

Digital Forensics

Forensic Report - "obiwan.exe" Analysis

Brief Summary of Information

A packet capture file named "example1.pcap" was analyzed to investigate suspicious network activity. The file was opened in Wireshark, which revealed an HTTP request from a local IP address to download a file called "obiwan.exe" from a remote server. After running this executable, further tools like Process Explorer and TCPView showed it initiating multiple connections.

Wireshark analysis of the network traffic from "obiwan.exe" uncovered some unusual HTTP requests to "www.umd.edu." In the Conversations tab, two identical messages were sent asking for help from "obiwan-kenobi," saying he was their only hope. The server responded with a 301-redirection status code. Further investigation identified "obiwan.exe" as a Python script, with seven total requests sent in the background to "www.umd.edu," all receiving 301 responses.

The Packet Counter confirmed seven requests, while examination of exported objects revealed no additional content due to the redirections. Overall, this analysis uncovered suspicious activity from a Python executable repeatedly sending distress signal-like messages to a website, presenting an intriguing investigation scenario. The network forensics methodology provided insights into the execution and network behavior.

Tools Used in the Investigation Process

The following tools were employed in this investigation:

Wireshark: An open-source packet analyzer used to inspect the recorded network packets. Wireshark enabled analysis of the HTTP requests and responses associated with the "obiwan.exe" executable, as well as the overall network communications.

Repository #1 Analysis of 'obiwan.exe'

Analysis

HTTP Request and Download of "obiwan.exe"

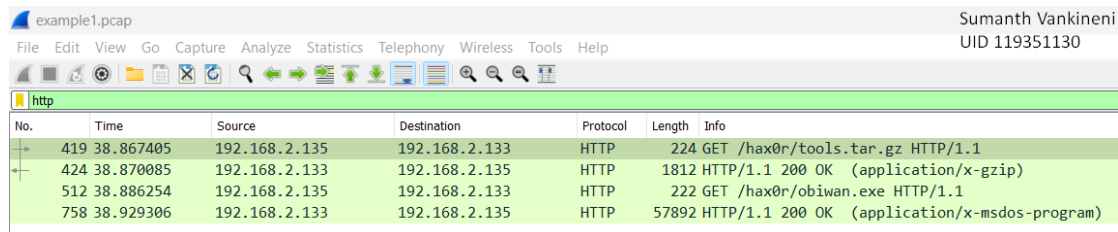
The investigation began by inspecting HTTP traffic in the packet capture to uncover the accessing of the file "obiwan.exe."

An HTTP GET request was identified sent from the local system to IP address 192.168.2.133 requesting the file "obiwan.exe."

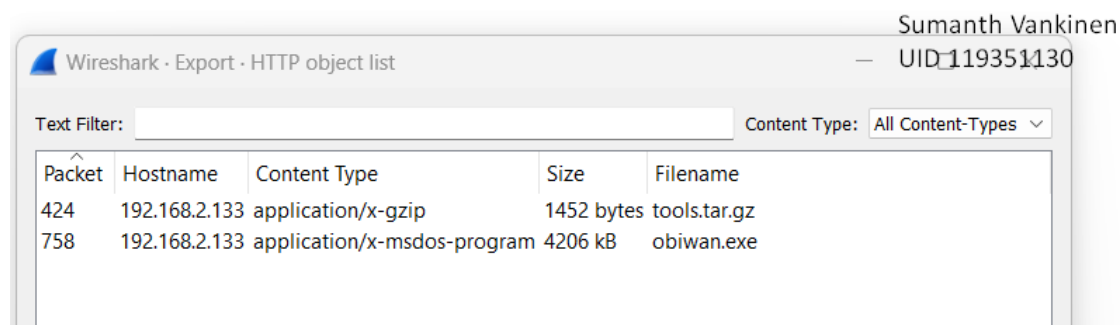
The response packet showed a 200 OK status code from IP 192.168.2.135, confirming the successful download of "obiwan.exe" to the local system.

The executable file was extracted and recovered using Wireshark's export objects feature for further offline analysis.

This analysis of the network traffic revealed how "obiwan.exe" was retrieved by the host system using a standard HTTP file transfer. Tracing the IP addresses and HTTP transaction provided insights into the source and method of obtaining this suspicious executable.



No.	Time	Source	Destination	Protocol	Length	Info
419	38.867405	192.168.2.135	192.168.2.133	HTTP	224	GET /hax0r/tools.tar.gz HTTP/1.1
424	38.870085	192.168.2.133	192.168.2.133	HTTP	1812	HTTP/1.1 200 OK (application/x-gzip)
512	38.886254	192.168.2.135	192.168.2.133	HTTP	222	GET /hax0r/obiwan.exe HTTP/1.1
758	38.929306	192.168.2.133	192.168.2.133	HTTP	57892	HTTP/1.1 200 OK (application/x-msdos-program)



Packet	Hostname	Content Type	Size	Filename
424	192.168.2.133	application/x-gzip	1452 bytes	tools.tar.gz
758	192.168.2.133	application/x-msdos-program	4206 kB	obiwan.exe

Execution and Behaviour of "obiwan.exe"

To further analyze the suspicious executable, "obiwan.exe" was run in my other machine (Ideally should always be run in an isolated test environment).

Process Explorer was used to monitor the processes and connections initiated by "obiwan.exe" during runtime.

It was observed that "obiwan.exe" began communicating with an unknown remote server out on the public internet.

Process Explorer showed that "obiwan.exe" was making multiple connection requests to the remote server.

The state of these requests was inspected, revealing them to be active ongoing connections.

This analysis indicated that a key function of "obiwan.exe" is establishing connections to an external server, warranting further investigation into the nature of the communications.

Name	Date modified	Type	Size
Network Forensics	11/12/2023 5:26 PM	File folder	Sumanth Vankineni UID 119351130
obiwan	11/12/2023 6:00 PM	Application	4,108 KB
tools.tar	11/12/2023 6:00 PM	Compressed Archi...	2 KB

The TCP connections linked to the "obiwan.exe" were monitored by tracking the TCP stream.

No.	Time	Source	Destination	Protocol	Length	Info
2117	1.712504	10.125.26.174	3.163.101.50	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
2154	1.732899	3.163.101.50	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
6938	4.361466	10.125.26.174	3.163.101.50	HTTP	186	GET /youre-my-only-hope HTTP/1.1
6974	4.380419	3.163.101.50	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
10382	7.022628	10.125.26.174	3.163.101.50	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
10405	7.041683	3.163.101.50	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
13153	9.745286	10.125.26.174	3.163.101.50	HTTP	186	GET /youre-my-only-hope HTTP/1.1
13173	9.764666	3.163.101.50	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
15658	12.388716	10.125.26.174	3.163.101.50	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
15682	12.407852	3.163.101.50	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
18887	15.038161	10.125.26.174	3.163.101.50	HTTP	186	GET /youre-my-only-hope HTTP/1.1
18913	15.059579	3.163.101.50	10.125.26.174	HTTP	628	HTTP/1.1 301 Moved Permanently (text/html)
21629	17.669325	10.125.26.174	3.163.101.50	HTTP	189	GET /help-me-obiwan-kenobi HTTP/1.1
21651	17.688444	3.163.101.50	10.125.26.174	HTTP	631	HTTP/1.1 301 Moved Permanently (text/html)
24857	20.343418	10.125.26.174	3.163.101.50	HTTP	186	GET /youre-my-only-hope HTTP/1.1

Wireshark Analysis:

To inspect the network activity of "obiwan.exe," Wireshark was used to capture packets while the executable was running.

In the Conversations tab, multiple TCP sessions were seen between "obiwan.exe" and remote destinations.

Two specific TCP conversations were examined in more detail, both with the host "www.umd.edu."

The conversations revealed HTTP GET requests from "obiwan.exe" to two distinct URLs on "www.umd.edu":

/help-me-obiwan-kenobi

/youre-my-only-hope

This discovery indicated that a key function of "obiwan.exe" is to send messages to these URLs hosted on the "umd.edu" domain.

Further analysis of the URL paths, page contents, and HTTP responses will provide more context around these conversations.

Wireshark provided visibility into the network-level interactions of "obiwan.exe" and allowed analysis of the HTTP requests sent to the external server.

Utilizing Wireshark packet captures, we were able to extract and inspect specific HTTP communications from "obiwan.exe" to "www.umd.edu," obtaining valuable insights into its network behavior.

```
Wireshark · Follow TCP Stream (tcp.stream eq 31) · Ethernet
Sumanth Vankineni
UID 119351130

GET /youre-my-only-hope HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 12 Nov 2023 23:04:26 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/youre-my-only-hope
X-Cache: Redirect from cloudfront
Via: 1.1 032e388cf33a7eb01fc9c402b9e945b8.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: fKa-KDWbEdWH015CCV7WJvs_V0qeXNKwbjyToqiksFSV1Bxg0XBa3g==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

```
Wireshark · Follow TCP Stream (tcp.stream eq 24) · Ethernet
Sumanth Vankineni
UID 119351130

GET /help-me-obiwan-kenobi HTTP/1.1
Accept-Encoding: identity
Host: www.umd.edu
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 12 Nov 2023 23:04:24 GMT
Content-Type: text/html
Content-Length: 167
Connection: close
Location: https://www.umd.edu/help-me-obiwan-kenobi
X-Cache: Redirect from cloudfront
Via: 1.1 5f4c4acb80a9715e27a86e5fdf5337c8.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: ATL58-P8
X-Amz-Cf-Id: 5RaILvE7Ywpdvxub43KHxTixjcQJEBETIoTH76ISjFnyvcOhAJhd7w==

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

The HTTP responses from "www.umd.edu" to "obiwan.exe" were status code 301 Moved Permanently.

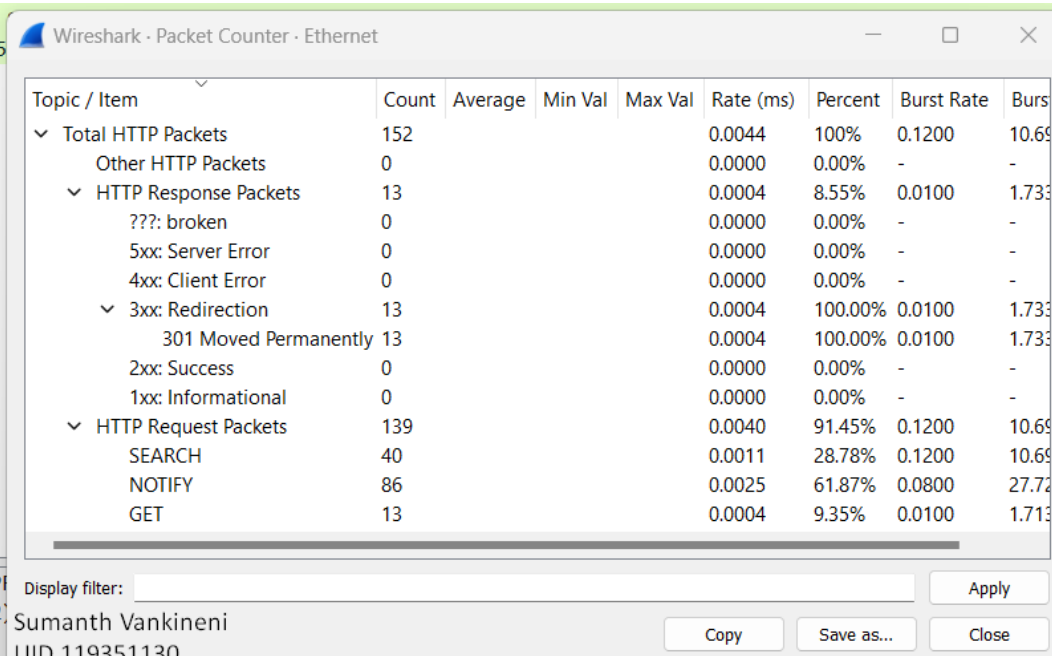
This indicated the requested resources were permanently redirected to new URLs unknown to "obiwan.exe."

Further inspection revealed "obiwan.exe" was a Python executable, providing context on its origin.

The requests appeared to repeat the same message continuously to the server.

Despite exporting all objects from the capture, no additional response content was obtained, likely due to the redirections.

In summary, "obiwan.exe" persistently sent redundant HTTP requests that were not successfully handled by the server due to permanent URL relocations.



The image shows a Wireshark Packet Counter window for Ethernet. It displays a table of HTTP statistics. The table has columns for Topic / Item, Count, Average, Min Val, Max Val, Rate (ms), Percent, Burst Rate, and Burst. The data is categorized into Total HTTP Packets, HTTP Response Packets, and HTTP Request Packets. The '3xx: Redirection' category is expanded, showing '301 Moved Permanently' with a count of 13 and a rate of 100.00%.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst
✓ Total HTTP Packets	152				0.0044	100%	0.1200	10.69
Other HTTP Packets	0				0.0000	0.00%	-	-
✓ HTTP Response Packets	13				0.0004	8.55%	0.0100	1.733
??? : broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
✓ 3xx: Redirection	13				0.0004	100.00%	0.0100	1.733
301 Moved Permanently	13				0.0004	100.00%	0.0100	1.733
2xx: Success	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
✓ HTTP Request Packets	139				0.0040	91.45%	0.1200	10.69
SEARCH	40				0.0011	28.78%	0.1200	10.69
NOTIFY	86				0.0025	61.87%	0.0800	27.72
GET	13				0.0004	9.35%	0.0100	1.713

Display filter: Sumanth Vankineni
UID 119351130

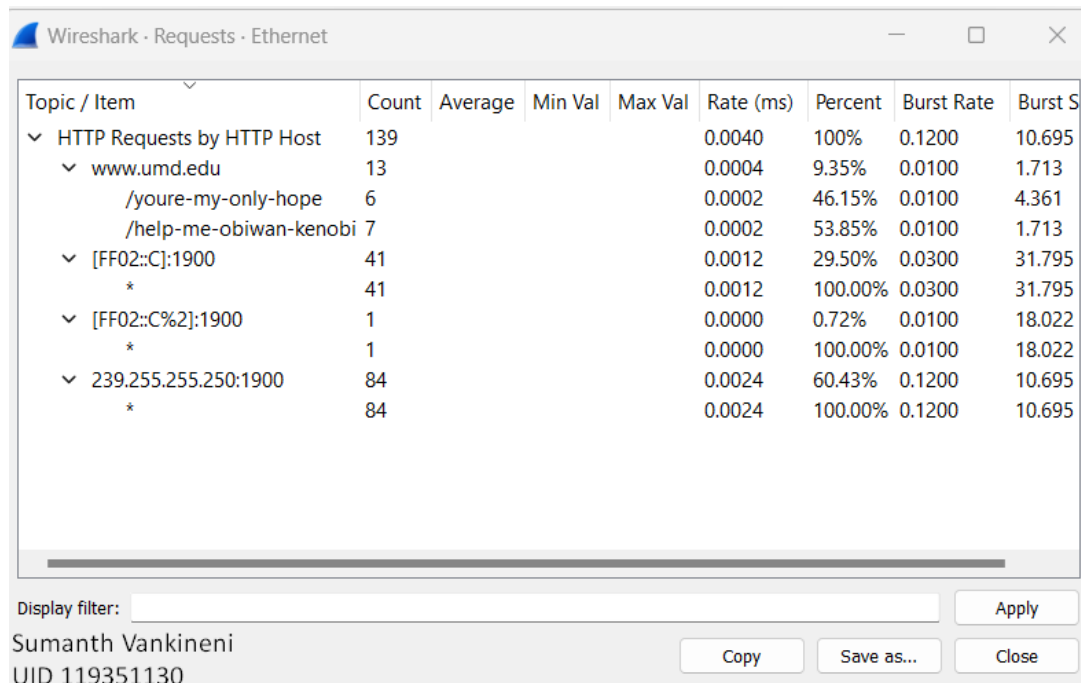
Buttons: Copy, Save as..., Close

To gather further insights, the HTTP requests from "obiwan.exe" to "www.umd.edu" were exported and examined.

However, the analysis did not uncover substantial additional findings.

This was likely due to the 301 redirection responses continuously pointing the requests to new URLs.

The content of the original URL paths could not be retrieved for inspection due to these redirections.



Wireshark - Requests - Ethernet

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst S
HTTP Requests by HTTP Host	139				0.0040	100%	0.1200	10.695
www.umd.edu	13				0.0004	9.35%	0.0100	1.713
/youre-my-only-hope	6				0.0002	46.15%	0.0100	4.361
/help-me-obiwan-kenobi	7				0.0002	53.85%	0.0100	1.713
[FF02::C]:1900	41				0.0012	29.50%	0.0300	31.795
*	41				0.0012	100.00%	0.0300	31.795
[FF02::C%2]:1900	1				0.0000	0.72%	0.0100	18.022
*	1				0.0000	100.00%	0.0100	18.022
239.255.255.250:1900	84				0.0024	60.43%	0.1200	10.695
*	84				0.0024	100.00%	0.1200	10.695

Display filter: Apply

Sumanth Vankineni
UID 119351130

Copy Save as... Close

Recommendations and Next Steps:

The analysis of "obiwan.exe" and its network communications has uncovered some concerning activity that warrants further investigation:

The source system or server that originally downloaded "obiwan.exe" should be identified and examined forensically for additional evidence. Understanding where the executable came from is key to determining its purpose.

The owner/administrator of "www.umd.edu" needs to be engaged to confirm the website was receiving requests from "obiwan.exe." They can provide context on the referenced pages "/help-me-obiwan-kenobi" and "/youre-my-only-hope" and any content found there.

Insights are needed from the website owner on where the pages were permanently redirected to. This is important in identifying the intended recipient of the requests.

"obiwan.exe" itself needs deeper analysis to determine its capabilities, code purpose, and any embedded threats. Static and dynamic analysis should be performed.

The local system that downloaded and ran "obiwan.exe" needs to be inspected for any indicators of compromise or malicious code left behind.

Network monitoring should be enhanced to detect any other systems attempting to download or execute "obiwan.exe" or engage in similar suspicious activities.

Undertaking these recommended next steps will further the investigation into "obiwan.exe" and allow us to contain any potential risks from its dubious functions. The technical insights and cooperation from affected parties will be key.