Practical Malware Analysis & Triage

Malware Analysis Report

Siko Mode Exfiltration Malware

Jun 2022 | b0ot3nd1ng | v1.0

Table of Contents

Executive Summary

SHA256 hash	3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E
MD5 hash	B9497FFB7E9C6F49823B95851EC874E3

Siko Mode is an exfiltrator malware sample first identified on June 20, 2022. It is a Nim-compiled exfiltrator that runs on the x64 Windows operating system.

It is a Malware that will steal data from your machine by sending it back to a callback URL encoded in RC4

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

High-Level Technical Summary

Siko Mode requires an active internet connection to execute. It starts off by making a DNS query to a first callback server (which also acts a kill-switch URL) – and once that callback server returns a valid response – it will proceed with stealing or exfiltrating the RC4 encoded data using a fixed key in a text file that is also generated by the malware at run-time passwrd.txt.

In this case, it targets the cosmo.jpeg file located on the desktop.

After execution or if the program encounters any error or exceptions like inactive DNS servers or a machine that is offline, it will delete itself from disk via Houdini.

MalwareComposition

Siko Mode consists of the following components:

File Name	SHA256 Hash
sikomode.exe	3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E
passwrd.txt	1eebfcf7b68b2b4ffe17696800740e199acf207afb5514bc51298c2fe758441

sikomode.exe

The initial executable that runs and makes a call to the urls within the program to steal data and send it back as encoded data

passwrd.txt:

A text file that contains the encryption key

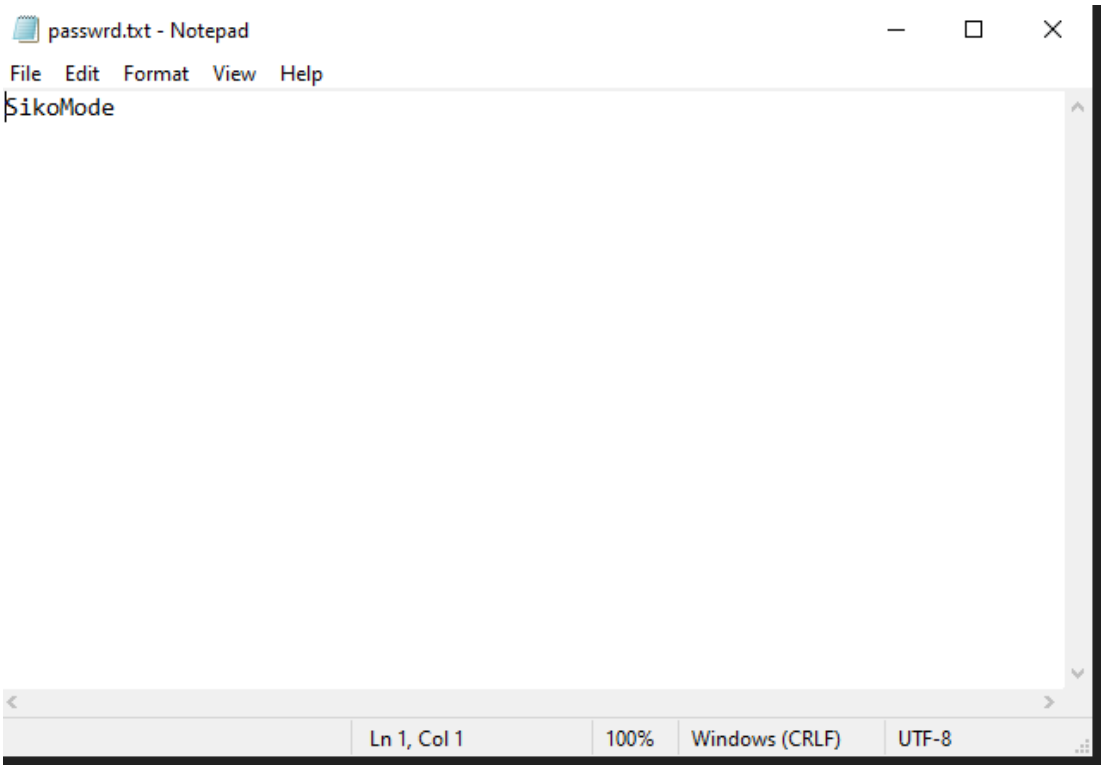

Fig 1: Text file containing encryption key.

Basic Static Analysis

VirusTotal and Floss

VirusTotal	Identified the sample as a Trojan Backdoor
Strings/floss	@:houdini @Authorization @Host @Transfer-Encoding @Content-Type @Content-Length @http://cdn.altimiter.local/feed?post= @Nim httpclient/1.6.2 @Desktop\cosmo.jpeg @SikoMode @Mozilla/5.0 @C:\Users\Public\passwrd.txt

Basic Dynamic Analysis

Network-based Indicators

DNS queries to two domains:

1. update.ec12-4-109-278-3-ubuntu20-04.local
2. cdn.altimiter.local

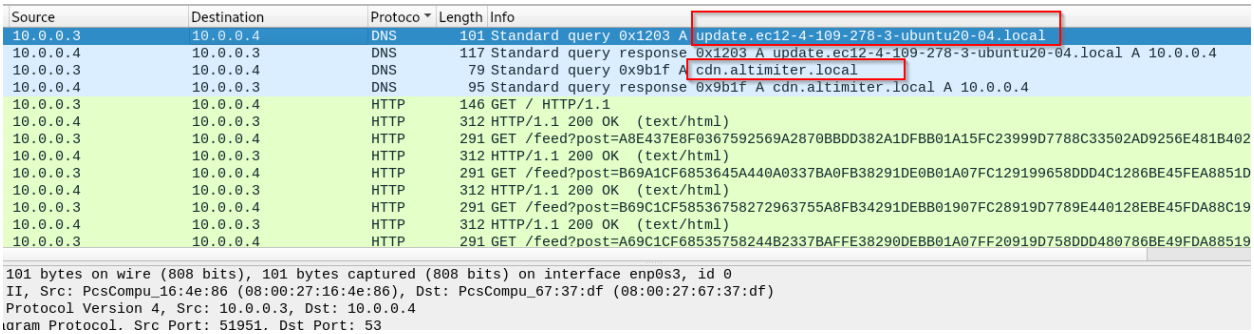

Fig 2: DNS queries to two(2) URLs

Makes a GET request to (does this in a loop until program stops execution):
http://cdn.altimiter.local/feed?post=ENCRYPTEDINFOHERE

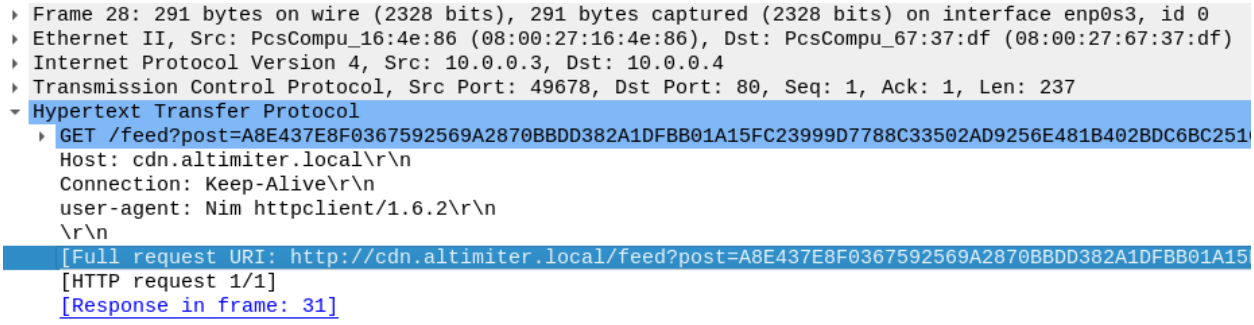

Fig 3: HTTP Get Requests to cdn.altimeter.local

Host-based Indicators

Procmon shows that SikoMode.exe is trying to manipulate files

- Passwrd.txt
- Cosmo.jpeg

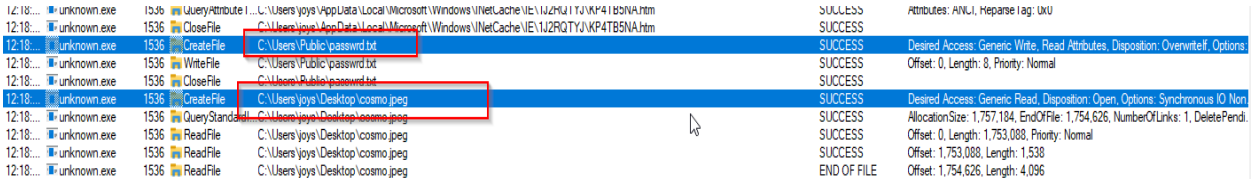

Fig 4: Creation of passwrd.txt and manipulation of cosmo.jpeg

Advanced Static Analysis

(via Cutter)

Initial investigation will show that the program will need to make a call to the function checkKillSwitchUrl – if it does not get a response, then it will proceed to delete itself by calling Houdini functionalities.

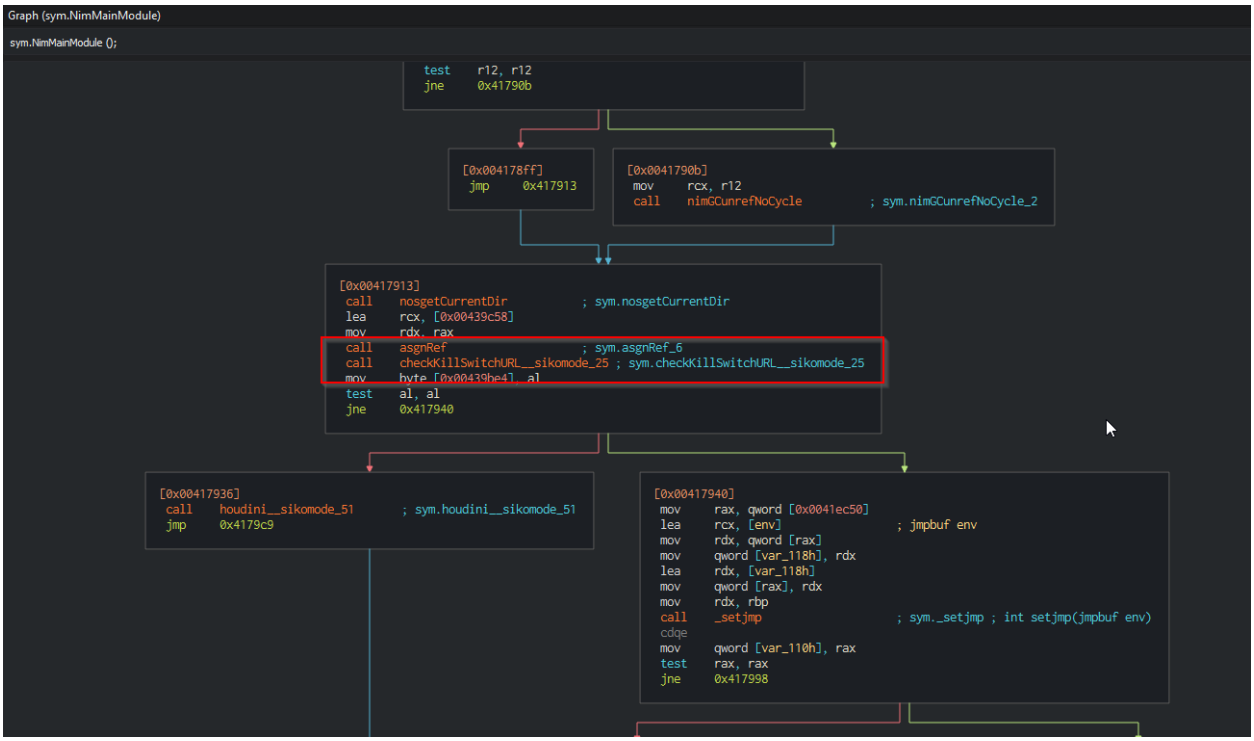

Fig 5: Program flow for checking kill-switch URL

If it does get a response from the first callback URL, it will proceed with the main functionality of the program which is to read, encode and send back data to the second callback URL

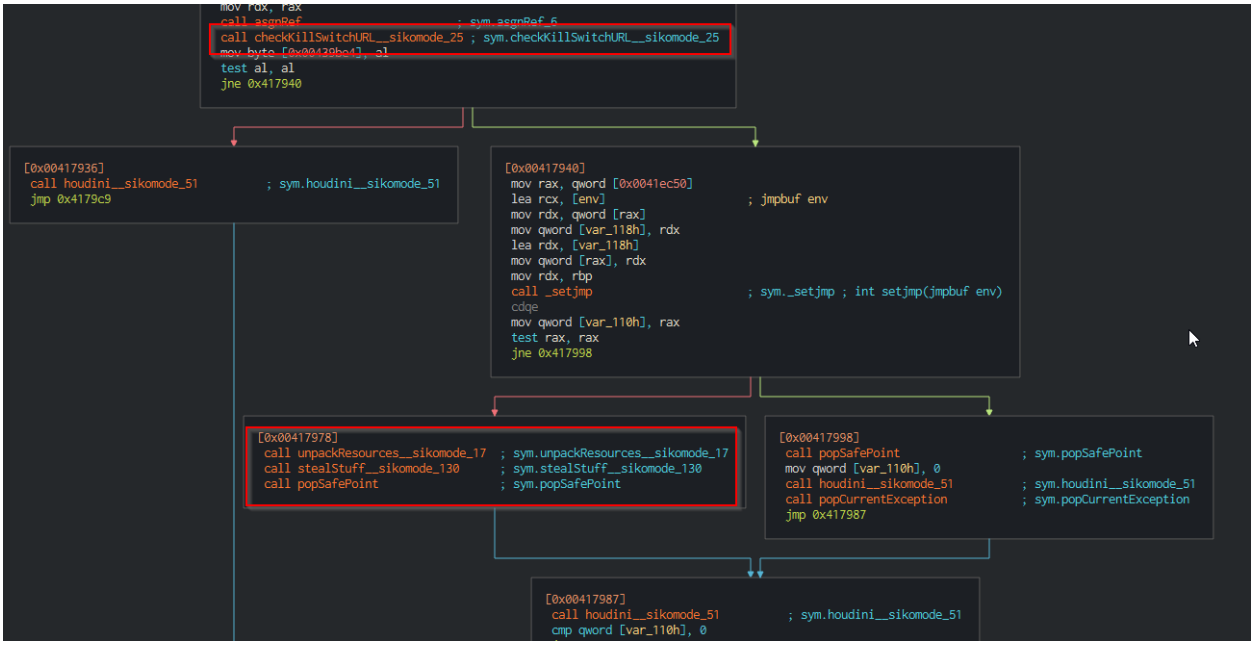

Fig 6: Program flow for steal and send data functionalities

Advanced Dynamic Analysis

No other pertinent details acquired from Advanced Dynamic Analysis

Indicators of Compromise

The full list of IOCs can be found in the Appendices.

Network Indicators

Sure-fire way to tell is through your network packet sniffing. If it sends out a GET request to the 2nd callback url multiple/infinite times.

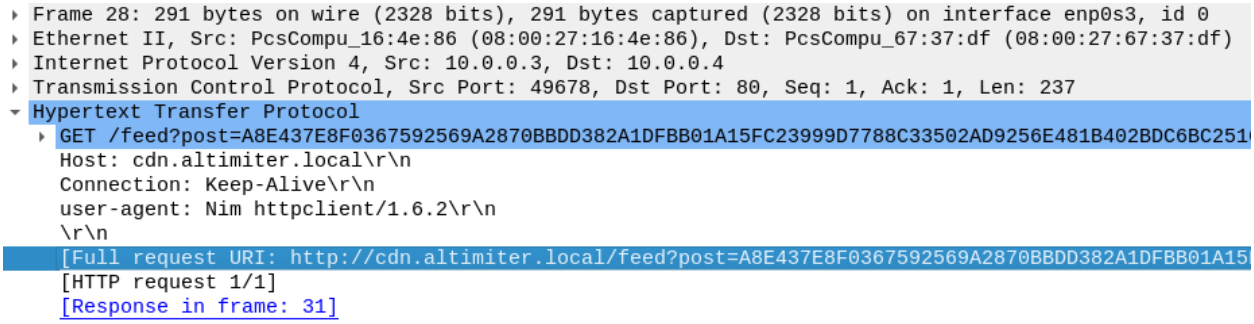

Fig 7: WireShark Packet Capture of GET Request

Host-based Indicators

Procmon will show that the executable creates a passwrd.txt encryption key file in the Users\Public folder

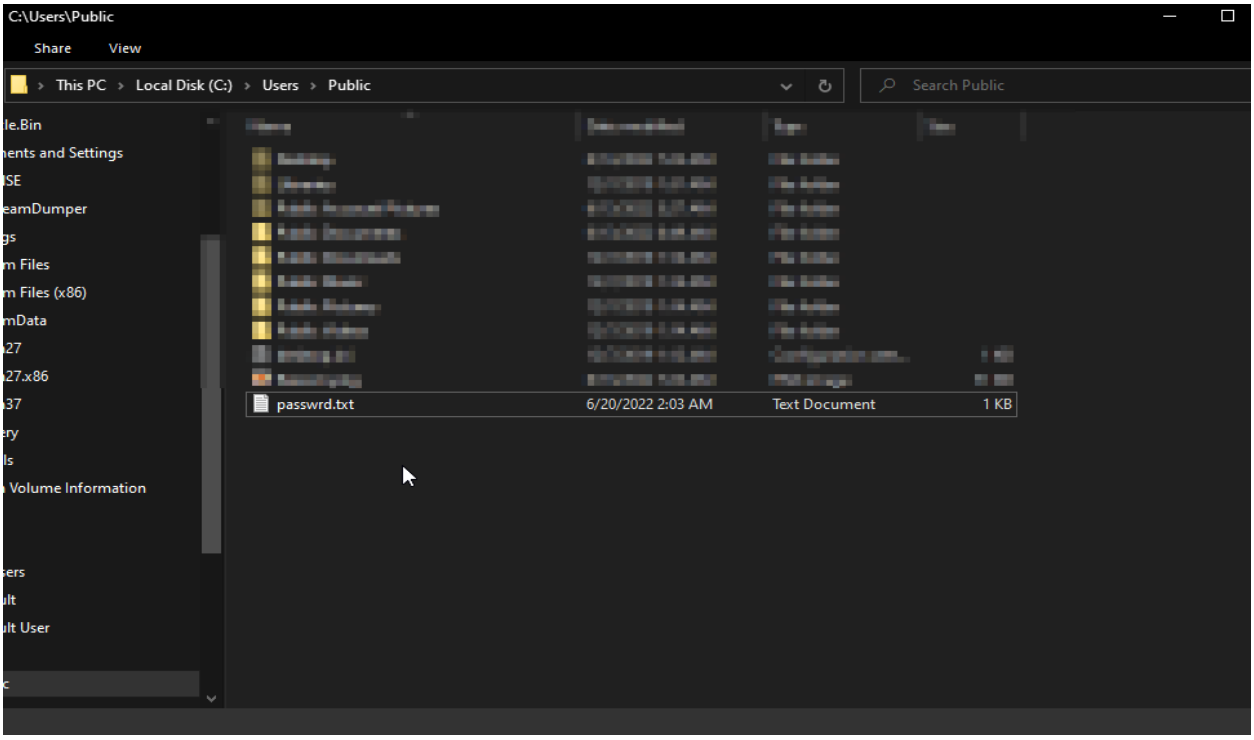

Fig 8: passwrd.txt on Users\Public folder

Rules & Signatures

A full set of YARA rules is included in Appendix A.

Appendices

A. Yara Rules

```
rule Exfil_YARA {

  meta:
    last_updated = "2022-06-20"
    author = "b0ot3nd1ng"
    description = "A sample Yara rule for Siko Mode Exfiltrator Malware"

  strings:
    // Fill out identifying strings and other criteria
    $string1 = "passwrd.txt" ascii
    $string2 = "nim"
    $PE_magic_byte = "MZ"

  condition:
    // Fill out the conditions that must be met to identify the binary
    $PE_magic_byte at 0 and //if it finds MZ at first byte
    ($string1 and $string2)
}
```

B. Callback URLs

Domain	Port
update.ec12-4-109-278-3-ubuntu20-04.local	53
cdn.altimiter.local	80