Liste des Indicateurs de Compromission (PDF)

- Contient une liste des IoCs à bloquer, incluant les IPs malveillantes, les domaines de phishing, les comptes compromis et les ports suspects.
- Actions immédiates à mettre en place : **filtrage des IPs malveillantes, réinitialisation des comptes compromis avec un mot de passe renforcé et activation du MFA, blocage des ports suspects et mise en place d'une surveillance accrue via le SIEM**.

Capture plan remédiation (the hive)

Basic Information

Title	Remédiation	**Start date**	*Not started yet*
Group	default	**Duration**	*Not started yet*
Assignee	Analyst	**Status**	Waiting

Description

📌 1. Identification et Isolation de l'Incident

🔍 Identification des Indicateurs de Compromission (IOC)

- Utilisateur compromis : john.elom, svcmysql
- IP de l'attaquant : 103.251.167.20, 87.88.180.40, 121.186.71.183, 92.184.123.78
- Mails de phishing utilisés : msa@communication.microsooft.com
- IP interne utilisée : 10.0.2.66, 10.0.2.59 (dans la CMDB ce sont les vpn utilisateurs)
- Fichier contenant des identifiants d'un compte admin : pass_adm_dom_svcmysql.txt
- Hash du script de persistance : 5ff01a325fa0f78ae2791f6497646e91f707ea8f9a607803e5c39e7f5b14abce
- Compte créé pour persistance : admin_backup

🚨 2. Endiguement de la Menace

🔒 Blocage des Flux Malveillants

- Bloquer les communications vers les IP malveillantes au niveau du pare-feu :
- Filtrage sur 103.251.167.20, 87.88.180.40, 121.186.71.183
- Blocage du trafic vers les ports suspects : 4567 (utilisé pour le reverse shell)
- Désactivation des connexions réseau suspectes
- Désactiver le compte malveillant admin_backup ajouté par l'attaquant
- Supprimer les règles ajoutées dans le registre Windows :("HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "BGInfo Sysinternals" /f)
- Arrêter et supprimer la tâche planifiée malveillante
- Interdire l'exécution de PowerShell non signé
- Mise en quarantaine et analyse du fichier suspect (pass_adm_dom_svcmysql.txt)
- Blocage des domaines de phishing et URL dans les règles de filtrage DNS :loginmicrosooft.com , x17qszcdzxlh6hb560dedk.65nlspaa2.ru
- Désactivation des comptes compromis et réinitialisation immédiate des mots de passe en activant MFA : john.elom, svcmysql, administrator, root

Regle snort mise en place pour bloquer les données vers ip malveillante :

- alert tcp $HOME_NET any -> 103.251.167.20 53 (msg:"Blocage IP malveillante - Exfiltration DNS"; sid:100001;)

Commentaire règle snort:

- Règle SNORT : Blocage de l'exfiltration DNS vers une IP malveillante

- Description :

Cette règle détecte et bloque les tentatives d'exfiltration de données DNS via le protocole TCP. Elle cible les communications sortantes depuis le réseau interne ($HOME_NET) vers l'IP malveillante identifiée : 103.251.167.20, sur le port 53 (DNS).

- Contexte :

L'IP 103.251.167.20 a été identifiée comme un serveur malveillant utilisé pour recevoir des données sensibles exfiltrées via des requêtes DNS falsifiées. Cette exfiltration fait partie d'une chaîne d'attaque plus large impliquant escalade de privilèges et persistance.

- Critères de détection :

- Trafic TCP sortant vers l'IP 103.251.167.20 sur le port 53.
- Trafic émis par des hôtes appartenant au réseau interne ($HOME_NET).

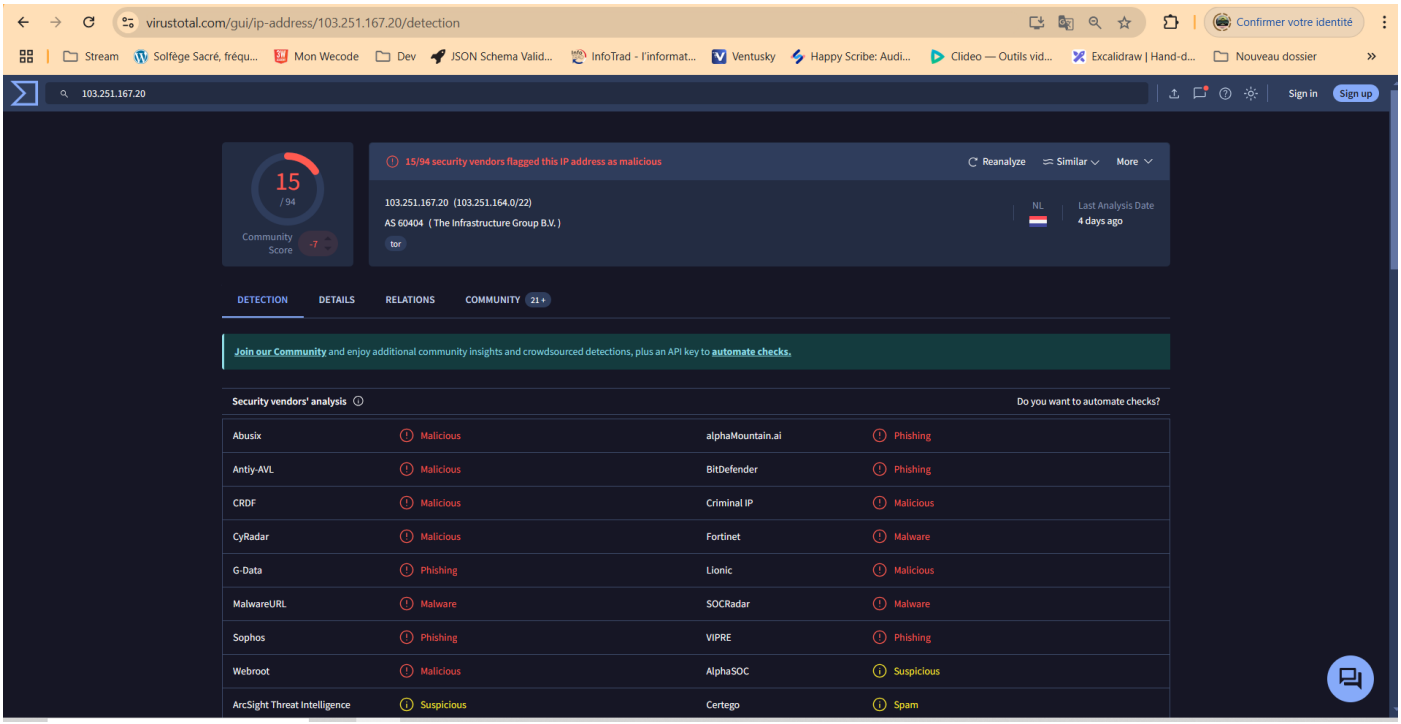
- Objectif :

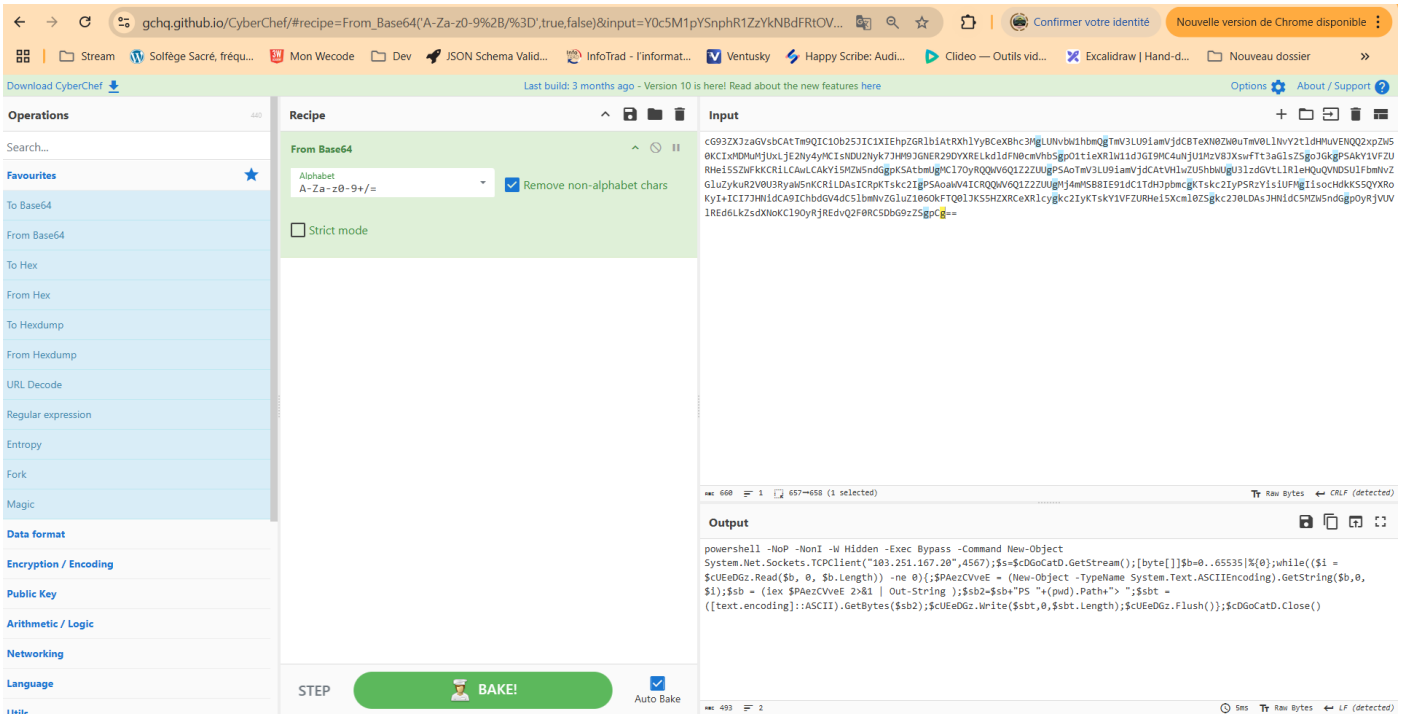
- Bloquer immédiatement les flux DNS suspectés d'exfiltrer des données critiques.

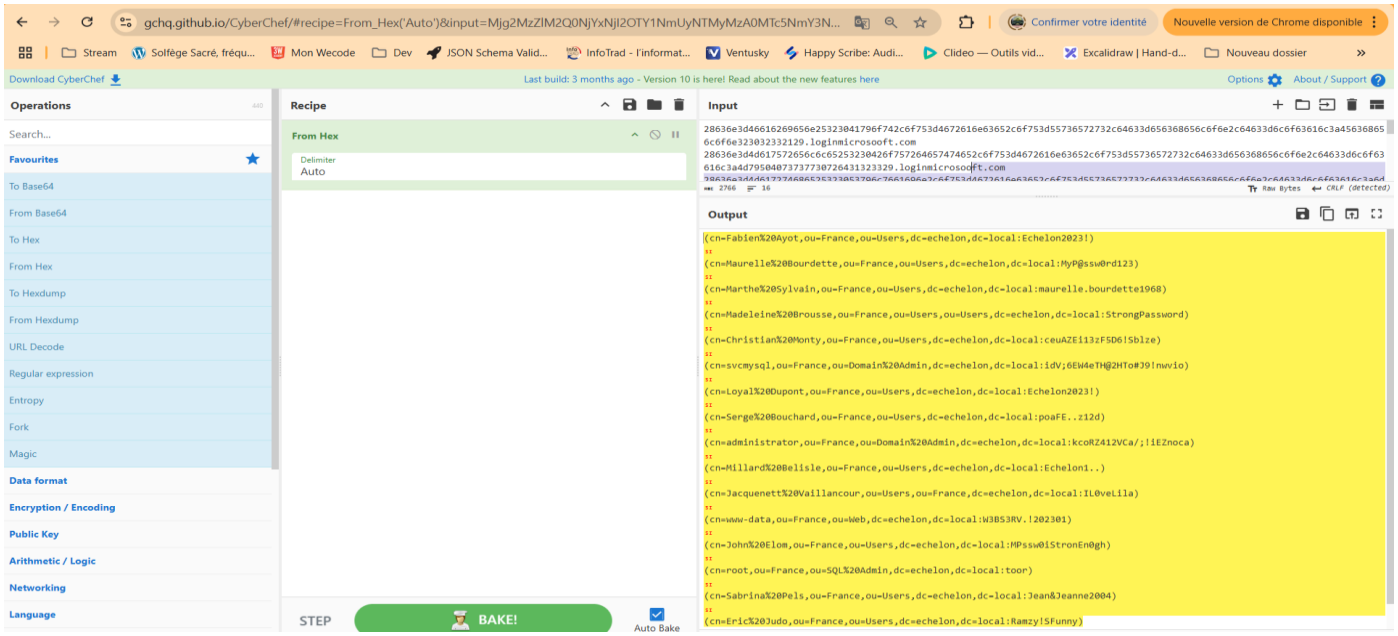
- Actions associées :

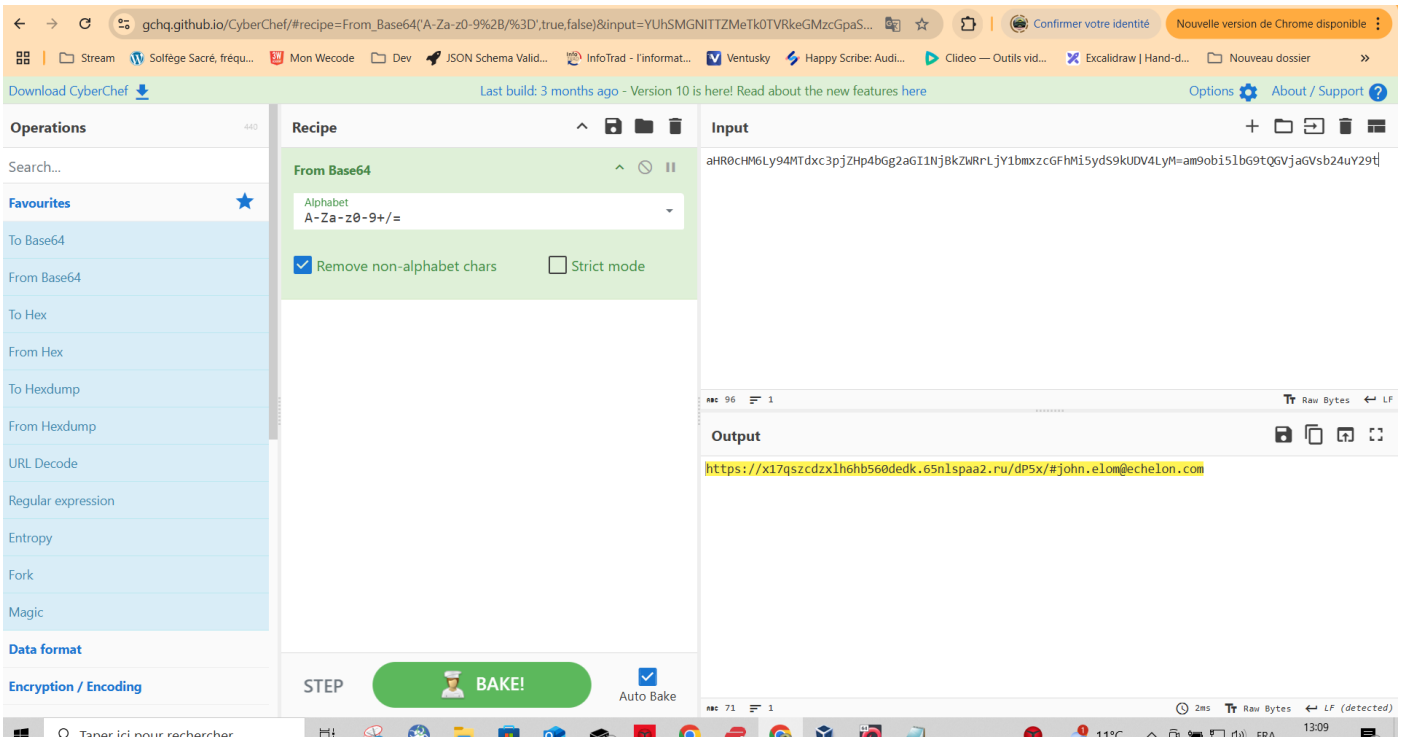
1. Surveiller les alertes générées par cette règle pour confirmer l'absence de flux résiduels.
2. Établir un blocage permanent de l'IP malveillante au niveau du pare-feu réseau.
3. Compléter l'analyse pour identifier d'autres IOCs associés et ajuster les règles en conséquence.

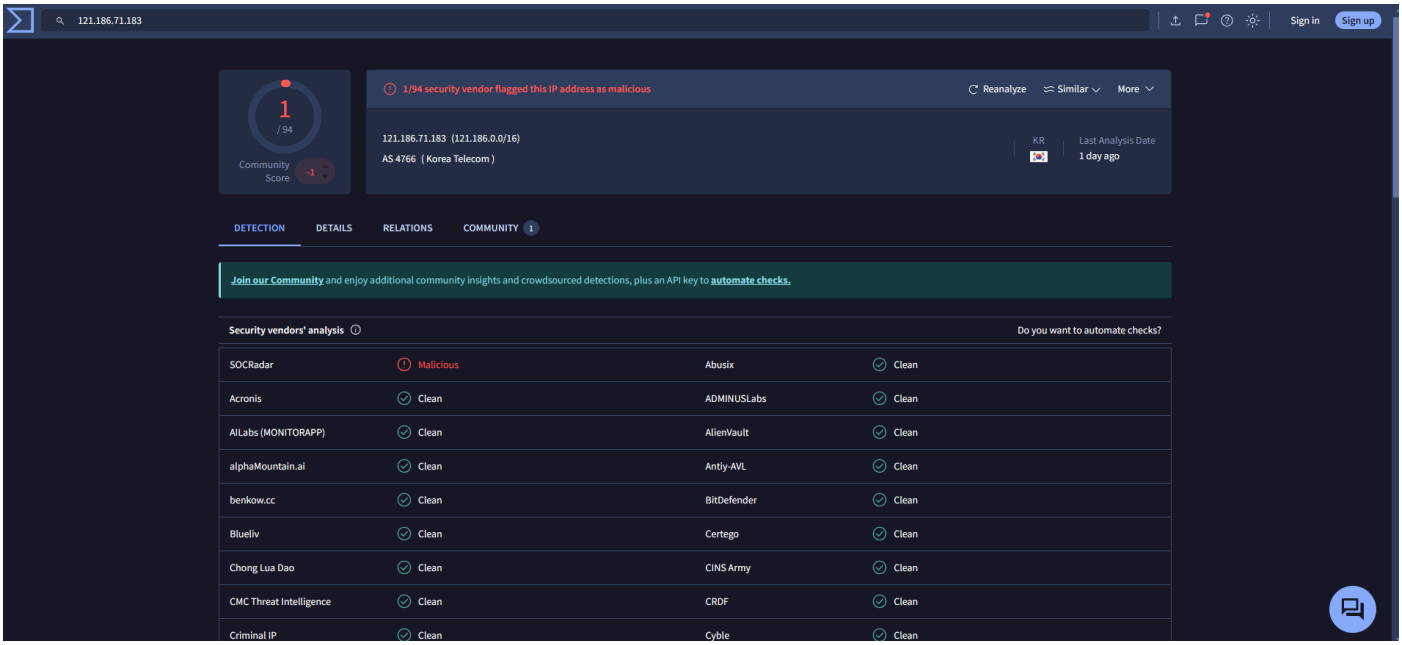
Captures des Iocs trouvé lors de l'analyse :






Operations
Recipe
From Hex
Delimiter
Auto
Input
Output
STEP
BAKE!
Auto Bake


Operations
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
Input
aHR0cHM6Ly94MTdxc3pjZHp4bGg2aGI1NjBkZWRrLjY1bmxzcGFhMi5ydS9kUDV4LyM=am9obi5lbG9tQGVjaGVsb24uY29t
Output
https://x17qszcdzxlh6hb560dedk.65nlspaa2.ru/dP5x/#john.elom@echelon.com
STEP
BAKE!
Auto Bake


121.186.71.183
1/94 security vendor flagged this IP address as malicious
Reanalyze
Similar
More
121.186.71.183 (121.186.0.0/16)
AS 4766 (Korea Telecom)
KR
Last Analysis Date
1 day ago
DETECTION
DETAILS
RELATIONS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
SOCRadar Malicious
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
alphaMountain.ai Clean
Antiy-AVL Clean
benkow.cc Clean
BitDefender Clean
Blueliv Clean
Certego Clean
Chong Lua Dao Clean
CINS Army Clean
CMC Threat Intelligence Clean
CRDF Clean
Criminal IP Clean
Cyble Clean