

JoeSandbox Cloud BASIC



ID: 403969

Sample Name: ordine n#U00b0
276.exe

Cookbook: default.jbs

Time: 15:32:00

Date: 04/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report ordine n#U00b0 276.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	5
Networking:	5
Signature Overview	5
AV Detection:	5
Networking:	5
System Summary:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
Anti Debugging:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
Contacted IPs	10
Public	11
Private	11
General Information	11
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASN	13
JA3 Fingerprints	13
Dropped Files	14
Created / dropped Files	14
Static File Info	14
General	14
File Icon	15
Static PE Info	15
General	15

Entrypoint Preview	15
Data Directories	17
Sections	17
Resources	17
Imports	17
Version Infos	17
Possible Origin	18
Network Behavior	18
Network Port Distribution	18
TCP Packets	18
UDP Packets	20
DNS Queries	21
DNS Answers	21
HTTPS Packets	22
SMTP Packets	22
Code Manipulations	22
Statistics	22
Behavior	22
System Behavior	23
Analysis Process: ordine n#U00b0 276.exe PID: 6888 Parent PID: 5912	23
General	23
File Activities	23
Analysis Process: RegAsm.exe PID: 1280 Parent PID: 6888	23
General	23
File Activities	24
File Created	24
File Deleted	25
File Written	25
File Read	26
Analysis Process: conhost.exe PID: 6896 Parent PID: 1280	26
General	26
Disassembly	27
Code Analysis	27

Analysis Report ordine n#U00b0 276.exe

Overview

General Information

Sample Name:	ordine n#U00b0 276.exe
Analysis ID:	403969
MD5:	10f03c95ba280cd..
SHA1:	c24232721d7ae..
SHA256:	11f63d2fda1055a..
Infos:	
Most interesting Screenshot:	

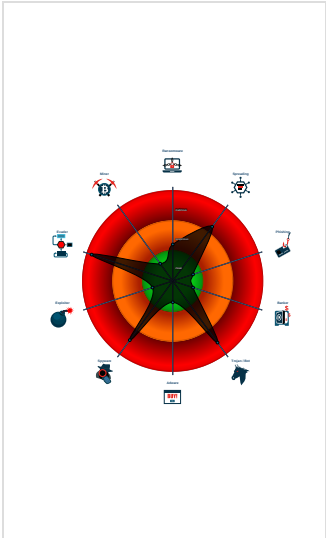
Detection

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

Signatures

Found malware configuration
Malicious sample detected (through ...
Sigma detected: RegAsm connects ...
Yara detected AgentTesla
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Detected RDTSC dummy instruction...
Found evasive API chain (trying to d...
Hides threads from debuggers
Queries sensitive BIOS Information ...
Queries sensitive network adapter in ...
Tries to detect Any.run
Tries to detect sandboxes and other...

Classification



Startup

- System is w10x64
- ordine n#U00b0 276.exe** (PID: 6888 cmdline: 'C:\Users\user\Desktop\ordine n#U00b0 276.exe' MD5: 10F03C95BA280CD5A82146269F89CA9D)
 - RegAsm.exe** (PID: 1280 cmdline: 'C:\Users\user\Desktop\ordine n#U00b0 276.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
 - conhost.exe** (PID: 6896 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496')
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Username": "Bx27nfj5fV0",
  "URL": "http://90ElorZCtFcqdkfzny.net",
  "To": "greendogman@yandex.com",
  "ByHost": "smtp.fil-net.com:587",
  "Password": "jEiJ6rphGxFJ",
  "From": "comercial@fil-net.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.1731275850.000000001DD01000.00000004.00000001.sdm	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.1731275850.000000001DD01000.00000004.00000001.sdm	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.772141814.000000000040C000.00000020.00020000.sdm	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	0x1298:\$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB

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 Any.run
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Tries to detect virtualization through RDTSC time measurements

Anti Debugging:



Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

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:

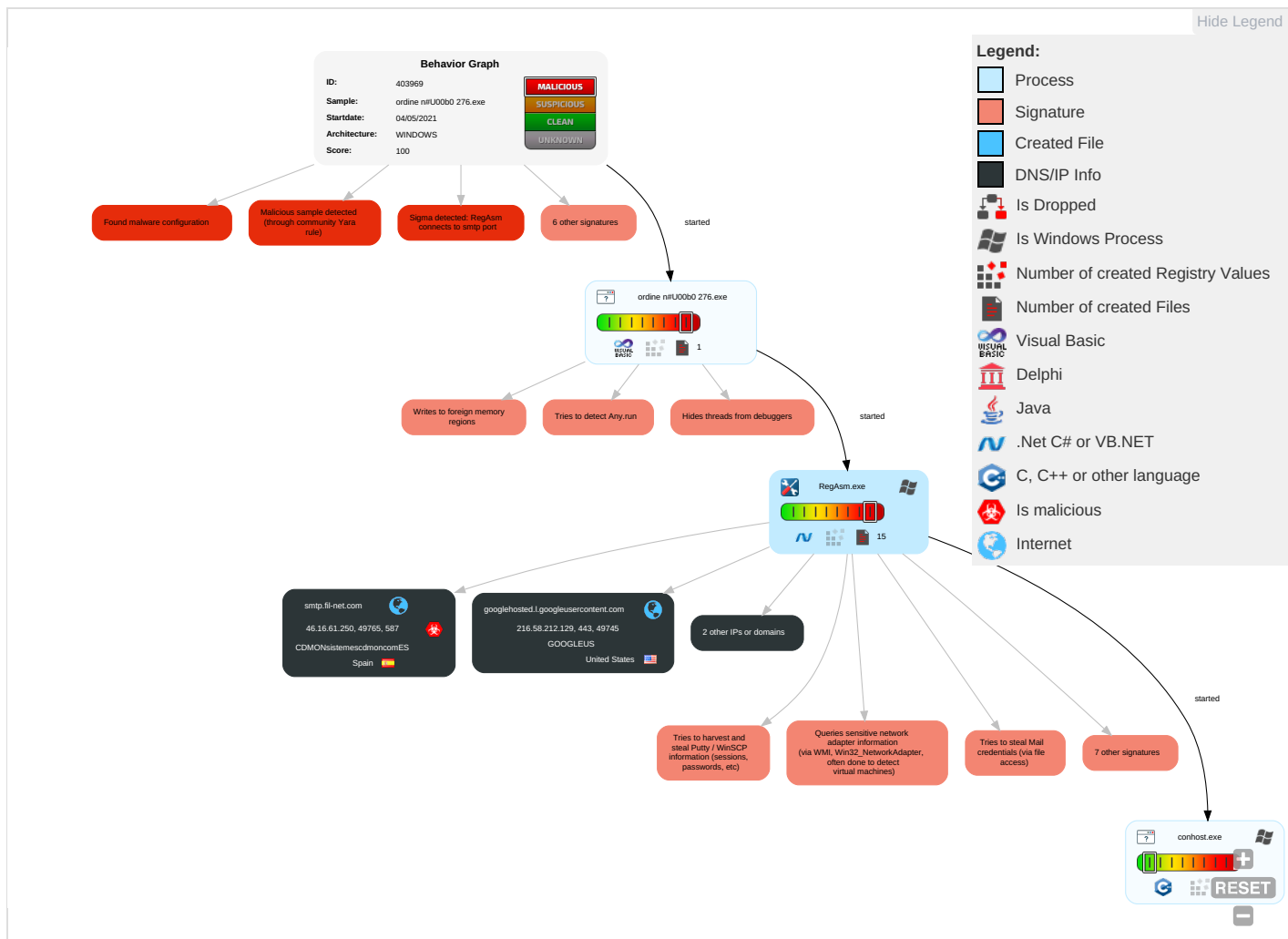


Yara detected AgentTesla

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	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Information Discovery 3 1 4	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Obfuscated Files or Information 1	Credentials in Registry 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	DLL Side-Loading 1	Security Account Manager	Security Software Discovery 6 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3 4 1	LSA Secrets	Virtualization/Sandbox Evasion 3 4 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

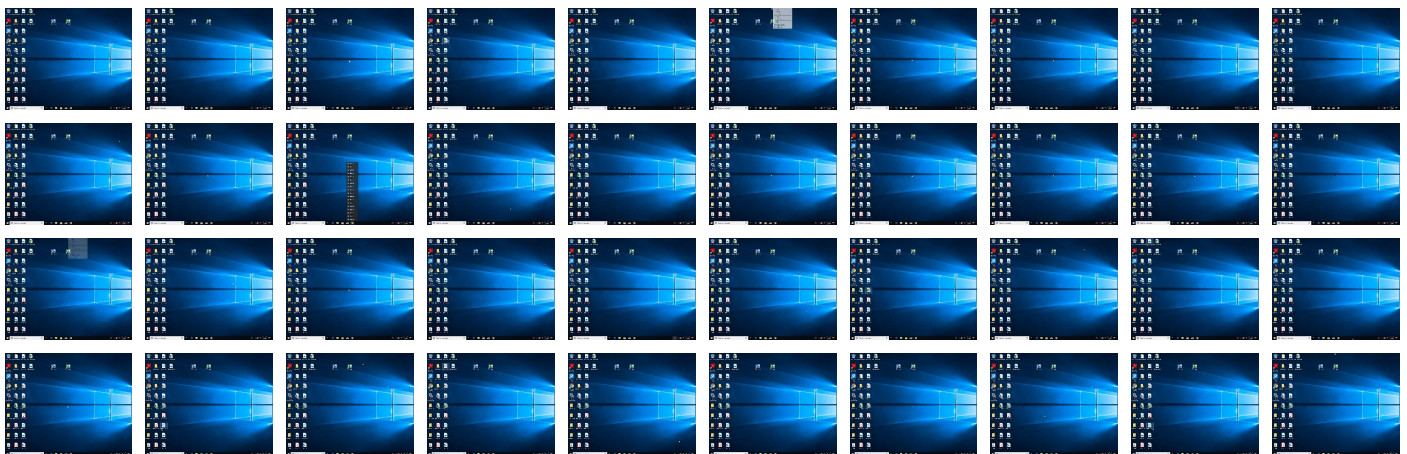
Behavior Graph



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
ordine n#U00b0 276.exe	9%	ReversingLabs	Win32.Worm.Wbvb	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
smtp.fil-net.com	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	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://crl.pki.goog/gsr1/gsr1.crl0;	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://9OElorZCtFCqdkfzny.net	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	Avira URL Cloud	safe	
http://pki.goog/gsr1/gsr1.crt02	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl0	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://mGfDbY.com	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0%	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gts1c3.der0	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gtsr1.der04	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtpl.fil-net.com	46.16.61.250	true	true	0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
doc-10-9k-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

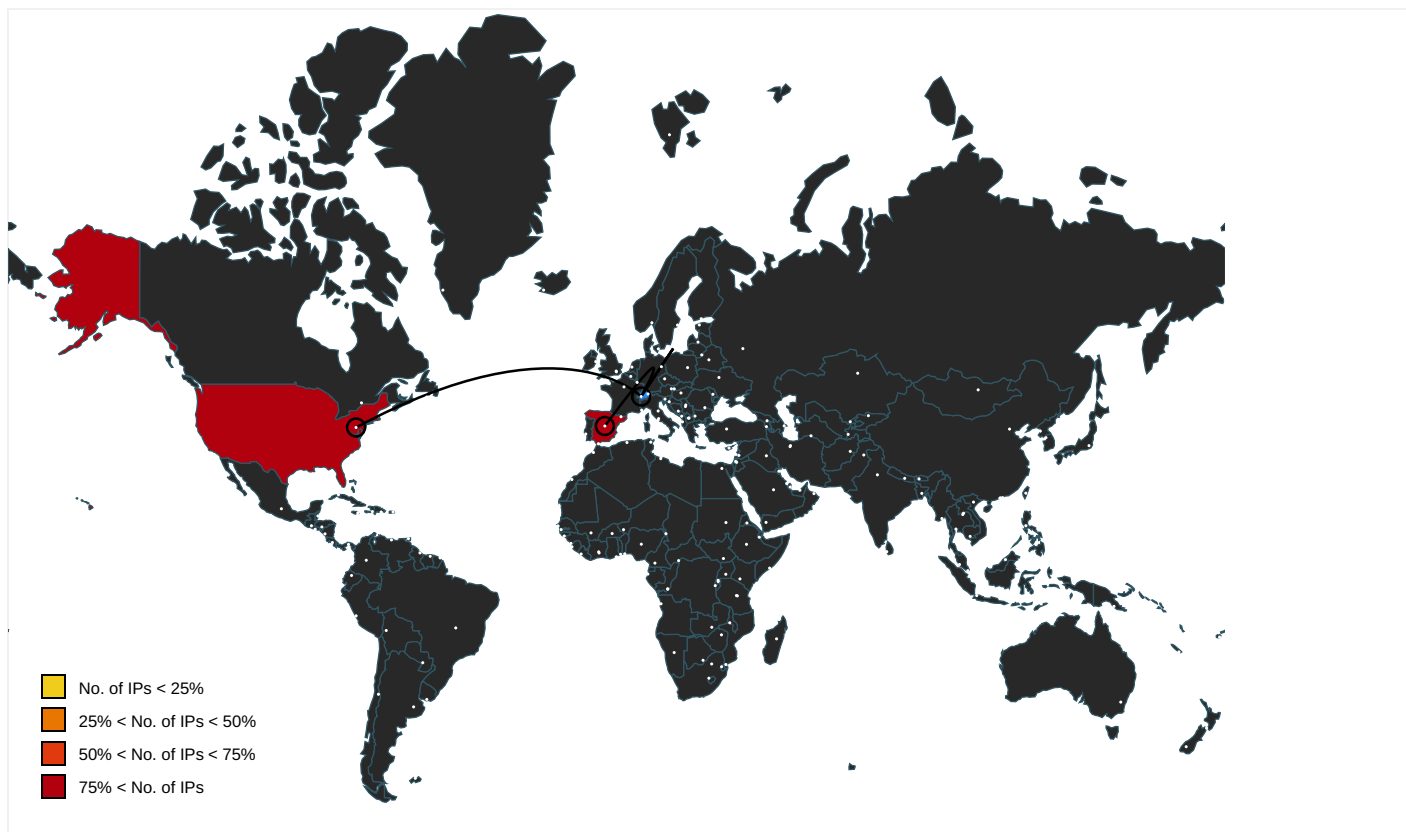
Name	Malicious	Antivirus Detection	Reputation
http://9OElorZCtFCqdkfzny.net	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000008.00000002. 1731275850.000000001DD01000.00 000004.00000001.sdmp	false	Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	RegAsm.exe, 00000008.00000002. 1731275850.000000001DD01000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr1/gsr1.crl0;	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	RegAsm.exe, 00000008.00000002. 1732276506.000000001FF5D000.00 000004.00000001.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	RegAsm.exe, 00000008.00000002. 1731275850.000000001DD01000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.org0	RegAsm.exe, 00000008.00000002. 1732276506.000000001FF5D000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-10-9k- docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7 defkksulhg5h7mbp1/ka3e4p4q	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	RegAsm.exe, 00000008.00000002. 1731275850.000000001DD01000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://crl.pki.goog/gtsr1/gtsr1.crl0W	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr1/gsr1.crt02	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pki.goog/repository/0	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl0	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doc-10-9k-docs.googleusercontent.com/	RegAsm.exe, 00000008.00000002. 1726751510.0000000001380000.00 000004.00000020.sdmp	false		high
http://https://api.ipify.org%	RegAsm.exe, 00000008.00000002. 1731275850.000000001DD01000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://mGfDbY.com	RegAsm.exe, 00000008.00000002. 1731275850.000000001DD01000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	RegAsm.exe, 00000008.00000002. 1732276506.000000001FF5D000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0%	RegAsm.exe, 00000008.00000002. 1732276506.000000001FF5D000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gts1c3.der0	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gtsr1.der04	RegAsm.exe, 00000008.00000003. 999365877.0000000001401000.000 00004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
46.16.61.250	smtp.fil-net.com	Spain		197712	CDMONsistemescdmoncomES	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403969
Start date:	04.05.2021
Start time:	15:32:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ordine n#U00b0 276.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:	32
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.spre.troj.spyw.evad.winEXE@4/2@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15% (good quality ratio 7.6%) • Quality average: 33.4% • Quality standard deviation: 36.5%
HCA Information:	• Successful, ratio: 95% • 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): 104.43.193.48, 52.255.188.83, 92.122.145.220, 20.82.210.154, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 142.250.185.78, 52.155.217.156, 20.54.26.129, 20.190.159.135, 20.190.159.137, 20.190.159.133, 40.126.31.9, 40.126.31.7, 40.126.31.136, 40.126.31.3, 40.126.31.142, 51.11.168.232, 40.127.240.158, 51.104.136.2 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprddcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, skypedataprddcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:33:51	API Interceptor	3896x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
46.16.61.250	a5FVSNazgr.exe	Get hash	malicious	Browse	
	HdgnMEvcFK.exe	Get hash	malicious	Browse	
	RTStyEQJpZ.exe	Get hash	malicious	Browse	
	PAGO.xlsx	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	Zapytanie -20216470859302.exe	Get hash	malicious	Browse	
	winlog.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	Nakit Akisi Detaylariniz.exe	Get hash	malicious	Browse	
	S67xSX1MNR.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.fil-net.com	Zapytanie -20216470859302.exe	Get hash	malicious	Browse	46.16.61.250
	Nakit Akisi Detaylariniz.exe	Get hash	malicious	Browse	46.16.61.250

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CDMONsistemescdmoncomES	a5FVSNazgr.exe	Get hash	malicious	Browse	46.16.61.250
	HdgnMEvcFK.exe	Get hash	malicious	Browse	46.16.61.250
	RTStyEQJpZ.exe	Get hash	malicious	Browse	46.16.61.250
	PAGO.xlsx	Get hash	malicious	Browse	46.16.61.250
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	46.16.61.250
	Zapytanie -20216470859302.exe	Get hash	malicious	Browse	46.16.61.250
	njGJ1eW44wshoMr.exe	Get hash	malicious	Browse	46.16.62.134
	3nG9LW7Z21dxUoM.exe	Get hash	malicious	Browse	46.16.62.134
	keeFDE9dhCGNNez.exe	Get hash	malicious	Browse	46.16.62.134
	74tF1foMeQyUMCh.exe	Get hash	malicious	Browse	46.16.62.134
	qm7JU84PFgfqvs.exe	Get hash	malicious	Browse	46.16.62.134
	winlog.exe	Get hash	malicious	Browse	46.16.61.250
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	46.16.61.250
	WbGKi8E5OE4eCFG.exe	Get hash	malicious	Browse	46.16.62.134
	r9SWnqQlK8PFPEp.exe	Get hash	malicious	Browse	46.16.62.134
	L9oOm9x3I7YZFcA.exe	Get hash	malicious	Browse	46.16.62.134
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	134.0.10.35
	jKiL1mzTAVltJ30.exe	Get hash	malicious	Browse	46.16.62.134
	09xcuRN2HJmRRCm.exe	Get hash	malicious	Browse	46.16.62.134
	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	185.66.41.128

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	statistic-2067311372.xlsm	Get hash	malicious	Browse	216.58.212.129
	statistic-2069354685.xlsm	Get hash	malicious	Browse	216.58.212.129
	statistic-2070252624.xlsm	Get hash	malicious	Browse	216.58.212.129
	statistic-2072807337.xlsm	Get hash	malicious	Browse	216.58.212.129
	statistic-207394368.xlsm	Get hash	malicious	Browse	216.58.212.129
	f97e137e_by_Libranalysis.exe	Get hash	malicious	Browse	216.58.212.129
	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	216.58.212.129
	MV RED SEA.docx	Get hash	malicious	Browse	216.58.212.129
	MyUY1HeWNL.exe	Get hash	malicious	Browse	216.58.212.129
	IMG-WA7905432.exe	Get hash	malicious	Browse	216.58.212.129
	catalog-1521295750.xlsm	Get hash	malicious	Browse	216.58.212.129
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	216.58.212.129
	Remittance Advice pdf.exe	Get hash	malicious	Browse	216.58.212.129
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	216.58.212.129

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 216.58.212.129
	Tree Top.html	Get hash	malicious	Browse	• 216.58.212.129
	PT6-1152.doc	Get hash	malicious	Browse	• 216.58.212.129
	s.dll	Get hash	malicious	Browse	• 216.58.212.129
	setup-lightshot.exe	Get hash	malicious	Browse	• 216.58.212.129
	s.dll	Get hash	malicious	Browse	• 216.58.212.129

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\3blxsn2e.5rk\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPX5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@C.....g...8.....

IDevice\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFF32302558111EE880BA0C41747A0853:
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NordVPN directory not found!..

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.764868199016906

General

TrID:	- Win32 Executable (generic) a (10002005/4) 99.15% - Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ordine n#U00b0 276.exe
File size:	98304
MD5:	10f03c95ba280cd5a82146269f89ca9d
SHA1:	c24232721d7aefe2c013b9642e0ab7db8007e48a
SHA256:	11f63d2fda1055ac66a71cb539c9d5ff66fd79f473e19171fd8f663e2c4979b9
SHA512:	4b537aec0eee96b506ac63fcbdfc4e1e2ac231ca8d5136cfe7a67e84ac5643424d7090ae88ddb3e809d94272fa15edb20ed70964076fbf05260dceabac5ab76
SSDEEP:	1536:kh70hrnoEdQNVX1/o3lAEmYY6qbtug0Oj1o/:kl0tnoO81/4OYZJGO5S
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.....u...1...1. ..1.....0...~...0.....0...Rich1.....PE..L.....UQ..... ..P.....`.....@.....

File Icon

	
Icon Hash:	b074cecec891b2e4

Static PE Info

General

Entrypoint:	0x40157c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x51551DDA [Fri Mar 29 04:51:38 2013 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	631ffe9ad0b821781f48149fabda62f6

Entrypoint Preview

Instruction

```
push 0040CC14h
call 00007FADB0C84B55h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esp], bl
```


Instruction
add byte ptr [eax], al
add al, 00h
insd
popad
jc 00007FADB0C84BCFh
add byte ptr [43000501h], cl
dec edi
push esi
inc ebp
push esp
add byte ptr [ecx], bl
add dword ptr [eax], eax
inc edx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15054	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x5a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x10c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x144d0	0x15000	False	0.33740234375	data	5.19887366844	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0xad4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5a4	0x1000	False	0.1826171875	data	1.71136635862	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x173bc	0x1e8	data		
RT_GROUP_ICON	0x173a8	0x14	data		
RT_VERSION	0x170f0	0x2b8	COM executable for DOS	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_Clics, _adj_fptan, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPEException, _Cilog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaStrToAnsi, __vbaFpI4, _Clatan, __vbaStrMove, _allmul, _Cltan, _Clexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	OPARBE

Description	Data
FileVersion	1.00
CompanyName	Mummys Technology
Comments	Mummys Technology
ProductName	Mummys Technology
ProductVersion	1.00
FileDescription	Mummys Technology
OriginalFilename	OPARBE.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:33:44.572319031 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.612984896 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.613104105 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.613687992 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.655802011 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.662863970 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.662900925 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.662920952 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.662941933 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.662962914 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.662972927 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.662986040 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.663006067 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.663026094 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.700042963 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.743093014 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.743417025 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.744574070 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.789469957 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.967124939 CEST	443	49745	216.58.212.129	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:33:44.967187881 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.967230082 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.967289925 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.967339039 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.968014956 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.968048096 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.968082905 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.968112946 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.971024990 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.971055984 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.971136093 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.971160889 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.973953009 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.973983049 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.974102974 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.974131107 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.976912975 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.976943016 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.976999044 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.979947090 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.979976892 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.980098009 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.982877970 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.982914925 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.982986927 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.983010054 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:44.985869884 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.985908985 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:44.985985994 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.008136988 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.008222103 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.008260965 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.008327007 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.010838985 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.010931015 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.011029005 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.012511015 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.012556076 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.012586117 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.012609005 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.015357018 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.015404940 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.015465021 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.015489101 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.018477917 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.018521070 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.018738985 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.021447897 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.021478891 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.021548986 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.024266005 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.024286032 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.024363995 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.027165890 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.027188063 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.027245998 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.030052900 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.030071020 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.030354977 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.032716990 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.032752991 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.032851934 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.035206079 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.035238028 CEST	443	49745	216.58.212.129	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:33:45.035271883 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.035298109 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.037623882 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.037648916 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.037714005 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.040081024 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.040105104 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.040188074 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.042586088 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.042644024 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.042689085 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.042738914 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.044986963 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.045033932 CEST	443	49745	216.58.212.129	192.168.2.4
May 4, 2021 15:33:45.045141935 CEST	49745	443	192.168.2.4	216.58.212.129
May 4, 2021 15:33:45.047472000 CEST	443	49745	216.58.212.129	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:32:40.045464993 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:40.094208956 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 15:32:40.954361916 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:41.003158092 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 15:32:41.736464977 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:41.785149097 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 15:32:42.659574986 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:42.708424091 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 15:32:42.896543026 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:42.963821888 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 15:32:43.541533947 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:43.592067003 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 15:32:44.592176914 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:44.646218061 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 15:32:46.039527893 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:46.108371019 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 15:32:47.007075071 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:47.055928946 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 15:32:48.739245892 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:48.787933111 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 15:32:49.873409986 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:49.925098896 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 15:32:50.810866117 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:50.859603882 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 15:32:51.947354078 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:52.000696898 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 15:32:53.351233959 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:53.400072098 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 15:32:54.265948057 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:54.323062897 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 15:32:55.132121086 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:55.192071915 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 15:32:56.250293016 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:56.299580097 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 15:32:57.100306988 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:57.149581909 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 15:32:57.967885971 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 15:32:58.016633034 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 15:33:15.147033930 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:15.197618961 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 15:33:29.537322044 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:29.601537943 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 15:33:35.353529930 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:35.415411949 CEST	53	51255	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:33:43.406893015 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:43.474893093 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 15:33:44.503277063 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:44.568542004 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 15:33:49.157248974 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:49.262083054 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 15:33:50.119745970 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:50.446191072 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 15:33:51.255096912 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:51.355187893 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 15:33:51.914782047 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:51.954771042 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:51.976136923 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 15:33:52.023849010 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 15:33:52.544280052 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:52.603557110 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 15:33:53.198702097 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:53.255937099 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 15:33:54.143522978 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:54.203474998 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 15:33:54.948461056 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:55.007996082 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 15:33:55.889342070 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:55.949563980 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 15:33:56.185600996 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:56.245059013 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 15:33:56.407876015 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 15:33:56.456758022 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 15:34:26.118033886 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 15:34:26.166835070 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 15:34:27.903454065 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 15:34:27.969216108 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 15:35:13.105088949 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 15:35:13.170341015 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 15:35:34.531362057 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 15:35:34.588290930 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 15:37:35.214534998 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 15:37:35.275285959 CEST	53	60689	8.8.8.8	192.168.2.4
May 4, 2021 15:37:35.884021044 CEST	64206	53	192.168.2.4	8.8.8.8
May 4, 2021 15:37:35.953700066 CEST	53	64206	8.8.8.8	192.168.2.4
May 4, 2021 15:37:39.018558979 CEST	50904	53	192.168.2.4	8.8.8.8
May 4, 2021 15:37:39.090518951 CEST	53	50904	8.8.8.8	192.168.2.4
May 4, 2021 15:37:42.572835922 CEST	57525	53	192.168.2.4	8.8.8.8
May 4, 2021 15:37:42.646023035 CEST	53	57525	8.8.8.8	192.168.2.4
May 4, 2021 15:37:43.007853031 CEST	53814	53	192.168.2.4	8.8.8.8
May 4, 2021 15:37:43.064872026 CEST	53	53814	8.8.8.8	192.168.2.4
May 4, 2021 15:39:58.554929018 CEST	53418	53	192.168.2.4	8.8.8.8
May 4, 2021 15:39:58.617453098 CEST	53	53418	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 15:33:44.503277063 CEST	192.168.2.4	8.8.8.8	0xfb42	Standard query (0)	doc-10-9k-docs.googleusercontent.com	A (IP address)	IN (0x0001)
May 4, 2021 15:35:13.105088949 CEST	192.168.2.4	8.8.8.8	0x881d	Standard query (0)	smtp.fil-net.com	A (IP address)	IN (0x0001)
May 4, 2021 15:35:34.531362057 CEST	192.168.2.4	8.8.8.8	0x53eb	Standard query (0)	smtp.fil-net.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:33:44.568542004 CEST	8.8.8.8	192.168.2.4	0xfb42	No error (0)	doc-10-9k-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:33:44.568542004 CEST	8.8.8.8	192.168.2.4	0xfb42	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)
May 4, 2021 15:35:13.170341015 CEST	8.8.8.8	192.168.2.4	0x881d	No error (0)	smtp.fil-net.com		46.16.61.250	A (IP address)	IN (0x0001)
May 4, 2021 15:35:34.588290930 CEST	8.8.8.8	192.168.2.4	0x53eb	No error (0)	smtp.fil-net.com		46.16.61.250	A (IP address)	IN (0x0001)
May 4, 2021 15:37:35.275285959 CEST	8.8.8.8	192.168.2.4	0xf915	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 15:33:44.662986040 CEST	216.58.212.129	443	192.168.2.4	49745	CN=*.googleusercontent.com, CN=GTS CA 1C3, O=Google Trust Services LLC, C=US, CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US, CN=GTS Root R1, O=Google Trust Services LLC, C=US, CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Apr 13 12:41:17 CEST 2021	Tue Jul 06 12:41:16 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CET 2028		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

SMTP Packets

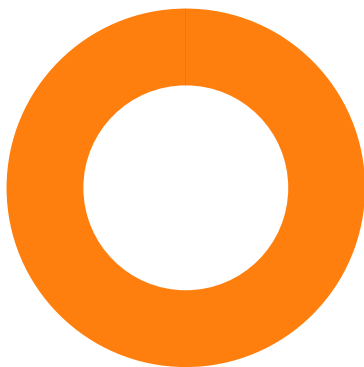
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 15:35:43.815591097 CEST	587	49765	46.16.61.250	192.168.2.4	220 vxsys-smtpclusterma-06.srv.cat ESMTPEHLO 468325
May 4, 2021 15:35:43.816262960 CEST	49765	587	192.168.2.4	46.16.61.250	
May 4, 2021 15:35:43.879950047 CEST	587	49765	46.16.61.250	192.168.2.4	250-vxsys-smtpclusterma-06.srv.cat250-PIPELINING250-SIZE 47185920250-ETRN250-STARTTLS250-AUTH LOGIN PLAIN CRAM-MD5 DIGEST-MD5250-ENHANCEDSTATUSCODES250-8BITMIME250-DSN250 CHUNKING
May 4, 2021 15:35:43.880307913 CEST	49765	587	192.168.2.4	46.16.61.250	STARTTLS
May 4, 2021 15:35:43.941596031 CEST	587	49765	46.16.61.250	192.168.2.4	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

- ordine n#U00b0 276.exe
- RegAsm.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: ordine n#U00b0 276.exe PID: 6888 Parent PID: 5912

General

Start time:	15:32:46
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ordine n#U00b0 276.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ordine n#U00b0 276.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	10F03C95BA280CD5A82146269F89CA9D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	- Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.772141814.000000000040C000.00000020.00020000.sdmp, Author: Florian Roth - Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000000.643378031.000000000040C000.00000020.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
File Path		Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 1280 Parent PID: 6888

General

Start time:	15:33:17
Start date:	04/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ordine n#U00b0 276.exe'

Imagebase:	0xbe0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.1731275850.000000001DD01000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.1731275850.000000001DD01000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

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	FB2C53	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	FB2C53	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	FB2C53	InternetOpenUrlA
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	FB2C53	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	FB2C53	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	FB2C53	InternetOpenUrlA
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	722760AC	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	722760AC	unknown
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	722760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	722760AC	unknown
C:\Users\user\AppData\Roaming\3blxsn2e.5rk	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	F734F9	CreateDirectoryW
C:\Users\user\AppData\Roaming\3blxsn2e.5rk\Chrome	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	F734F9	CreateDirectoryW
C:\Users\user\AppData\Roaming\3blxsn2e.5rk\Chrome\Default	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	F734F9	CreateDirectoryW
C:\Users\user\AppData\Roaming\3blxsn2e.5rk\Chrome\Default\Cookies	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	F735BC	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\3blxsn2e.5rk\Chrome\Default\Cookies	success or wait	1	F73676	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	F70EAF	WriteFile
\Device\ConDrv	unknown	30	4e 6f 72 64 56 50 4e 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 21 0d 0a	NordVPN directory not found!..	success or wait	1	F70EAF	WriteFile

[illegible]

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	F70EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	F70EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	F70EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	F70EAF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	40960	success or wait	1	F70EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	F70EAF	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\0497ecb2-71a4-436b-9d71-3b9de23c3cac	unknown	4096	success or wait	1	F70EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	F70EAF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	F70EAF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	F70EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	F70EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	F70EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	F70EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	F70EAF	ReadFile
C:\Users\user\AppData\Roaming\3blxs2nE.5rk\Chrome\Default\Cookies	unknown	16384	success or wait	2	F70EAF	ReadFile

Analysis Process: conhost.exe PID: 6896 Parent PID: 1280

General

Start time:	15:33:18
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis