ID: 798398
Sample Name: DPR602859651100125001V1100125154830E3-2-2023#U00b7pdf.exe
Cookbook: default.jbs
Time: 03:52:29
Date: 04/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

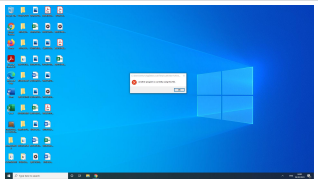
Windows Analysis Report

DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe

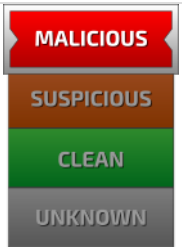
Overview

General Information

Sample Name:	DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Analysis ID:	798398
MD5:	91c0c4710db0…
SHA1:	63880c602b96…
SHA256:	a4d4961d124e…
Infos:	



Detection



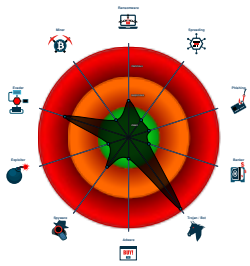
Nanocore, GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Tries to detect Any.run
- Hides that the sample has been dow…
- Uses schtasks.exe or at.exe to add…

Classification



Process Tree

- **System is w10x64native**
- DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe (PID: 2948 cmdline: C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe MD5: 91C0C4710DB096A4689D40E2CEB3814D)
  - CasPol.exe (PID: 4376 cmdline: C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - CasPol.exe (PID: 7876 cmdline: C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - schtasks.exe (PID: 6764 cmdline: schtasks.exe" /create /f /tn "DSL Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp673D.tmp MD5: 478BEAEC1C3A9417272BC8964ADD1CEE)
      - conhost.exe (PID: 1760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- CasPol.exe (PID: 4756 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe 0 MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - conhost.exe (PID: 4456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000008.00000003.167512023875.0000000039142000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0x2022:$a: NanoCore 0x2047:$a: NanoCore 0x20a0:$a: NanoCore 0x1223d:$a: NanoCore 0x12263:$a: NanoCore 0x122bf:$a: NanoCore 0x1f114:$a: NanoCore 0x1f16d:$a: NanoCore 0x1f1a0:$a: NanoCore 0x1f3cc:$a: NanoCore 0x1f448:$a: NanoCore 0x1fa61:$a: NanoCore 0x1fbaa:$a: NanoCore 0x2007e:$a: NanoCore 0x20365:$a: NanoCore 0x2037c:$a: NanoCore 0x23705:$a: NanoCore 0x24abf:$a: NanoCore 0x24b09:$a: NanoCore 0x25763:$a: NanoCore 0x2ad48:$a: NanoCore
00000008.00000003.167512023875.0000000039142000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0x2047:$a1: NanoCore.ClientPluginHost 0x12263:$a1: NanoCore.ClientPluginHost 0x1f3cc:$a1: NanoCore.ClientPluginHost 0x24abf:$a1: NanoCore.ClientPluginHost 0x2ad48:$a1: NanoCore.ClientPluginHost 0x35357:$a1: NanoCore.ClientPluginHost 0x3f782:$a1: NanoCore.ClientPluginHost 0x4a75f:$a1: NanoCore.ClientPluginHost 0x56501:$a1: NanoCore.ClientPluginHost 0x7b405:$a1: NanoCore.ClientPluginHost 0x8a845:$a1: NanoCore.ClientPluginHost 0x2022:$a2: NanoCore.ClientPlugin 0x1223d:$a2: NanoCore.ClientPlugin 0x1f448:$a2: NanoCore.ClientPlugin 0x24b09:$a2: NanoCore.ClientPlugin 0x2adc2:$a2: NanoCore.ClientPlugin 0x35441:$a2: NanoCore.ClientPlugin 0x3f822:$a2: NanoCore.ClientPlugin 0x4a736:$a2: NanoCore.ClientPlugin 0x564d8:$a2: NanoCore.ClientPlugin 0x7b3dc:$a2: NanoCore.ClientPlugin
00000002.00000002.167511188846.0000000008C46000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: CasPol.exe PID: 7876	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0x4e6b:$a: NanoCore 0x4e7f:$a: NanoCore 0x54df:$a: NanoCore 0x6c14:$a: NanoCore 0x6c77:$a: NanoCore 0x32355:$a: NanoCore 0xf71c3:$a: NanoCore 0xf71e8:$a: NanoCore 0xf7241:$a: NanoCore 0xfacdd:$a: NanoCore 0xfad00:$a: NanoCore 0xfad55:$a: NanoCore 0x105e6c:$a: NanoCore 0x105e90:$a: NanoCore 0x105ee8:$a: NanoCore 0x10d35e:$a: NanoCore 0x10d3b7:$a: NanoCore 0x10d3dd:$a: NanoCore 0x10d773:$a: NanoCore 0x10d7b7:$a: NanoCore 0x10d7fa:$a: NanoCore
Process Memory Space: CasPol.exe PID: 7876	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0xf71e8:$a1: NanoCore.ClientPluginHost 0xf71c3:$a2: NanoCore.ClientPlugin 0xfab2b:$b1: get_BuilderSettings 0xf71d9:$b4: IClientAppHost 0x10f427:$b7: LogClientException 0x11159d:$b8: PipeExists 0xfeffe:$b9: IClientLoggingHost

Unpacked PEs

Source	Rule	Description	Author	Strings
8.3.CasPol.exe.3914b6be.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0x6da5:$x1: NanoCore.ClientPluginHost 0x6dd2:$x2: IClientNetworkHost
8.3.CasPol.exe.3914b6be.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0x6da5:$x2: NanoCore.ClientPluginHost 0x7d74:$s2: FileCommand 0xc776:$s4: PipeCreated 0x6dbf:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
8.3.CasPol.exe.3914b6be.1.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x6d7f:$x2: NanoCore.ClientPlugin • 0x6da5:$x3: NanoCore.ClientPluginHost • 0x6d70:$i3: IClientNetwork • 0x6d95:$i5: IClientDataHost • 0x6dbf:$i6: IClientLoggingHost • 0x6dd2:$i7: IClientNetworkHost • 0x6de5:$i9: IClientNameObjectCollection • 0x6b02:$s1: ClientPlugin • 0x6d88:$s1: ClientPlugin
8.3.CasPol.exe.3914b6be.1.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x6da5:$a1: NanoCore.ClientPluginHost • 0x6d7f:$a2: NanoCore.ClientPlugin • 0x6dbf:$b9: IClientLoggingHost
8.3.CasPol.exe.39165717.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x3831:$x1: NanoCore.ClientPluginHost • 0x386a:$x2: IClientNetworkHost
Click to see the 12 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 91.193.75.146 - Destination IP: 192.168.11.20 −

Timestamp:	91.193.75.146192.168.11.203498498572810451 02/04/23-04:02:00.606308
SID:	2810451
Source Port:	3498
Destination Port:	49857
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 91.193.75.146 −

Timestamp:	192.168.11.2091.193.75.1464985734982816766 02/04/23-04:02:49.236881
SID:	2816766
Source Port:	49857
Destination Port:	3498
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 91.193.75.146 - Destination IP: 192.168.11.20 −

Timestamp:	91.193.75.146192.168.11.203498498572810290 02/04/23-04:02:33.039323
SID:	2810290
Source Port:	3498
Destination Port:	49857
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 91.193.75.146

Timestamp:	192.168.11.2091.193.75.1464985734982025019 02/04/23-03:57:12.109194
SID:	2025019
Source Port:	49857
Destination Port:	3498
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 91.193.75.146 - Destination IP: 192.168.11.20

Timestamp:	91.193.75.146192.168.11.203498498572841753 02/04/23-04:02:50.692460
SID:	2841753
Source Port:	3498
Destination Port:	49857
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 91.193.75.146

Timestamp:	192.168.11.2091.193.75.1464985734982816718 02/04/23-04:02:19.821499
SID:	2816718
Source Port:	49857
Destination Port:	3498
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking

Snort IDS alert for network traffic

Uses dynamic DNS services

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Tries to detect Any.run

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

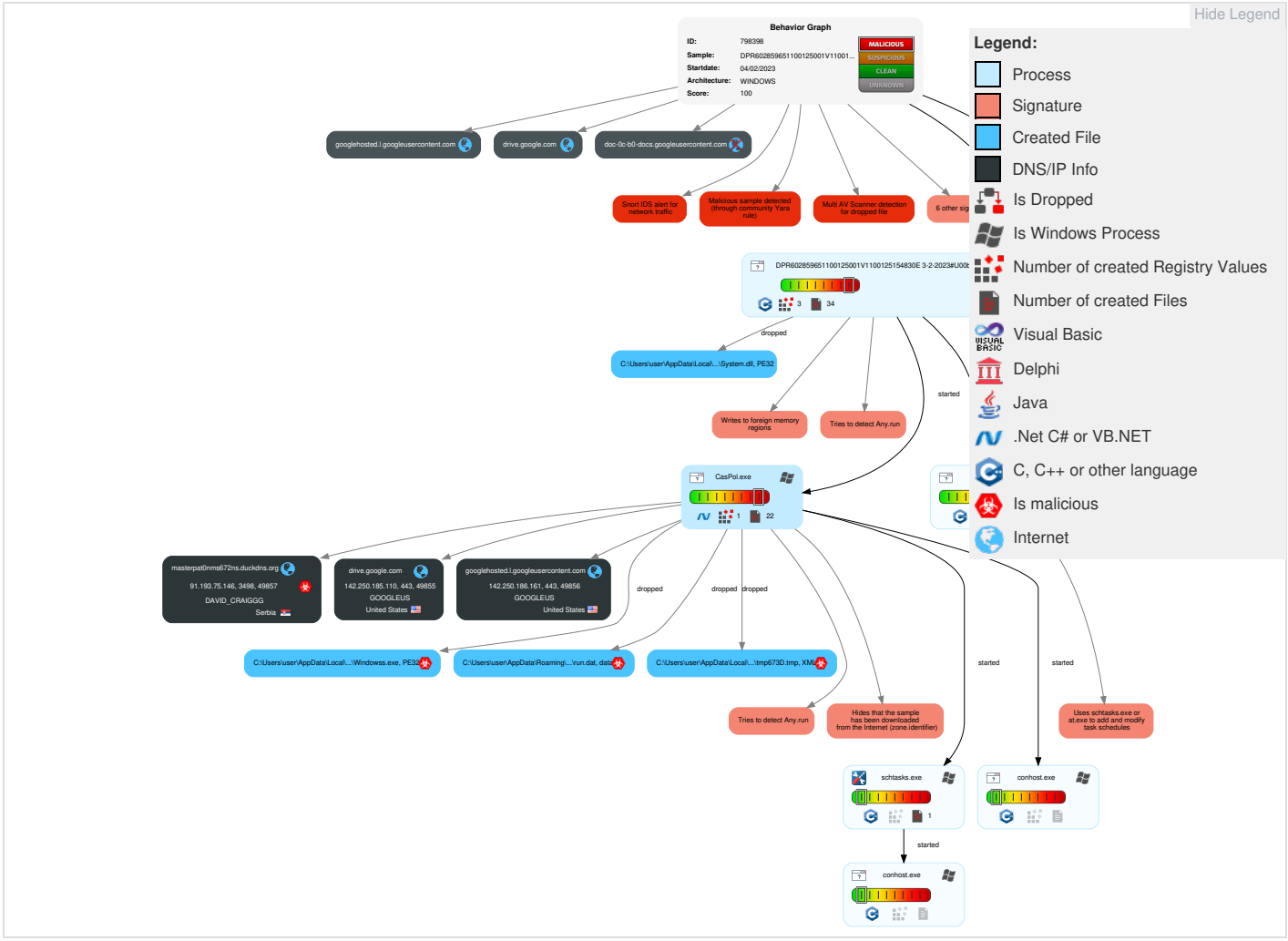
Remote Access Functionality

Detected Nanocore Rat

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	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	1 Scheduled Task/Job	1 Access Token Manipulation	1 Obfuscated Files or Information	LSASS Memory	4 System Information Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 DLL Side-Loading	Security Account Manager	2 1 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	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)	1 Scheduled Task/Job	1 1 Masquerading	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Registry Run Keys / Startup Folder	1 2 1 Virtualization/Sandbox Evasion	LSA Secrets	1 2 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	2 Non-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	1 1 3 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 2 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
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

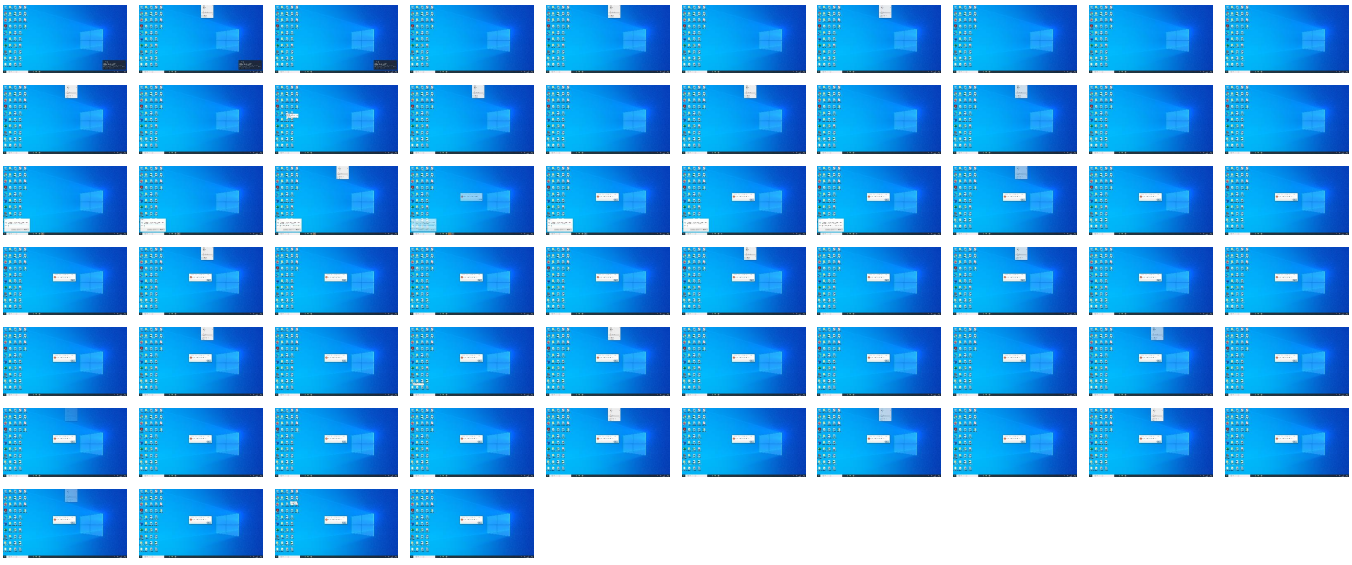
Behavior Graph

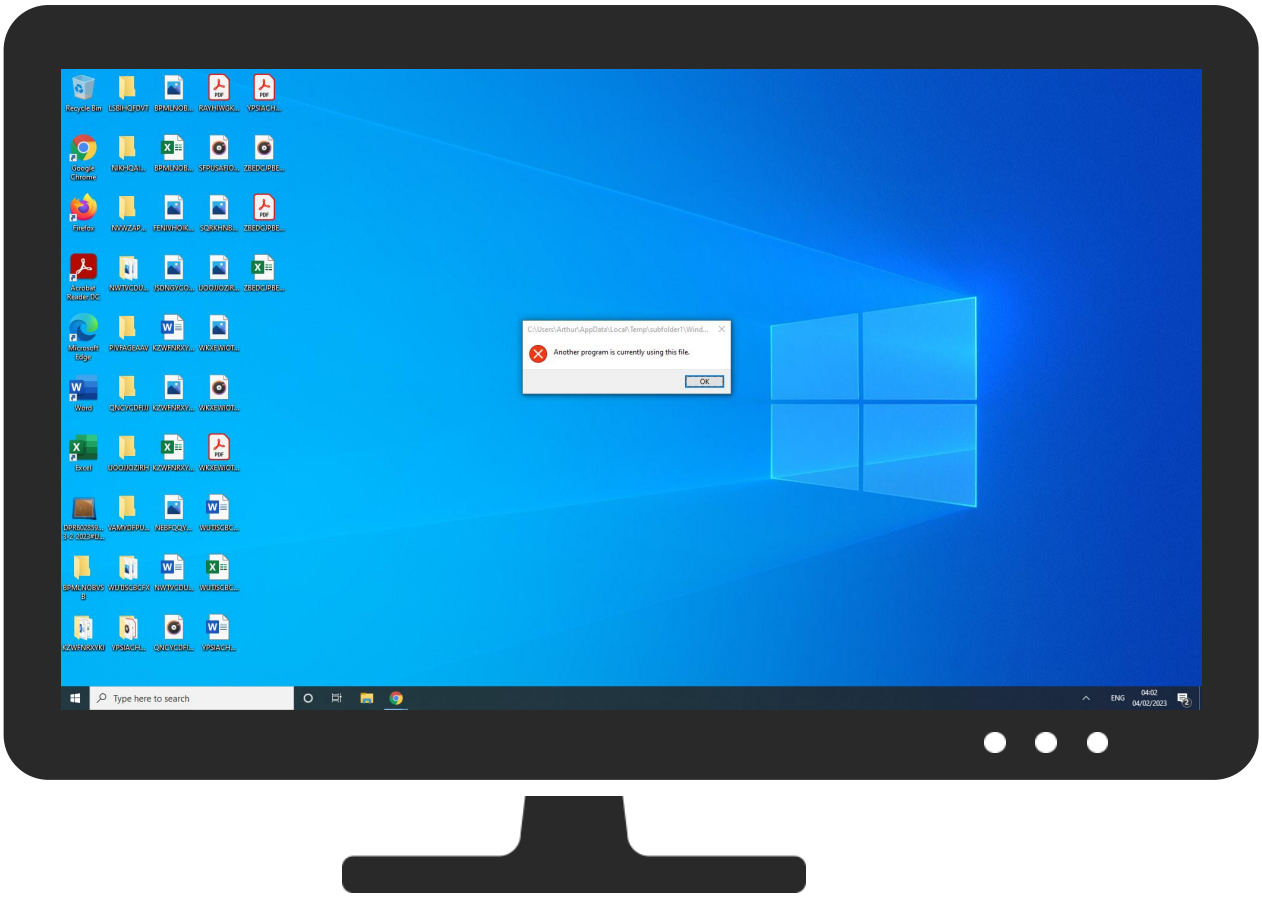


Screenshots

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
DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	46%	Virustotal		Browse
DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	47%	ReversingLabs	Win32.Trojan.Nsisx	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nssE334.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nssE334.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\subfolder1\Windowss.exe	47%	ReversingLabs	Win32.Trojan.Nsisx	
C:\Users\user\AppData\Local\Temp\subfolder1\Windowss.exe	46%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.185.110	true	false		high
masterpat0nms672ns.duckdns.org	91.193.75.146	true	true		unknown
googlehosted.l.googleusercontent.com	142.250.186.161	true	false		high
doc-0c-b0-docs.googleusercontent.com	unknown	unknown	false		high

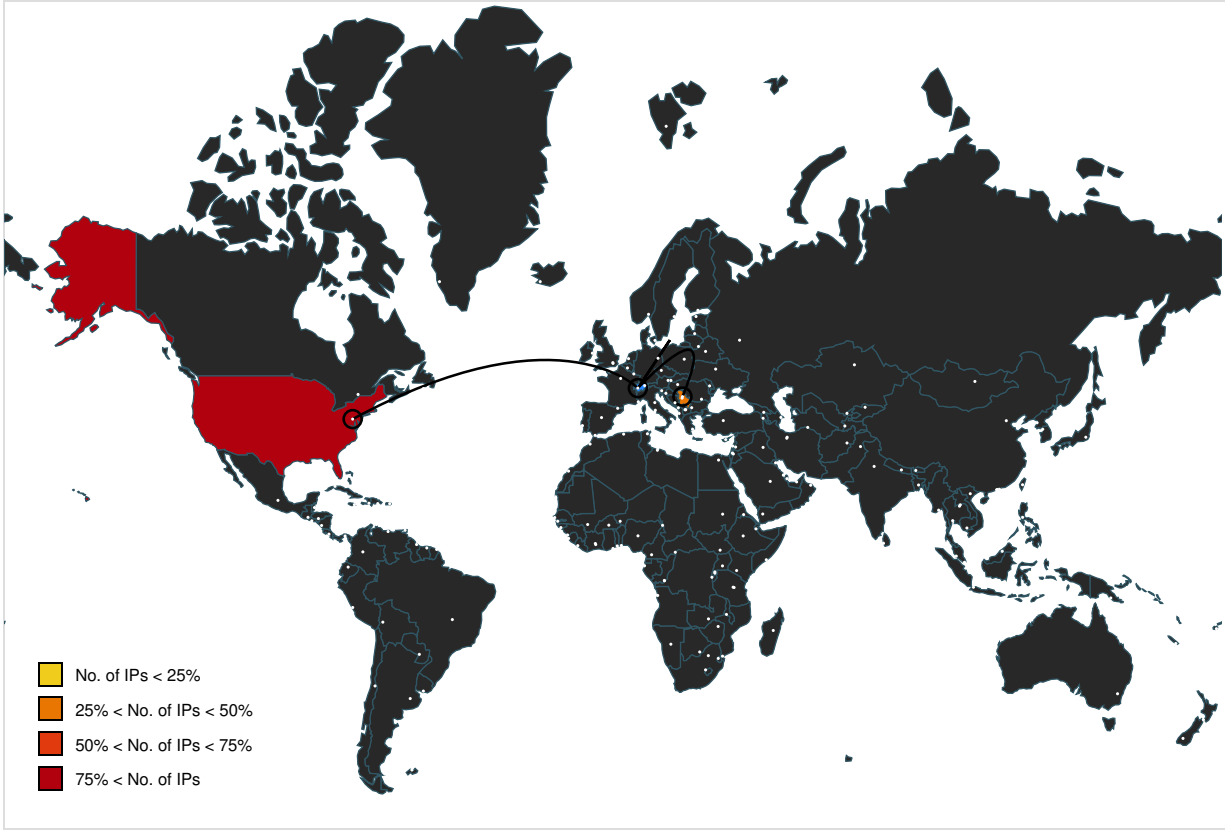
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0c-b0-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/gop7ht5qt6iu260mrr5822id2hevfvup/1675479375000/07900185898442636486/*/1GWkPMapRdWHnFBq8NG4QBMUUzbTsJcvy?e=download&uuid=5cfb3928-a799-4c74-b6f0-f4c0849b8739	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc-0c-b0-docs.googleusercontent.com/	CasPol.exe, 00000008.00000003.167744785159.0000000007194000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://doc-0c-b0-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/gop7ht5q	CasPol.exe, 00000008.00000003.167744785159.00000000071ED000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000008.00000003.167744785159.0000000007194000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000008.00000003.167481132146.00000000071F4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe, Windowss.exe.8.dr	false		high
http://google.com	CasPol.exe, 00000008.00000003.167512023875.0000000039142000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://drive.google.com/	CasPol.exe, 00000008.00000003.167744785159.000000000717A000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000008.00000003.167744785159.0000000007162000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://doc-0c-b0-docs.googleusercontent.com/H	CasPol.exe, 00000008.00000003.167744785159.0000000007194000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.185.110	drive.google.com	United States		15169	GOOGLEUS	false
91.193.75.146	masterpat0nms672ns.duckdns.org	Serbia		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	798398
Start date and time:	2023-02-04 03:52:29 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	15
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
Sample file name:	DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@11/16@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 63.1% (good quality ratio 61.9%) • Quality average: 88.1% • Quality standard deviation: 22.3%
HCA Information:	• Successful, ratio: 89% • 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, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, evoke-windowsservices-tas.msedge.net, ctldl.windowsupdate.com, wdcp.microsoft.com, manage.devcenter.microsoft.com
- 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.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:57:03	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\Windowss.exe
03:57:09	Task Scheduler	Run new task: DSL Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe" s>$(Arg0)
03:57:12	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\Windowss.exe

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\Deskriptiv155\Hjertere\Hynde.Una	
Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	ASCII text, with very long lines (34794), with no line terminators
Category:	dropped
Size (bytes):	34794
Entropy (8bit):	3.9997795398371228
Encrypted:	false
SSDEEP:	768:ccaHQHD7RgNO/PDcbf/CBrmE4Hi1r1scfUos2cX7nhL/djYY2v:iQHDyO4mrei7sqc7BdsYG
MD5:	DD18A90498456DFCAE95A46AFC33C475
SHA1:	65AB8F8342AF9C08FE39E7664E3DF9C9646DF211
SHA-256:	856D7590AB2EFC8C760BC37D652D5AE8A5DE982891ADB7A678E43A91D268DDE9
SHA-512:	BC6F1AED9B60D3C383E0A65C19E2FF031252DC9B193AE6AD3B5B6F3767EC2F7E6E6E4B3F65D2A3CBD501ED38C838C89A9648D255EAF1110BD7C5A0142F0A6A10
Malicious:	false
Preview:	6A34F0604AEE6DB314B378246D35FE80BFC162A6BA9C27C8E16DA2C9AE4B52DFB6BB4D14CCFA23C4B675E918121507BB7243C36C59FB457F64D397E98034F58490327D6C90C000BCD403F4272BEC91D0A33E5A0129628A58358949F71B9E468413A9F921ED449BFDFDFD8B52A2D79EC29D74E20791961A6CBC321812874EFFDA002DA4B6728BAC6F6A19E8DAA48014568DAC10440B68FF4911CE9C39E654E7BD5108097717BE2EF95C1A30EEFB3987C46DF521EAF29935CD47E5E692C36B39093D4C54B8F75D591A0FBE8521B1B811C1D5DE94F2446E4C6E3A52F9AF8CE6352838F7BFA2A9F2E978B6C63E24B131DB84C3D58F2272E6196F60D39BC78BC16F84DBD6729C7BE4C34C92F59F36A74676FEDD70E5E836CF8087A82BD101F899808FB96B6190BA47B820A5BABE361E59EC9FCCD938CFB68F2B3E0A7B59E68314002BFA8EE8E502796C53CD4716076F9F492DF2833BD6AD60228D25C9991C11A6CB28FAA225570F38AE4FC0F98A17CA0400AD9C6D66D92018971C0D79A5062B675A80F3A3E62E9196691C5DC24E022A718CA4F8012CAFE8F14181671A95F9D9650843B5EDCB80A8B14070975B13838161A8EFC0EB2E3233CE381BB0D822E3EA392FBE123D51467413E23E06FFF39AE85E5BAC5549DB7B405C6BEAC058711C90F3D73941BE2013BCBB2FC5FD5660B746D980317AD92DA8

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\Rouleredes.coe	
Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	223928
Entropy (8bit):	7.720384553629306
Encrypted:	false
SSDEEP:	3072:c5Nv/wHlbfgXh62+XKffH2i5A3Mz3xDD1TiBonOxOo0TUhBj4g2RgYyv:c5NvAbfgsrX6qMFdTiBQhooSBj4g2d4
MD5:	B32FFE1EC6ECA11009C35A0829450CB1
SHA1:	146529AFE038064ED79CAE0C62B108A14276D459
SHA-256:	151A299FCA8F459B7670EA4922931161D6E8024B19F1C723130F6576ACBDBC83
SHA-512:	CC32C0713B6E3C83D00682A73F2DB20FEAB0EBCD39A2CD768728FA9AD437CE0C24A6EBA7367DEC162447C14533064B93A2EB8422C843186AADADD6BEB99D7E4C
Malicious:	false
Preview:	..wh..8..ArM.0).LL....-G..t..N..."V.M.\og..Q].N...i.4...%.VV1.hK.'/..&.*$.U<....@.n..@..H.(.6.....C.i....z\uy.R.1.f...u.-..S..f....[5A..:b.....p...'..K..g.2O..A.....MGO....j.....l.N^.. .7W..$.6..D.q.....P&~.b4.Y8.@..n.....p..$.V.;.8\|k.\69+.P..Fr1.*.M$.Y.c..?.T...n.....0.....%.m%.#J._....<&-...%..v..4P..=..lz.YR.j.2.).j.*t..E.V.....U...7.R...G.+..ux.Fmg.n..D.. ..jz7...|...&.]K....A.....`oy..FM...(d:wx.._V....Y.bs..f.^$...Q.MZ.O.0.....x.a.t.nk.d....h3n.J8..R.$7..D2..g..f ...).c..=8C.. N.....B.a"...z..&...e.....'B%-2.Z.*.....&.B.....q5/..A .xG.R3B..@.\|.V.ss.*Y.P..iM.1.F0>....S..{gSc.^.<.kT..A.....%..w..A.....3..{.3id..?....-trml..O.....TH.qU.A.....].a.H.Q4.R.&.Dh.?....8e.....0Sf..r.....,_..S....~..<.i...*0.d.. .+.^..Ou(.6&.>....,*^.w....-:0..=."......l.....H....T.B.F.(..J.3#...f...8...-1.e...j.....{4....l....AG^%.....L./.$.....Qz.T.H.....1.r..?D8*'.n..b>(fo.w.....,....&.....}/6.(..#UJ0.lWB....

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\checkbox_checked.png	
Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	PNG image data, 32 x 32, 2-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	147
Entropy (8bit):	5.579261213353732
Encrypted:	false
SSDEEP:	3:yionv//thPl3MrpxyPuReVl/nRwPd/ggZcFmz3iVVyjXrC5RlH1p:6v/lhP6TwOeVV6Pd/MmgEK5RlVp
MD5:	0CA13C84736F193C4DDC36408B63EB79
SHA1:	DAF222B1B08D7F2645FDC2E25E63BE2AA50E9B79
SHA-256:	9B7DA86B40E8FE9DA37BA2A4337C9BCE14B07153A9722DD3DE7772C1C5933DED
SHA-512:	1F95694E920B1BE5A7D9A4C4F7EABCCDE8326965D8B1E3211085C67E84229F76300AED6AE29E2D79E817857CFE7608919233057FAD6FDA3BF515C59F3604099
Malicious:	false
Preview:	.PNG.....IHDR... ... .g....PLTE.....f.0....tRNS..v..8...7IDATx.c.....(."..@.& .....R;X...D8.....a^.....N'\..+....IEND.B`.

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\multimedia-volume-control-symbolic.svg	
Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	SVG Scalable Vector Graphics image

Category:	dropped
Size (bytes):	651
Entropy (8bit):	5.228667299529662
Encrypted:	false
SSDEEP:	12:t4Cp9xXnlWjoprGDWXYmfM26oprGhyGuC1hz4AeWrGdKdK:t4CpPlWsrGDoY32/rGYG/4AeWrGMQ
MD5:	367D90E6DF90CE72BAD009701DC3D941
SHA1:	C2070B79640687DBB8A64BFAC953CFA7625F7FFF
SHA-256:	2F11A00CC5DD755C1E5054AEF16CE293716532140B3DDB0F0623ABD460F99571
SHA-512:	F6DA3687D0676C11CD4B3D3F4C71797059DD62B05F09DC981684155671EB7924E6096B084DF43664D09B1A13BFADFE61C1FB678B3323ED7E9984EB8D7A2D19EC
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M2 5h2.484l2.97-3H8v12h-.475l-3.04-3H2z" style="marker:none" color="#bebebe" overflow="visible"/><path d="M14 8c0-2.166-.739-4.02-2-5h-1v2c.607.789 1 1.76 1 3 0 1.241-.393 2.22-1 3v2h1c1.223-.995 2-2.873 2-5z" style="marker:none" color="#000" overflow="visible"/><path d="M11 8c0-1.257-.312-2.216-1-3H9v6h1c.672-.837 1-1.742 1-3z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible"/></g></svg>

C:\Users\user\AppData\Local\Deskriptiv155\Hjertere\phone-symbolic.svg

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	629
Entropy (8bit):	4.45278069770929
Encrypted:	false
SSDEEP:	12:TMHdPnnl/nu3tln5CfYUtLLgpvAjmAKWlzmOA/e7/lsEbWlM:2dPnnxu3tlQfjngEmAKvOA/U/lsEbN
MD5:	DA3858070B89AA5D3B4D5FC724BED12F
SHA1:	A923CDD523E0519E96147A05DE6D0024135127E4
SHA-256:	3CC19ADDFE48119EB91D48E7FE510920394DC96F3006C384FFD4F63B92A73480
SHA-512:	FF7BE5CC591CD146E56DD22BCB9FD82A21272592EA7E807B57F8D33E77DA7FB2C632CA12980B0B8CDA4028C5802EA803BC75A642714B80AAC244538E4819E502
Malicious:	false
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 6 0 c -1.644531 0 -3 1.355469 -3 3 v 10 c 0 1.644531 1.355469 3 3 3 h 4 c 1.644531 0 3 -1.355469 3 -3 v -10 c 0 -1.644531 -1.355469 -3 -3 -3 z m 0 2 h 4 c 0.570312 0 1 0.429688 1 1 v 10 c 0 0.570312 -0.429688 1 -1 1 h -4 c -0.570312 0 -1 -0.429688 -1 -1 v -10 c 0 -0.570312 0.429688 -1 1 -1 z m 0 0"/>. <path d="m 7 1 h 2 c 0.550781 0 1 0.449219 1 1 s -0.449219 1 -1 1 h -2 c -0.550781 0 -1 -0.449219 -1 -1 s 0.449219 -1 1 -1 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E316
Malicious:	false
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Local\Temp\nssE334.tmp\System.dll

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.656065698421856
Encrypted:	false
SSDEEP:	192:eY24sihno00Wfl97nH6T2enXwWobpWBTU4VtHT7dmN35Ol+Sl:E8Qll975eXqlWBrz7YLOl+
MD5:	17ED1C86BD67E78ADE4712BE48A7D2BD
SHA1:	1CC9FE86D6D6030B4DAE45ECDDCE5907991C01A0

SHA-256:	BD046E6497B304E4EA4AB102CAB2B1F94CE09BDE0EEBBA4C59942A732679E4EB
SHA-512:	0CBED521E7D6D1F85977B3F7D3CA7AC34E1B5495B69FD8C7BFA1A846BAF53B0ECD06FE1AD02A3599082FFACAF8C71A3BB4E32DEC05F8E24859D736B828092CD5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....MX.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..b....P.....*.....@..B.....

C:\Users\user\AppData\Local\Temp\nsxE304.tmp

Process:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	296163
Entropy (8bit):	7.470506584929792
Encrypted:	false
SSDEEP:	6144:X5NvAbfgsrX6qMFdTiBQhooSBj4g2dgQ20cP7m:JjvTiapwjGdf20cP7m
MD5:	E0FD6297CF0E89D773C0AE44ED514229
SHA1:	EE4E3DEC2FFAD8B11887DD600B3A5D75982F0170
SHA-256:	5511DCF0AEFA2FDE583BEB5703774277C3ECB68B48AFA8B5D7F89F641B1F87F3
SHA-512:	5911A30953430870D7468C7BD48B57435FD6898800FC81EFA42FD340222E938D1C0889432C413163BC777044B412EF92A72740489FA620FE7220143D0A5A1C56
Malicious:	false
Preview:	.^.....,.....W...x?.....].....I^..... .....G...X.....j.....a..... .....

C:\Users\user\AppData\Local\Temp\subfolder1\Windowss.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	348136
Entropy (8bit):	7.836361315282437
Encrypted:	false
SSDEEP:	6144:twq3NpWyFr7S0HFwnNHF6pmK2DIuua9ma+T4cX+tTMZP3qtTaPwkYn5inpT4:tzayFfDwNg4RE864c4MZ/c2UinS
MD5:	91C0C4710DB096A4689D40E2CEB3814D
SHA1:	63880C602B960C5F91E55CBE4D5D18C7B8F1D63A
SHA-256:	A4D4961D124EA4276512C1584F1EBD30951CD469659B3A623594D6361772FAE7
SHA-512:	B5FC41A609EFB2946DDCE21F383B5AE8E70D93B0FD0DEC8E48B27F7660569CCDBAFE806BF56FC0CD7C4E43826B79F065D57CD66DA3C27E865CDCED3CA865EB2A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 47% • Antivirus: Virustotal, Detection: 46%, Browse
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...8.MX.....b...*.....J4.....@..... .....@.....text ....a.....b..... ..`.rdata.....f.....@..@.data...8.....z.....@....ndata.....rsrc.....@..@..... .....

C:\Users\user\AppData\Local\Temp\tmp673D.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.131285242271578
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnJxtn:cbk4oL600QydbQxIYODOLedq3ZJj
MD5:	497F298FC157762F192A7C42854C6FB6
SHA1:	04BEC630F5CC64EA17C0E3E780B3CCF15A35C6E0
SHA-256:	3462CBE62FBB64FC53A0FCF97E43BAAFE9DD9929204F586A86AFE4B89D8048A6
SHA-512:	C7C6FD3097F4D1CCD313160FEDF7CB031644E0836B8C3E25481095E5F4B003759BC84FC6EA9421E3A090E66DC2FF875FEC2F394A386691AB178CB164733411B

Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:7M:l
MD5:	E605984DC561B9F47F1CB5768EA0DF06
SHA1:	3CDBC8C449B53F919F51DA02322134F41B7ECB33
SHA-256:	026CF8CFDE23BEDCC5E60564D808C492580B9046DD1BDE5B1CF9167852986EA8
SHA-512:	3520CBDECFEC35785DCE152A84253934AAF3F554C1E74089010E556A9EA1D06EDB5E55D9F94CAB17281B2CD430B46C3FE8CE630D3CEB53C89B599928B1D23C4
Malicious:	**true**
Preview:	t...c..H

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bin

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\storage.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data

Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A0
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.l'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9..j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.745141646068962
Encrypted:	false
SSDEEP:	3:oMty8WbSmm:oMLWumm
MD5:	F781103B538E4159A8F01E3BE09B1F8D
SHA1:	27992585DE22A095BABCFD75E8F96710DD921C37
SHA-256:	BEA91983791C26C19AA411B2870E89AFC250EAF9855B6E1CE7BEA02B74E7F368
SHA-512:	D50AE0A01E74FC263B704FADE17CDF4993B61E34FD498827D546F090CE2DA5E8F24D4D34FBF360AE7EE5C5E7E3F032F3DDA8AD0C2A2CF0E1DAFEED61258AB4CA
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	182
Entropy (8bit):	5.07060597644582
Encrypted:	false
SSDEEP:	3:RGXKRjN3Mxm8d/AjhclROXDD9jmKXVM8/FOoDamd9xraWMZ4MKLJFcLEWgJya7:zx3M7ucLOdBXVNYmd9NaWM6MKnH5JyY
MD5:	B08826036A3E81B44E7D8C1284381013
SHA1:	96CF7E6BC1B55C69CE33BEC3B78FFF4EB8839B87
SHA-256:	E7AD5092F56BB2ACA26262C361FE5F83171D21AB134D4E5D2EF47E9BF641B549
SHA-512:	EB9908F6FB6398EDCE4F3B18AA64ABEE8774D1CA3A5B533617C97AAC5E795627CCB8B1176BE64371E6BEF6352004FC2B4862A388D61A6103D05B5B2D02CD0481
Malicious:	false
Preview:	Microsoft (R) .NET Framework CasPol 2.0.50727.9149..Copyright (c) Microsoft Corporation. All rights reserved.....ERROR: Invalid option: 0....For usage information, use 'caspol -?'..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.836361315282437
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:	DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe

File size:	348136
MD5:	91c0c4710db096a4689d40e2ceb3814d
SHA1:	63880c602b960c5f91e55cbe4d5d18c7b8f1d63a
SHA256:	a4d4961d124ea4276512c1584f1ebd30951cd469659b3a623594d6361772fae7
SHA512:	b5fc41a609efb2946ddce21f383b5ae8e70d93b0fd0dec8e48b27f7660569ccdbafe806bf56fc0cd7c4e43826b79f065d57cd66da3c27e865cdced3ca865eb2a
SSDEEP:	6144:twq3NpWyFr7S0HFwnNHF6pmK2DIuua9ma+T4cX+tTMZP3qtTaPwkYn5inpT4:tzayFfDwNg4RE864c4MZ/c2UinS
TLSH:	C6741208B548D9A7C9630932ED628AF67ABDDE613BB1A70733006F7C7D312618F45365
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...8.MX.....b...*.....J4.....@

File Icon

Icon Hash:	00c4c4dcdcd4d410

Static PE Info

General

Entrypoint:	0x40344a
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:	0x584DCA38 [Sun Dec 11 21:50:48 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
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 00007F9DD91D3BA3h
push ebx
call 00007F9DD91D6CFCh
cmp eax, ebx
je 00007F9DD91D3B99h
push 00000C00h
call eax

Instruction
mov esi, 004082B8h
push esi
call 00007F9DD91D6C76h
push esi
call dword ptr [0040815Ch]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F9DD91D3B7Ch
push ebp
push 00000009h
call 00007F9DD91D6CCEh
push 00000007h
call 00007F9DD91D6CC7h
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 00007F9DD91D68B0h
call dword ptr [004080ACh]
mov ebp, 00435000h
push eax
push ebp
call 00007F9DD91D689Eh
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	0x68000	0x19ef0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	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	0x61f1	0x6200	False	0.6656967474489796	data	6.477074763411717	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	0.501953125	data	3.9745558434885093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x3d000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x68000	0x19ef0	0x1a000	False	0.8527644230769231	data	7.543225711963014	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x683a0	0xbdfc	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x741a0	0x743a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x7b5e0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x7db88	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x7ec30	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x7fad8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x80380	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0x809e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x80f50	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x813b8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x816a0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x817c8	0x100	data	English	United States
RT_DIALOG	0x818c8	0x11c	data	English	United States
RT_DIALOG	0x819e8	0xc4	data	English	United States
RT_DIALOG	0x81ab0	0x60	data	English	United States
RT_GROUP_ICON	0x81b10	0xa0	data	English	United States
RT_MANIFEST	0x81bb0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

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

DLL	Import
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

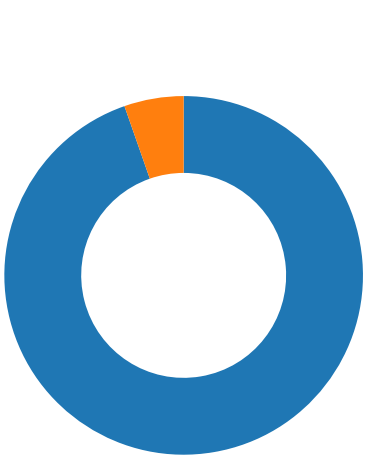
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
91.193.75.146192.168.11.203498498572810451 02/04/23-04:02:00.606308	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	3498	49857	91.193.75.146	192.168.11.20
192.168.11.2091.193.75.1464985734982816766 02/04/23-04:02:49.236881	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49857	3498	192.168.11.20	91.193.75.146
91.193.75.146192.168.11.203498498572810290 02/04/23-04:02:33.039323	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	3498	49857	91.193.75.146	192.168.11.20
192.168.11.2091.193.75.1464985734982025019 02/04/23-03:57:12.109194	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49857	3498	192.168.11.20	91.193.75.146
91.193.75.146192.168.11.203498498572841753 02/04/23-04:02:50.692460	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	3498	49857	91.193.75.146	192.168.11.20
192.168.11.2091.193.75.1464985734982816718 02/04/23-04:02:19.821499	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49857	3498	192.168.11.20	91.193.75.146

Network Port Distribution

Total Packets: 56

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 03:57:07.247711897 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.247756958 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.248142004 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.266587973 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.266625881 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.325129986 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.325377941 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.325377941 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.327606916 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.327816963 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.395785093 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.395886898 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.397012949 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.397233009 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.400418043 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.444497108 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.941315889 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.941545963 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.941631079 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.941788912 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.941920042 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:07.942172050 CET	443	49855	142.250.185.110	192.168.11.20
Feb 4, 2023 03:57:07.942363977 CET	49855	443	192.168.11.20	142.250.185.110
Feb 4, 2023 03:57:08.066267014 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.066365004 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.066636086 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.066870928 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.066915989 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.109862089 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.110160112 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.110721111 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.110939026 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.110939026 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.114398003 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.114425898 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.114804029 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.114958048 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.115420103 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.156486034 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.428867102 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.429054022 CET	49856	443	192.168.11.20	142.250.186.161

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 03:57:08.429109097 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.429677963 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.429836988 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.429837942 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.430469036 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.430753946 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.431325912 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.431509972 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.431567907 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.431759119 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.433943033 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.434127092 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.434180021 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.434446096 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.436647892 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.436927080 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.437504053 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.437681913 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.437737942 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.437948942 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.438008070 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.438170910 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.438222885 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.438263893 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.438333988 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.438430071 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.438463926 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.438666105 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.438920975 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.439110994 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.439165115 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.439433098 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.439486980 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.439693928 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.439755917 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.439925909 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.439964056 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.440180063 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.440222979 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.440383911 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.440632105 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.440804005 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.440854073 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.441011906 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.441065073 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.441524029 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.441632032 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.441922903 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.441956997 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.442022085 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.442126036 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.442212105 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.442545891 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.442792892 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.442836046 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.442862034 CET	443	49856	142.250.186.161	192.168.11.20
Feb 4, 2023 03:57:08.443027020 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.443027973 CET	49856	443	192.168.11.20	142.250.186.161
Feb 4, 2023 03:57:08.443404913 CET	443	49856	142.250.186.161	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2023 03:57:07.229824066 CET	51329	53	192.168.11.20	1.1.1.1
Feb 4, 2023 03:57:07.239095926 CET	53	51329	1.1.1.1	192.168.11.20
Feb 4, 2023 03:57:08.025192976 CET	54127	53	192.168.11.20	1.1.1.1
Feb 4, 2023 03:57:08.065241098 CET	53	54127	1.1.1.1	192.168.11.20
Feb 4, 2023 03:57:09.862443924 CET	55766	53	192.168.11.20	1.1.1.1
Feb 4, 2023 03:57:09.968810081 CET	53	55766	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
Feb 4, 2023 03:57:07.229824066 CET	192.168.11.20	1.1.1.1	0xbccb	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Feb 4, 2023 03:57:08.025192976 CET	192.168.11.20	1.1.1.1	0x6144	Standard query (0)	doc-0c-b0-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false
Feb 4, 2023 03:57:09.862443924 CET	192.168.11.20	1.1.1.1	0xf9a	Standard query (0)	masterpat0nms672ns.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

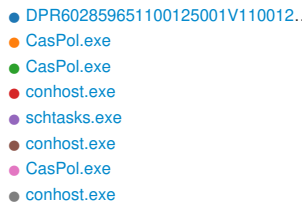
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 4, 2023 03:57:07.239095926 CET	1.1.1.1	192.168.11.20	0xbccb	No error (0)	drive.google.com		142.250.185.110	A (IP address)	IN (0x0001)	false
Feb 4, 2023 03:57:08.065241098 CET	1.1.1.1	192.168.11.20	0x6144	No error (0)	doc-0c-b0-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 4, 2023 03:57:08.065241098 CET	1.1.1.1	192.168.11.20	0x6144	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.161	A (IP address)	IN (0x0001)	false
Feb 4, 2023 03:57:09.968810081 CET	1.1.1.1	192.168.11.20	0xf9a	No error (0)	masterpat0nms672ns.duckdns.org		91.193.75.146	A (IP address)	IN (0x0001)	false

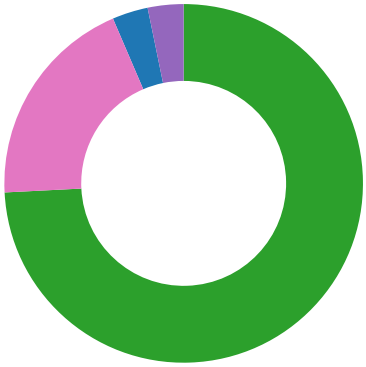
HTTP Request Dependency Graph

- drive.google.com
- doc-0c-b0-docs.googleusercontent.com

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe PID: **2948**, Parent PID: **4932**

General

Target ID:	2
Start time:	03:54:23
Start date:	04/02/2023
Path:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Imagebase:	0x400000
File size:	348136 bytes
MD5 hash:	91C0C4710DB096A4689D40E2CEB3814D
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: 00000002.00000002.167511188846.0000000008C46000.00000040.00001000.00020000.00000000.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: **4376**, Parent PID: **2948**

General

Target ID:	7
Start time:	03:56:47
Start date:	04/02/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Imagebase:	0x7ff683850000
File size:	106496 bytes

MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **7876**, Parent PID: **2948**

General

Target ID:	8
Start time:	03:56:47
Start date:	04/02/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe
Imagebase:	0xd80000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000008.00000003.167512023875.0000000039142000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000008.00000003.167512023875.0000000039142000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\subfolder1\Windowss.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	5621D7F	CreateFileW
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	5621D7F	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	5621D7F	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5621D7F	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	5621D7F	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	5621D7F	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	5621D7F	InternetOpenUrlA

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	6D1C614C	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	6D1C614C	unknown
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3A1B0E61	CreateDirectoryW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	3A1B0F5B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp673D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3A1B122C	GetTempFileNameW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	3A1B0F5B	CreateFileW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3A1B0E61	CreateDirectoryW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3A1B0E61	CreateDirectoryW
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	6D1C614C	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	6D1C614C	unknown
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	3A1B0F5B	CreateFileW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	3A1B0F5B	CreateFileW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	3A1B0F5B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp673D.tmp	success or wait	1	3A1B006E	DeleteFileW

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\Temp\subfolder1\Windowss.exe	0	348136	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd 31 fd fd 50 fd fd fd 50 fd fd fd 50 fd fd 2a 5f fd fd fd 50 fd fd fd 50 fd fd 4f 50 fd fd 2a 5f fd fd fd 50 fd bd 73 fd fd fd 50 fd fd 2e 56 fd fd fd 50 fd fd 52 69 63 68 fd 50 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 38 fd 4d 58 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 62 00 00 00 2a 02 00 00 08 00 00 4a 34 00 00 00 10 00 00 00 fd 00 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$1PPP*_PPOP*_Ps P.VPRichPPEL8MXb*J4@	success or wait	2	55FC1D5	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	0	8	74 fd 1a fd 63 06 fd 48	tcH	success or wait	1	3A1B1113	WriteFile
C:\Users\user\AppData\Local\Temp\tmp673D.tmp	0	1319	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	3A1B1113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat	0	56	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 63 61 73 70 6f 6c 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe	success or wait	1	3A1B1113	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	1	3A1B1113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\storage.dat	0	426832	fd fd 67 26 6a 6f 1f 01 fd 49 50 67 08 fd 62 47 4d 64 fd 0d fd 52 3e 69 fd fd 09 6f fd fd 04 49 fd 3e f0 26 fd 72 7b fd fd fd fd 38 fd e5 fd 7d fd 89 fd 45 03 7f fd fd 76 fd 21 37 fd 75 33 65 fd fd 20 fd fd 05 fd fd 64 62 fd fd 15 7d fd fd 1d 02 02 fd fd 22 fd 74 28 06 78 43 39 fd 63 70 15 42 fd fd fd fd 37 fd 0f 1b 27 fd fd fd fd fd 7f fd 25 fd 09 fd 06 fd fd 77 fd 5e fd fd 5f 13 fd fd 02 1d 34 fd 42 fd 57 25 fd 3c a6 64 69 fd 30 fd 7b 39 fd 78 53 fd fd fd 35 fd fd fd 29 05 fd 77 fd 0f 24 14 fd 43 fd fd 3f 60 46 cf fd 75 fd 35 d2 54 fd 58 fd 77 27 53 69 fd fd 7a fd 6e 7b fd fd c4 59 21 6d fd fd 1c 52 41 fd fd fd 78 67 fd 3a 03 fd 5b 37 fd 18 fd 7a fd fd 39 40 02 4b fd 2d fd fd fd 54 fd fd 2b fd 41 43 65	g&joIPgGMR>ioI>&r{8}E v!7u3e db }"t(xC9cpB7'%w^_BW% <i0{9xS5)w$C? `Fu5TXw'Sizn{Y!mRAxg[7z9@K-T+ACe	success or wait	1	3A1B1113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	3A1B1113	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DPR602859651100125001V1100125154830E 3-2-2023#U00b7pdf.exe	unknown	348136	success or wait	1	5621D7F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	6D1F87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	6D1F87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6D1F87D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	4096	success or wait	1	6D29BFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	512	success or wait	1	6D29BFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6D1F55E4	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3A1B1113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	3A1B1113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	3A1B1113	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\AppData\Local\Temp\subfolder1\Windowss.exe	success or wait	1	55FB530	RegSetValueExA

Analysis Process: conhost.exe PID: **872**, Parent PID: **7876**

General

Target ID:	9
Start time:	03:56:47
Start date:	04/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff683850000
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

Analysis Process: schtasks.exe PID: **6764**, Parent PID: **7876**

General

Target ID:	10
Start time:	03:57:08
Start date:	04/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DSL Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp673D.tmp
Imagebase:	0x140000
File size:	187904 bytes
MD5 hash:	478BEAEC1C3A9417272BC8964ADD1CEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp673D.tmp	unknown	2	success or wait	1	14B43E	ReadFile
C:\Users\user\AppData\Local\Temp\tmp673D.tmp	unknown	1320	success or wait	1	14B4E3	ReadFile

Analysis Process: conhost.exe PID: **1760**, Parent PID: **6764**

General

Target ID:	11
Start time:	03:57:08
Start date:	04/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff683850000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: CasPol.exe PID: **4756**, Parent PID: **1424**

General

Target ID:	12
Start time:	03:57:09
Start date:	04/02/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe 0
Imagebase:	0xd10000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6D1C614C	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	6D1C614C	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D1B3547	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	166A53F	WriteFile
\Device\ConDrv	52	52	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73	Copyright (c) Microsoft Corporation. All rights res	success or wait	3	166A53F	WriteFile
\Device\ConDrv	140	26	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	For usage information, u	success or wait	2	166A53F	WriteFile
\Device\ConDrv	182	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	166A53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log	0	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0	success or wait	1	6D49ACA5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	6D1F55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	6D1F55E4	unknown

Analysis Process: conhost.exe PID: **4456**, Parent PID: **4756**

General

Target ID:	13
Start time:	03:57:09
Start date:	04/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff700660000
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