
**ID:** 530857
**Sample Name:** CI_PL_BL_
4100675407_xls.exe
**Cookbook:** default.jbs
**Time:** 03:38:04
**Date:** 30/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents



Copyright Joe Security LLC 2021

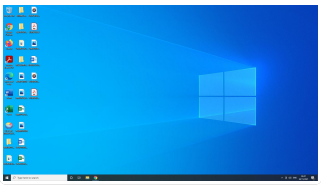
# Windows Analysis Report CI_PL_BL_ 4100675407_xls.e…

## Overview

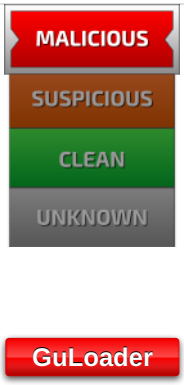
### General Information

| | |
|---|---|
| Sample Name: | CI_PL_BL_ 4100675407_xls.exe |
| Analysis ID: | 530857 |
| MD5: | 94cb19d0951996.. |
| SHA1: | fa319fb54dfb0b1… |
| SHA256: | 4ff14d83a926458.. |
| Infos: | |

Most interesting Screenshot:



### Detection



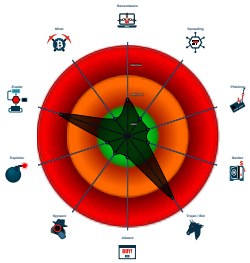

GuLoader

| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Tries to load missing DLLs

### Classification



## Process Tree

- **System is w10x64native**
- CI_PL_BL_ 4100675407_xls.exe (PID: 5884 cmdline: "C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe" MD5: 94CB19D0951996CDB8B4CB914248763E)
  - CI_PL_BL_ 4100675407_xls.exe (PID: 2904 cmdline: "C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe" MD5: 94CB19D0951996CDB8B4CB914248763E)
- **cleanup**

## Malware Configuration

### Threatname: GuLoader


```
{
  "Payload URL": "https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bin"
}
```


## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000002.00000002.410581088153.000000000 2510000.00000040.00000001.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |
| 00000009.00000000.410577418495.000000000 0560000.00000040.00000001.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

Copyright Joe Security LLC 2021

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

**Found malware configuration**

**Multi AV Scanner detection for submitted file**

## Networking:

**C2 URLs / IPs found in malware configuration**

## Data Obfuscation:

**Yara detected GuLoader**

## Malware Analysis System Evasion:

**Tries to detect Any.run**

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

## Anti Debugging:

**Hides threads from debuggers**

## Stealing of Sensitive Information:

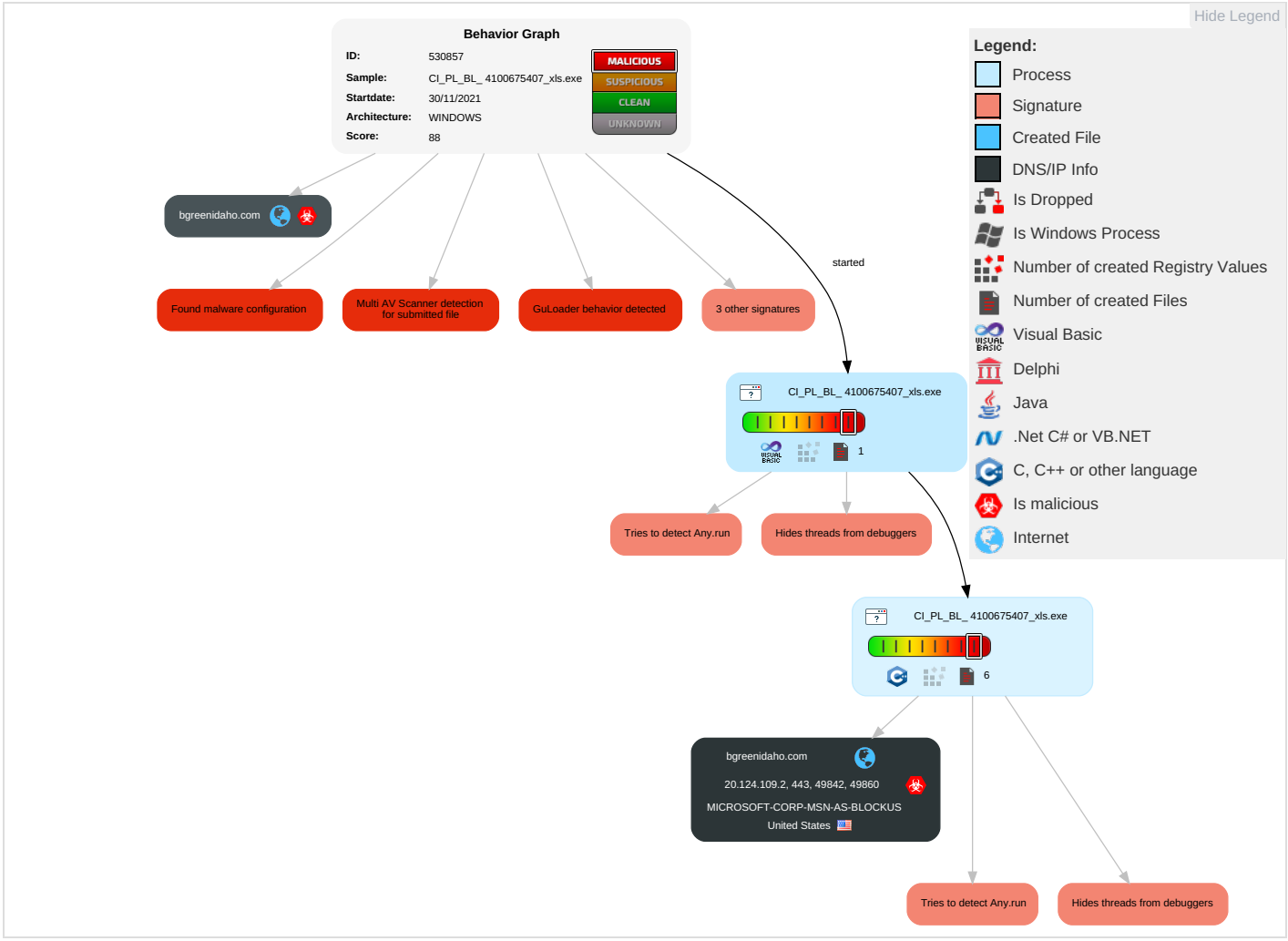
**GuLoader behavior detected**

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | DLL Side-Loading 1 | Process Injection 1 2 | Virtualization/Sandbox Evasion 2 1 | OS Credential Dumping | Security Software Discovery 3 1 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 2 | Eavesdrop on Insecure Network Communication |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | DLL Side-Loading 1 | Process Injection 1 2 | LSASS Memory | Virtualization/Sandbox Evasion 2 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Application Layer Protocol 1 | Exploit SS7 to Redirect Phone Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | DLL Side-Loading 1 | Security Account Manager | Process Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Application Layer Protocol 1 2 | Exploit SS7 to Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 1 | NTDS | System Information Discovery 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap |

# Behavior Graph

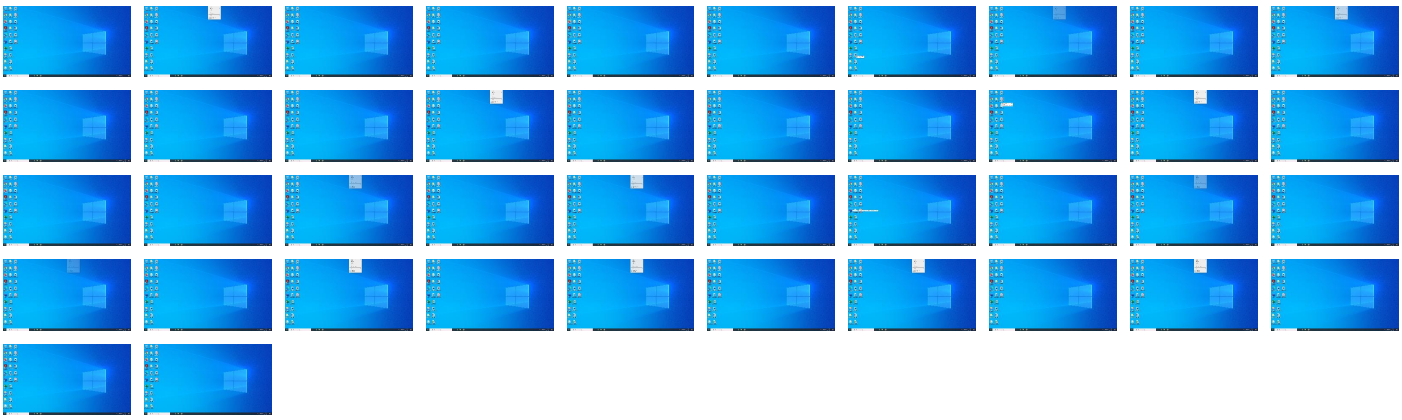
Copyright Joe Security LLC 2021

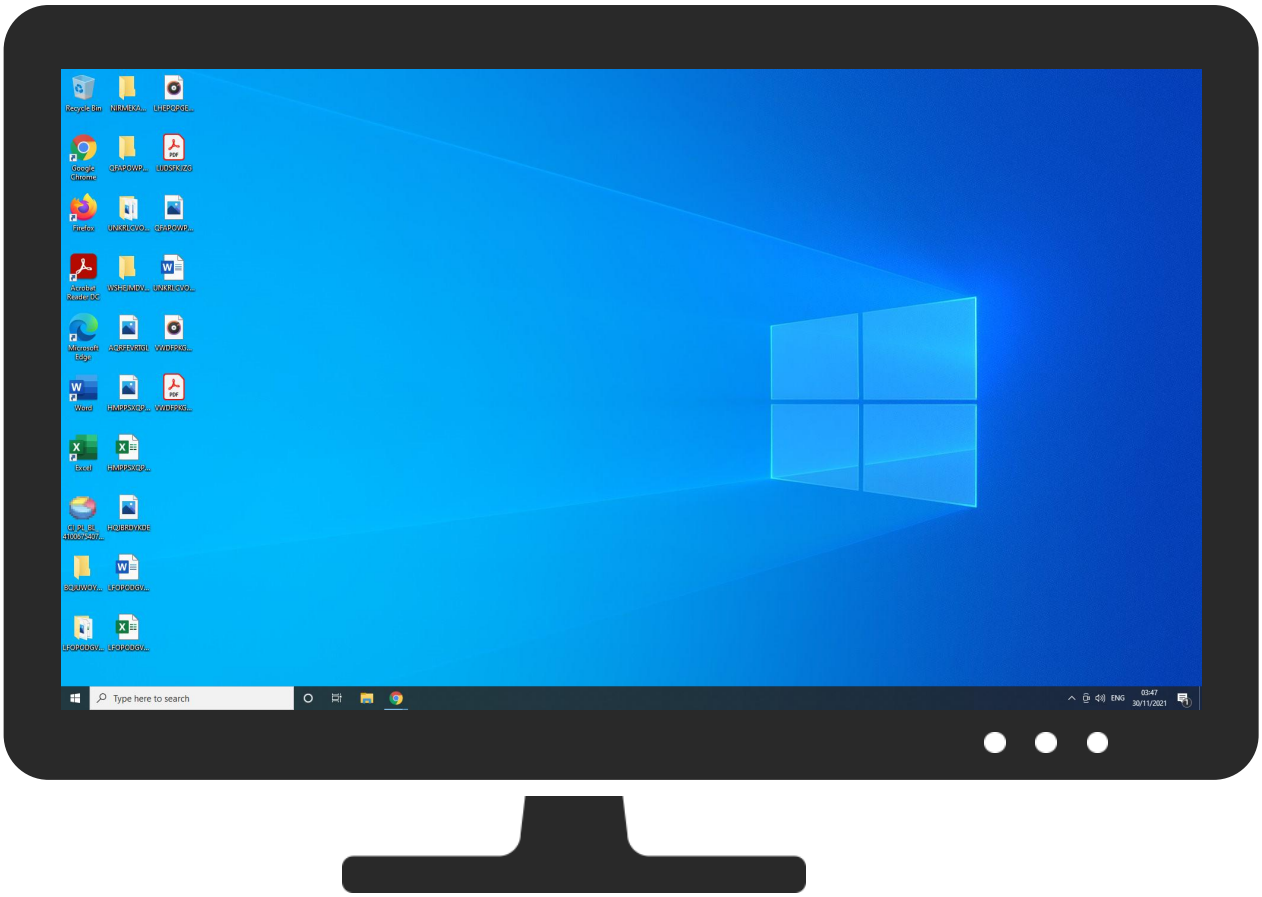



## Screenshots

### 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_PL_BL_ 4100675407_xls.exe | 36% | ReversingLabs | Win32.Trojan.Shelsy | |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

**No Antivirus matches**

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| bgreenidaho.com | 0% | Virustotal | | Browse |

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.binF | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/R | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/ocal | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/v | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/3 | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bin# | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZY6 | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.binws | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.binLMEMH | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/ | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bins | 0% | Avira URL Cloud | safe | |

Copyright Joe Security LLC 2021

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://bgreenidaho.com/Hostbgre | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.binn | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/1e03818b-e8b8-45f4-bd74-707e0f15a35d | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bindvmbusRFCOMM | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/g | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/8-45f4-bd74-707e0f15a35d0 | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.binJ | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/N | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/- | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bin | 0% | Avira URL Cloud | safe | |
| http://https://bgreenidaho.com/nidaho.com/: | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| bgreenidaho.com | 20.124.109.2 | true | true | • 0%, Virustotal, Browse | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bin | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 20.124.109.2 | bgreenidaho.com | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 530857 |
| Start date: | 30.11.2021 |
| Start time: | 03:38:04 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 12m 6s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | CI_PL_BL_ 4100675407_xls.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301 |
| Run name: | Suspected Instruction Hammering |
| Number of analysed new started processes analysed: | 20 |
| 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 |

Copyright Joe Security LLC 2021

| | |
|---|---|
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal88.troj.evad.winEXE@3/1@1/1 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 66%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 20.124.109.2 | BL_CI_PL.exe | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| bgreenidaho.com | BL_CI_PL.exe | Get hash | malicious | Browse | • 20.124.109.2 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| MICROSOFT-CORP-MSN-AS-BLOCKUS | Updated Proposal and Statements.docx | Get hash | malicious | Browse | • 52.109.8.20 |
| | t6rrqsi3Bp | Get hash | malicious | Browse | • 20.50.41.254 |
| | iapc1nXqL0.exe | Get hash | malicious | Browse | • 52.101.24.0 |
| | t2yFh0lOxM.exe | Get hash | malicious | Browse | • 52.101.24.0 |
| | 9hyE41yNDB | Get hash | malicious | Browse | • 40.105.241.198 |
| | D403yCH5gh | Get hash | malicious | Browse | • 20.187.1.20 |
| | UkuCbysP6T | Get hash | malicious | Browse | • 13.64.146.115 |
| | 7OoLG7JkFC | Get hash | malicious | Browse | • 40.111.155.152 |
| | BL_CI_PL.exe | Get hash | malicious | Browse | • 20.124.109.2 |
| | BL_CI_PL.exe | Get hash | malicious | Browse | • 52.109.88.174 |
| | d2REPCiUoq | Get hash | malicious | Browse | • 22.129.233.98 |
| | zsnJiVlhgN.exe | Get hash | malicious | Browse | • 20.68.110.75 |
| | 7JflEyuQmz | Get hash | malicious | Browse | • 52.155.149.221 |
| | m269vSilnu | Get hash | malicious | Browse | • 52.125.142.71 |
| | NkvaVLGroW | Get hash | malicious | Browse | • 40.113.32.125 |
| | MA4UA3e5xe | Get hash | malicious | Browse | • 52.96.135.139 |
| | n6sOKP0EjJ | Get hash | malicious | Browse | • 143.64.39.221 |
| | 3kzcNn1JUr | Get hash | malicious | Browse | • 13.78.147.147 |
| | p4o9OIbPjx | Get hash | malicious | Browse | • 20.136.249.210 |
| | 81RFAzyp8n | Get hash | malicious | Browse | • 20.110.162.9 |

Copyright Joe Security LLC 2021

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Temp\~DF3A963BF3568977ED.TMP | |
|---|---|
| Process: | C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe |
| File Type: | Composite Document File V2 Document, Cannot read section info |
| Category: | dropped |
| Size (bytes): | 16384 |
| Entropy (8bit): | 0.8889429216618719 |
| Encrypted: | false |
| SSDEEP: | 12:rl3lKFQCb77aqWPp8aFW3gJH6OXkDgIOJefKadcMqpwbmHZbGzJzzz/jP5prGI:rQYH6OCgLAMibm5bGzJzX/ |
| MD5: | E114AD50630A185807BCDFF5F7DACEF6 |
| SHA1: | 5091C562986C0A729FF4AC836083EFFBB4257977 |
| SHA-256: | 8C0B8DE53510102223758C6543D9EB102BC7423B83BDF902975FB221AB77E945 |
| SHA-512: | F8C4FA0ABA5BD5CE8246A9C2A0A525129B5461E90634FE406A1704F8E42240174C6D1D8CCBC42EBE14EE777F79A5C7E32618CC2ED532CA6264D614337840BF1<br>A |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....>.....<br>.....<br>.....<br>..... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 6.045005360835647 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.15%<br>• Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | CI_PL_BL_ 4100675407_xls.exe |
| File size: | 143360 |
| MD5: | 94cb19d0951996cdb8b4cb914248763e |
| SHA1: | fa319fb54dfb0b1f715a19924087cacef22ccbcf |
| SHA256: | 4ff14d83a926458439f039ea2e756a646b2bb63be4fd22ed8559138214efcaf8 |
| SHA512: | b06b3df9de83932c9f5013ce90720710ba9645c5bcce4b46dd377c541343b8095742a7923634805a61214ba1eda4ac3ecaaee935b73942c53c27190e792dc007 |
| SSDEEP: | 1536:5oDAE4euYT88tnh07k177v10aeb/by8W1hgW3rAITGLKy:ZEvuYT8CQm/v10aeixxCKy |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L.....G.....0.....@ |

## File Icon

| | |
|---|---|
| Icon Hash: | 28f0da9af0f0f034 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4016a4 |
| 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: | 0x47BEE20B [Fri Feb 22 14:54:03 2008 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: | 9b824bd6da8a9367fa6d96e7ab5dc79d |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x1f7cc | 0x20000 | False | 0.547492980957 | data | 6.30287654494 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x21000 | 0x19ec | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x23000 | 0xf3e | 0x1000 | False | 0.27490234375 | data | 3.55639650835 | 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

### Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Nov 30, 2021 03:41:23.455224991 CET | 192.168.11.20 | 1.1.1.1 | 0x8ea5 | Standard query (0) | bgreenidaho.com | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Nov 30, 2021 03:41:23.613805056 CET | 1.1.1.1 | 192.168.11.20 | 0x8ea5 | No error (0) | bgreenidaho.com | | 20.124.109.2 | A (IP address) | IN (0x0001) |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: CI_PL_BL_ 4100675407_xls.exe PID: 5884 Parent PID: 5484

#### General

| | |
|---|---|
| Start time: | 03:39:55 |
| Start date: | 30/11/2021 |
| Path: | C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe" |
| Imagebase: | 0x400000 |
| File size: | 143360 bytes |
| MD5 hash: | 94CB19D0951996CDB8B4CB914248763E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.410581088153.0000000002510000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

#### File Activities

Show Windows behavior

### Analysis Process: CI_PL_BL_ 4100675407_xls.exe PID: 2904 Parent PID: 5884

#### General

| | |
|---|---|
| Start time: | 03:40:39 |
| Start date: | 30/11/2021 |
| Path: | C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe |
| Wow64 process (32bit): | true |

| | |
|---|---|
| Commandline: | "C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe" |
| Imagebase: | 0x400000 |
| File size: | 143360 bytes |
| MD5 hash: | 94CB19D0951996CDB8B4CB914248763E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000000.410577418495.0000000000560000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

# Disassembly

## Code Analysis

Copyright Joe Security LLC


Copyright Joe Security LLC 2021