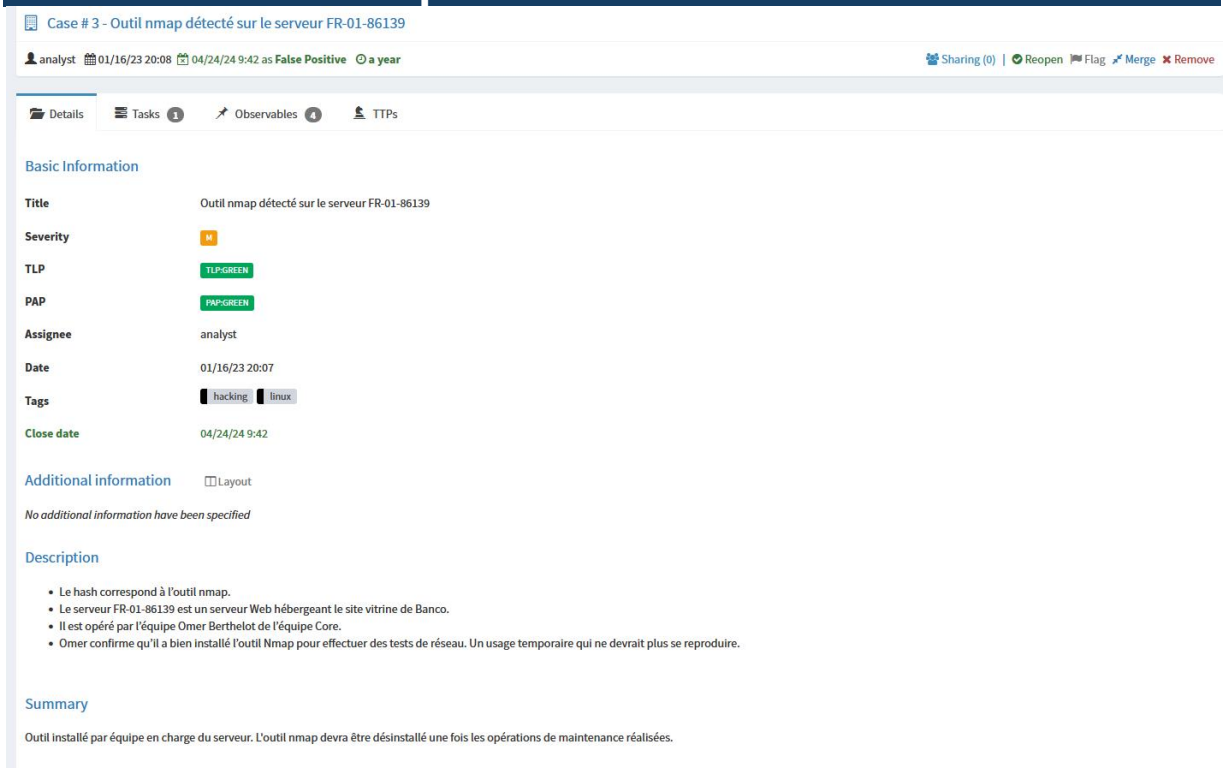
Clôture des alertes 1 à 5 sur TheHive

Avril 2024 – N. Clerbout

Alerte 1 : Outil nmap détecté sur le serveur FR-01-86139



Case # 3 - Outil nmap détecté sur le serveur FR-01-86139

analyst 01/16/23 20:08 04/24/24 9:42 as **False Positive** a year

Sharing (0) | Reopen Flag Merge Remove

Details Tasks 1 Observables 4 TTPs

Basic Information

Title	Outil nmap détecté sur le serveur FR-01-86139
Severity	M
TLP	TLP:GREEN
PAP	PAP:GREEN
Assignee	analyst
Date	01/16/23 20:07
Tags	hacking linux
Close date	04/24/24 9:42

Additional information Layout

No additional information have been specified

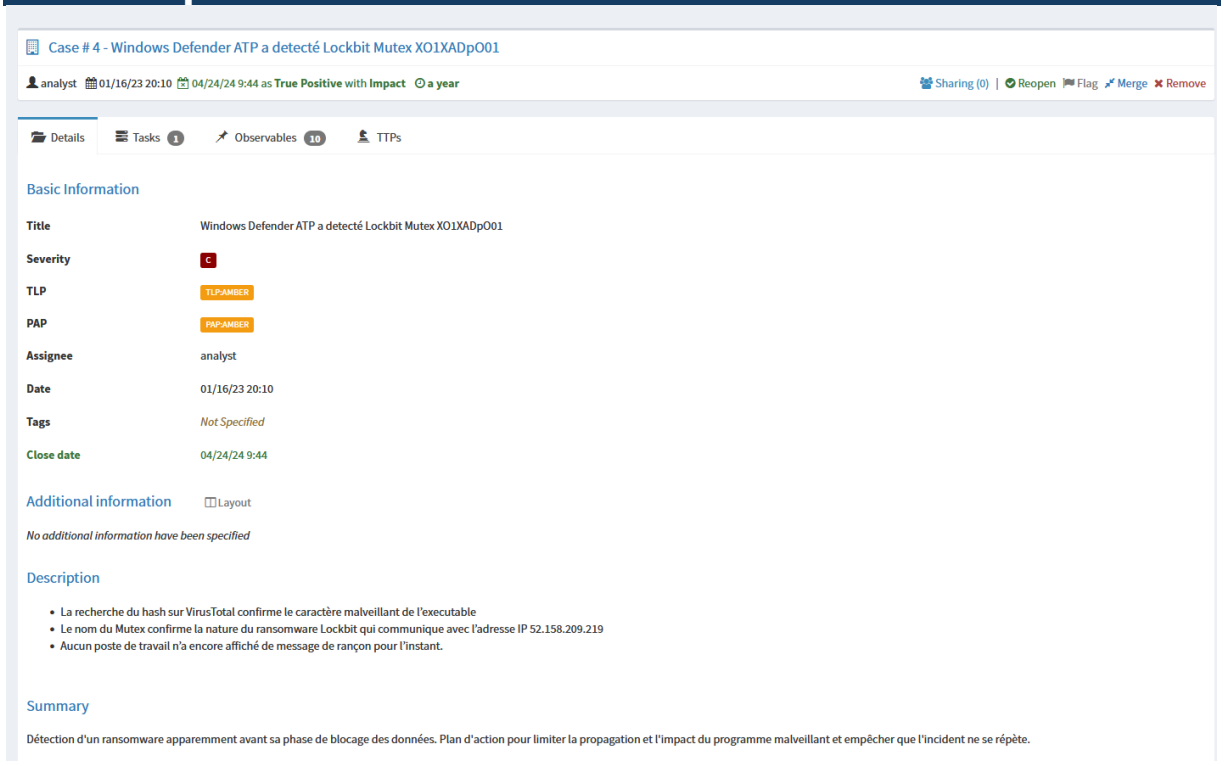
Description

- Le hash correspond à l'outil nmap.
- Le serveur FR-01-86139 est un serveur Web hébergeant le site vitrine de Banco.
- Il est opéré par l'équipe Omer Berthelot de l'équipe Core.
- Omer confirme qu'il a bien installé l'outil Nmap pour effectuer des tests de réseau. Un usage temporaire qui ne devrait plus se reproduire.

Summary

Outil installé par équipe en charge du serveur. L'outil nmap devra être désinstallé une fois les opérations de maintenance réalisées.

Alerte 2 : Windows Defender ATP a détecté Lockbit Mutex XO1XADpO01



Case # 4 - Windows Defender ATP a detecté Lockbit Mutex XO1XADpO01

analyst 01/16/23 20:10 04/24/24 9:44 as **True Positive with Impact** a year

Sharing (0) | Reopen Flag Merge Remove

Details Tasks 1 Observables 10 TTPs

Basic Information

Title	Windows Defender ATP a detecté Lockbit Mutex XO1XADpO01
Severity	C
TLP	TLP:AMBER
PAP	PAP:AMBER
Assignee	analyst
Date	01/16/23 20:10
Tags	*Not Specified*
Close date	04/24/24 9:44

Additional information Layout

No additional information have been specified

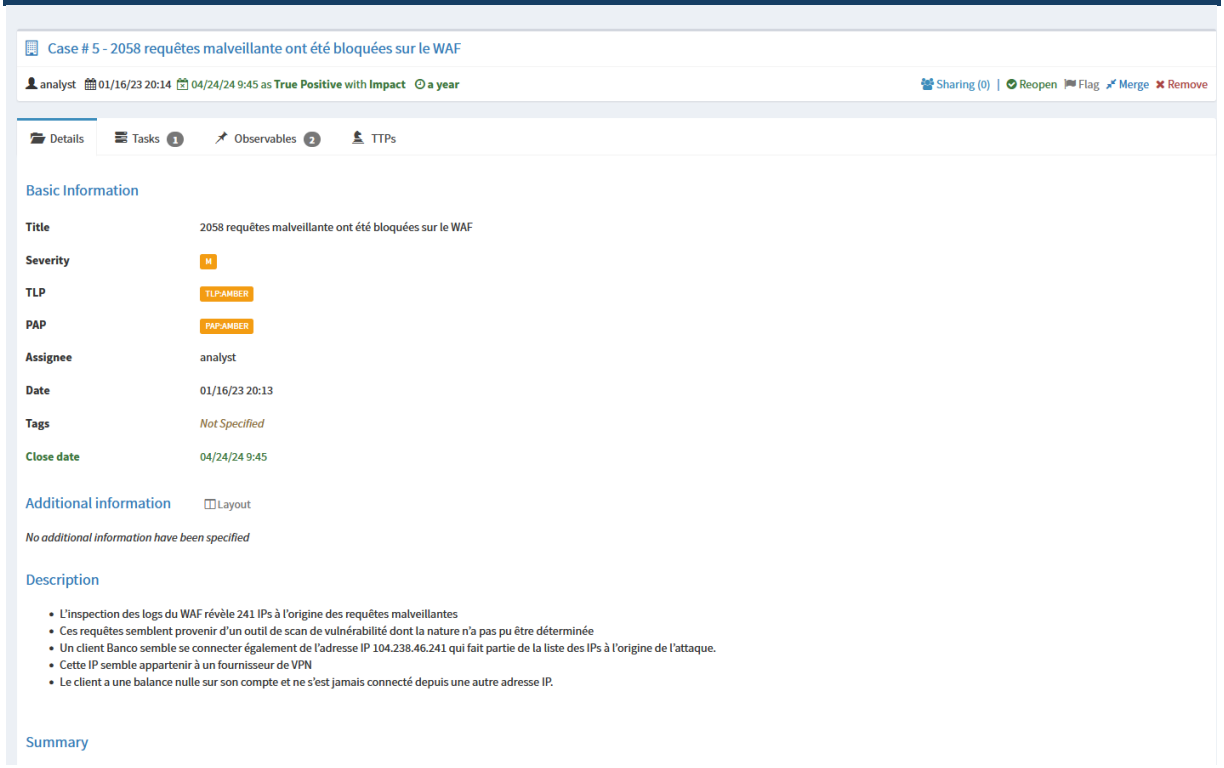
Description

- La recherche du hash sur VirusTotal confirme le caractère malveillant de l'executable
- Le nom du Mutex confirme la nature du ransomware Lockbit qui communique avec l'adresse IP 52.158.209.219
- Aucun poste de travail n'a encore affiché de message de rançon pour l'instant.

Summary

Détection d'un ransomware apparemment avant sa phase de blocage des données. Plan d'action pour limiter la propagation et l'impact du programme malveillant et empêcher que l'incident ne se répète.

Alerte 3 : 2058 requêtes malveillantes bloquées sur le WAF



Case # 5 - 2058 requêtes malveillante ont été bloquées sur le WAF

analyst 01/16/23 20:14 04/24/24 9:45 as **True Positive** with **Impact** a year

Sharing (0) | Reopen Flag Merge Remove

Details Tasks 1 Observables 2 TTPs

Basic Information

Title	2058 requêtes malveillante ont été bloquées sur le WAF
Severity	M
TLP	TLP:AMBER
PAP	PAP:AMBER
Assignee	analyst
Date	01/16/23 20:13
Tags	*Not Specified*
Close date	04/24/24 9:45

Additional information Layout

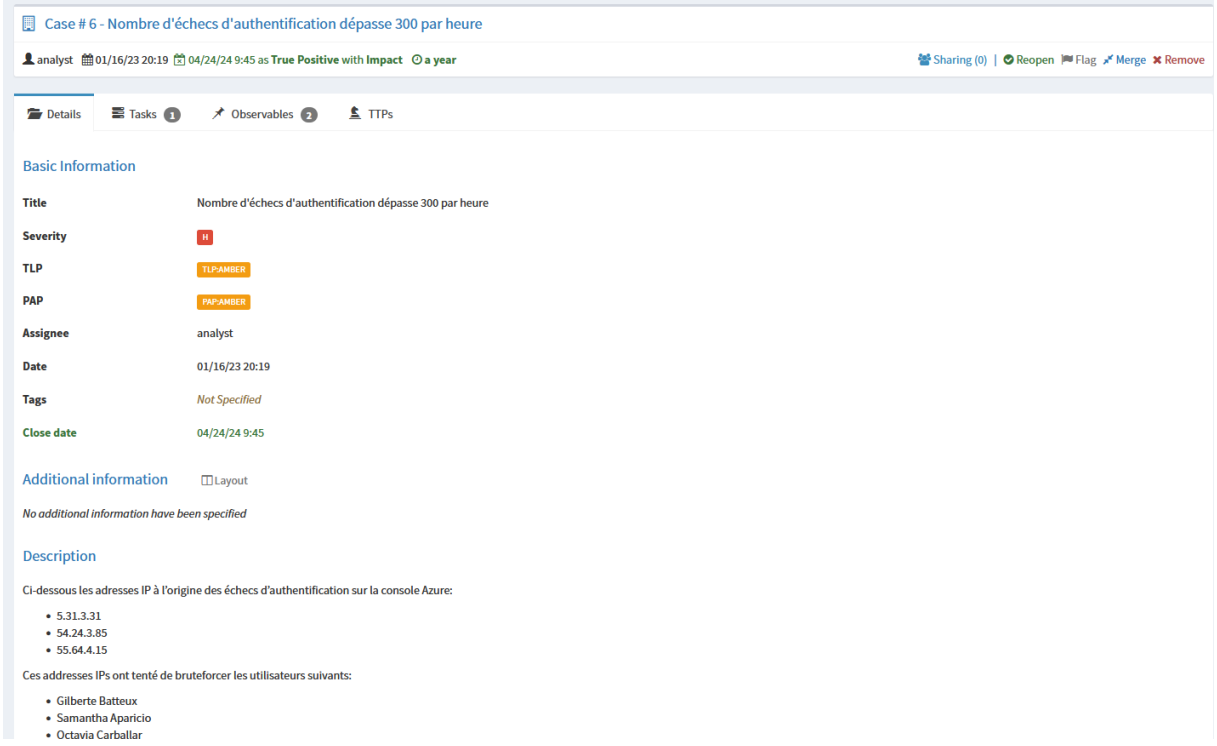
No additional information have been specified

Description

- L'inspection des logs du WAF révèle 241 IPs à l'origine des requêtes malveillantes
- Ces requêtes semblent provenir d'un outil de scan de vulnérabilité dont la nature n'a pas pu être déterminée
- Un client Banco semble se connecter également de l'adresse IP 104.238.46.241 qui fait partie de la liste des IPs à l'origine de l'attaque.
- Cette IP semble appartenir à un fournisseur de VPN
- Le client a une balance nulle sur son compte et ne s'est jamais connecté depuis une autre adresse IP.

Summary

Alerte 4 : Nombre d'échecs d'authentification dépasse 300 par heure



Case # 6 - Nombre d'échecs d'authentification dépasse 300 par heure

analyst 01/16/23 20:19 04/24/24 9:45 as **True Positive** with **Impact** a year

Sharing (0) | Reopen Flag Merge Remove

Details Tasks 1 Observables 2 TTPs

Basic Information

Title	Nombre d'échecs d'authentification dépasse 300 par heure
Severity	H
TLP	TLP:AMBER
PAP	PAP:AMBER
Assignee	analyst
Date	01/16/23 20:19
Tags	*Not Specified*
Close date	04/24/24 9:45

Additional information Layout

No additional information have been specified

Description

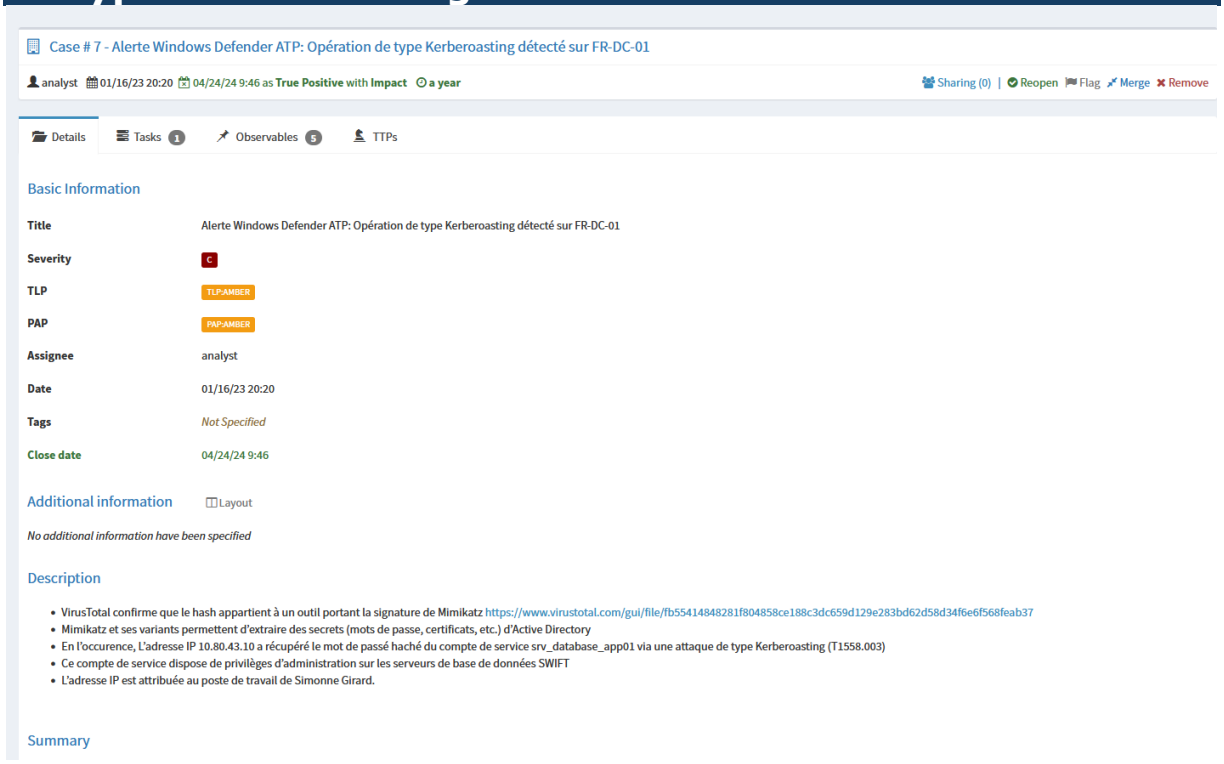
Ci-dessous les adresses IP à l'origine des échecs d'authentification sur la console Azure:

- 5.31.3.31
- 54.24.3.85
- 55.64.4.15

Ces addresses IPs ont tenté de bruteforcer les utilisateurs suivants:

- Gilberte Batteux
- Samantha Aparicio
- Octavia Carballar

Alerte 5 : Windows Defender ATP a détecté une opération de type Kerberoasting sur FR-DC-01



Case # 7 - Alerte Windows Defender ATP: Opération de type Kerberoasting détecté sur FR-DC-01

analyst 01/16/23 20:20 04/24/24 9:46 as **True Positive** with **Impact** **a year**

Sharing (0) | Reopen Flag Merge Remove

Details Tasks 1 Observables 5 TTPs

Basic Information

Title	Alerte Windows Defender ATP: Opération de type Kerberoasting détecté sur FR-DC-01
Severity	C
TLP	TLP:AMBER
PAP	PAP:AMBER
Assignee	analyst
Date	01/16/23 20:20
Tags	*Not Specified*
Close date	04/24/24 9:46

Additional information

Layout

No additional information have been specified

Description

- VirusTotal confirme que le hash appartient à un outil portant la signature de Mimikatz https://www.virustotal.com/gui/file/fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37
- Mimikatz et ses variants permettent d'extraire des secrets (mots de passe, certificats, etc.) d'Active Directory
- En l'occurence, L'adresse IP 10.80.43.10 a récupéré le mot de passé haché du compte de service srv_database_app01 via une attaque de type Kerberoasting (T1558.003)
- Ce compte de service dispose de privilèges d'administration sur les serveurs de base de données SWIFT
- L'adresse IP est attribuée au poste de travail de Simonne Girard.

Summary