
**ID:** 452731
**Sample Name:**
ENQUIRY_101.exe
**Cookbook:** default.jbs
**Time:** 19:11:21
**Date:** 22/07/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

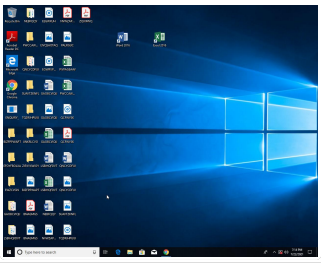
# Windows Analysis Report ENQUIRY_101.exe

## Overview

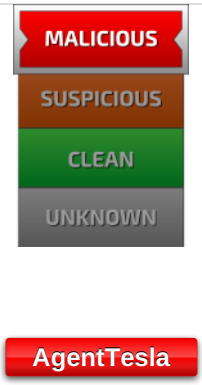
### General Information

| | |
|---|---|
| Sample Name: | ENQUIRY_101.exe |
| Analysis ID: | 452731 |
| MD5: | 5b14a7366cf5dbe. |
| SHA1: | 2a39f1d215a739d. |
| SHA256: | f6ef92f6911bb14… |
| Tags: | exe |
| Infos: | |

Most interesting Screenshot:



### Detection

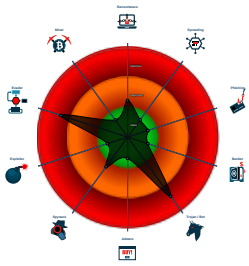



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AgentTesla
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Antivirus or Machine Learning detec…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Detected potential crypto function
- Enables debug privileges
- Found a high number of Window / Us…

### Classification



## Process Tree

- **System is w10x64**
- ENQUIRY_101.exe (PID: 6796 cmdline: 'C:\Users\user\Desktop\ENQUIRY_101.exe' MD5: 5B14A7366CF5DBEA3386C6AFBD25F012)
  - ENQUIRY_101.exe (PID: 6292 cmdline: C:\Users\user\Desktop\ENQUIRY_101.exe MD5: 5B14A7366CF5DBEA3386C6AFBD25F012)
- **cleanup**

## Malware Configuration

### Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "info@hajartrading.net",
  "Password": "Hajarbh@1993",
  "Host": "box5363.bluehost.com"
}
```


## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000007.00000002.943178137.000000000402000.00000040.00000001.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 00000007.00000002.943178137.000000000402000.00000040.00000001.sdmp | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 00000007.00000002.944445963.000000000341000.00000004.00000001.sdmp | JoeSecurity_CredentialStealer | Yara detected Credential Stealer | Joe Security | |
| Process Memory Space: ENQUIRY_101.exe PID: 6292 | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| Process Memory Space: ENQUIRY_101.exe PID: 6292 | JoeSecurity_CredentialStealer | Yara detected Credential Stealer | Joe Security | |

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 7.2.ENQUIRY_101.exe.400000.0.unpack | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 7.2.ENQUIRY_101.exe.400000.0.unpack | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

**Found malware configuration**

**Machine Learning detection for sample**

### System Summary:

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

### Malware Analysis System Evasion:

**Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)**

**Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)**

### HIPS / PFW / Operating System Protection Evasion:

**Injects a PE file into a foreign processes**

### Stealing of Sensitive Information:

**Yara detected AgentTesla**

**Yara detected AgentTesla**

### Remote Access Functionality:

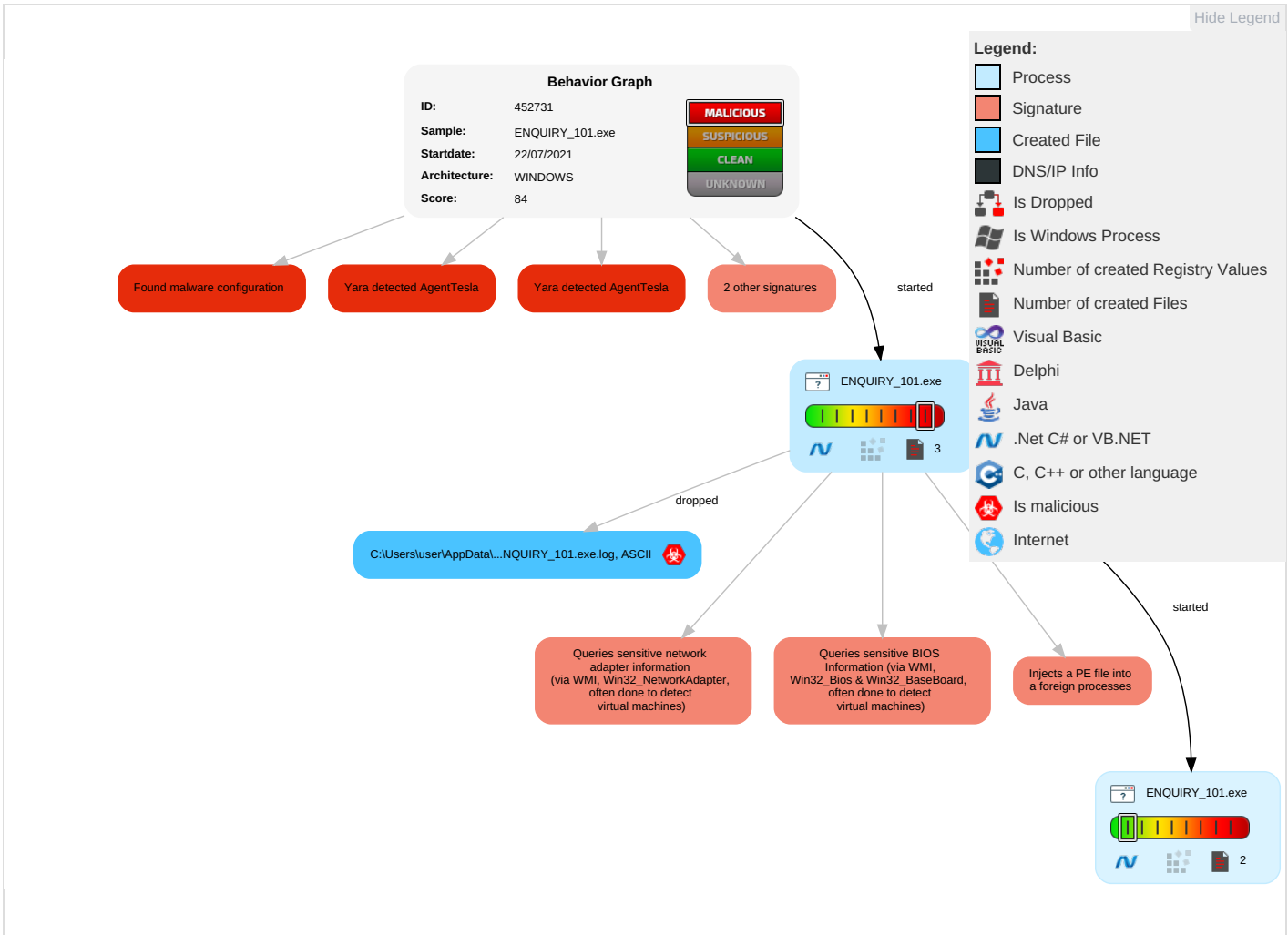
**Yara detected AgentTesla**

**Yara detected AgentTesla**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | I |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 2 1 1 | Path Interception | Process Injection 1 1 2 | Masquerading 1 | OS Credential Dumping | Security Software Discovery 1 1 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Disable or Modify Tools 1 | LSASS Memory | Process Discovery 2 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 1 3 1 | Security Account Manager | Virtualization/Sandbox Evasion 1 3 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 1 1 2 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Obfuscated Files or Information 2 | LSA Secrets | Account Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Software Packing 3 | Cached Domain Credentials | System Owner/User Discovery 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Compile After Delivery | DCSync | System Information Discovery 1 1 3 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | |

## 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 |
|---|---|---|---|---|
| ENQUIRY_101.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 7.2.ENQUIRY_101.exe.400000.0.unpack | 100% | Avira | TR/Spy.Gen8 | | Download File |

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.agfamonotype.c | 0% | Avira URL Cloud | safe | |
| http://127.0.0.1:HTTP/1.1 | 0% | Avira URL Cloud | safe | |
| http://AeXMrV.com | 0% | Avira URL Cloud | safe | |
| http://DynDns.comDynDNS | 0% | URL Reputation | safe | |
| http://DynDns.comDynDNS | 0% | URL Reputation | safe | |
| http://DynDns.comDynDNS | 0% | URL Reputation | safe | |
| http://www.fontbureau.comF | 0% | URL Reputation | safe | |
| http://www.fontbureau.comF | 0% | URL Reputation | safe | |
| http://www.fontbureau.comF | 0% | URL Reputation | safe | |
| http://www.agfamonotype. | 0% | URL Reputation | safe | |
| http://www.agfamonotype. | 0% | URL Reputation | safe | |
| http://www.agfamonotype. | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/Q | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/Q | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/Q | 0% | URL Reputation | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha | 0% | URL Reputation | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha | 0% | URL Reputation | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-d | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-d | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-d | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn_tr | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comma | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/L | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/L | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/L | 0% | URL Reputation | safe | |
| http://www.fonts.comic~ | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp//e | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 0% | URL Reputation | safe | |
| http://www.fontbureau.coma | 0% | URL Reputation | safe | |
| http://www.fontbureau.coma | 0% | URL Reputation | safe | |
| http://www.fontbureau.coma | 0% | URL Reputation | safe | |
| http://www.fontbureau.comd | 0% | URL Reputation | safe | |
| http://www.fontbureau.comd | 0% | URL Reputation | safe | |
| http://www.fontbureau.comd | 0% | URL Reputation | safe | |
| http://www.sakkal.comgu | 0% | Avira URL Cloud | safe | |
| http://www.fonts.comtx | 0% | Avira URL Cloud | safe | |
| http://www.tiro.comZ | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comituF | 0% | URL Reputation | safe | |
| http://www.fontbureau.comituF | 0% | URL Reputation | safe | |
| http://www.fontbureau.comituF | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/5 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/5 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/5 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/c | 0% | Avira URL Cloud | safe | |
| http://www.fonts.comD | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/Y0/ | 0% | URL Reputation | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.jiyu-kobo.co.jp/Y0/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/Y0/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/Y0-g | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://www.fontbureau.comFz | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/h | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/h | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/h | 0% | URL Reputation | safe | |
| http://www.fontbureau.comalic | 0% | URL Reputation | safe | |
| http://www.fontbureau.comalic | 0% | URL Reputation | safe | |
| http://www.fontbureau.comalic | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/c | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/c | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/c | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/s-ez | 0% | Avira URL Cloud | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.fontbureau.com.TTF | 0% | URL Reputation | safe | |
| http://www.fontbureau.com.TTF | 0% | URL Reputation | safe | |
| http://www.fontbureau.com.TTF | 0% | URL Reputation | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip | 0% | URL Reputation | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip | 0% | URL Reputation | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip | 0% | URL Reputation | safe | |
| http://www.fontbureau.comalse | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## URLs from Memory and Binaries

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 452731 |
| Start date: | 22.07.2021 |
| Start time: | 19:11:21 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 6s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | ENQUIRY_101.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: | 18 |
| 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: | mal84.troj.evad.winEXE@3/1@0/0 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 1.1% (good quality ratio 0.7%)<br>• Quality average: 41.9%<br>• Quality standard deviation: 33% |
| HCA Information: | • Successful, ratio: 99%<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

| Time | Type | Description |
|---|---|---|
| 19:12:53 | API Interceptor | 592x Sleep call for process: ENQUIRY_101.exe modified |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

**C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ENQUIRY_101.exe.log**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\ENQUIRY_101.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1216 |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ENQUIRY_101.exe.log | |
|---|---|
| Entropy (8bit): | 5.355304211458859 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY |
| MD5: | 69206D3AF7D6EFD08F4B4726998856D3 |
| SHA1: | E778D4BF781F7712163CF5E2F5E7C15953E484CF |
| SHA-256: | A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87 |
| SHA-512: | CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8 |
| Malicious: | **true** |
| Reputation: | high, very likely benign file |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.763416763918635 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.83%<br>• Win32 Executable (generic) a (10002005/4) 49.78%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Generic Win/DOS Executable (2004/3) 0.01%<br>• DOS Executable Generic (2002/1) 0.01% |
| File name: | ENQUIRY_101.exe |
| File size: | 747008 |
| MD5: | 5b14a7366cf5dbea3386c6afbd25f012 |
| SHA1: | 2a39f1d215a739ddf4e2daf87fb42e26f12f72ac |
| SHA256: | f6ef92f6911bb14f5b8905f3964d21a9569c41c4e5367d0ee8aec59d54eb7024 |
| SHA512: | df11b3ff17cb7a4508a7629e978ca175824f4dae73f9cbdde60da7825ebac73f9c335fc02883a0bcdd007e8806c6372400eeb1e746cc97cfcaf051d55169a172 |
| SSDEEP: | 12288:NCKE0cM4fvJZx2wzrO+kaA6i0NrJhVFo4actOTj1xcoPGniqEW5zh1Sly:NCKEZM4ZHNzrOlaA7u9S4jtOooenio |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....~.`.....P..Z.....x... .....@.. .....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00828e8e8686b000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4b78fe |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x60F87E15 [Wed Jul 21 20:05:41 2021 UTC] |

### General

| | |
|---|---|
| TLS Callbacks: | |
| CLR (.Net) Version: | v4.0.30319 |
| 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: | f34d5f2d4577ed6d9ceec516c1f5a744 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x2000 | 0xb5904 | 0xb5a00 | False | 0.862994935048 | data | 7.77326608249 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xb8000 | 0x650 | 0x800 | False | 0.34765625 | data | 3.55281808773 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xba000 | 0xc | 0x200 | False | 0.041015625 | data | 0.0815394123432 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

## Network Behavior

**No network behavior found**

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: ENQUIRY_101.exe PID: 6796 Parent PID: 5812

### General

| | |
|---|---|
| Start time: | 19:12:23 |
| Start date: | 22/07/2021 |
| Path: | C:\Users\user\Desktop\ENQUIRY_101.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\ENQUIRY_101.exe' |
| Imagebase: | 0x230000 |
| File size: | 747008 bytes |
| MD5 hash: | 5B14A7366CF5DBEA3386C6AFBD25F012 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Written**

**File Read**

## Analysis Process: ENQUIRY_101.exe PID: 6292 Parent PID: 6796

### General

| | |
|---|---|
| Start time: | 19:12:53 |
| Start date: | 22/07/2021 |
| Path: | C:\Users\user\Desktop\ENQUIRY_101.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\ENQUIRY_101.exe |
| Imagebase: | 0xfc0000 |
| File size: | 747008 bytes |
| MD5 hash: | 5B14A7366CF5DBEA3386C6AFBD25F012 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.943178137.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.943178137.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.944445963.0000000003431000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Read**

# Disassembly

## Code Analysis