ID: 680480
Sample Name: PO#8155
PC_ETG000137 CONT WT
Ashwagandha 07-08-2022
WRDOOO1.exe
Cookbook: default.jbs
Time: 17:18:13
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

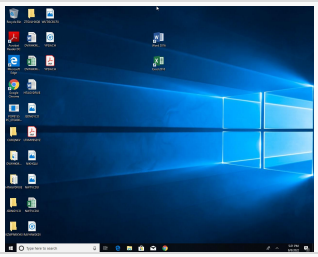
Windows Analysis Report

PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe

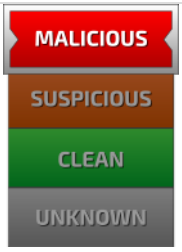
Overview

General Information

Sample Name:	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe
Analysis ID:	680480
MD5:	62881881e70f22..
SHA1:	e714f5f755f77c2..
SHA256:	b6b281587ead88.
Tags:	AgentTesla exe
Infos:	



Detection



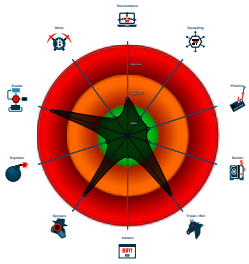
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe (PID: 6172 cmdline: "C:\Users\user\Desktop\PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe" MD5: 62881881E70F226D8C23A01CDC7287DD)
  - RegSvcs.exe (PID: 6444 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Host": "ftp://ftp.artrsllc.com/",
  "Username": "whitemoney11@artrsllc.com",
  "Password": "aJ{?30{raou;"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.367436517.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.367436517.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.367436517.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x3005f:$a13: get_DnsResolver • 0x2e86f:$a20: get_LastAccessed • 0x309dd:$a27: set_InternalServerPort • 0x30d0f:$a30: set_GuidMasterKey • 0x2e976:$a33: get_Clipboard • 0x2e984:$a34: get_Keyboard • 0x2fc7c:$a35: get_ShiftKeyDown • 0x2fc8d:$a36: get_AltKeyDown • 0x2e991:$a37: get_Password • 0x2f42c:$a38: get_PasswordHash • 0x3045f:$a39: get_DefaultCredentials
00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe.40487a8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe.40487a8.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe.40487a8.2.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d28:$s10: logins • 0x3078f:$s11: credential • 0x2cd76:$g1: get_Clipboard • 0x2cd84:$g2: get_Keyboard • 0x2cd91:$g3: get_Password • 0x2e06c:$g4: get_CtrlKeyDown • 0x2e07c:$g5: get_ShiftKeyDown • 0x2e08d:$g6: get_AltKeyDown
0.2.PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe.40487a8.2.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e45f:$a13: get_DnsResolver • 0x2cc6f:$a20: get_LastAccessed • 0x2eddd:$a27: set_InternalServerPort • 0x2f10f:$a30: set_GuidMasterKey • 0x2cd76:$a33: get_Clipboard • 0x2cd84:$a34: get_Keyboard • 0x2e07c:$a35: get_ShiftKeyDown • 0x2e08d:$a36: get_AltKeyDown • 0x2cd91:$a37: get_Password • 0x2d82c:$a38: get_PasswordHash • 0x2e85f:$a39: get_DefaultCredentials
4.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

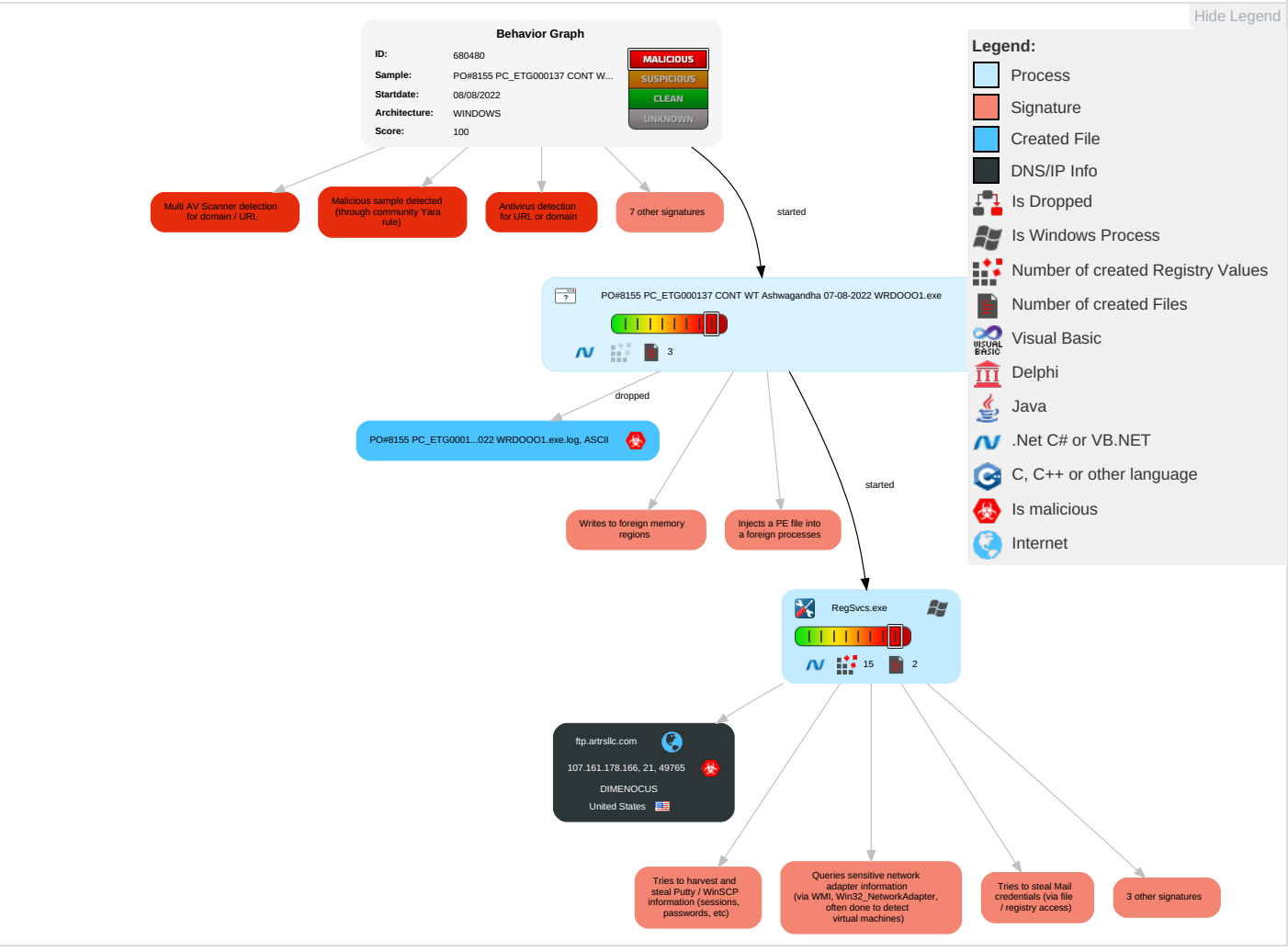
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	2 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	1 Exfiltration Over Alternative Protocol	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	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 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 1 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)	2 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User 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	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

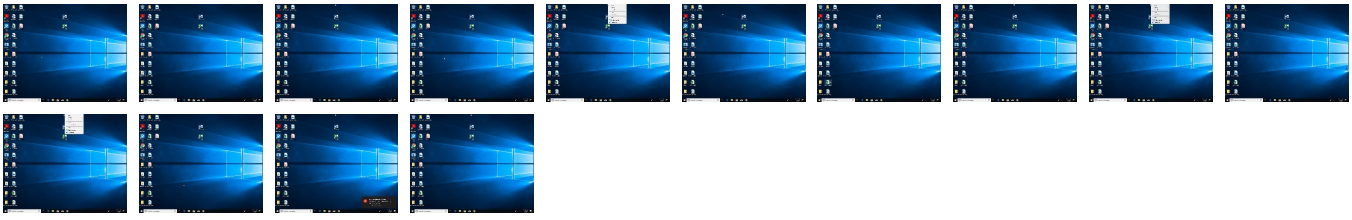
Behavior Graph



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
PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe	52%	Virustotal		Browse
PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe	12%	Metadefender		Browse
PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
ftp.artrsllc.com	15%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ZhDbKe.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://ftp.artrsllc.com	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://ftp://ftp.artrsllc.com/whitemoney11	100%	Avira URL Cloud	malware	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://A2hAjAc0p86apb.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.artrsllc.com	107.161.178.166	true	true	• 15%, Virustotal, Browse	unknown

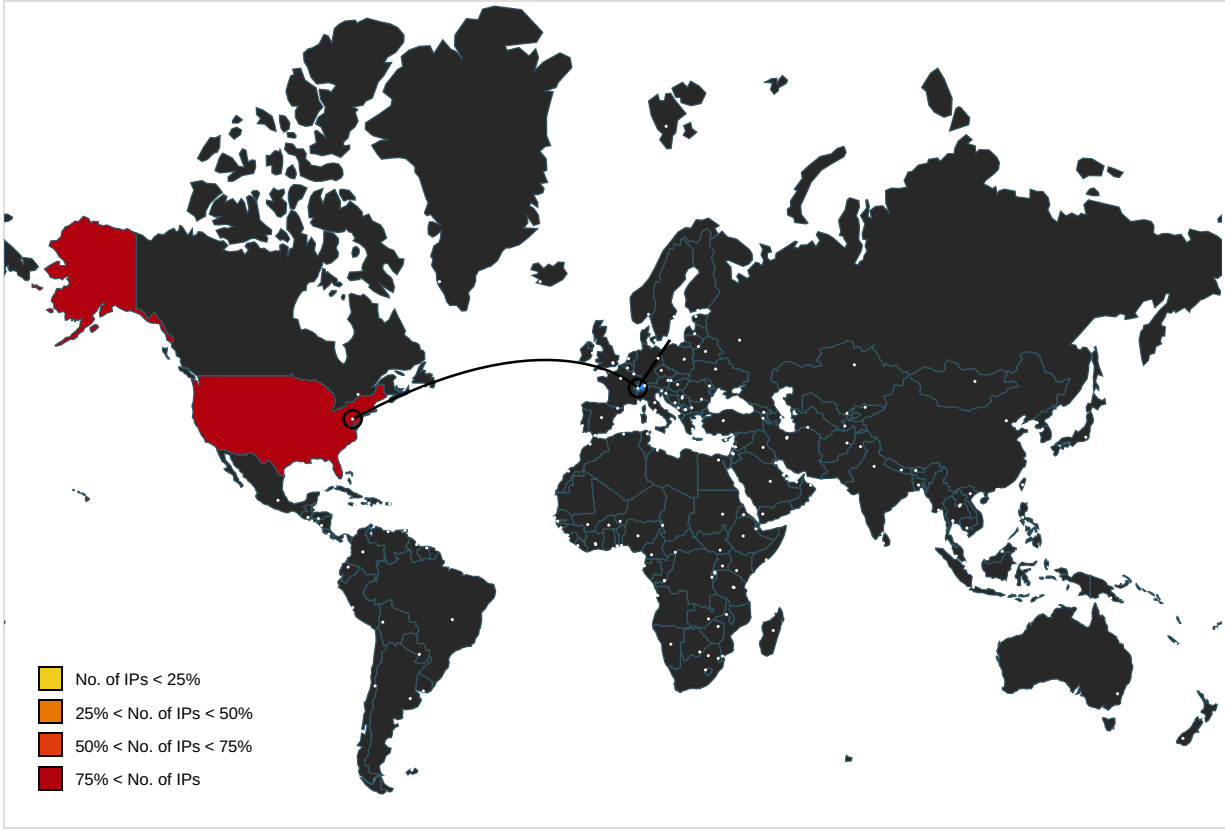
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ZhDbKe.com	RegSvcs.exe, 00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000003.345901174.0000000005C54000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cne	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000003.345835240.0000000005C54000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000003.345471162.0000000005C59000.00000004.00000800.00020000.00000000.sdmp, PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000003.345431980.0000000005C51000.00000004.00000800.00020000.00000000.sdmp, PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000003.345410083.0000000005C50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ftp.artrsllc.com	RegSvcs.exe, 00000004.00000002.614649601.00000000036AD000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ftp://ftp.artrsllc.com/whitemoney11	RegSvcs.exe, 00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://fontfabrik.com	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp, PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.38582 7875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comgrito	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.372509100.00000000013C7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.384454676.0000000006F32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegSvcs.exe, 00000004.00000002.614573955.000000000369F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe, 00000000.00000002.385827875.000000000701C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://A2hAjAc0p86apb.com	RegSvcs.exe, 00000004.00000002.614573955.000000000369F000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000004.00000003.398330369.00000000013D4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.161.178.166	ftp.artrsllc.com	United States		33182	DIMENOCUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680480
Start date and time: 08/08/202217:18:13	2022-08-08 17:18:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- 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
17:19:29	API Interceptor	1x Sleep call for process: PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe modified
17:19:39	API Interceptor	695x Sleep call for process: RegSvcs.exe modified

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\Microsoft\CLR_v4.0_32\UsageLogs\PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe.log

Process:	C:\Users\user\Desktop\PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false

SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.406669599964873
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe
File size:	880128
MD5:	62881881e70f226d8c23a01cdc7287dd
SHA1:	e714f5f755f77c24cc7ff4b8a593a3fe76cabeb7
SHA256:	b6b281587ead8881ceb6f0f6ba621f2d0c40e120e3314dcac601cc7f5877b3da
SHA512:	ae0cdefc3ae27ee559dd261eef14130210b243a37fd51d0cb3abb67f273cd9f3280adcaeeb8d544f6ff32c0d0f1bc8b6b8e4a9092f48e6cb0ac7cb27f130e4d3
SSDEEP:	24576:Jgrg0jwi9BHtgL1NSin5uq5n11fDARrII:qg0RBN8146uknrfDA
TLSH:	3F155CA9319071DFD927CA72CAA81C34EA517C77A71B921794633198DB3E987DF200B3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....P.b.....P..X.....v... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d76ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F05019 [Sun Aug 7 23:51:53 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd7654	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x11f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd56b4	0xd5800	False	0.7426186054596019	data	7.410029605740152	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x11f0	0x1200	False	0.3934461805555556	data	5.04651876632834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

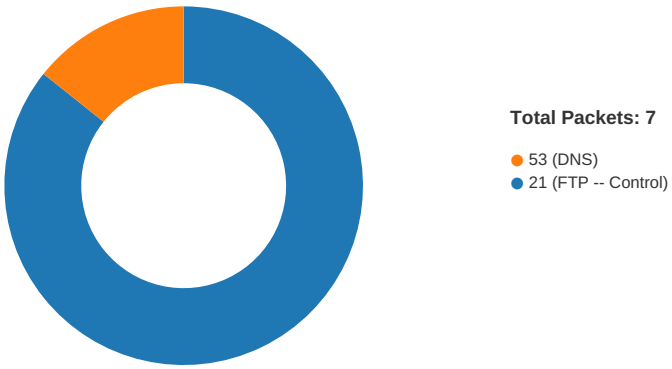
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd80a0	0x334	data		
RT_MANIFEST	0xd83d4	0xe15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:19:52.324122906 CEST	49765	21	192.168.2.7	107.161.178.166
Aug 8, 2022 17:19:52.453358889 CEST	21	49765	107.161.178.166	192.168.2.7
Aug 8, 2022 17:19:52.453870058 CEST	49765	21	192.168.2.7	107.161.178.166
Aug 8, 2022 17:19:52.461240053 CEST	49765	21	192.168.2.7	107.161.178.166
Aug 8, 2022 17:19:52.583769083 CEST	21	49765	107.161.178.166	192.168.2.7
Aug 8, 2022 17:19:52.583904028 CEST	49765	21	192.168.2.7	107.161.178.166
Aug 8, 2022 17:19:52.590502977 CEST	21	49765	107.161.178.166	192.168.2.7
Aug 8, 2022 17:19:52.590625048 CEST	49765	21	192.168.2.7	107.161.178.166
Aug 8, 2022 17:19:52.590635061 CEST	21	49765	107.161.178.166	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:19:52.590712070 CEST	49765	21	192.168.2.7	107.161.178.166

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:19:52.141880035 CEST	60978	53	192.168.2.7	8.8.8.8
Aug 8, 2022 17:19:52.280396938 CEST	53	60978	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:19:52.141880035 CEST	192.168.2.7	8.8.8.8	0xa05e	Standard query (0)	ftp.artrsllc.com	A (IP address)	IN (0x0001)

DNS Answers

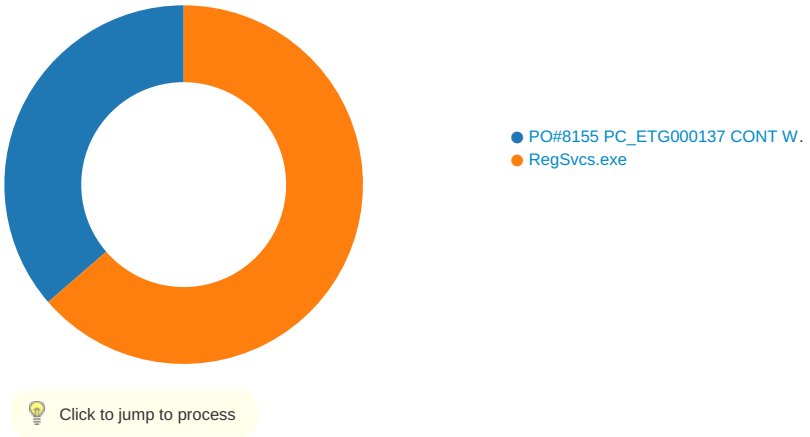
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:19:52.280396938 CEST	8.8.8.8	192.168.2.7	0xa05e	No error (0)	ftp.artrsllc.com		107.161.178.166	A (IP address)	IN (0x0001)

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 17:19:52.583769083 CEST	21	49765	107.161.178.166	192.168.2.7	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 10:21. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 10:21. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 10:21. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 10:21. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Aug 8, 2022 17:19:52.590502977 CEST	21	49765	107.161.178.166	192.168.2.7	220 Logout.

Statistics

Behavior



System Behavior

Analysis Process: PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe PID: 6172, Parent PID: 4312

General

Target ID:	0
Start time:	17:19:18
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe"
Imagebase:	0x910000
File size:	880128 bytes
MD5 hash:	62881881E70F226D8C23A01CDC7287DD
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: 00000000.00000002.379474394.0000000003E99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.379474394.0000000003E99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.379474394.0000000003E99000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CE2CF06	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	6CE2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D13C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO#8155 PC_ETG000137 CONT WT Ashwagandha 07-08-2022 WRDOOO1.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D13C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile

Analysis Process: RegSvcs.exe PID: **6444**, Parent PID: **6172**

General

Target ID:	4
Start time:	17:19:32
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf80000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000004.00000000.367436517.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.367436517.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000000.367436517.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.611090100.0000000003351000.00000004.00000800.00020000.00000000.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	6CE2CF06	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	6CE2CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CE0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CE05705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BC71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC71B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\be1af18b-6e62-43df-aad5-7e50d70b7937	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BC71B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly