Rapport d’analyse réseau

Pour l’instant ce ne sont que des notes, nous ajouterons des informations complémentaires et nous ferons une mise en forme plus soigné très prochainement.

Informations sur la caméra :

Modèle : Tapo C200

Adresse mac : 1C61B4010F77

Version materiel : 3.0

Version firmware : 1.1.22

Système d’exploitation : Linux 2.6.32 - 3.10

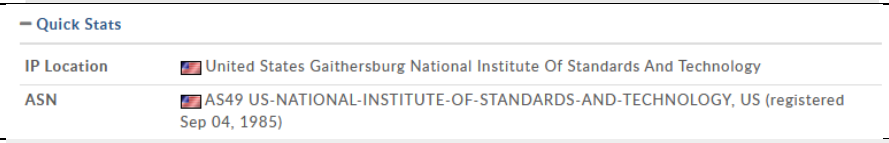
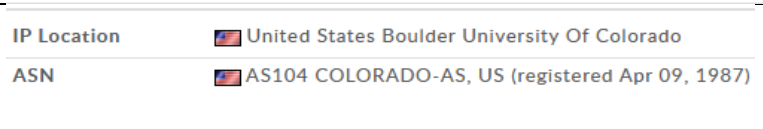
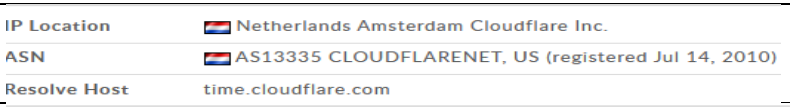
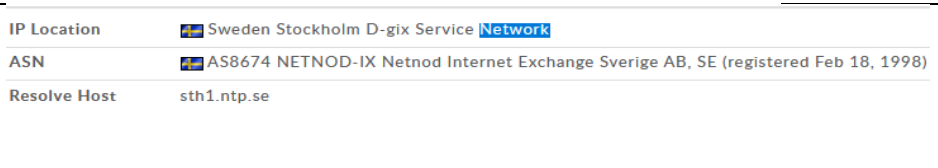
Informations Caméra D’après la doc :

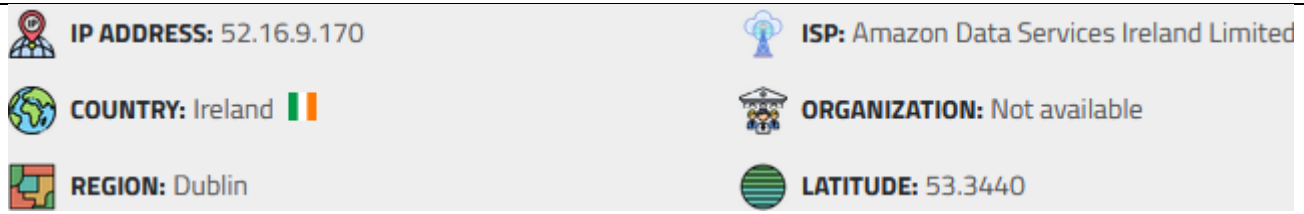
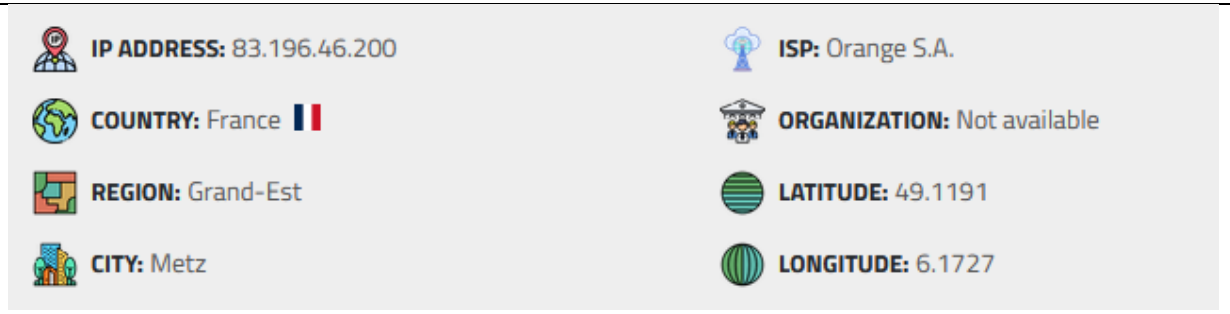
Sécurité 128 bit AES encryption with SSL/TLS => difficile à décrypter

Sécurité wifi : WPA/WPA2-PSK

Les adresses avec lesquelles la caméra communique :

Adresse IP	Protocole	Informations
103.242.70.4	Que NTP : synchronisation Heure	**IP Information** for 103.242.70.4 **Quick Stats** IP Location: New Zealand Wellington Telesmart Limited ASN: AS133075 TELESMARTLIMITED-NZ Telesmart Limited, NZ (registered Sep 16, 2013) Resolve Host: ns1.att.wlg.telesmart.co.nz Whois Server: whois.apnic.net IP Address: 103.242.70.4

131.107.13.100	Que NTP : synchronisation heure	
129.6.15.29	NTP	
129.6.15.28	NTP	
51.145.123.29	NTP	
128.138.140.44	NTP	
162.159.200.123	NTP	
192.36.144.22	NTP	
132.163.97.1	NTP	
34.246.240.3	TLSV1.2 Ack TCP	IP Location : Ireland Ireland Dublin Amazon Data Services Ireland Limited

54.194.8.137	TCP TLSV1.2	 Beaucoup de paquets ; ouverture de session securisé , envoi de certificat, échange de données application
52.16.9.170	TLSV1.2	 Beaucoup de paquets : applications data => toutes les 55 seconds à peu près
83.196.46.200	CLASSIC STUN	 ➔ Mon opérateur
99.80.203.8		Serveur Amazon

Sites utilisés pour trouver les adresses :

https://whois.domaintools.com/

https://www.iplocation.net/ip-lookup

https://whatismyipaddress.com/ip-lookup

Scan avec nmap :

Port	Statut	Service	Version
443 (tcp)	ouvert	ssl/nagios-nsca	Nagios NSCA
554 (tcp)	ouvert	rtsp	
2020 (tcp)	ouvert	soap	gSOAP 2.8
8800	ouvert	sunwebadmin	

Services actifs sur la caméra :

- **RTSP** : Real Time Streaming Protocol est un protocole de communication de niveau applicatif destiné aux systèmes de streaming média

- **sunwebadmin** : pas d'informations trouvés sur internet. Cela semble être utilisé pour administré la caméra a distance.

- **soap** : est un protocole d'échange d'information structurée dans l'implémentation de services web bâti sur XML. Il permet la transmission de messages entre objets distants, ce qui veut dire qu'il autorise un objet à invoquer des méthodes d'objets physiquement situés sur un autre serveur.

- **nagios-ncsa** : explications détaillés : https://www.techtarget.com/searchitoperations/definition/Nagios . NSCA est un service Nagios qui vous permet de recevoir des résultats de contrôle à partir de machines et d'applications distantes avec Nagios. Les résultats des vérifications sont reçus et soumis à Nagios en tant que vérifications passives.

- **ws-discovery** : La découverte dynamique des services Web est une spécification technique qui définit un protocole de découvertemultidiffusion pour localiser des services sur un réseau local.

- **ufsd** : Universal file driver system.

- **Time**

- **netcheque** : sécurisé le transfert de données.

- **Backorifice** : Back Orifice est un logiciel client/serveur d'administration et de prise de contrôle à distance de machines.

Analyser la fréquence d'envoi de données avec les adresses 54.194.8.137 et 34.246.240.3 ; 52.16.9.170 => impression que beaucoup d'envois

Premières notes d'analyses :

1) Il envoi tout le temps des paquets à 52.16.9.170 et de temps en temps il envoi un paquet à 54.194.8.137 qui répond par un application data et encrypted alert => envoyé lors d'une erreur. La caméra tente de se connecter sans succès à un nouveau serveur ?

Finalement, au bout d'un moment on a pu voir qu'il envoyait souvent des paquets à 54.194.8.137

2) Quand on regarde avec l'app les images en direct, il envoi directement au téléphone (l'IP du téléphone est l'adresse de destination) en UDT (envoi continue).

3) On remarque qu'il envoi à des laps de temps réguliers (toutes les 20s à peu près) des paquets à un serveur Amazon, qui semble être un serveur loué par TP-Link. Ces sont de petits paquets envoyés par le port 443, associé au service nagios-ncsa, cela semble donc être des paquets pour vérifier l'état de la caméra.

4) Lorsque la caméra ne voit aucun mouvement (même pendant une longue période), les paquets du service nagios-ncsa sont toujours envoyés sur les serveurs, à la même fréquence.

5) Pour le moment, aucun paquet n'est suspect.

Questionnement :

- Qu'est ce qui déclanche l'envoi des paquets NTP pour synchronisé l'horloge de la caméra ?
- Pourquoi Backorifice est utilisé sur la caméra ?
- Pourquoi des résultats de contrôles de la machine sont envoyés sur les serveur du constructeur ?
- Pourquoi la caméra tente de se connecter sur un nouveau serveur par moment ? Et pourquoi est-ce sans succès.

A faire :

- Refaire une capture wireshark pour analyser plus précisément les envois UDT lorsque l'on est sur l'application.
- Analyser plus précisément l'envoi des paquets et à quel service cela est associé.