


**ID:** 828570
**Sample Name:** Royalistic.exe
**Cookbook:** default.jbs
**Time:** 10:47:39
**Date:** 17/03/2023
**Version:** 37.0.0 Beryl

# Table of Contents

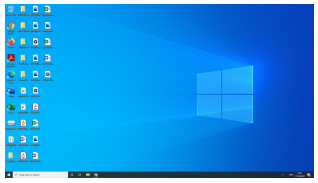
# Windows Analysis Report

## Royalistic.exe

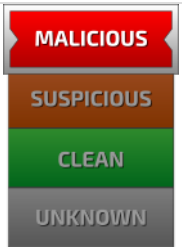
## Overview

### General Information

| | |
|---|---|
| Sample Name: | Royalistic.exe |
| Analysis ID: | 828570 |
| MD5: | d14335f61c99a… |
| SHA1: | f82f3481619be… |
| SHA256: | 08cabec4d012… |
| Infos: | |



### Detection



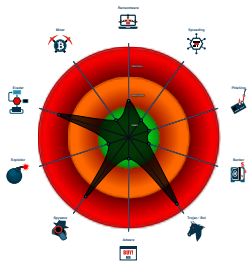

**AgentTesla, GuLoader**

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

### Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- May check the online IP address of…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

### Classification



## Process Tree

- **System is w10x64native**
- Royalistic.exe (PID: 5084 cmdline: C:\Users\user\Desktop\Royalistic.exe MD5: D14335F61C99A9B8A2D5E87CDF83CDD0)
  - CasPol.exe (PID: 2280 cmdline: C:\Users\user\Desktop\Royalistic.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 7428 cmdline: C:\Users\user\Desktop\Royalistic.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

## Malware Threat Intel

Provided by malpedia

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|
| **Agent Tesla, AgentTesla** | A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2. | • SWEED | http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/ | http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla |

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|

| Name | Description | Attribution | Blogpost URLs | Link |
|---|---|---|---|---|
| **CloudEyE, GuLoader** | CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored. | No Attribution | **http://** https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/ | **http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye |

## Malware Configuration

**No configs have been found**

## Yara Signatures

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000005.00000002.29396081799.00000000363AB000.00000004.00000800.00020000.00000000.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 00000005.00000002.29396081799.00000000363AB000.00000004.00000800.00020000.00000000.sdmp | JoeSecurity_CredentialStealer | Yara detected Credential Stealer | Joe Security | |
| 00000001.00000002.24657057833.00000000007BA000.00000004.00000020.00020000.00000000.sdmp | JoeSecurity_GuLoader_3 | Yara detected GuLoader | Joe Security | |
| 00000001.00000002.24658662982.00000000052B6000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |
| Process Memory Space: Royalistic.exe PID: 5084 | JoeSecurity_GuLoader_3 | Yara detected GuLoader | Joe Security | |

Click to see the 1 entries

## Sigma Signatures

**No Sigma rule has matched**

## Snort Signatures

**No Snort rule has matched**

## Joe Sandbox Signatures

### AV Detection

Multi AV Scanner detection for submitted file

### Networking

May check the online IP address of the machine

### Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

### Data Obfuscation

Yara detected GuLoader

### Malware Analysis System Evasion

Tries to detect Any.run

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

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

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

### HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

### Stealing of Sensitive Information

Yara detected AgentTesla

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

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

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

### Remote Access Functionality

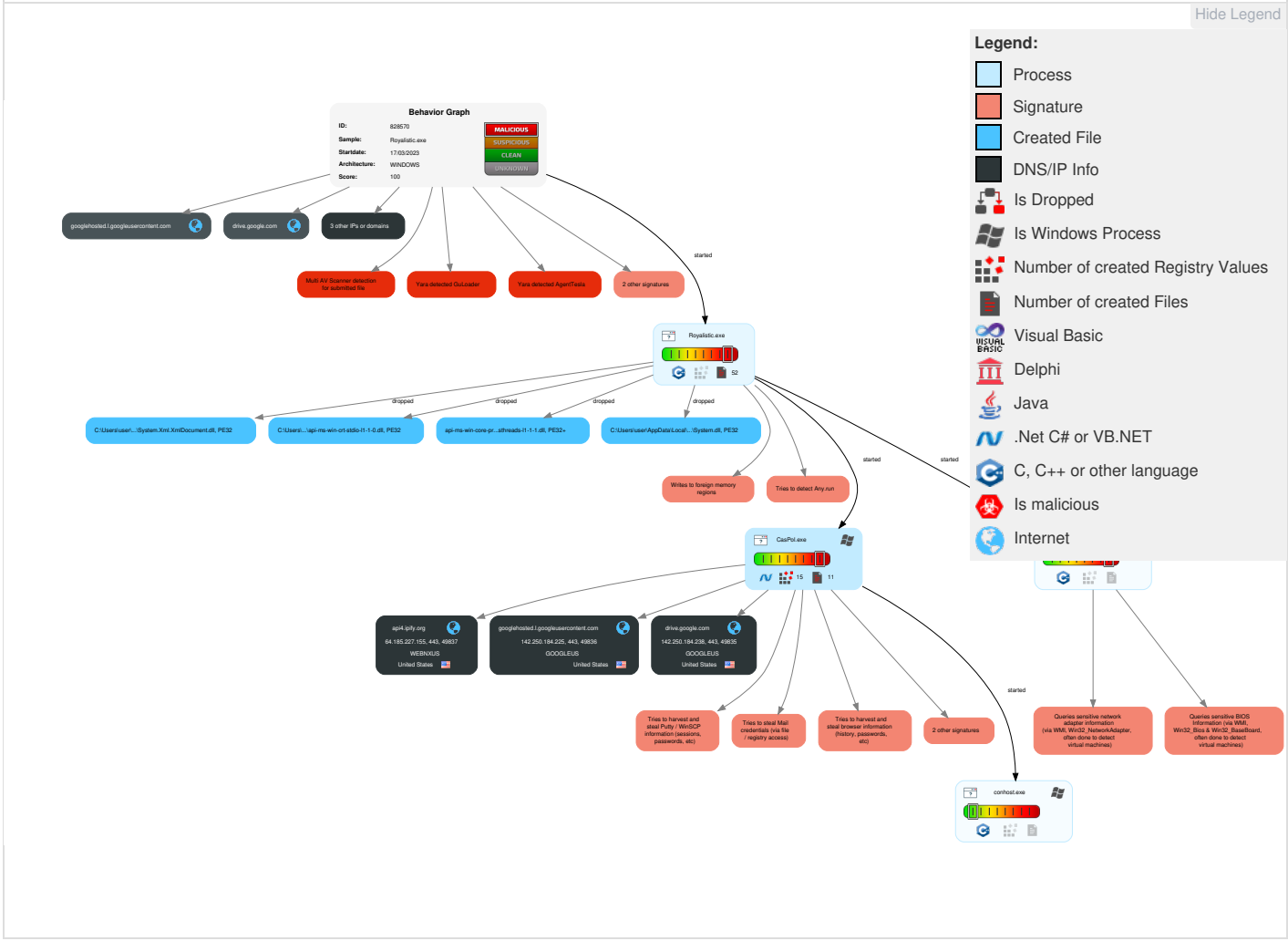
Yara detected AgentTesla

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | 2 1 1 Windows Management Instrumentation | 1 DLL Side-Loading | 1 DLL Side-Loading | 1 Disable or Modify Tools | 1 OS Credential Dumping | 3 File and Directory Discovery | Remote Services | 1 Archive Collected Data | Exfiltration Over Other Network Medium | 1 Ingress Tool Transfer | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | 1 System Shutdown/ Reboot |
| Default Accounts | 1 Native API | Boot or Logon Initialization Scripts | 1 Access Token Manipulation | 1 Obfuscated Files or Information | 1 1 Input Capture | 1 1 6 System Information Discovery | Remote Desktop Protocol | 1 Data from Local System | Exfiltration Over Bluetooth | 2 1 Encrypted Channel | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | 1 1 1 Process Injection | 1 Timestomp | 1 Credentials in Registry | 3 1 1 Security Software Discovery | SMB/Windows Admin Shares | 1 Email Collection | Automated Exfiltration | 2 Non-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 DLL Side-Loading | NTDS | 2 3 1 Virtualization/Sandbox Evasion | Distributed Component Object Model | 1 1 Input Capture | Scheduled Transfer | 1 3 Application Layer Protocol | 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 Masquerading | LSA Secrets | 1 Application Window Discovery | SSH | 2 Clipboard Data | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 2 3 1 Virtualization/Sandbox Evasion | Cached Domain Credentials | 1 System Network Configuration Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | 1 Access Token Manipulation | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points | | Data Encrypted for Impact |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | 1 1 1 Process Injection | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade to Insecure Protocols | | Generate Fraudulent Advertising Revenue |

## Behavior Graph




## Screenshots

### Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| Royalistic.exe | 51% | Virustotal | | Browse |
| Royalistic.exe | 26% | ReversingLabs | Win32.Trojan.Generic | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\nslE084.tmp\System.dll | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\nslE084.tmp\System.dll | 0% | Virustotal | | Browse |
| C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll | 0% | Virustotal | | Browse |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll | 0% | Virustotal | | Browse |
| C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Warehouse\Faithworthy\System.Xml.XmlDocument.dll | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Warehouse\Faithworthy\System.Xml.XmlDocument.dll | 0% | Virustotal | | Browse |

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 1.2.Royalistic.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1223491 | | Download File |
| 1.0.Royalistic.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1223491 | | Download File |

### Domains

No Antivirus matches

### URLs

No Antivirus matches

## Domains and IPs

### Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| api4.ipify.org | 64.185.227.155 | true | false | | high |
| drive.google.com | 142.250.184.238 | true | false | | high |
| googlehosted.l.googleusercontent.com | 142.250.184.225 | true | false | | high |
| doc-08-50-docs.googleusercontent.com | unknown | unknown | false | | high |
| api.ipify.org | unknown | unknown | false | | high |

### Contacted URLs

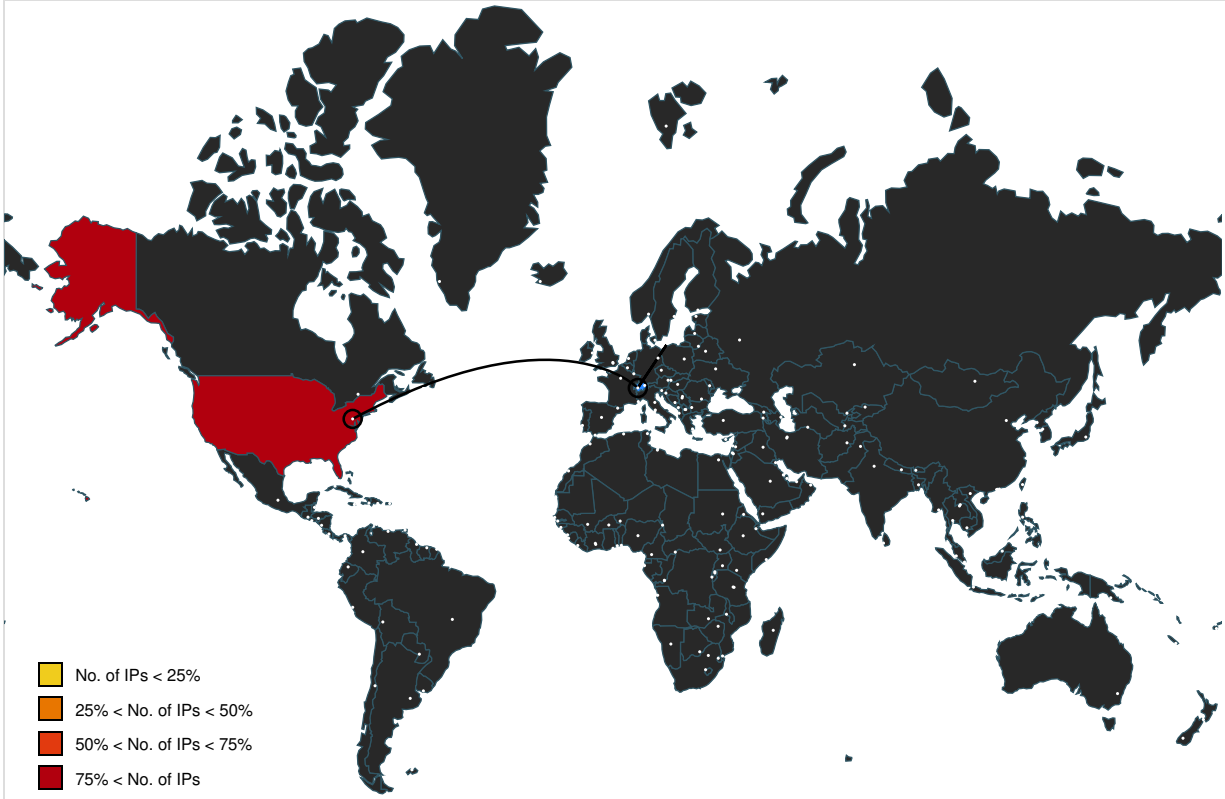
| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://api.ipify.org/ | false | | high |
| http://https://doc-08-50-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/n5qeluefaghr8f6hcddgpiu2u5tcuo8v/1679046600000/04783729953593762461/*/1UVMbNINla56ELELB-JwuaeCfH_gJxWsR?e=download&uuid=a3c458a3-e946-4640-bad5-e344d2665c90 | false | | high |

### URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://api.ipify.org | CasPol.exe, 00000005.00000002.2939608179 9.0000000036361000.00000004.00000800.000 20000.00000000.sdmp | false | | high |
| http://nsis.sf.net/NSIS_Error | Royalistic.exe, Royalistic.exe, 00000001.00000002. 24656159751.000000000040A000.00000004.00 000001.01000000.00000003.sdmp, Royalistic.exe, 00000001.00000000.24145483899.000000000040A 000.00000008.00000001.01000000.00000003.sdmp | false | | high |
| http://nsis.sf.net/NSIS_ErrorError | Royalistic.exe, 00000001.00000002.246561 59751.000000000040A000.00000004.00000001 .01000000.00000003.sdmp, Royalistic.exe, 00000001. 00000000.24145483899.000000000040A000.00 000008.00000001.01000000.00000003.sdmp | false | | high |
| http://https://doc-08-50-docs.googleusercontent.com/ | CasPol.exe, 00000005.00000003.2463350557 1.0000000005A24000.00000004.00000020.000 20000.00000000.sdmp | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | CasPol.exe, 00000005.00000002.2939608179 9.0000000036361000.00000004.00000800.000 20000.00000000.sdmp | false | | high |
| http://https://drive.google.com/ | CasPol.exe, 00000005.00000002.2937689973 5.0000000005992000.00000004.00000020.000 20000.00000000.sdmp | false | | high |
| http://https://doc-08-50-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/n5qeluef | CasPol.exe, 00000005.00000003.2462937744 1.0000000005A3B000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 5.00000002.29376899735.00000000059DA000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.29376899 735.00000000059FB000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 005.00000003.24628796513.00000000059FC00 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.24633505571.0000 0000059F8000.00000004.00000020.00020000. 00000000.sdmp | false | | high |

## World Map of Contacted IPs




### Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 142.250.184.225 | googlehosted.l.googleusercontent.com | United States | | 15169 | GOOGLEUS | false |
| 142.250.184.238 | drive.google.com | United States | | 15169 | GOOGLEUS | false |
| 64.185.227.155 | api4.ipify.org | United States | | 18450 | WEBNXUS | false |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 37.0.0 Beryl |
| Analysis ID: | 828570 |
| Start date and time: | 2023-03-17 10:47:39 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 16m 12s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |

| | |
|---|---|
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301 |
| Number of analysed new started processes analysed: | 8 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Sample file name: | Royalistic.exe |
| Detection: | MAL |
| Classification: | mal100.troj.spyw.evad.winEXE@6/16@3/3 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 47.2% (good quality ratio 46.5%)<br>• Quality average: 86.8%<br>• Quality standard deviation: 21.2% |
| HCA Information: | • Successful, ratio: 93%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .exe<br>• Sleeps bigger than 100000000ms are automatically reduced to 1000ms |

### Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.com, wdcp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

## Simulations

### Behavior and APIs

**No simulations**

## Joe Sandbox View / Context

### IPs

**No context**

### Domains

**No context**

### ASNs

**No context**

### JA3 Fingerprints

No context

### Dropped Files

No context

## Created / dropped Files

#### C:\Users\user\AppData\Local\Temp\nslE084.tmp\System.dll

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 11776 |
| Entropy (8bit): | 6.024446974480565 |
| Encrypted: | false |
| SSDEEP: | 192:Vm9rQDenC9VrcK7REgSWOprANupQYLRszDDH/d9CWlXo7U6Wxf:QJQEaVAK7R9SfpjpQYLRszfH/d9CWB1j |
| MD5: | E23600029D1B09BDB1D422FB4E46F5A6 |
| SHA1: | 5D64A2F6A257A98A689A3DB9A087A0FD5F180096 |
| SHA-256: | 7342B73593B3AA1B15E3731BFB1AFD1961802A5C66343BAC9A2C737EE94F4E38 |
| SHA-512: | C971F513142633CE0E6EC6A04C754A286DA8016563DAB368C3FAC83AEF81FA3E9DF1003C4B63D00A46351A9D18EAA7AE7645CAEF172E5E1D6E29123AB864E7AC |
| Malicious: | false |
| Antivirus: | • Antivirus: ReversingLabs, Detection: 0%<br>• Antivirus: Virustotal, Detection: 0%, Browse |
| Reputation: | moderate, very likely benign file |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../@t.k!..k!..k!..9T..l!.. Y..l!..k!..x!...T..o!...T..j!...T..j!...T..j!..Richk!....PE..L.....c....."!....."....@.....p.....@.....@.....A..P.....`.....@..X.....text...+!....."..... ..`.rdata.....@.....&.....@..@.data...D....P.....*.....@....reloc.....`.....,.....@..B..... |

#### C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Afdelingskontorer.Ate

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 263441 |
| Entropy (8bit): | 7.470128360205037 |
| Encrypted: | false |
| SSDEEP: | 6144:gW2L2lxw6CfR2hGhddAkBtTCNwQn4Sp5U2JvkCmLO6ta4Rh40FdmxMDoOz:gMHw9SGh1D6ndCtLO6s4R2eOMTz |
| MD5: | ED053E4B81682B3CEF98A00C188F9191 |
| SHA1: | 7824184CA7B4588B9665CF5D6ECDF3E6A20820C7 |
| SHA-256: | 64A7608273D8284E67F338F8B77230B0EF14C342747CE6C3F8792F567BC99498 |
| SHA-512: | 51C4089DE4328B5C37B759CF98FCDE4838C67413CF0F0EE8EB1D9CD6BB129A41C686BEC3DD424B553725C84787671FAE3F9E037C436E8D7D5B8F28F7D42CBE7D |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....?...s.....0.....'.....bbb.....>>.....II..}}.....;;;.....kk.....iiii.....XXXXX....qqq....iiii..++.....YY...00.....s.....7...EEE.....M.....&.....\\\\...../.....O.....6.....fff.....f.....AA.....^^^.....TT....*.....$.....=.....MM.....g.....O.....].xx.....aa.....gg.....CC.p.....BB.rr.....E....www.....xx....D.....'.....G.b....dd.....,,,.....h.....6.*.....h.....RRR.0..."....3.....B.55....ee.BB.....?.....-.22.....A.....e.```....5.....yy.DD.....b.....dddd..HH.....-.....lll.....2.....=.....#.....NN.....PPP.....ee.....c.....^^.T..... |

#### C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Affaldsproblem\x-office-spreadsheet.png

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PNG image data, 16 x 16, 8-bit colormap, non-interlaced |
| Category: | dropped |
| Size (bytes): | 546 |
| Entropy (8bit): | 6.786347340342328 |
| Encrypted: | false |

| | |
|---|---|
| SSDEEP: | 12:6v/7X0ZKjCVdCyXM8OYSd/AuKoOjTOH6BMLHEMA:C0oCDMUaAutUTQ60HED |
| MD5: | D4AEA6CA7A8B03C62C36FF2AEBE20C6C |
| SHA1: | F0BB798B40E4CA170ECFBD72161EF7796B58B444 |
| SHA-256: | EC1222609F69FE70F55C1817535B0138A295EB7C71CCC443D7B3ACAA44537B5B |
| SHA-512: | 9912AC7388A0138E809D8E25F4EE90B5952D8B4063969A79BCEB2C5E8A312878897BEF56FF3BBB0185A815262C343984D9C3113B5B5C2D0069716891110A0DFD |
| Malicious: | false |
| Preview: | .PNG.....IHDR.....(-.S....sBIT.....O.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtAuthor.Jakub Steiner.../....tEXtDescription.mimetypes7..d...!tEXtSource.http://jimmac.musichall.czif.^....PLTE.....P..Z.....W....tRNS.....RSYs.....=^....IDAT.W..G..@...!c ....,....YKM....c..~:s...l...U..\O..f...,..5..+.@....E.....b.B..H^..V..*.8\.r?....".z.....IEND.B`. |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-core-processthreads-l1-1-1.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PE32+ executable (DLL) (console) x86-64, for MS Windows |
| Category: | dropped |
| Size (bytes): | 19208 |
| Entropy (8bit): | 7.005927948691754 |
| Encrypted: | false |
| SSDEEP: | 384:dtUDfIeFrW1hWC5OZkum0GftpBjVzm3Sx56lgCoha6LDF:dteFuJoVijz1HB |
| MD5: | D699333637DB92D319661286DF7CC39E |
| SHA1: | 0BFFB9ED366853E7019452644D26E8E8F236241B |
| SHA-256: | FE760614903E6D46A1BE508DCCB65CF6929D792A1DB2C365FC937F2A8A240504 |
| SHA-512: | 6FA9FF0E45F803FAF3EB9908E810A492F6F971CB96D58C06F408980AB40CBA138B52D853AA0E3C68474053690DFAFA1817F4B4C8FB728D613696B6C516FA0F51 |
| Malicious: | false |
| Antivirus: | • Antivirus: ReversingLabs, Detection: 0%<br>• Antivirus: Virustotal, Detection: 0%, Browse |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.....<br>..PE..d....." .....0.....4....`.....`..... .....=.....T.....<br>.....rdata.....@..@.rsrc..... .....@..@.....<br>.....<br>..... |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\api-ms-win-crt-stdio-l1-1-0.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PE32 executable (DLL) (console) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 24328 |
| Entropy (8bit): | 6.867867660778997 |
| Encrypted: | false |
| SSDEEP: | 384:/ZpFVhHW1hWxgYBm0GftpBjMm3SNlndaYhpn3p:boEVi6DBp |
| MD5: | D5166AB3034F0E1AA679BFA1907E5844 |
| SHA1: | 851DD640CB34177C43B5F47B218A686C09FA6B4C |
| SHA-256: | 7BCAB4CA00FB1F85FEA29DD3375F709317B984A6F3B9BA12B8CF1952F97BEEE5 |
| SHA-512: | 8F2D7442191DE22457C1B8402FAAD594AF2FE0C38280AAAFC876C797CA79F7F4B6860E557E37C3DBE084FE7262A85C358E3EEAF91E16855A91B7535CB0AC832E |
| Malicious: | false |
| Antivirus: | • Antivirus: ReversingLabs, Detection: 0%<br>• Antivirus: Virustotal, Detection: 0%, Browse |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L.<br>.....G.....!.....0.....@.....@.....a.....0.....".=.....T.....text...<br>a..... ..`.rsrc.....0.....@..@v.....G.....8...d...d.....G.....d.....G.....RSDS9uG.l..k..y.....api-ms-win-crt-stdio-l1-1-0.pdb.....d....rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....G....^.....(..... .....<...y.....)...h..... ...].....H...<br>.....)...D...^...v.....T...u.....9...Z...{.....0...Q... |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Forhastelse\Kommandjsr\drive-multidisk.png**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 569 |
| Entropy (8bit): | 7.482468865601557 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7QkFqDaHfvZFpa7O/oH5kGxVI7F2bk7jv0E1YpA0sVrgY:x8qeH7MQ+px2qqj5Y60mr7 |
| MD5: | B0C0FEE6A573A2776A013307457B6556 |
| SHA1: | 95157DA2FAD0902832E25CBEBE3EE4E58C265346 |

| | |
|---|---|
| SHA-256: | 1A41F703735FD48EE79E423993B2C6695E326269F7A61304DFF4796F59977FF2 |
| SHA-512: | 28CDDB1071E69145AC1845EC573618EC6268FDEF795B0F3638EB1DEC834C8FE0FC65517D9ED784F81F67535F25333FC986BD9C9B3AAB73BCE4C42837C81E16C |
| Malicious: | false |
| Preview: | .PNG.....IHDR.....a....IDATx.}R..A.....:...}...8.n.m..d.|..Sk.X.....{m....8...1.l...m..vn..G.....n.o..W,]..f.H..h....[ .%.c.b.0...w.}../.~.F&.A.....s..ql....k%.....]..!.....R`..I..$.> @.F.F(.....a....b...;o.&L. ...*e....&....?.....Q.V.%...-J)<~...d.V.\...E....m..L...E..b..<...k.....}.....p<.G...U.b..V.].R.V\....J.8},.x..dT.9..!~.T?xp.... .N...c."...G.. .@..R..H.p..E .GR.....J...7.t.od.....p.%.iG.+v..\.....&\k...s.....T...}.....e0..e?l..{L..Vm.0u..f.....%c.~q.m\.,...Y..U`..O.h.p.9h%..).X...m...i@.8....IEND.B`. |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\System.Xml.XmlDocument.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 16024 |
| Entropy (8bit): | 6.768484247043723 |
| Encrypted: | false |
| SSDEEP: | 384:EVgGf2BiWOsWql//uPHRN7/2WF//dJR9ztBcvM:EVgGL4lXM/2WF//dj9zUvM |
| MD5: | 1FED3E9E68967F0903F43CF955EC8EAE |
| SHA1: | DA9D98424E2BB2AE625E9EBEBD90AD4B7F007CA4 |
| SHA-256: | B861237F55766E286E7008AC4B1E5CE88E88FDF7741EF9C6B00540E1765390F3 |
| SHA-512: | F030383C4D933EC13EE1E892654AEEFD5C722BE25461472639DF49FA0E165AC470BFB901A0A062CA145A6B693C607E279CDBA2A144E62A5B9D2FD6E999943364 |
| Malicious: | false |
| Antivirus: | • Antivirus: ReversingLabs, Detection: 0%<br>• Antivirus: Virustotal, Detection: 0%, Browse |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...B.....!..0.....+... .....@.. ..... `.....|+..O....@.....(...`.....*..8..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc .....`.....@..B.....+.....H..... .....P .....;??5.$\|BdQ..h.X.3\...!..@...C.3.qS.....rS.....?D...f...../....'.ov5..N.q.\|.FB..:....: .z!.rL.Q.... ...F&.....0."....+.$_BSJB.....v4.0.30319.....`.....#~..\.....#Strings....H.....#GUID...X.....#Blob.....3.....#.....P./...../.....O.. .....\...2.....g.....p...../..... |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Konini\Firsaarsfdselsdage\Whorehouse\Faithworthy\accessories-dictionary.png**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 639 |
| Entropy (8bit): | 7.594477595602655 |
| Encrypted: | false |
| SSDEEP: | 12:6v/7xXsWeAITRagJSezSlTm4IpuXLJNux3NdHbvHR+d0FKHrHPnwF4LWbf7H:wlNVSo4gud4NxbvxI0erv04Lcf7H |
| MD5: | B8367F3483C54EFE19D1426A98402829 |
| SHA1: | F9E9A067BFE5F2A3A4AE1C93D519B8B8792719C9 |
| SHA-256: | 0791574192B5767D904619B1F6BB30B3A5101FBD51F8C259C2CFFF078C7ECECD |
| SHA-512: | A4C0E3D1CAA4A828B9160D4936F5E11E42AFE00A9A611A0814884BBA9E18A691D16B142F5A23E2AEE11708C72AADAAB78F19733E1E541BD19E64437AC6E43AED |
| Malicious: | false |
| Preview: | .PNG.....IHDR.....a...FIDATx.....\k..7.....1k7...km...6..]...3....5....9.w....(3..2'...`..27X^S.XV.....Gck.\cKu...q...)...9..sYu~YYU~p\|r4..../..k.%.%.....s...A_.q~x.. ]P..h4.....LKC(.B . g2...0..z.....X.I..6...B.....J...i..n.\|>.D.`}/.I..@-.c.....VP..F'..$.s.$M...a.V..=6._i).:.....!....$..IR...3h.r.@q8@k+..i./.\p> ..ccs...F-I{.n'..JE...C@qE.).....I.+i....pE .b...D.Zr..m,.)!.H ..HY.(..t....uF.!.....H.....iBck5.....y..hk#S0.....,..H..n..a.Z.....\a.d..Y.7..oi.\%>.....165tl.L818j.c.....p.V..j..2....g?...=....._.z...;....?Vw.....^...;\|...../....w..... .?...=.....IEND.B`. |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Laboratories53\x-office-address-book-symbolic.svg**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | SVG Scalable Vector Graphics image |
| Category: | dropped |
| Size (bytes): | 2059 |
| Entropy (8bit): | 5.063551723274034 |
| Encrypted: | false |
| SSDEEP: | 24:t4CpYL7IyKbRAecFxMGMaMlF6Yi36fRMTXoUfQBjWIu4IZ715ByKbRAecFxMGMM:fNtAecFJM/FiqfQpQipvBNtAecFJMM |
| MD5: | 5447BF4EF18181AA69BEC4978E312549 |
| SHA1: | 4843AA2388FE80EE474F399061C6FDBB547BC2BA |
| SHA-256: | EC1CDEAD87BAD12FACA206F03D6748ED11F3A50FF32E8AD341BD44A3A44D6075 |

| | |
|---|---|
| SHA-512: | 611A25E6FE93CFA74DF01200914D730BB608B6EB05BDB8E77F13416800B45468D4067C8516C734B8C602EF4EFEF4B90D045B7456AA2BAF243526C8145BBA3D4D |
| Malicious: | false |
| Preview: | <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M3 1C1 1 1 3 1 3h11v11H1s0 2 2 2h9s.459.014.947-.23C13.436 15.524 14 14.832 14 14V3c0-.833-.564-1.525-1.053-1.77C12.46.986 12 1 12 1z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal" color="#000" font-weight="400" font-family="sans-serif" overflow="visible" fill-rule="evenodd"/><path d="M.5 4h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1zm0 2h2a.499.499 0 110 1h-2a.499.499 0 110-1z"/><path d="M7.285 5.004A3.506 3.506 0 004 |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Mitheithel\Homoplasy\Wice\AMD.Power.Processor.ppkg**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | HTML document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1245 |
| Entropy (8bit): | 5.462849750105637 |
| Encrypted: | false |
| SSDEEP: | 24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5 |
| MD5: | 5343C1A8B203C162A3BF3870D9F50FD4 |
| SHA1: | 04B5B886C20D88B57EEA6D8FF882624A4AC1E51D |
| SHA-256: | DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F |
| SHA-512: | E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949 |
| Malicious: | false |
| Preview: | <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. <h1>Server Error</h1> .. .. <div class="co |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-new-symbolic.symbolic.png**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 200 |
| Entropy (8bit): | 6.353867134664978 |
| Encrypted: | false |
| SSDEEP: | 6:6v/lhPys1AhcwQnKFxLsaV0MSFw6YB1L5jp:6v/7RgFKBE1L5N |
| MD5: | B1E1142D7EF33AD94E80A7394C036540 |
| SHA1: | D05408C3B4360DE12D0B7A1CCB04A27E946FD517 |
| SHA-256: | 9572648AC9CA12A253EFBFB3DB0160C56CBFAAC3157779285642FAEB1D86CA94 |
| SHA-512: | 18AC511A1916E99780BAB5D3CEDBCA816932D88A4230F8FFADE5C17DBF1511840033D5A05322B0AA3EE4D30A9105D2F211C84C46DDFAAA71008444669CB65AF |
| Malicious: | false |
| Preview: | .PNG.....IHDR.....a....sBIT....\|.d.....IDAT8..Q.. .D_...F....t..>d!jS....pa.....F`....t9.....D.`.{`M.7`H..2' >.xS.9W.\|..@[...;T5..Q.... .Y.q.._-..F#F...n..W..8.L'A...!.....IEND.B`. |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\folder-templates-symbolic.svg**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | SVG Scalable Vector Graphics image |
| Category: | dropped |
| Size (bytes): | 963 |
| Entropy (8bit): | 5.12784027591558 |
| Encrypted: | false |
| SSDEEP: | 24:t4CptM48A8A8F+yEcGZrGF19XQzyKbRAecFxMGM7:B8A8A8F+yEcGYFmNtAecFJM7 |
| MD5: | F5A69E814CB5E7713E3C624942DE1DA5 |
| SHA1: | 2919A07D2792295111CF54AF23742CEE14337B10 |
| SHA-256: | 06D97F580D3709C0EA0E2705425C621A17FF97CF3A449B468D2976BA0D55EFEB |
| SHA-512: | ABC0F7671B316DC01152253639319BED058C20D4E8C56F6D23B67AF6584F39E5F3191D97FD8F135C259E5BD7FE032939528A93029D747061500DFAE14C135D55 |
| Malicious: | false |

| | |
|---|---|
| Preview: | <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747" fill-rule="evenodd"><path d="M3 9h1v1H3zm-1 1h1v1H2zm1 1h1v1H3zm-1 1h 1v1H2zm1 1h1v1H3zm-1 1h1v1H2zm2 0h1v1H4zm2 0h1v1H6zm2 0h1v1H8zm2 0h1v1h-1zm-7 1h1v1H3zm2 0h1v1H5zm2 0h1v1H7zm2 0h1v1H9zm2 0h1v1h-1zm1-1h1v1h-1z" style="marker:none" color="#000" overflow="visible"/><path d="M3 1a1 1 0 00-1 1v7h2V3h5.086L12 5.914V14h2V5.5a1 1 0 00-.293-.707l-3.5-3.5A1 1 0 0 09.5 1z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates :normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal" color="#000" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M9 2v4h4z "/></g></svg> |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\printer-printing-symbolic.svg**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | SVG Scalable Vector Graphics image |
| Category: | dropped |
| Size (bytes): | 295 |
| Entropy (8bit): | 4.922153835627764 |
| Encrypted: | false |
| SSDEEP: | 6:tI9mc4slzcWER4W6UmUuksJtjdU0tytIN8uFWOXM2KchvXa7BGl0/:t4CDqW6zUmjW0ktl+sd1a7BM0/ |
| MD5: | 611C311204F39AB0E7F3CC8A0264246A |
| SHA1: | 9E4A3BEA0DE6D11491E5AA69A61E1FF051D79DED |
| SHA-256: | 1E6C4120B833698852CF451D0B5F8FCA83CD5591EA73EBC3C918547B67FBEB34 |
| SHA-512: | 919628653C7441CC4F82C7177D5A6EBBB86686A4E15435A21201B1D77B325808435323FA9FF906E6DB4D612ACEB1C00AC89B0571181D1F521636943EFE25EEF0 |
| Malicious: | false |
| Preview: | <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M2 4c-.5 0-1 .5-1 1v4c0 .5.5 1 1 1h1V8h10v2h1c.5 0 1-.5 1-1V5c0-.5-.5-1-1-1zm2-3v2h8V1z" fill="#2e3436"/><path class="success" d="M4 9v5h8V9zm2.99.998l2.03.011-.01 1 2.003-.01L8.03 13 5 11l2.002.011z" fill="#33d17a"/></svg> |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Paleograph\Statuskonto\Gusting\screen-shared-symbolic.symbolic.png**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 254 |
| Entropy (8bit): | 6.643831924508014 |
| Encrypted: | false |
| SSDEEP: | 6:6v/lhPysJ/dh3z6yXtAMoWACcF/byM2TnmLzU/Jqj84up:6v/7p/dh7tfbAC0uM2ygR94c |
| MD5: | 0DFD6D9ADF93297702595FA9A5D9A7AF |
| SHA1: | 23A4AAE7E34232870AACF6B48B24377EA16519C6 |
| SHA-256: | 8CB87F7A9BFFD886E5931B865AB5731DF7CDD7D2768DA05808FE2D40027ED9C1 |
| SHA-512: | 880643F4BFD6F660B272EE93D38EE2513F26197053E41DF4AFE3FEC77FDBC0A087B295256451A1FB83ABAC594E6A0A585C2619D3DD400AF1DB49035E23FE555F |
| Malicious: | false |
| Preview: | .PNG.....IHDR.....a....sBIT....\|.d.....IDAT8.....0.E_.H. L..4...t.t.....R....SD....EN.Ir..\|....l.`!.@.x`.)...Z...`\7.....4 5..$.`AL.....B]b...y`...g.4..l.;.NL7.p.^.i*.....:.(.S...P. .e.....@.<...#.K....f...x~...$.C.....IEND.B`. |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\AsMultiLang.ini**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 398 |
| Entropy (8bit): | 4.737590272626814 |
| Encrypted: | false |
| SSDEEP: | 6:SIMYmm7jVYNEiJuXLIM/Cnjkq5cKYAbSJ94r1WR0rD1pulzV+ML6JyMx:SI0m7pYNEiJuXLIM6hcKc6curfQzxOf |
| MD5: | D96836E1DD4D151DA0687D7251B528DB |
| SHA1: | CCF444F32EDE194FCDE18BB32EBFCCF921E7CB30 |
| SHA-256: | C013CFD743455DFFDBB614EA966EEC32977D7CBF096DD4A95081E7A650E8E6B9 |
| SHA-512: | 2442D9289CD7E741FF74DD99BEF39EBA7562B94DC153C3C4C4F7642455FFB0879330BC0C59B888F39A352C1C58418995F8AA319FB3BBA110B57FF7EE0A8751EF |
| Malicious: | false |
| Preview: | [Languages]..1028 = TChinese..3076 = TChinese..5124 = TChinese..2052 = SChinese..4100 = SChinese..30724 = SChinese..1034 = Spanish..3082 = Spanish..1046 = Portuguese..2070 = Portuguese..1043 = Dutch..1031 = German..1033 = English..1036 = French..1040 = Italian..1041 = Japanese..1049 = Russian..1055 = Turkish..1042 = Korean..1029 = Czech..1035 = Finnish..1044 = Norwegian..1053 = Swedish |

**C:\Users\user\AppData\Roaming\Kartoffelprodukterne\conchinine\Stinkbranden\Middagsselskaber\PSReadline.psd1**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\Royalistic.exe |
| File Type: | HTML document, ASCII text, with CRLF line terminators |

| | |
|---|---|
| Category: | dropped |
| Size (bytes): | 1245 |
| Entropy (8bit): | 5.462849750105637 |
| Encrypted: | false |
| SSDEEP: | 24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5 |
| MD5: | 5343C1A8B203C162A3BF3870D9F50FD4 |
| SHA1: | 04B5B886C20D88B57EEA6D8FF882624A4AC1E51D |
| SHA-256: | DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F |
| SHA-512: | E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949 |
| Malicious: | false |
| Preview: | <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">.. <head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..b ody{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;mar gin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. <h1>Server Error</h1> .. .. <div class="co |

## Static File Info

### General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive |
| Entropy (8bit): | 7.493705345043699 |
| 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: | Royalistic.exe |
| File size: | 385376 |
| MD5: | d14335f61c99a9b8a2d5e87cdf83cdd0 |
| SHA1: | f82f3481619be8f9f11d76638db3107b1d332912 |
| SHA256: | 08cabec4d0127fb3e6530b04448cb3539c2b8f28988e60499c2dbbfe475206df |
| SHA512: | 9d94b9bc836b9bb292b4e2b0ef83f1632fceb712bf60bdb3127ffaca3b4c2dcbe4aeb3f5ad3c712a47111d81c650b1a44a55e0e26f0f3f83e6727f8556d11ea2 |
| SSDEEP: | 6144:hGemq9vVMEHIx0Sc149PSjEeUlbojewwn1QuMQylhWsqfXatqMFJZV2H4ktcA8a:hmK9MNx0Sc149KAeyyeZ1QiyeVX8zHYX |
| TLSH: | E384F121F128BCCAD60358F01DBDA61051E5DFED80D5450D6ABA328994F239778AFF2E |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....Oa.....f..... ...3.....@ |

### File Icon

| | |
|---|---|
| Icon Hash: | 0355ccaeb2fe5500 |

### Static PE Info

#### General

| | |
|---|---|
| Entrypoint: | 0x4033b3 |
| Entrypoint Section: | .text |
| Digitally signed: | true |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x614F9D8B [Sat Sep 25 22:07:07 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: | 5f0c714c36e6cc016b3a1f4bc86559e4 |

| **Authenticode Signature** | |
|---|---|
| Signature Valid: | **false** |
| Signature Issuer: | E=squeaked@Dipsas.Ge, OU="Skumringstimes subhalid Cocitizen ", O=Alveolariform, L=Saint-Georges-de-Luzen\xe7on, S=Occitanie, C=FR |
| 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 | • 13/08/2022 07:32:24 12/08/2025 07:32:24 |
| Subject Chain | • E=squeaked@Dipsas.Ge, OU="Skumringstimes subhalid Cocitizen ", O=Alveolariform, L=Saint-Georges-de-Luzen\xe7on, S=Occitanie, C=FR |
| Version: | 3 |
| Thumbprint MD5: | 7AB231DCE5C6FFAD69D73B26E510B330 |
| Thumbprint SHA-1: | 78B2E08127E635C646392C64AE8048CE0274B9EB |
| Thumbprint SHA-256: | D5FDEC97888AB854DBF29C2F3CDDD20DE4CEEBF3C0264DBC1620ACC59A819E35 |
| Serial: | 6A4A99A1737DDB2714130F7ACA2C5BCFD03D4200 |

| **Entrypoint Preview** |
|---|
| **Instruction** |
| push ebp |
| mov ebp, esp |
| sub esp, 00000220h |
| push esi |
| push edi |
| xor edi, edi |
| push 00008001h |
| mov dword ptr [ebp-10h], edi |
| mov dword ptr [ebp-04h], 0040A198h |
| mov dword ptr [ebp-08h], edi |
| mov byte ptr [ebp-0Ch], 00000020h |
| call dword ptr [004080B8h] |
| mov esi, dword ptr [004080BCh] |
| lea eax, dword ptr [ebp-000000C0h] |
| push eax |
| mov dword ptr [ebp-000000ACh], edi |
| mov dword ptr [ebp-2Ch], edi |
| mov dword ptr [ebp-28h], edi |
| mov dword ptr [ebp-000000C0h], 0000009Ch |
| call esi |
| test eax, eax |
| jne 00007FDEA4FB4431h |
| lea eax, dword ptr [ebp-000000C0h] |
| mov dword ptr [ebp-000000C0h], 00000094h |
| push eax |
| call esi |
| cmp dword ptr [ebp-000000B0h], 02h |
| jne 00007FDEA4FB441Ch |
| movsx cx, byte ptr [ebp-0000009Fh] |
| mov al, byte ptr [ebp-000000ACh] |
| sub ecx, 30h |
| sub al, 53h |
| mov byte ptr [ebp-26h], 00000004h |
| neg al |
| sbb eax, eax |
| not eax |
| and eax, ecx |
| mov word ptr [ebp-2Ch], ax |
| cmp dword ptr [ebp-000000B0h], 02h |
| jnc 00007FDEA4FB4414h |
| and byte ptr [ebp-26h], 00000000h |

| Instruction |
|---|
| cmp byte ptr [ebp-000000ABh], 00000041h |
| jl 00007FDEA4FB4403h |
| movsx ax, byte ptr [ebp-000000ABh] |
| sub eax, 40h |
| mov word ptr [ebp-2Ch], ax |
| jmp 00007FDEA4FB43F6h |
| mov word ptr [ebp-2Ch], di |
| cmp dword ptr [ebp-000000BCh], 0Ah |
| jnc 00007FDEA4FB43FAh |
| and word ptr [ebp+00000000h], 0000h |

### Rich Headers

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

### Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x8544 | 0xa0 | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0xcf000 | 0x14bf8 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x5d730 | 0xa30 | .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 | 0x29c | .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 | 0x65ba | 0x6600 | False | 0.6783088235294118 | data | 6.475278602230841 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x8000 | 0x1382 | 0x1400 | False | 0.4626953125 | data | 5.262676635269928 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xa000 | 0x48538 | 0x600 | False | 0.4615885416666667 | data | 4.125526322488032 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .ndata | 0x53000 | 0x7c000 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rsrc | 0xcf000 | 0x14bf8 | 0x14c00 | False | 0.16929828689759036 | data | 4.457664961464067 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0xcf250 | 0x10828 | Device independent bitmap graphic, 128 x 256 x 32, image size 0 | English | United States |
| RT_ICON | 0xdfa78 | 0x25a8 | Device independent bitmap graphic, 48 x 96 x 32, image size 0 | English | United States |
| RT_ICON | 0xe2020 | 0x10a8 | Device independent bitmap graphic, 32 x 64 x 32, image size 0 | English | United States |
| RT_ICON | 0xe30c8 | 0x468 | Device independent bitmap graphic, 16 x 32 x 32, image size 0 | English | United States |

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_DIALOG | 0xe3530 | 0x100 | data | English | United States |
| RT_DIALOG | 0xe3630 | 0x11c | data | English | United States |
| RT_DIALOG | 0xe3750 | 0xc4 | data | English | United States |
| RT_DIALOG | 0xe3818 | 0x60 | data | English | United States |
| RT_GROUP_ICON | 0xe3878 | 0x3e | data | English | United States |
| RT_MANIFEST | 0xe38b8 | 0x33e | XML 1.0 document, ASCII text, with very long lines (830), with no line terminators | English | United States |

**Imports**

| DLL | Import |
|---|---|
| ADVAPI32.dll | RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA |
| SHELL32.dll | SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA |
| ole32.dll | IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree |
| COMCTL32.dll | ImageList_Create, ImageList_Destroy, ImageList_AddMasked |
| USER32.dll | SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, SetWindowPos, SetCursor, GetSysColor, SetClassLongA, GetWindowLongA, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard |
| GDI32.dll | SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject |
| KERNEL32.dll | GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersionExA, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv |

**Possible Origin**

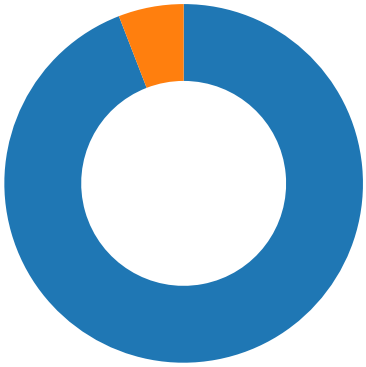
| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States |  |

# Network Behavior

## Network Port Distribution

**Total Packets: 51**

- 53 (DNS)
- 443 (HTTPS)



## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Mar 17, 2023 10:50:21.814665079 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:21.814757109 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:21.815057039 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:21.839333057 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:21.839395046 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:21.909576893 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:21.909811020 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:21.911075115 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:21.911446095 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:21.975106001 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:21.975178003 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:21.976231098 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:21.976440907 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:21.979921103 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:22.020489931 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.076155901 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.076381922 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:23.076458931 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.076620102 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:23.076739073 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:23.076982021 CET | 443 | 49835 | 142.250.184.238 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.077193022 CET | 49835 | 443 | 192.168.11.20 | 142.250.184.238 |
| Mar 17, 2023 10:50:23.162549973 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.162590027 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.162870884 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.163238049 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.163265944 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.226531029 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.226744890 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.228517056 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.228774071 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.232059002 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.232100964 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.232681036 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.232892036 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.233177900 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.276480913 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.509140968 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.509370089 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.509437084 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.509609938 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Mar 17, 2023 10:50:23.510006905 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.510340929 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.511176109 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.511471987 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.511785030 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.512290955 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.512365103 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.512661934 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.513920069 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.514188051 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.514225960 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.514381886 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.516531944 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.516721964 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.518826962 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519010067 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.519031048 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519048929 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519188881 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519244909 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519299984 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.519326925 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519342899 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.519388914 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.519623041 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519648075 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.519675016 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.519835949 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.520343065 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.520580053 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.520597935 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.520886898 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.521034956 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.521508932 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.521522045 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.521795988 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.521820068 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.521835089 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.522102118 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.522438049 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.522537947 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.522810936 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.522838116 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.523034096 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.523266077 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.523371935 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.523494005 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.523508072 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.523678064 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.524259090 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.524411917 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.524482012 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.524508953 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.524624109 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.524739981 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.525156021 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.525305033 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.525352955 CET | 49836 | 443 | 192.168.11.20 | 142.250.184.225 |
| Mar 17, 2023 10:50:23.525374889 CET | 443 | 49836 | 142.250.184.225 | 192.168.11.20 |

### UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Mar 17, 2023 10:50:21.796883106 CET | 60241 | 53 | 192.168.11.20 | 1.1.1.1 |
| Mar 17, 2023 10:50:21.806250095 CET | 53 | 60241 | 1.1.1.1 | 192.168.11.20 |
| Mar 17, 2023 10:50:23.140407085 CET | 59915 | 53 | 192.168.11.20 | 1.1.1.1 |
| Mar 17, 2023 10:50:23.160876036 CET | 53 | 59915 | 1.1.1.1 | 192.168.11.20 |
| Mar 17, 2023 10:50:25.073568106 CET | 59437 | 53 | 192.168.11.20 | 1.1.1.1 |
| Mar 17, 2023 10:50:25.083336115 CET | 53 | 59437 | 1.1.1.1 | 192.168.11.20 |

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|
| Mar 17, 2023 10:50:21.796883106 CET | 192.168.11.20 | 1.1.1.1 | 0x8696 | Standard query (0) | drive.google.com | A (IP address) | IN (0x0001) | false |
| Mar 17, 2023 10:50:23.140407085 CET | 192.168.11.20 | 1.1.1.1 | 0xe52e | Standard query (0) | doc-08-50-docs.googleusercontent.com | A (IP address) | IN (0x0001) | false |
| Mar 17, 2023 10:50:25.073568106 CET | 192.168.11.20 | 1.1.1.1 | 0x37af | Standard query (0) | api.ipify.org | A (IP address) | IN (0x0001) | false |

### DNS Answers

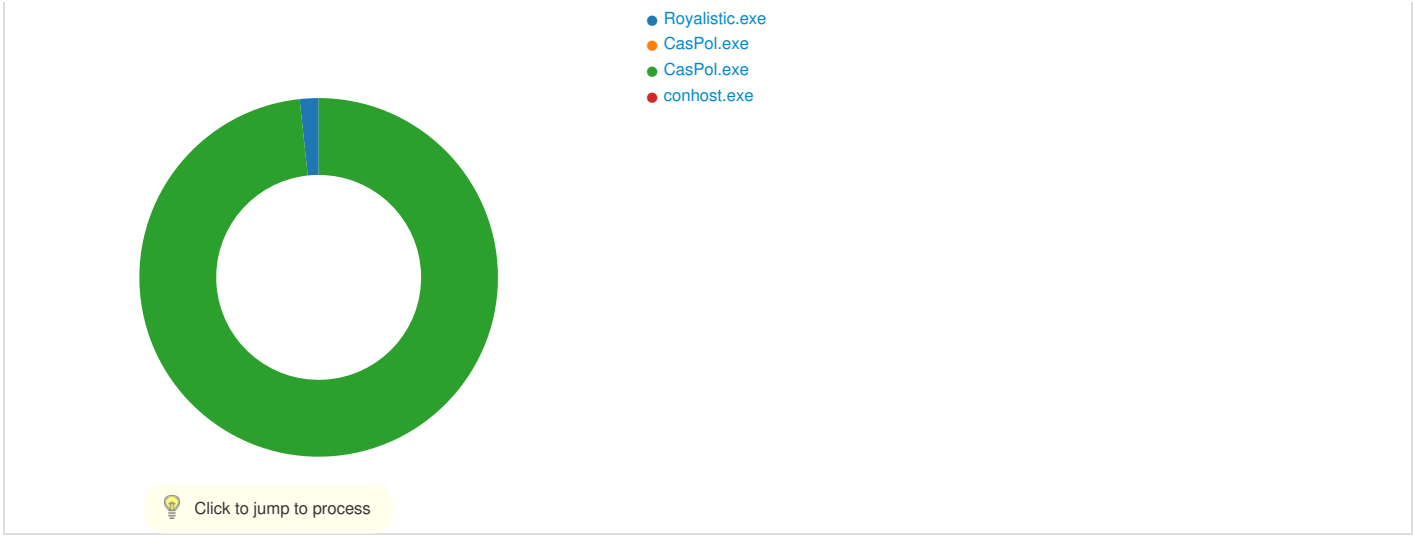
| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class | DNS over HTTPS |
|---|---|---|---|---|---|---|---|---|---|---|
| Mar 17, 2023 10:50:21.806250095 CET | 1.1.1.1 | 192.168.11.20 | 0x8696 | No error (0) | drive.google.com | | 142.250.184.238 | A (IP address) | IN (0x0001) | false |
| Mar 17, 2023 10:50:23.160876036 CET | 1.1.1.1 | 192.168.11.20 | 0xe52e | No error (0) | doc-08-50-docs.googleusercontent.com | googlehosted.l.googleusercontent.com | | CNAME (Canonical name) | IN (0x0001) | false |
| Mar 17, 2023 10:50:23.160876036 CET | 1.1.1.1 | 192.168.11.20 | 0xe52e | No error (0) | googlehosted.l.googleusercontent.com | | 142.250.184.225 | A (IP address) | IN (0x0001) | false |
| Mar 17, 2023 10:50:25.083336115 CET | 1.1.1.1 | 192.168.11.20 | 0x37af | No error (0) | api.ipify.org | api4.ipify.org | | CNAME (Canonical name) | IN (0x0001) | false |
| Mar 17, 2023 10:50:25.083336115 CET | 1.1.1.1 | 192.168.11.20 | 0x37af | No error (0) | api4.ipify.org | | 64.185.227.155 | A (IP address) | IN (0x0001) | false |
| Mar 17, 2023 10:50:25.083336115 CET | 1.1.1.1 | 192.168.11.20 | 0x37af | No error (0) | api4.ipify.org | | 104.237.62.211 | A (IP address) | IN (0x0001) | false |
| Mar 17, 2023 10:50:25.083336115 CET | 1.1.1.1 | 192.168.11.20 | 0x37af | No error (0) | api4.ipify.org | | 173.231.16.76 | A (IP address) | IN (0x0001) | false |

### HTTP Request Dependency Graph

- drive.google.com
- doc-08-50-docs.googleusercontent.com
- api.ipify.org

## Statistics

### Behavior




# System Behavior

## Analysis Process: Royalistic.exe PID: **5084**, Parent PID: **4696**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 10:49:33 |
| Start date: | 17/03/2023 |
| Path: | C:\Users\user\Desktop\Royalistic.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\Royalistic.exe |
| Imagebase: | 0x400000 |
| File size: | 385376 bytes |
| MD5 hash: | D14335F61C99A9B8A2D5E87CDF83CDD0 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000001.00000002.24657057833.00000000007BA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.24658662982.00000000052B6000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

## Analysis Process: CasPol.exe PID: **2280**, Parent PID: **5084**

### General

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 10:50:07 |
| Start date: | 17/03/2023 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\Desktop\Royalistic.exe |
| Imagebase: | 0x1a0000 |
| File size: | 108664 bytes |
| MD5 hash: | 914F728C04D3EDDD5FBA59420E74E56B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: CasPol.exe PID: **7428**, Parent PID: **5084**

### General

| | |
|---|---|
| Target ID: | 5 |
| Start time: | 10:50:07 |
| Start date: | 17/03/2023 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\Royalistic.exe |
| Imagebase: | 0x840000 |
| File size: | 108664 bytes |
| MD5 hash: | 914F728C04D3EDDD5FBA59420E74E56B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.29396081799.00000000363AB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.29396081799.00000000363AB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

#### File Created

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 1B5E506 | 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 | 1B5E506 | 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 | 1B5E506 | 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 | 1B5E506 | 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 | 1B5E506 | 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 | 1B5E506 | 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 | 73963263 | unknown |
| C:\Users\user\AppData\Roaming | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 73963263 | unknown |

| 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 | 73963263 | unknown |
| C:\Users\user\AppData\Roaming | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 73963263 | unknown |

**File Read**

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 4095 | success or wait | 1 | 7396099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 8173 | end of file | 1 | 7396099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4095 | success or wait | 1 | 7396099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 6135 | success or wait | 1 | 7396099B | unknown |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux | unknown | 176 | success or wait | 1 | 738B62DE | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 4095 | success or wait | 1 | 7396D97A | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 8173 | end of file | 1 | 7396D97A | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4095 | success or wait | 1 | 7396D97A | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux | unknown | 620 | success or wait | 1 | 738B62DE | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux | unknown | 864 | success or wait | 1 | 738B62DE | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux | unknown | 900 | success or wait | 1 | 738B62DE | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux | unknown | 748 | success or wait | 1 | 738B62DE | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4095 | success or wait | 1 | 7396099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 8171 | end of file | 1 | 7396099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | unknown | 4096 | end of file | 1 | 727F9B71 | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 4096 | end of file | 1 | 727F9B71 | ReadFile |
| C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux | unknown | 764 | success or wait | 1 | 738B62DE | ReadFile |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 4095 | success or wait | 1 | 7396099B | unknown |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config | unknown | 8173 | end of file | 1 | 7396099B | unknown |
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data | unknown | 45056 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State | unknown | 4096 | success or wait | 26 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State | unknown | 4096 | end of file | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data | unknown | 49152 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | end of file | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini | unknown | 4096 | end of file | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612 | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\37d692c8-75d5-43c5-89ec-67d65f09e454 | unknown | 4096 | success or wait | 2 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612 | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D | unknown | 11104 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D | unknown | 11104 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612 | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\37d692c8-75d5-43c5-89ec-67d65f09e454 | unknown | 4096 | success or wait | 2 | 727F9B71 | ReadFile |

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612 | unknown | 4096 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D | unknown | 11104 | success or wait | 1 | 727F9B71 | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D | unknown | 11104 | success or wait | 1 | 727F9B71 | ReadFile |

### Registry Activities

#### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | success or wait | 1 | 74A4FDB8 | unknown |

#### Key Value Created

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | EnableFileTracing | dword | 0 | success or wait | 1 | 74A4FDB8 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | EnableAutoFileTracing | dword | 0 | success or wait | 1 | 74A4FDB8 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | EnableConsoleTracing | dword | 0 | success or wait | 1 | 74A4FDB8 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | FileTracingMask | dword | -65536 | success or wait | 1 | 74A4FDB8 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | ConsoleTracingMask | dword | -65536 | success or wait | 1 | 74A4FDB8 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | MaxFileSize | dword | 1048576 | success or wait | 1 | 74A4FDB8 | unknown |
| HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS | FileDirectory | expand unicode | %windir%\tracing | success or wait | 1 | 74A4FDB8 | unknown |

## Analysis Process: conhost.exe PID: **564**, Parent PID: **7428**

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 10:50:07 |
| Start date: | 17/03/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7c2510000 |
| File size: | 875008 bytes |
| MD5 hash: | 81CA40085FC75BABD2C91D18AA9FFA68 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

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

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

## Disassembly

No disassembly