


**ID:** 780203
**Sample Name:** 8082-x64.dll.dll
**Cookbook:** default.jbs
**Time:** 16:08:56
**Date:** 08/01/2023
**Version:** 36.0.0 Rainbow Opal

# Table of Contents

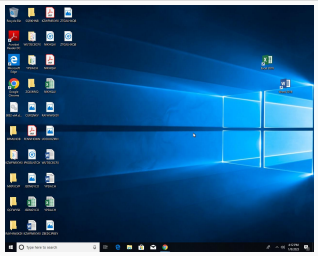
# Windows Analysis Report

## 8082-x64.dll.dll

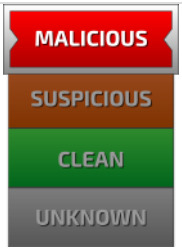
## Overview

### General Information

| | |
|---|---|
| Sample Name: | 8082-x64.dll.dll |
| Analysis ID: | 780203 |
| MD5: | 43616639411a59. |
| SHA1: | 416932059dc348.. |
| SHA256: | 6a289f491c8d5d.. |
| Tags: | 45139105143 exe opendir |
| Infos: | |



### Detection



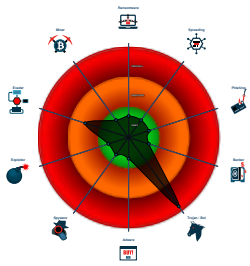

CobaltStrike

| | |
|---|---|
| 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…
- Yara signature match
- Tries to load missing DLLs
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

### Classification



## Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 3648 cmdline: loaddll64.exe "C:\Users\user\Desktop\8082-x64.dll.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 2884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6104 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\8082-x64.dll.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4848 cmdline: rundll32.exe "C:\Users\user\Desktop\8082-x64.dll.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 3480 cmdline: regsvr32.exe /s C:\Users\user\Desktop\8082-x64.dll.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 1304 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllGetClassObject MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1004 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllMain MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4532 cmdline: rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- **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-x64.dll.dll | CobaltStrike_Resources_Artifact64_v3_14_to_v4_x | Cobalt Strike\'s resources/artifact64{.exe,.dll,svc.exe,svcbig.exe,big.exe,big.dll,.x64.dll,big.x64.dll} and resource/artifactuac(alt)64.exe signature for versions v3.14 through v4.x | gssincla@google.com | • 0xa25:$fmtBuilder: 41 B8 5C 00 00 00 C7 44 24 50 5C 00 00 00 C7 44 24 48 65 00 00 00 C7 44 24 40 70 00 00 00 C7 44 24 38 69 00 00 00 C7 44 24 30 70 00 00 00 C7 44 24 28 5C 00 00 00 C7 44 24 20 2E 00 00 00 89 54 ...<br>• 0x44a00:$fmtString: %c%c%c%c%c%c%c%c%cMSSE-%d-server |
| 8082-x64.dll.dll | JoeSecurity_CobaltStrike_4 | Yara detected CobaltStrike | Joe Security | |

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.579279943.00000267603C6000.00000004.00000001.00020000.00000000.sdmp | SUSP_PS1_FromBase64String_Content_Indicator | Detects suspicious base64 encoded PowerShell expressions | Florian Roth | • 0x7498:$: ::FromBase64String("H4s<br>• 0x7498:$: ::FromBase64String("H4sIA |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.579279943.00000267603C6000.00000004.00000001.00020000.00000000.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 | • 0x7470:$ps1: $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String(<br>• 0x30379:$ps2: ));IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd(); |
| 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp | CobaltStrike_Sleeve_BeaconLoader_VA_x64_o_v4_3_v4_4_v4_5_and_v4_6 | Cobalt Strike\'s sleeve/BeaconLoader.VA.x64.o (VirtualAlloc) Versions 4.3 through at least 4.6 | gssincla@google.com | • 0x16ce5:$core_sig: C6 44 24 48 56 C6 44 24 49 69 C6 44 24 4A 72 C6 44 24 4B 74 C6 44 24 4C 75 C6 44 24 4D 61 C6 44 24 4E 6C C6 44 24 4F 41 C6 44 24 50 6C C6 44 24 51 6C C6 44 24 52 6F C6 44 24 53 63 C6 44 24 54 ...<br>• 0x16755:$deobfuscator: 8B 04 24 FF C0 89 04 24 8B 44 24 28 39 04 24 73 20 8B 04 24 0F B6 4C 24 30 48 8B 54 24 20 0F BE 04 02 33 C1 8B 0C 24 48 8B 54 24 20 88 04 0A |
| 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp | Cobaltbaltstrike_Beacon_x64 | Detects CobaltStrike payloads | Avast Threat Intel Team | • 0x3:$h01: 4D 5A 41 52 55 48 89 E5 48 81 EC 20 00 00 00 48 8D 1D EA FF FF FF 48 89<br>• 0x3b633:$h13: 2E 2F 2E 2F 2E 2C 2E 2E 2E 2C 2E 2F 2E 2C 31 BC 2E |
| 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp | CobaltStrike_C2_Encoded_XOR_Config_Indicator | Detects CobaltStrike C2 encoded profile configuration | yara@s3c.za.net | • 0x3b633:$s046: 2E 2F 2E 2F 2E 2C 2E 2E 2E 2C 2E 2F 2E 2C 31 BC 2E 2D 2E 2C 2E 2A 2E 2E B8 4A 2E 2A 2E 2C 2E 2A 2E 3B 75 19 2E 2B 2E 2F 2E 2C 2E 35 |
| Click to see the 10 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

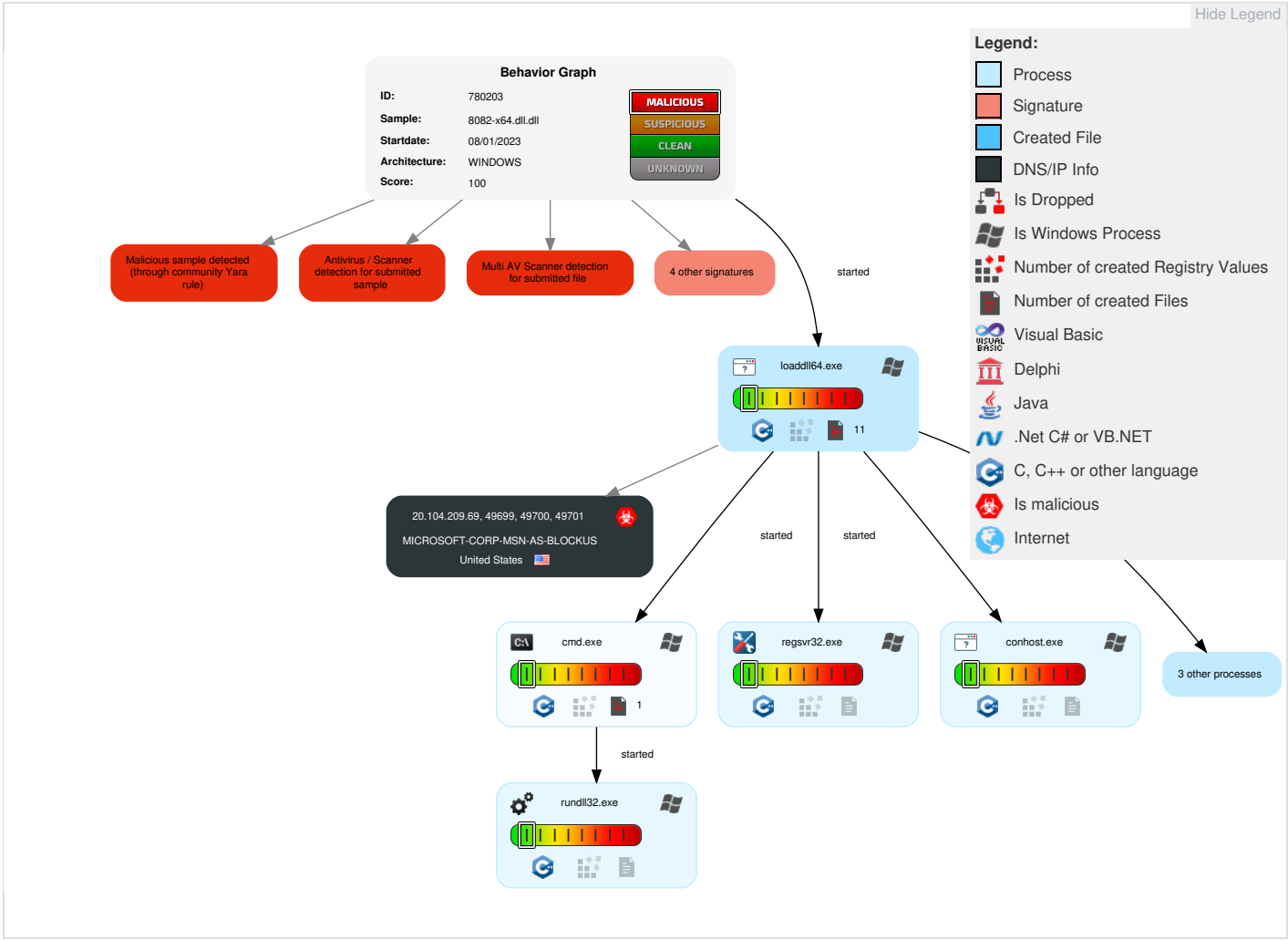
Uses known network protocols on non-standard ports

Yara detected CobaltStrike

## 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 | Windows Management Instrumentation | 1 DLL Side-Loading | 1 1 Process Injection | 1 1 Virtualization/Sandbox Evasion | OS Credential Dumping | 1 Security Software Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | 1 1 Non-Standard Port | 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 | 1 Process Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | 1 Ingress Tool Transfer | 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 Obfuscated Files or Information | Security Account Manager | 1 1 Virtualization/Sandbox Evasion | SMB/Windows Admin Shares | Data from Network Shared Drive | 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 Regsvr32 | NTDS | 2 System Information Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | 1 1 2 Application Layer Protocol | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 1 Rundll32 | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 1 DLL Side-Loading | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |

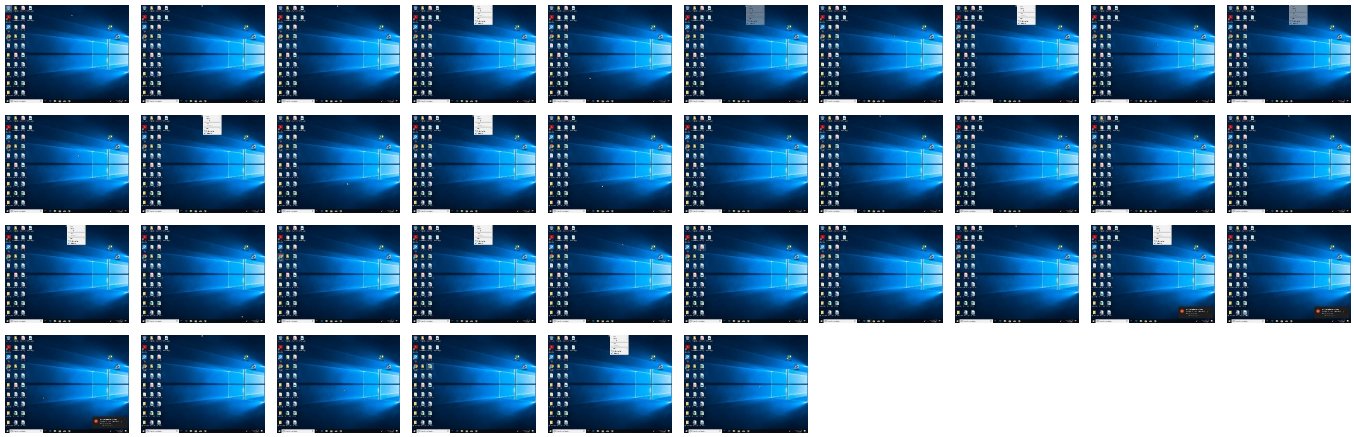
## Behavior Graph




## Screenshots

### Thumbnails

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




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 8082-x64.dll.dll | 78% | ReversingLabs | Win64.Backdoor.CobaltStrike | |
| 8082-x64.dll.dll | 63% | Virustotal | | Browse |
| 8082-x64.dll.dll | 100% | Avira | HEUR/AGEN.1235510 | |
| 8082-x64.dll.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/broadcastp | 0% | Avira URL Cloud | safe | |
| http://20.104.209.69:8082/broadcast? | 0% | Avira URL Cloud | safe | |
| http://20.104.209.69:8082/broadcast | 0% | Virustotal | | Browse |
| http://20.104.209.69:8082/broadcast | 0% | Avira URL Cloud | safe | |
| 20.104.209.69 | 0% | Avira URL Cloud | safe | |
| http://20.104.209.69:8082/broadcast2 | 0% | Avira URL Cloud | safe | |
| http://20.104.209.69:8082/1/events/com.amazon.csm.csa.prod | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

No contacted domains info

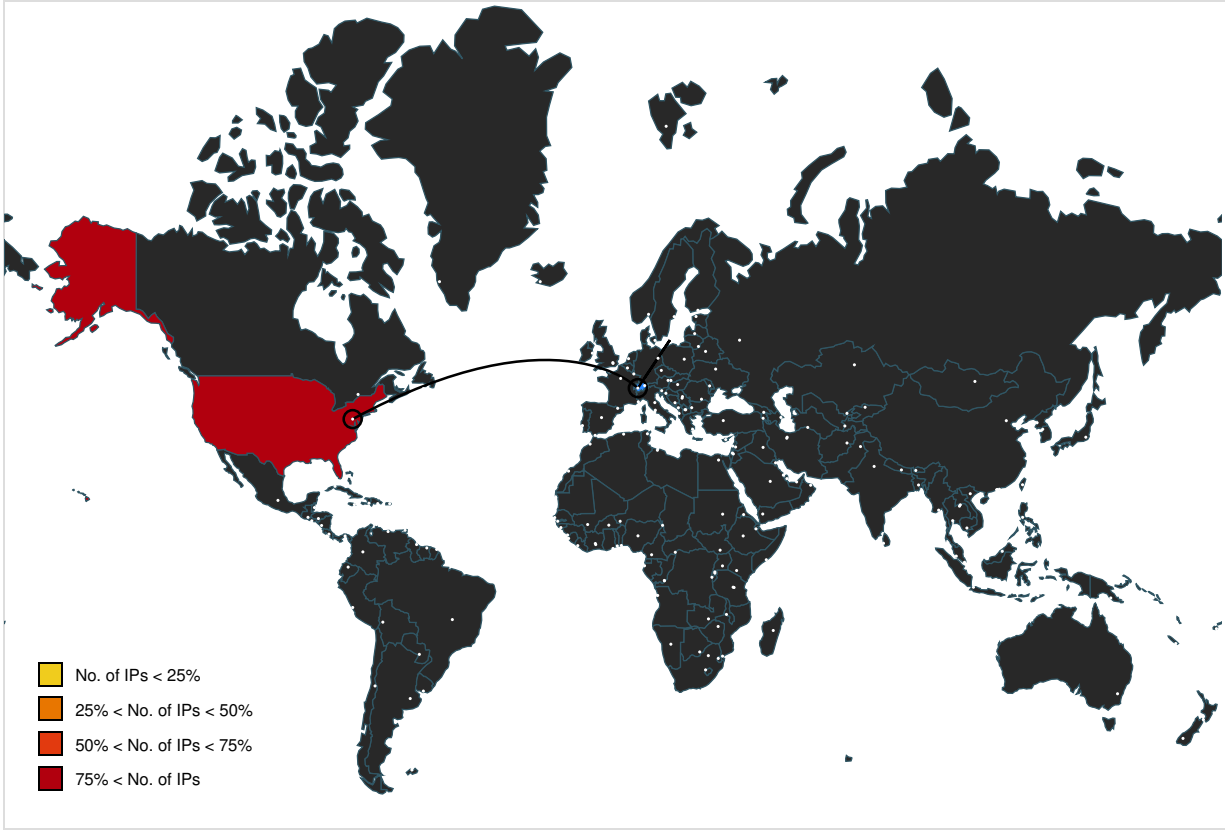
## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://20.104.209.69:8082/broadcast | true | • 0%, Virustotal, Browse<br>• 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://20.104.209.69:8082/broadcast? | loaddll64.exe, 00000000.00000003.395924452.00000267603A7000.00000004.00001000.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000002.579245580.00000267603A5000.00000004.00000001.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://20.104.209.69:8082/broadcastp | loaddll64.exe, 00000000.00000002.579185009.0000026760353000.00000004.00000001.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://20.104.209.69:8082/broadcast(( | loaddll64.exe, 00000000.00000003.395924452.00000267603A7000.00000004.00001000.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000002.579245580.00000267603A5000.00000004.00000001.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://www.amazon.com | loaddll64.exe, 00000000.00000002.579185009.0000026760353000.00000004.00000001.00020000.00000000.sdmp | false | | high |
| http://20.104.209.69:8082/broadcast2 | loaddll64.exe, 00000000.00000003.395924452.00000267603A7000.00000004.00001000.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000002.579245580.00000267603A5000.00000004.00000001.00020000.00000000.sdmp | false | • Avira URL Cloud: safe | unknown |
| http://https://d22u79neyj432a.cloudfront.net/bfc50dfa-8e10-44b5-ae59-ac26bfc71489/54857e6d-c060-4b3c-914a-8 | loaddll64.exe, 00000000.00000002.579668975.0000026760402000.00000004.00000001.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000002.579895773.00000267605C1000.00000004.00001000.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000002.579889103.0000026760597000.00000004.00001000.00020000.00000000.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: | 780203 |
| Start date and time: | 2023-01-08 16:08:56 +01:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 28s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 8082-x64.dll.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: | 11 |
| 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: | Failed |
| HDC Information: | Failed |
| HCA Information: | Failed |

| 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, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target loaddll64.exe, PID 3648 because there are no executed function
- Not all processes where analyzed, report is missing behavior information

## 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) x86-64 (stripped to external PDB), for MS Windows |
|---|---|
| Entropy (8bit): | 7.250454733634642 |
| TrID: | • Win64 Dynamic Link Library (generic) (102004/3) 86.41%<br>• Win64 Executable (generic) (12005/4) 10.17%<br>• Generic Win/DOS Executable (2004/3) 1.70%<br>• DOS Executable Generic (2002/1) 1.70%<br>• VXD Driver (31/22) 0.03% |
| File name: | 8082-x64.dll.dll |
| File size: | 287744 |

| | |
|---|---|
| MD5: | 43616639411a590f022505998a6f567e |
| SHA1: | 416932059dc3488000b171beeac258fc792d4c71 |
| SHA256: | 6a289f491c8d5d789e31e89c73ba06ef6fc075458a1106b7213b29da798f6c03 |
| SHA512: | 9989fc8ee3a07db0a9f9a98395e75178507f20e9189f15c9b9dc51f55efe23c324388edc0032ded78db392f69ae9560505a979e165661a0fe46ca7c73c41139a |
| SSDEEP: | 6144:49TczeYIVeH21LD3rMPwjEMSUEufxTUhYohcnxK7xERM5jy45yrjz:weAP3QPKEeEuShYohcnx+xEsUT |
| TLSH: | 9954ADC0D6EEE60CEA36C5B72B9762679030F344FAD62BB124660B0696D647DD0D027F |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....^....."..... ...`.....k..... ..... |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x6bac13f0 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x6bac0000 |
| Subsystem: | windows cui |
| Image File Characteristics: | EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, DLL |
| DLL Characteristics: | |
| Time Stamp: | 0x5EDED517 [Tue Jun 9 00:17:27 2020 UTC] |
| TLS Callbacks: | 0x6bac1910 |
| 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: | f73cb1b8999c7e79c50459b8e1f144f0 |

## Entrypoint Preview

| Instruction |
|---|
| dec eax |
| sub esp, 48h |
| mov dword ptr [00047C22h], 00000000h |
| cmp edx, 01h |
| je 00007FE0409C534Fh |
| dec eax |
| add esp, 48h |
| jmp 00007FE0409C51C9h |
| nop dword ptr [eax+00h] |
| mov dword ptr [esp+30h], edx |
| dec eax |
| mov dword ptr [esp+38h], ecx |
| dec esp |
| mov dword ptr [esp+28h], eax |
| call 00007FE0409C5F62h |
| call 00007FE0409C62CDh |
| dec esp |
| mov eax, dword ptr [esp+28h] |
| dec eax |
| mov ecx, dword ptr [esp+38h] |
| mov edx, dword ptr [esp+30h] |
| dec eax |

| Instruction |
|---|
| add esp, 48h |
| jmp 00007FE0409C5196h |
| nop |
| push ebp |
| push edi |
| push esi |
| push ebx |
| dec eax |
| sub esp, 58h |
| inc ebp |
| xor eax, eax |
| inc ecx |
| mov ecx, 00000001h |
| dec eax |
| mov edi, ecx |
| mov esi, edx |
| mov dword ptr [esp+4Ch], 00000000h |
| dec eax |
| mov dword ptr [esp+38h], 00000000h |
| mov dword ptr [esp+30h], 00000000h |
| mov edx, 00000002h |
| mov dword ptr [esp+28h], 00000000h |
| mov dword ptr [esp+20h], 00000000h |
| dec eax |
| lea ecx, dword ptr [00048475h] |
| call dword ptr [00049D6Bh] |
| dec eax |
| mov ebx, eax |
| dec eax |
| lea eax, dword ptr [eax-01h] |
| dec eax |
| cmp eax, FFFFFFFDh |
| jnbe 00007FE0409C5390h |
| xor edx, edx |
| dec eax |
| mov ecx, ebx |
| call dword ptr [00049D43h] |
| test eax, eax |
| dec eax |
| mov ebp, dword ptr [00049E32h] |
| jne 00007FE0409C536Ch |
| jmp 00007FE0409C5378h |
| dec eax |

**Data Directories**

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x4a000 | 0xb0 | .edata |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x4b000 | 0x7bc | .idata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x47000 | 0x27c | .pdata |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x4e000 | 0x2c4 | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x4d000 | 0x28 | .tls |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x4b1e4 | 0x1a8 | .idata |

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| 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 | 0x1f10 | 0x2000 | False | 0.5732421875 | data | 6.021842385150596 | 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 |
| .data | 0x3000 | 0x42470 | 0x42600 | False | 0.5997381120527306 | data | 7.257802920028994 | 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_READ, IMAGE_SCN_MEM_WRITE |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .rdata | 0x46000 | 0x170 | 0x200 | False | 0.416015625 | data | 3.5502048501802737 | 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_READ |
| .pdata | 0x47000 | 0x27c | 0x400 | False | 0.3515625 | data | 2.9537206983747 | 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 |
| .xdata | 0x48000 | 0x200 | 0x200 | False | 0.380859375 | locale data table | 3.772885986330123 | 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 |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .bss | 0x49000 | 0x990 | 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 |
| .edata | 0x4a000 | 0xb0 | 0x200 | False | 0.271484375 | data | 1.9824304709536775 | 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 | 0x4b000 | 0x7bc | 0x800 | False | 0.357421875 | data | 4.239308826637131 | 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 |
|---|---|---|---|---|---|---|---|---|
| .CRT | 0x4c000 | 0x58 | 0x200 | False | 0.0546875 | data | 0.20153937813451883 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .tls | 0x4d000 | 0x48 | 0x200 | False | 0.0546875 | data | 0.29046607431271465 | IMAGE_SCN_CNT_INITIALIZED_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 |
| .reloc | 0x4e000 | 0x2c4 | 0x400 | False | 0.626953125 | GLS_BINARY_LSB_FIRST | 4.699885638394994 | 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, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetProcAddress, GetSystemTimeAsFileTime, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, LoadLibraryW, QueryPerformanceCounter, ReadFile, RtlAddFunctionTable, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualAlloc, VirtualProtect, VirtualQuery, WriteFile |

| DLL | Import |
|---|---|
| msvcrt.dll | __dllonexit, __iob_func, _amsg_exit, _initterm, _lock, _onexit, _unlock, abort, calloc, free, fwrite, malloc, memcpy, signal, sprintf, strlen, strncmp, vfprintf |

**Exports**

| Name | Ordinal | Address |
|---|---|---|
| DllGetClassObject | 1 | 0x6bac170b |
| DllMain | 2 | 0x6bac16c7 |
| DllRegisterServer | 3 | 0x6bac1705 |
| DllUnregisterServer | 4 | 0x6bac1708 |
| StartW | 5 | 0x6bac1714 |

# Network Behavior

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 8, 2023 16:10:04.046937943 CET | 49699 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:04.161695004 CET | 8082 | 49699 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:04.162079096 CET | 49699 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:04.162940025 CET | 49699 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:04.276777983 CET | 8082 | 49699 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:04.281196117 CET | 8082 | 49699 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:04.281222105 CET | 8082 | 49699 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:04.281239986 CET | 8082 | 49699 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:04.281378031 CET | 49699 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:04.292589903 CET | 49699 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:04.406682968 CET | 8082 | 49699 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:36.778028965 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:36.892846107 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:36.893060923 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:36.902221918 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.016406059 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028742075 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028786898 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028812885 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028836012 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028846979 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.028861046 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028884888 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.028887033 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028913021 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028928995 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.028937101 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028956890 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.028974056 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.029061079 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143208981 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143250942 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143270016 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143287897 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143311977 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143332958 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143352032 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143369913 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143368959 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143389940 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143409967 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |

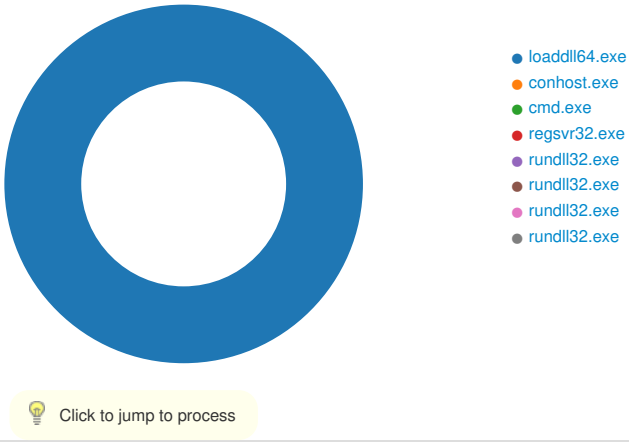
| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Jan 8, 2023 16:10:37.143428087 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143429041 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143450975 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143457890 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143475056 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143486023 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143493891 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143513918 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143521070 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143532991 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143560886 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143603086 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143801928 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143826008 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143846035 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143852949 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143867970 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.143888950 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.143919945 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257618904 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257693052 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257721901 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257751942 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257778883 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257806063 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257811069 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257833958 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257854939 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257863045 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257879972 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257893085 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257903099 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257914066 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257924080 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257937908 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257952929 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.257982016 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.257982016 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258012056 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258012056 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258038044 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258038998 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258059978 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258065939 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258094072 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258094072 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258122921 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258126974 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258152008 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258162975 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258178949 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258200884 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258204937 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258210897 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258219957 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258234024 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258249998 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |
| Jan 8, 2023 16:10:37.258263111 CET | 8082 | 49700 | 20.104.209.69 | 192.168.2.5 |
| Jan 8, 2023 16:10:37.258279085 CET | 49700 | 8082 | 192.168.2.5 | 20.104.209.69 |

## HTTP Request Dependency Graph

- https:
  - 20.104.209.69:8082

# Statistics

## Behavior




# System Behavior

## Analysis Process: loaddll64.exe PID: **3648**, Parent PID: **3324**

### General

| | |
|---|---|
| Target ID: | 0 |
| Start time: | 16:09:52 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\loaddll64.exe |
| Wow64 process (32bit): | false |
| Commandline: | loaddll64.exe "C:\Users\user\Desktop\8082-x64.dll.dll" |
| Imagebase: | 0x7ff6c0910000 |
| File size: | 139776 bytes |
| MD5 hash: | C676FC0263EDD17D4CE7D644B8F3FCD6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: SUSP_PS1_FromBase64String_Content_Indicator, Description: Detects suspicious base64 encoded PowerShell expressions, Source: 00000000.00000002.579279943.00000267603C6000.00000004.00000001.00020000.00000000.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: 00000000.00000002.579279943.00000267603C6000.00000004.00000001.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: CobaltStrike_Sleeve_BeaconLoader_VA_x64_o_v4_3_v4_4_v4_5_and_v4_6, Description: Cobalt Strike\'s sleeve/BeaconLoader.VA.x64.o (VirtualAlloc) Versions 4.3 through at least 4.6, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: gssincla@google.com<br>• Rule: Cobaltbaltstrike_Beacon_x64, Description: Detects CobaltStrike payloads, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team<br>• Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net<br>• Rule: CobaltStrike_MZ_Launcher, Description: Detects CobaltStrike MZ header ReflectiveLoader launcher, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.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: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CobaltStrike_4, Description: Yara detected CobaltStrike, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security<br>• Rule: Windows_Trojan_CobaltStrike_f0b627fc, Description: Rule for beacon reflective loader, Source: 00000000.00000003.323615011.0000026760590000.00000020.00001000.00020000.00000000.sdmp, Author: unknown |
| Reputation: | high |

**File Activities**

## Analysis Process: conhost.exe PID: **2884**, Parent PID: **3648**

### General

| | |
|---|---|
| Target ID: | 1 |
| Start time: | 16:09:52 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7fcd70000 |
| 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: **6104**, Parent PID: **3648**

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 16:09:53 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\8082-x64.dll.dll",#1 |
| Imagebase: | 0x7ff627730000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| 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: **3480**, Parent PID: **3648**

| General | |
|---|---|
| Target ID: | 3 |
| Start time: | 16:09:53 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | regsvr32.exe /s C:\Users\user\Desktop\8082-x64.dll.dll |
| Imagebase: | 0x7ff7ffce0000 |
| File size: | 24064 bytes |
| MD5 hash: | D78B75FC68247E8A63ACBA846182740E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **4848**, Parent PID: **6104**

| General | |
|---|---|
| Target ID: | 4 |
| Start time: | 16:09:53 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\8082-x64.dll.dll",#1 |
| Imagebase: | 0x7ff7a6a20000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **1304**, Parent PID: **3648**

| General | |
|---|---|
| Target ID: | 5 |
| Start time: | 16:09:53 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllGetClassObject |
| Imagebase: | 0x7ff7a6a20000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **1004**, Parent PID: **3648**

| General | |
|---|---|
| Target ID: | 6 |
| Start time: | 16:09:56 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllMain |
| Imagebase: | 0x7ff7a6a20000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **4532**, Parent PID: **3648**

| General | |
|---|---|
| Target ID: | 7 |
| Start time: | 16:09:59 |
| Start date: | 08/01/2023 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe C:\Users\user\Desktop\8082-x64.dll.dll,DllRegisterServer |
| Imagebase: | 0x7ff7a6a20000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Disassembly

**No disassembly**