

Malware Analysis Report

ImageExfil Malware

Oct 2024 | Ra-Sec | v1.0



Table of Contents

Executive Summary	3
High-Level Technical Summary	4
Malware Composition	5
ImageExfil.exe	5
Basic Static Analysis	6
Basic Dynamic Analysis	7
Advanced Static Analysis	8
Advanced Dynamic Analysis	9
Indicators of Compromise	10
Network Indicators	10
Host-based Indicators	11
Rules & Signatures	13
Appendices	14
A. Yara Rules	14
B. Callback URLs	14
C. Decompiled Code Snippets	15



Executive Summary

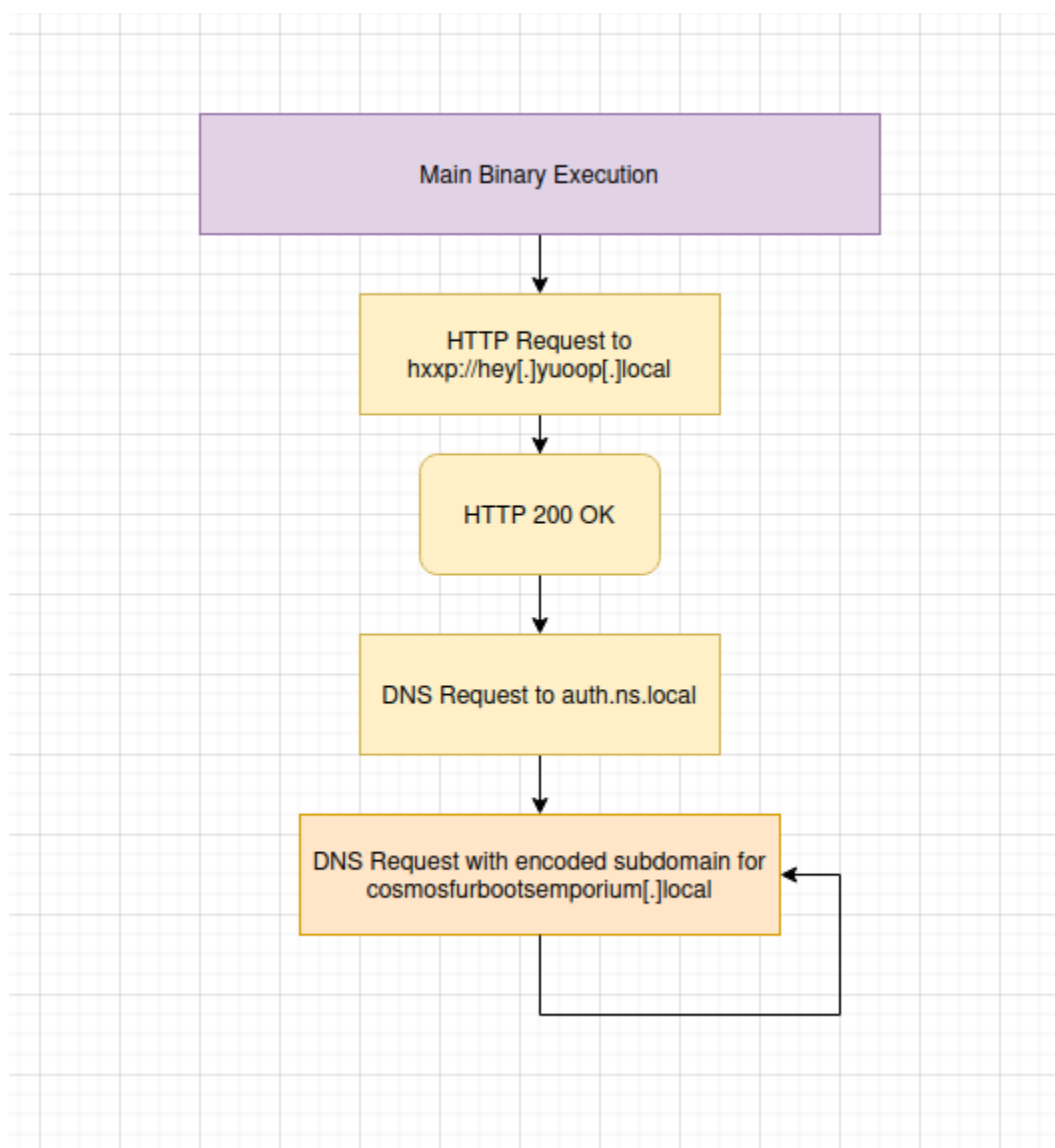
SHA256 hash	81A10784AE60A58A969E858C9C4A2AE0D4EBE46E9BD6776992461C062F70099D
-------------	--

ImageExfil Malware is a exfiltration malware sample first identified on 19th Oct 2024. It is a Nim compiled binary that run on 32/64 bit Windows operating system. It consists of one payload only which when is able to ping to a specific domain, starts with the exfiltration of cosmo.jpeg that is stored on the desktop of the system. The URLs are listed in Appendix B. A lot of encoded DNS requests are done from the endpoint and it seems to be in a constant loop.

YARA signature rules are attached in Appendix A.

High-Level Technical Summary

The binary consists of one payload. That is designed in such a way that it will exfiltrate cosmo.jpeg file that is stored on the desktop of the endpoint. If it is unable to find the file, it will simply not work. Initially it attempts to connect to a URL hey[.]youup[.]com. Once the response from the server is acquired, it sends a DNS query for auth[.]ns[.]local. Immediately after the query, it starts sending encoded DNS queries for the domain encodedtext[.]cosmosfuremporium[.]local.





Malware Composition

DemoWare consists of the following components:

File Name	SHA256 Hash
ImageExfil.exe	81A10784AE60A58A969E858C9C4A2AE0D4EBE46E9BD6776992461C062F70099D

ImageExfil.exe

The initial executable that runs all the operations after the initial execution on the endpoint



Basic Static Analysis

property	value
file	
file > sha256	81A10784AE60A58A969E858C9C4A2AE0D4EBE46E9BD6776992461C062F70099D
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	MZ
size	123392 bytes
entropy	6.402
file > type	executable
cpu	32-bit
subsystem	GUI
version	n/a
description	n/a
entry-point > first-bytes-hex	83 EC 0C C7 05 D4 22 42 00 01 00 00 00 E8 CE 7F 01 00 83 C4 0C E9 A6 FC FF FF 8D B6 00 00 00 00 83
entry-point > location	0x000014A0 (section[.text])
signature tooling	Nim Compiler

This shows that the PE is a 32-bit executable. And the MZ magic byte shows that it is indeed a PE file.

The size of the file is rather small so it is highly likely that it is not compiled in GO

```
@https
@No uri scheme supplied.
@Desktop\cosmo.jpeg
@200 OK
@Authorization
@Host
@httpClient.nim(1144, 15) `false`
@Transfer-Encoding
@Content-Type
@Content-Length
@httpClient.nim(1082, 13) `not url.contains({'\r', '\n'})` url shouldn't contain any newline characters
@Nim httpClient/1.6.2
@hwtwtwtpw:w/w/whweyww.wywowuwuwpw.wlwowcwawlw
@axuxtzhx.xnxsx.xlxoxcxaxlx
@.BcBoBsBmBoBsBfBuBrBbBoBoBtBsBeBmBpBoBrBiBuBmB.B1BoBcBaB1B
Unknown error
_matherr(): %s in %s(%g, %g) (retval=%g)
Argument domain error (DOMAIN)
Argument singularity (SIGN)
Overflow error (OVERFLOW)
```

The strings output gives out a good overview of the activity of the binary. The highlighted section gives a lot of confidence to the fact that we will be seeing some HTTP traffic. In the third row, we can see that the specific file is also mentioned. In this case it is cosmo.jpeg.



The URLs have been contaminated with a few characters which can be easily fixed.

Input + 📁 🔄 🗑️ 📄

@hwtwtwpw:w/w/whwewyw.wywowuwuwpw.wlwowcwawlw
@axuxtzhx.xnxsx.xlxocxaxlx
@.BcBoBsBmBoBsBfBuBrBbBoBoBtBsBeBmBpBoBrBiBuBmB.BlBoBcBaBlB

Output 📄 📁 🔄 🗑️ 📄

@http://hey.youup.local
@auth.ns.local
@.cosmosfurbootsemporium.local

Here we can see the URLs in clean sight.



Basic Dynamic Analysis

TCPView - Sysinternals: www.sysinternals.com

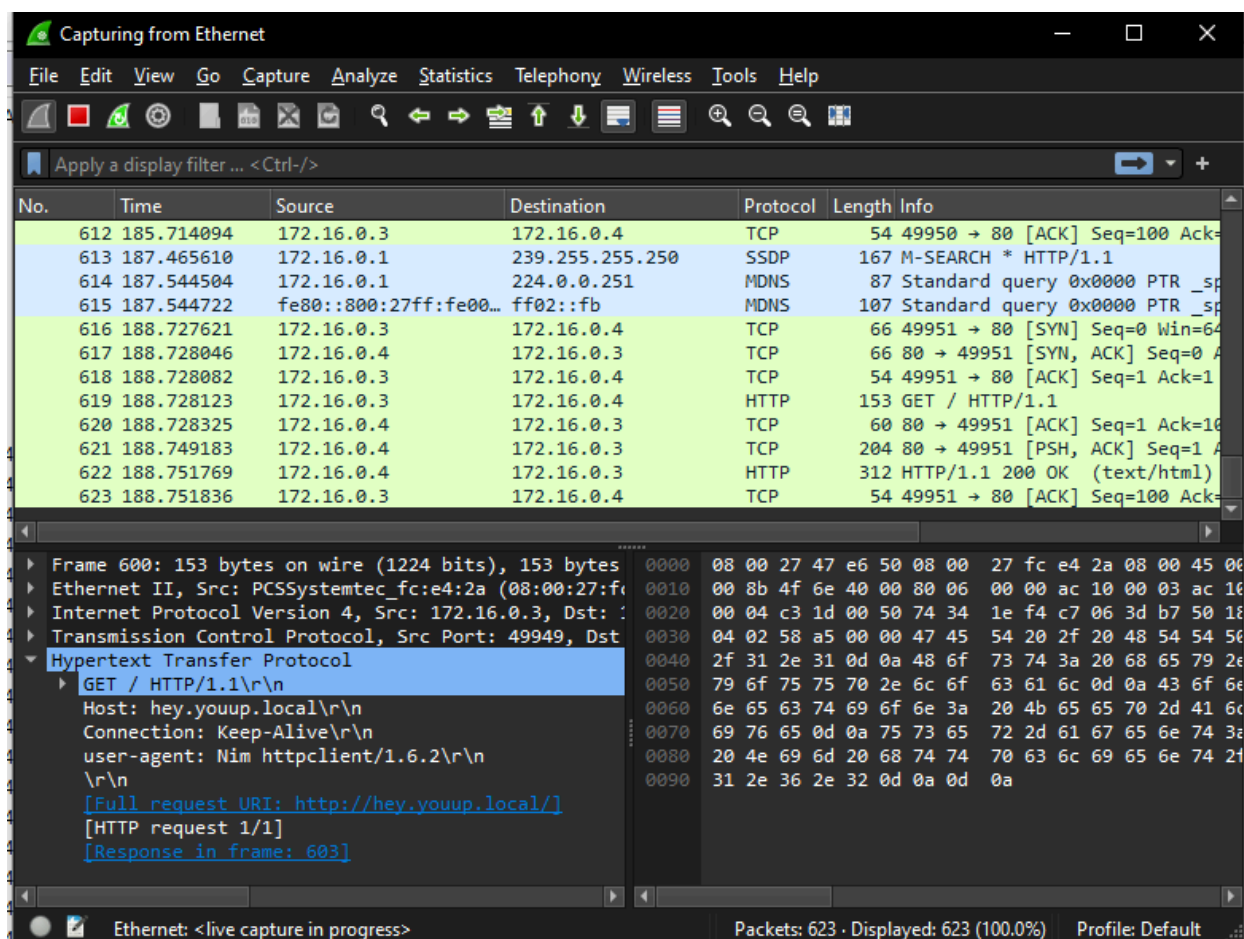
File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

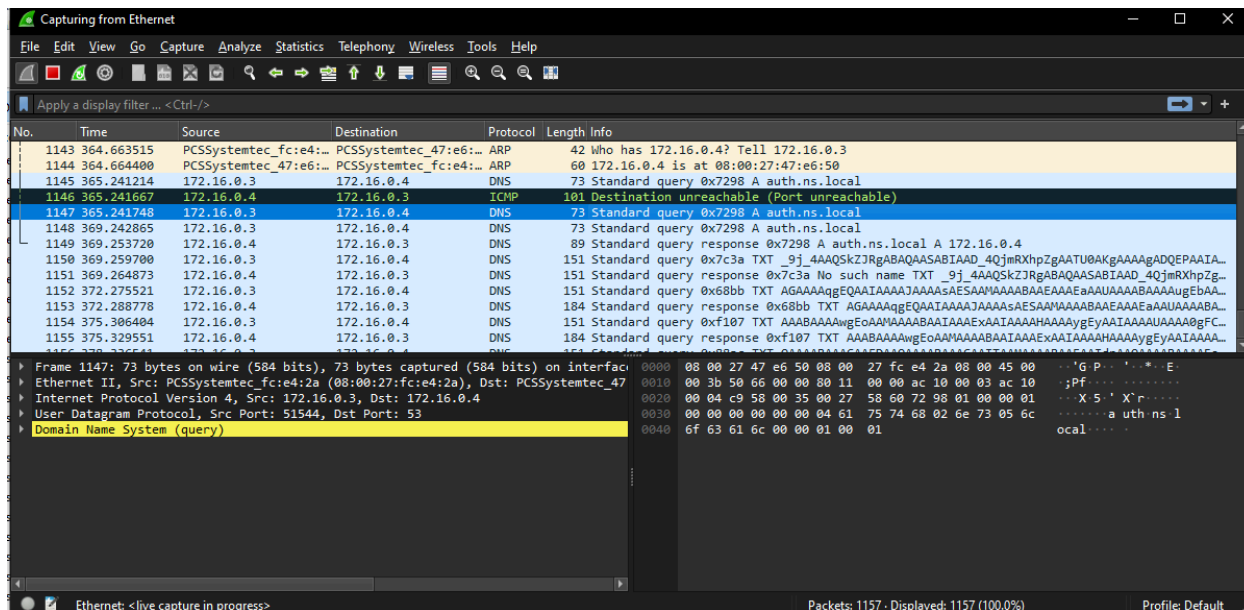
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	864	TCP	Listen	0.0.0.0	135	0.0.0.0	0	04-09-2024 17:17:49	RpcSs	
System	4	TCP	Listen	172.16.0.3	139	0.0.0.0	0	20-10-2024 10:36:12	System	
svchost.exe	1112	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	04-09-2024 04:47:56	CDPSvc	
lsass.exe	628	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	04-09-2024 17:17:49	lsass.exe	
wininit.exe	484	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	04-09-2024 17:17:49	wininit.exe	
svchost.exe	944	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	04-09-2024 17:17:50	EventLog	
svchost.exe	336	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	04-09-2024 17:17:50	Schedule	
spoolsv.exe	1900	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	04-09-2024 04:47:52	Spooler	
services.exe	620	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	04-09-2024 04:47:53	services.exe	
svchost.exe	1480	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	04-09-2024 04:47:54	PolicyAgent	
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49882	172.16.0.4	80	20-10-2024 12:21:20	Malware.unknown.exe	
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49883	172.16.0.4	80	20-10-2024 12:21:23	Malware.unknown.exe	
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49884	172.16.0.4	80	20-10-2024 12:21:26	Malware.unknown.exe	
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49885	172.16.0.4	80	20-10-2024 12:21:29	Malware.unknown.exe	
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49886	172.16.0.4	80	20-10-2024 12:21:32	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49887	172.16.0.4	80	20-10-2024 12:21:35	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49888	172.16.0.4	80	20-10-2024 12:21:38	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49889	172.16.0.4	80	20-10-2024 12:21:42	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49890	172.16.0.4	80	20-10-2024 12:21:45	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49891	172.16.0.4	80	20-10-2024 12:21:48	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49892	172.16.0.4	80	20-10-2024 12:21:51	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49893	172.16.0.4	80	20-10-2024 12:21:54	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49894	172.16.0.4	80	20-10-2024 12:21:57	Malware.unknown.exe	
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49895	172.16.0.4	80	20-10-2024 12:22:00	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49896	172.16.0.4	80	20-10-2024 12:22:03	Malware.unknown.exe	
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49897	172.16.0.4	80	20-10-2024 12:22:06	Malware.unknown.exe	1
Malware.unknown.exe	3332	TCP	Close Wait	172.16.0.3	49898	172.16.0.4	80	20-10-2024 12:22:09	Malware.unknown.exe	1

Endpoints: 64 Established: Listening: 20 Time Wait: Close Wait: 21 Update: 2 sec States: (All)

Upon execution initially we do not see any window and we can see it create requests to port 80 on the remote server. It continues to do so for each subsequent port.



On wireshark, we can see it repeatedly sending HTTP requests to the initial domain. To move it to the next stage, we have to somehow disrupt the outbound HTTP requests. It is as simple as disconnecting it from the internet for a few seconds.



After a simple disconnect and reconnect, we can see it query the second domain. And right after the response from the DNS server, we can see that it begins to exfiltrate the data using DNS queries.

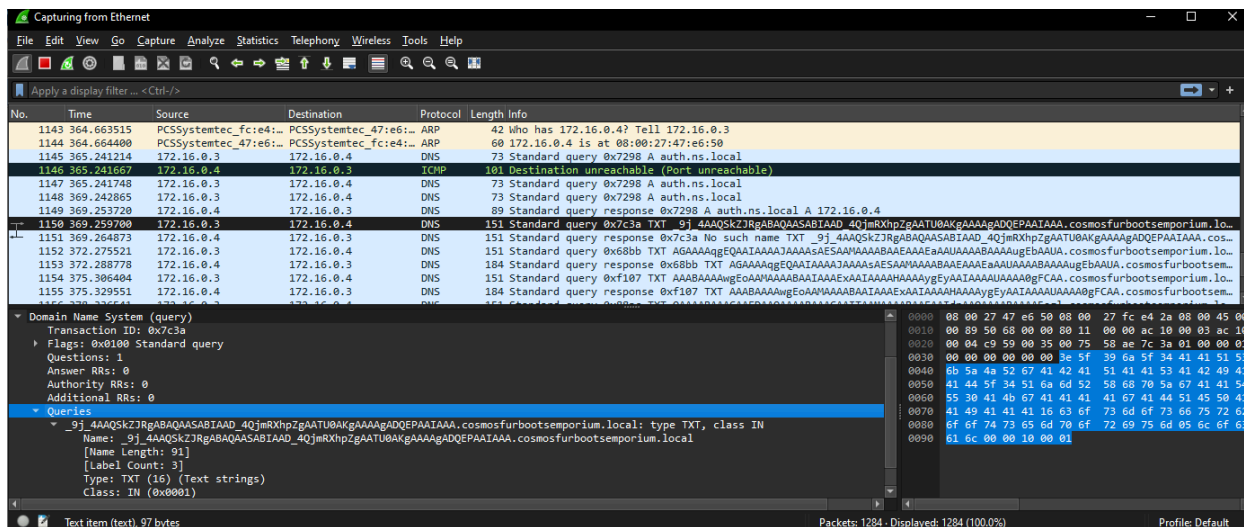


Image Exfiltration Malware
Oct 2024
v1.0



Advanced Static Analysis

```
[0x0041aaa0]
int main(int argc, char **argv, char **envp);
; var int32_t var_1ch @ stack - 0x1c
; var int32_t var_18h @ stack - 0x18
; var int32_t var_14h @ stack - 0x14
; var int32_t var_ch @ stack - 0xc
; arg int argc @ stack + 0x4
0x0041aaa0      lea     ecx, [argc]
0x0041aaa4      and     esp, 0xffffffff
0x0041aaa7      push   dword [ecx - 4]
0x0041aaaa      push   ebp
0x0041aaab      mov     ebp, esp
0x0041aaad      push   ecx
0x0041aaae      sub     esp, 0x14
0x0041aab1      call   fcn.00419440 ; fcn.00419440 ; fcn.00419440(void)
0x0041aab6      mov     eax, dword [section..data] ; 0x41b000
0x0041aabb      mov     dword [var_1ch], 0
0x0041aac3      mov     dword [var_14h], eax
0x0041aac7      mov     eax, dword [0x422318]
0x0041aacc      mov     dword [var_18h], eax
0x0041aad0      mov     eax, dword [0x42231c]
0x0041aad5      mov     dword [esp], eax
0x0041aad8      call   fcn.00419128 ; fcn.00419128
0x0041aadd      mov     ecx, dword [var_ch]
0x0041aae0      sub     esp, 0x10
0x0041aae3      leave
0x0041aae4      lea     esp, [ecx - 4]
0x0041aae7      ret
```

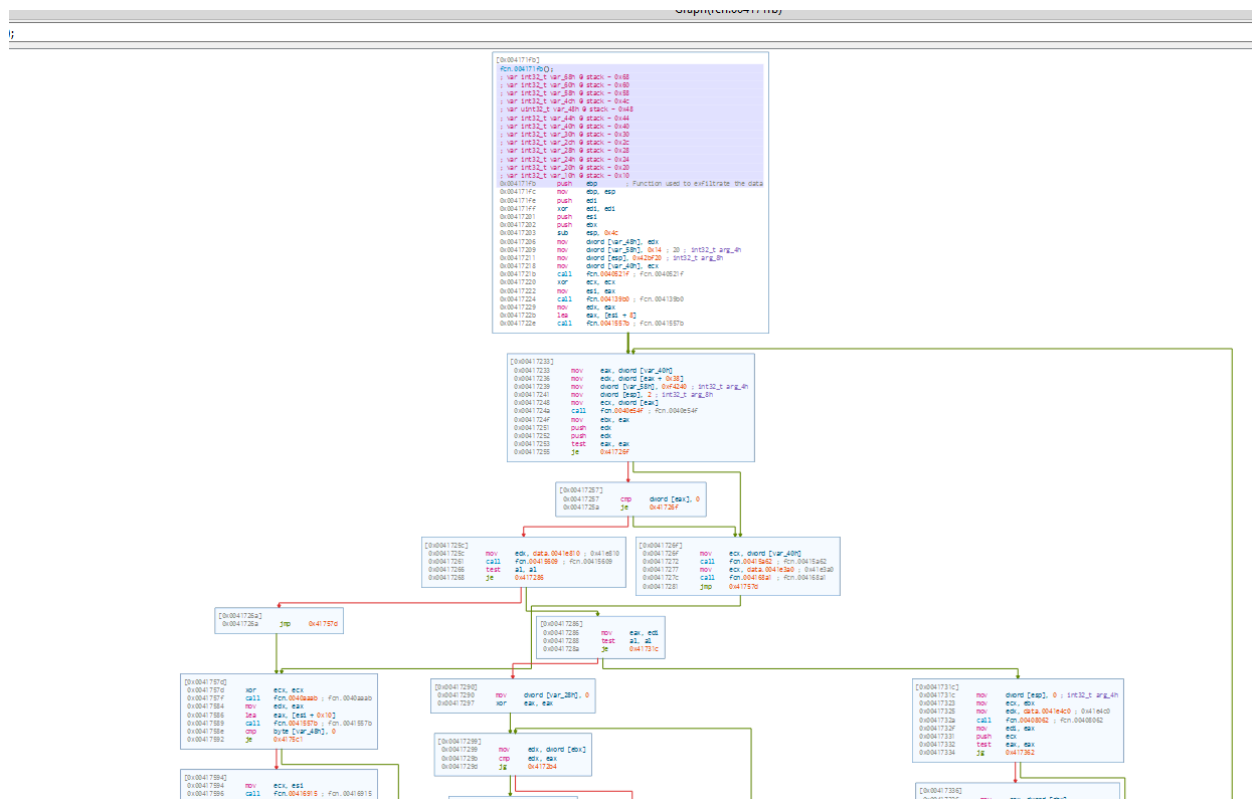
Main Function



Advanced Dynamic Analysis

The screenshot shows a debugger (x64dbg) and Wireshark. The debugger window displays assembly code for a function, with the CPU register window showing the current state. The Wireshark window shows network traffic, including a DNS query and response. The DNS query is for the domain '00000000' and the response is a standard query response.

The particular function that started exfiltrating the data as can be seen from the wireshark output and a debugger.





Indicators of Compromise

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

Network Indicators

No.	Time	Source	Destination	Protocol	Length	Info
9730	8147.976160	PCSSystemtec_fc1e4i...	PCSSystemtec_47:e6i...	ARP	42	Who has 172.16.0.4? Tell 172.16.0.3
9731	8147.976735	PCSSystemtec_47:e6i...	PCSSystemtec_fc1e4i...	ARP	60	172.16.0.4 is at 08:00:27:47:e6:50
9732	8149.492982	172.16.0.3	172.16.0.4	DNS	151	Standard query 0x9aba TXT Tk1pIzvGc0H1lQkRhfn6VT8qNFK85NaJ2kbG5qLl8rgRC1IE6rJFH5J850s.cosmosfurbootsemporium.local
9733	8149.504282	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0x9aba TXT Tk1pIzvGc0H1lQkRhfn6VT8qNFK85NaJ2kbG5qLl8rgRC1IE6rJFH5J850s.cosmosfurbootsemporium.local TXT
9734	8151.556837	PCSSystemtec_47:e6i...	PCSSystemtec_fc1e4i...	ARP	60	Who has 172.16.0.3? Tell 172.16.0.4
9735	8151.556881	PCSSystemtec_fc1e4i...	PCSSystemtec_47:e6i...	ARP	42	172.16.0.3 is at 08:00:27:fc1e:42:a
9736	8152.509704	172.16.0.3	172.16.0.4	DNS	151	Standard query 0xd61 TXT RtwakDCaM7-INGfYwFXEQ3D1Ushzku7DRkPjmljOV3Li1TXMkH8zjBoe4E1Ju.cosmosfurbootsemporium.local
9737	8152.526284	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0xd61 TXT RtwakDCaM7-INGfYwFXEQ3D1Ushzku7DRkPjmljOV3Li1TXMkH8zjBoe4E1Ju.cosmosfurbootsemporium.local TXT
9738	8155.541202	172.16.0.3	172.16.0.4	DNS	151	Standard query 0x99a1 TXT GD1Pul2bEQ709mW7JH50baWWh3pVCOPOQ80BVfX5UV7J1mLRvuUVMVc.cosmosfurbootsemporium.local
9739	8155.578105	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0x99a1 TXT GD1Pul2bEQ709mW7JH50baWWh3pVCOPOQ80BVfX5UV7J1mLRvuUVMVc.cosmosfurbootsemporium.local TXT
9740	8158.572205	172.16.0.3	172.16.0.4	DNS	151	Standard query 0xa812 TXT 66GpW4E1qq24LjkmopE86XevSuiyEw-XjgetSINjHbyWYCN6A1lqnJ8xi10fN.cosmosfurbootsemporium.local
9741	8158.580020	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0xa812 TXT 66GpW4E1qq24LjkmopE86XevSuiyEw-XjgetSINjHbyWYCN6A1lqnJ8xi10fN.cosmosfurbootsemporium.local TXT
9742	8161.602554	172.16.0.3	172.16.0.4	DNS	151	Standard query 0x24f4 TXT Rv0zibXlWrsKjJAVGwQ8mq25sdrnq2B8K559aqzqhyeah-YfNwQ4bw-y.cosmosfurbootsemporium.local
9743	8161.612003	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0x24f4 TXT Rv0zibXlWrsKjJAVGwQ8mq25sdrnq2B8K559aqzqhyeah-YfNwQ4bw-y.cosmosfurbootsemporium.local TXT
9744	8164.618030	172.16.0.3	172.16.0.4	DNS	151	Standard query 0xee67 TXT -xe1P18tQvQJHaneVg5Xqal1VoZdPugCSAq14-5pBLt5J8-FNMCssu3PFP16.cosmosfurbootsemporium.local
9745	8164.629419	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0xee67 TXT -xe1P18tQvQJHaneVg5Xqal1VoZdPugCSAq14-5pBLt5J8-FNMCssu3PFP16.cosmosfurbootsemporium.local TXT
9746	8167.633406	172.16.0.3	172.16.0.4	DNS	151	Standard query 0x9fef TXT -NAJFAEwUE_QlFhpkjyTHUDE1WKDmPx2ZoiCde9QtwtwJQPvP3qat5nvgKai.cosmosfurbootsemporium.local
9747	8167.641591	172.16.0.4	172.16.0.3	DNS	151	Standard query response 0x9fef No such name TXT -NAJFAEwUE_QlFhpkjyTHUDE1WKDmPx2ZoiCde9QtwtwJQPvP3qat5nvgKai.cosmosfurbootsemporium.local
9748	8170.659666	172.16.0.3	172.16.0.4	DNS	151	Standard query 0x33ed TXT RQGA3UVMT5RA8zvgldf13LuRUKmHVckZqD55HYHFTK2wKKAHEB338DHakGQ248.cosmosfurbootsemporium.local
9749	8170.669030	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0x33ed TXT RQGA3UVMT5RA8zvgldf13LuRUKmHVckZqD55HYHFTK2wKKAHEB338DHakGQ248.cosmosfurbootsemporium.local TXT
9750	8173.682711	172.16.0.3	172.16.0.4	DNS	151	Standard query 0xe900 TXT vU10ZSe95y10Z2Xg1D3ae7R5P5a_LnvT12kJO5KURwGyV4puFXmLrTugJ3nD...cosmosfurbootsemporium.local
9751	8173.693642	172.16.0.4	172.16.0.3	DNS	151	Standard query response 0xe900 No such name TXT vU10ZSe95y10Z2Xg1D3ae7R5P5a_LnvT12kJO5KURwGyV4puFXmLrTugJ3nD...cosmosfurbootsemporium.local
9752	8176.696566	172.16.0.3	172.16.0.4	DNS	151	Standard query 0xb8ba TXT 1x60L1NWdKYCpXgd396KCBxulCiqACmH3e90Kgt1Ti01JdtvSpB65-60aGzKwA.cosmosfurbootsemporium.local
9753	8176.706477	172.16.0.4	172.16.0.3	DNS	184	Standard query response 0xb8ba TXT 1x60L1NWdKYCpXgd396KCBxulCiqACmH3e90Kgt1Ti01JdtvSpB65-60aGzKwA.cosmosfurbootsemporium.local TXT
9754	8178.388790	172.16.0.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 9736: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface \Device\NPF_{6B29FD98-6280-435D-A95D-6D567C}

Ethernet II, Src: PCSSystemtec_fc1e4:2a (08:00:27:fc1e:42:a), Dst: PCSSystemtec_47:e6:50 (08:00:27:47:e6:50)

Internet Protocol Version 4, Src: 172.16.0.3, Dst: 172.16.0.4

User Datagram Protocol, Src Port: 62525, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xd61

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

RtwakDCaM7-INGfYwFXEQ3D1Ushzku7DRkPjmljOV3Li1TXMkH8zjBoe4E1Ju.cosmosfurbootsemporium.local: type TXT, class IN

[Response In: 9737]

0000 08 00 27 47 e6 50 00 00 27 fc e4 2a 08 00 45 00 ... G P ... E

0010 00 80 60 12 00 00 00 11 00 00 ac 10 00 03 ac 10 ... i ...

0020 00 04 44 2d 00 35 00 75 50 aa 0d 01 01 00 00 01 ... 5 u X a

0030 00 00 00 00 00 3e 52 74 76 77 61 6b 44 43 61 ... PR twakDCa

0040 4d 37 2d 31 4e 47 46 79 77 46 5b 45 51 33 44 69 ... H7-INGfYwFXEQ3D1

0050 55 73 60 7a 6b 55 37 44 52 6b 50 6a 6d 6c 6a 4f ... Ushku7D RkPjmljO

0060 5b 33 4c 31 7a 54 58 4d 0b 68 42 7a 6d 42 6f 65 ... 3Li1TXMkH8zjBoe

0070 34 45 69 4a 75 16 63 6f 73 6d 6f 73 66 75 72 62 ... 4E1Ju:co smofurb

0080 6f 6f 74 73 65 6d 70 6f 72 69 75 6d 05 6c 6f 63 ... ootsemporium:loc

0090 61 6c 00 00 10 00 01 ... al:....

DNS Requests for cosmosfurbootsemporium.local with encoded data as subdomain



The DNS request to the auth[.]ns[.]local domain after the HTTP traffic was disrupted

The initial HTTP requests to the domain

v1.0



Rules & Signatures

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



Appendices

A. Yara Rules

```
rule Yara_ImageExfil {  
  meta:  
    last_updated = "2024-11-02"  
    author = "RA"  
    description = "A Yara rule for ImageExfil Malware"  
  strings:  
    $string1 = "cosmo.jpeg"  
    $string2 = "n1m"  
    $string3 = "@hwtwtwpw:w/w/whwewyw.wywowuwuwpw.wlwowcwawlw"  
    $string4 = "@axuxtzhx.xnxsx.xlxocxaxlx"  
    $string5 = "@.BcBoBsBmBoBsBfBuBrBbBoBoBtBsBeBmBpBoBrBiBuBmB.BlBoBcBaBlB"  
    $PE_magic_byte = "MZ"  
  condition:  
    $PE_magic_byte at 0 and  
    ($string1 and $string2 and $string3 and $string4 and $string5)  
}
```

B. Callback URLs

Domain	Port
hxxps://hey.yuooop.local	80
hxxps://auth.ns.local	53
hxxp://cosmosfuremoprium.local	53