


**ID:** 395203
**Sample Name:** udmugning.exe
**Cookbook:** default.jbs
**Time:** 09:55:58
**Date:** 22/04/2021
**Version:** 31.0.0 Emerald

# Table of Contents

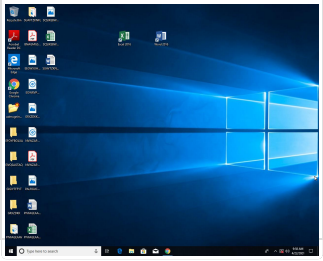
# Analysis Report udmugning.exe

## Overview

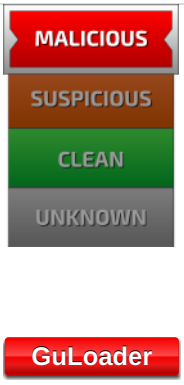
### General Information

| | |
|---|---|
| Sample Name: | udmugning.exe |
| Analysis ID: | 395203 |
| MD5: | 3d04ed12388c92.. |
| SHA1: | 8820ff07e1f6012… |
| SHA256: | 99227f9bb099737. |
| Infos: | |

Most interesting Screenshot:



### Detection

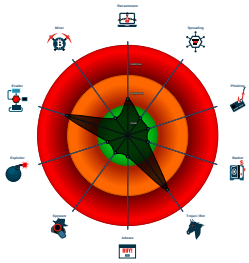



| | |
|---|---|
| Score: | 72 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Icon mismatch, binary includes an ic…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Detected potential crypto function
- Found a high number of Window / Us…
- PE file contains an invalid checksum
- PE file contains strange resources
- Program does not show much activi…
- Sample execution stops while proce…
- Sample file is different than original …

### Classification



## Startup

- **System is w10x64**
- udmugning.exe (PID: 3440 cmdline: 'C:\Users\user\Desktop\udmugning.exe' MD5: 3D04ED12388C92E15361681EF1921D7F)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| udmugning.exe | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000001.00000002.474162328.000000000401000.00000020.00020000.sdmp | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |
| 00000001.00000000.206225191.000000000401000.00000020.00020000.sdmp | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

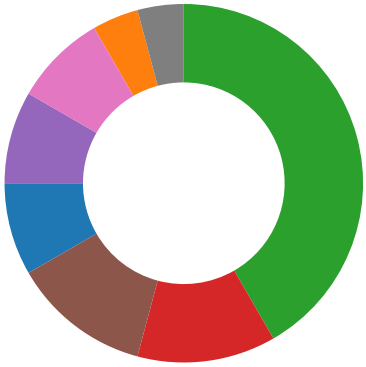
### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 1.0.udmugning.exe.400000.0.unpack | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |
| 1.2.udmugning.exe.400000.0.unpack | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview



- AV Detection
- Compliance
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

### AV Detection:

**Multi AV Scanner detection for submitted file**

**Machine Learning detection for sample**

### Data Obfuscation:

**Yara detected GuLoader**

### Hooking and other Techniques for Hiding and Protection:

**Icon mismatch, binary includes an icon from a different legit application in order to fool users**

### Anti Debugging:

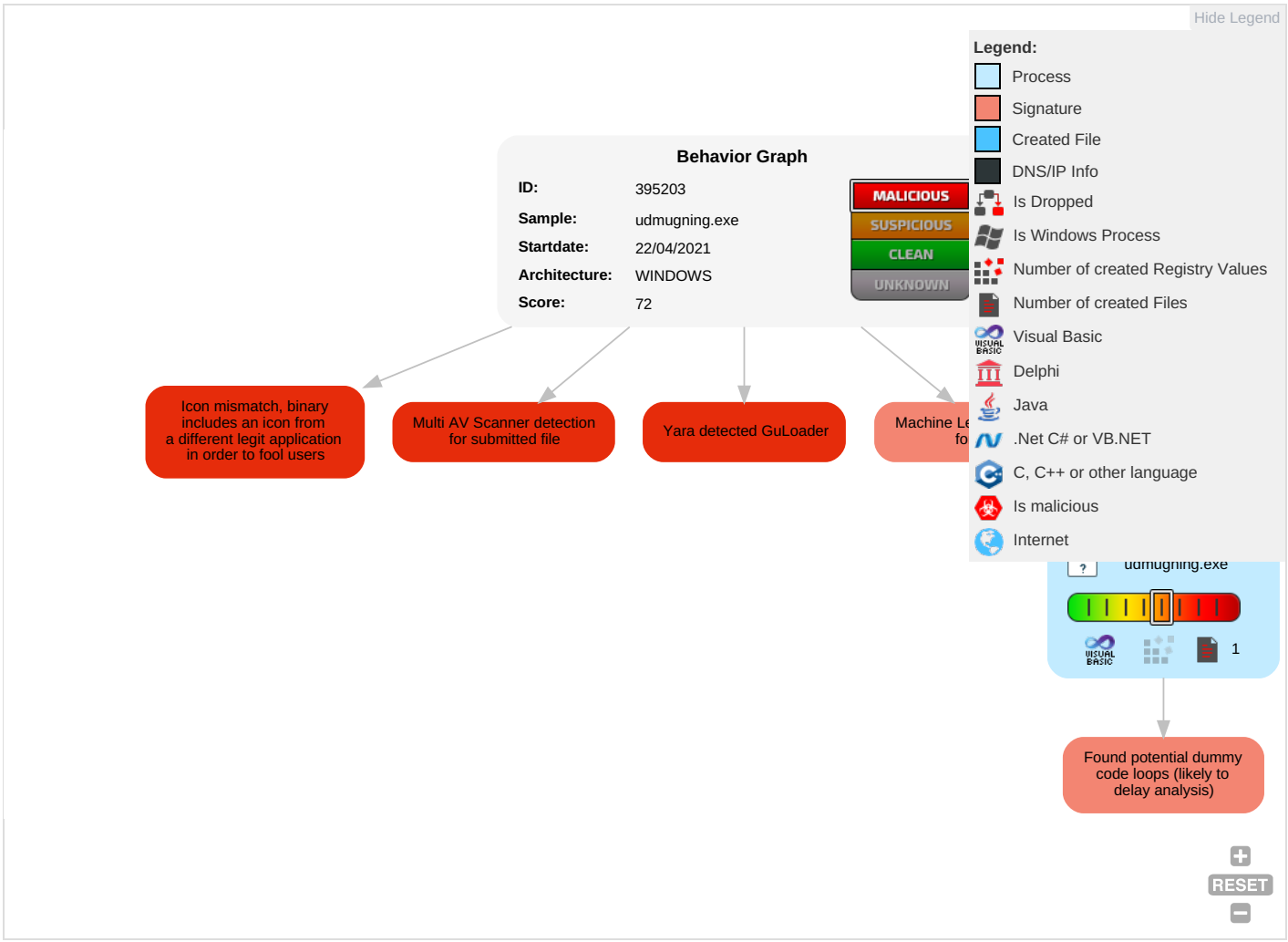
**Found potential dummy code loops (likely to delay analysis)**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | R S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Masquerading 1 | OS Credential Dumping | Security Software Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | R T W A |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 1 1 | LSASS Memory | Virtualization/Sandbox Evasion 1 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | R W W A |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | R S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | O D C B |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Obfuscated Files or Information 1 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Software Packing | LSA Secrets | System Information Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | |

## 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 |
|---|---|---|---|---|
| udmugning.exe | 35% | Metadefender | | Browse |
| udmugning.exe | 79% | ReversingLabs | Win32.Trojan.VBObfuse | |
| udmugning.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### 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: | 31.0.0 Emerald |
| Analysis ID: | 395203 |
| Start date: | 22.04.2021 |
| Start time: | 09:55:58 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 11s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | udmugning.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: | 23 |
| 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: | mal72.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 97.7% (good quality ratio 48.7%)<br>• Quality average: 27%<br>• Quality standard deviation: 30.5% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe<br>• VT rate limit hit for: /opt/package/joesandbox/database/analysis/395203/sample/udmugning.exe |

# 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): | 5.747482043975765 |
| 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: | udmugning.exe |
| File size: | 118784 |
| MD5: | 3d04ed12388c92e15361681ef1921d7f |
| SHA1: | 8820ff07e1f60121a057b0303dc7746ea4960617 |
| SHA256: | 99227f9bb099737a3f356f266c5b8d5e1f4313715f37a4b7b0b6c1ae65c00925 |
| SHA512: | 39d85417c5667971a8b84eb358656672a2291c8e5214336591c6c5afd7d1a45d6cdd837002797f509e071aa508ce300097c65642cf5ba7d5fc3c6874f08c9f |
| SSDEEP: | 1536:o96yzDtLzOdb4E4Ql9p9LUaYu/+QR15nZ5ioT1VnrveqOrNThdFfwuqltL:oHDtLzOdDLhemaFf |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....O.....p...`.....h.....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | c0c6f2e0e4fefe3f |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x401968 |
| 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: | 0x4FE4DC12 [Fri Jun 22 20:56:50 2012 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: | 7677b40f5f8927412a58af017314f1ed |

### Entrypoint Preview

| Instruction |
|---|
| push 0040F3B0h |
| call 00007F70D0F0A383h |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| xor byte ptr [eax], al |
| add byte ptr [eax], al |
| cmp byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| cmp al, 47h |
| add eax, 838AF2EAh |
| dec esp |
| xchg dword ptr [edx-41h], esp |
| popfd |
| sub eax, 0066210Bh |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [ecx], al |
| add byte ptr [eax], al |
| add byte ptr [ecx+00h], al |
| push es |
| push eax |
| xchg eax, ebx |
| add dl, byte ptr [esi+65h] |
| jnc 00007F70D0F0A406h |
| jnc 00007F70D0F0A392h |
| and al, 02h |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| dec esp |
| xor dword ptr [eax], eax |
| or al, 79h |
| push ebx |
| mov esi, 80015E4Dh |

| Instruction |
|---|
| dec edx |
| lodsd |
| stc |
| xchg eax, ebx |
| or al, bl |
| mov ch, 73h |
| sub ebp, ebx |
| xor dword ptr [edx+5CEADEADh], edi |
| dec edi |
| mov dword ptr [AAF3C737h], eax |
| xchg eax, esi |
| movsd |
| add byte ptr [edx], bh |
| dec edi |
| lodsd |
| xor ebx, dword ptr [ecx-48EE309Ah] |
| or al, 00h |
| stosb |
| add byte ptr [eax-2Dh], ah |
| xchg eax, ebx |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| aaa |
| fld dword ptr [eax] |
| add byte ptr [ecx], bh |
| xlatb |
| add byte ptr [eax], al |
| add byte ptr [ebx], cl |
| add byte ptr [esi+61h], al |
| insb |
| imul esp, dword ptr [edi+68h], 72656465h |
| add byte ptr [55000601h], cl |
| outsb |
| outsd |
| jc 00007F70D0F0A3F3h |
| insb |
| add byte ptr [ecx], bl |
| add dword ptr [eax], eax |
| inc edx |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x17624 | 0x28 | .text |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x1a000 | 0x382a | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x228 | 0x20 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x1000 | 0x1a8 | .text |
| 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 | 0x16c08 | 0x17000 | False | 0.446204144022 | data | 6.13431444514 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x18000 | 0x1260 | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x1a000 | 0x382a | 0x4000 | False | 0.461853027344 | data | 5.140747892 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

## Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x1cf82 | 0x8a8 | data | | |
| RT_ICON | 0x1c8ba | 0x6c8 | data | | |
| RT_ICON | 0x1c352 | 0x568 | GLS_BINARY_LSB_FIRST | | |
| RT_ICON | 0x1b2aa | 0x10a8 | data | | |
| RT_ICON | 0x1a922 | 0x988 | data | | |
| RT_ICON | 0x1a4ba | 0x468 | GLS_BINARY_LSB_FIRST | | |
| RT_GROUP_ICON | 0x1a460 | 0x5a | data | | |
| RT_VERSION | 0x1a1e0 | 0x280 | data | English | United States |

## Imports

| DLL | Import |
|---|---|
| MSVBVM60.DLL | _CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaLateMemCall, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, __vbaFPInt, _CIexp, __vbaFreeStr, __vbaFreeObj |

## Version Infos

| Description | Data |
|---|---|
| Translation | 0x0409 0x04b0 |
| InternalName | udmugning |
| FileVersion | 1.00 |
| CompanyName | Cluster-C |
| Comments | Cluster-C |
| ProductName | Cluster-C |
| ProductVersion | 1.00 |
| FileDescription | Cluster-C |
| OriginalFilename | udmugning.exe |

## Possible Origin

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

| 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: udmugning.exe PID: 3440 Parent PID: 5600

#### General

| | |
|---|---|
| Start time: | 09:56:48 |
| Start date: | 22/04/2021 |
| Path: | C:\Users\user\Desktop\udmugning.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\udmugning.exe' |
| Imagebase: | 0x400000 |
| File size: | 118784 bytes |
| MD5 hash: | 3D04ED12388C92E15361681EF1921D7F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000001.00000002.474162328.0000000000401000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000001.00000000.206225191.0000000000401000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | low |

#### File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

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

## Disassembly

## Code Analysis