

# MALWARE 2 ANALYSIS

RAMNICK FRANCIS P. RAMOS

## METADATA

```
[12/02/25]seed@VM:~/.../malware$ file malware2.exe
malware2.exe: PE32 executable (GUI) Intel 80386, for MS Windows
[12/02/25]seed@VM:~/.../malware$ ls -lg malware2.exe
-rw-rw-r-- 1 seed 2560 Dec  6 2021 malware2.exe

[12/02/25]seed@VM:~/.../malware$ r2 -q -c 'IH-AddressOfEntryPoint; iH-subsys; iH-LinkerVersion; iH-Characteristics' malware2.exe
[{"name": "iH-AddressOfEntryPoint", "value": "0x1400", "type": "hex"}, {"name": "iH-LinkerVersion", "value": "0x1", "type": "hex"}, {"name": "iH-Characteristics", "value": "0x0", "type": "hex"}]
```

malware2.exe is identified as a Windows executable. Based on an inspection of the PE Header, it has been determined to be a PE32 (32-bit) Windows GUI application. This indicates that it operates within a Windows GUI subsystem.

It is also just 2560 kb. Notably, it is very small for a malware. It is also indicated here that it was compiled on Dec 06 2021.

## CRYPTANALYSIS

```
[12/02/25]seed@VM:~/.../malware$ sha256sum malware2.exe
f194cec4e81b74370be90b71f7d6300baafef5ef3916ad1648d40feae2ac3d  malware2.exe
[12/02/25]seed@VM:~/.../malware$ md5sum malware2.exe
36b75de0f5b9371efdf0f167490f493c  malware2.exe
[12/02/25]seed@VM:~/.../malware$ shasum malware2.exe
03ab2cc6b016da635606dc34a0dc1239218084f6  malware2.exe
```

Using Linux hashing commands for sha256, md5sum, and sha1, the cryptographic hashes of the executable were calculated to identify the sample across various systems. These hash values can serve as identification indicators if the malware spreads to other machines. The collected values are displayed above.

## SECTION ANALYSIS

### PE sections

```
[12/02/25]seed@VM:~/.../malware$ r2 -q -c "iS" malware2.exe
[Sections]
nth paddr      size vaddr      vsiz perm name
0  0x00000200  0x800 0x00401000  0x1000 -rwx .text
```

### Entropy

```
[12/02/25]seed@VM:~/.../malware$ r2 -q -c "iSj" malware2.exe
[{"name": ".text", "size": 2048, "vsize": 4096, "perm": "-rwx", "paddr": 512, "vaddr": 4198400}]

[12/02/25]seed@VM:~/.../malware$
```

The malware contains only one section, the text section. The text section of the malware is incredibly small.

This suggests that this malware is non-infectious and does not contain heavy operations.

## STRING ANALYSIS

### Domain, URL, IPs

```
[12/02/25]seed@VM:~/.../malware$ strings -n 5 malware2.exe | grep -Ei "http|https|ftp|.com|.net|.cn|.sec"
GoLink www.GoDevtool.com
- GreetTz From CMSC191:CNSEC, ICS-UPLB -
- GreetTz From CMSC191:CNSEC, ICS-UPLB -
```

### Executable or commands

```
[12/02/25]seed@VM:~/.../malware$ strings -n 5 malware2.exe | grep -Ei "exe|cmd|run|shell"
* .exe
* .exe
```

### GoDeveTool



The strings content of the malware, however, reveals that the binary is linked to a certain goDevtool.com. This website appears to be a windows+assembler tutorial site. It also contains information about it being made from CNSEC class for CMSC 191.

## IMPORT ANALYSIS

### NO IMPORT

```
[12/02/25]seed@VM:~/.../malware$ r2 -q -c "ii-WININET" malware2.exe
[12/02/25]seed@VM:~/.../malware$ r2 -q -c "ii-USER32" malware2.exe
[12/02/25]seed@VM:~/.../malware$ r2 -q -c "ii-GDI32" malware2.exe
[12/02/25]seed@VM:~/.../malware$ r2 -q -c "ii-gdiplus" malware2.exe
[12/02/25]seed@VM:~/.../malware$ r2 -q -c "ii" malware2.exe
[Imports]
nth vaddr bind type lib name
```

## SUMMARY OF FINDINGS

This is a no security risk malware. IT appears that it is a non-functional malware that may have been created under GoDevTools.com for a certain CMSC191:CNSEC class in Dec 06, 2021.

## VIRUS TOTAL ANALYSIS

A screenshot of the VirusTotal analysis interface. It shows a summary bar at the top indicating 48/72 vendors flagged the file as malicious. Below this, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is selected, showing a table of results from various engines. Some notable detections include Avast, ESET-NOD32, and BitDefender.

A screenshot of the VirusTotal analysis interface showing the COMMUNITY tab. It displays information about contacted domains, IP addresses, and bundled files. The COMMUNITY tab also includes a 'Graph Summary' section which is currently empty.