**INCIDENT REPORT: 18517**

**Date: 02-12-24**

**Executive summary:**

**Examine the PCAP to determine the exploit kit (EK), the payload, and the compromised website that kicked off this infection chain.**

**Victim details:**

* **IP address: 192.168.137.239**
* **MAC address: 68:7f:74:ca:f7:0b**
* **Host name: CiscoLinksys\_ca**

**Indicators of compromise (IOCs):** A GET request directly after visiting a commonly visited website with a high indicator of suspicious/malicious traffic via VirusTotal

**SHA256 hash:**

* 75a11da44c802486bcf65640aa48a730f0f684c5c07a42ba3cd1735eb3fb070

**ID of the payload**

* Mozilla /5.0 (Window nt 6.1; trident/7.0; rv:11.0)

**Compromised Website**

* web.feeddigest.com

**IP address and domain:**

* IP address: 52.2.210
* Domain: web.feeddigest.com
* Mac: 00:02:a5:1c:d4:92