

JoeSandbox Cloud BASIC



ID: 483265

Sample Name: CI and PL of
CMZBD-210090.exe

Cookbook: default.jbs

Time: 18:28:11

Date: 14/09/2021

Version: 33.0.0 White Diamond




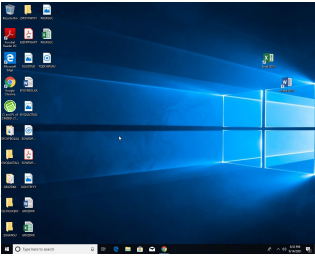
Table of Contents

| | |
|---|----|
| Table of Contents | 2 |
| Windows Analysis Report CI and PL of CMZBD-210090.exe | 3 |
| Overview | 3 |
| General Information | 3 |
| Detection | 3 |
| Signatures | 3 |
| Classification | 3 |
| Process Tree | 3 |
| Malware Configuration | 3 |
| Threatname: GuLoader | 3 |
| Yara Overview | 3 |
| Memory Dumps | 3 |
| Sigma Overview | 3 |
| Jbx Signature Overview | 3 |
| AV Detection: | 4 |
| Networking: | 4 |
| Data Obfuscation: | 4 |
| Anti Debugging: | 4 |
| Mitre Att&ck Matrix | 4 |
| Behavior Graph | 4 |
| Screenshots | 5 |
| Thumbnails | 5 |
| Antivirus, Machine Learning and Genetic Malware Detection | 6 |
| Initial Sample | 6 |
| Dropped Files | 6 |
| Unpacked PE Files | 6 |
| Domains | 6 |
| URLs | 6 |
| Domains and IPs | 7 |
| Contacted Domains | 7 |
| Contacted IPs | 7 |
| General Information | 7 |
| Simulations | 7 |
| Behavior and APIs | 7 |
| Joe Sandbox View / Context | 8 |
| IPs | 8 |
| Domains | 8 |
| ASN | 8 |
| JA3 Fingerprints | 8 |
| Dropped Files | 8 |
| Created / dropped Files | 8 |
| Static File Info | 8 |
| General | 8 |
| File Icon | 8 |
| Static PE Info | 8 |
| General | 9 |
| Entrypoint Preview | 9 |
| Data Directories | 9 |
| Sections | 9 |
| Resources | 9 |
| Imports | 9 |
| Version Infos | 9 |
| Possible Origin | 9 |
| Network Behavior | 9 |
| Code Manipulations | 9 |
| Statistics | 9 |
| System Behavior | 10 |
| Analysis Process: CI and PL of CMZBD-210090.exe PID: 5472 Parent PID: 764 | 10 |
| General | 10 |
| File Activities | 10 |
| Disassembly | 10 |
| Code Analysis | 10 |

Windows Analysis Report CI and PL of CMZBD-210090.e...

Overview

General Information

| | |
|---|--|
| Sample Name: | CI and PL of CMZBD-210090.exe |
| Analysis ID: | 483265 |
| MD5: | 1f9b03378d7dc85. |
| SHA1: | 670bf2c5dbc7f6f... |
| SHA256: | ce8385347104cf1.. |
| Tags: | <div>exe</div> <div>guloader</div> |
| Infos: | <div>  </div> |
| Most interesting Screenshot: | |
|  | |

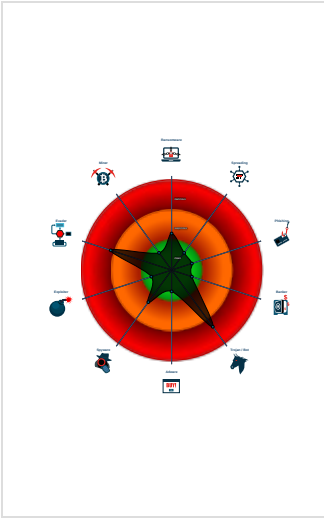
Detection

| | |
|--|---------|
| <div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div> | |
| <div>GuLoader</div> | |
| Score: | 76 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |


Signatures

| |
|--|
| Found malware configuration |
| Multi AV Scanner detection for subm... |
| Yara detected GuLoader |
| C2 URLs / IPs found in malware con... |
| Found potential dummy code loops (...) |
| Machine Learning detection for samp... |
| Creates a DirectInput object (often fo... |
| Uses 32bit PE files |
| Antivirus or Machine Learning detec... |
| Sample file is different than original ... |
| PE file contains strange resources |
| Contains functionality to read the PEB |

Classification



Process Tree

| |
|--|
| ▪ System is w10x64 |
| •  CI and PL of CMZBD-210090.exe (PID: 5472 cmdline: 'C:\Users\user\Desktop\CI and PL of CMZBD-210090.exe' MD5: 1F9B03378D7DC859A1C6E13A5832582E) |
| ▪ cleanup |

Malware Configuration

Threatname: GuLoader

| |
|---|
| <pre>{ "Payload URL": "https://drive.google.com/uc?export=downlo" }</pre> |
|---|

Yara Overview

Memory Dumps

| Source | Rule | Description | Author | Strings |
|--|------------------------|------------------------|--------------|---------|
| 00000000.00000002.753956643.000000000022C 0000.00000040.00000001.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

Data Obfuscation:



Yara detected GuLoader

Anti Debugging:

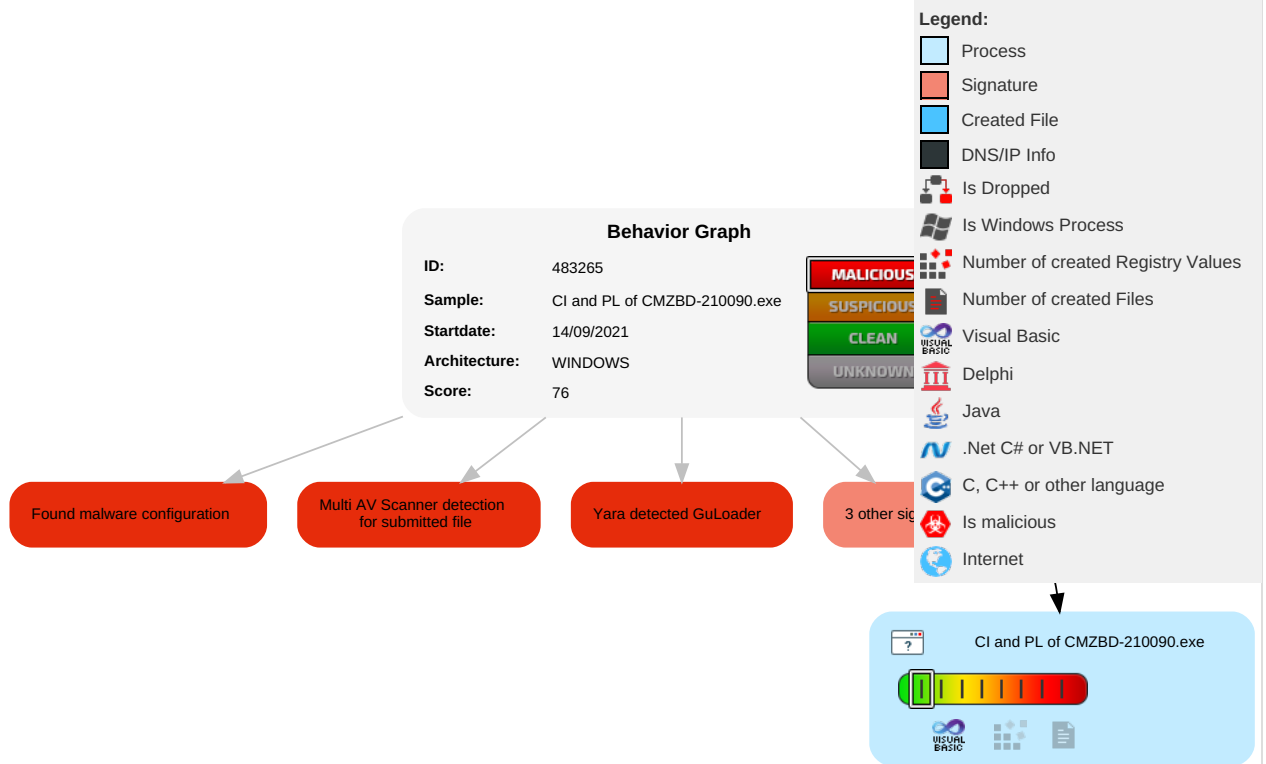


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Recovery |
|------------------|------------------------------------|--------------------------------------|--------------------------------------|------------------------------------|--------------------------|------------------------------------|------------------------------------|--------------------------------|--|------------------------------|---|----------|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Virtualization/Sandbox Evasion 1 1 | Input Capture 1 | Security Software Discovery 1 1 | Remote Services | Input Capture 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | Recovery |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Software Packing 1 | LSASS Memory | Virtualization/Sandbox Evasion 1 1 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Application Layer Protocol 1 | Exploit SS7 to Redirect Phone Calls/SMS | Recovery |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 | Security Account Manager | Process Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Recovery |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 1 | NTDS | System Information Discovery 1 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | Recovery |

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 |
|-------------------------------|-----------|----------------|-------------------|------|
| CI and PL of CMZBD-210090.exe | 18% | ReversingLabs | Win32.Trojan.Mucc | |
| CI and PL of CMZBD-210090.exe | 100% | Joe Sandbox ML | | |

Dropped Files

No Antivirus matches

Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|-----------|---------|-------------------|------|-------------------------------|
| 0.0.CI and PL of CMZBD-210090.exe.400000.0.unpack | 100% | Avira | TR/Dropper.VB.Gen | | Download File |
| 0.2.CI and PL of CMZBD-210090.exe.400000.0.unpack | 100% | Avira | TR/Dropper.VB.Gen | | Download File |

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

| | |
|--|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 483265 |
| Start date: | 14.09.2021 |
| Start time: | 18:28:11 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 1s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | CI and PL of CMZBD-210090.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 31 |
| 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: | <ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal76.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | <ul style="list-style-type: none">• Successful, ratio: 24.3% (good quality ratio 11.5%)• Quality average: 26.6%• Quality standard deviation: 33.9% |
| HCA Information: | Failed |
| Cookbook Comments: | <ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe• Override analysis time to 240s for sample files taking high CPU consumption |
| Warnings: | Show All |

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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 (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 5.999486188270087 |
| TrID: | <ul style="list-style-type: none">Win32 Executable (generic) a (10002005/4) 99.15%Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%Generic Win/DOS Executable (2004/3) 0.02%DOS Executable Generic (2002/1) 0.02%Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | CI and PL of CMZBD-210090.exe |
| File size: | 126976 |
| MD5: | 1f9b03378d7dc859a1c6e13a5832582e |
| SHA1: | 670bf2c5dbc7f6f8d9d1ec4b8d6c527a5eefdb8b |
| SHA256: | ce8385347104cf190b23811bb67ba8edac9186073d6953ca23720f1e92af7eb3 |
| SHA512: | 40b070c01703ae37541b1b6d079144771bc0db0284ebbc45f715889b6b5a959f4f2bad5b3e38c882e95240f55249b0e332b7e318b3c450743c15b7b66f5403df |
| SSDEEP: | 1536:bW30on+jXsoPTna24R4xoT12l41yJEmxJjQ1CkZri k3QKRv93snKLH:lbrwGxeX+sEPCUek3QKRFI |
| File Content Preview: | MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......i...i... i...d...i.Rich..i.....PE..L....wX.....@..... |

File Icon

| | |
|---|------------------|
|  | |
| Icon Hash: | eca24dd23ca5cce8 |

Static PE Info

| | |
|-----------------------------|---|
| General | |
| Entrypoint: | 0x401114 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | |
| Time Stamp: | 0x5877ECB2 [Thu Jan 12 20:53:06 2017 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: | 82687acae94d2aed1f61dd47940dabd7 |

Entrypoint Preview

Data Directories

Sections


| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|-------|-----------------|--------------|----------|----------|-----------------|-----------|---------------|---|
| .text | 0x1000 | 0x17d0c | 0x18000 | False | 0.522064208984 | data | 6.30520790061 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x19000 | 0x1938 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x1b000 | 0x5a4c | 0x6000 | False | 0.357218424479 | data | 5.10422339689 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: CI and PL of CMZBD-210090.exe PID: 5472 Parent PID: 764

General

| | |
|-------------------------------|--|
| Start time: | 18:29:02 |
| Start date: | 14/09/2021 |
| Path: | C:\Users\user\Desktop\CI and PL of CMZBD-210090.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\CI and PL of CMZBD-210090.exe' |
| Imagebase: | 0x400000 |
| File size: | 126976 bytes |
| MD5 hash: | 1F9B03378D7DC859A1C6E13A5832582E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | <ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.753956643.00000000022C0000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

File Activities

Show Windows behavior

Disassembly

Code Analysis