[Forensic] Analyse IPs / domaines

Introduction

Lors de l'analyse de vos trames, il vous sera utile d'identifier les IPs et les domaines notamment pour déterminer s'ils sont malveillants et s'il s'agit d'un serveur de l'attaquant.

Cheat-sheet

Trouver le provider d'une IP

```
whois <IP> | grep -i "orgname" | cut -f2 -d':' | sed 's/^[[:space:]]*//'
```

Retirer les IPs selon le provider

```
cat ips.txt | while read ip; do if ! whois "$ip" | grep -iE "orgname|role" | grep -iq "microsoft"; then echo "$ip"; fi; done
```

> Vous pouvez filtrer sur **Microsoft** mais aussi **Akamai** ou **Cloudflare** en modifiant le grep. Cela retirera ces IPs de la liste.

> Vous pouvez remplacer le *cat ips.txt* par une commande **tshark** ou autre, cela fonctionnera parfaitement.

Analyse virustotal

Pour analyser une IP :

```
curl -s -X GET "https://www.virustotal.com/api/v3/ip_addresses/194.180.191.64" -H "x-apikey: API_KEY" | jq '.data.attributes.last_analysis_stats'
```

Pour analyser plusieurs IPs :

```
cat ips.txt| while read -r ip; do curl -s -X GET "https://www.virustotal.com/api/v3/ip_addresses/$ip" -H "x-apikey: 1e04da01b0aa70136ef46bfdf8302db049d5dbc78c9bd0f0a6f8cdf59597b6e7" | jq -r --arg ip "$ip" '"\($ip): \(.data.attributes.last_analysis_stats.malicious)"'; done
```

Revision #6
Created 12 March 2025 10:46:26 by Elieroc
Updated 12 March 2025 14:58:38 by Elieroc