


**ID:** 780200
**Sample Name:** 8082-x86.dll
**Cookbook:** default.jbs
**Time:** 16:02:07
**Date:** 08/01/2023
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

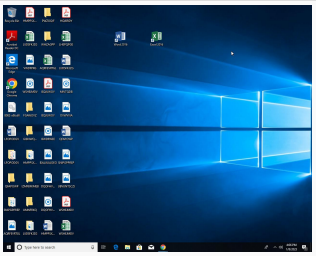
# Windows Analysis Report

## 8082-x86.dll

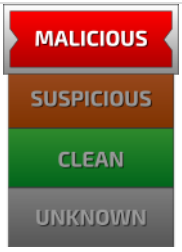
## Overview

### General Information

| | |
|---|---|
| Sample Name: | 8082-x86.dll |
| Analysis ID: | 780200 |
| MD5: | 8d72fc6ff9cb097… |
| SHA1: | d6031029133084. |
| SHA256: | 0b7d19cf030839.. |
| Tags: | 45139105143 CobaltStrike dll opendir |
| Infos: | |



### Detection



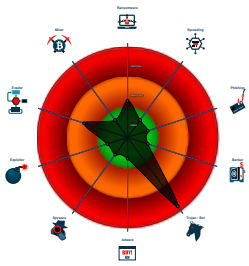

CobaltStrike

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

### Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected CobaltStrike
- C2 URLs / IPs found in malware con…
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Yara signature match
- Tries to load missing DLLs
- Contains functionality to read the PE…
- Uses a known web browser user age…

### Classification



## Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5560 cmdline: loaddll32.exe "C:\Users\user\Desktop\8082-x86.dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 5568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5604 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\8082-x86.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5624 cmdline: rundll32.exe "C:\Users\user\Desktop\8082-x86.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5612 cmdline: regsvr32.exe /s C:\Users\user\Desktop\8082-x86.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 5632 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x86.dll,DllGetClassObject MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5676 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x86.dll,DllMain MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5696 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x86.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

## Malware Configuration

**Threatname: CobaltStrike**

```
{
  "BeaconType": [
    "HTTP"
  ],
  "Port": 8082,
  "SleepTime": 38500,
  "MaxGetSize": 1399607,
  "Jitter": 27,
  "C2Server": "20.104.209.69,/broadcast",
  "HttpPostUri": "/1/events/com.amazon.csm.csa.prod",
  "Malleable_C2_Instructions": [
    "Remove 1308 bytes from the end",
    "Remove 1 bytes from the end",
    "Remove 194 bytes from the beginning",
    "Base64 decode"
  ],
  "SpawnTo": "16nKFaB/gr/TtjAg2jiqFg==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  "HttpPostChunk": 0,
  "Spawnto_x86": "%windir%\\syswow64\\gpupdate.exe",
  "Spawnto_x64": "%windir%\\sysnative\\gpupdate.exe",
  "CryptoScheme": 0,
  "Proxy_Behavior": "Use IE settings",
  "Watermark": 1670873463,
  "bStageCleanup": "True",
  "bCFGCaution": "True",
  "KillDate": 0,
  "bProcInject_StartRWX": "True",
  "bProcInject_UseRWX": "False",
  "bProcInject_MinAllocSize": 16700,
  "ProcInject_PrependAppend_x86": [
    "kJCQ",
    "Empty"
  ],
  "ProcInject_PrependAppend_x64": [
    "kJCQ",
    "Empty"
  ],
  "ProcInject_Execute": [
    "ntdll.dll:RtlUserThreadStart",
    "SetThreadContext",
    "NtQueueApcThread-s",
    "kernel32.dll:LoadLibraryA",
    "CreateRemoteThread",
    "RtlCreateUserThread"
  ],
  "ProcInject_AllocationMethod": "NtMapViewOfSection",
  "bUsesCookies": "False",
  "HostHeader": ""
}
```


# Yara Signatures

## Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 8082-x86.dll | CobaltStrike_Resources_Artifact32_v3_14_to_v4_x | Cobalt Strike\'s resources/artifact32{.dll,.exe,big.exe,big.dll,bigsvc.exe} signature for versions 3.14 to 4.x and resources/artifact32svc.exe for 3.14 to 4.x and resources/artifact32uac.dll for v3.14 and v4.0 | gssincla@google.com | • 0xacb:$pushFmtStr: C7 44 24 28 5C 00 00 00 C7 44 24 24 65 00 00 00 C7 44 24 20 70 00 00 00 C7 44 24 1C 69 00 00 00 C7 44 24 18 70 00 00 00 F7 F1 C7 44 24 14 5C 00 00 00 C7 44 24 10 2E 00 00 00 C7 44 24 0C 5C 00 ...<br>• 0x44624:$fmtStr: %c%c%c%c%c%c%c%cMSSE-%d-server |
| 8082-x86.dll | JoeSecurity_CobaltStrike_4 | Yara detected CobaltStrike | Joe Security | |

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.620024884.0000000000950000.00000020.00001000.00020000.00000000.sdmp | CobaltStrike_Sleeve_Beacon_Dll_v4_3_v4_4_v4_5_and_v4_6 | Cobalt Strike\'s sleeve/beacon.dll Versions 4.3 and 4.4 | gssincla@google.com | • 0x72da:$version_sig: 48 57 8B F2 83 F8 65 0F 87 47 03 00 00 FF 24<br>• 0x96c3:$decoder: 80 B0 20 10 98 00 2E 40 3D 00 10 00 00 7C F1 |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000003.435119690.00000000012D8000.00000004.00000800.00020000.00000000.sdmp | SUSP_PS1_FromBase64String_Content_Indicator | Detects suspicious base64 encoded PowerShell expressions | Florian Roth | • 0x1bb8:$: ::FromBase64String("H4s<br>• 0x1bb8:$: ::FromBase64String("H4sIA |
| 00000000.00000003.435119690.00000000012D8000.00000004.00000800.00020000.00000000.sdmp | CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x | Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x | gssincla@google.com | • 0x1b90:$ps1: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(<br>• 0x2aa99:$ps2: ));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd(); |
| 00000000.00000003.436145653.00000000012D8000.00000004.00000800.00020000.00000000.sdmp | SUSP_PS1_FromBase64String_Content_Indicator | Detects suspicious base64 encoded PowerShell expressions | Florian Roth | • 0x1bb8:$: ::FromBase64String("H4s<br>• 0x1bb8:$: ::FromBase64String("H4sIA |
| 00000000.00000003.436145653.00000000012D8000.00000004.00000800.00020000.00000000.sdmp | CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x | Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x | gssincla@google.com | • 0x1b90:$ps1: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(<br>• 0x2aa99:$ps2: ));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd(); |
| Click to see the 21 entries | | | | |

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

### Networking

C2 URLs / IPs found in malware configuration

Uses known network protocols on non-standard ports

### System Summary

Malicious sample detected (through community Yara rule)

### Hooking and other Techniques for Hiding and Protection

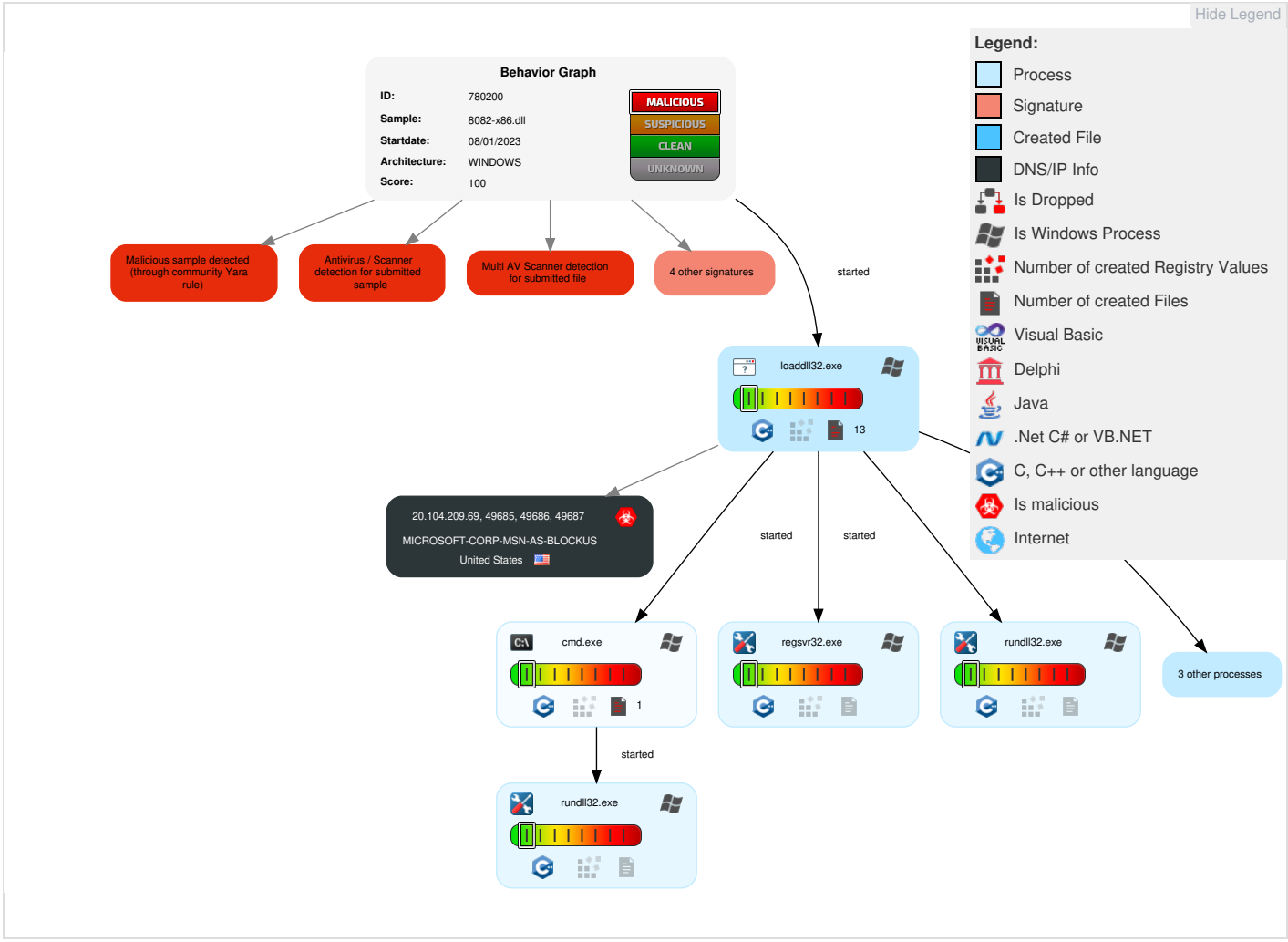
Uses known network protocols on non-standard ports

### Remote Access Functionality

## 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 1 Process Injection | 1 Virtualization/Sandbox Evasion | OS Credential Dumping | 1 Virtualization/Sandbox Evasion | Remote Services | 1 Archive Collected Data | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | 1 DLL Side-Loading | 1 1 Process Injection | LSASS Memory | 2 Process Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 1 1 Non-Standard Port | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | 1 Deobfuscate/Decode Files or Information | Security Account Manager | 1 Account Discovery | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | 2 Ingress Tool Transfer | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 2 Obfuscated Files or Information | NTDS | 1 System Owner/User Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 2 Non-Application Layer Protocol | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 1 Regsvr32 | LSA Secrets | 2 System Information Discovery | SSH | Keylogging | Data Transfer Size Limits | 1 1 2 Application Layer Protocol | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 1 Rundll32 | 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 |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | 1 DLL Side-Loading | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points | | Data Encrypted for Impact |

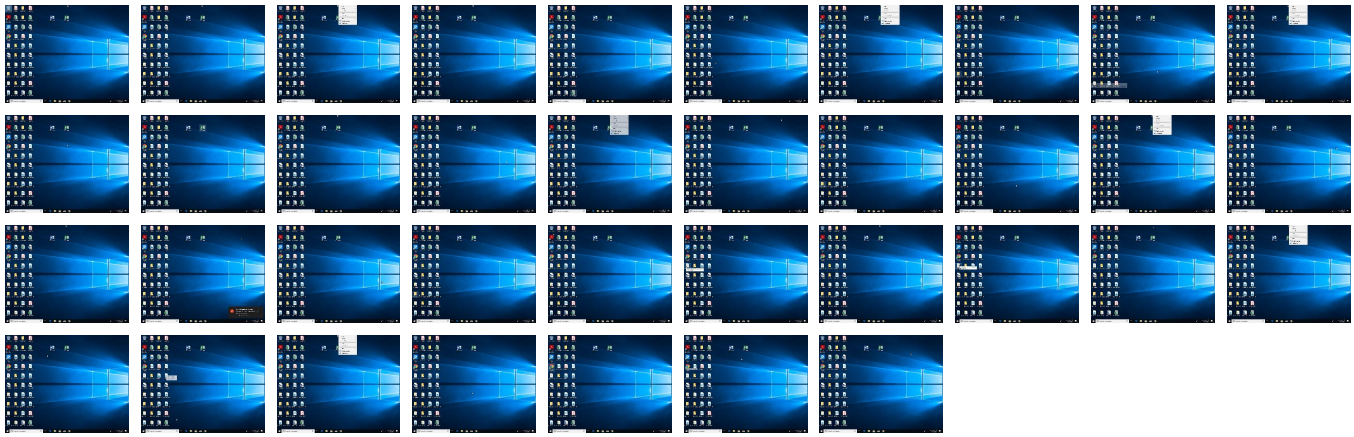
## Behavior Graph




## Screenshots

### Thumbnails

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




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 8082-x86.dll | 88% | ReversingLabs | Win32.Trojan.CobaltStrike | |
| 8082-x86.dll | 70% | Virustotal | | Browse |
| 8082-x86.dll | 100% | Avira | HEUR/AGEN.1235510 | |
| 8082-x86.dll | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://20.104.209.69:8082/broadcast | 0% | Avira URL Cloud | safe | |
| http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prod | 0% | Avira URL Cloud | safe | |
| 20.104.209.69 | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

No contacted domains info

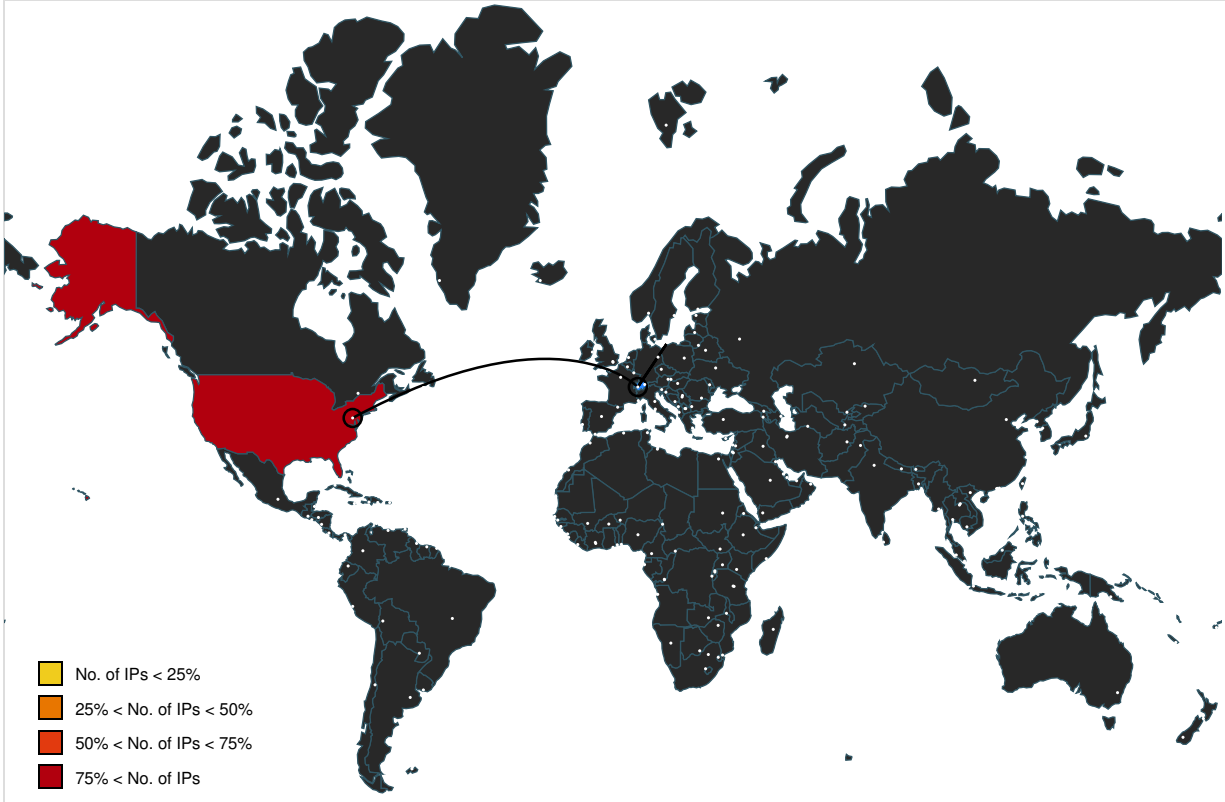
## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://20.104.209.69:8082/broadcast | true | • Avira URL Cloud: safe | unknown |
| 20.104.209.69 | true | • Avira URL Cloud: safe | unknown |
| http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prod | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://d22u79neyj432a.cloudfront.net/bfc50dfa-8e10-44b5-ae59-ac26bfc71489/54857e6d-c060-4b3c-914a-8 | loaddll32.exe, 00000000.00000002.6201618 36.0000000000E2E000.00000004.00000800.00 020000.00000000.sdmp, loaddll32.exe, 000 00000.00000002.620169392.0000000000E5800 0.00000004.00000800.00020000.00000000.sdmp | false | | high |

## World Map of Contacted IPs




## Public IPs

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 20.104.209.69 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | true |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 36.0.0 Rainbow Opal |
| Analysis ID: | 780200 |
| Start date and time: | 2023-01-08 16:02:07 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 19s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 8082-x86.dll |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Run name: | Run with higher sleep bypass |
| Number of analysed new started processes analysed: | 13 |
| 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: | mal100.troj.winDLL@14/0@0/1 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 98%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Found application associated with file extension: .dll<br>• Sleeps bigger than 100000000ms are automatically reduced to 1000ms |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- 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 NtQueryValueKey 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

No created / dropped files found

## Static File Info

### General

| | |
|---|---|
| File type: | PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows |
| Entropy (8bit): | 6.6495124481937875 |
| TrID: | • Win32 Dynamic Link Library (generic) (1002004/3) 99.60%<br>• Generic Win/DOS Executable (2004/3) 0.20%<br>• DOS Executable Generic (2002/1) 0.20%<br>• VXD Driver (31/22) 0.00%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | 8082-x86.dll |
| File size: | 285184 |
| MD5: | 8d72fc6ff9cb0971df587d20dda5e8c8 |
| SHA1: | d6031029133084901392b856fe66f00f438d95d9 |
| SHA256: | 0b7d19cf030839c3df481069772c7a32b5a3be4c41ce6b436ab69015fa90d98a |
| SHA512: | 9c2074e9e68676ce41346f9bce266fb1155d75fc4f1efc6f40bbcb7871ab6a2f7eda724c4381dd288d817929117fbea9bd3a6d0c977f3db5a55fad1bb35e294d |
| SSDEEP: | 3072:GjXnzH5O+xdKYgC2F/bHnOdisDmtam6SBSZge2x7WBNvjxDld7JOwy6t7bAl+dBj:mNaYn+HNtaJD7VUwl7Y+T |
| TLSH: | 1154CFE5B1DC6B67F844BABA93E1EA0A32A93CD88214E511B3FDDFF6210145CB8D44C5 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....#.....V.....<br>.....0.....k.....4..... ..... |

### File Icon

| | |
|---|---|
| Icon Hash: | 74f0e4ecccdce0e4 |

### Static PE Info

#### General

| | |
|---|---|
| Entrypoint: | 0x6bac1420 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x6bac0000 |
| Subsystem: | windows cui |
| Image File Characteristics: | EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DEBUG_STRIPPED, DLL |
| DLL Characteristics: | |
| Time Stamp: | 0x5EDED50C [Tue Jun 9 00:17:16 2020 UTC] |
| TLS Callbacks: | 0x6bac1a50, 0x6bac1a00 |
| 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: | e1dcffde169ed8b947dc63acdb78aeca |

| Entrypoint Preview |
|---|
| **Instruction** |
| sub esp, 1Ch |
| mov edx, dword ptr [esp+24h] |
| mov dword ptr [6BB07018h], 00000000h |
| cmp edx, 01h |
| je 00007FBA3CA7FA6Ch |
| mov ecx, dword ptr [esp+28h] |
| mov eax, dword ptr [esp+20h] |
| call 00007FBA3CA7F872h |
| add esp, 1Ch |
| retn 000Ch |
| lea esi, dword ptr [esi+00000000h] |
| mov dword ptr [esp+0Ch], edx |
| call 00007FBA3CA807ECh |
| mov edx, dword ptr [esp+0Ch] |
| jmp 00007FBA3CA7FA29h |
| nop |
| push ebp |
| mov ebp, esp |
| sub esp, 18h |
| mov eax, dword ptr [6BB05418h] |
| test eax, eax |
| je 00007FBA3CA7FA8Eh |
| mov dword ptr [esp], 6BB06000h |
| call dword ptr [6BB09138h] |
| mov edx, 00000000h |
| sub esp, 04h |
| test eax, eax |
| je 00007FBA3CA7FA68h |
| mov dword ptr [esp+04h], 6BB0600Eh |
| mov dword ptr [esp], eax |
| call dword ptr [6BB0913Ch] |
| sub esp, 08h |
| mov edx, eax |
| test edx, edx |
| je 00007FBA3CA7FA5Bh |
| mov dword ptr [esp], 6BB05418h |
| call edx |
| leave |
| ret |
| lea esi, dword ptr [esi+00h] |
| push ebp |
| mov ebp, esp |
| pop ebp |
| ret |
| nop |
| nop |
| nop |
| nop |
| nop |
| nop |
| nop |

| Instruction |
| --- |
| nop |
| nop |
| nop |
| nop |
| push ebp |
| mov ebp, esp |
| push edi |
| push esi |
| push ebx |
| sub esp, 4Ch |
| mov edi, dword ptr [ebp+08h] |
| mov esi, dword ptr [ebp+0Ch] |
| mov dword ptr [ebp-1Ch], 00000000h |
| mov dword ptr [esp+1Ch], 00000000h |
| mov dword ptr [esp+18h], 00000000h |
| mov dword ptr [eax+eax+00h], 00000000h |

**Data Directories**

| Name | Virtual Address | Virtual Size | Is in Section |
| --- | --- | --- | --- |
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x48000 | 0xb0 | .edata |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x49000 | 0x5bc | .idata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x4c000 | 0x4ac | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x4b000 | 0x18 | .tls |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x49108 | 0xcc | .idata |
| 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 | 0x1a84 | 0x1c00 | False | 0.5262276785714286 | data | 5.9055220621274644 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .data | 0x3000 | 0x4241c | 0x42600 | False | 0.5397871056967984 | data | 6.6586521702558805 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .rdata | 0x46000 | 0x1a0 | 0x200 | False | 0.529296875 | data | 4.462802731767267 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ |
| .bss | 0x47000 | 0x418 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .edata | 0x48000 | 0xb0 | 0x200 | False | 0.2734375 | data | 1.9817948694706844 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ |
| .idata | 0x49000 | 0x5bc | 0x600 | False | 0.4296875 | data | 4.870768861754693 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .CRT | 0x4a000 | 0x2c | 0x200 | False | 0.052734375 | data | 0.18120187678200297 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .tls | 0x4b000 | 0x20 | 0x200 | False | 0.0546875 | data | 0.2797047950073886 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .reloc | 0x4c000 | 0x4ac | 0x600 | False | 0.7005208333333334 | data | 5.557340256736937 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Imports

| DLL | Import |
|---|---|
| KERNEL32.dll | CloseHandle, ConnectNamedPipe, CreateFileA, CreateNamedPipeA, CreateThread, DeleteCriticalSection, EnterCriticalSection, FreeLibrary, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetProcAddress, GetSystemTimeAsFileTime, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, LoadLibraryA, LoadLibraryW, QueryPerformanceCounter, ReadFile, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualAlloc, VirtualProtect, VirtualQuery, WriteFile |
| msvcrt.dll | __dllonexit, _amsg_exit, _initterm, _iob, _lock, _onexit, _unlock, _winmajor, abort, calloc, free, fwrite, malloc, memcpy, sprintf, strlen, strncmp, vfprintf |

### Exports

| Name | Ordinal | Address |
|---|---|---|
| DllGetClassObject | 1 | 0x6bac17ee |
| DllMain | 2 | 0x6bac178b |
| DllRegisterServer | 3 | 0x6bac17e0 |
| DllUnregisterServer | 4 | 0x6bac17e7 |
| StartW | 5 | 0x6bac1803 |

## Network Behavior

### TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 8, 2023 16:03:30.432375908 CET | 49685 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:03:30.547492981 CET | 8082 | 49685 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:03:30.547652960 CET | 49685 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:03:30.574161053 CET | 49685 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:03:30.690412045 CET | 8082 | 49685 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:03:30.692807913 CET | 8082 | 49685 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:03:30.692890882 CET | 8082 | 49685 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:03:30.692893028 CET | 49685 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:03:30.692970037 CET | 49685 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:03:30.692990065 CET | 8082 | 49685 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:03:30.693047047 CET | 49685 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:03:30.694236040 CET | 49685 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:03:30.809875965 CET | 8082 | 49685 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.041449070 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.155930996 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.156147957 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.156966925 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.270982027 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285484076 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285547018 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285581112 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285617113 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285650969 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285684109 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285711050 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.285716057 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285751104 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285788059 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285801888 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.285828114 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.285830975 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.285868883 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400144100 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400207043 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400235891 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400262117 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400286913 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400311947 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400336981 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400366068 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400386095 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400424004 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400440931 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400471926 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400480986 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400501966 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400507927 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400528908 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400530100 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400547981 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400557041 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400567055 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400584936 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400602102 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400613070 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400628090 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400638103 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400662899 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400680065 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |

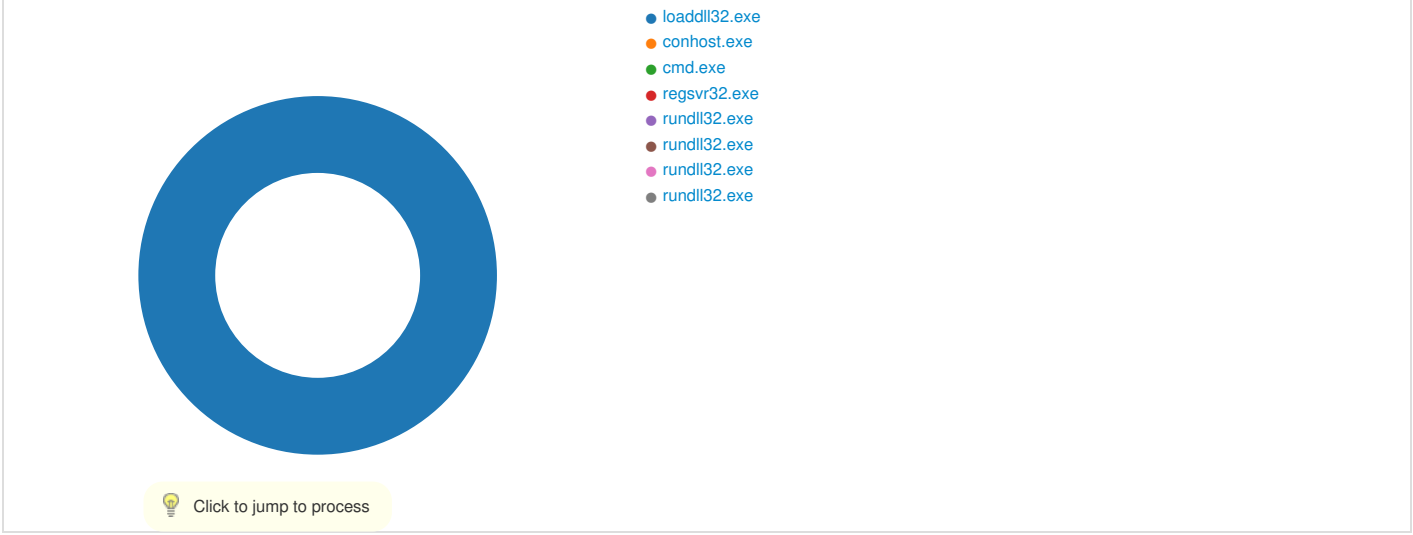
| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 8, 2023 16:04:02.400741100 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400769949 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400798082 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400813103 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400819063 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400845051 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.400854111 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.400887966 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.515465975 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515511036 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515531063 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515554905 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515674114 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.515723944 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515738010 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.515748978 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515769958 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515774012 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.515791893 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.515799046 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.515832901 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.516217947 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516247034 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516267061 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516287088 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516295910 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.516344070 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.516704082 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516726017 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516746044 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516767025 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516777992 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.516788006 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516823053 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.516834974 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516855955 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516875982 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |
| Jan 8, 2023 16:04:02.516885996 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.516904116 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.516952038 CET | 49686 | 8082 | 192.168.2.4 | 20.104.209.69 |
| Jan 8, 2023 16:04:02.517013073 CET | 8082 | 49686 | 20.104.209.69 | 192.168.2.4 |

### HTTP Request Dependency Graph

- https:
  - 20.104.209.69:8082

## Statistics

### Behavior




## System Behavior

### Analysis Process: loaddll32.exe PID: **5560**, Parent PID: **3528**

| General | |
|---|---|
| Target ID: | 0 |
| Start time: | 16:03:18 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe "C:\Users\user\Desktop\8082-x86.dll" |
| Imagebase: | 0x13d0000 |
| File size: | 116736 bytes |
| MD5 hash: | 1F562FBF37040EC6C43C8D5EF619EA39 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: CobaltStrike_Sleeve_Beacon_Dll_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/beacon.dll Versions 4.3 and 4.4, Source: 00000000.00000002.620024884.0000000000950000.00000020.00001000.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000000.00000003.435119690.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x, Description: Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x, Source: 00000000.00000003.435119690.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000000.00000003.436145653.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x, Description: Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x, Source: 00000000.00000003.436145653.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000000.00000003.435087941.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x, Description: Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x, Source: 00000000.00000003.435087941.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000000.00000003.581071660.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x, Description: Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x, Source: 00000000.00000003.581071660.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000000.00000003.511799758.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x, Description: Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x, Source: 00000000.00000003.511799758.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000000.00000002.620198943.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: CobaltStrike_Resources_Command_Ps1_v2_5_to_v3_7_and_Resources_Compress_Ps1_v3_8_to_v4_x, Description: Cobalt Strike\'s resources/command.ps1 for versions 2.5 to v3.7 and resources/compress.ps1 from v3.8 to v4.x, Source: 00000000.00000002.620198943.00000000012D8000.00000004.00000800.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: CobaltStrike_Sleeve_BeaconLoader_VA_x86_o_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/BeaconLoader.VA.x86.o (VirtualAlloc) Versions 4.3 through at least 4.6, Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: Trojan_Raw_Generic_4, Description: unknown, Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: FireEye<br>• Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net<br>• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key., Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Metasploit_7bc0f998, Description: Identifies the API address lookup function leverage by metasploit shellcode, Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: unknown<br>• Rule: Windows_Trojan_Metasploit_c9773203, Description: Identifies the 64 bit API hashing function used by Metasploit. This has been re-used by many other malware families., Source: 00000000.00000003.364898115.0000000000CE0000.00000020.00001000.00020000.00000000.sdmp, Author: unknown |
| Reputation: | high |

### File Activities

## Analysis Process: conhost.exe PID: **5568**, Parent PID: **5560**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 16:03:18 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7c72c0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: cmd.exe PID: **5604**, Parent PID: **5560**

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 16:03:18 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\8082-x86.dll",#1 |
| Imagebase: | 0xd90000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| 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 | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Analysis Process: regsvr32.exe PID: 5612, Parent PID: 5560

### General

| | |
|---|---|
| Target ID: | 3 |
| Start time: | 16:03:18 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\SysWOW64\regsvr32.exe |
| Wow64 process (32bit): | true |
| Commandline: | regsvr32.exe /s C:\Users\user\Desktop\8082-x86.dll |
| Imagebase: | 0x2a0000 |
| File size: | 20992 bytes |
| MD5 hash: | 426E7499F6A7346F0410DEAD0805586B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 5624, Parent PID: 5604

### General

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 16:03:18 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\8082-x86.dll",#1 |
| Imagebase: | 0x200000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 5632, Parent PID: 5560

### General

| | |
|---|---|
| Target ID: | 5 |
| Start time: | 16:03:18 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\8082-x86.dll,DllGetClassObject |
| Imagebase: | 0x200000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **5676**, Parent PID: **5560**

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 16:03:22 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\8082-x86.dll,DllMain |
| Imagebase: | 0x200000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **5696**, Parent PID: **5560**

### General

| | |
|---|---|
| Target ID: | 7 |
| Start time: | 16:03:25 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\8082-x86.dll,DllRegisterServer |
| Imagebase: | 0x200000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

# Disassembly

**No disassembly**