

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

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

## Filtrer uniquement les paquets envoyés vers ces IP :

No.	Time	Source	Destination	Protocol	Length	Info
2426..	16032.386555	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=401851 Win=65536 Len=0
2426..	16032.386583	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=407691 Win=65536 Len=0
2426..	16032.386607	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=416451 Win=65536 Len=0
2426..	16032.386629	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=420831 Win=829184 Len=0
2426..	16032.386660	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=423751 Win=829184 Len=0
2426..	16032.386687	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=426671 Win=829184 Len=0
2426..	16032.386714	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=428131 Win=829184 Len=0
2426..	16032.386763	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=432511 Win=829184 Len=0
2426..	16032.386785	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=436891 Win=829184 Len=0
2426..	16032.386802	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=442731 Win=826112 Len=0
2426..	16032.386818	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7160 Ack=449987 Win=818944 Len=0
2426..	16032.386833	10.42.85.10	203.78.103.109	TCP	60	[TCP Window Update] 62414 → 443 [ACK] Seq=7160 Ack=449987 Win=826112 Len=0
2426..	16032.445083	10.42.85.10	203.78.103.109	TCP	438	62414 → 443 [PSH, ACK] Seq=7160 Ack=449987 Win=826112 Len=384 [TCP PDU reassembled in 242774]
2427..	16050.617824	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=7544 Ack=450131 Win=826112 Len=0
2427..	16050.617919	10.42.85.10	203.78.103.109	TCP	1514	62414 → 443 [ACK] Seq=7544 Ack=450131 Win=826112 Len=1460 [TCP PDU reassembled in 242774]
2427..	16050.617945	10.42.85.10	203.78.103.109	TCP	1514	62414 → 443 [ACK] Seq=9804 Ack=450131 Win=826112 Len=1460 [TCP PDU reassembled in 242774]
2427..	16050.617968	10.42.85.10	203.78.103.109	SSLv2	1514	Encrypted Data
2427..	16050.617992	10.42.85.10	203.78.103.109	TCP	1514	62414 → 443 [ACK] Seq=11924 Ack=450131 Win=826112 Len=1460
2427..	16050.618013	10.42.85.10	203.78.103.109	TCP	582	62414 → 443 [PSH, ACK] Seq=13384 Ack=450131 Win=826112 Len=528
2427..	16050.678397	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=13912 Ack=450291 Win=825856 Len=0
2427..	16050.678574	10.42.85.10	203.78.103.109	TCP	230	62414 → 443 [PSH, ACK] Seq=13912 Ack=450291 Win=825856 Len=176

## 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

No.	Time	Source	Destination
2423..	16031.285423	203.78.103.109	10.42.85.10
2423..	16031.285444	203.78.103.109	10.42.85.10
2423..	16031.285459	203.78.103.109	10.42.85.10
2423..	16031.285475	203.78.103.109	10.42.85.10
2423..	16031.285495	203.78.103.109	10.42.85.10
2423..	16031.285513	203.78.103.109	10.42.85.10
2423..	16031.285529	203.78.103.109	10.42.85.10
2423..	16031.285546	203.78.103.109	10.42.85.10
2423..	16031.285561	203.78.103.109	10.42.85.10
2423..	16031.285577	203.78.103.109	10.42.85.10
2423..	16031.285593	203.78.103.109	10.42.85.10
2423..	16031.285610	203.78.103.109	10.42.85.10
2423..	16031.285627	203.78.103.109	10.42.85.10
2423..	16031.285643	203.78.103.109	10.42.85.10
2423..	16031.285659	203.78.103.109	10.42.85.10
2423..	16031.285676	203.78.103.109	10.42.85.10
2423..	16031.285694	203.78.103.109	10.42.85.10
2423..	16031.285713	203.78.103.109	10.42.85.10
2423..	16031.285729	203.78.103.109	10.42.85.10
2423..	16031.285747	203.78.103.109	10.42.85.10
2423..	16031.285763	203.78.103.109	10.42.85.10

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),**