Subject: Data leakage analysis

From: JO

To: Christopher Walker

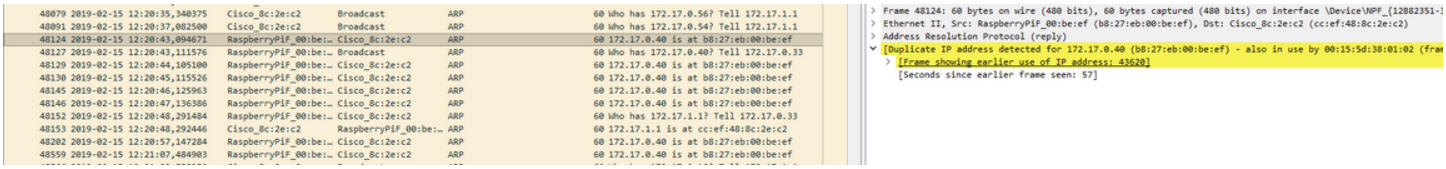
Date: 20.09.2025

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.



Picture 1. Arp spoofing happening.

Picture 2. Server confirms successful file transfer.

HaiTek Company Ltd.

15.2.2018

OFFER to customer

Item A	100 000 €
Item B	80 000 €
Item C	20 200 €
Total	220 200 € incl. tax

Details enclosed

Picture 3. Content of the leaked confidential document.

Best regards,

JO