**Logo**

# Cyber Malware Analysis Report

**Cyber Security Incident Response Team: Hayder Sarhan**

**16/09/2024**

# Executive Summary

**Provide an executive summary about the malware here.**

# Case Details

| | |
|---|---|
| **Date** | **16/09/2024** |
| **Analyst** | **Hayder Sarhan** |

**Sample information**

| | |
|---|---|
| **File name** | **98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe** |
| **File size** | **638,1 kB** |
| **File type** | **exe** |
| **MD5** | **DD4F1C6A119D800280DCCC0F7A53EC18** |
| **SHA1** | **48278C926D2E97905A791C018004D07175919D1F** |
| **SHA256** | **98270FC07F41677127B9490D540AA5C4AA32B78706A2C288E93BBF9D95E5D901** |
| **Packer / compiler info** | |
| **Compile time** | **120 s** |

# Case Specific Requirements

- **Request?** (Who/what brought your attention to the malware? Maybe it was detected on your SIEM platform?)
    a. I was looking for a malware that can hide itself in an environment and take advantage of it, since a lot of people face this problem me included
- Where was the sample found? (You can state a fictitious endpoint)
    a. it was found on MalwareBazaar
- Why is this sample interesting?
    a. For the technologies it uses(SnakeKeylogger)

# Standing Information Requirements

- **What functionality does the malware provide the attacker once it is installed successfully?**
    a. Having access to user's data by stealing it from the apps caches and recording the keyboard input of the user

- **Is this known malware affecting multiple organizations, malware targeting the Software Health Industry or are there indicators that this is a tailored attack?**
    - **a.** It can affect anyone who has online accounts. It's a tool to steal people's personal data and possibly money.

- **What indicators of compromise are associated with this malware?**
    - a. It's hard for such malware to be detected since it can exclude itself from the list of threats on the system, and it doesn't require a lot of computational power to do its job. On of the few ways to detected it is when the user notices credential theft.

- **Does the malware maintain persistence on the victim system? If so, how?**
    - a. Yes, the malware tries to manipulate the Windows defender system by excluding itself from being a malicious threat

- **Which application, service or other vulnerability does this malware exploit?**
    - a. Is it related to an existing CVE?
        I couldn't find an existing CVE for it but it can't be considered a 0-day vulnerability, since it's a common malware that can be traced back to 2020, with over 14k samples found on MalwareBazzar
    - **b.** Does a patch exist? There can be found
    - **c.** Does Endpoint Protection protect against this attack? Can help yes

- **What remediation options are available to effectively remove the malware and return the system to a secure state?**
    - a. Remove the causing threat from the device.
    - b. Clearing the caches of all the apps that can store online accounts information.
    - c. Change the passwords for all the accounts that could be stored on the device.

## Additional Information / Examiner Notes

## IOCs

- **Main object: 98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901.exe**
- **md5: dd4f1c6a119d800280dccc0f7a53ec18**
- **sha1: 48278c926d2e97905a791c018004d07175919d1f**
- **sha256: 98270fc07f41677127b9490d540aa5c4aa32b78706a2c288e93bbf9d95e5d901**

## Attachments

ANY.RUN analysis