ID: 404980
Sample Name: ordine n#U00b0 276.exe
Cookbook: default.jbs
Time: 17:00:25
Date: 05/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

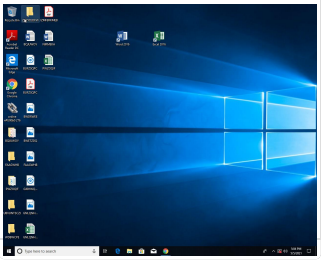
Analysis Report ordine n#U00b0 276.exe

Overview

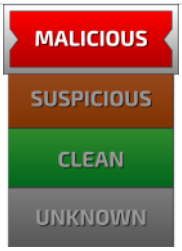
General Information

Sample Name:	ordine n#U00b0 276.exe
Analysis ID:	404980
MD5:	10f03c95ba280cd..
SHA1:	c24232721d7aefe.
SHA256:	11f63d2fda1055a..
Infos:	

Most interesting Screenshot:



Detection



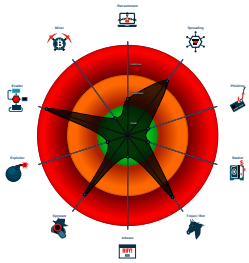
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- 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…

Classification



Startup

- **System is w10x64**
- ordine n#U00b0 276.exe (PID: 6992 cmdline: 'C:\Users\user\Desktop\ordine n#U00b0 276.exe' MD5: 10F03C95BA280CD5A82146269F89CA9D)
  - RegAsm.exe (PID: 2588 cmdline: 'C:\Users\user\Desktop\ordine n#U00b0 276.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 6592 cmdline: 'C:\Users\user\Desktop\ordine n#U00b0 276.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 6412 cmdline: 'C:\Users\user\Desktop\ordine n#U00b0 276.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 6468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "MS4FGDMtaO",
  "URL: ": "http://5Z6zzpV4pHjt.com",
  "To: ": "",
  "ByHost: ": "smtp.fil-net.com:587",
  "Password: ": "OLotoUPgHE9Y",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.638126535.000000000040C000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x1298:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000000.00000002.749114091.000000000040C000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x1298:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB

Copyright Joe Security LLC 2021

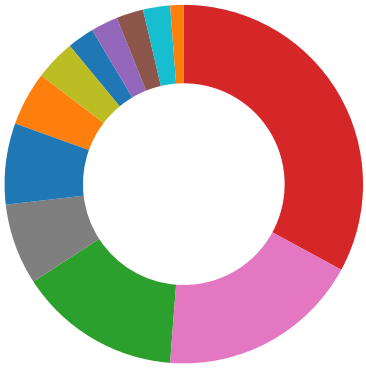
Source	Rule	Description	Author	Strings
00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 6412	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

Networking:

Sigma detected: RegAsm connects to smtp port

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Copyright Joe Security LLC 2021

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

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)

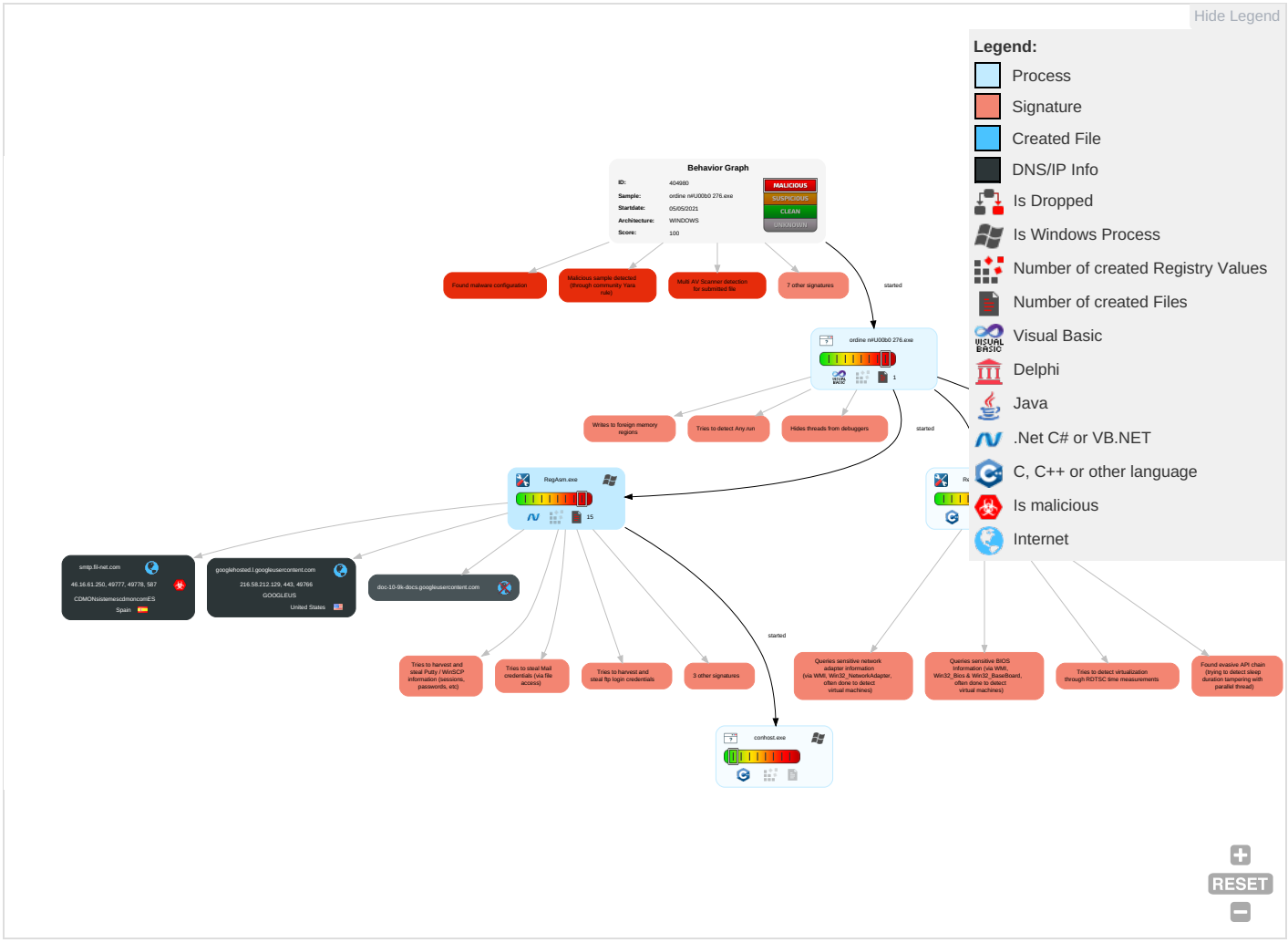
Remote Access Functionality:

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	26%	Virustotal		Browse
ordine n#U00b0 276.exe	36%	ReversingLabs	Win32.Trojan.Mucc	

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://5Z6zzpV4pHjt.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://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://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://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://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	Avira URL Cloud	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://pki.goog/gsr1/gsr1.crt02	0%	Avira URL Cloud	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://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
smtp.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

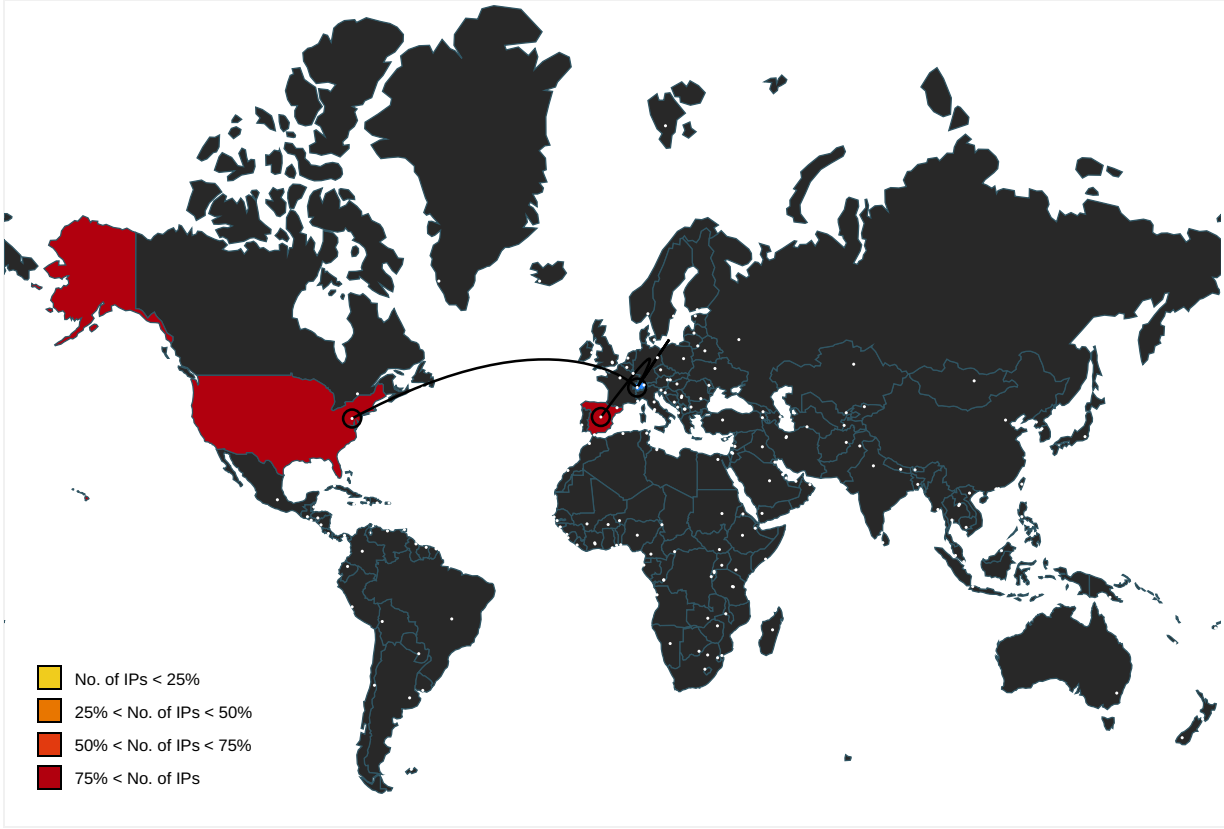
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://5Z6zzpV4pHjt.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr1/gsr1.crl0;	RegAsm.exe, 00000007.00000003.976218379.0000000001036000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doc-10-9k-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/uf4tta3o	RegAsm.exe, 00000007.00000002.1031722866.000000000100D000.00000004.00000020.sdmp	false		high
http://cps.letsencrypt.org0	RegAsm.exe, 00000007.00000002.1035500549.000000001DBB8000.00000004.00000001.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, 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-10-9k-docs.googleusercontent.com/G	RegAsm.exe, 00000007.00000002.1031722866.000000000100D000.00000004.00000020.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	RegAsm.exe, 00000007.00000002.1031722866.000000000100D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.org0	RegAsm.exe, 00000007.00000002.1035500549.000000001DBB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	RegAsm.exe, 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://crl.pki.goog/gtsr1/gtsr1.crl0W	RegAsm.exe, 00000007.00000002.1031747956.000000000103D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	RegAsm.exe, 00000007.00000002.1031722866.000000000100D000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr1/gsr1.crt02	RegAsm.exe, 00000007.00000003.976218379.0000000001036000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	RegAsm.exe, 00000007.00000002.1031709055.0000000000FEF000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	RegAsm.exe, 00000007.00000002.1031747956.000000000103D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl0	RegAsm.exe, 00000007.00000002.1031747956.000000000103D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doc-10-9k-docs.googleusercontent.com/	RegAsm.exe, 00000007.00000002.1031722866.000000000100D000.00000004.00000020.sdmp	false		high
http://https://api.ipify.org%	RegAsm.exe, 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://mGfDbY.com	RegAsm.exe, 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	RegAsm.exe, 00000007.00000002.1035500549.000000001DBB8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0%	RegAsm.exe, 00000007.00000002.1035500549.000000001DBB8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gts1c3.der0	RegAsm.exe, 00000007.00000002.1031747956.000000000103D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/repo/certs/gtsr1.der04	RegAsm.exe, 00000007.00000002.1031747956.000000000103D000.00000004.00000001.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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404980
Start date:	05.05.2021
Start time:	17:00:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 58s
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:	20
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@8/2@3/2

Copyright Joe Security LLC 2021

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 3.5% (good quality ratio 1.7%) • Quality average: 32.8% • Quality standard deviation: 37%
HCA Information:	• Successful, ratio: 96% • 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): 52.113.196.254, 104.43.139.144, 13.107.3.254, 13.107.246.254, 168.61.161.212, 52.255.188.83, 20.50.102.62, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 142.250.185.78, 13.107.4.50, 93.184.220.29, 20.82.209.183 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, s-ring.msedge.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, 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, elasticShed.au.au-msedge.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, afdap.au.au-msedge.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, au.au-msedge.net, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, crl3.digicert.com, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, t-ring.t-9999.t-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:02:05	API Interceptor	1130x 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	ordine n#U00b0 276.exe	Get hash	malicious	Browse	
	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	ordine n#U00b0 276.exe	Get hash	malicious	Browse	• 46.16.61.250
	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
	qm7JU84PFgfqvgs.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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	tncGQWIL6H.exe	Get hash	malicious	Browse	• 216.58.212.129
	CT3nHWujrM.exe	Get hash	malicious	Browse	• 216.58.212.129
	build.exe	Get hash	malicious	Browse	• 216.58.212.129
	eDg92MgQgh.exe	Get hash	malicious	Browse	• 216.58.212.129
	c2de9c66_by_Libranalysis.exe	Get hash	malicious	Browse	• 216.58.212.129
	SecuriteInfo.com.Mal.Generic-S.21221.exe	Get hash	malicious	Browse	• 216.58.212.129
	SecuriteInfo.com.W32.AIDetect.malware2.12980.exe	Get hash	malicious	Browse	• 216.58.212.129
	proforma invoice No. 42037,pdf.exe	Get hash	malicious	Browse	• 216.58.212.129
	jt50apTCUS.docx	Get hash	malicious	Browse	• 216.58.212.129
	SecuriteInfo.com.Heur.32597.xls	Get hash	malicious	Browse	• 216.58.212.129
	SecuriteInfo.com.ArtemisTrojan.25081.exe	Get hash	malicious	Browse	• 216.58.212.129
	Update_new32.exe	Get hash	malicious	Browse	• 216.58.212.129
	PaymentAdvice - Copy.htm	Get hash	malicious	Browse	• 216.58.212.129
	INVOICE & STATEMENTS -COPY.htm	Get hash	malicious	Browse	• 216.58.212.129
	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 216.58.212.129
	Proforma adjunta N#U00ba 42037,pdf.exe	Get hash	malicious	Browse	• 216.58.212.129
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 216.58.212.129
	7D1E.exe	Get hash	malicious	Browse	• 216.58.212.129

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5.exe	Get hash	malicious	Browse	• 216.58.212.129
	ordine n#U00b0 276.exe	Get hash	malicious	Browse	• 216.58.212.129

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\1sxxov2t.dy0\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..... ....

\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):	4.764868199016906
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

Copyright Joe Security LLC 2021

General

SHA1:	c24232721d7aefe2c013b9642e0ab7db8007e48a
SHA256:	11f63d2fda1055ac66a71cb539c9d5ff66fd79f473e19171fd8f663e2c4979b9
SHA512:	4b537aec0eee96b506ac63fcbdffc4e1e2ac231ca8d5136cfe7a67e84ac5643424d7090ae88ddb3e809d94272fa15edb20ed70964076fbf05260dceabac5ab76
SSDEEP:	1536:kh70hrnoEdQNvX1/o3IAEmYY6qbtug0Oj1o/:kl0tnoO81/4OYZJGO5S
File Content Preview:	MZ.....@.....!..L.!This 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 00007FF0B45C6375h
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
or eax, CA69BFC2h
inc edi
lodsb
jmp far 22F3h : 4FE1EAFFh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al

Instruction
or eax, 270A0D0Ah
dec ebp
push ebp
dec esi
push edx
inc ebp
push ecx
push ebp
dec ecx
push esp
add byte ptr [0A0D200Ah], cl
or eax, 0000000Ah
add bh, bh
int3
xor dword ptr [eax], eax
sub byte ptr [ecx-1Bh], bl
aaa
int3
std
mov dword ptr [F68E487Eh], eax
pop ebx
or eax, AFD57F95h
jl 00007FF0B45C635Dh
test eax, E711F84Fh
dec edi
pushfd
adc dword ptr [esi+48E65169h], ebx
sub al, 3Ah
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor eax, 470000B5h
add al, byte ptr [eax]
add byte ptr [eax], al
add al, 00h
insd
popad
jc 00007FF0B45C63EFh
add byte ptr [43000501h], cl
dec edi
push esi
inc ebp

Instruction
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	_CIcos, _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, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaStrToAnsi, __vbaFpI4, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	OPARBE
FileVersion	1.00
CompanyName	Mummys Technology
Comments	Mummys Technology
ProductName	Mummys Technology
ProductVersion	1.00
FileDescription	Mummys Technology
OriginalFilename	OPARBE.exe

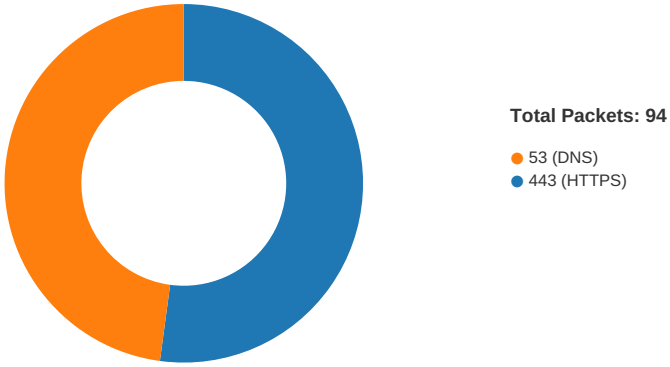
Possible Origin

Copyright Joe Security LLC 2021

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 5, 2021 17:01:59.135849953 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.178808928 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.179025888 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.181459904 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.222148895 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.229161978 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.229185104 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.229208946 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.229227066 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.229264021 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.229285002 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.229300976 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.229361057 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.229367018 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.282052040 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.323013067 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.323106050 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.324456930 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.370457888 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.583566904 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.583615065 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.583657026 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.583673000 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.583693981 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.583713055 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.584429026 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.584486008 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.584516048 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.584552050 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.587285995 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.587330103 CEST	443	49766	216.58.212.129	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2021 17:01:59.587373972 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.587399960 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.590076923 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.590120077 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.590176105 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.590215921 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.592981100 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.593024015 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.593056917 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.593084097 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.595828056 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.595870972 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.595913887 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.595940113 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.598767042 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.598818064 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.598855972 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.598871946 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.601583958 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.601624966 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.601670027 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.601696968 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.624628067 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.624690056 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.624756098 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.624783993 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.625996113 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.626038074 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.626087904 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.626105070 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.628684044 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.628725052 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.628751993 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.628784895 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.631668091 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.631711960 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.631751060 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.631772041 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.634428024 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.634474039 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.634510994 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.634531021 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.637259007 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.637299061 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.637339115 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.637358904 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.640144110 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.640194893 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.640223026 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.640248060 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.643033981 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.643075943 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.643100023 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.643137932 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.645854950 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.645896912 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.645924091 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.645945072 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.648542881 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.648590088 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.648606062 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.648638964 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.650917053 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.650959969 CEST	443	49766	216.58.212.129	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2021 17:01:59.650995970 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.651015043 CEST	49766	443	192.168.2.4	216.58.212.129
May 5, 2021 17:01:59.653450012 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.653491974 CEST	443	49766	216.58.212.129	192.168.2.4
May 5, 2021 17:01:59.653515100 CEST	49766	443	192.168.2.4	216.58.212.129

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2021 17:01:03.690494061 CEST	58028	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:03.739600897 CEST	53	58028	8.8.8.8	192.168.2.4
May 5, 2021 17:01:03.983526945 CEST	53097	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:04.033890963 CEST	53	53097	8.8.8.8	192.168.2.4
May 5, 2021 17:01:04.040508032 CEST	49257	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:04.092152119 CEST	53	49257	8.8.8.8	192.168.2.4
May 5, 2021 17:01:04.267797947 CEST	62389	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:04.319478989 CEST	53	62389	8.8.8.8	192.168.2.4
May 5, 2021 17:01:05.427966118 CEST	49910	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:05.481971025 CEST	53	49910	8.8.8.8	192.168.2.4
May 5, 2021 17:01:07.142071962 CEST	55854	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:07.193872929 CEST	53	55854	8.8.8.8	192.168.2.4
May 5, 2021 17:01:08.334923029 CEST	64549	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:08.387028933 CEST	53	64549	8.8.8.8	192.168.2.4
May 5, 2021 17:01:09.247404099 CEST	63153	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:09.304781914 CEST	53	63153	8.8.8.8	192.168.2.4
May 5, 2021 17:01:10.437279940 CEST	52991	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:10.487998009 CEST	53	52991	8.8.8.8	192.168.2.4
May 5, 2021 17:01:11.466536999 CEST	53700	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:11.515269041 CEST	53	53700	8.8.8.8	192.168.2.4
May 5, 2021 17:01:12.525285959 CEST	51726	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:12.574664116 CEST	53	51726	8.8.8.8	192.168.2.4
May 5, 2021 17:01:13.431174040 CEST	56794	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:13.480317116 CEST	53	56794	8.8.8.8	192.168.2.4
May 5, 2021 17:01:14.339106083 CEST	56534	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:14.395970106 CEST	53	56534	8.8.8.8	192.168.2.4
May 5, 2021 17:01:15.286114931 CEST	56627	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:15.346343994 CEST	53	56627	8.8.8.8	192.168.2.4
May 5, 2021 17:01:16.277062893 CEST	56621	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:16.327723026 CEST	53	56621	8.8.8.8	192.168.2.4
May 5, 2021 17:01:17.205954075 CEST	63116	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:17.257935047 CEST	53	63116	8.8.8.8	192.168.2.4
May 5, 2021 17:01:18.124769926 CEST	64078	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:18.173777103 CEST	53	64078	8.8.8.8	192.168.2.4
May 5, 2021 17:01:19.120851040 CEST	64801	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:19.171756029 CEST	53	64801	8.8.8.8	192.168.2.4
May 5, 2021 17:01:19.999878883 CEST	61721	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:20.048785925 CEST	53	61721	8.8.8.8	192.168.2.4
May 5, 2021 17:01:21.745997906 CEST	51255	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:21.796354055 CEST	53	51255	8.8.8.8	192.168.2.4
May 5, 2021 17:01:27.584459066 CEST	61522	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:27.635942936 CEST	53	61522	8.8.8.8	192.168.2.4
May 5, 2021 17:01:34.861730099 CEST	52337	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:34.922353029 CEST	53	52337	8.8.8.8	192.168.2.4
May 5, 2021 17:01:39.237457991 CEST	55046	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:39.297370911 CEST	53	55046	8.8.8.8	192.168.2.4
May 5, 2021 17:01:52.846262932 CEST	49612	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:52.994647980 CEST	53	49612	8.8.8.8	192.168.2.4
May 5, 2021 17:01:53.728523016 CEST	49285	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:53.861010075 CEST	53	49285	8.8.8.8	192.168.2.4
May 5, 2021 17:01:54.406605959 CEST	50601	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:54.464427948 CEST	53	50601	8.8.8.8	192.168.2.4
May 5, 2021 17:01:54.866115093 CEST	60875	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:54.928509951 CEST	53	60875	8.8.8.8	192.168.2.4
May 5, 2021 17:01:55.453356028 CEST	56448	53	192.168.2.4	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2021 17:01:55.512281895 CEST	53	56448	8.8.8.8	192.168.2.4
May 5, 2021 17:01:55.862121105 CEST	59172	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:55.927783012 CEST	53	59172	8.8.8.8	192.168.2.4
May 5, 2021 17:01:56.062057972 CEST	62420	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:56.110846043 CEST	53	62420	8.8.8.8	192.168.2.4
May 5, 2021 17:01:56.558742046 CEST	60579	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:56.621804953 CEST	53	60579	8.8.8.8	192.168.2.4
May 5, 2021 17:01:57.367877007 CEST	50183	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:57.429572105 CEST	53	50183	8.8.8.8	192.168.2.4
May 5, 2021 17:01:57.893667936 CEST	61531	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:57.950640917 CEST	53	61531	8.8.8.8	192.168.2.4
May 5, 2021 17:01:58.288770914 CEST	49228	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:58.346333981 CEST	53	49228	8.8.8.8	192.168.2.4
May 5, 2021 17:01:58.408456087 CEST	59794	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:58.466267109 CEST	53	59794	8.8.8.8	192.168.2.4
May 5, 2021 17:01:58.743185043 CEST	55916	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:59.041968107 CEST	53	55916	8.8.8.8	192.168.2.4
May 5, 2021 17:01:59.065201998 CEST	52752	53	192.168.2.4	8.8.8.8
May 5, 2021 17:01:59.133631945 CEST	53	52752	8.8.8.8	192.168.2.4
May 5, 2021 17:02:10.696511984 CEST	60542	53	192.168.2.4	8.8.8.8
May 5, 2021 17:02:10.772339106 CEST	53	60542	8.8.8.8	192.168.2.4
May 5, 2021 17:02:10.826412916 CEST	60689	53	192.168.2.4	8.8.8.8
May 5, 2021 17:02:10.900535107 CEST	53	60689	8.8.8.8	192.168.2.4
May 5, 2021 17:02:15.434143066 CEST	64206	53	192.168.2.4	8.8.8.8
May 5, 2021 17:02:15.493031979 CEST	53	64206	8.8.8.8	192.168.2.4
May 5, 2021 17:02:43.400177956 CEST	50904	53	192.168.2.4	8.8.8.8
May 5, 2021 17:02:43.460458994 CEST	53	50904	8.8.8.8	192.168.2.4
May 5, 2021 17:02:44.388366938 CEST	57525	53	192.168.2.4	8.8.8.8
May 5, 2021 17:02:44.457710981 CEST	53	57525	8.8.8.8	192.168.2.4
May 5, 2021 17:02:46.015604973 CEST	53814	53	192.168.2.4	8.8.8.8
May 5, 2021 17:02:46.088701010 CEST	53	53814	8.8.8.8	192.168.2.4
May 5, 2021 17:03:28.515350103 CEST	53418	53	192.168.2.4	8.8.8.8
May 5, 2021 17:03:28.581509113 CEST	53	53418	8.8.8.8	192.168.2.4
May 5, 2021 17:03:29.291996956 CEST	62833	53	192.168.2.4	8.8.8.8
May 5, 2021 17:03:29.367165089 CEST	53	62833	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2021 17:01:59.065201998 CEST	192.168.2.4	8.8.8.8	0xbabd	Standard query (0)	doc-10-9k-docs.googleusercontent.com	A (IP address)	IN (0x0001)
May 5, 2021 17:03:28.515350103 CEST	192.168.2.4	8.8.8.8	0xff76	Standard query (0)	smtp.fil-net.com	A (IP address)	IN (0x0001)
May 5, 2021 17:03:29.291996956 CEST	192.168.2.4	8.8.8.8	0x726d	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
May 5, 2021 17:01:59.133631945 CEST	8.8.8.8	192.168.2.4	0xbabd	No error (0)	doc-10-9k-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 5, 2021 17:01:59.133631945 CEST	8.8.8.8	192.168.2.4	0xbabd	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)
May 5, 2021 17:03:28.581509113 CEST	8.8.8.8	192.168.2.4	0xff76	No error (0)	smtp.fil-net.com		46.16.61.250	A (IP address)	IN (0x0001)
May 5, 2021 17:03:29.367165089 CEST	8.8.8.8	192.168.2.4	0x726d	No error (0)	smtp.fil-net.com		46.16.61.250	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
May 5, 2021 17:01:59.229300976 CEST	216.58.212.129	443	192.168.2.4	49766	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 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jul 06 12:41:16 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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 CEST 2027		
					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		

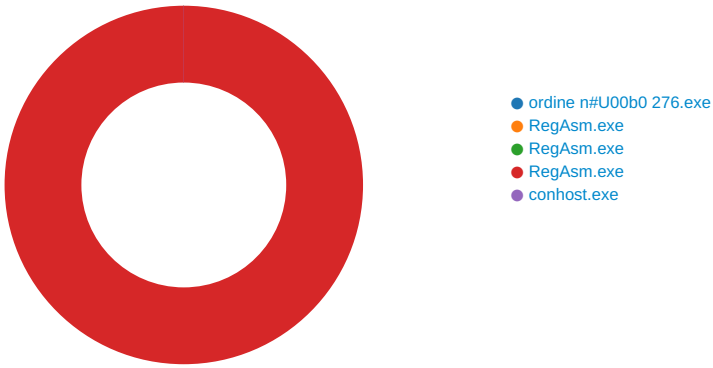
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 5, 2021 17:03:28.999555111 CEST	587	49777	46.16.61.250	192.168.2.4	220 vxsys-smtpclusterma-05.srv.cat ESMTP
May 5, 2021 17:03:29.495770931 CEST	587	49778	46.16.61.250	192.168.2.4	220 vxsys-smtpclusterma-03.srv.cat ESMTP
May 5, 2021 17:03:29.496217966 CEST	49778	587	192.168.2.4	46.16.61.250	EHLO 131521
May 5, 2021 17:03:29.579648972 CEST	587	49778	46.16.61.250	192.168.2.4	250-vxsys-smtpclusterma-03.srv.cat 250-PIPELINING 250-SIZE 47185920 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 5, 2021 17:03:29.579931021 CEST	49778	587	192.168.2.4	46.16.61.250	STARTTLS
May 5, 2021 17:03:29.642256975 CEST	587	49778	46.16.61.250	192.168.2.4	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



Copyright Joe Security LLC 2021

Click to jump to process

System Behavior

Analysis Process: ordine n#U00b0 276.exe PID: 6992 Parent PID: 5888

General

Start time:	17:01:09
Start date:	05/05/2021
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: 00000000.00000000.638126535.000000000040C000.00000020.00020000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.749114091.000000000040C000.00000020.00020000.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: 2588 Parent PID: 6992

General

Start time:	17:01:35
Start date:	05/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\ordine n#U00b0 276.exe'
Imagebase:	0x360000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 6592 Parent PID: 6992

General

Start time:	17:01:36
Start date:	05/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\ordine n#U00b0 276.exe'
Imagebase:	0x2d0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 6412 Parent PID: 6992

General

Start time:	17:01:36
Start date:	05/05/2021
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:	0x880000
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: 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.1035317634.000000001DA61000.00000004.00000001.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	D02C53	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	D02C53	InternetOpenUrlA
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	D02C53	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	D02C53	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	D02C53	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	D02C53	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
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\1sxxov2t.dy0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	CF34F9	CreateDirectoryW
C:\Users\user\AppData\Roaming\1sxxov2t.dy0\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	CF34F9	CreateDirectoryW
C:\Users\user\AppData\Roaming\1sxxov2t.dy0\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	CF34F9	CreateDirectoryW
C:\Users\user\AppData\Roaming\1sxxov2t.dy0\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	CF35BC	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1sxxov2t.dy0\Chrome\Default\Cookies	success or wait	1	CF3676	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	CF0EAF	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	CF0EAF	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1sxxov2t.dy0\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	CF35BC	CopyFileW

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	CF0EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	CF0EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	CF0EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	CF0EAF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	CF0EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	CF0EAF	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\12d5b7df-e012-4d89-ba77-431faa4f341c	unknown	4096	success or wait	1	CF0EAF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	CF0EAF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	CF0EAF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	CF0EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	CF0EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	CF0EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	CF0EAF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	CF0EAF	ReadFile
C:\Users\user\AppData\Roaming\1sxxov2t.dy0\Chrome\Default\Cookies	unknown	16384	success or wait	2	CF0EAF	ReadFile

Analysis Process: conhost.exe PID: 6468 Parent PID: 6412

General

Copyright Joe Security LLC 2021

Start time:	17:01:37
Start date:	05/05/2021
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