Joe Sandbox Cloud BASIC

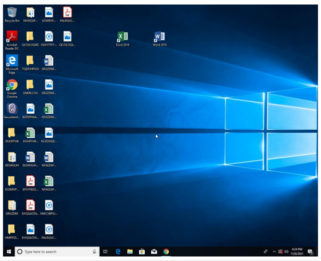
**ID:** 451415
**Sample Name:**
SecuriteInfo.com.__vbaHresultCheckObj.11013.exe
**Cookbook:** default.jbs
**Time:** 16:15:36
**Date:** 20/07/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

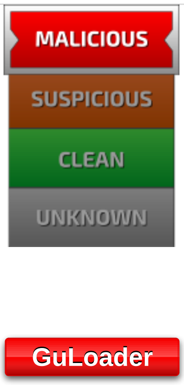
# Windows Analysis Report SecuriteInfo.com.__vbaHresu…

## Overview

### General Information

| | |
|---|---|
| Sample Name: | SecuriteInfo.com.__vbaHresultCheckObj.11013.exe |
| Analysis ID: | 451415 |
| MD5: | c6066a473750ed.. |
| SHA1: | b2c181c008fd857.. |
| SHA256: | 932f31e90730214.. |
| Tags: | exe |
| Infos: | |
| Most interesting Screenshot: |  |

### Detection

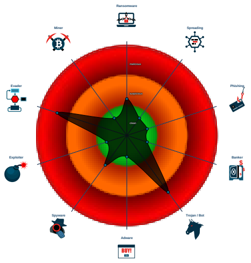


| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to query CPU …
- Contains functionality to read the PEB

### Classification



## Process Tree

- **System is w10x64**
- SecuriteInfo.com.__vbaHresultCheckObj.11013.exe (PID: 5424 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.11013.exe' MD5: C6066A473750ED5AD023D20CE532C8C8)
- **cleanup**

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "https://andreameixueiro.com/IRANSAT_Vsidob74.bin"
}
```

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| SecuriteInfo.com.__vbaHresultCheckObj.11013.exe | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.1302794449.0000000000401000.00000020.00020000.sdmp | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |
| 00000000.00000000.218200781.0000000000401000.00000020.00020000.sdmp | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0.0.SecuriteInfo.com.__vbaHresultCheckObj.11013.exe.400000.0.unpack | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |
| 0.2.SecuriteInfo.com.__vbaHresultCheckObj.11013.exe.400000.0.unpack | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Click to jump to signature section

### 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**

### Malware Analysis System Evasion:

**Contains functionality to detect hardware virtualization (CPUID execution measurement)**

**Detected RDTSC dummy instruction sequence (likely for instruction hammering)**

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

### Anti Debugging:

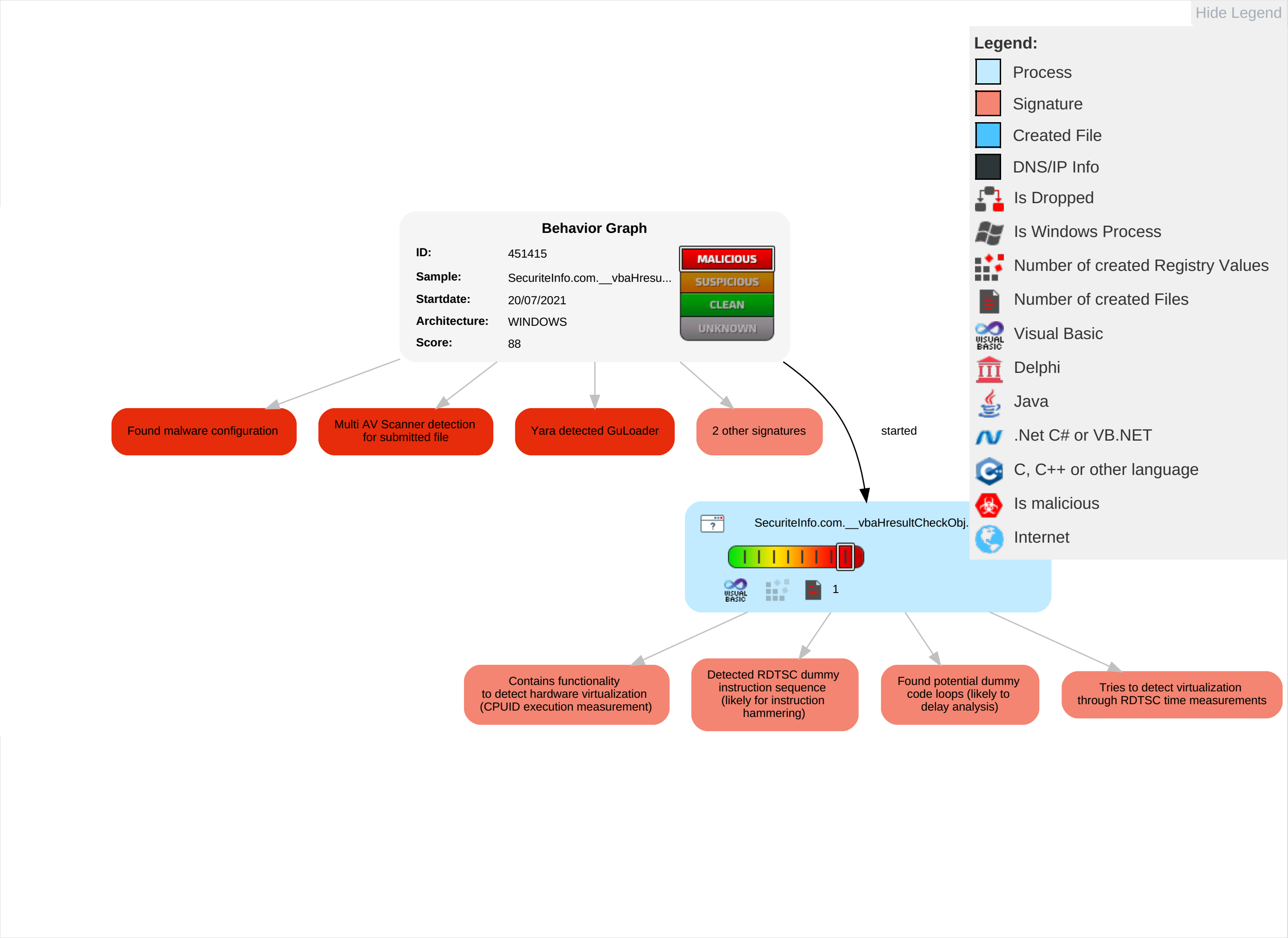
**Found potential dummy code loops (likely to delay analysis)**

## 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 | Virtualization/Sandbox Evasion 1 1 | OS Credential Dumping | Security Software Discovery 4 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 | Process Injection 1 | LSASS Memory | Virtualization/Sandbox Evasion 1 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Application Layer Protocol 1 | 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) | 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 3 1 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |

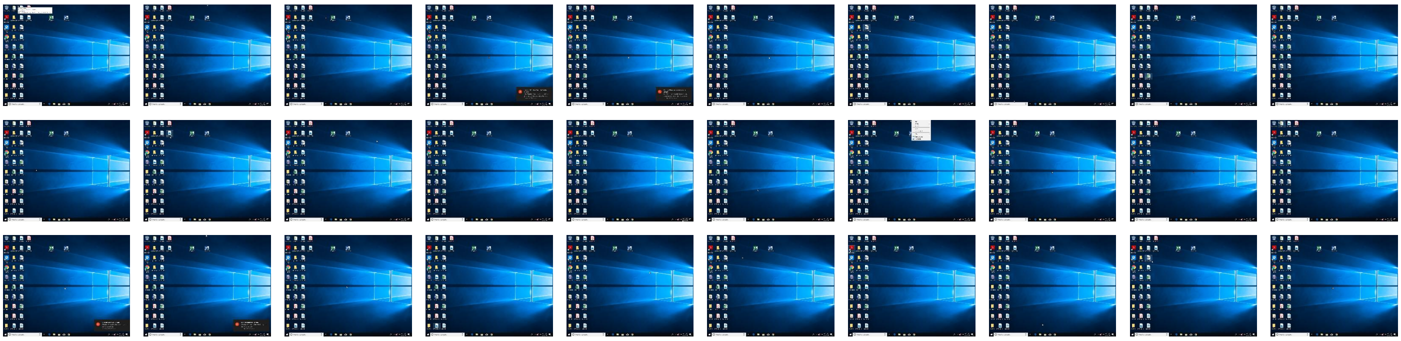
## Behavior Graph

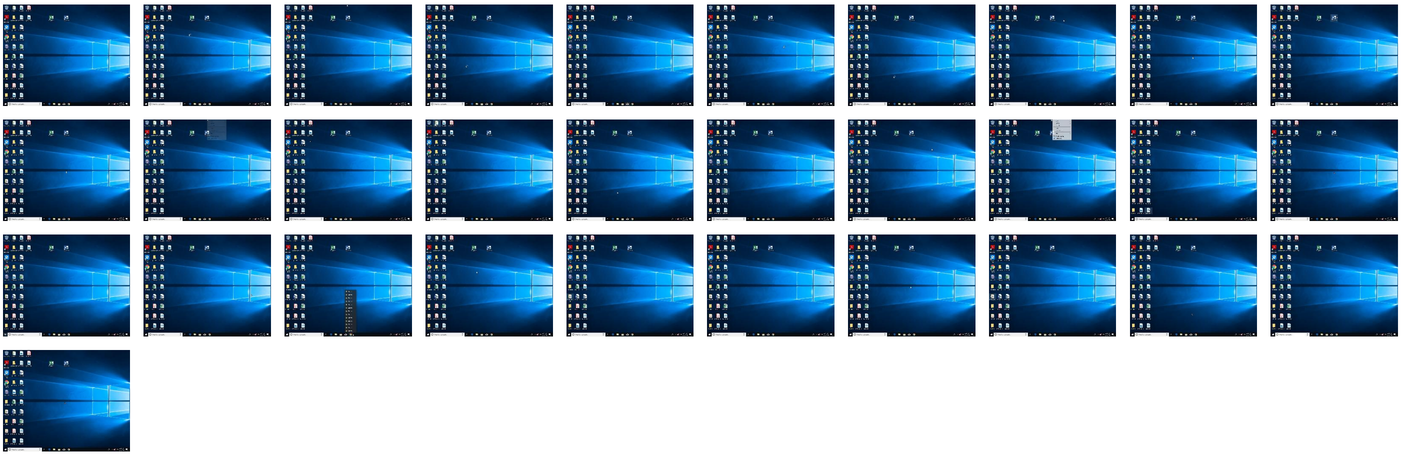

Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
ID: 451415
Sample: SecuriteInfo.com.__vbaHresu...
Startdate: 20/07/2021
Architecture: WINDOWS
Score: 88
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected GuLoader
2 other signatures
started
SecuriteInfo.com.__vbaHresultCheckObj.
1
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Detected RDTSC dummy instruction sequence (likely for instruction hammering)
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements

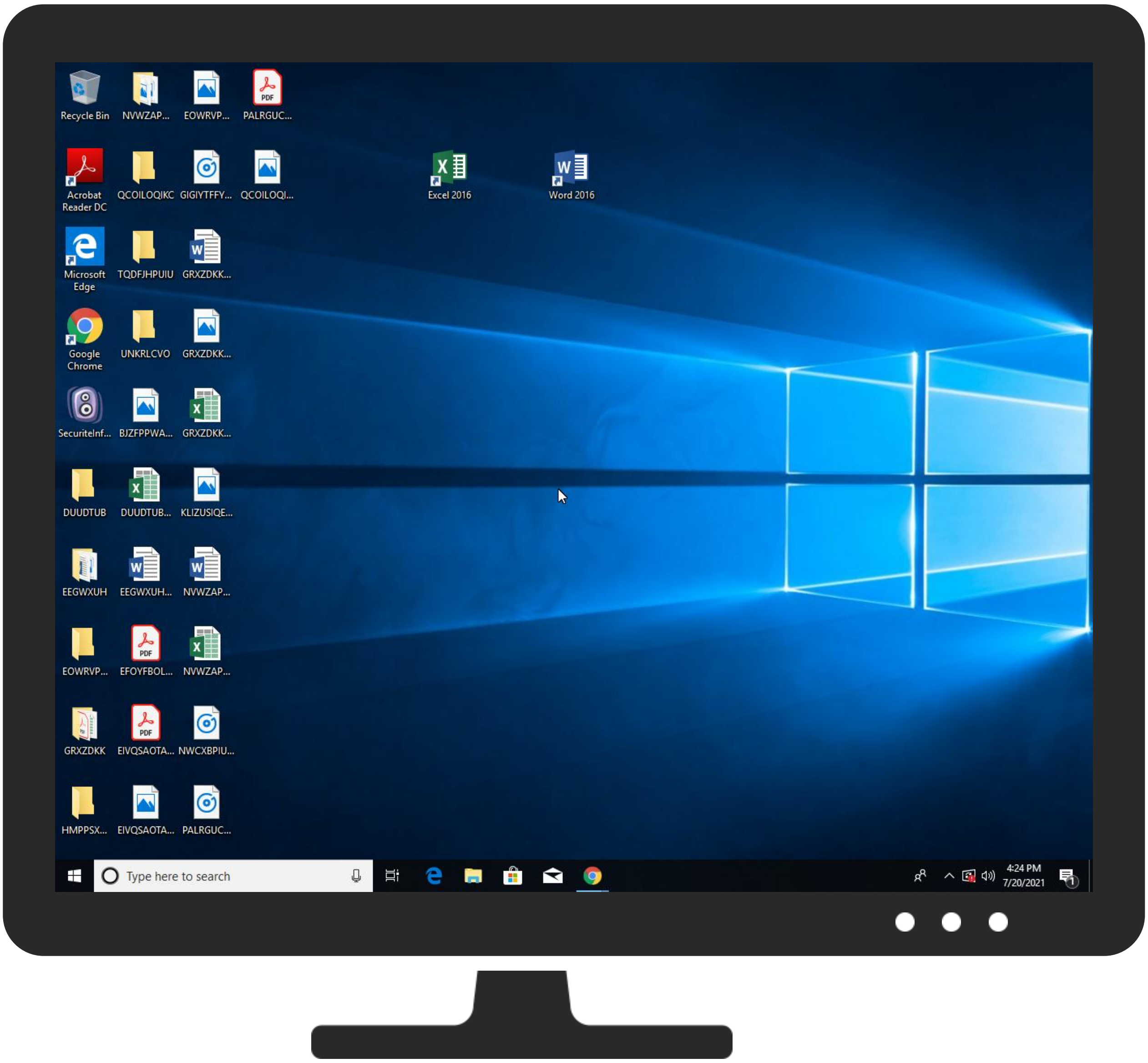
## Screenshots

### 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 |
|---|---|---|---|---|
| SecuriteInfo.com.__vbaHresultCheckObj.11013.exe | 26% | Virustotal | | Browse |
| SecuriteInfo.com.__vbaHresultCheckObj.11013.exe | 30% | ReversingLabs | Win32.Trojan.GuLoader | |
| SecuriteInfo.com.__vbaHresultCheckObj.11013.exe | 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://https://andreameixueiro.com/IRANSAT_Vsidob74.bin | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://andreameixueiro.com/IRANSAT_Vsidob74.bin | true | • Avira URL Cloud: safe | unknown |

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 451415 |
| Start date: | 20.07.2021 |
| Start time: | 16:15:36 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 12m 42s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SecuriteInfo.com.__vbaHresultCheckObj.11013.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 |
| Run name: | Suspected Instruction Hammering Hide Perf |
| Number of analysed new started processes analysed: | 36 |
| 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: | mal88.troj.evad.winEXE@1/0@0/0 |
| EGA Information: | Failed |

| | |
|---|---|
| HDC Information: | Successful, ratio: 6.3% (good quality ratio 1.8%)<br>Quality average: 16.1%<br>Quality standard deviation: 26.2% |
| HCA Information: | Failed |
| 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

**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): | 6.2543149496955905 |
| 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: | SecuriteInfo.com.__vbaHresultCheckObj.11013.exe |
| File size: | 241664 |

## General

| | |
|---|---|
| MD5: | c6066a473750ed5ad023d20ce532c8c8 |
| SHA1: | b2c181c008fd857b0f0122dbfd05d4193654ccc2 |
| SHA256: | 932f31e907302148994f479eafe8dfbf203537491bbd586c43190c59afa248ff |
| SHA512: | eb1bc3dfd845ba94e4e936b48dda25fff41fb59267593eb82facf9e92688ec5c0ed81d8db69855d5e39563ab8449466b3e7cb28ba1eb25c045481283293a6a3b |
| SSDEEP: | 3072:Or3BepJlZa/X16SU2Aara5K8EyrNRlu2mHJlZapGBR:OFiUXI15KHyrDMHP |
| 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....B.O................ ...................0....@................ |

## File Icon

| | |
|---|---|
| Icon Hash: | f8fcd4ccf4e4e8d0 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4019b0 |
| 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: | 0x4FA642B9 [Sun May 6 09:22:01 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: | e9f7dd0da1a2a1266893e1ae4ef42b67 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x31b94 | 0x32000 | False | 0.394462890625 | data | 6.41394682438 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x33000 | 0x1290 | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x35000 | 0x6d12 | 0x7000 | False | 0.482003348214 | data | 5.46106000111 | 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 |
|---|---|---|

| 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: SecuriteInfo.com.__vbaHresultCheckObj.11013.exe PID: 5424 Parent PID: 5572

#### General

| | |
|---|---|
| Start time: | 16:16:31 |
| Start date: | 20/07/2021 |
| Path: | C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.11013.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.11013.exe' |
| Imagebase: | 0x400000 |
| File size: | 241664 bytes |
| MD5 hash: | C6066A473750ED5AD023D20CE532C8C8 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Yara matches: | • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.1302794449.0000000000401000.00000020.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.218200781.0000000000401000.00000020.00020000.sdmp, Author: Joe Security |
| Reputation: | low |

#### File Activities

Show Windows behavior

## Disassembly

### Code Analysis