Fake CAPTCHA Campaign on Arabic Pirated Movie Sites Delivers Lumma Stealer

Ahmed Farouk · Follow
3 min read · Oct 21, 2024

Summary

I began investigating an incident where **multiple users** in **various environments** executed the **same PowerShell command** via the **Run dialog**. Upon further analysis, I discovered a **fake CAPTCHA campaign** targeting visitors of **Arabic pirated movie websites**, including but not limited to:

1. **Egybest**
2. **Halacima**
3. **Shahedpro**
4. **Mycima**

The threat actor appears to have **purchased ads** on these and other similar

This **blog** is **broken** down into **3 main sections**

1. **Technical Details**
2. **Detection Opportunities**
3. **Hunting Hypothesis**

1. Technical details

My investigation revealed that several users visited the same fake verification CAPTCHA site, which they were redirected to from various pirated movie hosting platforms, such as Egybest, Halacima, Shahedpro, and Mycima. These ads led users to a page where they were instructed to open the Run dialog and execute a PowerShell command.

The PowerShell command that the user was asked to paste and run was:

This script performed three main actions:

1. Downloaded a ZIP file and extracted it into the AppData directory.
2. Executed the extracted setup.exe (1e5e32c35af6bebeb800083f5c637cb03fac3e37), a legitimate Adobe-signed AcroBroker.exe that is vulnerable to **DLL side-loading.**
3. Added persistence by modifying the Run key in the Windows registry.

The dropped files included legitimate DLLs and a malicious **sqlite.dll** (Lumma Stealer) (bfc1422d1c5351561087bd3e6d82ffbad5221dae), which was loaded via DLL side-loading to execute the malware.

2. Detection Opportunities

The `Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU` registry key logs all commands executed via the Run dialog. We can create a detection rule based on activity recorded in this key.

The rule below detects any PowerShell execution from the run dialog with suspicious commands, such as hidden executions `-W Hidden`, `iex`, or

```
    selection_sus_keywords:
        Details|contains:
            - 'http'
            - 'ftp'
            - 'Hidden'
            - 'iex'
            - ' -e '
            - ' -en '
            - ' -enc '
            - ' -enco'
            - ' -ec '
    condition: all of selection_*

falsepositives:
    - Unknown
level: high
```

3. Hunting Hypothesis

Similarly, we can develop a broader threat hunting rule based on the RunMRU key to detect any threat actors employing the same technique, possibly using different images, commands, or methods not covered in the detection rule above.

```
title: Suspicious Commands in RunMRU key
id: f9d091f6-f1c7-4873-a24f-050b4a02b4dd
status: test
description: |
    Detects suspicious commands in the RunMRU registry key, commonly used by threat
    into pasting and executing malicious commands in the Run dialog, often disguised
references:
    - https://www.forensafe.com/blogs/runmrukey.html
    - https://medium.com/@shaherzakaria8/downloading-trojan-lumma-infostealer-throug
author: Ahmed Farouk
date: 2024/10/21
tags:
    - detection.threat-hunting
```

Sigma Rules

--

Written by Ahmed Farouk

6 Followers

Follow

Help Status About Careers Press Blog Privacy Terms Text to speech Teams