Icon

Description automatically generated

Yazeed Al-Zwiri

Malware Analysis Report

Siko Mode Challenge

Self-Deleting Data Exfiltration Malware

Sep 23, 2022 | SHOBAKIY | v1.0

# Table of Contents

[Table of Contents 2](#_Toc114856233)

[Table of Figures 2](#_Toc114856234)

[Introduction 3](#_Toc114856235)

[Executive Summary 4](#_Toc114856236)

[High-Level Technical Summary 5](#_Toc114856237)

[Malware Composition 6](#_Toc114856238)

[Basic Static Analysis 7](#_Toc114856239)

[Basic Dynamic Analysis 8](#_Toc114856240)

[Advanced Analysis 9](#_Toc114856241)

[Advanced Analysis (Cont.) 10](#_Toc114856242)

[Indicators of Compromise 11](#_Toc114856243)

[Host-based Indicators 11](#_Toc114856244)

[Rules & Signatures 12](#_Toc114856245)

[Appendices 13](#_Toc114856246)

[A. Yara Rules 13](#_Toc114856247)

[B. Callback URLs 13](#_Toc114856248)

# Table of Figures

[Figure 1: Floss result helped me to know it's a Nim language 7](#_Toc114856162)

[Figure 2: Some Strings from PE Studio 7](#_Toc114856163)

[Figure 3: Wireshark packets 8](#_Toc114856164)

[Figure 4: Wireshark packets 8](#_Toc114856165)

[Figure 5: Strings from x64 dbg helped me to know it's a Nim language 9](#_Toc114856166)

[Figure 6: Strings from Cutter helped me to know it's a Nim language 9](#_Toc114856167)

[Figure 7: Procmon result filtered by operation is create file 10](#_Toc114856168)

[Figure 8: Procmon result filtered by operation is create file inerests create 10](#_Toc114856169)

[Figure 9: passwrd.txt 11](#_Toc114856170)

# Introduction

This document is a sample report completed as a final project for a course from TCM Security (<https://academy.scm-sec.com> ), titled “Practical Malware Analysis and Triage” presented by Matt Kiely.

The course was a well prepared and presented entry level course. it was a realistic adroitly, and artfully contrived scenario with a very functional well controlled malicious file.

This was a thoroughly excited practical exercise that left me feeling to move forward with my education in this area.

Best regards,

Yazeed Al-Zwiri

# Executive Summary

**Hash Values:**

|  |  |
| --- | --- |
| Md5 | B9497FFB7E9C6F49823B95851EC874E3 |
| Sha256 | 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E |

Siko Mode is a self-deleting data exfiltration malware package. Siko Mode can target specific locations on a compromised machine, and it is a self-deleting when tasks are completed or cannot make a successful connection to the initial callback URL or interrupted in the middle of its exfiltration routine.

Symptoms of attack may be noticed in reduced system performance because of continuous data exfiltration. Another indicator is the presence of a file named “passwrd.txt” located at C:\Users\Public\passwrd.txt.

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

|  |  |
| --- | --- |
| File type | x64 (64-bit CPU) executable file. |
| Written with | NIM language. |
| **Virus Total result** | 41 of 71 security vendors and no sandboxes flagged this file as malicious. |

# High-Level Technical Summary

Siko Mode consists of a single stage. While Analysis progress it was located at C:\Users\Public\

The first attempt to contact its callback URL (hxxp://update.ec12-4-109-278-3-ubuntu20-04.local) and if there is a successful response it will go to the second attempt to contact the exfiltration URL (hxxp://cdn.altimiter.local).

Unknown.exe

No

Initial callback

Delete your self

Yes

Exfiltration

Yes

Interrupt

Delete your self

No

No

Finished

Yes

# Malware Composition

Siko Mode malware consists of a single file unknown.exe with the following characteristics:

File type; x64 (64-bit CPU) executable file written in NIM language.

Exfiltration data encrypted with RC4.

**Hash Values**

|  |  |  |
| --- | --- | --- |
| Md5 | B9497FFB7E9C6F49823B95851EC874E3 | |
| Sha256 | 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E | |
| Sha1 | 6C8F50040545D8CD9AF4B51564DE654266E592E3 | |
|  | |  |
| **Virus Total** | 41 of 71 security vendors and no sandboxes flagged this file as malicious. | |
| Ad-Aware | Gen:Variant.Tedy.75424 | |
| Ikarus | Virus.Win32.Meterpreter | |

Siko Mode also writes a file named password to the file system located at: C:\users\public\password.txt containing the encryption key values.

There are three circumstances where the malware will delete itself:

1. If the data exfiltration is completed.
2. If there is no response of initial callback address.
3. If there is an interrupted during the exfiltration process.

# Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

During the basic static analysis process, I found some sort of string information are suspicious and came with malware products. In the next steps of analysis, I was able to reveal strings that help identify that the malware was written in the NIM programming language in figure 1, there are some strings were only visible for us at runtime while working in x64 dbg, and Cutter. There were a few interesting strings available from PE Studio seen in figure 2 below.

Graphical user interface, text, application, email

Description automatically generated

Figure : Floss result helped me to know it is a Nim language

**![Table

Description automatically generated]()**

Figure : Some Strings from PE Studio

# Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

It was during the basic dynamic analysis that I was able to begin determining what I might have utilized inetsim and Wireshark.

![Graphical user interface, table

Description automatically generated]()

Figure : Wireshark packets

![Table

Description automatically generated]()

Figure : Wireshark packets

* This process above repeated every one second this appears to be the exfiltration taking place it is continually repeated with a different string attached each time.

# Advanced Analysis

{Screenshots and description about findings during advanced analysis}

During the advanced analysis of unknown.exe I was able to determine the language of the malware.

Oher tools give me a hint like floss, here is some indication of Nim. Look to figure 5 & 6.

Text

Description automatically generated

Figure : Strings from x64 dbg helped me to know it is a Nim language

|  |
| --- |
| Text  Description automatically generated  Figure : Strings from Cutter helped me to know it is a Nim language |
|  |

# Advanced Analysis (Cont.)

{Screenshots and description about advanced artifacts and methods}

In advanced analysis I used Procmon, and it was helpful in confirming the existence of encryption and location of the key.

![Graphical user interface

Description automatically generated with medium confidence]()

Figure : Procmon result filtered by operation is create file

**![Graphical user interface, text, application, email

Description automatically generated]()**

Figure : Procmon result filtered by operation is create file inerests create

# Indicators of Compromise

|  |  |
| --- | --- |
| URLs | hxxp://update.ec12-4-109-278-3-ubuntu20-04.local  hxxp://cdn.altimiter.local |
| Files | C:\Users\SHOBAKI\Desktop  C:\Users\Public\passwrd.txt |

## Host-based Indicators

{Description of host-based indicators}

And here is a screenshot of the text file which is create by the malware.

![A screenshot of a computer

Description automatically generated with medium confidence]()

Figure : passwrd.txt

|  |
| --- |
|  |
|  |

# Rules & Signatures

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

# Appendices

## Yara Rules

Rule Siko Mode Challenge {

    meta:

        last\_updated = "2022/09/23"

        author = "Yazeed Al-Zwiri"

        description = "A rule to suspect Siko Mode Malware"

    strings:

        // Fill out identifying strings and other criteria

        $string1 = "SikoMode" 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

        ($string1 or $string2)

}

## Callback URLs

|  |  |
| --- | --- |
| Domain | Port |
| hxxps:// update.ec12-4-109-278-3-ubuntu20-04.local | 443 |
| hxxps:// cdn.altimiter.local/fees? Post=(random string) | 443 |