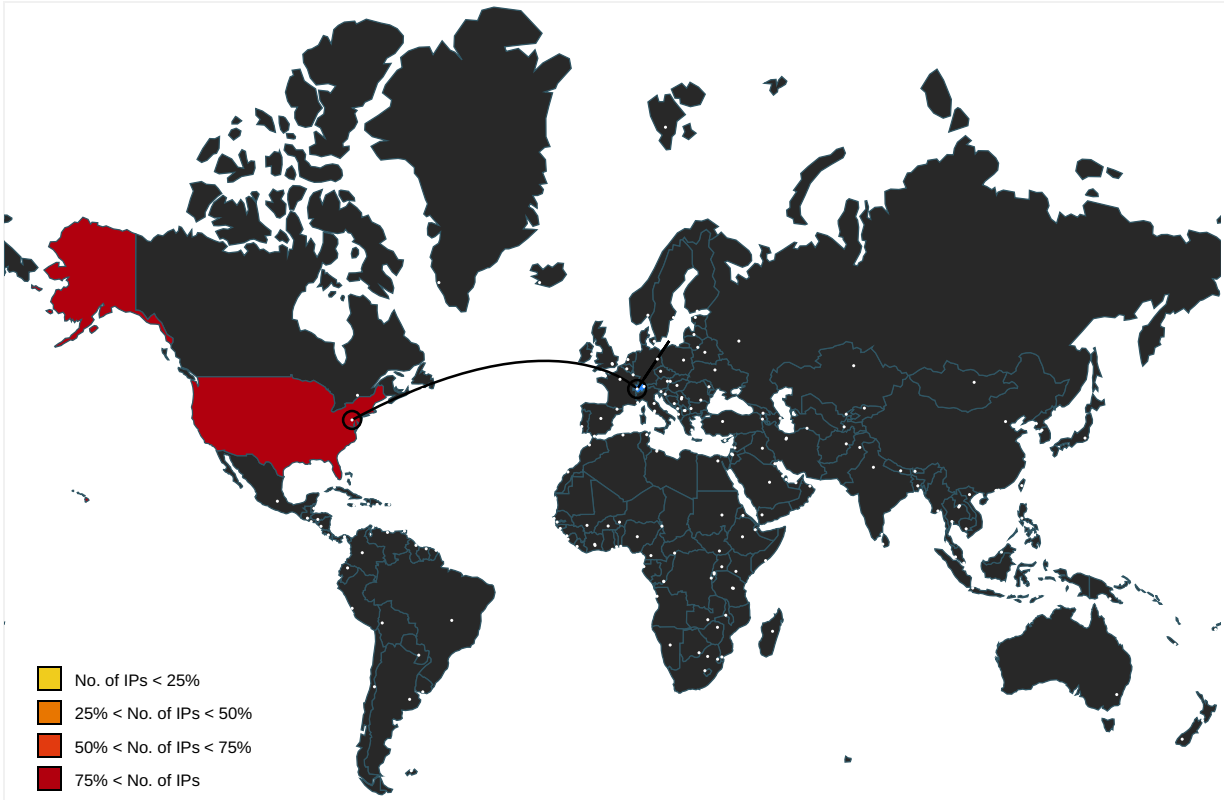
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.kaeiser.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://vn95dHBD7e.net4	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	tLes2JdtRw.exe, 00000003.00000002.908788243.000000000347D000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vn95dHBD7e.net	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp, tLes2JdtRw.exe, 00000003.00000002.908718423.000000000342C000.00000004.00000001.sdmp, tLes2JdtRw.exe, 00000003.00000002.908802618.000000003487000.00000004.00000001.sdmp, tLes2JdtRw.exe, 00000003.00000002.908815420.000000000348C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://qdovFN.com	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://smtp.kaeiser.com	tLes2JdtRw.exe, 00000003.00000002.908788243.000000000347D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	tLes2JdtRw.exe, 00000000.00000002.655983993.0000000002BE1000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	tLes2JdtRw.exe, 00000003.00000002.908393469.0000000003121000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	tLes2JdtRw.exe, 00000000.00000002.657948952.0000000003BE9000.00000004.00000001.sdmp, tLes2JdtRw.exe, 00000003.00000002.906500988.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	tLes2JdtRw.exe, 00000000.00000002.656178946.0000000002C25000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412499
Start date:	12.05.2021
Start time:	18:30:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tLes2JdtRw.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:	21
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:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 52.3% • Quality standard deviation: 9.5%
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 • Excluded IPs from analysis (whitelisted): 13.107.246.254, 104.43.139.144, 92.122.145.220, 104.43.193.48, 20.49.157.6, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, arc.msn.com, t-ring.msedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, iris-de-ppe-azsc-uks.uksouth.cloudapp.azure.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, t-ring.t-9999.t-msedge.net, displaycatalog-rp.md.mp.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:31:22	API Interceptor	752x Sleep call for process: tLes2JdtRw.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	NEW PI#001890576.exe	Get hash	malicious	Browse	
	B5Cg5YZIzp.exe	Get hash	malicious	Browse	
	Quotation..exe	Get hash	malicious	Browse	
	RFQ-Quotation..exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	presupuesto.xlsx	Get hash	malicious	Browse	
	Product Range #2828915.exe	Get hash	malicious	Browse	
	payment.exe	Get hash	malicious	Browse	
	LM Approved Invoices 06052021.doc	Get hash	malicious	Browse	
	DHL 46773482551423.exe	Get hash	malicious	Browse	
	jkj.exe	Get hash	malicious	Browse	
	Mlj6rE49Bf.exe	Get hash	malicious	Browse	
	DHL Shipment Delivery Notification.exe	Get hash	malicious	Browse	
	QuoteXrequestX-DAX31312.exe	Get hash	malicious	Browse	
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	
	razi.exe	Get hash	malicious	Browse	
	Project Enquiry - KHI To LSG.exe	Get hash	malicious	Browse	
	LM Approved Invoice-02-05-2021.doc	Get hash	malicious	Browse	
	KJ29joA7RS.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.624.32220.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	presupuesto.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 4500379537.exe	Get hash	malicious	Browse	• 208.91.199.225
	B5Cg5YZIzp.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 2345566 hisob-faktura.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation..exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Quotation..exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.224
	QUOTATION ORDER.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ_SGCCUP_24 590 34 532 -11052021.exe	Get hash	malicious	Browse	• 208.91.198.143
	Request Sample products.exe	Get hash	malicious	Browse	• 208.91.198.143
	QTY-3322.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	Letter of Demand.doc	Get hash	malicious	Browse	• 103.21.59.173
	7b4NmGxyY2.exe	Get hash	malicious	Browse	• 162.215.24 1.145
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\tLes2JdtRw.exe.log

Process:	C:\Users\user\Desktop\tLes2JdtRw.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.368651744936592
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	tLes2JdtRw.exe
File size:	828928
MD5:	2edb5a087966f25f972506500a48c9f3
SHA1:	ba38e69ebe87da9e49d45b2b291ee3024f8bd743

General	
SHA256:	1b80ed1165b46b410fbc236e2e19baa9e0d71b6992a41e 5d30b7d70670bb2c08
SHA512:	eb8a0301460513ad00e37642be99925b0626533d38587 75ba7f2fb3366d23f73c68a5b2637b7036635d0496f854d 29ebaf8ef6d4f984ce959668bff0b14f015
SSDEEP:	12288:WAXCx2Kb/B3bxRp1fjOfzLDiX8Sv++7YlAhoLW DWZH:W9zZmDJS2bGh/WZH
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L..... .`..............P.................. ... .@.. .... @................................

File Icon

pdf	
Icon Hash:	8a8ccae6e0fcc4aa

Static PE Info

General	
Entrypoint:	0x4b0ec2
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:	0x609BDA1B [Wed May 12 13:37:31 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb0e70	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb2000	0x1b0b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	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	0xaeec8	0xaf000	False	0.804772600446	data	7.64323527692	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb2000	0x1b0b0	0x1b200	False	0.12309187788	data	3.50745189553	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb2220	0x1b5f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb3d80	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xc45a8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xc87d0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xcad78	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xcbe20	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xcc288	0x5a	data		
RT_VERSION	0xcc2e4	0x39c	data		
RT_MANIFEST	0xcc680	0xa2e	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

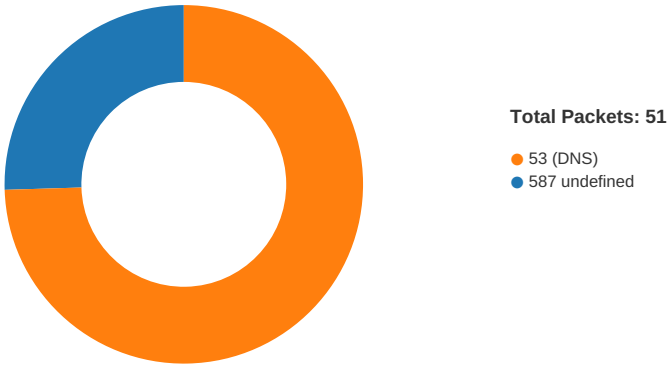
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	BindableVectorToListAdapter.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LibraryManagementSystem
ProductVersion	1.0.0.0
FileDescription	LibraryManagementSystem
OriginalFilename	BindableVectorToListAdapter.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-18:33:11.558436	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49768	587	192.168.2.4	208.91.199.223

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:33:09.733745098 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:09.904205084 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:09.904330015 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:10.523529053 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:10.523992062 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:10.692286015 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:10.692349911 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:10.697154999 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:10.866780043 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:10.868251085 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.038870096 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:11.039875031 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.209472895 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:11.209925890 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.387448072 CEST	587	49768	208.91.199.223	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:33:11.387923956 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.556490898 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:11.558435917 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.558599949 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.559396982 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.559489012 CEST	49768	587	192.168.2.4	208.91.199.223
May 12, 2021 18:33:11.726953030 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:11.727773905 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:11.825989008 CEST	587	49768	208.91.199.223	192.168.2.4
May 12, 2021 18:33:11.877177000 CEST	49768	587	192.168.2.4	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:31:13.000648022 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:13.052093029 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 18:31:14.486854076 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:14.538635015 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 18:31:15.216005087 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:15.278109074 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 18:31:15.397133112 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:15.448967934 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 18:31:16.270628929 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:16.319526911 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 18:31:17.844137907 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:17.892843008 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 18:31:19.222548962 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:19.272584915 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 18:31:20.249919891 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:20.299088955 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 18:31:22.778238058 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:22.827513933 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 18:31:23.703378916 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:23.754858017 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 18:31:25.823679924 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:25.874551058 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 18:31:26.894315958 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:26.944556952 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 18:31:27.849112034 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:27.902183056 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 18:31:28.794675112 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:28.843360901 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 18:31:29.733302116 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:29.782136917 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 18:31:31.093420029 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:31.142330885 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 18:31:32.038659096 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:32.091114998 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 18:31:33.692508936 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:33.744218111 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 18:31:35.016109943 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:35.067823887 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 18:31:37.920304060 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:37.969316006 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 18:31:38.938080072 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:38.987049103 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 18:31:44.021934032 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:44.095408916 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 18:31:48.082925081 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 18:31:48.141783953 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 18:32:03.870563984 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:03.974404097 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 18:32:04.692900896 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:04.750056982 CEST	53	56448	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:32:05.352232933 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:05.532748938 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 18:32:05.651247025 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:05.725193977 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 18:32:06.051594973 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:06.103178978 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 18:32:06.680185080 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:06.742635012 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 18:32:07.410607100 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:07.462007046 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 18:32:07.946609974 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:08.003762007 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 18:32:08.786604881 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:08.844605923 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 18:32:10.254878998 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:10.313143015 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 18:32:10.788036108 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:10.847855091 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 18:32:20.709436893 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:20.770606041 CEST	53	60542	8.8.8.8	192.168.2.4
May 12, 2021 18:32:53.786892891 CEST	60689	53	192.168.2.4	8.8.8.8
May 12, 2021 18:32:53.844396114 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 18:33:09.211232901 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 18:33:09.402455091 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 18:33:09.431077957 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 18:33:09.615881920 CEST	53	50904	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 18:33:09.211232901 CEST	192.168.2.4	8.8.8.8	0xd25b	Standard query (0)	smtp.kaeiser.com	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.431077957 CEST	192.168.2.4	8.8.8.8	0x40e6	Standard query (0)	smtp.kaeiser.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 18:33:09.402455091 CEST	8.8.8.8	192.168.2.4	0xd25b	No error (0)	smtp.kaeiser.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:33:09.402455091 CEST	8.8.8.8	192.168.2.4	0xd25b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.402455091 CEST	8.8.8.8	192.168.2.4	0xd25b	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.402455091 CEST	8.8.8.8	192.168.2.4	0xd25b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.402455091 CEST	8.8.8.8	192.168.2.4	0xd25b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.615881920 CEST	8.8.8.8	192.168.2.4	0x40e6	No error (0)	smtp.kaeiser.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 18:33:09.615881920 CEST	8.8.8.8	192.168.2.4	0x40e6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.615881920 CEST	8.8.8.8	192.168.2.4	0x40e6	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.615881920 CEST	8.8.8.8	192.168.2.4	0x40e6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 18:33:09.615881920 CEST	8.8.8.8	192.168.2.4	0x40e6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

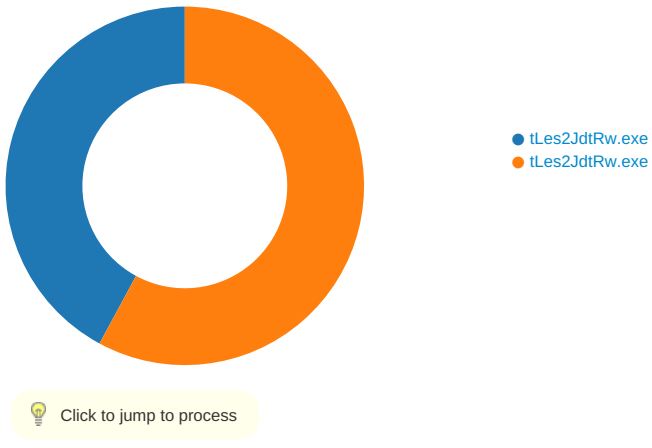
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 18:33:10.523529053 CEST	587	49768	208.91.199.223	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 12, 2021 18:33:10.523992062 CEST	49768	587	192.168.2.4	208.91.199.223	EHLO 928100
May 12, 2021 18:33:10.692349911 CEST	587	49768	208.91.199.223	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 12, 2021 18:33:10.697154999 CEST	49768	587	192.168.2.4	208.91.199.223	AUTH login c2VyZ2lvLmFycm95b0BrYWVpc2VyLmNvbQ==
May 12, 2021 18:33:10.866780043 CEST	587	49768	208.91.199.223	192.168.2.4	334 UGFzc3dvcmQ6
May 12, 2021 18:33:11.038870096 CEST	587	49768	208.91.199.223	192.168.2.4	235 2.7.0 Authentication successful
May 12, 2021 18:33:11.039875031 CEST	49768	587	192.168.2.4	208.91.199.223	MAIL FROM:<sergio.arroyo@kaeiser.com>
May 12, 2021 18:33:11.209472895 CEST	587	49768	208.91.199.223	192.168.2.4	250 2.1.0 Ok
May 12, 2021 18:33:11.209925890 CEST	49768	587	192.168.2.4	208.91.199.223	RCPT TO:<sergio.arroyo@kaeiser.com>
May 12, 2021 18:33:11.387448072 CEST	587	49768	208.91.199.223	192.168.2.4	250 2.1.5 Ok
May 12, 2021 18:33:11.387923956 CEST	49768	587	192.168.2.4	208.91.199.223	DATA
May 12, 2021 18:33:11.556490898 CEST	587	49768	208.91.199.223	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 18:33:11.559489012 CEST	49768	587	192.168.2.4	208.91.199.223	.
May 12, 2021 18:33:11.825989008 CEST	587	49768	208.91.199.223	192.168.2.4	250 2.0.0 Ok: queued as 4DA4BD7A5E

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: tLes2JdtRw.exe PID: 6888 Parent PID: 5844

General

Start time:	18:31:19
Start date:	12/05/2021

Path:	C:\Users\user\Desktop\tLes2JdtRw.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\tLes2JdtRw.exe'
Imagebase:	0x7a0000
File size:	828928 bytes
MD5 hash:	2EDB5A087966F25F972506500A48C9F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.656178946.0000000002C25000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.657948952.0000000003BE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.657948952.0000000003BE9000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\tLes2JdtRw.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\tLes2JdtRw.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: tLes2JdtRw.exe PID: 7072 Parent PID: 6888

General

Start time:	18:31:25
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\tLes2JdtRw.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\tLes2JdtRw.exe
Imagebase:	0xc50000
File size:	828928 bytes
MD5 hash:	2EDB5A087966F25F972506500A48C9F3
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.906500988.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.906500988.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.908393469.0000000003121000.00000004.00000001.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	6D38CF06	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	6D38CF06	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c9e7052d-c9c4-47a4-a61e-8b3703213c21	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Disassembly

Code Analysis