

SikoMode Exfiltrator Malware

Sept 2022 | Cuteness-overload

# Table of Contents

[Table of Contents 2](#_Toc113906818)

[Executive Summary 3](#_Toc113906819)

[High-Level Technical Summary 4](#_Toc113906820)

[Basic Static Analysis 6](#_Toc113906821)

[Basic Dynamic Analysis 6](#_Toc113906822)

[Advanced Static Analysis 9](#_Toc113906823)

[Advanced Dynamic Analysis Error! Bookmark not defined.](#_Toc113906824)

[Indicators of Compromise 11](#_Toc113906825)

[Network Indicators 11](#_Toc113906826)

[Host-based Indicators 12](#_Toc113906827)

[Rules & Signatures 13](#_Toc113906828)

[Appendices Error! Bookmark not defined.](#_Toc113906829)

[A. Yara Rules **Error! Bookmark not defined.**](#_Toc113906830)

[B. Callback URLs **Error! Bookmark not defined.**](#_Toc113906831)

[C. Decompiled Code Snippets **Error! Bookmark not defined.**](#_Toc113906832)

# Executive Summary

|  |  |
| --- | --- |
| SHA256 hash | 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E |
| MD5 hash | B9497FFB7E9C6F49823B95851EC874E3 |

SikoMode is an exfiltrator/stealer malware first submitted to VirusTotal on the 11th of January 2022 with auto-deletion capabilities. It is a portable executable written in NIM, made to run on Windows x64 systems. It consists of a single payload to be executed in the context of an already infected PC or via a phishing campaign. Symptoms of infection include frequent beaconing to hxxp://cdn.altimiter.local/ as well as the appearance of a passwrd.txt file in C:\Users\Public\.

It seems to only target a specific file named cosmo.jpeg, but future iterations could very well take aim at the entire hard drive

YARA signature rules are attached in Rules & Signatures. Malware sample and hashes have been submitted to VirusTotal for further examination.

# High-Level Technical Summary

SikoMode is a one stage data exfiltrator with auto-deletion and RC4 encryption capabilities.

Once executed it will attempt to contact its initial callback domain “hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/”.

If a connection is established, it will then attempt to connect to a second domain, to which exfiltration of data will also go: “hxxp://cdn.altimiter.local/”.

If that connection is established it will exfiltrate the data packet by packet using RC4 encrypted, base64 encoded GET request strings.

Ex: hxxp://cdn.altimiter.local/feed ?post=A8E437E8F0367592569A2870BBD….

Once the data is fully exfiltrated, the program will auto-delete itself using a function dubbed “Houdini”.

At every stage of the process, this malware will check for connectivity to the above domains. If a connection can no longer be established, it will auto-delete.

# Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

Hashes were extracted at the very beginning:

|  |  |
| --- | --- |
| SHA256 hash | 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E |
| MD5 hash | B9497FFB7E9C6F49823B95851EC874E3 |

Analysis was straightforward as no signs of obfuscation were found. The string output gave interesting results.

(Floss and Jupyter Notebook were used)

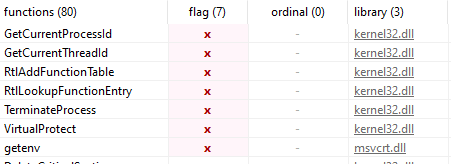
|  |
| --- |
| @C:\Users\Public\passwrd.txt |
| stdlib\_httpclient.nim.c |
| httpclient.nim |
| @httpclient.nim(1082, 13) `not url.contains({'\r', '\n'})` url shouldn't contain any newline characters |
| @http://cdn.altimiter.local/feed?post= |
| passwrd\_\_sikomode\_14 |
| @:houdini |
| @Nim httpclient/1.6.2 |
| @Desktop\cosmo.jpeg |
| @SikoMode |
| @Mozilla/5.0 |

The file is a 64bit executable written in nim, which we can defer based off of the strings found as well as the function names found in Cutter.

It is not a packed executable as the Virtual size and Raw Data size are very similar.



PEview flagged a few suspicious IATs, including GetCurrentProcessId and GetCurrentThreadId.



# Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

## Initial Detonation (No Inetsim)

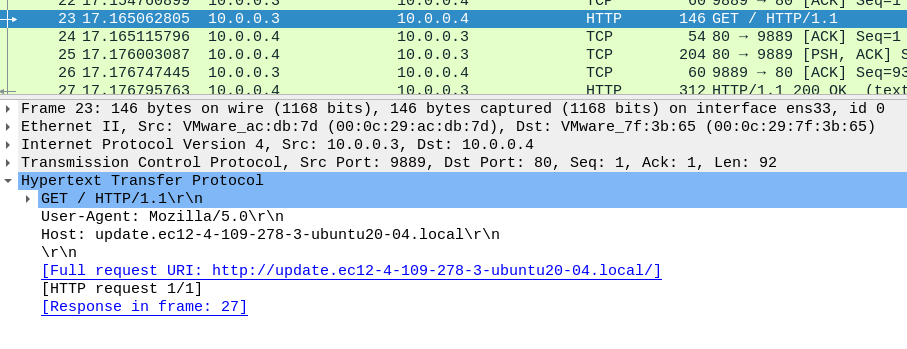
On execution, the program tries reaching out to the initial callback domain, then auto-deletes since no connection has been established.

No child processes are detected.

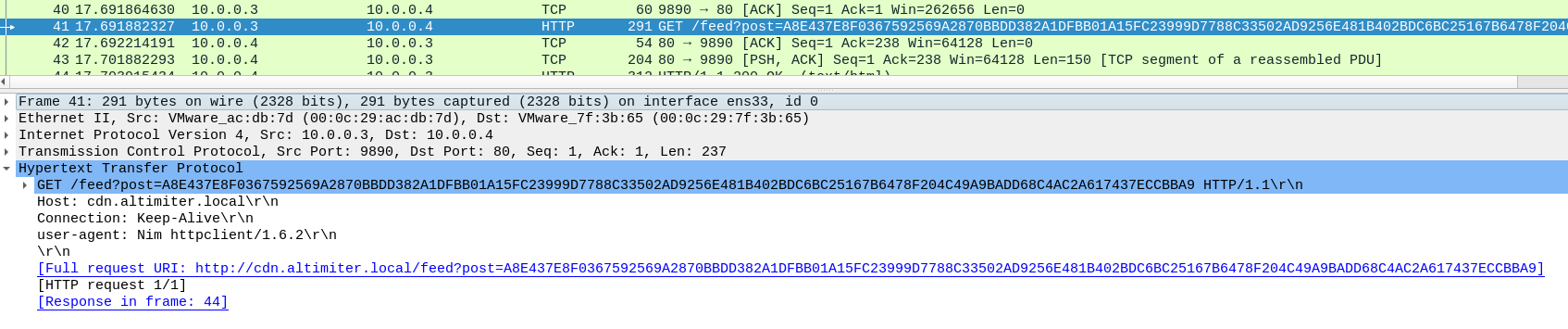
## Initial Detonation (With Inetsim)

On this execution a lot more happens immediately. While there still are no child processes, the initial callback domain is reached.

hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/

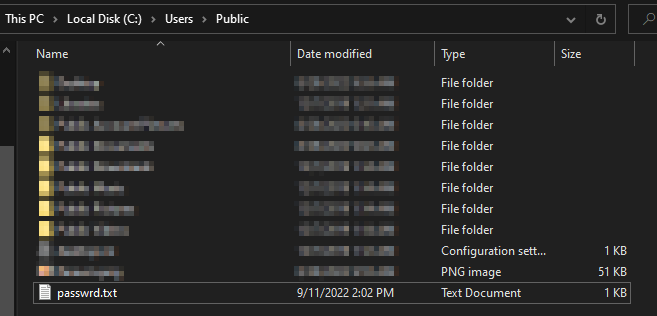


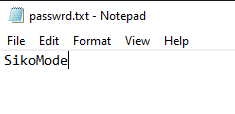
Repeated connections and GET requests to hxxp://cdn.altimiter.local/ are then made with ever changing base64 encoded strings.



All connections to the above url follow the “url/feed?post=(base64 string)” schema, suggesting this is the data exfiltration method used. We will later find out that the base64 string has been previously RC4 encoded.

A “password.txt” file appeared in C:/Users/Public/, the content of which is “SikoMode”, which we therefor used to name this malware sample.





If Inetsim is cut off at any point during this process, the malware will auto-delete.

## PC Restart

We tried detecting any possible persistence mechanisms. On PC reboot and login, no persistence was noticed.

* No suspicious autruns
* No registry modifications
* No further connection attempts to either of the domains

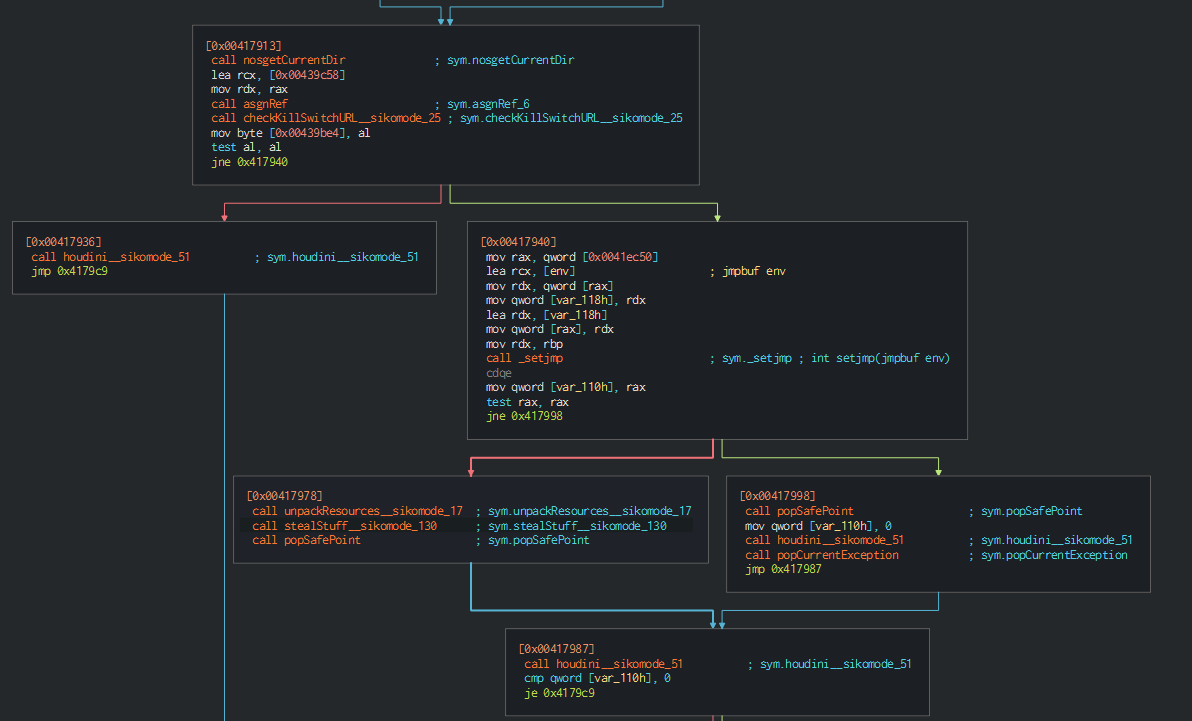
# Advanced Analysis

{Screenshots and description about findings during advanced analysis}

Advanced Analysis reveals little more than we already discovered so far.

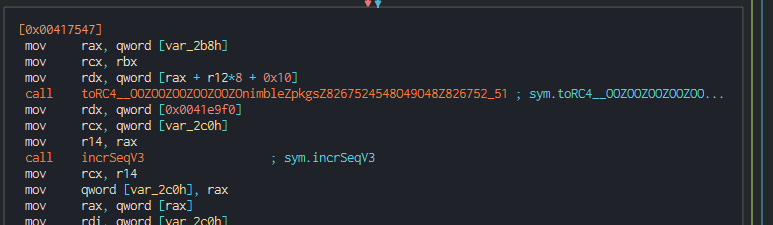
However, the graph view of the program finally gives us an insight on the mysterious “houdini” string we saw in the string output.

We can also notice the recurring use of this “Houdini\_\_sikomode\_51” function. This is the auto-deletion function built into the binary that will be called if a connection is not established.



“checkKillSwitchURL\_\_sikomode\_25” is the check to the initial callback domain: hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/

We also see an interesting function called “stealStuff\_\_sikomode\_130”. If we follow it through, we eventually find a “toRC4…” function that is in charge of encrypting the data to, you guessed it, RC4.



# Indicators of Compromise

## Network Indicators

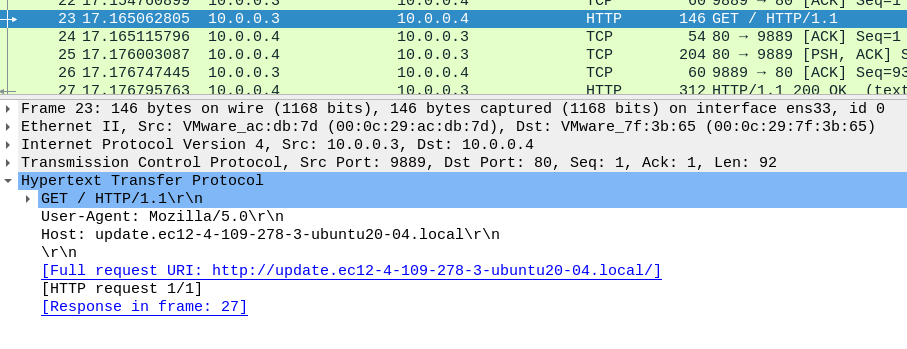


Fig1. Initial callback domain connection

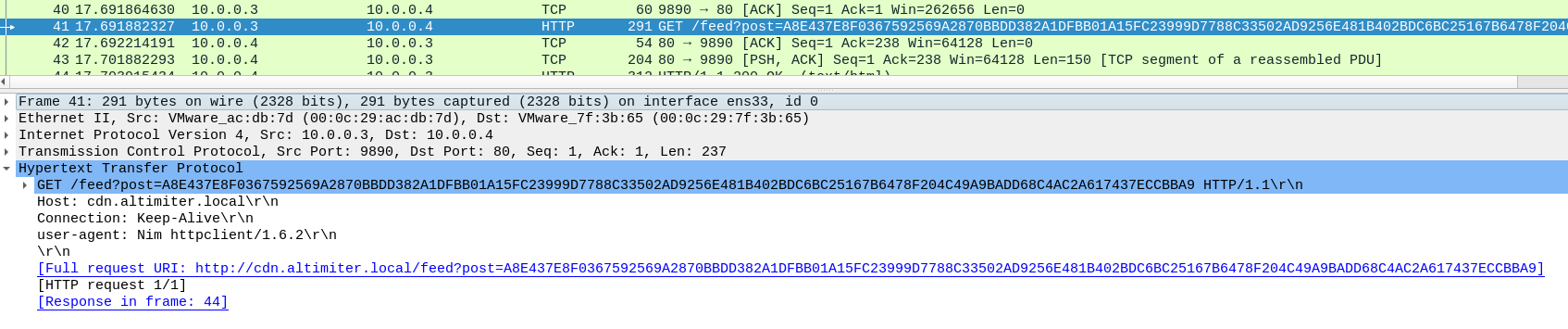


Fig2. Data exfiltration domain

## Host-based Indicators

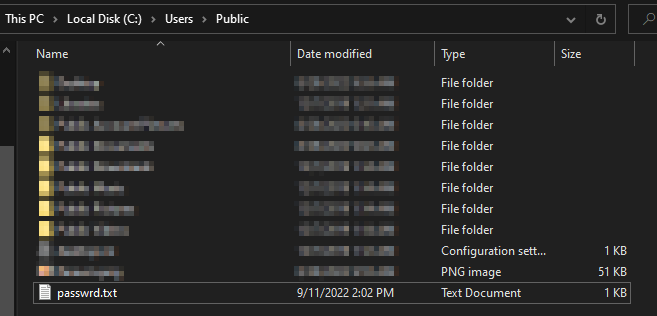


Fig3. Password.txt file

# Rules & Signatures

SikoMode.yara available on my github:

*https://github.com/Cuteness-overload/PMAT-Final*

All encountered samples of this malware met a few identical criteria.

* The use of C:/Users/Public/password.txt
* Hxxp://cdn.altimiter.local
* SikoMode as a password
* Written in nim
* All portable executables
* The “Houdini” string

rule SikoMode {

    meta:

        last\_updated = "2022-09-11"

        author = "Cuteness-overload"

        description = "A rule set for the detection of the SikoMode Malware"

        sha256 = "3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E"

    strings:

*// Fill out identifying strings and other criteria*

*$string1* = "houdini" ascii

*$string2* = "C:\\Users\\Public\\passwrd.txt" ascii

*$string3* = "http://cdn.altimiter.local/" ascii

*$string4* = "SikoMode" ascii

*$string5* = "nim" fullword ascii

    condition:

*// Not checking for filesize in case of obfuscation in later iterations*

        uint16(0) == 0x5A4D and

        uint32(uint32(0x3C)) == 0x00004550 and

*$string1* and *$string2* and *$string3* and *$string4* and *$string5*

}