ID: 756266
Sample Name: PO.exe
Cookbook: default.jbs
Time: 22:45:33
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

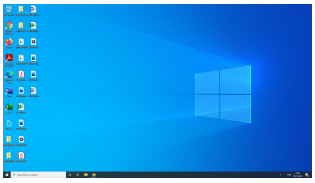
Windows Analysis Report

PO.exe

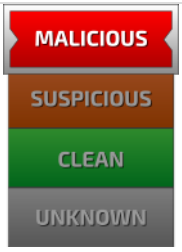
Overview

General Information

Sample Name:	PO.exe
Analysis ID:	756266
MD5:	9297126fd9624f7.
SHA1:	c30b3c8fddd49f7..
SHA256:	edd8e1858bcc70..
Infos:	



Detection



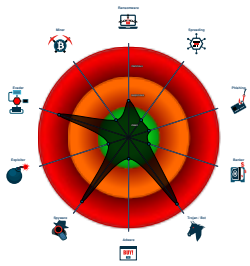
AgentTesla, GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64native**
- PO.exe (PID: 5272 cmdline: C:\Users\user\Desktop\PO.exe MD5: 9297126FD9624F7DC2D4F64F072668A2)
  - CasPol.exe (PID: 7240 cmdline: C:\Users\user\Desktop\PO.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 1336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "561616954",
  "Chat URL": "https://api.telegram.org/bot5088709131:AAFHCIxHU907RAI3XEaH2G6LgE9wrdrAgI0/sendDocument"
}
```


Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot5088709131:AAFHCIxHU907RAI3XEaH2G6LgE9wrdrAgI0/sendMessage"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.89339190222.000000001D990000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.85191335084.00000000032A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000000.84958072563.0000000001110000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000002.89336734210.000000001D8B1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.89336734210.000000001D8B1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 6 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.11.20 - Destination IP: 149.154.167.220

Timestamp:	192.168.11.20149.154.167.220498544432851779 11/29/22-22:50:36.593124
SID:	2851779
Source Port:	49854
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Uses the Telegram API (likely for C&C communication)

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

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

Stealing of Sensitive Information

Yara detected Telegram RAT

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

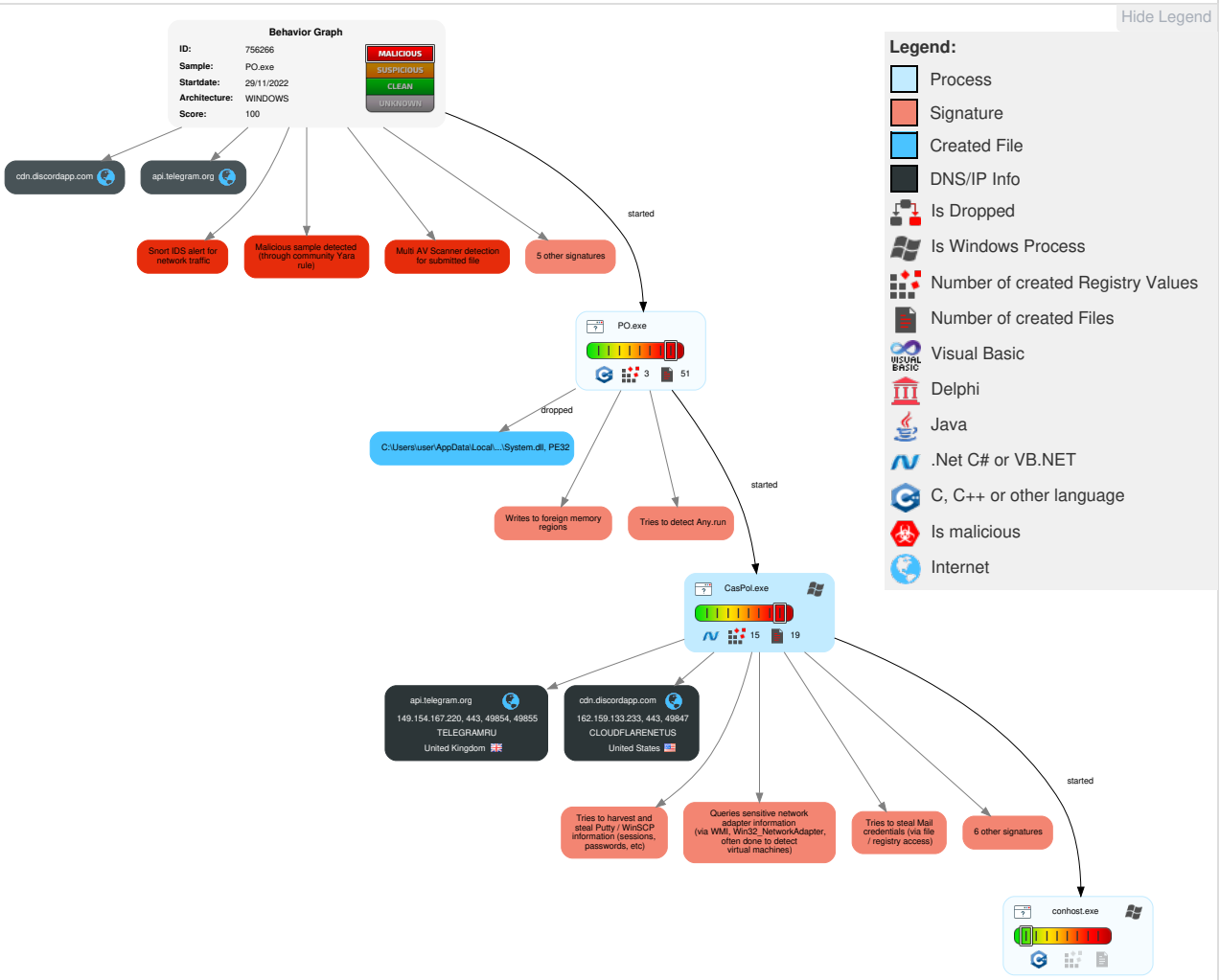
Yara detected Telegram RAT

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	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Obfuscated Files or Information	2 1 Input Capture	1 2 7 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	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)	1 Windows Service	1 DLL Side-Loading	1 Credentials in Registry	3 3 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 1 Process Injection	1 1 Masquerading	NTDS	1 Process Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 4 1 Virtualization/Sandbox Evasion	LSA Secrets	2 4 1 Virtualization/Sandbox Evasion	SSH	2 Clipboard Data	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	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	1 1 1 Process Injection	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

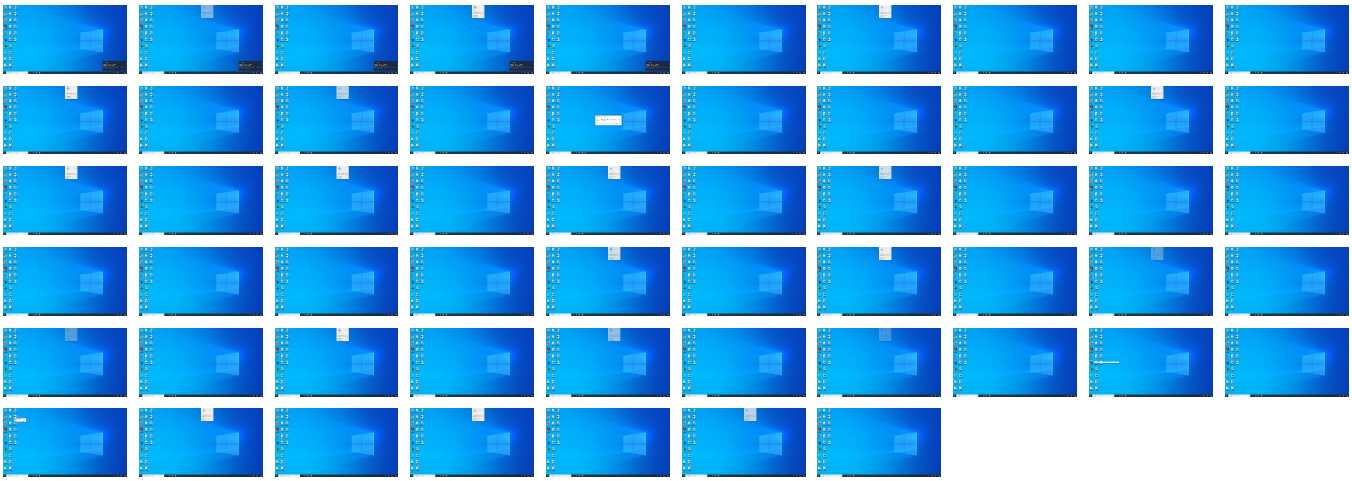
Behavior Graph

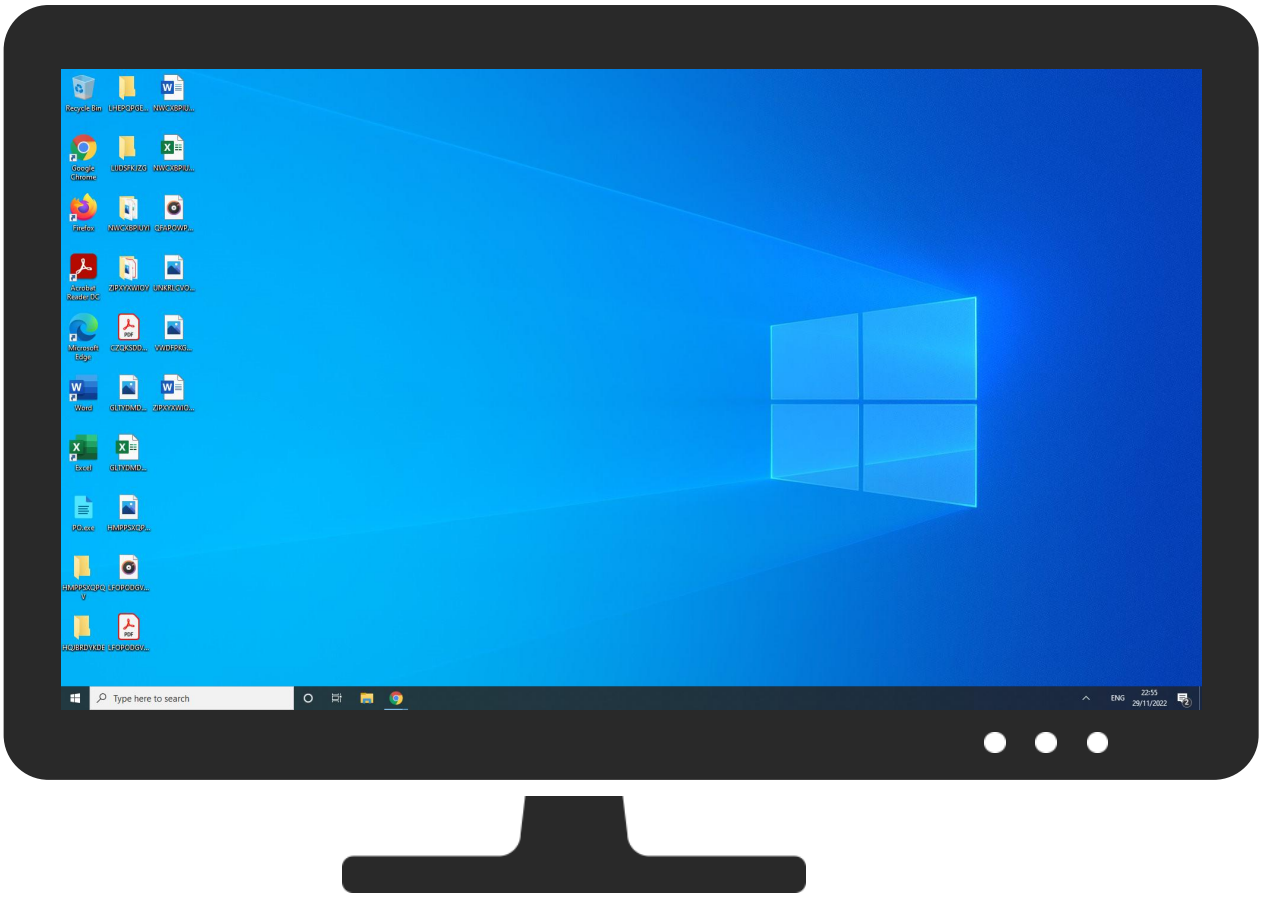


Screenshots

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.exe	29%	Virustotal		Browse
PO.exe	27%	ReversingLabs	Win32.Downloader.Nemesis	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsr9735.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sFTel9k7EYFPshk.comt-WI	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	Avira URL Cloud	safe	
http://https://sFTel9k7EYFPshk.com	0%	Avira URL Cloud	safe	
http://bLCeYs.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.133.233	true	false		high
api.telegram.org	149.154.167.220	true	false		high

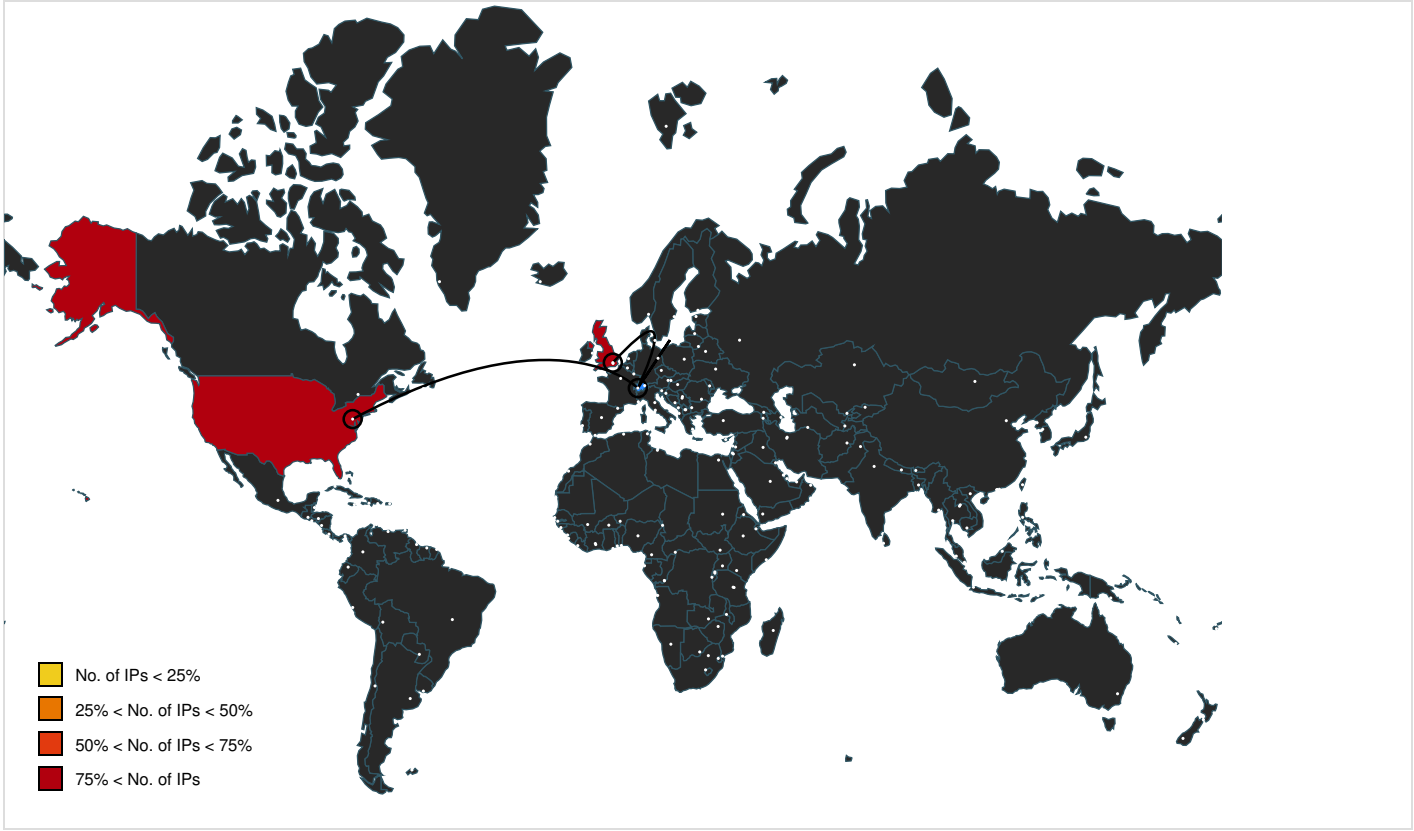
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/1044649962652307570/1047171731867054230/bnezjstiSAD111.ocx	false		high
http://https://api.telegram.org/bot5088709131:AAFHCIxHU907RAI3XEaH2G6LgE9wrdrAgI0/sendDocument	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000004.00000002.8933673421 0.000000001D8B1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	CasPol.exe, 00000004.00000002.8933673421 0.000000001D8B1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org	CasPol.exe, 00000004.00000002.8933959206 8.000000001D9C0000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 4.00000002.89340758768.000000001DA29000. 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.zip%tordir%%ha	CasPol.exe, 00000004.00000002.8933673421 0.000000001D8B1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot5088709131:AAFHCIxHU907RAI3XEaH2G6LgE9wrdrAgI0/sendDocumentdocument-----	CasPol.exe, 00000004.00000002.8933673421 0.000000001D8B1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://sFTel9k7EYFPshk.com	CasPol.exe, 00000004.00000002.8933673421 0.000000001D8B1000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 4.00000002.89339798750.000000001D9D4000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000004.00000002.8933779220 5.000000001D922000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/	CasPol.exe, 00000004.00000002.8931698020 7.00000000014CB000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	PO.exe	false		high
http://https://sFTel9k7EYFPshk.comt-Wl	CasPol.exe, 00000004.00000002.8933673421 0.000000001D8B1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.telegram.org	CasPol.exe, 00000004.00000002.8933979875 0.000000001D9D4000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 00000004.00000002.8933959206 8.000000001D9C0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://bLCeYs.com	CasPol.exe, 00000004.00000002.8933673421 0.000000001D8B1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/1044649962652307570/1047171731867054230/bnezjstiSAD111.ocxT	CasPol.exe, 00000004.00000002.8931739196 8.0000000001506000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/attachments/1044649962652307570/1047171731867054230/bnezjstiSAD111.ocxt	CasPol.exe, 00000004.00000002.8931739196 8.0000000001506000.00000004.00000020.000 20000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756266
Start date and time:	2022-11-29 22:45:33 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	8
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@4/7@2/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 34.2% (good quality ratio 33.7%) • Quality average: 87.7% • Quality standard deviation: 21.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com
- Not all processes where analyzed, report is missing behavior 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.
- Report size getting too big, too many NtReadVirtualMemory 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\Microsoft\Windows\INetCache\Diakonernes\Incongeniality\Ableptically\Omfattede\Iblanding\Heterodoxical.Ufo

Process:	C:\Users\user\Desktop\PO.exe
File Type:	data
Category:	dropped
Size (bytes):	169298
Entropy (8bit):	6.993422708563822
Encrypted:	false

SSDEEP:	3072:3H36doFRBxbYjEigfKAFBx4klY9HcLYO6P7tbLkXlBDPn4rrHIRqkFjOjz:XHRojYfLqkqFZbSjDKrSnpOH
MD5:	E9CD51B8DF0E079A6D84286C4F8FB583
SHA1:	30BB91305F4BAD22563D16D837405BD105982218
SHA-256:	B1DFFFB8EE9D8CB22BF5C8660D793719ACFEC38A08F2A78E90EE8D4067512159
SHA-512:	D33B5DED1B891A2BEB68B0127FFB8E0B30AE3856877F7BEF93D42440D15FFEF6EADC8007137E0BC1B1257CB09777344B22773CEA9F9FDDC81FBDAC3A66DF65AD
Malicious:	false
Reputation:	low
Preview:	.:.V,:.. E....-^,z..3U.g...v.Q.sY..x.....@...m|..I...V.y...@.....S.....G.+...UQg5...@..:..o8.v.j.5.<../..3..0,E.b.v...._...h..b...J.M..._.E/x24.K...\.R.....X.~...._4..%...2\.....:6.5.>E...N &j)yc.F....o....R.tZZ.F.UW....0.....N.,GTMj.....I.....[{..0U..4..3...,I$..}.g.&.u..!.".lstg.5..{..~az..U..J.....j.c[...z.j./...!m.....Cy.U....X.. 9...@..V$...M..*%...O.@..V5.....+".}.4.>.. ...<..e.....;..b9;"D...&E.....A_Q.%..^..t.N&1^....c.....G..h=H.....?.....W.....`.4.,..3.IaaH.B.ZmB....f.J.....a..(p.-X..*...f..W.'.D(O...,..4..cG...../G./..^....6X..x.CD{\g.....{...F:.. 4...tJ>J..=..#K...-.....v...f....J.=7@oM.e.$l..U..m..<..:.O6.,...\.Y|[do.8.w....#]2..f.. ....[...J....g.h`.....Q.f.C_..T...iIR.....A..%t._6fYH.]g.....o.i.c..U.H...h....M...@.n...9.[t.X.....o... ...t.....%PWY.t@..Ce..WG.%.I..b}eF....B.6K.N....Qf.C.P....f....2.>.#...3.5Y.=...d..3.....\f.J..9S.16bQ...}..'.g..M.I.B^e\.8...A.L....v.p..u.....:....Y~t...i...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Diakonernes\Referenceliste\holdovers\open-menu-symbolic.svg

Process:	C:\Users\user\Desktop\PO.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	314
Entropy (8bit):	4.555782614723155
Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYl/n7S3mc4slLlNkRI7NtAlaRI7SdtAlaRI7UNtAlBC:TMHdPnnl/nu3tln7NWlz7MWlz7UNWlM
MD5:	53C42FCA9E64A93B4C572D5BA805FD4D
SHA1:	1659423CA8F981CFD2EEB6ADD25C03CA5B37FFBD
SHA-256:	DD3F1C117437A6F5124905DE7212A1A320E76F9B33D8411BF70DBDBEFA8E9BAD
SHA-512:	2852EB784E5090F298259F04516C1413734ECF20EA7D143864FE0312A6410E83FFF49E16DCE3CF7F61177238B4DECEBD540FD839E3721965A5141856908392DD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 1 2 h 14 v 2 h -14 z m 0 0"/>. <path d="m 1 7 h 14 v 2 h -14 z m 0 0"/>. <path d="m 1 12 h 14 v 2 h -14 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Temp\TOBEN.lnk

Process:	C:\Users\user\Desktop\PO.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:25:52 1600, mtime=Sun Dec 31 23:25:52 1600, atime=Sun Dec 31 23:25:52 1600, length=0, window=hide
Category:	dropped
Size (bytes):	850
Entropy (8bit):	2.925859933343773
Encrypted:	false
SSDEEP:	12:8gl0gsXUCV/tz+7RafgKD7mWH/rNJkKAh4t2YCBTo8:8/raRMgKh5HALJT
MD5:	AF9FC18C6E2F55A80586FD4B43D24674
SHA1:	482192CAF81B1E06F761929AFF7CAADB8D91328A
SHA-256:	500184B06DBC9F859D31AF68D726A7C282D6016E1ABE241A80BF4119C1A073F7
SHA-512:	9DFE5CA18F0E68C868BDE1C0ADC5CB20B38C0D08570769935D1EE53803E4D33E1E949C422FD80F395B250A897219339F97D7198ADDEB86A94A887084D8EA76F
Malicious:	false
Reputation:	low
Preview:	L.....F.....#....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>..... .....A.r.t.h.u.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1..... .Temp..:.....T.e.m.p.....\.2.....TOBEN.txt.D.....T.O.B.E.N...t.x.t.....\.T.O.B.E.N...t.x.t.....(.....l^".`G...3..q s.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.4.2.5.3.1.6.5.6.7.-.2.9.6.9.5.8.8.3.8.2.-.3.7.7.8.2.2.2.4.1.4.-.1.0.0.1.....

C:\Users\user\AppData\Local\Temp\nsr9735.tmp\System.dll

Process:	C:\Users\user\Desktop\PO.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.6557532861400945
Encrypted:	false
SSDEEP:	192:eK24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35OlASl:u8Qll975eXqlWBrz7YLOlA
MD5:	0FF2D70CFDC8095EA99CA2DABBEC3CD7
SHA1:	10C51496D37CECD0E8A503A5A9BB2329D9B38116

SHA-256:	982C5FB7ADA7D8C9BC3E419D1C35DA6F05BC5DD845940C179AF3A33D00A36A8B
SHA-512:	CB5FC0B3194F469B833C2C9ABF493FCEC5251E8609881B7F5E095B9BD09ED468168E95DDA0BA415A7D8D6B7F0DEE735467C0ED8E52B223EB5359986891BA6E2E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L....z.W.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..b....P.....*.....@..B.....

C:\Users\user\AppData\Roaming\hw3hufbj.yur\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, file counter 36, database pages 24, 1st free page 14, free pages 11, cookie 0x5, schema 4, UTF-8, version-valid-for 36
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	2.9216957692876595
Encrypted:	false
SSDEEP:	384:ST8XNcKu0iTwbAziYN570RMZXVuKnQM2V6ofbDO4xmTgZcZygSA2O9RVHfwrhhxV:JNcgiD5Q6luKQM2V7DXcAgSA2KD4jL
MD5:	1A706D20E96086886B5D00D9698E09DF
SHA1:	DACF81D90647457585345BEDD6DE222E83FDE01F
SHA-256:	759F62B61AA65D6D5FAC95086B26D1D053CE1FB24A8A0537ACB42DDF45D2F19F
SHA-512:	CFF7D42AA3B089759C5ACE934A098009D1A58111FE7D99AC7669B7F0A1C973907FD16A4DC1F37B5BE5252EC51B8D876511F4F6317583FA9CC48897B1B913C7F
Malicious:	false
Preview:	SQLite format 3.....@ ...$.....$..S`.....g.....[.[.[..... ....

C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3036000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	modified
Size (bytes):	98304
Entropy (8bit):	0.08231524779339361
Encrypted:	false
SSDEEP:	12:DQANJfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQANJff32mNVpP965Ra8KN0MG/lO
MD5:	886A5F9308577FDF19279AA582D0024D
SHA1:	CDCCC11837CDDB657EB0EF6A01202451ECDF4992
SHA-256:	BA7EB45B7E9B6990BC63BE63836B74FA2CCB64DCD0C199056B6AE37B1AE735F2
SHA-512:	FF0692E52368708B36C161A4BFA91EE01CCA1B86F66666F7FC4979C6792D598FF7720A9FAF258F61439DAD61DB55C50D992E99769B1E4D321EC5B98230684BC5
Malicious:	false
Preview:	SQLite format 3.....@ .....S`.....}..}..... ....

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.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

Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.435141913006391
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	PO.exe
File size:	269537
MD5:	9297126fd9624f7dc2d4f64f072668a2
SHA1:	c30b3c8fddd49f7dfba687026daf6293f6d90b1b
SHA256:	edd8e1858bcc704fdea75837bb448eceda61317e7f8028e82aa2a0e5559c658a
SHA512:	57fd81274b3f16cb8f0056c9afe2c697649db154c12e63a4ed8bad65ccb6b598845adce9883bd2695335e05e8f3c877fc9f2e32a637c01e170d0b671e32c6d0b
SSDEEP:	6144:DB+pqUiH1YF0tV1R5nqyw8TqwiV6lMATl:DgcHyF+Hqyw83iLATl
TLSH:	39448B147A6CE127F11AC6709B52AD1B7E783F040865D203BEC4FB5E353B14299FA26B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P..*_...P...P..OP..*_...P...s...P...V...P..Rich.P.....PE..L....z.W.....b...*.....3.....@

File Icon

Icon Hash:	b474f4c4c4c4c4d4

Static PE Info

General

Entrypoint:	0x4033b6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x57017AB0 [Sun Apr 3 20:18:56 2016 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:	4ea4df5d94204fc550be1874e1b77ea7

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h

Instruction
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080B4h]
call dword ptr [004080B0h]
cmp ax, 00000006h
je 00007FFA70B1BD33h
push ebx
call 00007FFA70B1EE8Ch
cmp eax, ebx
je 00007FFA70B1BD29h
push 00000C00h
call eax
mov esi, 004082B8h
push esi
call 00007FFA70B1EE06h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FFA70B1BD0Ch
push ebp
push 00000009h
call 00007FFA70B1EE5Eh
push 00000007h
call 00007FFA70B1EE57h
mov dword ptr [0042A244h], eax
call dword ptr [0040803Ch]
push ebx
call dword ptr [004082A4h]
mov dword ptr [0042A2F8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408188h]
push 0040A384h
push 00429240h
call 00007FFA70B1EA40h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007FFA70B1EA2Eh
push ebx
call dword ptr [00408174h]
add word ptr [eax], 0000h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6c000	0x19f28	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b4	.rdata
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	0x615d	0x6200	False	0.6616709183673469	data	6.45041359169741	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x13a4	0x1400	False	0.4529296875	data	5.163001655755973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.5026041666666666	data	3.9824009583068882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x41000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x6c000	0x19f28	0x1a000	False	0.062424879807692304	data	2.7337265494354486	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x6c358	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x6c6c0	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x7cee8	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x81110	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x836b8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x84760	0x9ee	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x85150	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x855b8	0x144	data	English	United States
RT_DIALOG	0x85700	0x13c	data	English	United States
RT_DIALOG	0x85840	0x100	data	English	United States
RT_DIALOG	0x85940	0x11c	data	English	United States
RT_DIALOG	0x85a60	0xc4	data	English	United States
RT_DIALOG	0x85b28	0x60	data	English	United States
RT_GROUP_ICON	0x85b88	0x5a	data	English	United States
RT_MANIFEST	0x85be8	0x340	XML 1.0 document, ASCII text, with very long lines (832), with no line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	SetCurrentDirectoryW, GetFileAttributesW, GetFullPathNameW, Sleep, GetTickCount, CreateFileW, GetFileSize, MoveFileW, SetFileAttributesW, GetModuleFileNameW, CopyFileW, ExitProcess, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, WaitForSingleObject, GetCurrentProcess, CompareFileTime, GlobalUnlock, GlobalLock, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, GetTempFileNameW, WriteFile, lstrcpyA, lstrcpyW, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GlobalFree, GlobalAlloc, GetShortPathNameW, SearchPathW, lstrcmpiW, SetFileTime, CloseHandle, ExpandEnvironmentStringsW, lstrcmpW, GetDiskFreeSpaceW, lstrlenW, lstrcpynW, GetExitCodeProcess, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, MulDiv, MultiByteToWideChar, lstrlenA, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, IsWindowEnabled, EnableMenuItem, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, wsprintfW, ScreenToClient, GetWindowRect, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, LoadImageW, SetTimer, SetWindowTextW, PostQuitMessage, ShowWindow, GetDlgItem, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, DrawTextW, EndPaint, CreateDialogParamW, SendMessageTimeoutW, SetForegroundWindow
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW
ADVAPI32.dll	RegDeleteKeyW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, AdjustTokenPrivileges, RegOpenKeyExW, RegEnumValueW, RegDeleteValueW, RegCloseKey, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

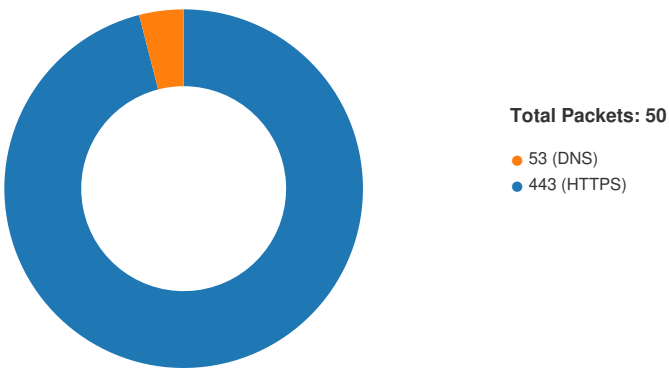
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20149.154.167.220498544432851779 11/29/22-22:50:36.593124	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49854	443	192.168.11.20	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:48:56.877616882 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:56.877716064 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:56.877887964 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:56.908607960 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:56.908684015 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:56.957823992 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:56.958023071 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.067698002 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.067722082 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.068057060 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.068178892 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.072216988 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.112457991 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136059046 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136152029 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136217117 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136225939 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.136249065 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136323929 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.136369944 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136431932 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136507988 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.136516094 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136528015 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136554956 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.136635065 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.136635065 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136694908 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136826992 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.136826992 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.136838913 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.136847973 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137010098 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.137010098 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.137022972 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137036085 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137248993 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.137248993 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.137258053 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137568951 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137614012 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.137625933 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137691021 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137804985 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.137813091 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.137996912 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.137996912 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.138003111 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.138344049 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.144891977 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.145090103 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.145133018 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.145158052 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.145361900 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.145381927 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.145440102 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.145677090 CET	49847	443	192.168.11.20	162.159.133.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:48:57.145677090 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.145699978 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.145767927 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.145921946 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.146023989 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146023989 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146043062 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.146117926 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.146148920 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146311998 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.146394014 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146394968 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146486998 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.146533966 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146648884 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.146712065 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146754026 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.146883011 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.146934986 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147067070 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147093058 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147118092 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147255898 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147255898 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147295952 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147439003 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147481918 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147521973 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147574902 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147703886 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147705078 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147754908 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147896051 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147907972 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.147937059 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.147964001 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.148104906 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.148106098 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.148155928 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.148188114 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.148289919 CET	49847	443	192.168.11.20	162.159.133.233
Nov 29, 2022 22:48:57.148339033 CET	443	49847	162.159.133.233	192.168.11.20
Nov 29, 2022 22:48:57.148468971 CET	49847	443	192.168.11.20	162.159.133.233

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 22:48:56.855335951 CET	50313	53	192.168.11.20	1.1.1.1
Nov 29, 2022 22:48:56.865253925 CET	53	50313	1.1.1.1	192.168.11.20
Nov 29, 2022 22:50:36.482291937 CET	57620	53	192.168.11.20	1.1.1.1
Nov 29, 2022 22:50:36.492578030 CET	53	57620	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 22:48:56.855335951 CET	192.168.11.20	1.1.1.1	0xf7f5	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:50:36.482291937 CET	192.168.11.20	1.1.1.1	0x1e1d	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

DNS Answers

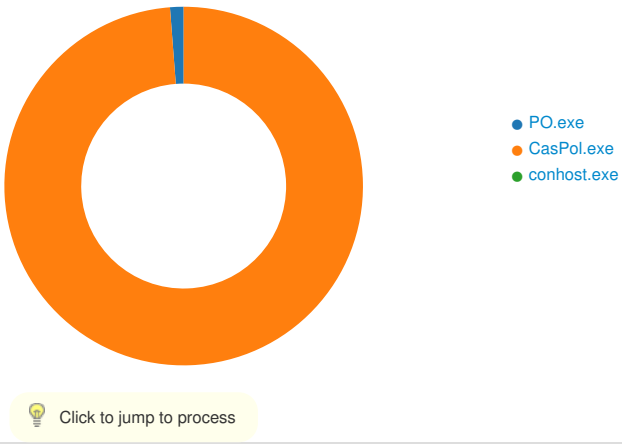
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 22:48:56.865253925 CET	1.1.1.1	192.168.11.20	0xf7f5	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:48:56.865253925 CET	1.1.1.1	192.168.11.20	0xf7f5	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:48:56.865253925 CET	1.1.1.1	192.168.11.20	0xf7f5	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:48:56.865253925 CET	1.1.1.1	192.168.11.20	0xf7f5	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:48:56.865253925 CET	1.1.1.1	192.168.11.20	0xf7f5	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)	false
Nov 29, 2022 22:50:36.492578030 CET	1.1.1.1	192.168.11.20	0x1e1d	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- cdn.discordapp.com
- api.telegram.org

Statistics

Behavior



System Behavior

Analysis Process: PO.exe PID: 5272, Parent PID: 5080

General

Target ID:	1
Start time:	22:47:26
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\PO.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO.exe
Imagebase:	0x400000
File size:	269537 bytes
MD5 hash:	9297126FD9624F7DC2D4F64F072668A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.85191335084.00000000032A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

Analysis Process: CasPol.exe PID: **7240**, Parent PID: **5272**

General

Target ID:	4
Start time:	22:48:35
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO.exe
Imagebase:	0xd30000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
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: 00000004.00000002.89339190222.000000001D990000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000000.84958072563.0000000001110000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.89336734210.000000001D8B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.89336734210.000000001D8B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000004.00000002.89336734210.000000001D8B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000004.00000002.89336734210.000000001D8B1000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	1136121	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	1136121	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1136121	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	1136121	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	1136121	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	1136121	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	6DB83263	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	6DB83263	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	6DB83263	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	6DB83263	unknown
C:\Users\user\AppData\Roaming\hw3hufbj.yur	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA20794	CreateDirectoryW
C:\Users\user\AppData\Roaming\hw3hufbj.yur\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	6CA20794	CreateDirectoryW
C:\Users\user\AppData\Roaming\hw3hufbj.yur\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	6CA20794	CreateDirectoryW
C:\Users\user\AppData\Roaming\hw3hufbj.yur\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	6CA213BB	CopyFileW
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA20794	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA20794	CreateDirectoryW
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles\ol7uiqa8.default-release	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA20794	CreateDirectoryW
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6CA213BB	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Chrome\Default\Cookies	success or wait	1	6CA1E04E	DeleteFileW
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	success or wait	1	6CA1E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CA19B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CA19B71	WriteFile
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Chrome\Default\Cookies	0	98304	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 24 00 00 00 18 00 00 00 0e 00 00 00 0b 00 00 00 05 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 00 00 00 24 00 2e 53 60 0d 0c fd 00 04 09 fd 00 0f 67 0f fd 09 fd 0c 5b 0c 5b 0c 5b 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@ $$.S`g[[[	success or wait	1	6CA213BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 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 53 60 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 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@ .S`}}	success or wait	1	6CA213BB	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB8099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DAD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DAD62DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\a1c07371-6395-44d7-b261-e6a4a7e61fe5	unknown	4096	success or wait	2	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CA19B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6CA19B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DB8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DB8099B	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Chrome\Default\Cookies	unknown	16384	success or wait	6	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Chrome\Default\Cookies	unknown	16384	end of file	1	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	success or wait	6	6CA19B71	ReadFile
C:\Users\user\AppData\Roaming\hw3hufbj.yur\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	end of file	1	6CA19B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	success or wait	1	6BCAFDB8	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableFileTracing	dword	0	success or wait	1	6BCAFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	6BCAFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	6BCAFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	6BCAFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	6BCAFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	6BCAFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6BCAFDB8	unknown

Analysis Process: conhost.exe PID: **1336**, Parent PID: **7240**

General	
Target ID:	5
Start time:	22:48:36
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60d240000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly