**Banco – Cellule SOC**

# Plans d’action

## Alertes 1 à 5

Analyste : Nicolas Clerbout
Avril 2024

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

## Caractéristiques de l'alerte

- Hash : bcab5d490feb0e41d4ac2a73f4cd8cf2ff4a9c78
- Actif concerné : serveur FR-01-86139
- Utilisateur : omer.berthelot

## Détails d'investigation

- Le hash correspond à l'outil nmap : https://www.virustotal.com/gui/file/17e6235f28332367d640dd8d91359f826b1eaae888b2060e9868f1ba58ac4f67
- Nmap (Network Mapper) est un outil de scan de réseau qui permet de réunir des informations diverses (types d'équipements, systèmes d'exploitation utilisés, ports ouverts, services en fonction, vulnérabilités…)
- Le serveur FR-01-86139 héberge le site vitrine de Banco (espace client)
- Le serveur FR-01-86139 est opéré par l'équipe Core.
- Omer Berthelot fait partie de l'équipe Core, sur le site principal de Banco.
- Omer Berthelot confirme avoir installé nmap pour effectuer des tests réseau.

## Plan d'action

- Suppression de nmap une fois les tâches de test réalisées.
- Rappel des procédures :
    - Droits du compte omer.berthelot (en particulier d'installer ce type d'outil) ;
    - Nécessité d'annoncer à l'avance ce genre d'action (ticket)

# Alerte 2 : Windows Defender ATP a détecté Lockbit Mutex XO1XADpO01

## Caractéristiques de l'alerte

- Hash : a72e18efa33f1e3438dbb4451c335d487cbd4082
- Nom : B6kDLnDpHBYpjlGVLWwnZEX.exe
- Mutex : XO1XADpO01
- IP : 52.158.209.219
- Actifs concernés :
    - 6 postes de travail du site de Bordeaux :
        - WRK-BO-5789
        - WRK-BO-5792
        - WRK-BO-5797
        - WRK-BO-5798
        - WRK-BO-5804
        - WRK-BO-5807

## Détails d'investigation

- Le hash correspond à un outil identifié comme malveillant sur VirusTotal : https://www.virustotal.com/gui/file/ffbb6c4d8d704a530bdd557890f367ad904c09c03f53fda5615a7208a0ea3e4d
- Le Mutex utilisé est XO1XADpO01.
- Ce Mutex est utilisé dans la première version du ransomware Lockbit : https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/
- Le ransomware communique avec l'adresse IP 52.158.209.219
- Pas de message de rançon affiché pour l'instant. Pas d'indication sur l'avancement du chiffrement des machines infectées.

## Plan d'action

- Déconnecter les machines infectées du réseau.
- Isoler temporairement le site Bordeaux du reste du SI pour éviter la propagation à d'autres sites.
- Bloquer l'adresse IP 52.158.209.219 sur le firewall Cisco ASA et sur le proxy Zscaler ; ajouter l'adresse au script de blocage d'IP via le WAF.
- Investiguer le vecteur d'infection utilisé pour compromettre les machines.
    - Vérifier que ce vecteur n'a pas été utilisé sur d'autres machines
- Analyser le programme malveillant
    - En particulier, déterminer son mode de propagation
- Nettoyer et restaurer les machines infectées
- Mise à jour de Defender ATP (reconnaissance et blocage du programme via son hash).

# Alerte 3 : 2058 requêtes malveillantes bloquées sur le WAF

## Caractéristiques de l'alerte

- Alerte issue de l'inspection des logs du WAF
- url :
  hxxps://api-endpoint[.]banco[.]com?product=-1+union+select+1,2,3,4,5,6,7,8,9,(SELECT+group_concat(table_name)+from+information_schema[.]tables+where+table_schema=database())<script\x0Ctype="text/javascript">javascript:alert(document[.]cookie);</script>
- 241 adresses IP à l'origine des requêtes identifiées

## Détails d'investigation

- Une adresse IP identifiée semble également utilisée par un client Banco : 104.238.46.241
- Cette IP semble appartenir à un fournisseur de VPN
- Les requêtes malveillantes semblent provenir d'un outil non identifié de scan de vulnérabilités

## Plan d'action

- Ajouter les adresses IP identifiées au script de blocage d'IP.
- Informer le client concerné du blocage de l'adresse IP du fournisseur de VPN.
- Analyser tout le trafic provenant de ces IP pour confirmation des dégâts éventuels.

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

## Caractéristiques de l'alerte

- 3 adresses IP externes à l'origine des tentatives d'authentification
- 5 comptes utilisateurs concernés
- 1 tentative réussie sur l'un des comptes concernés

## Détails d'investigation

- Adresses IP sources de tentatives de bruteforce :
  - 5.31.3.31
  - 54.24.3.85
  - 55.64.4.15
- Comptes utilisateurs visés :
  - Gilberte Batteux (utilisatrice Site Principal)
  - Samantha Aparicio (utilisatrice Site Barcelone)
  - Octavia Carballar (utilisatrice Site Barcelone)
  - Santiago Franco (utilisateur Site Barcelone)
  - Emilio Villa (utilisateur Site Barcelone)
- Compte compromis :
  - Emilio Villa – utilisateur Site Barcelone, pas de double authentification activée

## Plan d'action

- Désactivation temporaire du compte d'Emilio Villa.
- Invalidation du mot de passe compromis (ajout à liste des mots de passe expirés).
- Isolement de la machine accédée.
- Ajout des adresses IP identifiées à la liste des IP à bannir grâce au script.
- Recherche sur la console Azure d'autres tentatives de connexion par ces adresses IP, sans filtre sur le nombre de tentatives par heure.
- Bannir ces adresses IP sur la console Azure.
- Durcir le protocole d'accès à distance. Par exemple :
  - Changer le port par défaut pour ssh,
  - Etablir une liste blanche d'adresses IP autorisées,
  - Configurer Azure pour forcer l'authentification à deux facteurs pour les connexions distantes (jeton SMS ou jeton logiciel),
  - Ajouter un CAPTCHA.

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

## Caractéristiques de l'alerte

- Hash : d007f64dae6bc5fdfe4ff30fe7be9b7d62238012
- Nom du processus : yolokatz.exe
- Actif concerné : serveur FR-DC-01
- Compte de service : srv_database_app01
- IP source : 10.80.43.10

## Détails d'investigation

- TTP : T1558.003
- Le hash correspond à l'outil mimikatz : https://www.virustotal.com/gui/file/fb55414848281f804858ce188c3dc659d129e283bd62d58d34f6e6f568feab37
- Le serveur FR-DC-01 est un contrôleur de domaine situé sur le Site Principal de Banco
- Le compte de service srv_database_app01 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

## Plan d'action

- Isoler, analyser et nettoyer le poste de travail de Simonne Girard.
- Isoler, analyser et nettoyer le server FR-DC-01.
- Mettre à jour Defender ATP pour reconnaître et bloquer le programme malveillant via son hash.
- Changer les mots de passe du compte de Simonne Girard et du compte de service srv_database_app01.
    - Vérifier que la fonctionnalité Managed Service Accounts est appliquée,
    - Vérifier l'application de l'authentification à deux facteurs.
- Vérifier que la politique du moindre privilège est appliquée.
- Vérifier la configuration du pare-feu interne isolant les postes de travail des serveurs.