

JOeSandbox Cloud BASIC



**ID:** 339333

**Sample Name:** URGENT  
MEDICAL REQUIREMENT.exe

**Cookbook:** default.jbs

**Time:** 21:09:25

**Date:** 13/01/2021

**Version:** 31.0.0 Red Diamond

# Table of Contents

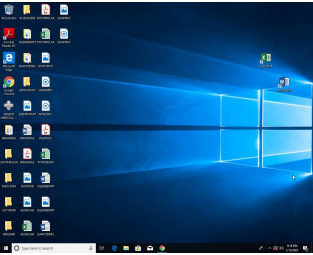
|   |    |
|---|----|
| Table of Contents   | 2  |
| Analysis Report URGENT MEDICAL REQUIREMENT.exe            | 4  |
| Overview  | 4  |
| General Information                                       | 4  |
| Detection   | 4  |
| Signatures  | 4  |
| Classification  | 4  |
| Startup   | 4  |
| Malware Configuration                                     | 4  |
| Yara Overview   | 4  |
| Memory Dumps  | 4  |
| Sigma Overview  | 4  |
| Signature Overview  | 4  |
| AV Detection:   | 5  |
| Data Obfuscation:   | 5  |
| Malware Analysis System Evasion:                          | 5  |
| Anti Debugging:   | 5  |
| Mitre Att&ck Matrix                                       | 5  |
| Behavior Graph  | 6  |
| Screenshots   | 6  |
| Thumbnails  | 6  |
| Antivirus, Machine Learning and Genetic Malware Detection | 7  |
| Initial Sample  | 7  |
| Dropped Files   | 7  |
| Unpacked PE Files   | 7  |
| Domains   | 7  |
| URLs  | 7  |
| Domains and IPs   | 8  |
| Contacted Domains   | 8  |
| Contacted IPs   | 8  |
| General Information                                       | 8  |
| Simulations   | 8  |
| Behavior and APIs   | 8  |
| Joe Sandbox View / Context                                | 9  |
| IPs   | 9  |
| Domains   | 9  |
| ASN   | 9  |
| JA3 Fingerprints  | 9  |
| Dropped Files   | 9  |
| Created / dropped Files                                   | 9  |
| Static File Info  | 9  |
| General   | 9  |
| File Icon   | 9  |
| Static PE Info  | 10 |
| General   | 10 |
| Entrypoint Preview  | 10 |
| Data Directories  | 11 |
| Sections  | 11 |
| Resources   | 11 |
| Imports   | 11 |
| Version Infos   | 11 |
| Possible Origin   | 11 |
| Network Behavior  | 12 |
| Code Manipulations  | 12 |
| Statistics  | 12 |
| System Behavior   | 12 |

|   |    |
|---|----|
| Analysis Process: URGENT MEDICAL REQUIREMENT.exe PID: 6388 Parent PID: 5652 | 12 |
| General   | 12 |
| File Activities   | 12 |
| Disassembly   | 12 |
| Code Analysis   | 12 |

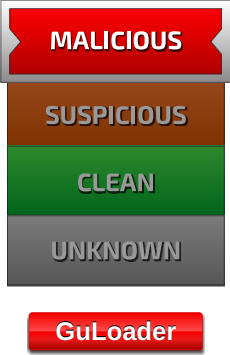
# Analysis Report URGENT MEDICAL REQUIREMENT.exe

## Overview

### General Information

|   |                                |
|---|--------------------------------|
| Sample Name:  | URGENT MEDICAL REQUIREMENT.exe |
| Analysis ID:  | 339333                         |
| MD5:  | 8272ecc1672ecb...              |
| SHA1:   | a77c9fc2b255398..              |
| SHA256:   | 1a4407fd4588109.               |
| Tags:   | exe GuLoader                   |
| Most interesting Screenshot:  |                                |
|  |                                |

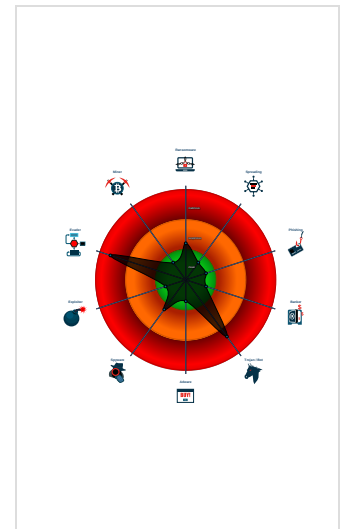
### Detection

|   |         |
|---|---------|
|  |         |
| Score:  | 84      |
| Range:  | 0 - 100 |
| Whitelisted:  | false   |
| Confidence:   | 100%    |


### Signatures

|   |
|---|
| Multi AV Scanner detection for subm...    |
| Yara detected GuLoader                    |
| Contains functionality to detect hard...  |
| Detected RDTSC dummy instruction...       |
| Found potential dummy code loops (...)    |
| Potential time zone aware malware         |
| 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 query CPU ...   |
| Contains functionality to read the PER... |

### Classification



## Startup

- System is w10x64
-  URGENT MEDICAL REQUIREMENT.exe (PID: 6388 cmdline: 'C:\Users\user\Desktop\URGENT MEDICAL REQUIREMENT.exe' MD5: 8272ECC1672ECB390CDEDB27DF85B20D)
- cleanup

## Malware Configuration

No configs have been found

## Yara Overview

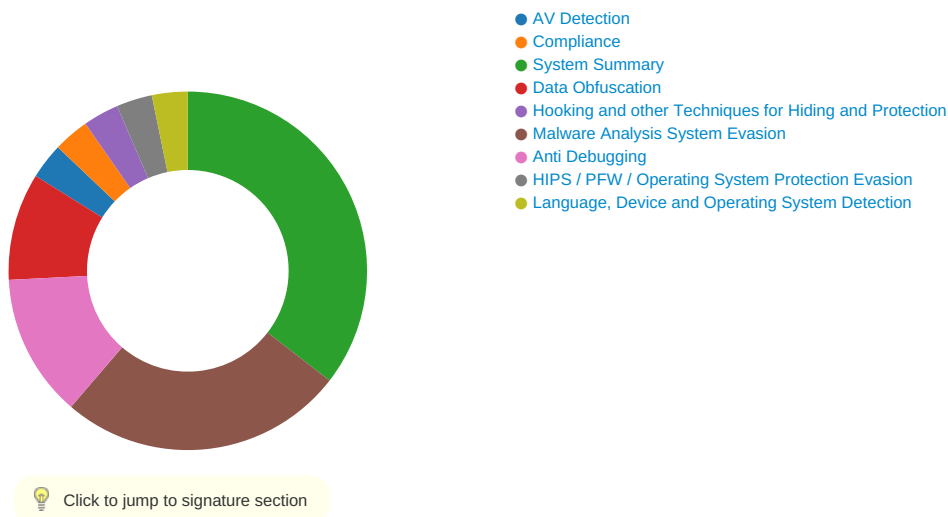
### Memory Dumps

| Source   | Rule                                 | Description                                | Author       | Strings |
|--|--------------------------------------|--|--------------|---------|
| Process Memory Space: URGENT MEDICAL REQ<br>UIREMENT.exe PID: 6388 | JoeSecurity_VB6Download<br>erGeneric | Yara detected VB6<br>Downloader<br>Generic | Joe Security |         |
| Process Memory Space: URGENT MEDICAL REQ<br>UIREMENT.exe PID: 6388 | JoeSecurity_GuLoader                 | Yara detected<br>GuLoader                  | Joe Security |         |

## Sigma Overview

No Sigma rule has matched

## Signature Overview



## AV Detection:



Multi AV Scanner detection for submitted file

## Data Obfuscation:



Yara detected GuLoader

Yara detected VB6 Downloader Generic

## Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Potential time zone aware malware

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

Tries to detect virtualization through RDTSC time measurements

## Anti Debugging:

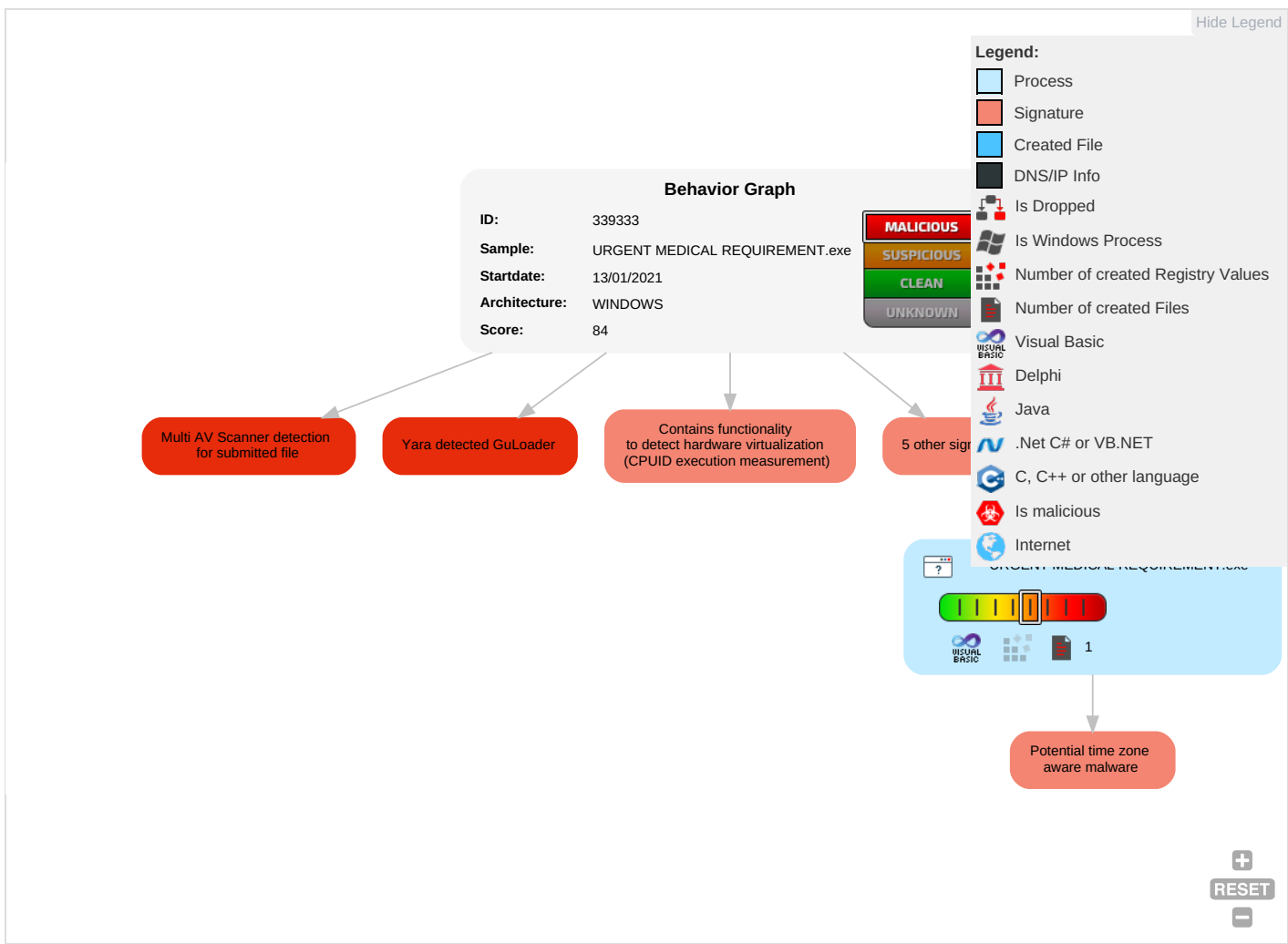


Found potential dummy code loops (likely to delay analysis)

## Mitre Att&ck Matrix

| Initial Access   | Execution                          | Persistence                          | Privilege Escalation                 | Defense Evasion                    | Credential Access        | Discovery                          | Lateral Movement                   | Collection                     | Exfiltration                           | Command and Control    | Network Effects                             | Recovery |
|------------------|------------------------------------|--------------------------------------|--------------------------------------|------------------------------------|--------------------------|------------------------------------|------------------------------------|--------------------------------|--|------------------------|---|----------|
| Valid Accounts   | Windows Management Instrumentation | Path Interception                    | Process Injection 1                  | Virtualization/Sandbox Evasion 1 1 | OS Credential Dumping    | System Time Discovery 1            | Remote Services                    | Archive Collected Data 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 | Process Injection 1                | LSASS Memory             | Security Software Discovery 5 1 1  | Remote Desktop Protocol            | Data from Removable Media      | Exfiltration Over Bluetooth            | Junk Data              | Exploit SS7 to Redirect Phone Calls/SMS     | Recovery |
| Domain Accounts  | At (Linux)                         | Logon Script (Windows)               | Logon Script (Windows)               | Obfuscated Files or Information 1  | Security Account Manager | Virtualization/Sandbox Evasion 1 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)                   | Binary Padding                     | NTDS                     | Process Discovery 1                | Distributed Component Object Model | Input Capture                  | Scheduled Transfer                     | Protocol Impersonation | SIM Card Swap                               | Recovery |
| Cloud Accounts   | Cron                               | Network Logon Script                 | Network Logon Script                 | Software Packing                   | LSA Secrets              | System Information Discovery 3 1 1 | SSH                                | Keylogging                     | Data Transfer Size Limits              | Fallback Channels      | Manipulate Device Communication             | Recovery |

## Behavior Graph

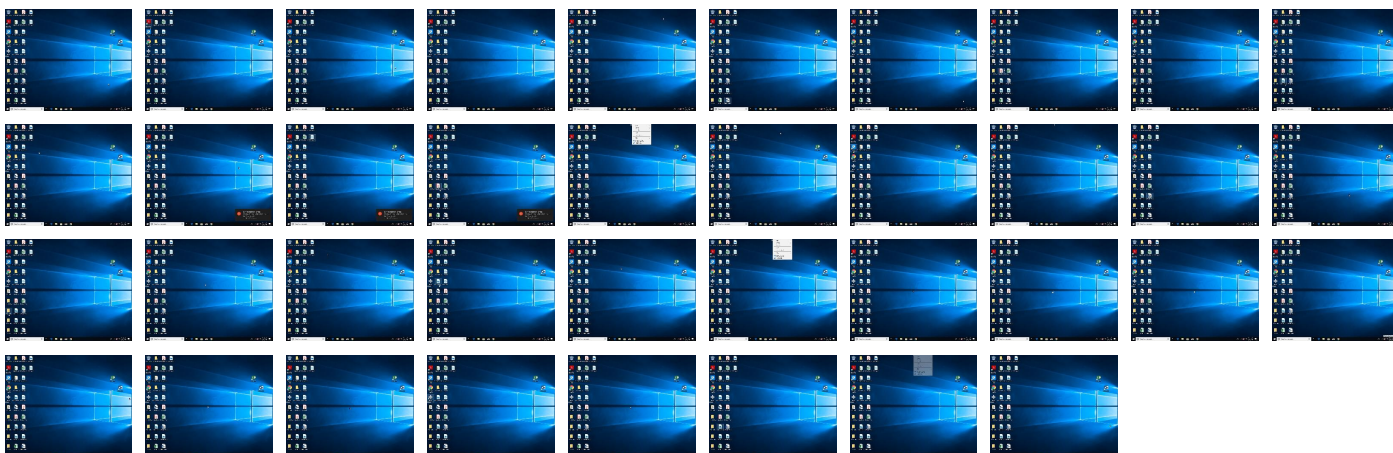


## Screenshots

## Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

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                   |
|--------------------------------|-----------|------------|-------|------------------------|
| URGENT MEDICAL REQUIREMENT.exe | 24%       | Virustotal |       | <a href="#">Browse</a> |

### 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:                                       | 339333   |
| Start date:  | 13.01.2021   |
| Start time:  | 21:09:25   |
| Joe Sandbox Product:                               | CloudBasic   |
| Overall analysis duration:                         | 0h 10m 45s   |
| Hypervisor based Inspection enabled:               | false  |
| Report type:                                       | light  |
| Sample file name:                                  | URGENT MEDICAL REQUIREMENT.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: | 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:                                      | <ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>   |
| Analysis Mode:                                     | default  |
| Analysis stop reason:                              | Timeout  |
| Detection:   | MAL  |
| Classification:                                    | mal84.troj.evad.winEXE@1/0@0/0   |
| EGA Information:                                   | Failed   |
| HDC Information:                                   | <ul style="list-style-type: none"><li>• Successful, ratio: 18% (good quality ratio 9.5%)</li><li>• Quality average: 32.5%</li><li>• Quality standard deviation: 34.6%</li></ul>  |
| HCA Information:                                   | Failed   |
| Cookbook Comments:                                 | <ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .exe</li><li>• Override analysis time to 240s for sample files taking high CPU consumption</li></ul>  |
| Warnings:  | Show All <ul style="list-style-type: none"><li>• Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe</li></ul> |

## Simulations

### Behavior and APIs



|                |
|----------------|
| No simulations |
| 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):       | 5.134415776571089   |
| TrID:                 | <ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul> |
| File name:            | URGENT MEDICAL REQUIREMENT.exe  |
| File size:            | 65536   |
| MD5:                  | 8272ecc1672ecb390cdedb27df85b20d  |
| SHA1:                 | a77c9fc2b255398f53d28f6e67633c62a0143fa5  |
| SHA256:               | 1a4407fd45881091495f927612c7be23ab6de71949e419;cdc58154986d2c827  |
| SHA512:               | e67cefef757b83d16f598b3780cdb34d604cc0cfb89aaff75f01a46d93734fd855d9dbc653dff78f254e87af193491bd3cd8db62986ec5fef64a70aabf03ee20  |
| SSDEEP:               | 768:IkQzo6k3c8OPfkCdmhrvbQEGF67WCCfEIQZ:pQzcsgCq/QNFUaEIS   |
| File Content Preview: | MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...E4.T.....0.....@.....  |

### File Icon

|  |                  |
|--|------------------|
|  |                  |
| Icon Hash:   | f030f0c6f030b100 |

## Static PE Info

### General

|                             |   |
|-----------------------------|---|
| Entrypoint:                 | 0x401200  |
| 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:                 | 0x54C53445 [Sun Jan 25 18:21:57 2015 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:                | e4e19abc2b8b3cdf6beb846e51c393a2  |

## Entrypoint Preview

### Instruction

```

push 00401E64h
call 00007F9854858B25h
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
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+643D901Fh], dl
clc
dec ebx
inc ebp
mov ch, C9h
mov bl, 38h
pop ecx
sub ah, byte ptr [edi+00000000h]
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
jnc 00007F9854858BA6h
outsd
jc 00007F9854858B9Bh
push eax
jc 00007F9854858BA1h
push 00000065h
arpl word ptr [ecx+esi+00h], si
je 00007F9854858BABh
insb
and byte ptr [00000020h], bh
add bh, bh
int3
xor dword ptr [eax], eax
add eax, dword ptr [645E3E9Fh]
```

|                    |
|--------------------|
| <b>Instruction</b> |
| test ch, ch        |
| dec ecx            |
| test al, 7Eh       |
| pop edx            |
| adc al, BAh        |

Data Directories

| Name                                 | Virtual Address | Virtual Size | Is in Section |
|--------------------------------------|-----------------|--------------|---------------|
| IMAGE_DIRECTORY_ENTRY_EXPORT         | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_IMPORT         | 0xd254          | 0x28         | .text         |
| IMAGE_DIRECTORY_ENTRY_RESOURCE       | 0x10000         | 0x8c0        | .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   | 0x228           | 0x20         |               |
| IMAGE_DIRECTORY_ENTRY_IAT            | 0x1000          | 0xc4         | .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          | 0xc5f8       | 0xd000   | False    | 0.514047475962  | data      | 5.83494280245 | IMAGE_SCN_MEM_EXECUTE,<br>IMAGE_SCN_CNT_CODE,<br>IMAGE_SCN_MEM_READ           |
| .data | 0xe000          | 0x1158       | 0x1000   | False    | 0.00634765625   | data      | 0.0           | IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_WRITE,<br>IMAGE_SCN_MEM_READ |
| .rsrc | 0x10000         | 0x8c0        | 0x1000   | False    | 0.137939453125  | data      | 1.31495882197 | IMAGE_SCN_CNT_INITIALIZED_DATA,<br>IMAGE_SCN_MEM_READ                         |

Resources

| Name          | RVA     | Size  | Type                 | Language | Country       |
|---------------|---------|-------|----------------------|----------|---------------|
| RT_ICON       | 0x10358 | 0x568 | GLS_BINARY_LSB_FIRST |          |               |
| RT_GROUP_ICON | 0x10344 | 0x14  | data                 |          |               |
| RT_VERSION    | 0x100f0 | 0x254 | data                 | English  | United States |


Imports

| DLL          | Import   |
|--------------|--|
| MSVBVM60.DLL | __vbaCyForInit, __Clicos, __adj_fptan, __vbaFreeVar, __vbaEnd, __adj_fdiv_m64, __adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, __adj_fdiv_m32, __vbaObjSet, __adj_fdiv_m16i, __adj_fdivr_m16i, __vbaVarTstLt, __Clsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaCyl2, __vbaStrCmp, __vbaCyl4, __adj_fpatan, EVENT_SINK_Release, __Clsqrt, EVENT_SINK_QueryInterface, __vbaExceptionHandler, __adj_fprem, __adj_fdivr_m64, __vbaFPEException, __vbaCyForNext, __Cllog, __vbaNew2, __adj_fdiv_m32i, __adj_fdivr_m32i, __vbaI4Str, __vbaFreeStrList, __adj_fdivr_m32, __adj_fdiv_r, __Clatan, __vbaStrMove, __allmul, __Cltan, __Clexp, __vbaFreeObj, __vbaFreeStr |

Version Infos

| Description      | Data             |
|------------------|------------------|
| Translation      | 0x0409 0x04b0    |
| InternalName     | Hybridizers5     |
| FileVersion      | 2.00             |
| CompanyName      | Axis Corp        |
| Comments         | Axis Corp        |
| ProductName      | Project1         |
| ProductVersion   | 2.00             |
| OriginalFilename | Hybridizers5.exe |

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: URGENT MEDICAL REQUIREMENT.exe PID: 6388 Parent PID: 5652

### General

|                               |  |
|-------------------------------|--|
| Start time:                   | 21:10:15   |
| Start date:                   | 13/01/2021   |
| Path:                         | C:\Users\user\Desktop\URGENT MEDICAL REQUIREMENT.exe   |
| Wow64 process (32bit):        | true   |
| Commandline:                  | 'C:\Users\user\Desktop\URGENT MEDICAL REQUIREMENT.exe' |
| Imagebase:                    | 0x400000   |
| File size:                    | 65536 bytes  |
| MD5 hash:                     | 8272ECC1672ECB390CDEDB27DF85B20D                       |
| Has elevated privileges:      | true   |
| Has administrator privileges: | true   |
| Programmed in:                | Visual Basic   |
| Reputation:                   | low  |

### File Activities

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

## Disassembly

### Code Analysis