Detect Mortis Locker Ransomware With YARA Rule

m4lcode.github.io/malware analysis/Mortis-Locker-YARA-Rule/

January 10, 2024

Overview

Mortis Locker is a ransomware that was first discovered on 29 September 2023 by @MalGamy12.

Mortis Samples

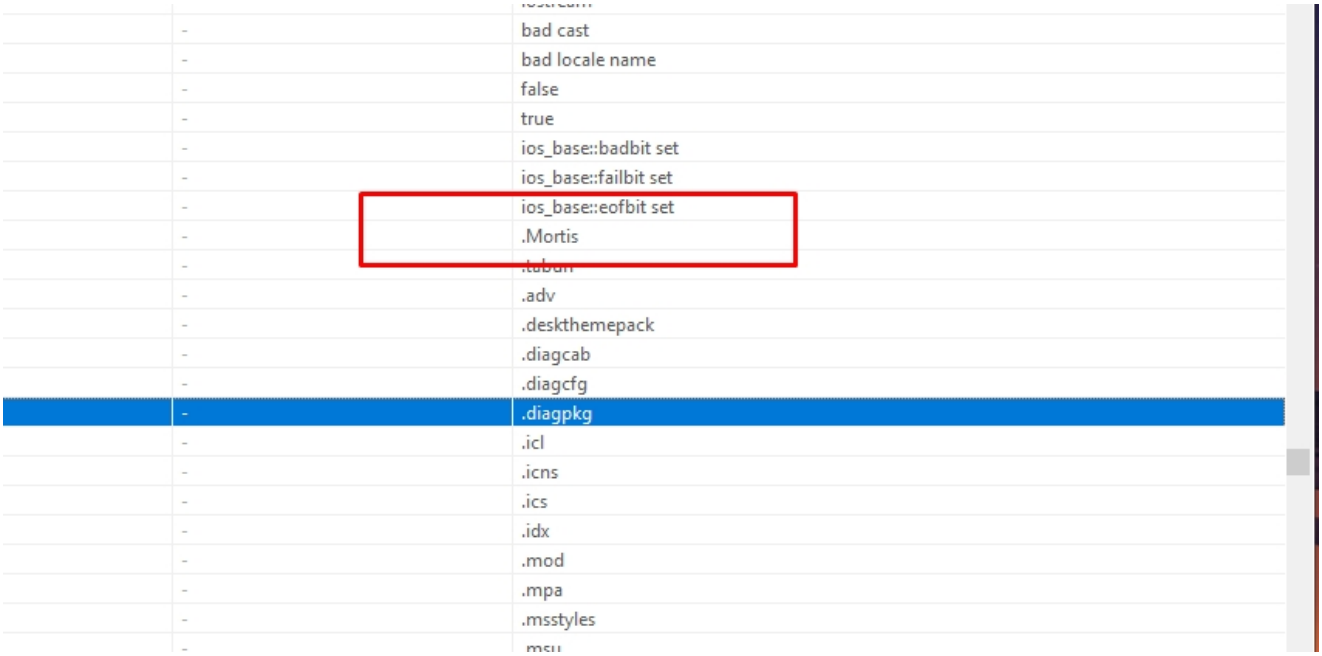
I'll use these samples in my yara rule. (You can download them from Triage)

```
a5012e20342f4751360fd0d15ab013385cecd2a5f3e7a3e8503b1852d8499819
b6a4331334a16af65c5e4193f45b17c874e3eff8dd8667fd7cb8c7a570e2a8b9
c6df9cb7c26e0199106bdcd765d5b93436f373900b26f23dfc03b8b645c6913f
dac667cfc7824fd45f511bba83ffbdb28fa69cdeff0909979de84064ca2e0283
```

Loading samples with pestudio

Let's open the samples in pestudio to find some common strings

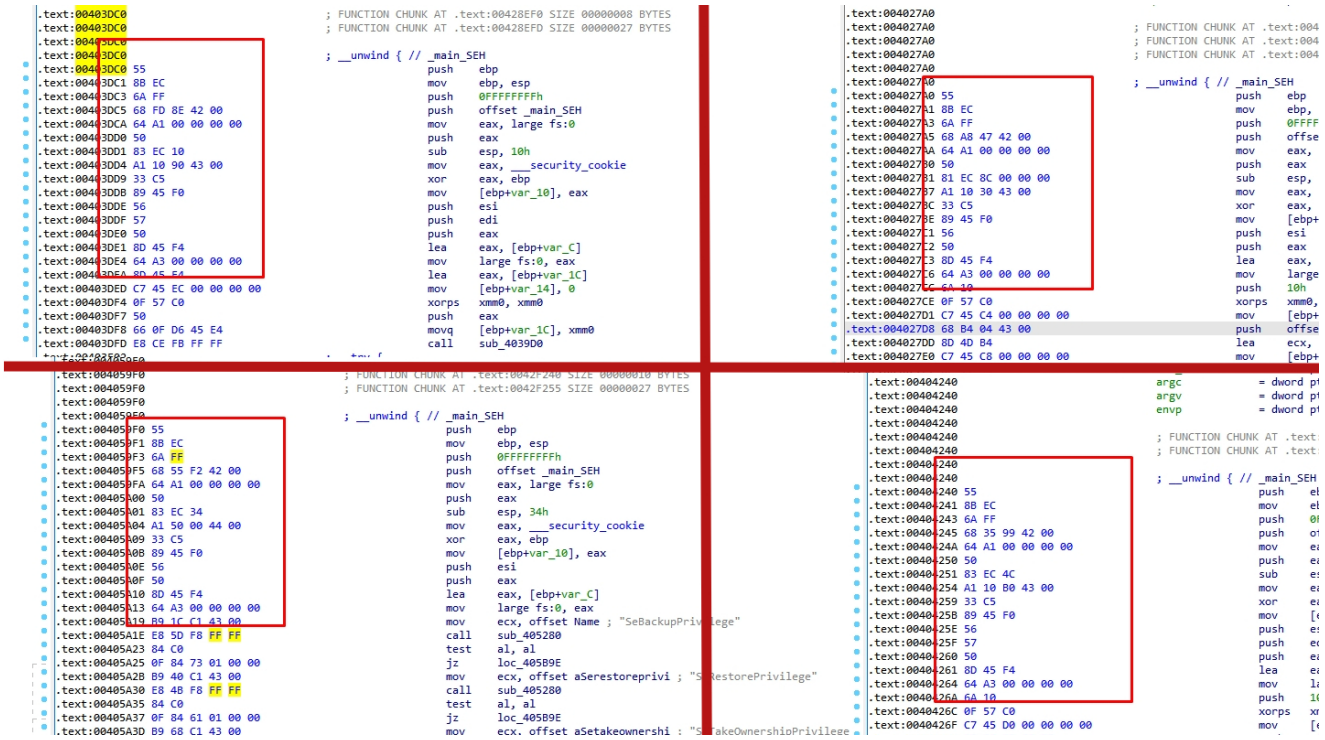
I found some here



Loading samples with IDA pro

Let’s go to IDA and search for common bytes.

I found some common bytes



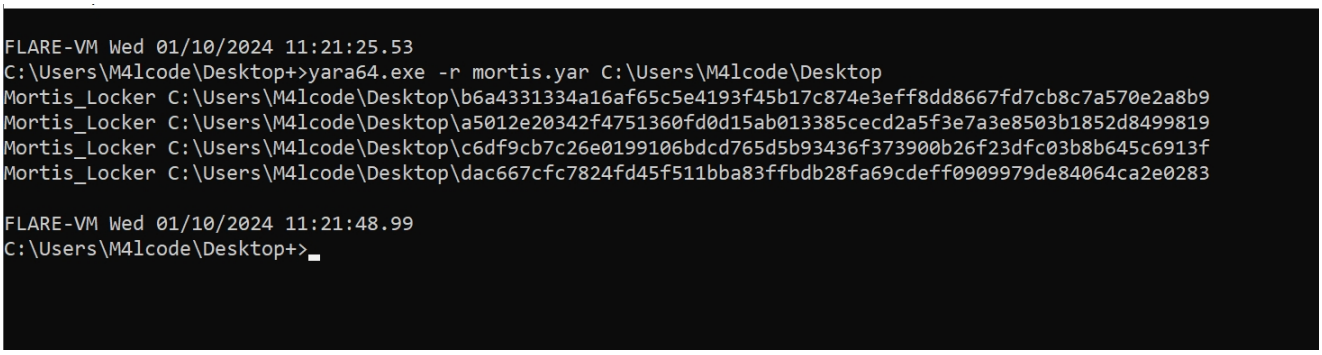
Let’s see our final yara rule.

Yara Rule

```
rule Mortis_Locker {
    meta:
        description = "Detect Mortis Locker ransomware"
        author = "@M4lcode"
        date = "2024-1-10"
        hash1 = "a5012e20342f4751360fd0d15ab013385cecd2a5f3e7a3e8503b1852d8499819"
        hash2 = "b6a4331334a16af65c5e4193f45b17c874e3eff8dd8667fd7cb8c7a570e2a8b9"
        hash3 = "c6df9cb7c26e0199106bdcd765d5b93436f373900b26f23dfc03b8b645c6913f"
        hash4 = "dac667cfc7824fd45f511bba83ffbdb28fa69cdeff0909979de84064ca2e0283"
    strings:
        $s1 = "\\MortisLocker.pdb" ascii
        $s2 = {55 8B EC 6A FF 68 ?? ?? 42 00 64 A1 00 00 00 00 50 8? EC}
        $s3 = ".Mortis" ascii
    condition:
        uint16(0) == 0x5A4D and 2 of them
        or all of them
}
```

Testing Yara Rule

It works!



Thanks For Reading :)