cyna
secure your future

RETEX

DARK GATE

12/10/2023

Table des matières

Introduction

Ce document est un résumé de la réponse à incident réalisée par CynaCSIRT chez un nos clients. Cette vague d'attaques avait pour but la compromission du parc informatique via le ransomware DarkGate[1] sur l'infrastructure. Le rapport a pour objectif d'exposer le déroulé de la réponse à incident ainsi que les méthodes d'investigations de l'équipe CynaCSIRT et les remédiations qui ont pu être apportées.

Le document s'adresse aux personnes ou fonctions suivantes :

- Les RSSI et leurs adjoints
- Les DSI et leurs adjoints
- Les administrateurs

Nos canaux de discussion :

- Cybersecurity@cyna-it.fr
- +33 9 70 70 41 81 (Heure ouvrés)

Si un point de ce document ne semble pas clair ou n'est pas assez précis, merci de contacter nos équipes.

Contexte

CynaCSIRT est intervenu chez un de ses clients (nommé « CLIENT » pour la suite du rapport) dans le cadre d'une réponse à incident chez qui Cyna effectuait déjà des activités de SOC. Cette surveillance repose sur :

- Un EDR managé (SentinelOne) ;
- Un XDR WAZUH (fork Elastic) ;
- Les logs firewall;
- Les logs O365.

Les machines du parc sont équipées d'un agent SentinelOne et d'un agent WAZUH.

[1] https://www.it-connect.fr/une-campagne-de-phishing-sur-microsoft-teams-darkgate/

Déroulement de la RI

Cellule de crise

Vendredi 15/09

15/09 - 12H40 : Premier message Teams envoyé à un grand nombre d'employés de CLIENT. La méthode employée par l'attaquant consiste à envoyer un message Teams à toutes l'organisation en utilisant le nom John Doe (personne de la direction de CLIENT).

Le message fait état de changements importants dans l'entreprise et invitant à prendre connaissance des documents fournis. En pièce jointe, un dossier .ZIP nommé « Significant company changes.zip ».

Ce dossier contient un document « exploit.pdf.lnk »

15/09 – 12H43 -> 13H16 : Premières détections de la part des agents SentinelOne qui remontent l'exécution du fichier « exploit.pdf.lnk ».

15/09 – 13H10 : CynaCSIRT prend contact avec CLIENT pour établir une cellule de crise et faire un point sur la situation.

15/09 – 13H20 : Investigations de la part de CynaCSIRT, mise en quarantaine des fichiers sur les machines l'ayant exécuté et ajout à la blocklist de SentinelOne des hashs du fichier « exploit.pdf.lnk » et du dossier « Significant company changes.zip ». L'objectif est de prévenir une nouvelle utilisation sur les machines de nos clients. Le fichier et le dossier .ZIP seront automatiquement mis en quarantaine.

15/09 – 13H30 : Exclusion de toutes machines ayant exécuté le fichier « exploit.pdf.lnk » du réseau en prévention d'une possible propagation dans le réseau mais également afin de couper l'accès au C2 (Command to Control).

Le client informe CyanCSIRT qu'un utilisateur a exécuté le fichier et que cette machine ne possède pas d'agent SentinelOne. Isolation de la machine du réseau physique (cette machine sera nommée POSTE101).

15/09 – 14H06 : Identification du nombre de message envoyé par l'attaquant (220 messages) à l'organisation CLIENT. Identification de l'adresse IP utilisé par le compte Teams (147[.]78[.]47[.]21). Mise en place d'une règle de blocage pour cette adresse sur les firewalls de CLIENT.

Début des investigations sur les logs firewall pour savoir s'il y a eu des communications entre une machine CLIENT et un potentiel C2 derrière l'adresse IP.

15/09 – 14H18 : Il est établi que l'adresse IP obtenue ne correspond pas à celle du serveur de commande et de contrôle (C2), et aucune communication n'a été établie entre les machines et cette adresse. La recherche de l'IP du C2 se poursuit.

15/09 – 14h34 : Transmission de la liste des utilisateurs ayant reçu le message Teams ; liste obtenue via les logs O365. Cette liste sera utilisée dans les minutes suivantes afin de communiquer à chaque utilisateur par mail sur la nature malveillante du message reçu via Teams.

15/09 – 15H04 : Isolation d'une machine (POSTE102) par précaution sur SentinelOne. L'utilisatrice rapporte que chaque application qu'elle ouvre s'ouvre dans le bloc note avec des caractères illisibles.

15/09 – 15H38 : Récupération de l'adresse l'adresse IP du C2 (5[.]188[.]87[.]58) à la suite de l'exécution du fichier « exploit.pdf.lnk » dans un sandbox. Blocage de l'IP sur les firewalls.

15/09 – 17H00 : En accord avec le client, la cellule de crise prend fin. Mise en place d'une astreinte sur le week-end (Samedi 16/09 et dimanche 17/09) afin de prolonger la surveillance du SOC en dehors des heures ouvrées.

Investigations à froid

Samedi 16/09

16/09 – 10H30 : Investigations matérielles sur les machines POSTE101 et POSTE102.

16/09 – 13H27 : Confirmation apporté au client que la machine POSTE101 n'a pas été chiffré mais recommandons de remasteriser la machine avant de la rendre à l'utilisateur.

Les investigations permettent de confirmer que la machine POSTE102 n'a pas été chiffré et que le problème rapporté par l'utilisatrice est un problème lié au système d'exploitation (le problème cité n'était pas présent en changeant d'utilisateur).

16/09 – 14H00 : Rédaction d'un compte rendu sur l'attaque à destination du client.

Lundi 18/09

18/09 – 9H00 : Fin de la réponse à incident chez CLIENT.

Fin de l'incident

Après un travail plus approfondi sur les IOCs (Indicator of compromise - IP et hash) ainsi que la méthode utilisée nous avons pu identifier que l'attaque faisait partie d'une vague d'attaque utilisant le ransomware DarkGate.

Réplique de l'attaque

Mardi 03/10

03/10 – 15H50 : Le client nous à de nouveaux sollicité pour une tentative de phishing identique à la précédente via Teams. Cette fois-ci le dossier .ZIP était nommée « Found_Items_Photos.zip », contenant 4 fichiers.

Par chance, les utilisateurs étant sensibilisés depuis la dernière attaque, personne n'a téléchargé le dossier sur sa machine.

03/10 – 16H12 : Nous avons pu récupérer le dossier concerné et bloquer ajouter son hash à la blocklist SentinelOne afin de prévenir tout téléchargement sur les postes CLIENT.

03/10 – 16H22 : Après avoir passé fait passer le dossier dans une sandbox, nous avons pu récupérer l'adresse IP du nouveau C2 (185[.]39[.]18[.]170) et la bloquer sur les firewalls.

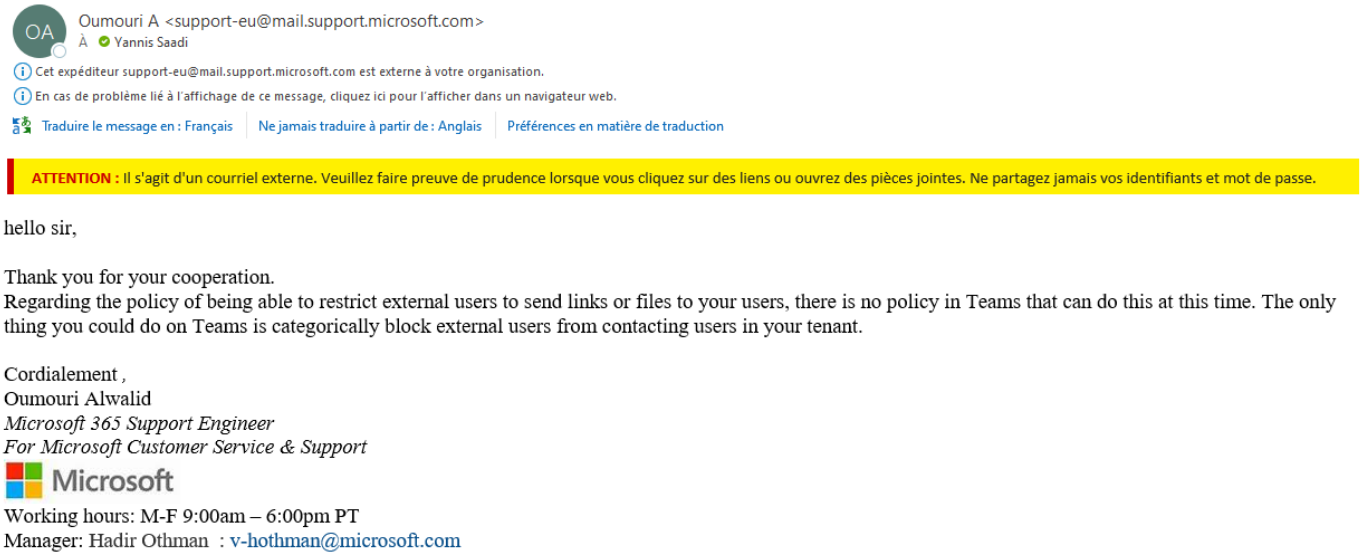
Fin de la réplique

Détection et défense

Après avoir subi une réplique de l'attaque, nous avons dû travailler à ne plus subir et réagir mais à empêcher, détecter et protéger. Pour se faire, nous nous sommes tournés vers les configurations du tenant o365 de CLIENT. Le problème est que le vecteur d'attaque n'est pas un email mais un fichier sur Teams. Les configurations et les options de sécurisation pour les mails sont nombreuses mais sur Teams, les options sont extrêmement limitées :

- Autoriser toutes les communications de l'extérieur
- Autoriser une liste de domaine
- Bannir une liste de domaine
- Bannir toutes les communications de l'extérieur

L'option pour bloquer les liens et les fichiers venus d'une organisation extérieure n'existe simplement pas.



OA Oumouri A <support-eu@mail.support.microsoft.com>
À Yannis Saadi
Cet expéditeur support-eu@mail.support.microsoft.com est externe à votre organisation.
En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.
Traduire le message en : Français | Ne jamais traduire à partir de : Anglais | Préférences en matière de traduction

ATTENTION : Il s'agit d'un courriel externe. Veuillez faire preuve de prudence lorsque vous cliquez sur des liens ou ouvrez des pièces jointes. Ne partagez jamais vos identifiants et mot de passe.

hello sir,

Thank you for your cooperation.
Regarding the policy of being able to restrict external users to send links or files to your users, there is no policy in Teams that can do this at this time. The only thing you could do on Teams is categorically block external users from contacting users in your tenant.

Cordialement ,
Oumouri Alwalid
Microsoft 365 Support Engineer
For Microsoft Customer Service & Support
Microsoft
Working hours: M-F 9:00am – 6:00pm PT
Manager: Hadir Othman : v-hothman@microsoft.com

Figure 1 Echange avec le support Microsoft

La décision peu idéale a été d'extraire les noms de domaine les plus contacté le mois dernier et de les whitelist puis de faire du cas par cas.
Cette solution n'étant que peu satisfaisante, l'équipe Cyna continue de travailler à une configuration de tenant qui permettrait d'empêcher une attaque du type de DarkGate.

Pour détecter cette attaque il est possible de mettre en place quelques règles sur un SIEM récoltant les logs o365.

Conclusions et Recommandations :

La réponse à l'incident de CynaCSIRT chez le client a été efficace pour contenir l'attaque, mais des améliorations sont nécessaires pour prévenir les futures attaques. Voici les principales conclusions et recommandations :

Conclusions :
La réaction rapide du CynaCSIRT a permis d'isoler l'attaque évitant ainsi le chiffrement des machines et la perte de données.

- Aucune donnée critique n'a été compromis.
- Malgré une tentative de réplique, aucune machine n'a été infectée grâce à la sensibilisation des utilisateurs.

Recommandations :
- Sensibilisation des employés contre le phishing et renforcer la vigilance.
- Mise en place des règles de détection dans un SIEM pour surveiller les activités suspectes liées à Teams.
- Maintenir une surveillance constante de l'infrastructure informatique pour détecter rapidement les activités malveillantes.
- Élaborer et tester un plan de continuité d'activité pour garantir la disponibilité des services informatiques.
- Partager les enseignements tirés pour renforcer la résilience collective contre les ransomwares et le phishing.

Annexes Règles Elastic

O365_FILE_SENDING_CAMPAIGN

La “requête” permet le tri des logs avant de faire l’analyse avec les conditions du “seuil de détection”.

Requête :

- Event Action : FileUploaded
  - Action lorsqu’un utilisateur envoie un fichier dans une conversation.
- o365.audit.TargetUserOrGroupType : "Member”
  - Cette valeur permet d’identifier si le fichier est envoyé dans une discussion privée.

Le “seuil de détection” permet définir les conditions pour déclencher une alerte.

Seuil de détection :

- **Count :** o365.audit.TargetUserOrGroupType ≥ 4
  - Si dans les logs, la valeur “o365.audit.TargetUserOrGroupType” est différente pour 4 logs et plus, alors une alerte sera levée.

Résumé:

Si un utilisateur envoie un fichier en message personnel à 4 personnes différentes, une alerte sera créée.

Récurrence d’observation de l’alerte

Se lance toutes les :

- 5 minutes

Intervalle de temps supplémentaire d’observation :

10 minutes

O365_MASSIVE_SENDING_ONEonONE_MESSAGE

Requête :

- Event Action : MessageSent
  - Action lorsqu'un utilisateur envoie un lien dans un message
- o365.audit.CommunicationType : "OneOnOne"
  - Valeur permettant d'identifier une conversation 1↔1

Seuil de détection :

- **Count :** o365.audit.ChatThreadId ≥ 5
  - ID qui permet d'identifier la conversation
  - Si dans les logs, la valeur "o365.audit.ChatThreadId" est différente pour 5 logs et plus, alors une alerte sera levée.

Résumé:

Si un utilisateur envoie un message personnel à 5 personnes différentes, une alerte sera créée.

Récurrence d'observation de l'alerte

Se lance toutes les :

- 5 minutes

Intervalle de temps supplémentaire d'observation :

- 15 minutes

O365_MULTIPLE_ADDING_GROUP

Requête :

- Event Action: "added-users-to-group"
  - Action lorsqu'un utilisateur ajoute une personne dans un groupe

Seuil de détection :

- **Group By**: user.email and user.id ≥ 10
  - Si dans les logs, la paire de valeur "user.email" et "user.id" est identique dans 10 logs et plus, alors une alerte sera levée.

Résumé:

Si un utilisateur invite plus de 10 personnes dans un groupe, une alerte sera créée.

Récurrence d'observation de l'alerte

Se lance toutes les :

- 5 minutes

Intervalle de temps supplémentaire d'observation :

- 10 minutes

O365_LINK_SENDING_CAMPAIGN

Requête :

- Event Action : MessageCreatedHasLink
  - Action lorsqu'un utilisateur envoie un lien dans un message

Seuil de détection :

- **Count :** o365.audit.ChatThreadId ≥ 4
  - ID qui permet d'identifier la conversation
  - Si dans les logs, la valeur "o365.audit.ChatThreadId" est différente pour 4 logs et plus, alors une alerte sera levée.

Résumé:

Si un utilisateur envoie un fichier contenant un lien en message personnel à 4 personnes différentes, une alerte sera créée.

Récurrence d'observation de l'alerte

Se lance toutes les :

- 5 minutes

Intervalle de temps supplémentaire d'observation :

- 10 minutes

Annexe IOCs

Objet	Valeur
IP Compte Teams 1	147[.]78[.]47[.]21
Hash Dossier « Significant company changes.zip” (SHA1)	34744fc5c4cfa9603b2557454813029735e2f36c
Hash Fichier “exploit.pdf.lnk” (SHA256)	6da2a31b996f25ab826e6fc7fd5c8217b44bc70f4ec9e78cb741c671fa8d71a5
IP C2 - 1	5[.]188[.]87[.]58
Hash Dossier “Found_Items_Photos” (SHA1)	14c5be701f642793c21609a9c2a8b7b4eea6d370
Hash Fichier “Found_Bag_Photo1_October_3_2023_123095199.pdf.lnk” (SHA256)	0ad7c11192e797dc1981ffeeb689a0b2912317966fecbb88f01e8639d62a2d9f
Hash Fichier “Found_Items_Overview_Photo5_October_3_2023_123095199.pdf.lnk” (SHA256)	d94654fe5b715d07e514ca592195472f033d639e8268f389a8c8e102487340d5
Hash Fichier “Found_Keys_Photo3_October_3_2023_123095199.pdf.lnk” (SHA256)	a8622fb9831fd1290062bc8b37c238e7fe5732023f354299a7aea40177ff7a7e
Hash Fichier “Found_Phone_Photo2_October_3_2023_123095199.pdf.lnk” (SHA256)	ebfc09fccdabc8b5d5b404bbd005f7d789426d4335f936fea4ceebe270bf3856
Hash Fichier “Found_Wallet_Photo4_October_3_2023_123095199.pdf.lnk” (SHA256)	7c444ac31bf0d35c13aaa8dccaccd80daaa04f2ef413d129130effc0b7d22535
IP C2 - 2	185[.]39[.]18[.]170

Figure 2 tableau des IOCs