# Les attaques en APT : Phases, dégâts et contre-mesures

Hakima/Marie BENYAMINA
MBA-Management du risque
Institut Léonard de Vinci
mbenyamina45@gmail.com

## SOMMAIRE



## I. Qu'est-ce qu'une attaque APT ?

Une attaque APT (Advanced persistent threat) est une menace persistante avancée sur le long terme ayant pour but une collecte de données sensibles par la compromission et le maintien des portes dérobées sur le système d'information sans forcément se baser sur des trésors d'ingéniosité et de technique mais surtout sur une préparation rigoureuse et bien structurée par un groupe de cybercriminels, chacun avec une tâche précise à effectuer.

## II . Cycle APT : Quelles sont les phases des attaques en APT ?

### Phase 1 : Reconnaissance

Les attaquants démarrent leurs opérations par cette phase efficace qui consiste à collecter toutes les données exploitables en utilisant les principales sources d'informations

#### Reconnaissance passive

Une phase de recherche et collecte d'informations qui ne déclenche aucune alarme du côté de la Cible, outils utilisés : les sites de l'entreprise, les communiqués de presse, les documents publics, livres blancs, rapports, réseaux sociaux, collecte d'adresses mails.
Durant cette phase, l'attaquant peut avoir une vue sur des projets en cours, sur l'état de santé de la société, ou même deviner quelles technologies informatiques sont utilisées en interne ou les noms des chercheurs impliqués sur un projet, cette dernière information est très intéressante pour un cybercriminel qui cherche des secrets industriels.

#### Reconnaissance active

Nécessite plus de préparation par le cybercriminel parce qu'elle laisse des traces qui pourraient alerter l'entreprise. Parmi les méthodes et outils utilisés : l'anonymat, les aspirateurs de sites web, les scanners de vulnérabilités, les moteurs de recherche.

L'attaquant peut récupérer des informations concernant les serveurs, domaines, sous-domaines ainsi que les adresses, les e-mails, les numéros de téléphone et de fax pour les contacts techniques et administratifs du dépositaire du nom de domaine. Si l'attaquant par exemple découvre dans le Whois un e-mail tel que nom-prenom@nomdel'entrepriseX.fr, il pourra deviner le format des e-mails de l'entreprise et n'aura besoin que du nom des employés pour trouver leur e-mail. Les noms d'employés sont généralement disponibles sur différents réseaux sociaux, que le cybercriminel pourra utiliser par la suite pour envoyer des mails en SpearPhishing et potentiellement les infecter. Cette dernière tâche fait partie de la deuxième phase expliquée ci-dessous

Les contre-mesures :

- La sensibilisation de tous les employés aux dangers du cyberespace
- La nécessité de ne communiquer que ce que les employés pensent que le correspondant est en droit de savoir

## Phase 2 : Compromission initiale

Cette phase repose sur la recherche d'une porte d'entrée dans le réseau informatique de la société.

Les attaquants utilisent énormément la technique du SpearPhishing, et disposent ainsi d'une bonne connaissance de leur cible grâce aux informations collectées durant la phase de reconnaissance.
Contrairement aux mails de Phishing qui sont envoyés à des personnes choisies aléatoirement par les cybercriminels, la technique de SpearPhishing permet de créer des e-mails personnalisés convaincants et adaptés à la cible.
Le but est de compromettre l'ordinateur du destinataire soit en incluant une pièce jointe qui infectera l'ordinateur, soit en incitant l'utilisateur à cliquer sur un lien contenu dans l'e-mail, qui mènera lui aussi à une infection.
Les contre-mesures pour limiter ce risque, sont d'être prudent lorsqu'on reçoit des e-mails contenant des liens vers des sites web ou des pièces jointes, même s'ils semblent provenir d'une amie ou d'un collègue.

### Comment peut-on savoir s'il s'agit bien d'un vrai mail ou d'un mail de SpearPhishing ?

Souvent, un mail suspect contient beaucoup de fautes d'orthographe, mais il faut reconnaître que c'est de moins en moins le cas.
L'expéditeur du mail a l'habitude d'utiliser la même signature, les mêmes phrases, les mêmes formulations.
En cas de doute, il est indispensable de contacter la personne émettrice par téléphone afin de lui demander confirmation que c'est bien elle qui a envoyé le e-mail.
Si le e-mail provient d'un organisme financier, ne jamais cliquer sur le lien proposé, saisir l'URL dans le navigateur directement.
Le cybercriminel peut utiliser une autre méthode d'infection rapide et de masse, il s'agit de l'infection par Watering Hole :
Le Watering Hole consiste en infecter un site légitime connu et fortement visité par de nombreux internautes, afin de tenter d'exploiter des vulnérabilités sur le système qui visite le site.

## Phase 3 : Compromission initiale-malwares et exploits

Le renforcement des accès intervient à l'issue de la compromission initiale. Cette étape permet aux attaquants de placer des backdoors à différents endroits du réseau informatique de la cible, afin de disposer de plusieurs accès différents, notamment dans l'hypothèse où l'un de ces accès serait découvert et désactivé par la cible.
Le pirate utilise les exploits, des programmes développés pour exploiter les vulnérabilités du système et des logiciels qui sont quasi obligatoires en entreprise tel que le navigateur internet, les logiciel d'Adobe, Word, Excel, Java ou encore différents types d'outils et de malwares. Il en existe des centaines et qui évoluent régulièrement, tel que Cheval de Troie qui permet d'obtenir une porte dérobée, et a la possibilité d'enregistrer des frappes de

clavier ou faire des captures d'écran ou un Dropper qui est un malware qui installe d'autres fichiers et s'efface par la suite pour ne pas laisser de trace.
Notons que certains cybercriminels modifient ou chiffrent les malwares pour contourner les antivirus et les pare feux.

## Phase 4 : Renforcement des accès et mouvements latéraux

Les mouvements latéraux permettent aux attaquants l'obtention de droits d'accès vers d'autres systèmes internes et de parcourir tout le réseau de la cible pour rechercher les informations intéressantes à détourner. Pour cela, le cybercriminel profite de la faiblesse de configuration des postes de travail comme des droits d'écriture inappropriés sans oublier la mauvaise configuration des applications, les exécutables présentant un chemin d'installation non sécurisé permettant de passer d'administrateur local, à celui d'administrateur de domaine.

Les contre-mesures :

- Éviter les configurations incorrectes
- Installer les patchs dans les applications
- Éviter les mots de passe par defaut ou l'absence de mots de passe, surtout sur certains comptes systèmes.

## Phase 5 : Exfiltration de données

Une fois les données trouvées, il faut les exfiltrer. Cette phase consiste donc en l'envoi des informations volées vers l'attaquant, ce dernier peut utiliser plusieurs types d'exfiltrations tel que l'exfiltration par DNS.

La détection complète des attaques APT avant exfiltration de données est ostensiblement difficile. Néanmoins, grâce à l'analyse des logs de façon transversale, SIEM (*Security information and event management)* peut récolter les évènements de sécurité de tout type et du Big Data qui, en corrélant signaux, signaux faibles et signaux lents pourra dans l'avenir, être une réponse aux attaques en APT.

## II. Les victimes ?

Aujourd'hui, une attaque APT peut viser des individus, associations, fondations, groupes d'activistes, entreprises et gouvernements du moment où une de ces entités détient des informations sensibles.

## III. Les attaquants ?

Ces cybercriminels partagent entre eux les ressources, ne laissent aucune trace exploitable par les experts en sécurité informatique.
Personne ne connaît le nombre d'attaquants qui compose le groupe ni les profils de ces attaquants.
On peut imaginer qu'il s'agit de plusieurs profils : hacker, analyste-Threat Intelligence, développeur et administrateur système.

## V. Conclusion

Il est indispensable de disposer d'outils utilisés efficacement par des experts, accompagnés d'une forte capacité en Threat Intelligence, analyse centrée sur l'identification de la menace et sur ce qui intéresse les cybercriminels au sein de l'organisation, afin d'éviter le déclenchement de l'attaque.

Il est également exhorté d'effectuer des analyses de vulnérabilités et des tests d'intrusion de façon régulière.

Et une bonne préparation consiste à procéder à des simulations réelles d'APT, déployant l'ensemble des phases d'attaque.