Cas 2 : Rapport d’investigation et Analyse de trafic suspect et exfiltration potentielle

Fait par le groupe **Lets'hack, 19/09/2025 à 09 :38**

Réseau LAN : 10.42.85.0/24

Server C2 Host Name : CITADEL-DC01

IP Hosts : 10.42.85.10 ; 10.42.85.115

Noms de domaine observés: www.microsoft.com

Contexte

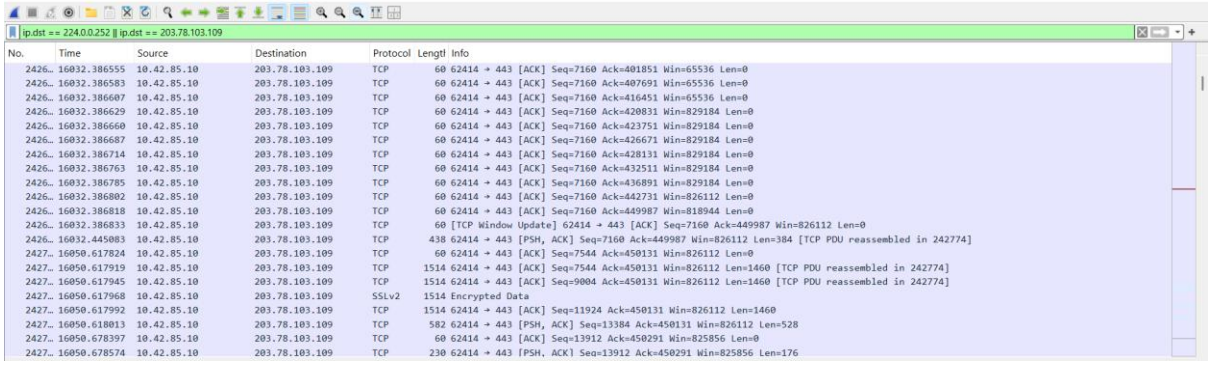
Une série de **captures réseau** ont été analysées à l’aide de **Wireshark** afin d’identifier des comportements suspects sur le réseau interne. Plusieurs communications ont été détectées entre **des machines locales et des IP externes**, dont certaines ont été confirmées comme malveillantes via **VirusTotal.** L’objectif de cette investigation est de détecter toute tentative d’exfiltration de données, d’implant malveillant ou d’activité post-exploitation.

Chaîne de traçabilité

Étape	Description
1	**Identification des IP suspectes** : `203.78.103.109`, `224.0.0.252`
2	**Filtrage du trafic** : Utilisation de filtres Wireshark pour isoler les paquets liés à ces IP
3	**Analyse des flux TCP/TLS** : Présence de paquets `[PSH, ACK]`, `Client Hello`, `Server Hello`, `Application Data`
4	**Extraction de contenu suspect** : Fonctions typiques de malware détectées (`core_channel_write`, `ReflectiveLoader`)
5	**Vérification de réputation** : IP confirmées comme malveillantes via VirusTotal

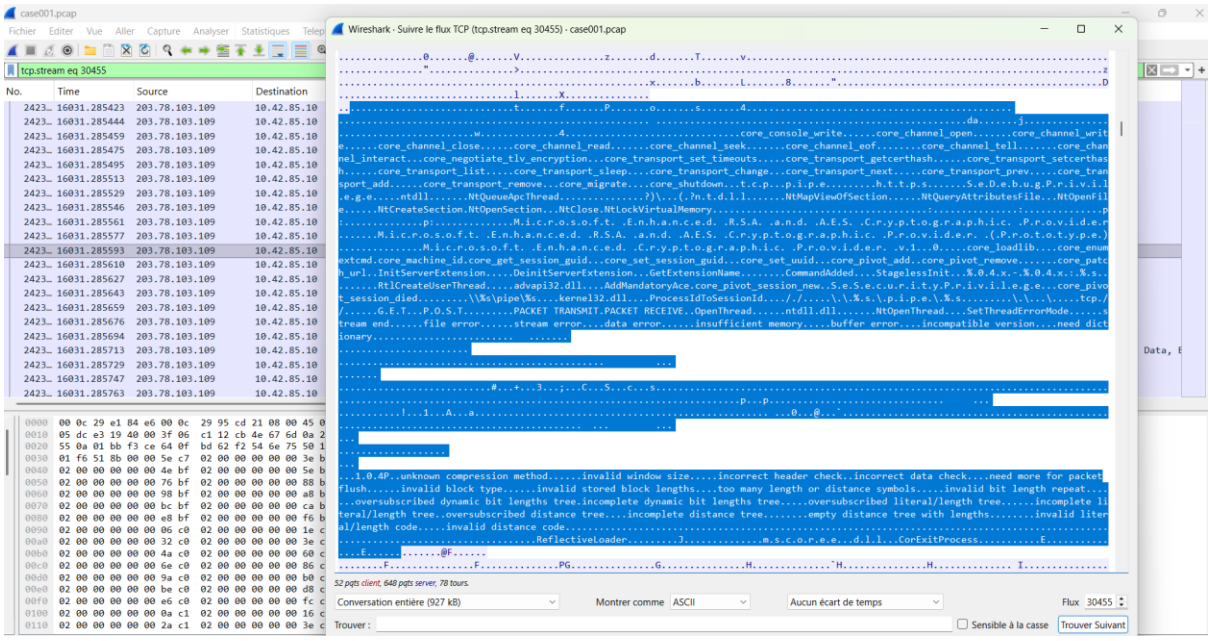
6	**Corrélation avec les processus système** : Références à DLL système (`ntdll.dll`, `advapi32.dll`)
7	**Présomption d'exfiltration** : Chaînes comme `PACKET TRANSMIT`, `tcp://`, `POST`, `pipe` indiquent une transmission de données

Filtrer uniquement les paquets envoyés vers ces IP :



Filtrer uniquement les paquets provenant de ces IP :

```
4051… 26690.826116  10.42.85.10          224.0.0.252          LLMNR      66 Standard query 0xa463 A isatap
4051… 26691.247695  10.42.85.10          224.0.0.252          LLMNR      66 Standard query 0xa463 A isatap
```



Nous observons les différents flux de communication avec le Protocol TCP, LLMNR

Typologie des malwares et attaques identifiées

Types de malwares potentiels

Type de malware	Description	Exemples
Implant mémoire	S'exécute en mémoire sans fichier disque	`ReflectiveLoader`, `NtQueueApcThread`
Backdoor / RAT	Contrôle à distance de la machine	`core_channel_read`, `core_shutdown`
C2 Framework	Infrastructure de commande et contrôle	`core_transport_add`, `core_patch_url`
Credential Harvester	Vol d'identifiants via LLMNR spoofing	`224.0.0.252`, `isatap`
Outil d'exfiltration	Transfert de données vers l'extérieur	`tcp://`, `POST`, `core_channel_write`

Types d'attaques observées ou suspectées

Type de malware	Description	Exemples
Reconnaissance réseau	Identification des services actifs	Requêtes DNS vers `a-msedge.net`
Spoofing / Man-in-the-middle LLMNR/NBT-NS	Interception de requêtes réseau	`224.0.0.252`, `isatap`

Injection en mémoire	Chargement de code malveillant	`NtCreateSection`, `ReflectiveLoader`
Exfiltration de données	Transfert discret d'informations	Flux TLS vers IP malveillantes
Persistance furtive	Maintien d'accès prolongé	`core_migrate`, `core_set_uuid`

Corrélation avec outils connus

- **Metasploit** : `core_channel_*`, `core_transport_*`, `core_shutdown`
- **Cobalt Strike** : `ReflectiveLoader`, `Beacon`, `pipe`, `pivot`

Analyse LLMNR et risques associés

- **IP multicast** : `224.0.0.252`
- **Protocole** : LLMNR
- **Nom demandé** : `isatap`
- **Risques** :

  Spoofing / Man-in-the-middle

  Configuration IPv6 mal gérée

  Activité réseau anormale

Recommandations spécifiques LLMNR

- Désactiver LLMNR si non nécessaire
- Vérifier la configuration ISATAP
- Surveiller les réponses aux requêtes LLMNR

Recommandations globales

Sécurité réseau

- Bloquer les IP malveillantes
- Surveiller les flux TLS sortants
- Désactiver LLMNR sur les postes

Réponse à incident

- Isoler les machines concernées
- Scanner avec EDR, NESSUS ou antivirus avancé
- Identifier les processus initiateurs des connexions

Prévention

- Mettre en place un SIEM

- Activer la journalisation réseau
- Sensibiliser les utilisateurs aux risques LLMNR et spoofing

Conclusion

L’analyse révèle une activité post-exploitation avancée, probablement liée à un implant en mémoire utilisant des techniques furtives. La présence de fonctions de communication, de chiffrement, et de pivot suggère une exfiltration de données ou une préparation à une attaque plus large. Une réponse rapide et coordonnée est essentielle pour contenir la menace et sécuriser l’environnement.

LLMNR (Link-Local Multicast Name Resolution)

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol),