ID: 382848
Sample Name: Ordine d'acquisto 240517_04062021.exe
Cookbook: default.jbs
Time: 18:51:46
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

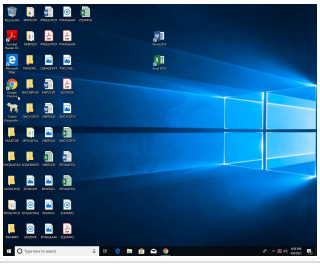
Analysis Report Ordine d'acquisto 240517_04062021.exe

Overview

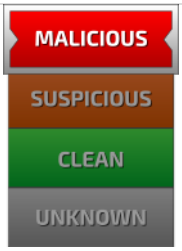
General Information

Sample Name:	Ordine d'acquisto 240517_04062021.exe
Analysis ID:	382848
MD5:	c81b0ec94cb5bc…
SHA1:	ed6f7c97ab1d9cc..
SHA256:	51b0a2f869f9fe3…
Infos:	

Most interesting Screenshot:



Detection



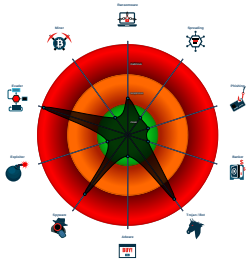
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: RegAsm connects …
- Yara detected AgentTesla
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found evasive API chain (trying to d…
- Hides threads from debuggers
- Installs a global keyboard hook
- May check the online IP address of …
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- Ordine d'acquisto 240517_04062021.exe (PID: 2160 cmdline: 'C:\Users\user\Desktop\Ordine d'acquisto 240517_04062021.exe' MD5: C81B0EC94CB5BC1E76B355D7E1125A48)
  - RegAsm.exe (PID: 5324 cmdline: 'C:\Users\user\Desktop\Ordine d'acquisto 240517_04062021.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 1044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "sFYXIfZKCzm3DG",
  "URL: ": "https://dex62ukWey0O8Y.net",
  "To: ": "",
  "ByHost: ": "smtp.yandex.com:587",
  "Password: ": "5XOud",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.750710271.000000000116 2000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000012.00000002.757510449.000000001DF1 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.757510449.000000001DF1 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 5324	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

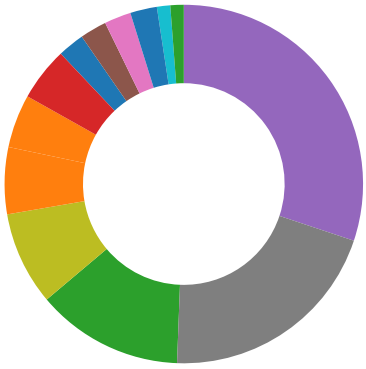
Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 5324	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: RegAsm connects to smtp port

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Networking:

C2 URLs / IPs found in malware configuration

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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)

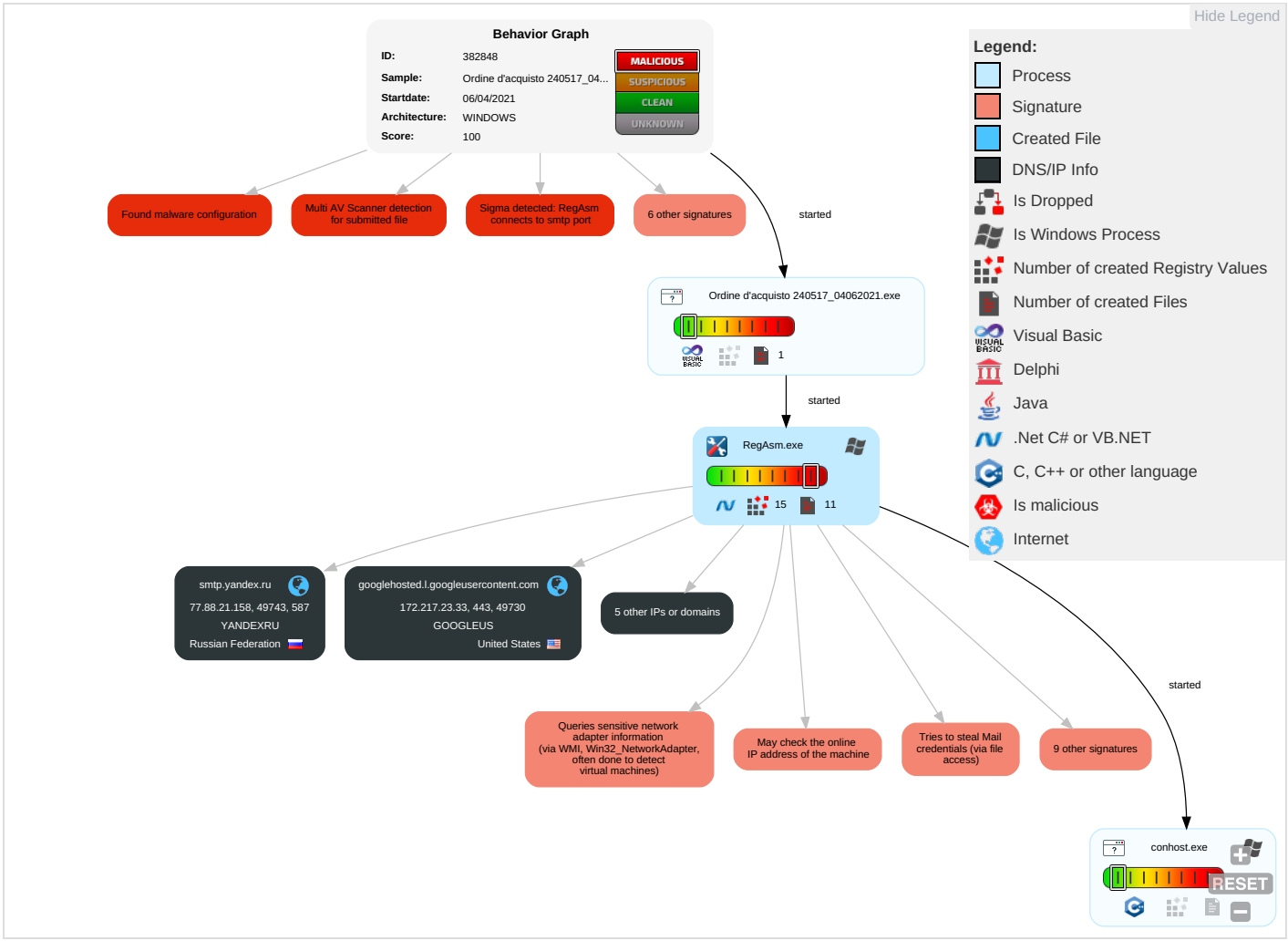
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm Contr
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 4 1 3	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingres Trans
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Obfuscated Files or Information 1	Input Capture 1 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encry Chan
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 2	DLL Side-Loading 1	Security Account Manager	Security Software Discovery 7 3 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-S Port
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 4 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	Non-A Layer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Access Token Manipulation 1	LSA Secrets	Virtualization/Sandbox Evasion 3 4 1	SSH	Clipboard Data 2	Data Transfer Size Limits	Applic Proto
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 2	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comn
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comn Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Proto

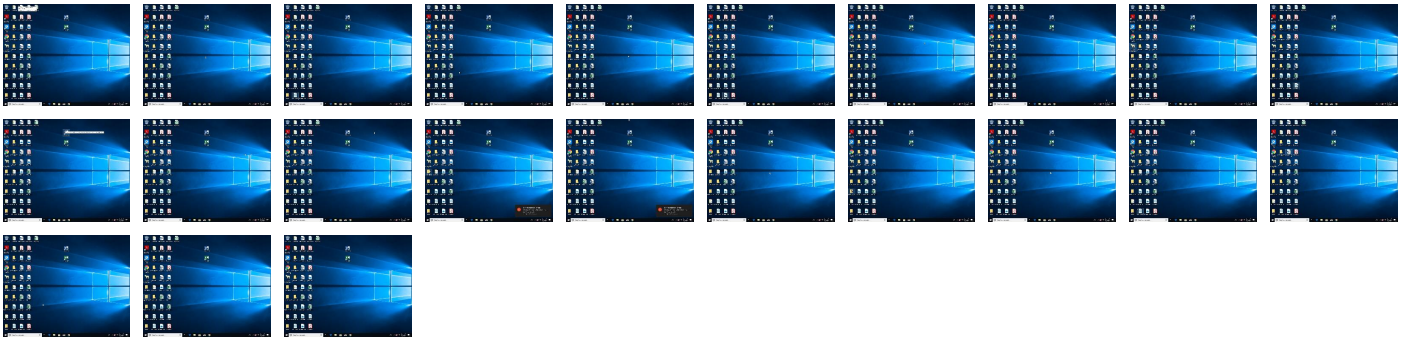
Behavior Graph



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 d'acquisto 240517_04062021.exe	20%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://dex62ukWey0O8Y.net	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	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://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://nafUNc.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	23.21.140.41	true	false		high
smtp.yandex.ru	77.88.21.158	true	false		high
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
smtp.yandex.com	unknown	unknown	false		high
doc-0o-6o-docs.googleusercontent.com	unknown	unknown	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

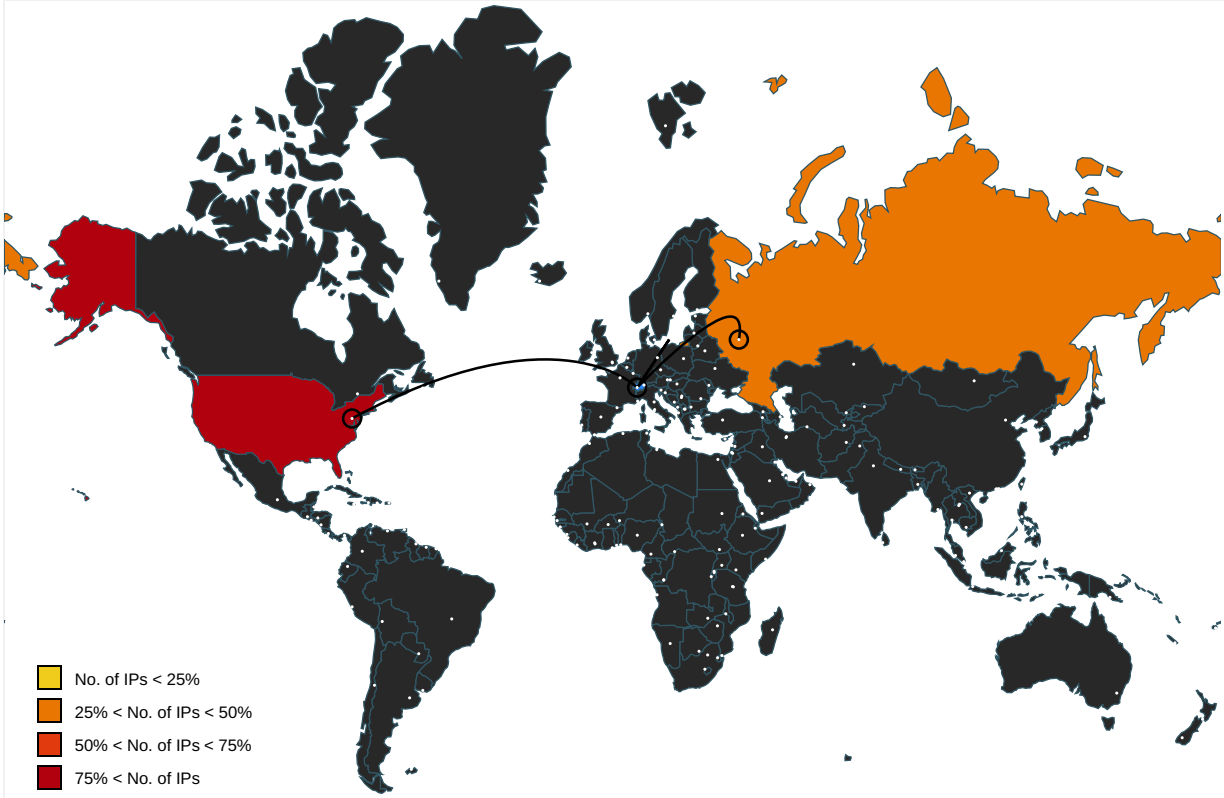
Name	Malicious	Antivirus Detection	Reputation
http://https://dex62ukWey0O8Y.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	RegAsm.exe, 00000012.00000002.758794914.00000000201B3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-0o-6o-docs.googleusercontent.com/	RegAsm.exe, 00000012.00000002.751551309.0000000001580000.00000004.00000020.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	RegAsm.exe, 00000012.00000002.758794914.00000000201B3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	RegAsm.exe, 00000012.00000002.758794914.00000000201B3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	RegAsm.exe, 00000012.00000003.699422242.0000000001618000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-0o-6o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/vkk0ofrs	RegAsm.exe, 00000012.00000003.699511713.00000000015F0000.00000004.00000001.sdmp, RegAsm.exe, 00000012.00000003.699495875.00000000015E8000.00000004.00000001.sdmp	false		high
http://pki.goog/gsr2/GTS1O1.crt0	RegAsm.exe, 00000012.00000003.699422242.0000000001618000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	RegAsm.exe, 00000012.00000003.699422242.0000000001618000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	RegAsm.exe, 00000012.00000003.699422242.0000000001618000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org/(	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false		high
http://https://doc-0o-6o-docs.googleusercontent.com/(	RegAsm.exe, 00000012.00000002.751551309.0000000001580000.00000004.00000020.sdmp	false		high
http://nafUNc.com	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false
23.21.140.41	elb097307-934924932.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382848
Start date:	06.04.2021
Start time:	18:51:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ordine d'acquisto 240517_04062021.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 97.9% (good quality ratio 46.5%) • Quality average: 28.2% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 98% • 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 • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 204.79.197.200, 13.107.21.200, 52.255.188.83, 104.43.139.144, 52.147.198.201, 23.57.80.111, 13.88.21.125, 20.82.210.154, 2.20.142.210, 2.20.142.209, 8.241.90.126, 8.238.85.254, 8.238.85.126, 8.238.35.126, 67.26.83.254, 20.190.159.136, 20.190.159.134, 40.126.31.8, 20.190.159.138, 40.126.31.141, 40.126.31.6, 40.126.31.1, 40.126.31.137, 92.122.213.247, 92.122.213.194, 172.217.20.238, 52.155.217.156, 20.54.26.129 • 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, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:54:38	API Interceptor	1044x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	
	Shandong CIRS Form.exe	Get hash	malicious	Browse	
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	
	Q99Eljz7IT.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.576.12750.exe	Get hash	malicious	Browse	
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	
	PO#ZA3MMA_pdf.exe	Get hash	malicious	Browse	
	kfMrlKSN4F.exe	Get hash	malicious	Browse	
	xjvIB3Wkvk.exe	Get hash	malicious	Browse	
	Placement approval.exe	Get hash	malicious	Browse	
	DHL INV+AWB5501980113371714001.pdf___.exe	Get hash	malicious	Browse	
	83MIDEF8fD.exe	Get hash	malicious	Browse	
	5DhRNTGBUk.exe	Get hash	malicious	Browse	
	WEF2WOfWeo.exe	Get hash	malicious	Browse	
	PAYMENT-FB21026518_10493_PINQ_20210216_PDF.exe	Get hash	malicious	Browse	
	payment advice.pdf.exe	Get hash	malicious	Browse	
23.21.140.41	Jg5HD77Nyo.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	msals.dll	Get hash	malicious	Browse	• api.ipify.org/
	0302_21678088538951.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	Static.dll	Get hash	malicious	Browse	• api.ipify.org/
	RFQ- 978002410.exe	Get hash	malicious	Browse	• api.ipify.org/
	E2ucBaWqpe.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	0210_1723194332604.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	SecuriteInfo.com.Generic.mg.a7d038f64060412d.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	SecuriteInfo.com.BehavesLike.Win32.Generic.pm.exe	Get hash	malicious	Browse	• api.ipify.org/
	0fiasS.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	0fiasS.dll	Get hash	malicious	Browse	• api.ipify.org/
	DyssrxQNS8.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	W0rd.dll	Get hash	malicious	Browse	• api.ipify.org/
	Our New Order Jan 11 2020 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	02_extracted.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	msals.pumpl.dll	Get hash	malicious	Browse	• 107.22.233.72
	0406_37400496097832.doc	Get hash	malicious	Browse	• 54.225.157.230
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 54.225.165.85
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 23.21.48.44
	iUavNne3hp.exe	Get hash	malicious	Browse	• 23.21.76.253
	7919bd3d8ee49fb1803f25bd73682f5fde4164ad65230.exe	Get hash	malicious	Browse	• 50.19.242.215
	45ed95c173fd2df5f05f42c2121698db4484f032344c8.exe	Get hash	malicious	Browse	• 54.235.175.90
	L87N50MbDG.exe	Get hash	malicious	Browse	• 54.225.165.85
	msals.pumpl.dll	Get hash	malicious	Browse	• 23.21.48.44
	z2t2UjaWQ0.exe	Get hash	malicious	Browse	• 54.235.175.90
	30QD3GAnw7.exe	Get hash	malicious	Browse	• 54.225.157.230
	4QVwajpcdz.exe	Get hash	malicious	Browse	• 54.221.253.252
	8uADV5QTqx.exe	Get hash	malicious	Browse	• 50.19.252.36
	scan-100218.docm	Get hash	malicious	Browse	• 54.225.165.85
	FB11.exe	Get hash	malicious	Browse	• 23.21.76.253
	6PKQHgSfco.exe	Get hash	malicious	Browse	• 54.225.157.230
	msals.pumpl.dll	Get hash	malicious	Browse	• 54.243.164.148
	5YB4gJt3c7.exe	Get hash	malicious	Browse	• 54.221.253.252
	t7pQaphHHn.exe	Get hash	malicious	Browse	• 54.235.83.248
	MGTrWXtimL.exe	Get hash	malicious	Browse	• 50.19.242.215
smtp.yandex.ru	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	• 77.88.21.158
	Q99Eljz7IT.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.PackedNET.576.12750.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	PO#ZA3MMA_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	kfMrlKSN4F.exe	Get hash	malicious	Browse	• 77.88.21.158
	xjvIB3Wkvk.exe	Get hash	malicious	Browse	• 77.88.21.158
	Placement approval.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL INV+AWB5501980113371714001.pdf___.exe	Get hash	malicious	Browse	• 77.88.21.158
	83MlDEF8fD.exe	Get hash	malicious	Browse	• 77.88.21.158
	EVpfhXQLoN.exe	Get hash	malicious	Browse	• 77.88.21.158
	0LyaS3hVE5.exe	Get hash	malicious	Browse	• 77.88.21.158
	5DhRNTGBUk.exe	Get hash	malicious	Browse	• 77.88.21.158
	WEF2WOfWeo.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 77.88.21.179
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#ZAEL67012_doc.exe	Get hash	malicious	Browse	• 77.88.21.158
	Q99Eljz7IT.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.PackedNET.576.12750.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	scan-100218.docm	Get hash	malicious	Browse	• 93.158.134.119
	PO#ZA3MMA_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	kfMrlKSN4F.exe	Get hash	malicious	Browse	• 77.88.21.158
	xjvIB3Wkvk.exe	Get hash	malicious	Browse	• 77.88.21.158
	Placement approval.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL INV+AWB5501980113371714001.pdf___.exe	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	83MlDEF8fD.exe	Get hash	malicious	Browse	• 77.88.21.158
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 87.250.250.22
	5DhRNTGBUk.exe	Get hash	malicious	Browse	• 77.88.21.158
AMAZON-AESUS	0406_37400496097832.doc	Get hash	malicious	Browse	• 54.225.157.230
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• 100.24.184.24
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• 52.71.133.130
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 54.225.165.85
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 23.21.48.44
	TT COPY.exe	Get hash	malicious	Browse	• 52.20.218.92
	iUavNne3hp.exe	Get hash	malicious	Browse	• 23.21.76.253
	Reports-018315.xlsm	Get hash	malicious	Browse	• 34.205.48.95
	Reports-018315.xlsm	Get hash	malicious	Browse	• 34.205.48.95
	Reports-018315.xlsm	Get hash	malicious	Browse	• 34.205.48.95
	Financial Doc.html	Get hash	malicious	Browse	• 3.222.43.26
	anchor_x64.exe	Get hash	malicious	Browse	• 52.20.197.7
	PaymentInvoice.exe	Get hash	malicious	Browse	• 34.202.122.77
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	7919bd3d8ee49fb1803f25bd73682f5fde4164ad65230.exe	Get hash	malicious	Browse	• 50.19.242.215
	45ed95c173fd2df5f05f42c2121698db4484f032344c8.exe	Get hash	malicious	Browse	• 54.235.175.90
	L87N50MbDG.exe	Get hash	malicious	Browse	• 54.225.165.85
	befQY8YuZp.exe	Get hash	malicious	Browse	• 52.6.206.192
	38da70826e367c9808b135717c5ea31e4e69ef03eef30.exe	Get hash	malicious	Browse	• 52.6.206.192
	wzdu53.exe	Get hash	malicious	Browse	• 34.231.69.13

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	Purchase Order.exe	Get hash	malicious	Browse	• 23.21.140.41
	visa-eth.com-Setup.exe.danger.exe	Get hash	malicious	Browse	• 23.21.140.41
	PO#.exe	Get hash	malicious	Browse	• 23.21.140.41
	Matrix.exe	Get hash	malicious	Browse	• 23.21.140.41
	Matrix.exe	Get hash	malicious	Browse	• 23.21.140.41
	PowerShell_Input.ps1	Get hash	malicious	Browse	• 23.21.140.41
	OUR PO NO. CWI19150.exe	Get hash	malicious	Browse	• 23.21.140.41
	hostsvc.dll	Get hash	malicious	Browse	• 23.21.140.41
	FN vw Safety 1 & 2.exe	Get hash	malicious	Browse	• 23.21.140.41
	MV TBN.uslfze.exe	Get hash	malicious	Browse	• 23.21.140.41
	Launcher.exe	Get hash	malicious	Browse	• 23.21.140.41
	ORDER.exe	Get hash	malicious	Browse	• 23.21.140.41
	KUWAIT NATIONAL PETROLEUM COMPANY (KNPC) .pdf.exe	Get hash	malicious	Browse	• 23.21.140.41
	TW#9898748948-TZE.exe	Get hash	malicious	Browse	• 23.21.140.41
	Order PONSB 04042021.pdf(939MB).exe	Get hash	malicious	Browse	• 23.21.140.41
	dAbE67VwvD.exe	Get hash	malicious	Browse	• 23.21.140.41
	extremeinjectorv3.7.2.exe	Get hash	malicious	Browse	• 23.21.140.41
	Setup[1].exe	Get hash	malicious	Browse	• 23.21.140.41
	Donate_Caper_Fixed.exe	Get hash	malicious	Browse	• 23.21.140.41
	DCRatBuild.exe	Get hash	malicious	Browse	• 23.21.140.41
37f463bf4616ecd445d4a1937da06e19	catalogue-41.xlsb	Get hash	malicious	Browse	• 172.217.23.33
	ddff.exe	Get hash	malicious	Browse	• 172.217.23.33
	Doc_58YJ54-521DERG701-55YH701.exe	Get hash	malicious	Browse	• 172.217.23.33
	1e#U0414.exe	Get hash	malicious	Browse	• 172.217.23.33
	svhost.exe	Get hash	malicious	Browse	• 172.217.23.33
	beaconxx.exe	Get hash	malicious	Browse	• 172.217.23.33
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 172.217.23.33
	5H957qLghX.exe	Get hash	malicious	Browse	• 172.217.23.33
	FK58.vbs	Get hash	malicious	Browse	• 172.217.23.33
	ZgaBWrz3HH.exe	Get hash	malicious	Browse	• 172.217.23.33
	RFQ#8086A_461A_0000086_300_3550_2021.exe	Get hash	malicious	Browse	• 172.217.23.33
	wzdu53.exe	Get hash	malicious	Browse	• 172.217.23.33
	Opik_lk.exe	Get hash	malicious	Browse	• 172.217.23.33
	document-895003104.xls	Get hash	malicious	Browse	• 172.217.23.33
	Dimmock5.exe	Get hash	malicious	Browse	• 172.217.23.33
	pQlSDfwyYkf.js	Get hash	malicious	Browse	• 172.217.23.33

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Balance payment..exe	Get hash	malicious	Browse	• 172.217.23.33
	pQlSDfwyYkf.js	Get hash	malicious	Browse	• 172.217.23.33
	document-1641473761.xls	Get hash	malicious	Browse	• 172.217.23.33
	ObJRDAd8jZ.exe	Get hash	malicious	Browse	• 172.217.23.33

Dropped Files

No context

Created / dropped Files

\Device\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:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
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):	5.730320746181446
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 d'acquisto 240517_04062021.exe
File size:	122880
MD5:	c81b0ec94cb5bc1e76b355d7e1125a48
SHA1:	ed6f7c97ab1d9cc4dec729c591243ce5285136f1
SHA256:	51b0a2f869f9fe39cc1860dec5ef153af89e00c4a8c3b4c813cdd30cdebc0b11
SHA512:	1ec18a5d8f7c04b95cc52d9edf25eb64654775c66738df2092a0a4e22c246e77de1887e889acbe477c116b861797c8c5126b6fdadf2ad4b8e2c5035328bd4be4
SSDEEP:	3072:MGZBQh3333333333333333333334xDe2IDriZ2wWit+6ihG:t+h3333333333333333333333Yflv5v
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L.....N.....p...`.....(.....@.....

File Icon

Icon Hash:	0ccea09899191898

Static PE Info

General

Entrypoint:	0x401328
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:	0x4EF40617 [Fri Dec 23 04:39:51 2011 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:	efa774b90ad6b9ab8c4fabb031ebe78d

Entrypoint Preview

Instruction
push 00413E20h
call 00007F4A64A05A35h
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
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
wait
mov cl, AAh
rcr dword ptr [esi-03h], cl
inc edx
mov ebx, 5E4FAF49h
mov al, byte ptr [0000DE8Eh]
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc ecx
add byte ptr [esi+66018250h], al
jc 00007F4A64A05AA7h
insd
add byte ptr [esi+0000022Fh], ah
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
sub ch, dh
mov dword ptr [9F8E37B2h], eax
pop es
inc esi
mov ah, 4Fh
wait

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x17614	0x28	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0x484e	.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	0xd4	.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	0x16a04	0x17000	False	0.344864555027	data	6.19080638319	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x18000	0xa88	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x484e	0x5000	False	0.41416015625	data	4.36110878625	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1b2a6	0x25a8	data		
RT_ICON	0x1a1fe	0x10a8	data		
RT_ICON	0x19876	0x988	data		
RT_ICON	0x1940e	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x193d0	0x3e	data		
RT_VERSION	0x19180	0x250	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaVarForInit, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

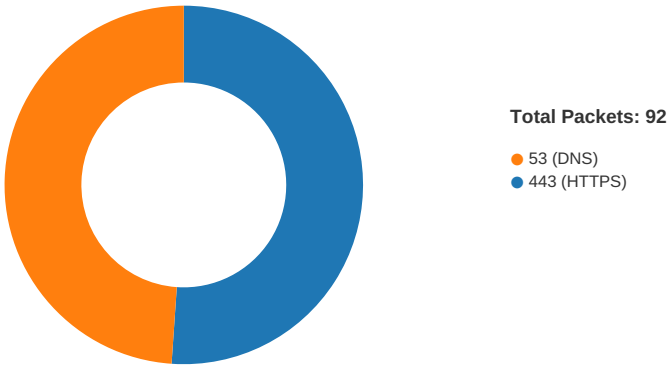
Description	Data
Translation	0x0409 0x04b0
InternalName	Quic2
FileVersion	3.00
CompanyName	Salty
Comments	Salty
ProductName	Salty
ProductVersion	3.00
FileDescription	Salty
OriginalFilename	Quic2.exe

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
Apr 6, 2021 18:54:27.079484940 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.119896889 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.120019913 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.120778084 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.161086082 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.174860954 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.174901009 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.174927950 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.174952030 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.174971104 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.175005913 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.192457914 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.233161926 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.233257055 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.235057116 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.279968977 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.492690086 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.492717981 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.492733002 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.492749929 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.492763042 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.492827892 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.492893934 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.495436907 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.495455027 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.495510101 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.495543957 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.498260021 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.498281002 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.498328924 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.498359919 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.501091003 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.501107931 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.501159906 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.501192093 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.503946066 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.503964901 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.504033089 CEST	49730	443	192.168.2.7	172.217.23.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 18:54:27.504066944 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.506354094 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.506421089 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.507683992 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.507749081 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.533988953 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.534009933 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.534058094 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.534132004 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.535352945 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.535375118 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.535408974 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.535448074 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.538177013 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.538217068 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.538244963 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.538275003 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.541028023 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.541048050 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.541095972 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.541121006 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.543849945 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.543868065 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.543922901 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.543942928 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.546725988 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.546742916 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.546793938 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.546834946 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.549515963 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.549535036 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.549604893 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.549628973 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.552376986 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.552390099 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.552565098 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.555228949 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.555250883 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.555775881 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.557689905 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.557724953 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.557766914 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.557816982 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.560244083 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.560276985 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.560319901 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.560368061 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.562839031 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.562860966 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.562908888 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.562933922 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.565434933 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.565454960 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.565495968 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.565526962 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.568022966 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.568042040 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.568092108 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.568125010 CEST	49730	443	192.168.2.7	172.217.23.33
Apr 6, 2021 18:54:27.570672989 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.570691109 CEST	443	49730	172.217.23.33	192.168.2.7
Apr 6, 2021 18:54:27.570741892 CEST	49730	443	192.168.2.7	172.217.23.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 18:52:27.043487072 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:27.100406885 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:27.198561907 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:27.269776106 CEST	53	57820	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:30.119698048 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:30.165960073 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:31.219028950 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:31.267676115 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:32.870345116 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:32.916373014 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:34.543693066 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:34.589579105 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:35.341646910 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:35.390599966 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:37.283277035 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:37.329569101 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:38.342735052 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:38.388812065 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:39.517055035 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:39.566643953 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:40.420792103 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:40.480279922 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:48.466373920 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:48.514775038 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:52.945040941 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:52.991061926 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:53.745815039 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:53.795988083 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 6, 2021 18:52:54.513411045 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:52:54.569854021 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:00.096822023 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:00.142946959 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:01.047570944 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:01.093612909 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:05.238318920 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:05.296926022 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:12.758459091 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:12.804546118 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:13.713293076 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:13.761545897 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:14.656886101 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:14.703078032 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:15.452898026 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:15.501919031 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:16.298557043 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:16.352917910 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:17.484208107 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:17.530670881 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:18.332710981 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:18.379271984 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:23.422787905 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:23.478924990 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 6, 2021 18:53:24.580077887 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:53:24.636138916 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:05.323687077 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:05.394366026 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:06.239960909 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:06.288866043 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:20.056550980 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:20.118805885 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:25.768981934 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:25.834656000 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:27.002216101 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:27.077100039 CEST	53	51919	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 18:54:38.768755913 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:38.826103926 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:39.389470100 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:39.452634096 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:39.922218084 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:40.024259090 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:40.623907089 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:40.683710098 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:41.008770943 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:41.078684092 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:42.084820986 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:42.139271021 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:43.631331921 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:43.686048985 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:44.168102026 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:44.222723007 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:45.102093935 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:45.159179926 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:46.328105927 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:46.374629974 CEST	53	58367	8.8.8.8	192.168.2.7
Apr 6, 2021 18:54:46.845742941 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:54:46.935544968 CEST	53	60599	8.8.8.8	192.168.2.7
Apr 6, 2021 18:55:57.907483101 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:55:57.955302954 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 6, 2021 18:56:01.264106989 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 6, 2021 18:56:01.318274975 CEST	53	52689	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 18:54:27.002216101 CEST	192.168.2.7	8.8.8.8	0xcff5	Standard query (0)	doc-0o-6o-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.907483101 CEST	192.168.2.7	8.8.8.8	0x58e5	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Apr 6, 2021 18:56:01.264106989 CEST	192.168.2.7	8.8.8.8	0x79cf	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 18:54:05.394366026 CEST	8.8.8.8	192.168.2.7	0x514f	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 18:54:27.077100039 CEST	8.8.8.8	192.168.2.7	0xcff5	No error (0)	doc-0o-6o-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 18:54:27.077100039 CEST	8.8.8.8	192.168.2.7	0xcff5	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.140.41	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.221.253.252	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.48.44	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.175.90	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
Apr 6, 2021 18:55:57.955302954 CEST	8.8.8.8	192.168.2.7	0x58e5	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.76.253	A (IP address)	IN (0x0001)
Apr 6, 2021 18:56:01.318274975 CEST	8.8.8.8	192.168.2.7	0x79cf	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 18:56:01.318274975 CEST	8.8.8.8	192.168.2.7	0x79cf	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	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
Apr 6, 2021 18:54:27.174952030 CEST	172.217.23.33	443	192.168.2.7	49730	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 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 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 6, 2021 18:55:58.246937037 CEST	23.21.140.41	443	192.168.2.7	49742	CN=*.ipify.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Feb 20 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

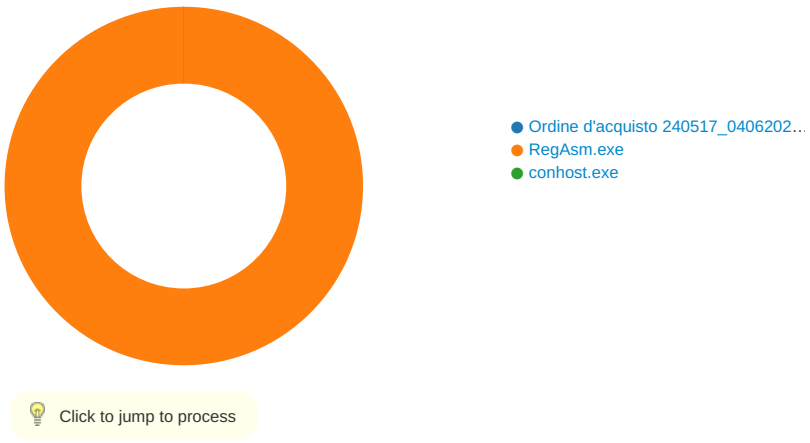
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 6, 2021 18:56:01.762383938 CEST	587	49743	77.88.21.158	192.168.2.7	220 vla1-ef285479e348.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Ordine d'acquisto 240517_04062021.exe PID: 2160 Parent PID: 5796

General

Start time:	18:52:34

Start date:	06/04/2021
Path:	C:\Users\user\Desktop\Ordine d'acquisto 240517_04062021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Ordine d'acquisto 240517_04062021.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	C81B0EC94CB5BC1E76B355D7E1125A48
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
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: 5324 Parent PID: 2160

General

Start time:	18:54:13
Start date:	06/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Ordine d'acquisto 240517_04062021.exe'
Imagebase:	0xd90000
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_GuLoader, Description: Yara detected GuLoader, Source: 00000012.00000002.750710271.0000000001162000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.757510449.000000001DF11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.757510449.000000001DF11000.00000004.00000001.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	1164779	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	1164779	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1164779	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	1164779	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	1164779	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1164779	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	724660AC	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	724660AC	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	724660AC	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	724660AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	1131093	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	1131093	WriteFile

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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	1131093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1131093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	1131093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	1131093	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	1131093	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	1131093	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bbbff251-4388-4706-8d69-3623c990b80a	unknown	4096	success or wait	1	1131093	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	1131093	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	1131093	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	1131093	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1044 Parent PID: 5324

General

Start time:	18:54:14
Start date:	06/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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