
# Travaux pratiques 02 : OSINT et CTI sur un groupe de ransomware

Département de Génie Informatique et Génie Logiciel

INF8108 : Gestion et chasse de la cybermenace

Heimanu Tepu 2007764
Ilias Bettayeb 2092408

# 1 Profil de l’entreprise [/5pts]

1.1. Créer une entreprise fictive, en tenant compte d’un budget de PME de 2 000 000 CAD.

L’entreprise que l’on a choisi pour ce TP :

Nom de l’entreprise : Cyber Auction Inc

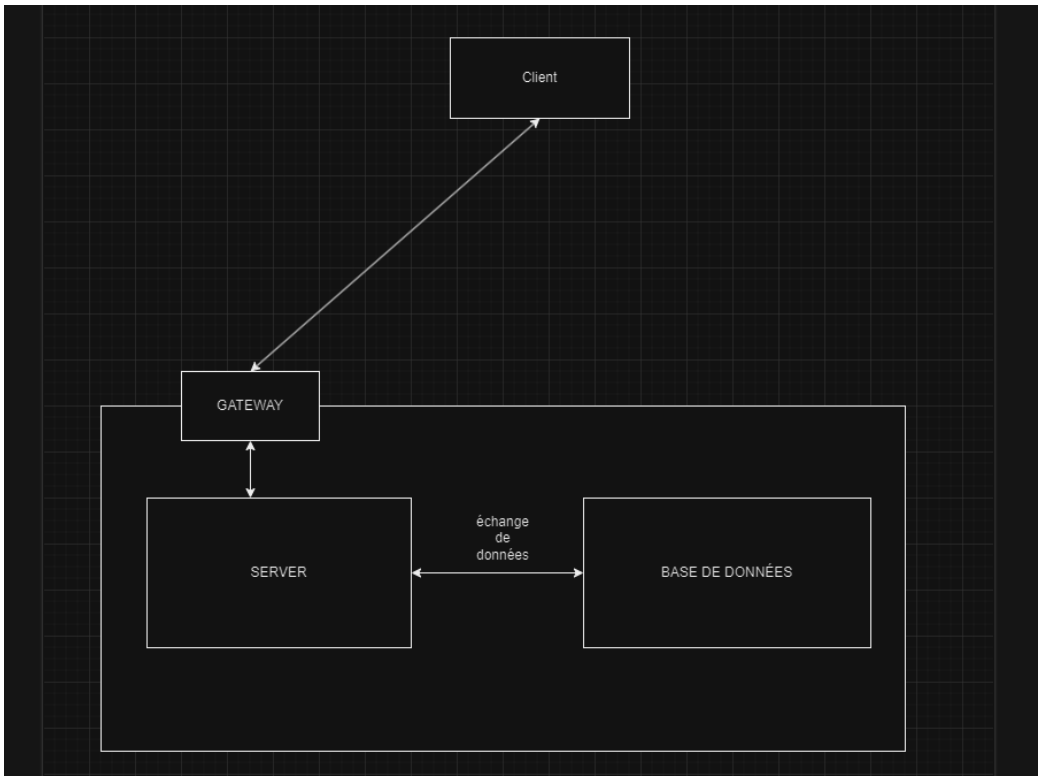
**Description de l’entreprise :** Cyber Auction Inc est une entreprise proposant une platform d’enchère en ligne. Les clients auront la possibilité de participer à des enchères qui se produiront sur plusieurs jours. Lorsqu’un client donnera un prix, ce dernier sera prélevé en crédit et remboursé si le client en question ne remporte pas l’enchère. Le remboursement se fera sous 10 jours ouvrables. Les principaux clients ciblés sont les grands musées et les grands collectionneurs voulant vendre leur collection.

Objectif de l’entreprise :

- Proposer à une solution pour les musées du monde entier et les collectionneurs du monde entier pour pouvoir participer à des enchères sur plusieurs jours dans le monde entier.

1.2. Élaborer un schéma réseau exhaustif de l’entreprise, comprenant une description des technologies actuelles en place et leurs versions, la configuration du parc informatique et les mesures de sécurité mises en œuvre.

Ci-dessous la structure de notre application web :



La partie client utilisera le Framework Angular (version 16.2.10) et le Server utilisera Node.js (version 21.1.0).

Le Serveur sera dupliqué sur 3 machines. Un load balancer viendra égaliser le trafic entre les 3 serveurs pour que la charge de chacun des serveurs soit amoindrie.

On aura le même système pour la base de données qui sera composé de 3 serveurs de stockage avec un serveur de backup.

Étant une petite entreprise, nous utiliserons les service cloud AWS. Cela évitera à l'entreprise de payer une fortune pour l'achat de l'équipement. Ainsi l'entreprise ne payera que ce les fonctionnalités qu'elle utilise et pourra facilement agrandir son infrastructure dans le futur.

Les serveurs utiliseront les instances amazones EC2 sur lesquelles nous installerons des machines virtuelles Microsoft window. Chaque machine fera tourner les servers, et chaque serveur communiquera avec les bases de données.

Pour la base de données nous utiliserons le service proposé par Amazon :

| | | | |
|---|---|---|---|
| **Amazon Neptune**<br>Service de base de données orientée graphe | Base de données orientée graphe haute performance et entièrement gérée utilisant les API open source courants, comme Gremlin, SPARQL et openCypher. | **ESSAI GRATUIT DE 30 JOURS**<br>**750 heures** d'utilisation des instance Neptune s t3.medium ou t4g.medium<br>**10 millions** de demandes E/S<br>**1 Go** de stockage<br>**1 Go** de sauvegarde | Tarification d'Amazon Neptune |

Pour ce qui est de la Gateway, elle servira principalement à bloquer les adresses IP non connues lorsqu'il y a un transfert de fichier et de laisser passer la requête ou la réponse lorsque l'adresse IP est connue.

## 2 Volet Stratégique [/15pts]

2.1. Qui est ce groupe ?

Wizard Spider est un groupe de cybercriminel basé en Russie/Ukraine, ils sont aussi connus sous le nom Trickbot

2.2. Pourquoi doit-il être surveiller ?

Il est important de les surveiller car le groupe de cybercriminel Wizard Spider est une organisation complexe avec des sous-teams et plusieurs groupes avec « un workflow professionnel hautement distribué pour maintenir la sécurité et un rythme opérationnel élevé (source : https://www.zdnet.com/article/wizard-spider-hacking-group-hires-cold-callers-to-scare-ransomware-victims-into-paying-up/).

Selon la même source que précédent, Wizard Spider possède un groupe de recherche et développement qui leurs permet d'améliorer leurs techniques ou leurs outils plus rapidement.

2.3. Pourquoi votre entreprise intéresserait ce groupe ?

Notre entreprise gère de manière digitale des actifs avec une certaines valeurs et un constent transfert de fonds entre la compagnie et les clients. De plus les données sur les clients que le groupe peut voler sont conséquent et peux mener à des pertes financières énormes, car les clients visés sont de gros collectionneurs ou des institutions d'art dans le monde entier.

2.4. Quels sont les risques associés aux types d'attaques que ce groupe pourrait lancer ?

Les risques associés aux types d'attaques de ce groupe, sont la perte des données bancaires des clients ou le vol de ces données qui peuvent être revendue au plus offrant sur des sites spécifiques. Il est possible que le groupes demande une rançon pour débloquer nos systèmes.

2.5. Existe-t-il des vulnérabilités au sein de votre entreprise que ce groupe pourrait exploiter ?

Les principales vulnérabilités au sein de notre entreprise possiblement sont :

- Les employées gérant la plateforme car wizard spider procède principalement par phishing

- le transfert de donner si le compte user des employées est compromis, car cela peut permettre à l'attaquant de faire une requête et l'upload d'un payload sur le serveur ce qui entrainerait la compromission du server et des bases de données.

- Une mauvaise gestion et surveillance des rôles et des privilèges pour certains employées

- Avoir des backups liés constamment à l'architecture. Le groupe va utiliser un script pour tuer tous les services de backups.

- utilisation de la vulnérabilité log4j qui touche les logs

2.6. Avez-vous connaissance d'attaques antérieures perpétrées par ce groupe contre des entreprises similaires à la vôtre ? Si oui, quelles ont été les conséquences de ces attaques ?

Une attaque a été perpétré contre la compagnie Colonial Pipeline qui a coûté 4.4 millions de dollars qui ont été payer en bitcoin par la compagnie. Cette entreprise n'est pas similaire à la nôtre mais la conséquence de l'attaque reste quand même énorme.

2.7. Évaluez votre niveau de préparation pour faire face à une éventuelle attaque de ce groupe.

Notre niveau de préparation actuel est minimal avec comme sécurité un simple Gateway

2.8. Quels sont les couts estimés pour renforcer votre préparation face à ce groupe ?

Pour sécuriser notre application web et notre server web, on pourrait utiliser un service que aws propose pour surveiller les cybermenaces, GuardDuty.

Ensuite on pourrait aussi embaucher des pentester pour avoir un avis extérieur sur la sécurité de notre infrastructure.

Les coûts estimés :

- GuardDuty pour une utilisation

| Analyse d'événements AWS CloudTrail Management | |
|---|---|
| Pour un million d'événements / mois | 4,00 USD pour 1 million d'événements |

| Analyse des journaux de flux VPC et des journaux de requêtes DNS | |
|---|---|
| Premiers 500 Go/mois | 1,00 USD par Go |
| 2 000 Go suivants par mois | 0,50 USD par Go |
| 7 500 Go suivants par mois | 0,25 USD par Go |
| Plus de 10 000 Go par mois | 0,15 USD par Go |

Si on considère que le nombre de Go par est de 5000 Go plus 1 million d'évènements par mois on aurait un prix de 2379 USD par mois, soit 28 500 USD par ans

- salaire minimum d'un pentester est de 60 000 CAD par ans aux Canada, si on l'embauche pour 6 mois, on devrait payer 30 000 CAD, soit 21699,03 USD

Cela coutera au total 58 500 USD par ans (cela est une estimation du coûts).

2.9. Quelles recommandations stratégiques préconiseriez-vous pour faire face à ce groupe ?

Pour faire face à ce groupe les points importants à prendre en compte est une forte sensibilisation des employés contre les campagnes de phishing. Peut-être mettre en place un mail unique utilisable seulement dans le cadre de la société. Ensuite il faudrait filtrer aux maximum tous les courriels internes et externes.

Ensuite il serait important de respecté au maximum le concept de least privilege.

Guard Duty devrait pouvoir surveiller le système au total (incluant les vulnérabilités liées aux logs), mais il serait important de continuer d'investiguer des vulnérabilités via des penteste ou des tests interne. (Source pour log4j : https://aws.amazon.com/fr/blogs/security/using-aws-security-services-to-protect-against-detect-and-respond-to-the-log4j-vulnerability/#:~:text=ECR%20private%20registries.-,GuardDuty,will%20continue%20to%20do%20so )

# 3 Volet Tactique [/15pts]

3.1. Utilisez le modelé MITRE pour détailler les TTP employés par le groupe.

Le groupe Wizard Spider utilise un nombre important de TTP, voici quelques exemples :

| | | | | |
|---|---|---|---|---|
| Enterprise | T1543 | .003 | Create or Modify System Process: Windows Service | Wizard Spider has installed TrickBot as a service named ControlServiceA in order to establish persistence.[6][7] |
| Enterprise | T1555 | .004 | Credentials from Password Stores: Windows Credential Manager | Wizard Spider has used PowerShell cmdlet `Invoke-WCMDump` to enumerate Windows credentials in the Credential Manager in a compromised network.[7] |
| Enterprise | T1005 | | Data from Local System | Wizard Spider has collected data from a compromised host prior to exfiltration.[7] |
| Enterprise | T1074 | | Data Staged | Wizard Spider has collected and staged credentials and network enumeration information, using the networkdll and psfin TrickBot modules.[6] |
| | | .001 | Local Data Staging | Wizard Spider has staged ZIP files in local directories such as, `C:\PerfLogs\1\` and `C:\User\1\` prior to exfiltration.[7] |

https://attack.mitre.org/groups/G0102/

3.2. Fournissez une description détaillée de la séquence d'attaques employée par le groupe.

Wizard Spider se focusse principalement sur les extorsions via attaques de ransomware.

Le groupe utilise une première injection du malware Qbot pour l'injection initial, puis un second malware, comme ransomware, stealer, Cobalt Strike ou reverse proxy agent, sur les machines infectées.

Afin de distribuer le malware, QBot, utilisé par Wizard Spider, organise une campagne de spam de courriels et utilise une attaque Business courriel compromise. La chaine classique d'attaque par QBot est la suivante : Campagne de spam, une victime exécute le spam, un fichier zip et téléchargé sur le bureau de la victime, le fichier est automatiquement téléchargé sur le second stage DLL et s'exécute.

La plupart du temps, il est possible de se connecter C&C Servers avec des proxys.

SI l'attaque QBot est successives, le groupe utilise SystemBC, un proxy malware exploitant socks proxy. L'équipe déploie un cluster des servers de SystemBC  pour contrôler des milliers de client. Si le client semble une bonne victime, le groupe déploie une attaque Cobalt Strike pour lateral movement, privilege escalation et exfiltration de données.

Puis on passe par l'Intrusion Server qui contient plusieurs fichiers et outils pour attaque.

L'équipe utilise alors leur propre cracking tools et maintien un server fort

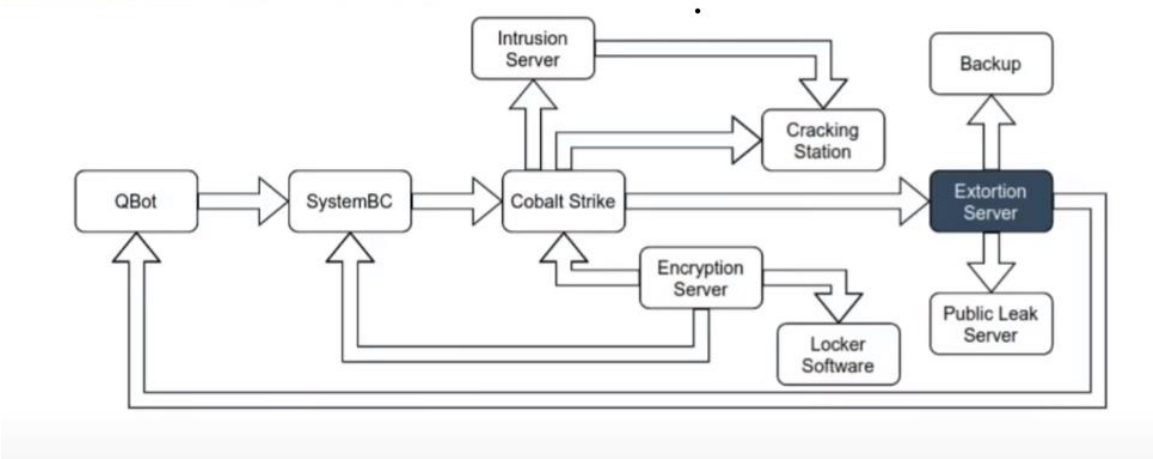
L'équipe utilise activement des extortion servers situés en France pour extraire de l'information critique sur les victimes. Les données récupérées sont souvent transféreés par réseau proxy établit par Wireguard VPN.

Les données de la victime sont aussi envoyées dans un Backup server situé en Russie pour faire un backing-up des données et dans un Public Leak Server.

L'équipe a développé un script PHP pour encrypter les machines virtuelles de la victime ou des servers Linux traditionnels qui ont un port SSH ouvert. Tout cela à l'aide du Encryption Server.

Wizard Spider compile un échantillon pour chaque victime depuis le Locker Software Server. Si l'attauqe n'est pas réussite complétement, le groupe utilise le même Locker Software pour d'autres attaques.

Voici un schéma globalde la séquence d'attaque employée par Wizard Spider.




https://www.youtube.com/watch?v=2MOsKS4La4c

3.3. Présentez des exemples concrets de malicieux, de campagnes et d'autres éléments tactiques que vos collègues pourraient utiliser pour renforcer la posture de sécurité de l'entreprise.

Selon un article du département de justice des États-Unis, Trickbot fut arrêté en 2022. Trickbot était un support de plusieurs variantes de rançongiciels comme Conti, Ryuk (source : https://www.justice.gov/opa/pr/multiple-foreign-nationals-charged-connection-trickbot-malware-and-conti-ransomware ). Un autre exemple plus concret serait la campagne qui implique BokBot et TrickBot en juillet 2017, les machines des victimes étaient infectées par BokBot qui émet une commande pour exécuter un Trickbot payload (source : https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-

same-web/ ). Selon un article de « the register », Wizard Spider serait en lien avec plusieurs organisations dont le gouvernement Russe suite à l'invasion de l'Ukraine mais aussi des organisation cybercriminel comme ceux derrière REvil et Qbot. Une grande partie des attaques de Wizard Spider sont faites selon ces étapes (ou une variation équivalente) :

- Compagne de spam utilisant Qbot, SystemBC ou des emails professionnels corrompues

- installation des malwares sur les ordinateurs Windows cible

- En utilisant « domain-based selection », ils peuvent réussir trouver la cible pour leur demande de rançon

- ils déploient Cobalt Strike pour les activités de « mouvement latéral » pour obtenir les droits administrateurs du Domain

- ils déploient Conti

(Source : https://www.theregister.com/2022/05/18/wizard-spider-ransomware-conti/ )

D'autres ressources qui pourraient être intéressants à prendre en compte :

https://malpedia.caad.fkie.fraunhofer.de/actor/wizard_spider (donne plusieurs articles qui discutent d'actualité lié aux groupes Wizard Spider ou ces sous-groupes)

https://www.cert.ssi.gouv.fr/uploadSs/CERTFR-2023-CTI-007.pdf (Rapport suite à l'attaque d'un centre hospitalier universitaire en France dans la ville de Brest. Utilisation des rançongiciel Ryuk et Conti)

3.4. Quelles recommandations tactiques préconiseriez-vous pour faire face à ce groupe ?

Pour faire face à ce groupe, il serait possible de faire l'analyse du trafic sur le réseau. Cette méthode de détection consiste à surveiller et analyser les modèles de trafic et l'inspection des paquets associés à LDAP et MSRPC qui ne suivent pas les normes de protocole et les flux de trafic attendus.

https://attack.mitre.org/techniques/T1087/002/

Surveiller les commandes et les arguments suspicieux qui pourrait servir à la modification d'un compte ou la modification des paramètres d'un compte (des commandes qui utiliserait des fichiers similaires à authorized_keys ou /etc/ssh/sshd_config.

Pour pouvoir lutter contre l'utilisation de logiciel comme Mimikatz

https://attack.mitre.org/techniques/T1098/

## 4 Volet Opérationnel [/15pts]

4.1. Indiquez les affiliations de ce groupe ainsi que ses différents noms pour chaque vendeur.

Wizard Spider est associé à Grim Spider et Lunar Spider. Wizard Spider est l'opérateur du malware TrickBot. Grim Spider est être un sous-ensemble de Wizard Spider. Lunar Spider est l'opérateur et développeur du malware BokBot (alias IcedID). Wizard Spider est aussi associé à UNC1878, TEMP.MixMaster, FIN12, GOLD BLACKBURN, ITG23 et Periwinkle Tempest

https://malpedia.caad.fkie.fraunhofer.de/actor/wizard_spider

https://attack.mitre.org/groups/G0102/

4.2. Décrivez en détail une attaque complété perpétrée par ce groupe contre votre entreprise, avec comme objectif final l'exfiltration de données.

L'attaque se déroulera comme ci-dessous (On a utilisé le pattern décrit dans la question 3.3):

- Compagne de spam utilisant Qbot

- installation un Backdoor (ex : chopstick) sur les ordinateurs Windows cible

- Via le Backdoor on pourrait l'utiliser pour initialiser une connexion ssh sur une des machines du réseau Cloud

- En utilisant « domain-based selection », ils peuvent réussir trouver la cible pour leur demande de rançon

- ils déploient Cobalt Strike pour les activités de « mouvement latéral » pour obtenir les droits administrateurs du Domain

- ils déploient Pacu pour le vol de données ou Conti pour le rançongiciel

4.3. Effectuez un mapping complet de cette attaque en utilisant le modèle MITRE ATT&CK.

Dans la question 3.3, nous avons donner comme exemple un pattern d'attaque que le groupe Wizard Spider utilise selon l'article de « the register ». Nous allons partir sur ce pattern pour mapper au complet une attaque de Wizard Spider en utilisant le modèle MITRE ATT&CK :

(Les informations dans le tableau ci-dessous sont tirées des sources suivantes : https://attack.mitre.org/groups/G0102/

https://attack.mitre.org/ )

| Tactique | Technique | Command/Exemple |
|---|---|---|
| Reconnaissance | Gather Victim Identity Information:<br>Email Addresses, Employee Names, Credentials<br><br>Phishing for Information | Exemple : Les adresses e-mail pourraient également être énumérées via des moyens plus actifs comme active scanning.<br><br>Envoie d'email (avec un formulaire à remplir) pour avoir plus d'information sur l'employée ou sur l'entreprise. |
| Initial Access | Phishing | Envoie d'email vers plusieurs acteurs de l'entreprise avec une pièce jointe malicieuse |
| Execution<br>Credential Access | Command and Scripting Interpreter | Exemple :<br>CHOPSTICK est capable d'exécuter des commandes à distance dans notre cas pour fouiller les donner de l'ordinateur cible et se connecter au réseau par ssh via les crédentials présent sur la machine infecté |
| Privilege Escalation | Abuse Elevation Control Mechanism | Exemple :<br>Accéder au compte SYSTEM grâce à l'outil Cobalt Strike |
| Discovery | Account Discovery : Domain account | Command :<br>`net user /domain` et `net group /domain`<br>Pour pouvoir avoir les cibles de valeurs pour leur attaque |
| Lateral Movement | Remote Services: SBM/Windows Admin Shares | Cobalt Strike peut utiliser Windows admin shares (C$ et ADMIN$) pour les mouvements latéraux |
| Collection<br>Exfiltration | Data from Cloud Storage | Utilisation du Framework PACU pour énumérer et télécharger les fichiers depuis un service de stockage comme AWS |
| Command and Control | Remote Access Software | Exemple :<br>TrickBot utilise le module vncDll pour contrôler à distance la machine victime. |
| Impact | Data Manipulation: Stored Data Manipulation<br>Financial Theft | Exemple: Télécharger les données ou encrypter les données et demander une rançon contre les données encryptées. |

43.4. Quelles recommandations opérationnelles préconiseriez-vous pour faire face à ce groupe ?

Pour lutter contre ce groupe on pourrait faire :

- Une compagne de sensibilisation contre les attaques de phishing
- Surveiller et analysé le trafic et les paquets d'inspection associer à des protocoles qui ne suivent pas les protocoles standards (source : https://attack.mitre.org/techniques/T1595/ )
- Surveiller les processus qui utilise le trafic réseau alors que de base ils ne le font pas (source : https://attack.mitre.org/techniques/T1595/ )

- Surveiller l'exécution de certaines commandes comme net user /domain et net group /domain (source : https://attack.mitre.org/techniques/T1087/002/ )
- Surveiller le trafic et les communications vers des IP inconnues ou qui n'ont encore jamais communiquer avec le système
- Surveiller l'utilisation d'outil Windows ou de librairie souvent utiliser par les malwares comme par exemple vncDll.
- Respecter au maximum le principe de least Privilege, et n'accorder de permission plus élever que dans des cas urgent.