LOST IN TRANSMISSION

[Publish Date]

European Cyber Security Challenge 2018
London, United Kingdom

1. Initial Write-Up

One of our corporate backup servers has been possibly compromised. Our Data Loss Prevention (DLP) system has discovered some suspicious traffic late last night between this machine and what seems to be a Command and Control (C&C) server.

Fortunately, we have a cron task that encrypts all our backups every couple of minutes. Still, there is a slight chance some data was exfiltrated.

Our Security department needs your high level expertise to check if any critical data has been compromised by understanding the communication protocol between the compromised machine and the C&C.

2. Artifacts

- The relevant traffic has been anonymised (cnc.pcap).
- The relevant C&C server traffic has been isolated (10.21.0.17) and our backup server has the IPv4 10.21.0.3. On that particular day, the critical files being uploaded on the backup server had the following MD5 hashes (critical.txt)

3. Challenge specifications

- Category: Traffic Analysis

4. Artifacts hashing

FILES	MD5	SHA256
cnc.pcap	06b48efe9d6c3b4a8ba1bec0ee2d744a	50e7fdc477420499b2a29bcf40ef641c117ce9bc8a604238718ee0241e98440c

Critical.txt	95b9d41174d4f17fa14c92a3e9de9ffd	fad8235c624d729520e61400ac3a74494da5190546f543e15bbb3a8022a3f8ab
Solution.py	baa875e949e8da7e069df838d1c4a837	ad10674cfe04f8119f0dbe40e2b1d4f937c6b319fd780d543fe53b07c8822b11

5. Tools needed

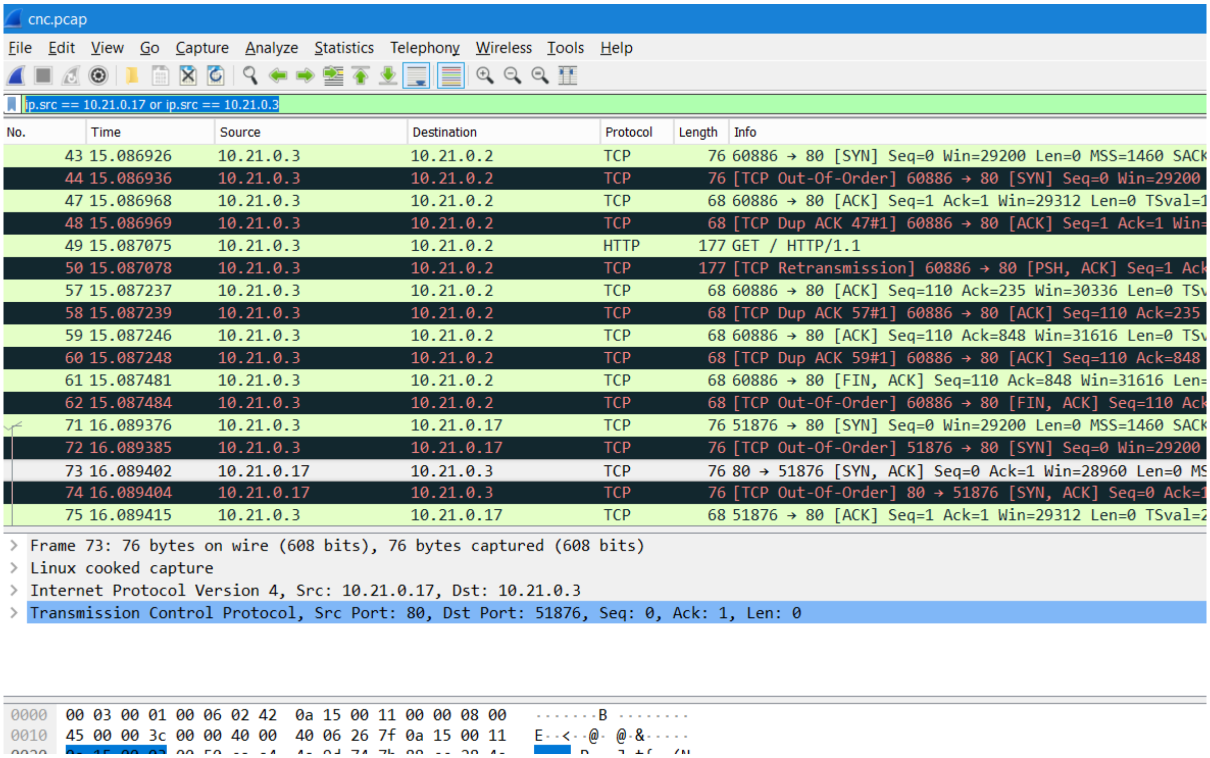
Description:

Tools needed for the solution of the challenge:

- General Linux tools
- PCAP analysis tools(Wireshark)

6. Walkthrough (writeup)

1. Open the pcap in Wireshark
2. Apply the filer: ip.src == 10.21.0.17 or ip.src == 10.21.0.3

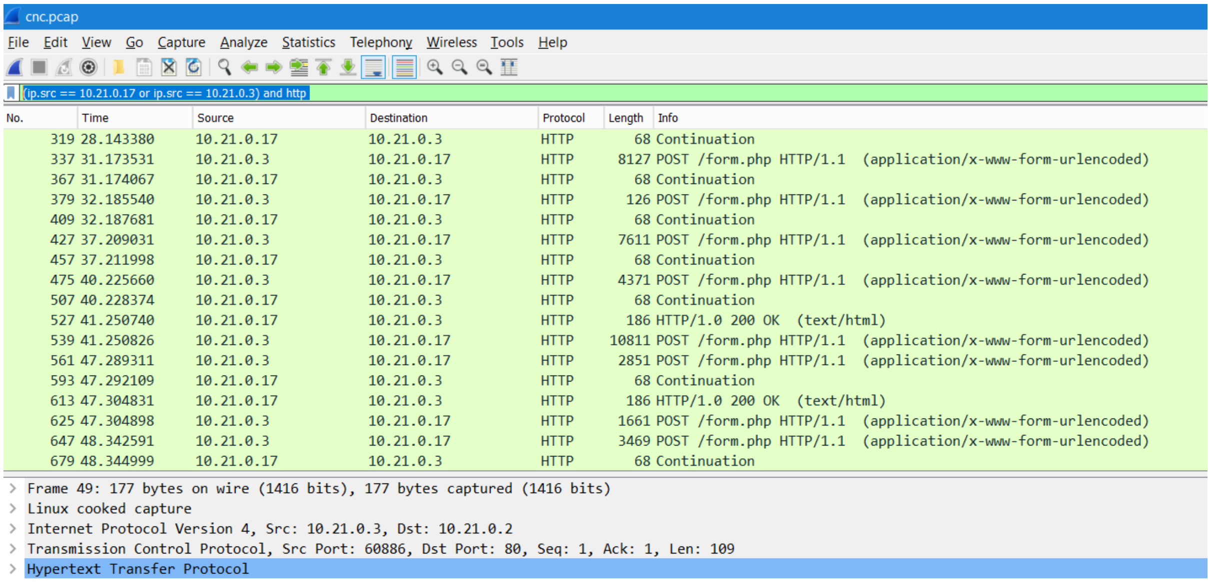


```
ip.src == 10.21.0.17 or ip.src == 10.21.0.3

No.    Time        Source        Destination   Protocol  Length  Info
   43 15.086926   10.21.0.3     10.21.0.2     TCP         76 60886 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK
   44 15.086936   10.21.0.3     10.21.0.2     TCP         76 [TCP Out-Of-Order] 60886 → 80 [SYN] Seq=0 Win=29200
   47 15.086968   10.21.0.3     10.21.0.2     TCP         68 60886 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1
   48 15.086969   10.21.0.3     10.21.0.2     TCP         68 [TCP Dup ACK 47#1] 60886 → 80 [ACK] Seq=1 Ack=1 Win=
   49 15.087075   10.21.0.3     10.21.0.2     HTTP       177 GET / HTTP/1.1
   50 15.087078   10.21.0.3     10.21.0.2     TCP        177 [TCP Retransmission] 60886 → 80 [PSH, ACK] Seq=1 Ack
   57 15.087237   10.21.0.3     10.21.0.2     TCP         68 60886 → 80 [ACK] Seq=110 Ack=235 Win=30336 Len=0 TSv
   58 15.087239   10.21.0.3     10.21.0.2     TCP         68 [TCP Dup ACK 57#1] 60886 → 80 [ACK] Seq=110 Ack=235
   59 15.087246   10.21.0.3     10.21.0.2     TCP         68 60886 → 80 [ACK] Seq=110 Ack=848 Win=31616 Len=0 TSv
   60 15.087248   10.21.0.3     10.21.0.2     TCP         68 [TCP Dup ACK 59#1] 60886 → 80 [ACK] Seq=110 Ack=848
   61 15.087481   10.21.0.3     10.21.0.2     TCP         68 60886 → 80 [FIN, ACK] Seq=110 Ack=848 Win=31616 Len=
   62 15.087484   10.21.0.3     10.21.0.2     TCP         68 [TCP Out-Of-Order] 60886 → 80 [FIN, ACK] Seq=110 Ack
   71 16.089376   10.21.0.3     10.21.0.17    TCP         76 51876 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK
   72 16.089385   10.21.0.3     10.21.0.17    TCP         76 [TCP Out-Of-Order] 51876 → 80 [SYN] Seq=0 Win=29200
   73 16.089402   10.21.0.17    10.21.0.3     TCP         76 80 → 51876 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MS
   74 16.089404   10.21.0.17    10.21.0.3     TCP         76 [TCP Out-Of-Order] 80 → 51876 [SYN, ACK] Seq=0 Ack=1
   75 16.089415   10.21.0.3     10.21.0.17    TCP         68 51876 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2

> Frame 73: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.21.0.17, Dst: 10.21.0.3
> Transmission Control Protocol, Src Port: 80, Dst Port: 51876, Seq: 0, Ack: 1, Len: 0

0000  00 03 00 01 00 06 02 42  0a 15 00 11 00 00 08 00   ·······B ········
0010  45 00 00 3c 00 00 40 00  40 06 26 7f 0a 15 00 11   E··<··@· @·&·····
```

cnc.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

We observe some HTTP traffic. Let’s isolate it.

3. Apply the filet: (ip.src == 10.21.0.17 or ip.src == 10.21.0.3) and http



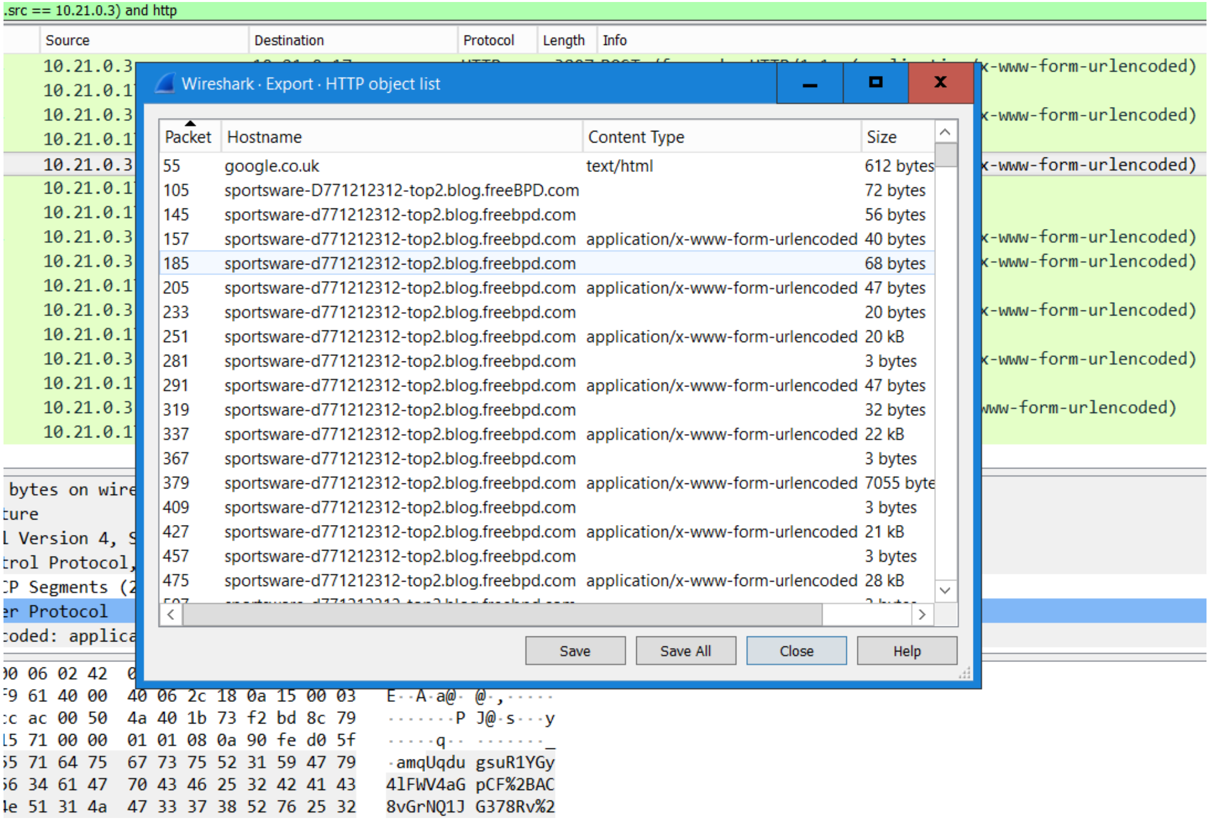
```
(ip.src == 10.21.0.17 or ip.src == 10.21.0.3) and http

No.    Time        Source        Destination   Protocol  Length  Info
  319 28.143380   10.21.0.17    10.21.0.3     HTTP        68 Continuation
  337 31.173531   10.21.0.3     10.21.0.17    HTTP      8127 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  367 31.174067   10.21.0.17    10.21.0.3     HTTP        68 Continuation
  379 32.185540   10.21.0.3     10.21.0.17    HTTP       126 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  409 32.187681   10.21.0.17    10.21.0.3     HTTP        68 Continuation
  427 37.209031   10.21.0.3     10.21.0.17    HTTP      7611 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  457 37.211998   10.21.0.17    10.21.0.3     HTTP        68 Continuation
  475 40.225660   10.21.0.3     10.21.0.17    HTTP      4371 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  507 40.228374   10.21.0.17    10.21.0.3     HTTP        68 Continuation
  527 41.250740   10.21.0.17    10.21.0.3     HTTP       186 HTTP/1.0 200 OK  (text/html)
  539 41.250826   10.21.0.3     10.21.0.17    HTTP     10811 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  561 47.289311   10.21.0.3     10.21.0.17    HTTP      2851 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  593 47.292109   10.21.0.17    10.21.0.3     HTTP        68 Continuation
  613 47.304831   10.21.0.17    10.21.0.3     HTTP       186 HTTP/1.0 200 OK  (text/html)
  625 47.304898   10.21.0.3     10.21.0.17    HTTP      1661 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  647 48.342591   10.21.0.3     10.21.0.17    HTTP      3469 POST /form.php HTTP/1.1  (application/x-www-form-urlencoded)
  679 48.344999   10.21.0.17    10.21.0.3     HTTP        68 Continuation

> Frame 49: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.21.0.3, Dst: 10.21.0.2
> Transmission Control Protocol, Src Port: 60886, Dst Port: 80, Seq: 1, Ack: 1, Len: 109
> Hypertext Transfer Protocol
```

cnc.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

We observe the following protocol:

- GET register.php > likely generates Unique ID (reply sent back in base64): dWlkOiBFM1pJRzZBTDNaVDgzQ1JaTE83NjdYSTlDNFFKNkJUQUFHOFk=
- GET up.php > likely gets the uploading server
- GET cmd.php > gets a command list_files
- POST from.php > base64 information using the uid

4. Extract all HTTP objects using Wireshark



```
.src == 10.21.0.3) and http
```

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size
55	google.co.uk	text/html	612 bytes
105	sportsware-D771212312-top2.blog.freeBPD.com		72 bytes
145	sportsware-d771212312-top2.blog.freebpd.com		56 bytes
157	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	40 bytes
185	sportsware-d771212312-top2.blog.freebpd.com		68 bytes
205	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	47 bytes
233	sportsware-d771212312-top2.blog.freebpd.com		20 bytes
251	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	20 kB
281	sportsware-d771212312-top2.blog.freebpd.com		3 bytes
291	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	47 bytes
319	sportsware-d771212312-top2.blog.freebpd.com		32 bytes
337	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	22 kB
367	sportsware-d771212312-top2.blog.freebpd.com		3 bytes
379	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	7055 byte
409	sportsware-d771212312-top2.blog.freebpd.com		3 bytes
427	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	21 kB
457	sportsware-d771212312-top2.blog.freebpd.com		3 bytes
475	sportsware-d771212312-top2.blog.freebpd.com	application/x-www-form-urlencoded	28 kB

```
90 06 02 42  0
f9 61 40 00  40 06 2c 18 0a 15 00 03   E··A·a@· @·,·····
cc ac 00 50  4a 40 1b 73 f2 bd 8c 79   ·······P J@·s···y
15 71 00 00  01 01 08 0a 90 fe d0 5f   ·····q·· ·······_
55 71 64 75  67 73 75 52 31 59 47 79   ·amqUqdu gsuR1YGy
56 34 61 47  70 43 46 25 32 42 41 43   41FWV4aG pCF%2BAC
4e 51 31 4a  47 33 37 38 52 76 25 32   8vGrNQ1J G378Rv%2
```

5. We remove all files that are irrelevant (replies from C&C server – "OK!")

```
find . -name "*" -size -4 -delete
```

6. We write a python script to pars all the files, decode the URL string from base64. (solution.py)
7. We see the recovered data are archive files

```
recover50.tar: gzip compressed data, last modified:
Mon May 28 16:22:34 2018, from Unix
```

8. We decompress the files

```
for file in $(ls -1); do tar -xvf $file; done
```

9. We identify the compromised file:

90a1a87ceccef2abc24dbf56ba2906546E7R6YV8SOHC0W.acc