


**ID:** 337759
**Sample Name:**
21558_Invoice_confirmation.exe
**Cookbook:** default.jbs
**Time:** 08:24:23
**Date:** 10/01/2021
**Version:** 31.0.0 Red Diamond

# Table of Contents

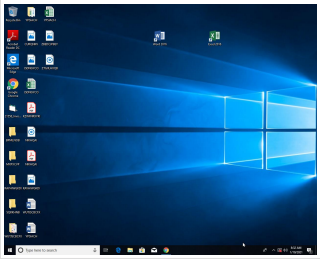
# Analysis Report 21558_Invoice_confirmation.exe

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 21558_Invoice_confirmation.exe |
| Analysis ID: | 337759 |
| MD5: | 2c4f59a6c931a32.. |
| SHA1: | 51e56d7fb64cc3a.. |
| SHA256: | 859bd0c7c174ff2.. |
| Tags: | exe GuLoader |

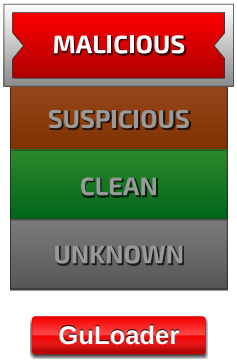
Most interesting Screenshot:



**Errors**

Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

### Detection

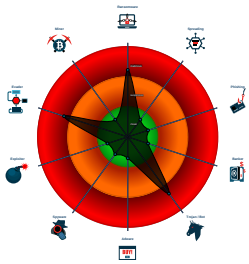



| | |
|---|---|
| Score: | 76 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Potential malicious icon found
- Yara detected GuLoader
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to detect virtu…
- Contains functionality to read the PEB
- PE file contains strange resources
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (…

### Classification



## Startup

- **System is w10x64**
- 21558_Invoice_confirmation.exe (PID: 7052 cmdline: 'C:\Users\user\Desktop\21558_Invoice_confirmation.exe' MD5: 2C4F59A6C931A328DD5D6113C995C35B)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

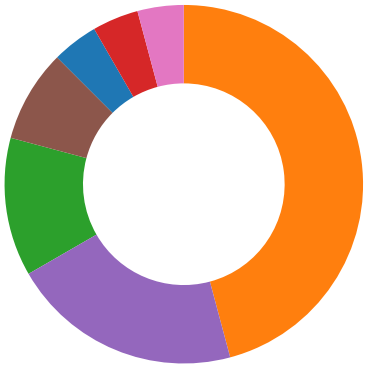
### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| Process Memory Space: 21558_Invoice_confirmation.exe PID: 7052 | JoeSecurity_VB6DownloaderGeneric | Yara detected VB6 Downloader Generic | Joe Security | |
| Process Memory Space: 21558_Invoice_confirmation.exe PID: 7052 | JoeSecurity_GuLoader | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview



- 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

### System Summary:

**Potential malicious icon found**

**Executable has a suspicious name (potential lure to open the executable)**

**Initial sample is a PE file and has a suspicious name**

### Data Obfuscation:

**Yara detected GuLoader**

**Yara detected VB6 Downloader Generic**

### Malware Analysis System Evasion:

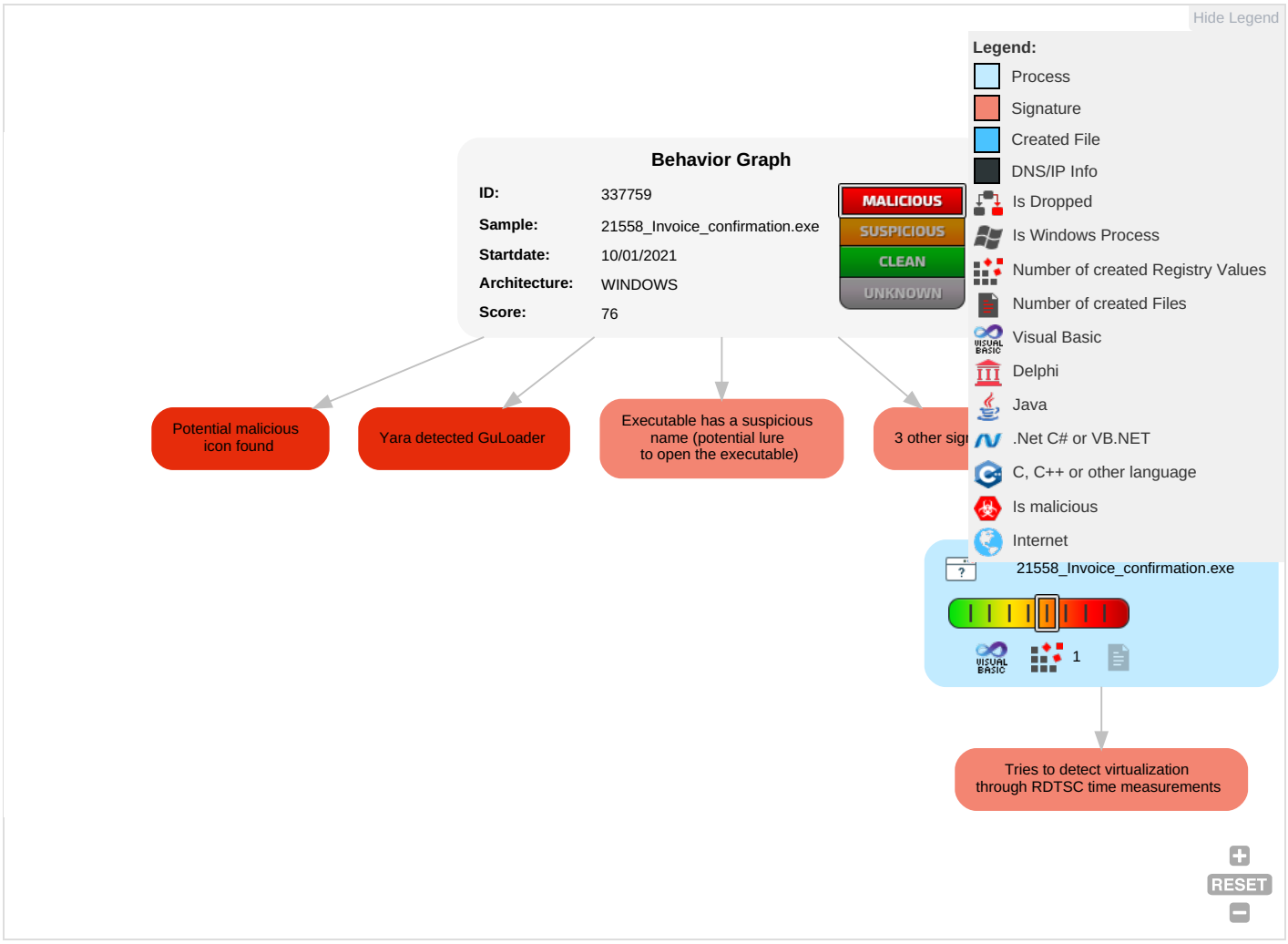
**Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)**

**Tries to detect virtualization through RDTSC time measurements**

## 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 | Virtualization/Sandbox Evasion 1 | OS Credential Dumping | Security Software Discovery 2 1 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop on Insecure Network Communication | R T W A |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1 | LSASS Memory | Virtualization/Sandbox Evasion 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | R W W A |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information 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) | Binary Padding | NTDS | System Information Discovery 1 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |

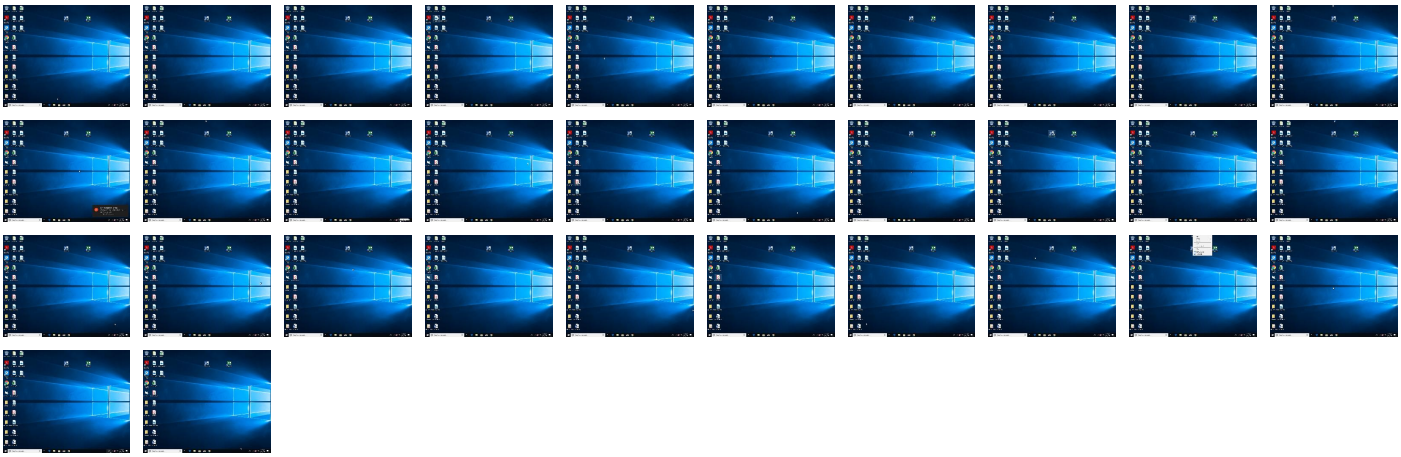
## Behavior Graph




## 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

No Antivirus matches

### 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 Red Diamond |
| Analysis ID: | 337759 |
| Start date: | 10.01.2021 |
| Start time: | 08:24:23 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 4s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 21558_Invoice_confirmation.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: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal76.rans.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 17.6% (good quality ratio 11.2%)<br>• Quality average: 34%<br>• Quality standard deviation: 31.1% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe<br>• Override analysis time to 240s for sample files taking high CPU consumption |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe |
| Errors: | • Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO |

# 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): | 5.714133896280267 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<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: | 21558_Invoice_confirmation.exe |
| File size: | 90112 |
| MD5: | 2c4f59a6c931a328dd5d6113c995c35b |
| SHA1: | 51e56d7fb64cc3a071b12410bcecbf38675fadcc |
| SHA256: | 859bd0c7c174ff2237da9fac27c2feb0e0bbbfe536b273a495440ccd3b748729 |
| SHA512: | 1f7beda5e21464a30c5a03ba063ff07defffc9d54ee9e391e73d8d677e3cc27cdd1bb86cd8dbcac6fc5be4fae2426aa2603a134b0326e1172af7437c8cf3ab90 |
| SSDEEP: | 768:g+J1MqP00si/MIeaz0YIHMqmIISCQA0gtE9shwrDzwNBeIznTg4gyTR3q7xSQ1n7:xMAMRavIsrSCJc2Bn1gyTR3gXm8 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...W...W...W...K...W...u...W...q...W..Rich.W.....PE..L....._.....0...0.....@....@ |

## File Icon

| | |
|---|---|
| Icon Hash: | 20047c7c70f0e004 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x401600 |
| 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: | 0x5FF9D002 [Sat Jan 9 15:47:14 2021 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: | 690ed9eee3aab240a93936dee17050b4 |

### Entrypoint Preview

| Instruction |
|---|
| push 00401C64h |
| call 00007F3534776825h |
| 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 |
| pop edi |
| stosb |
| scasd |
| jnc 00007F3534776800h |
| sbb eax, 40A343B8h |
| mov al, 89h |
| or eax, 00AC48CDh |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [ecx], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [ecx+70h], dl |
| je 00007F3534776833h |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| add byte ptr [eax], al |
| dec esp |
| xor dword ptr [eax], eax |
| sbb dword ptr [eax+5Eh], eax |
| les eax, fword ptr [ecx+6Fh] |
| stosd |
| cmp cl, byte ptr [edx-67h] |
| mov dl, BAh |
| pop ss |
| push esp |
| inc ebp |
| cmp ah, bh |

| Instruction |
|---|
| sti |
| mov cl, bh |
| sbb eax, 4651AB31h |
| mov eax, dword ptr [032F7D1Eh] |
| jnp 00007F353477680Ah |
| cmp cl, byte ptr [edi-53h] |
| 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 |
| test dword ptr [ebx], 003F0000h |
| add byte ptr [eax], al |
| add byte ptr [edi], al |
| add byte ptr [ebx+6Ch], dl |
| popad |
| jnc 00007F3534776895h |
| xor dword ptr [eax], eax |
| or eax, 64000501h |
| jc 00006895h |
| add byte ptr [ecx], bl |
| add dword ptr [eax], eax |
| inc edx |
| add byte ptr [edx], ah |
| add eax, 00000524h |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x13634 | 0x28 | .text |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x16000 | 0x89c | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| 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 | 0x238 | 0x20 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x1000 | 0x184 | .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 | 0x12c18 | 0x13000 | False | 0.416156969572 | data | 6.17855517942 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x14000 | 0x14b0 | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x16000 | 0x89c | 0x1000 | False | 0.16162109375 | data | 1.88975541248 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_ICON | 0x1676c | 0x130 | data | | |
| RT_ICON | 0x16484 | 0x2e8 | data | | |
| RT_ICON | 0x1635c | 0x128 | GLS_BINARY_LSB_FIRST | | |
| RT_GROUP_ICON | 0x1632c | 0x30 | data | | |
| RT_VERSION | 0x16150 | 0x1dc | data | Chinese | Taiwan |

### Imports

| DLL | Import |
|---|---|
| MSVBVM60.DLL | _CIcos, _adj_fptan, __vbaHresultCheck, __vbaVarMove, __vbaFreeVar, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaLateMemSt, __vbaExitProc, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, __vbaAryConstruct2, __vbaR4Str, __vbaObjVar, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, __vbaDateVar, _CIlog, __vbaFileOpen, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaUI1Str, _allmul, _CItan, __vbaFPInt, _CIexp, __vbaFreeStr, __vbaFreeObj |

### Version Infos

| Description | Data |
|---|---|
| Translation | 0x0404 0x04b0 |
| ProductVersion | 1.00 |
| InternalName | ASSACU |
| FileVersion | 1.00 |
| OriginalFilename | ASSACU.exe |
| ProductName | Logaritm |

### Possible Origin

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

## Network Behavior

**No network behavior found**

## Code Manipulations

## Statistics

# System Behavior

## Analysis Process: 21558_Invoice_confirmation.exe PID: 7052 Parent PID: 5736

### General

| | |
|---|---|
| Start time: | 08:25:15 |
| Start date: | 10/01/2021 |
| Path: | C:\Users\user\Desktop\21558_Invoice_confirmation.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\21558_Invoice_confirmation.exe' |
| Imagebase: | 0x400000 |
| File size: | 90112 bytes |
| MD5 hash: | 2C4F59A6C931A328DD5D6113C995C35B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Reputation: | low |

### File Activities

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

### Registry Activities

#### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\VB and VBA Program Settings | success or wait | 1 | 660E2872 | RegCreateKeyW |
| HKEY_CURRENT_USER\Software\VB and VBA Program Settings\unwall | success or wait | 1 | 660E2872 | RegCreateKeyW |
| HKEY_CURRENT_USER\Software\VB and VBA Program Settings\unwall\Oculus | success or wait | 1 | 660E2872 | RegCreateKeyW |

#### Key Value Created

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\VB and VBA Program Settings\unwall\Oculus | Karseklippet | unicode | prenominate | success or wait | 1 | 660E2183 | RegSetValueExW |

# Disassembly

## Code Analysis