

Subject: Data leakage analysis

From: JO

To: Christopher Walker

Date: 20.09.2025

Hi Christopher,

Based on my forensic analysis of the network capture, I have identified a likely data breach involving the archive system at sp.wpk.tpu.fi.

On 15 February 2019 at 10:21, the user “sunshine” (Peter Sunshine) accessed the server and downloaded a confidential document titled “2018-02-15_offer.jpg,” which contained HaiTek Company Ltd.'s €220,200 proposal. The download occurred via NTLM authentication, indicating use of valid internal credentials.

However, the same IP address (172.17.0.40) was simultaneously associated with two different MAC addresses from one belonging to a Raspberry Pi device. This suggests a high probability of ARP spoofing, where the Raspberry Pi impersonated a trusted workstation. Wireshark logs confirm that the Raspberry Pi initiated the GET request and received the file. Prior to this, normal traffic from a legitimate Microsoft device was observed using the same IP. The evidence points to a targeted network attack resulting in unauthorized access to sensitive documents. Immediate mitigation should include credential resets, device isolation, and ARP traffic monitoring.

48079	2019-02-15 12:20:35,340375	Cisco_Bc2e:c2	Broadcast	ARP	60 who has 172.17.0.56? Tell 172.17.1.1	> Frame 48124: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{12B82351-12B82351-12B82351-12B82351-12B82351}
48091	2019-02-15 12:20:37,062500	Cisco_Bc2e:c2	Broadcast	ARP	60 who has 172.17.0.54? Tell 172.17.1.1	> Ethernet II, Src: RaspberryPiF_00:be:ef (b8:27:eb:00:be:ef), Dst: Cisco_Bc2e:c2 (cc:ef:48:8c:2e:c2)
48124	2019-02-15 12:20:43,004671	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 172.17.0.40 is at b8:27:eb:00:be:ef	> Address Resolution Protocol (reply)
48127	2019-02-15 12:20:43,111576	RaspberryPiF_00:be:ef	Broadcast	ARP	60 who has 172.17.0.40? Tell 172.17.0.33	> [Duplicate IP address detected for 172.17.0.40 (b8:27:eb:00:be:ef) - also in use by 00:15:5d:38:01:02 (frame 43620)]
48129	2019-02-15 12:20:44,105100	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 172.17.0.40 is at b8:27:eb:00:be:ef	> [Frame showing earlier use of IP address: 43620]
48130	2019-02-15 12:20:45,115526	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 172.17.0.40 is at b8:27:eb:00:be:ef	[Seconds since earlier frame seen: 57]
48145	2019-02-15 12:20:46,125963	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 172.17.0.40 is at b8:27:eb:00:be:ef	
48146	2019-02-15 12:20:47,136386	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 172.17.0.40 is at b8:27:eb:00:be:ef	
48152	2019-02-15 12:20:48,201484	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 who has 172.17.1.1? Tell 172.17.0.33	
48153	2019-02-15 12:20:48,292446	Cisco_Bc2e:c2	RaspberryPiF_00:be:ef	ARP	60 172.17.1.1 is at cc:ef:48:8c:2e:c2	
48202	2019-02-15 12:20:57,147284	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 172.17.0.40 is at b8:27:eb:00:be:ef	
48559	2019-02-15 12:21:07,484903	RaspberryPiF_00:be:ef	Cisco_Bc2e:c2	ARP	60 172.17.0.40 is at b8:27:eb:00:be:ef	

Picture 1. Arp spoofing happening.

```
> Frame 48626: 1357 bytes on wire (10856 bits), 1357 bytes captured (10856 bits) on interface \Device\NPF_{12B82351-12B82351-12B82351-12B82351-12B82351}
> Ethernet II, Src: Cisco_Bc2e:c2 (cc:ef:48:8c:2e:c2), Dst: RaspberryPiF_00:be:ef (b8:27:eb:00:be:ef)
> Internet Protocol Version 4, Src: 172.16.1.62, Dst: 172.17.0.40
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1343
  Identification: 0x4a54 (19028)
> 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 127
  Protocol: TCP (6)
  Header Checksum: 0x52dd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.16.1.62
  Destination Address: 172.17.0.40
  [Stream index: 95]
> Transmission Control Protocol, Src Port: 80, Dst Port: 1231, Seq: 66594, Ack: 3641, Len: 130:
> [45 Reassembled TCP Segments (65543 bytes): #48573(1460), #48574(1460), #48575(1460), #48577(1460)]
> Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  > HTTP/1.1 200 OK\r\n
    Cache-Control: private\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: application/octet-stream\r\n
    Server: Microsoft-IIS/7.5\r\n
    X-AspNet-Version: 2.0.50727\r\n
    Content-Disposition: attachment;filename="2018-02-15_offer.jpg"\r\n
    Persistent-Auth: true\r\n
    X-Powered-By: ASP.NET\r\n
    MicrosoftSharePointTeamServices: 12.0.0.6421\r\n
    Date: Fri, 15 Feb 2019 10:21:10 GMT\r\n
    \r\n
    [Request in frame: 48572]
    [Time since request: 0.077740000 seconds]
    [Request URI: /_layouts/download.aspx?SourceUrl=%2FShared%20Documents%2F2018%2D02%2D15%5F%20Offer%20Image%20.jpg]
    [Full request URI: http://sp.wpk.tpu.fi/_layouts/download.aspx?SourceUrl=%2FShared%20Documents%2F2018%2D02%2D15%5F%20Offer%20Image%20.jpg]
  > HTTP chunked response
    File Data: 65169 bytes
  > Data (65169 bytes)
```

Picture 2. Server confirms successful file transfer.

HaiTek Company Ltd.

15.2.2018

OFFER to customer

Item A	100 000 €
Item B	80 000 €
<u>Item C</u>	20 200 €

Total	220 200 € incl. tax
-------	---------------------

Details enclosed

Picture 3. Content of the leaked confidential document.

Best regards,

JO