Icon

Description automatically generated

Practical Malware Analysis & Triage

Malware Analysis Report

SikoMode Malware

July 2023 | Harrison Louis | v1.0

# Table of Contents

[Table of Contents 2](#_Toc141616668)

[Executive Summary 3](#_Toc141616669)

[High-Level Technical Summary 4](#_Toc141616670)

[Malware Composition 5](#_Toc141616671)

[Basic Static Analysis 6](#_Toc141616672)

[Basic Dynamic Analysis 7](#_Toc141616673)

[Advanced Static and Dynamic Analysis 8](#_Toc141616674)

[Indicators of Compromise 10](#_Toc141616675)

[Network Indicators 10](#_Toc141616676)

[Host-based Indicators 10](#_Toc141616677)

[Rules & Signatures 12](#_Toc141616678)

[Appendices 13](#_Toc141616679)

[A. Yara Rule 13](#_Toc141616680)

[B. Callback URLs 13](#_Toc141616681)

# Executive Summary

|  |  |
| --- | --- |
| SHA256 hash | 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E |

SikoMode is malware that can exfiltrate files from the user’s machine. We first identified this malware in July 2023. It is a Nim compiled binary that runs on x64 Windows machines. It consists of a single binary which is distributed by a threat actor sending out malicious links. Symptoms of infection include extensive GET requests sent to a malicious C2 and an encryption password written to disk.

We have labelled this malware as SikoMode due to the password identified for encryption as well as references to “SikoMode” found within the code.

YARA signature rules are attached in Appendix A.

# High-Level Technical Summary

SikoMode is a single executable binary. It first attempts to establish contact with a kill switch domain (update[.]ec12-4-109-278-3-ubuntu20-04[.]local) before proceeding with its next stage objectives. After confirming this domain is active, it identifies a file called cosmo.jpeg on the user’s desktop. Once this file has been located, the malware grabs a copy of its bytes, encrypts it with the RC4 algorithm, Base64 encodes the encrypted output and utilizes HTTP GET requests to exfiltrate the data to a C2 (cdn[.]altimeter[.]local). After successful exfiltration, the binary deletes itself.

# Malware Composition

SikoMode is composed of a single 64 bit executable. The sample our team was able to recover was titled “unknown.exe” and it was downloaded after a user clicked a malicious link.

|  |  |
| --- | --- |
| File Name | SHA256 Hash |
| unknown.exe | 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E |

# Basic Static Analysis

This file was observed in the wild before it was identified within our environment.

A screenshot of a computer

Description automatically generated

Figure : VirusTotal results

After utilizing FLOSS to dump the strings, we identified a multitude of strings that indicate this file may have been originally written in Nim and has the capabilities to make network connections. Additionally, we saw file paths and a domain within the strings.

|  |
| --- |
| @HTTP/  @Proxy-Authorization: basic  @Connection: Keep-Alive  @Host:  @ HTTP/1.1  @User-Agent  @tables.nim(1144, 13) `len(t) == L` the length of the table changed while iterating over it  @iterators.nim(240, 11) `len(a) == L` the length of the seq changed while iterating over it  @; filename="  @iterators.nim(249, 11) `len(a) == L` the length of the seq changed while iterating over it  @SSL support is not available. Cannot connect over SSL. Compile with -d:ssl to enable.  @https  @No uri scheme supplied.  @httpclient.nim(1144, 15) `false`  @Transfer-Encoding  @httpclient.nim(1082, 13) `not url.contains({'\r', '\n'})` url shouldn't contain any newline characters  @http://cdn.altimiter.local/feed?post=  @Nim httpclient/1.6.2  @Desktop\cosmo.jpeg  @SikoMode  @iterators.nim(240, 11) `len(a) == L` the length of the seq changed while iterating over it  @ccc  @Mozilla/5.0  @C:\Users\Public\passwrd.txt |

# Basic Dynamic Analysis

We first ran the binary in an isolated VM and found that it quickly deleted itself. We then tried again after utilizing a second VM running INetsim to simulate an internet connection and found that the binary stayed on the machine and made a call to update[.]ec12-4-109-278-3-ubuntu20-04[.]local.



Figure : DNS Request

After this, we observed an extensive amount of HTTP GET requests that seemed to be used to send Base64 encoded strings to a C2 server at cdn[.]altimeter[.]local.

A screen shot of a computer

Description automatically generated

Figure : GET Requests

Within Process Monitor, we observed the application writing a file to C:\Users\Public\passwrd.txt. Inside this text file was the string “SikoMode”. We also observed the binary interacting with the cosmo.jpeg image on the Desktop.

A screenshot of a computer

Description automatically generated

Figure : File Operations

# Advanced Static and Dynamic Analysis

Walking through the disassembled code, we find the binary runs a function called “checkKillSwitchURL”. Based on the return value, the binary will either call a function called “houdini”, which we have identified as a function that kills and deletes the binary, or run further through the program to carry out the malicious functionality.

A screenshot of a computer screen

Description automatically generated

Figure : Disassembled code

Walking through the “stealStuff” function, we observe the binary utilizing the nim “toRC4” library to encrypt data.

A computer code on a black background

Description automatically generated

Figure : RC4 Encryption Function

Then we see the binary call some SSL and HTTP functions to exfiltrate the encrypted and encoded data.

A screen shot of a computer code

Description automatically generated

Figure : HTTP Functions

No matter what path the binary takes through execution, any execution without interruption will lead to the “houdini” function being called resulting in the binary disappearing from the machine.

# Indicators of Compromise

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

## Network Indicators

Two malicious domains have been identified in relation to this malware:

A close-up of a number

Description automatically generated

DNS Request : update[.]ec12-4-109-278-3-ubuntu20-04[.]local

A screen shot of a computer

Description automatically generated

DNS Request : cdn[.]altimeter[.]local

## Host-based Indicators

A trademark of this infection is the passwrd.txt file with the string “SikoMode” located in C:\Users\Public

A screenshot of a computer

Description automatically generated

# Rules & Signatures

Through our research we have identified some unique IOCs related to the SikoMode malware. We have created a YARA rule, which can be found in Appendix A, and the known Callback URLs, which can be found in Appendix B.

# Appendices

## Yara Rule

rule SikoMode {

    meta:

        last\_updated = "2023-07-30"

        author = "Harrison Louis"

        description = "This rule can be used to identify the SikoMode malware"

    strings:

        $string1 = "SikoMode"

        $string2 = "nim"

        $string3 = "HTTP"

        $string4 = "C:\\Users\\Public\\passwrd.txt"

        $string5 = "cdn.altimiter.local"

        $PE\_magic\_byte = "MZ"

    condition:

        $PE\_magic\_byte at 0 and

        all of ($string\*)

}

## Callback URLs

|  |  |
| --- | --- |
| Domain | Port |
| *update[.]ec12-4-109-278-3-ubuntu20-04[.]local* | 53 |
| cdn[.]altimeter[.]local | 53, 80 |