


**ID:** 634139
**Sample Name:** pago.exe
**Cookbook:** default.jbs
**Time:** 16:54:53
**Date:** 25/05/2022
**Version:** 34.0.0 Boulder Opal

# Table of Contents

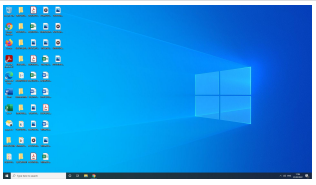
# Windows Analysis Report

## pago.exe

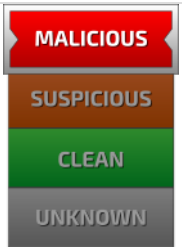
## Overview

### General Information

| | |
|---|---|
| Sample Name: | pago.exe |
| Analysis ID: | 634139 |
| MD5: | 41db491c763c2a.. |
| SHA1: | 20c45ae71feccf7.. |
| SHA256: | 904211f6f92bb8e. |
| Infos: | |



### Detection



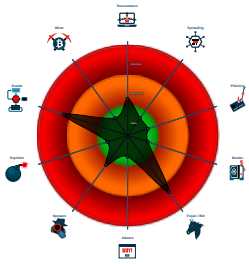

**GuLoader**

| | |
|---|---|
| Score: | 80 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- May sleep (evasive loops) to hinder…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Detected potential crypto function

### Classification



## Process Tree

- **System is w10x64native**
- pago.exe (PID: 3984 cmdline: "C:\Users\user\Desktop\pago.exe" MD5: 41DB491C763C2AA61A8F4305591E3139)
  - CasPol.exe (PID: 6636 cmdline: "C:\Users\user\Desktop\pago.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 3936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=14p4RqgiFGwvudzlCweA8Cs_gKBFB_1pQ`5"
}
```

## Yara Signatures

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000001.00000002.10964117045.0000000002BA0000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |
| 00000003.00000000.10305977883.0000000001100000.00000040.00000400.00020000.00000000.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

### Networking

C2 URLs / IPs found in malware configuration

### Data Obfuscation

Yara detected GuLoader

### Malware Analysis System Evasion

Tries to detect Any.run

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

### HIPS / PFW / Operating System Protection Evasion

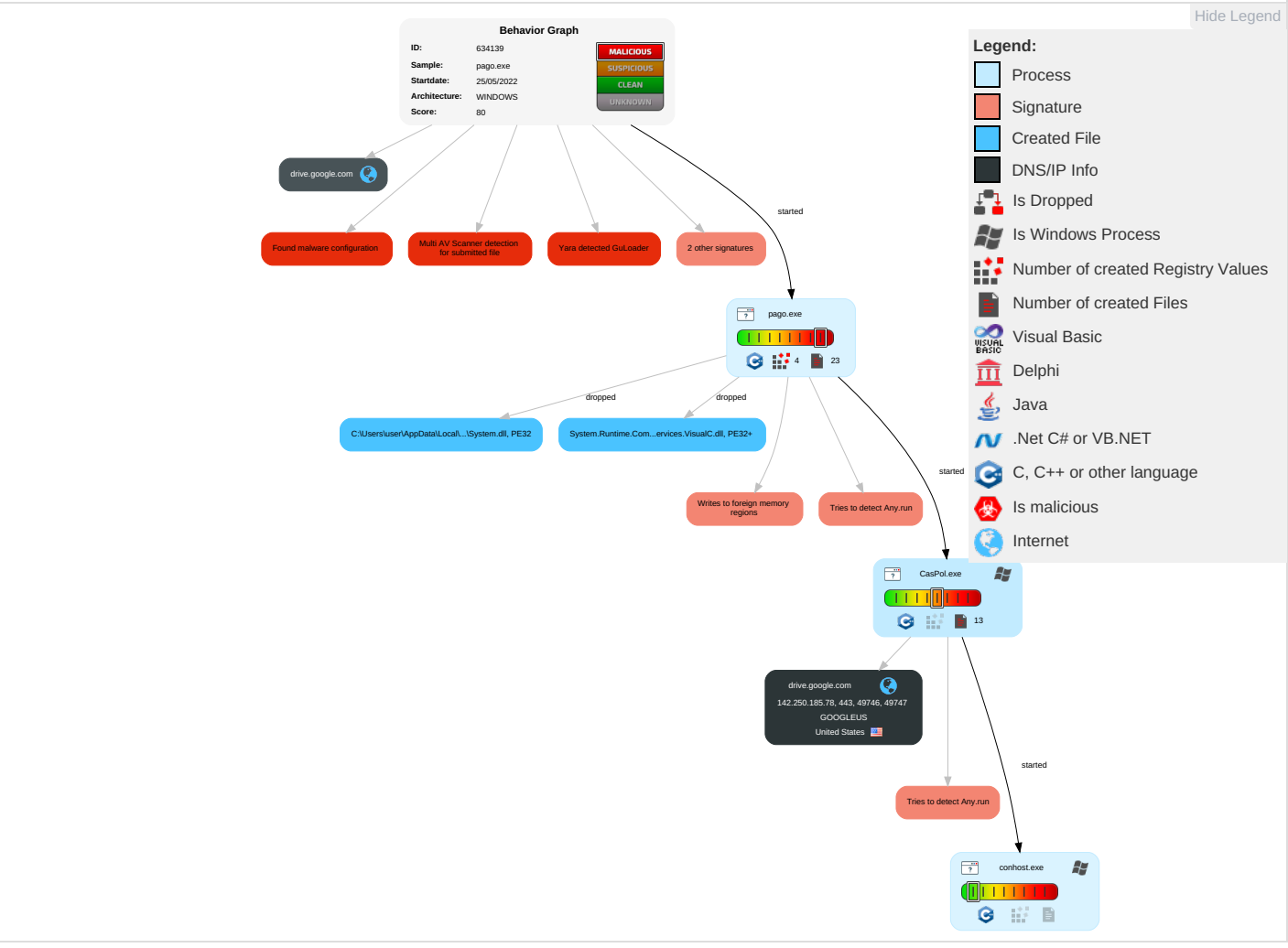
Writes to foreign memory regions

## 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 Native API | 1 DLL Side-Loading | 1 Access Token Manipulation | 1 2 Virtualization/Sandbox Evasion | OS Credential Dumping | 2 2 1 Security Software Discovery | Remote Services | 1 Archive Collected Data | Exfiltration Over Other Network Medium | 1 2 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | 1 System Shutdown/ Reboot |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | 1 1 1 Process Injection | 1 Access Token Manipulation | LSASS Memory | 1 2 Virtualization/Sandbox Evasion | Remote Desktop Protocol | 1 Clipboard Data | Exfiltration Over Bluetooth | 1 Non-Application Layer Protocol | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | 1 DLL Side-Loading | 1 1 1 Process Injection | Security Account Manager | 1 Application Window Discovery | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 1 2 Application Layer Protocol | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 1 Obfuscated Files or Information | NTDS | 2 File and Directory Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 1 Timestomp | LSA Secrets | 4 System Information Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 1 DLL Side-Loading | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |

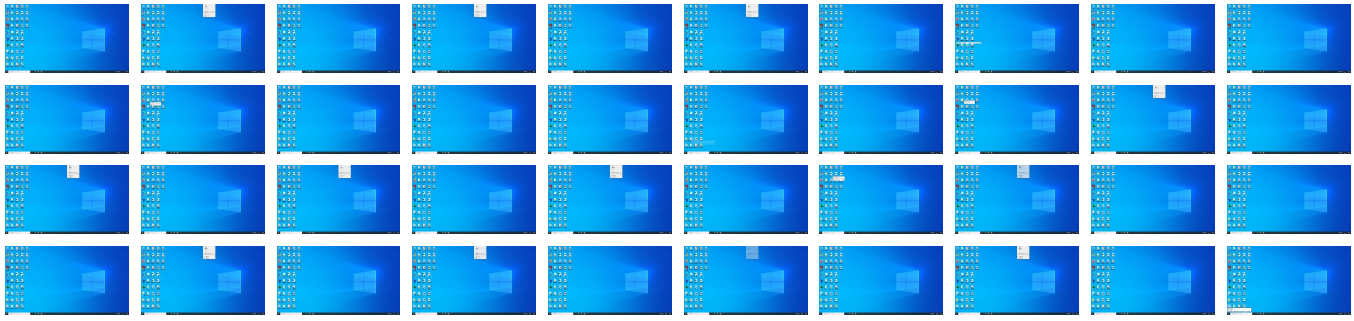
## Behavior Graph

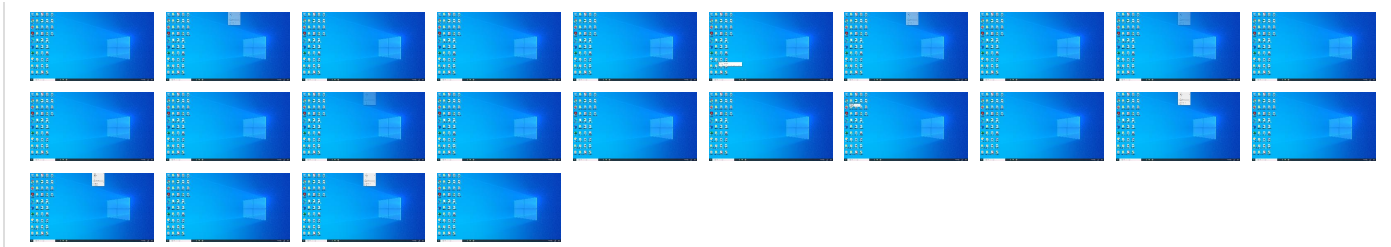



## Screenshots

### 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 |
|---|---|---|---|---|
| pago.exe | 32% | Virustotal | | Browse |
| pago.exe | 5% | ReversingLabs | Win32.Downloader.GuLoader | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\nsrF138.tmp\System.dll | 3% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsrF138.tmp\System.dll | 0% | ReversingLabs | | |

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://csp.wit | 0% | Avira URL Cloud | safe | |
| http://https://csp.wit= | 0% | Avira URL Cloud | safe | |
| http://https://csp.wit; | 0% | Avira URL Cloud | safe | |
| http://https://csp.wit9 | 0% | Avira URL Cloud | safe | |
| http://https://csp.wit%Z | 0% | Avira URL Cloud | safe | |
| http://subca.ocsp-certum.com05 | 0% | Avira URL Cloud | safe | |
| http://subca.ocsp-certum.com02 | 0% | Avira URL Cloud | safe | |
| http://subca.ocsp-certum.com01 | 0% | Avira URL Cloud | safe | |
| http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external | 0% | Avira URL Cloud | safe | |
| http://https://csp.wit?_ | 0% | Avira URL Cloud | safe | |

## Domains and IPs

### Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| drive.google.com | 142.250.185.78 | true | false | | high |

### URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/EN | CasPol.exe, 00000003.00000003.1051247523<br>4.0000000001644000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.10473851646.0000000001644000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10462243<br>555.0000000001644000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.10470093101.000000000164400<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10450877531.0000<br>000001644000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.10590133678.0000000001644000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10454670711.000000000164<br>4000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10497322070.0<br>0000000001644000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.10466142710.0000000001644000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.10501316607<br>.0000000001644000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.10458487274.0000000001644000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.105865467<br>30.0000000001644000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.10481515123.0000000001644000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10493368770.00000<br>00001644000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.10508779607.0000000001644000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10485368855.0000000001644<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10505157106.00<br>00000001644000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.10477673791.0000000001644000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.10489320415.<br>0000000001644000.00000004.00000020.00020<br>000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/Nx | CasPol.exe, 00000003.00000003.1132965875<br>6.0000000001652000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.11005886364.0000000001652000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11326002<br>160.0000000001652000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.10454779102.000000000165200<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10990500451.0000<br>000001652000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.11691835610.0000000001652000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11651022001.000000000165<br>2000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10450948577.0<br>000000001652000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11197437395.0000000001652000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.11778679798<br>.0000000001652000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.11775025967.0000000001652000.0<br>0000004.00000020.00020000.00000000.sdmp | false | | high |
| http://crl.certum.pl/ctsca2021.crl0o | pago.exe | false | | high |
| http://repository.certum.pl/ctnca.cer09 | pago.exe | false | | high |
| http://crl.certum.pl/ctnca.crl0k | pago.exe | false | | high |
| http://https://drive.google.com/pNA | CasPol.exe, 00000003.00000003.1044323385<br>4.0000000001644000.00000004.00000020.000<br>20000.00000000.sdmp | false | | high |
| http://https://drive.google.com/or | CasPol.exe, 00000003.00000003.1047734763<br>7.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.10458150869.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10481182<br>540.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.10442906491.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10489062079.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.10473539920.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10435303653.000000000161<br>0000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10439116142.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.10589857417.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.10469767911<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.10586224494.0000000001610000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.104850582<br>31.0000000001610000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.10725676845.0000000001610000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10496974061.00000<br>00001610000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.10722204238.0000000001610000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10465841943.0000000001610<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10500989666.00<br>00000001610000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.10512175315.0000000001610000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.10461940744.<br>0000000001610000.00000004.00000020.00020<br>000.00000000.sdmp, CasPol.exe, 00000003.<br>00000003.10493005273.0000000001610000.00<br>000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.1045059117<br>6.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://csp.wit | CasPol.exe, 00000003.00000003.1128838583 6.0000000001641000.00000004.00000020.000 20000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://drive.google.com/r | CasPol.exe, 00000003.00000003.1142778860 1.0000000001652000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11412959950.0000000001652000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11888411 931.0000000001652000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10737542731.000000000165200 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11431329632.0000 000001652000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.11884685432.0000000001652000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11877288268.000000000165 2000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11088531521.0 000000001652000.00000004.00000020.000200 00.00000000.sdmp | false | | high |
| http://https://drive.google.com/&xx | CasPol.exe, 00000003.00000003.1154113146 2.0000000001652000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10960956292.0000000001652000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11385693 456.0000000001652000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10812894314.000000000165200 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11381866487.0000 000001652000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.10823870957.0000000001652000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10968641946.000000000165 2000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10903513518.0 000000001652000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.11277670821.0000000001652000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.11146628922 .0000000001652000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000003 .00000003.10590205424.0000000001652000.0 0000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.109722812 60.0000000001652000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 03.00000003.10979625239.0000000001652000 .00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10899832876.00000 00001652000.00000004.00000020.00020000.0 0000000.sdmp, CasPol.exe, 00000003.00000 003.11563332151.0000000001652000.0000000 4.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10733897731.0000000001652 000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11566967101.00 00000001652000.00000004.00000020.0002000 0.00000000.sdmp, CasPol.exe, 00000003.00 000003.10957408022.0000000001652000.0000 0004.00000020.00020000.00000000.sdmp, Ca sPol.exe, 00000003.00000003.11190168208. 0000000001652000.00000004.00000020.00020 000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/0 | CasPol.exe, 00000003.00000003.1087475289 3.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11430915788.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11370430 339.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10852845632.000000000161000 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11936516446.0000 000001610000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.10986315495.0000000001610000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11522651189.000000000161 0000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10819644928.0 000000001610000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.11880488126.0000000001610000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.11240029390 .0000000001610000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000003 .00000003.11409010342.0000000001610000.0 0000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.112187021 23.0000000001610000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 03.00000003.11664820128.0000000001610000 .00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11025068972.00000 00001610000.00000004.00000020.00020000.0 0000000.sdmp, CasPol.exe, 00000003.00000 003.11452754183.0000000001610000.0000000 4.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11032375205.0000000001610 000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11796544361.00 000000001610000.00000004.00000020.0002000 0.00000000.sdmp, CasPol.exe, 00000003.00 000003.11624374128.0000000001610000.0000 0004.00000020.00020000.00000000.sdmp, Ca sPol.exe, 00000003.00000003.11113467457. 0000000001610000.00000004.00000020.00020 000.00000000.sdmp, CasPol.exe, 00000003. 00000003.10777826659.0000000001610000.00 000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.1075618370 9.0000000001610000.00000004.00000020.000 20000.00000000.sdmp | false | | high |
| http://https://drive.google.com/N | CasPol.exe, 00000003.00000003.1058985741 7.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10586224494.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10725676 845.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10722204238.000000000161000 0.00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://csp.wit= | CasPol.exe, 00000003.00000003.1111346745 7.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11120500920.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11116994 997.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.11131458070.000000000161000 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11124152394.0000 000001610000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.11127780563.0000000001610000.000000 04.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | low |
| http://nsis.sf.net/NSIS_ErrorError | pago.exe | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/D | CasPol.exe, 00000003.00000003.1143091578<br>8.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.11370430339.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11522651<br>189.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.11240029390.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11409010342.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.11218702123.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11664820128.000000000161<br>0000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11452754183.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11624374128.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.11113467457<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.11643187107.0000000001610000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.111386766<br>39.0000000001610000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.11381318779.0000000001610000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11654105332.00000<br>00001610000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.11471038381.0000000001610000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11333346775.0000000001610<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11200613571.00<br>00000001610000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.11725868249.0000000001610000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.11236564730.<br>0000000001610000.00000004.00000020.00020<br>000.00000000.sdmp, CasPol.exe, 00000003.<br>00000003.11481937364.0000000001610000.00<br>000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.1148997369<br>6.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp | false | | high |
| http://https://csp.wit; | CasPol.exe, 00000003.00000003.1191025937<br>0.0000000001641000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.11591361210.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11584109<br>786.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.11566539347.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11587826848.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.11602128374.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11906616575.000000000164<br>1000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11595022091.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11598710092.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.11570352755<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp | false | • Avira URL Cloud: safe | low |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/:O | CasPol.exe, 00000003.00000003.1044705726 9.0000000001644000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10450877531.0000000001644000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10443233 854.0000000001644000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10454670711.000000000164400 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10439433586.0000 000001644000.00000004.00000020.00020000. 00000000.sdmp | false | | high |
| http://https://csp.wit9 | CasPol.exe, 00000003.00000003.1165410533 2.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11646915586.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11650600 802.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.11657721764.000000000161000 0.00000004.00000020.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://github.com/dotnet/runtime | System.Runtime.CompilerServices.VisualC.dll.1.dr | false | | high |
| http://https://csp.wit%Z | CasPol.exe, 00000003.00000003.1179654436 1.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11752718459.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11763848 646.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.11785504010.000000000161000 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11767485841.0000 000001610000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.11017932797.0000000001610000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11760090323.000000000161 0000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11792762219.0 000000001610000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.11789379310.0000000001610000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.11756813377 .0000000001641000.00000004.00000020.0002 0000.00000000.sdmp | false | • Avira URL Cloud: safe | low |
| http://https://drive.google.com/DO | CasPol.exe, 00000003.00000003.1044705726 9.0000000001644000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10462243555.0000000001644000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10431930 783.0000000001644000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10470093101.000000000164400 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10450877531.0000 000001644000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.10443233854.0000000001644000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10454670711.000000000164 4000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10466142710.0 000000001644000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.10458487274.0000000001644000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.10439433586 .0000000001644000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000003 .00000003.10435616398.0000000001644000.0 0000004.00000020.00020000.00000000.sdmp | false | | high |
| http://repository.certum.pl/ctsca2021.cer0 | pago.exe | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/X | CasPol.exe, 00000003.00000003.1047734763 7.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10874752893.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11430915 788.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.11370430339.000000000161000 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10852845632.0000 000001610000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.11936516446.0000000001610000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10458150869.000000000161 0000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10986315495.0 000000001610000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.11522651189.0000000001610000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.10819644928 .0000000001610000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000003 .00000003.11880488126.0000000001610000.0 0000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.112400293 90.0000000001610000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 03.00000003.11409010342.0000000001610000 .00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11218702123.00000 00001610000.00000004.00000020.00020000.0 0000000.sdmp, CasPol.exe, 00000003.00000 003.11664820128.0000000001610000.0000000 4.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11025068972.0000000001610 000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10729536768.00 000000001610000.00000004.00000020.0002000 0.00000000.sdmp, CasPol.exe, 00000003.00 000003.11452754183.0000000001610000.0000 0004.00000020.00020000.00000000.sdmp, Ca sPol.exe, 00000003.00000003.11032375205. 0000000001610000.00000004.00000020.00020 000.00000000.sdmp, CasPol.exe, 00000003. 00000003.11796544361.0000000001610000.00 000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.1162437412 8.0000000001610000.00000004.00000020.000 20000.00000000.sdmp | false | | high |
| http://subca.ocsp-certum.com05 | pago.exe | false | • Avira URL Cloud: safe | unknown |
| http://https://drive.google.com/ | CasPol.exe, 00000003.00000003.1080524955 7.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11190168208.0000000001652000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11873151 954.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.11551627441.000000000161000 0.00000004.00000020.00020000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/V | CasPol.exe, 00000003.00000003.1047734763<br>7.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.10874752893.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11430915<br>788.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.11370430339.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10852845632.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.11936516446.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10458150869.000000000161<br>0000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10986315495.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11522651189.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.10819644928<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.11880488126.0000000001610000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.112400293<br>90.0000000001610000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.11409010342.0000000001610000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11218702123.00000<br>00001610000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.11664820128.0000000001610000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11025068972.0000000001610<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10729536768.00<br>00000001610000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.11452754183.0000000001610000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.11032375205.<br>0000000001610000.00000004.00000020.00020<br>000.00000000.sdmp, CasPol.exe, 00000003.<br>00000003.11796544361.0000000001610000.00<br>000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.1162437412<br>8.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/ertificates | CasPol.exe, 00000003.00000003.1047734763<br>7.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.10874752893.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10852845<br>632.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.10458150869.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10986315495.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.10819644928.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11025068972.000000000161<br>0000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10729536768.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11032375205.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.10777826659<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.10756183709.0000000001610000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.110010157<br>20.0000000001610000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.10481182540.0000000001610000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11013074459.00000<br>00001610000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.10845316161.0000000001610000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10838156567.0000000001610<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10442906491.00<br>00000001610000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.11062778150.0000000001610000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.10489062079.<br>0000000001610000.00000004.00000020.00020<br>000.00000000.sdmp, CasPol.exe, 00000003.<br>00000003.10990071600.0000000001610000.00<br>000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.1089574010<br>6.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/vy | CasPol.exe, 00000003.00000003.1131841880 8.0000000001652000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11599073404.0000000001652000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11595481 769.0000000001652000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10794875834.000000000165200 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11719025756.0000 000001652000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.11658141520.0000000001652000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11109860515.000000000165 2000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11807865757.0 000000001652000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.11204814683.0000000001652000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.11613837370 .0000000001652000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000003 .00000003.11811534853.0000000001652000.0 0000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.116175176 62.0000000001652000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 03.00000003.11270221356.0000000001652000 .00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11661625882.00000 00001652000.00000004.00000020.00020000.0 0000000.sdmp, CasPol.exe, 00000003.00000 003.11621145763.0000000001652000.0000000 4.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11113913042.0000000001652 000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11013524081.00 000000001652000.00000004.00000020.0002000 0.00000000.sdmp | false | | high |
| http://subca.ocsp-certum.com02 | pago.exe | false | • Avira URL Cloud: safe | unknown |
| http://subca.ocsp-certum.com01 | pago.exe | false | • Avira URL Cloud: safe | unknown |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external | CasPol.exe, 00000003.00000003.1143091578 8.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11370430339.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11714178 018.0000000001641000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.11936516446.000000000161000 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10986315495.0000 000001610000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.11880488126.0000000001610000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11240029390.000000000161 0000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11409010342.0 000000001610000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.11218702123.0000000001610000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.10942261401 .0000000001643000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000003 .00000003.10938392847.0000000001643000.0 0000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.116648201 28.0000000001610000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 03.00000003.11899268890.0000000001641000 .00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11452754183.00000 00001610000.00000004.00000020.00020000.0 0000000.sdmp, CasPol.exe, 00000003.00000 003.11796544361.0000000001610000.0000000 4.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11624374128.0000000001610 000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11113467457.00 000000001610000.00000004.00000020.0002000 0.00000000.sdmp, CasPol.exe, 00000003.00 000003.11643187107.0000000001610000.0000 0004.00000020.00020000.00000000.sdmp, Ca sPol.exe, 00000003.00000003.11001015720. 0000000001610000.00000004.00000020.00020 000.00000000.sdmp, CasPol.exe, 00000003. 00000003.11381318779.0000000001610000.00 000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.1106654465 3.0000000001642000.00000004.00000020.000 20000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://drive.google.com/gN | CasPol.exe, 00000003.00000003.1044705726 9.0000000001644000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10450877531.0000000001644000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10443233 854.0000000001644000.00000004.00000020.0 0020000.00000000.sdmp | false | | high |
| http://crl.certum.pl/ctnca2.crl0l | pago.exe | false | | high |
| http://repository.certum.pl/ctnca2.cer09 | pago.exe | false | | high |
| http://https://drive.google.com/tagservices-cn.com | CasPol.exe, 00000003.00000003.1059020542 4.0000000001652000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10586662872.0000000001652000. 00000004.00000020.00020000.00000000.sdmp | false | | high |
| http://https://drive.google.com/crosoft | CasPol.exe, 00000003.00000003.1155162744 1.0000000001610000.00000004.00000020.000 20000.00000000.sdmp | false | | high |
| http://https://github.com/dotnet/runtimeBSJB | System.Runtime.CompilerServices.VisualC.dll.1.dr | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/Fx | CasPol.exe, 00000003.00000003.1131841880<br>8.0000000001652000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.11329658756.0000000001652000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11326002<br>160.0000000001652000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.11322295871.000000000165200<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10447130085.0000<br>000001652000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.11219049182.0000000001652000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11255028714.000000000165<br>2000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10726142476.0<br>000000001652000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11767865151.0000000001652000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.11240464156<br>.0000000001652000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.11613837370.0000000001652000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.105866628<br>72.0000000001652000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.11341231194.0000000001652000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10722621602.00000<br>00001652000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.11356392120.0000000001652000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10733897731.0000000001652<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11153845329.00<br>00000001652000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.11367241986.0000000001652000.0000<br>0004.00000020.00020000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/_1 | CasPol.exe, 00000003.00000003.1087475289 3.0000000001610000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.11430915788.0000000001610000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11370430 339.0000000001610000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10852845632.000000000161000 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11936516446.0000 000001610000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.10986315495.0000000001610000.000000 04.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11522651189.000000000161 0000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10819644928.0 000000001610000.00000004.00000020.000200 00.00000000.sdmp, CasPol.exe, 00000003.0 0000003.11880488126.0000000001610000.000 00004.00000020.00020000.00000000.sdmp, C asPol.exe, 00000003.00000003.11240029390 .0000000001610000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 00000003 .00000003.11409010342.0000000001610000.0 0000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.112187021 23.0000000001610000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 03.00000003.11664820128.0000000001610000 .00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11025068972.00000 00001610000.00000004.00000020.00020000.0 0000000.sdmp, CasPol.exe, 00000003.00000 003.10729536768.0000000001610000.0000000 4.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11452754183.0000000001610 000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.11032375205.00 000000001610000.00000004.00000020.0002000 0.00000000.sdmp, CasPol.exe, 00000003.00 000003.11796544361.0000000001610000.0000 0004.00000020.00020000.00000000.sdmp, Ca sPol.exe, 00000003.00000003.11624374128. 0000000001610000.00000004.00000020.00020 000.00000000.sdmp, CasPol.exe, 00000003. 00000003.11113467457.0000000001610000.00 000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.1077782665 9.0000000001610000.00000004.00000020.000 20000.00000000.sdmp | false | | high |
| http://www.certum.pl/CPS0 | pago.exe | false | | high |
| http://https://drive.google.com/;N | CasPol.exe, 00000003.00000003.1047385164 6.0000000001644000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 3.00000003.10462243555.0000000001644000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10470093 101.0000000001644000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 003.00000003.10454670711.000000000164400 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000003.00000003.10466142710.0000 000001644000.00000004.00000020.00020000. 00000000.sdmp, CasPol.exe, 00000003.0000 0003.10458487274.0000000001644000.000000 04.00000020.00020000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/d | CasPol.exe, 00000003.00000003.1193651644<br>6.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.11880488126.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11796544<br>361.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.11909906632.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11752718459.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.11858479014.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11902460650.000000000161<br>0000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11763848646.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11914595364.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.11836730304<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.11854750366.0000000001610000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.118440210<br>10.0000000001610000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.11825610002.0000000001610000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11785504010.00000<br>00001610000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.11778308394.0000000001610000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11884212900.0000000001610<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11876915856.00<br>00000001610000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.11865819520.0000000001610000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.11943762088.<br>0000000001610000.00000004.00000020.00020<br>000.00000000.sdmp, CasPol.exe, 00000003.<br>00000003.11918231677.0000000001610000.00<br>000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.1193290200<br>8.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://csp.wit?_ | CasPol.exe, 00000003.00000003.1143091578<br>8.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.11409010342.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11333346<br>775.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.11412600461.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11321825420.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.11318016128.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11405436979.000000000161<br>0000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11449080284.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.11427357394.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.11329226727<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.11672143077.0000000001610000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.114235366<br>00.0000000001610000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.11171577849.0000000001610000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11401691671.00000<br>00001610000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.11441676251.0000000001610000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.11307080583.0000000001610<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.11314366430.00<br>00000001610000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.11310795151.0000000001610000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.11419850890.<br>0000000001610000.00000004.00000020.00020<br>000.00000000.sdmp, CasPol.exe, 00000003.<br>00000003.11416125224.0000000001610000.00<br>000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.1139646561<br>2.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://drive.google.com/a | CasPol.exe, 00000003.00000003.1047734763<br>7.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp, CasPol.exe, 0000000<br>3.00000003.10458150869.0000000001610000.<br>00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10481182<br>540.0000000001610000.00000004.00000020.0<br>0020000.00000000.sdmp, CasPol.exe, 00000<br>003.00000003.10442906491.000000000161000<br>0.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10489062079.0000<br>000001610000.00000004.00000020.00020000.<br>00000000.sdmp, CasPol.exe, 00000003.0000<br>0003.10473539920.0000000001610000.000000<br>04.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10435303653.000000000161<br>0000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10439116142.0<br>000000001610000.00000004.00000020.000200<br>00.00000000.sdmp, CasPol.exe, 00000003.0<br>0000003.10589857417.0000000001610000.000<br>00004.00000020.00020000.00000000.sdmp, C<br>asPol.exe, 00000003.00000003.10469767911<br>.0000000001610000.00000004.00000020.0002<br>0000.00000000.sdmp, CasPol.exe, 00000003<br>.00000003.10586224494.0000000001610000.0<br>0000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.104850582<br>31.0000000001610000.00000004.00000020.00<br>020000.00000000.sdmp, CasPol.exe, 000000<br>03.00000003.10725676845.0000000001610000<br>.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10496974061.00000<br>00001610000.00000004.00000020.00020000.0<br>0000000.sdmp, CasPol.exe, 00000003.00000<br>003.10722204238.0000000001610000.0000000<br>4.00000020.00020000.00000000.sdmp, CasPol.exe,<br>00000003.00000003.10465841943.0000000001610<br>000.00000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.10500989666.00<br>00000001610000.00000004.00000020.0002000<br>0.00000000.sdmp, CasPol.exe, 00000003.00<br>000003.10431603703.0000000001610000.0000<br>0004.00000020.00020000.00000000.sdmp, Ca<br>sPol.exe, 00000003.00000003.10512175315.<br>0000000001610000.00000004.00000020.00020<br>000.00000000.sdmp, CasPol.exe, 00000003.<br>00000003.10461940744.0000000001610000.00<br>000004.00000020.00020000.00000000.sdmp,<br>CasPol.exe, 00000003.00000003.1049300527<br>3.0000000001610000.00000004.00000020.000<br>20000.00000000.sdmp | false | | high |

## World Map of Contacted IPs


**Public IPs**

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 142.250.185.78 | drive.google.com | United States | | 15169 | GOOGLEUS | false |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 634139 |
| Start date and time: 25/05/202216:54:53 | 2022-05-25 16:54:53 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 13m 40s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | pago.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301 |
| Run name: | Suspected Instruction Hammering |
| Number of analysed new started processes analysed: | 6 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal80.troj.evad.winEXE@4/7@1/1 |
| EGA Information: | • Successful, ratio: 100% |

| | |
|---|---|
| HDC Information: | • Successful, ratio: 21.9% (good quality ratio 21.5%)<br>• Quality average: 88.2%<br>• Quality standard deviation: 21.4% |
| HCA Information: | • Successful, ratio: 96%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .exe<br>• Adjust boot time<br>• Enable AMSI |

### Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.93.58.141, 20.54.122.82
- Excluded domains from analysis (whitelisted): wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, wd-prod-cp-eu-north-1-fe.northeurope.cloudapp.azure.com, wdcpalt.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, wd-prod-cp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx 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 |
|---|---|---|
| 16:57:16 | API Interceptor | 1394x 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\Temp\Adventure_15.bmp**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\pago.exe |
| File Type: | JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3 |
| Category: | dropped |

| | |
|---|---|
| Size (bytes): | 10390 |
| Entropy (8bit): | 7.903542919804659 |
| Encrypted: | false |
| SSDEEP: | 192:oXRNg0EZjs8IqPEZuNslVO+4maXz0/UXNmoSClcbUHDbq7QHofXMK5/AXBEC:KRN4sZAvBOFmGzGUIoSCabqHGXMU/aBZ |
| MD5: | A82E06031DCD06EB3C8A5FAD0F365431 |
| SHA1: | C1EDFB9FA004A8959ABAD35AC80D85BBCE6D491A |
| SHA-256: | 7B1FFF6C0A7F458D8DE95D0820E39C5501DC1E045B4DB29B9649A399DA77DC47 |
| SHA-512: | C7D524633E84D8A58912E3BBAFF9A08DF9F0B54760CC5375BD30C11737D395BCD94BE9F3884D92B260BAF8A30956E025CBDC348C364BA6300B70D2EF73CDE8<br>3C |
| Malicious: | false |
| Reputation: | low |
| Preview: | ......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n..".....<br>.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....?.....#~.....o..f...Y...N.....Yi~..~-.....V..y0.s....-.e..eR.O.....J...O.)..y...uo;...T~D1JWs).....c.A\| dZ..a'...z..qR.._y..E~R.....\.}...8...T~1i....w..H.{.!X.....3..P.' s...<br>.?m.._j.M...k..5.....?.~..Kxf..t.K...#.a..+.....p.e./..z..%5..W..O..wR.?.....?.F.}2.T.g...xgF.....,..O"D...hf |

**C:\Users\user\AppData\Local\Temp\BRUGERMSSIGE.dis**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\pago.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 97167 |
| Entropy (8bit): | 6.6932651335642435 |
| Encrypted: | false |
| SSDEEP: | 1536:EfXAWCQ6T7mcMoluztlNfcC4VRZIoMbHSEfn+BAy+:Ev+Q6Wc+lNf8ioMbN+BP+ |
| MD5: | 6F25FEEFB6A9A623BA078478EE1AEEC2 |
| SHA1: | 4D3FD6287027B2DE74867136478569CCBF86631A |
| SHA-256: | C21E1406829942B630592ED3844D4F102A3C7DEF56B605B8DA16714A7373C235 |
| SHA-512: | 051A50DE535F20FC9928CAD362BBE896F1D04603E6372AADCC37707287B369BE5F36538CBCD879C666134112FC1A5D4A573B2FEE6BE0B8721596074B818ED56 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....$...----------.....`...f.....2.\|mY.....f.....Z.....f.....f.r...5..UX.....r.i.....b..2]..V..<br>.....f.....f.....+;..&==========.....f.s....f.....f.....\k*ddddddddddddddddddddddddddd..f..j.....2R.DY.....<br>.....f.....~.f.....f.a.....1,).i----------f=o"f.u...../.....0..8.GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGf..9.....0e.#_.....,.....f.b.....7j..ooooooooooooooooooooooooooooooooooooooooooooooooo.....o.f.e.....'<br>....ccccccccccccccccccccccccccccccccc.....f.r.....f.n..,.\.a.....f.....f.`.f...f.....f. |

**C:\Users\user\AppData\Local\Temp\Lovprisendes8.omb**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\pago.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 48940 |
| Entropy (8bit): | 3.999620856152349 |
| Encrypted: | false |
| SSDEEP: | 768:Q6Ng3Z7BTx5kWGy0GXHhdq7R04CFNNGFdGf2c4nUqABwgtX0Y9ct4ekzzQ:dN4PrCaYRkrGF62c4UZBwe07t4hzU |
| MD5: | A41261EC6495500632E1437958CBD9EF |
| SHA1: | 1F1AC7AAEA6BFA125C61D49AF3DB5BAA7282D0E4 |
| SHA-256: | 3C7C286698CCBE7918CAC68318462094EA40F6A8501CF5E947CFF2AB08612CF4 |
| SHA-512: | 18D3CB0A741607DEE4F09374842C2EA2E5093D3E8DFF7B8ED6A6022ED4622142B97C8C92A48A907F67FD3AE33E50A8B4337E55B3A18BB448CD6A08A94796EE<br>3 |
| Malicious: | false |
| Preview: | 4A6D9A95C3AD8B8313D5017E5C7345F700E9ADFB7A0B74D8C58A24912FF5430FFA44EE0BBFFFE3187852D0D519CA9222A58A5FF8C8344F893B8242AA<br>0D47F87ABE4B5A0D8432057C6C5A8AFDAF35E9C046A93DF774213E88282EC07A5A277F07C2AAB535B8395D8A04AD3AFAE72A30E5FFAD22A076630B63<br>044E10C00CBB00D04546DCA6EAFCF96134C3701296FB556AE59919932D019C2E7BC07B81A2FD3DB232BBFF90A5D09102C73A40C9F6C41F9EB5A7C51C<br>E1981D65896581B79A4C4ABB5DA400A6E990F3B0994BB9176DB70A4FE1C20F57C13073461FBD2D29B2D7C54496BD5F8F0500512300E99A9A8803F1D8<br>26E351306A5D182BA2AE764E7FAA4946A4405278969EE637F0D8E8D8F6558AA680C4A6B5FEBAB8A290ECC9E4326B3FA336893FFF7799D71AC90D1AC7<br>BFF244CBC0F9E1B5BECA89F17C475A119EDF7804C53BB284FA391F934D93B1634C0D08B93E2A02229BF43EE204632CECD42385CDB38194671D2B42DE<br>31B8E4558579042EA0A86C2E33520373DE6EA1A52C4080E0BFF3DBC347BE055739739B43AA4B727F004E5D8EA4071945D23FE0734503E17F9891C78D<br>934DFA3C7B96BB3C7CBA197688C5DC1C3886679AD7C945D7987665A51F5AEDB4E3B9C8615DF12C8E9B4968870EC72403D9AE866BD8B23C9D197FE851<br>6C30C7CD3697D5AC4099DFCFA9E0A6BA2617D581 |

**C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\pago.exe |
| File Type: | PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 19056 |
| Entropy (8bit): | 6.442411564417779 |
| Encrypted: | false |
| SSDEEP: | 384:8WhLWql40uIrRDTveaVEc2gK/uPHRN7xpJ/AlGseCvy:rfl40uqDTveaVCMxv/xj4y |
| MD5: | E3F74999CDB00FCAAA6A40A97B8F199B |
| SHA1: | F3A2C8DF8E98F7DCB49CBE5C4A717A6087A656D2 |
| SHA-256: | 6929BC473DF404FCED714F345479216B66B72ACF116061DF1CDD8ACAEE961333 |
| SHA-512: | 3BE3EEAB3304EFEB9594FA516B61528587CFA8453AB7B4AF991137E3A1D7E23270DA600FC341EEF703932CCFF53571ACF3CD00AEEAE47347CC36EE69B71DB37C |
| Malicious: | false |
| Antivirus: | • Antivirus: ReversingLabs, Detection: 0% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...(_+.....".... .....P..... ..`...@.....@..... .....&..p$...@.....T.....H.....text...X..... ..... ..`.data...D....0.....".....@....reloc.....@.....$.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...h.(...C.o.m.m.e.n.t.s...S.y.s.t.e.m...R.u.n.t.i.m.e...C.o.m.p.i.l.e.r.S.e.r.v.i.c.e.s...V.i.s.u.a.l.C...L.....C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...x.(...F.i.l.e.D. |

**C:\Users\user\AppData\Local\Temp\application-exit-symbolic.symbolic.png**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\pago.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 217 |
| Entropy (8bit): | 6.534586335380934 |
| Encrypted: | false |
| SSDEEP: | 6:6v/lhPysy9LkyYu1RTqYPVFb77PhjC0E6IO7lNX5p:6v/7SNkq1lRdh77Z46IO73X3 |
| MD5: | 92DBF28E22A2BFCDDA0BCC8FB01565D7 |
| SHA1: | 2FD88523B68E1F078F7A0728039017C4886F7154 |
| SHA-256: | 71D4F559AAECBD739CF9921FDA88072D125000E3E97BF2A534D3647D79505203 |
| SHA-512: | 00C886F5C2DDB4B979FF9BCE550D6B2AAC245087FB43EA94BED81587C356F664FF2A50BE42E0BABA0E1C3D62A45E73DD51DAD64CDCF262F616C81AA2365CBC34 |
| Malicious: | false |
| Preview: | .PNG.....IHDR.....a....sBIT....|.d.....IDAT8...A.. .E..W(..]..q.nu.r.\..R.L.?....|f&.....p!.....9gp....n...h.....=)t..`.O.FM7...x#/.....-].a.?._....y.. 6X..J..... h.AW....I.P. ..Y.....IEND.B`. |

**C:\Users\user\AppData\Local\Temp\nsrF138.tmp\System.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\pago.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 12288 |
| Entropy (8bit): | 5.814115788739565 |
| Encrypted: | false |
| SSDEEP: | 192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr |
| MD5: | CFF85C549D536F651D4FB8387F1976F2 |
| SHA1: | D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E |
| SHA-256: | 8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8 |
| SHA-512: | 531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88 |
| Malicious: | false |
| Antivirus: | • Antivirus: Metadefender, Detection: 3%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X.....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... |

**C:\Users\user\AppData\Local\Temp\process-stop-symbolic.svg**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\pago.exe |
| File Type: | SVG Scalable Vector Graphics image |
| Category: | dropped |
| Size (bytes): | 774 |
| Entropy (8bit): | 4.396237619919732 |

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 24:2dPnnxu3nC7ZFftJhrV5VCpCCm2csZXyn1ekBhnrwdlj:cfnGC777LGx3U15rwb |
| MD5: | 068B4AD014326E7A847F2F7BBCC1CE3A |
| SHA1: | 7AAA833DBDA8BFBB882FA6545A9488E3A1D50943 |
| SHA-256: | D44417A453C6EB038275C3A44A9523E0B2D6EF6297B89E1DE20FF87BA59A351C |
| SHA-512: | EDBDD70019CCB3E0CCB9599EC3479FF8166F9E121739D86BE06E10F52BA3DBC7FF4F81FA52558E725FD25D058A89B191FEE86B7FE61690D1CC1CBD246E329E BF |
| 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">. <path d="m 2.003906 2 h 1 h 0 .03125 c 0.253906 0.011719 0.507813 0.128906 0.6875 0.3125 l 4.28125 4.28125 l 4.3125 -4.28125 c 0.265625 -0.230469 0.445313 -0.304688 0.6875 -0.3125 h 1 v 1 c 0 0.285156 -0.035156 0.550781 -0.25 0.75 l -4.28125 4.28125 l 4.25 4.25 c 0.1875 0.1875 0.28125 0.453125 0.28125 0.71875 v 1 h -1 c -0.265625 0 -0.53125 -0.09375 -0.71875 -0.28125 l -4.28125 -4.28125 l -4.28125 4.28125 c -0.1875 0.1875 -0.453125 0.28125 -0.71875 0.28125 h -1 v -1 c 0 -0.265625 0.09375 -0.53125 0.28125 -0.71875 l 4.28125 -4.25 l -4.28125 -4.28125 c -0.210937 -0.195312 -0.304687 -0.46875 -0.28125 -0.75 z m 0 0" fill="#2e3436"/>.</svg>. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive |
| Entropy (8bit): | 7.043083620309494 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | pago.exe |
| File size: | 271408 |
| MD5: | 41db491c763c2aa61a8f4305591e3139 |
| SHA1: | 20c45ae71feccf738620764f70154f0ac5b6ac59 |
| SHA256: | 904211f6f92bb8e96d8a56077c3b95ed22c746ee17caf7fb769d786821521585 |
| SHA512: | 4626fa0b838883da5960e341fcb7e23f8cdf1df106bf73ac1ca340d8580a15384ff0beaefd0cbfc841b6b73807ce614ef788e515b3c3f456841874496ed5f781 |
| SSDEEP: | 6144:TbE/HUUZ2WM2HSOCDIqfmFE/xgCT3ZkANqLT:TbJ2y5DwS/xgkJkj |
| TLSH: | 9F44B041F3C0ECF6E46194B3E82ED3640A57EE59C0A68B1B22567A172CA33D31657EC7 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j..... |

## File Icon

| | |
|---|---|
| Icon Hash: | e4c2aeaebcb0f004 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40352d |
| Entrypoint Section: | .text |
| Digitally signed: | true |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x614F9B5A [Sat Sep 25 21:57:46 2021 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: | 56a78d55f3f7af51443e58e0ce2fb5f6 |

| Authenticode Signature | |
|---|---|
| Signature Valid: | **false** |
| Signature Issuer: | CN="Brugerinitialerne1 Naaet5 SHELFS ", O=Thorleks, L=Washington, S=District of Columbia, C=US |
| Signature Validation Error: | **A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider** |
| Error Number: | -2146762487 |
| Not Before, Not After | • 24/05/2022 02:23:57 24/05/2023 02:23:57 |
| Subject Chain | • CN="Brugerinitialerne1 Naaet5 SHELFS ", O=Thorleks, L=Washington, S=District of Columbia, C=US |
| Version: | 3 |
| Thumbprint MD5: | A18E59CB3B586070B1D452E15DBA379F |
| Thumbprint SHA-1: | 9676FFAA1E0AE9B83CDEB62AF1657A1C07483B3E |
| Thumbprint SHA-256: | FA06C8621275BD31C7EA9C2886C8C7FA106B7635FE9F3ADC5EC24510DC441350 |
| Serial: | 843A121514829DD0 |

| Entrypoint Preview |
|---|
| **Instruction** |
| push ebp |
| mov ebp, esp |
| sub esp, 000003F4h |
| push ebx |
| push esi |
| push edi |
| push 00000020h |
| pop edi |
| xor ebx, ebx |
| push 00008001h |
| mov dword ptr [ebp-14h], ebx |
| mov dword ptr [ebp-04h], 0040A2E0h |
| mov dword ptr [ebp-10h], ebx |
| call dword ptr [004080CCh] |
| mov esi, dword ptr [004080D0h] |
| lea eax, dword ptr [ebp-00000140h] |
| push eax |
| mov dword ptr [ebp-0000012Ch], ebx |
| mov dword ptr [ebp-2Ch], ebx |
| mov dword ptr [ebp-28h], ebx |
| mov dword ptr [ebp-00000140h], 0000011Ch |
| call esi |
| test eax, eax |
| jne 00007F1EA8BA903Ah |
| lea eax, dword ptr [ebp-00000140h] |
| mov dword ptr [ebp-00000140h], 00000114h |
| push eax |
| call esi |
| mov ax, word ptr [ebp-0000012Ch] |
| mov ecx, dword ptr [ebp-00000112h] |
| sub ax, 00000053h |
| add ecx, FFFFFFD0h |
| neg ax |
| sbb eax, eax |
| mov byte ptr [ebp-26h], 00000004h |
| not eax |
| and eax, ecx |
| mov word ptr [ebp-2Ch], ax |
| cmp dword ptr [ebp-0000013Ch], 0Ah |
| jnc 00007F1EA8BA900Ah |
| and word ptr [ebp-00000132h], 0000h |
| mov eax, dword ptr [ebp-00000134h] |
| movzx ecx, byte ptr [ebp-00000138h] |
| mov dword ptr [00434FB8h], eax |

| Instruction |
|---|
| xor eax, eax |
| mov ah, byte ptr [ebp-0000013Ch] |
| movzx eax, ax |
| or eax, ecx |
| xor ecx, ecx |
| mov ch, byte ptr [ebp-2Ch] |
| movzx ecx, cx |
| shl eax, 10h |
| or eax, ecx |

### 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 | 0x8610 | 0xa0 | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x6c000 | 0x19100 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x40570 | 0x1ec0 | .ndata |
| 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 | 0x2b0 | .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 | 0x6897 | 0x6a00 | False | 0.666126179245 | data | 6.45839821493 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x8000 | 0x14a6 | 0x1600 | False | 0.439275568182 | data | 5.02410928126 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xa000 | 0x2b018 | 0x600 | False | 0.521484375 | data | 4.15458210409 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .ndata | 0x36000 | 0x36000 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rsrc | 0x6c000 | 0x19100 | 0x19200 | False | 0.288858442164 | data | 4.88265504154 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x6c2c8 | 0x10828 | dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 16777216, next used block 16777216 | English | United States |
| RT_ICON | 0x7caf0 | 0x4228 | dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0 | English | United States |
| RT_ICON | 0x80d18 | 0x25a8 | data | English | United States |
| RT_ICON | 0x832c0 | 0x10a8 | data | English | United States |
| RT_ICON | 0x84368 | 0x468 | GLS_BINARY_LSB_FIRST | English | United States |
| RT_DIALOG | 0x847d0 | 0x100 | data | English | United States |
| RT_DIALOG | 0x848d0 | 0x11c | data | English | United States |

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_DIALOG | 0x849f0 | 0xc4 | data | English | United States |
| RT_DIALOG | 0x84ab8 | 0x60 | data | English | United States |
| RT_GROUP_ICON | 0x84b18 | 0x4c | data | English | United States |
| RT_VERSION | 0x84b68 | 0x254 | data | English | United States |
| RT_MANIFEST | 0x84dc0 | 0x33e | XML 1.0 document, ASCII text, with very long lines, with no line terminators | English | United States |

### Imports

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

### Version Infos

| Description | Data |
|---|---|
| LegalCopyright | moletsgavn |
| FileVersion | 7.22.20 |
| CompanyName | wimpinessgri |
| LegalTrademarks | Gear255 |
| Comments | Draabet |
| ProductName | Afspnd |
| FileDescription | UKONVENTIO |
| Translation | 0x0409 0x04b0 |

### Possible Origin

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

# Network Behavior

### TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 25, 2022 16:57:17.362483978 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 25, 2022 16:57:17.362586975 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.362759113 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.383088112 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.383141994 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.432952881 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.433126926 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.433232069 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.436079979 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.436358929 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.567878008 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.567965984 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.568682909 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.568819046 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.572362900 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.614641905 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.766274929 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.766446114 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.766532898 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.766654968 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.766777992 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.766958952 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.767080069 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.767229080 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.767302036 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.767417908 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.767453909 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.767544031 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.767596960 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.767674923 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.772680044 CEST | 49746 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.772742987 CEST | 443 | 49746 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.940288067 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.940325022 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.940489054 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.940845013 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.940850973 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.968775988 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:17.968905926 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.969152927 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.969376087 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:17.969403028 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.149180889 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.149339914 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.149389029 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.149545908 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.149585009 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.149733067 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.149768114 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.149919987 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.149962902 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.150181055 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.150260925 CEST | 49747 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.150298119 CEST | 443 | 49747 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.314505100 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.314588070 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.314732075 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.315243006 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.315304041 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.350122929 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 25, 2022 16:57:18.350310087 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.350632906 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.350826979 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.351031065 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.519058943 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.519181013 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.519226074 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.519257069 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.519368887 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.519505978 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.519552946 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.519746065 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.520512104 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.520656109 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.520700932 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.520759106 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.520780087 CEST | 443 | 49748 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.520817995 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.520922899 CEST | 49748 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.705384970 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.705459118 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.705650091 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.706238031 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.706284046 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.738774061 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.738893986 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.739399910 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.739589930 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.739844084 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.901290894 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.901453018 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.901514053 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.901667118 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.901696920 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.901901007 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.901957035 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.902156115 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.902239084 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |
| May 25, 2022 16:57:18.902359009 CEST | 49749 | 443 | 192.168.11.20 | 142.250.185.78 |
| May 25, 2022 16:57:18.902388096 CEST | 443 | 49749 | 142.250.185.78 | 192.168.11.20 |

### DNS Queries

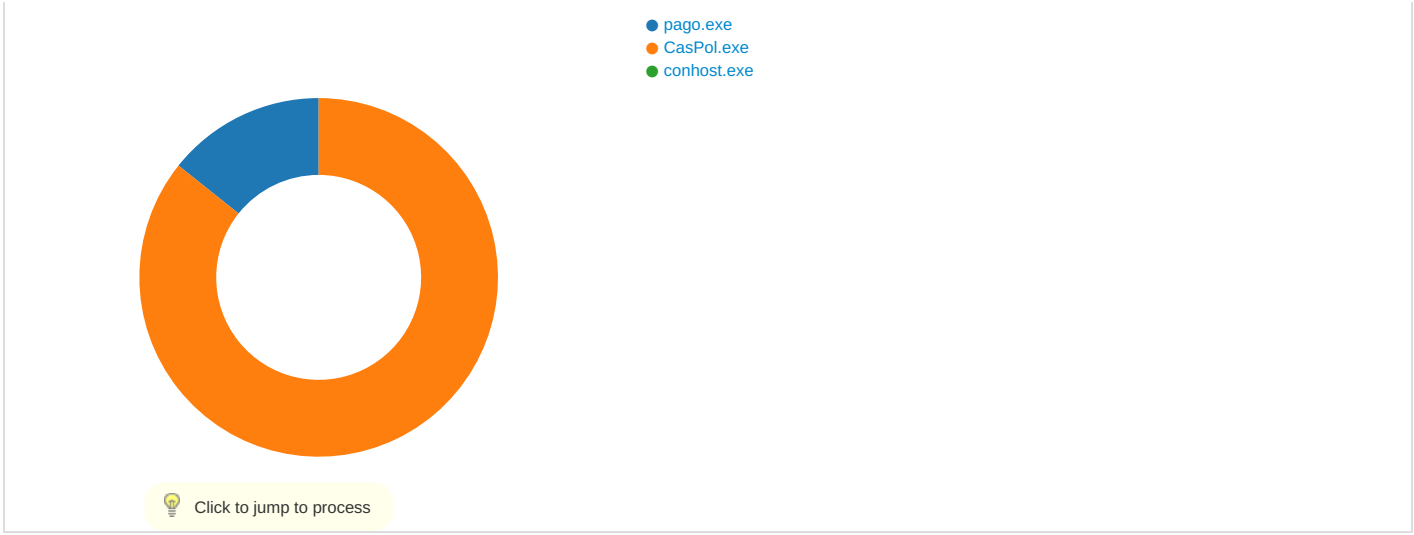
| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| May 25, 2022 16:57:17.345375061 CEST | 192.168.11.20 | 1.1.1.1 | 0x86ca | Standard query (0) | drive.google.com | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| May 25, 2022 16:57:17.354451895 CEST | 1.1.1.1 | 192.168.11.20 | 0x86ca | No error (0) | drive.google.com | | 142.250.185.78 | A (IP address) | IN (0x0001) |

## Statistics

### Behavior




# System Behavior

## Analysis Process: pago.exe PID: **3984**, Parent PID: **1796**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 16:56:44 |
| Start date: | 25/05/2022 |
| Path: | C:\Users\user\Desktop\pago.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\pago.exe" |
| Imagebase: | 0x400000 |
| File size: | 271408 bytes |
| MD5 hash: | 41DB491C763C2AA61A8F4305591E3139 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.10964117045.0000000002BA0000.00000040.00001000.00020000.00000000.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: **6636**, Parent PID: **3984**

### General

| | |
|---|---|
| Target ID: | 3 |
| Start time: | 16:57:04 |
| Start date: | 25/05/2022 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\pago.exe" |
| Imagebase: | 0xce0000 |
| File size: | 108664 bytes |

| | |
|---|---|
| MD5 hash: | 914F728C04D3EDDD5FBA59420E74E56B |
| 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: 00000003.00000000.10305977883.0000000001100000.00000040.00000400.00020000.00000000.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 | 1114ECE | 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 | 1114ECE | 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 | 1114ECE | 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 | 1114ECE | 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 | 1114ECE | 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 | 1114ECE | InternetOpenUrlA |

## Analysis Process: conhost.exe PID: **3936**, Parent PID: **6636**

### General

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 16:57:04 |
| Start date: | 25/05/2022 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7c3b60000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

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

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Disassembly

No disassembly