APT (Advanced Persistent Threat)
Les menaces persistantes avancées

Gérard PELIKS
ARCSI
Les « Lundi de la Cybersécurité »

Organisateurs

Pr Ahmed Mehaoua
Université Paris Cité

Béatrice Laurent

Gérard Peliks

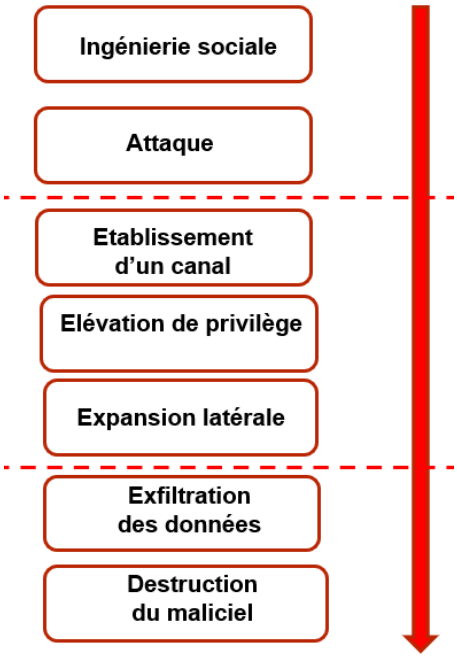
Une menace terrible pèse sur vos données : Les APT

Lorsqu'une TPE/PME est piratée, elle est victime de ses lacunes en sécurité.
Lorsqu'une grande organisation est piratée, elle est victime d'une **APT.**

Ceci est bien sûr une légende urbaine et les APT, Advanced Persistent Threats ou menaces persistantes avancées, qui concernent les organisations petites et grandes, sont l'une des menaces les plus insidieuses parmi les agressions possibles venant du cyberespace.

Les APT mettent vos informations les plus sensibles en mesure d'être dérobées, de manière furtive et pendant longtemps. Que ce soit pour voler les informations qui peuvent compromettre une réputation, mais aussi pour dérober des informations sensibles, les APT peuvent frapper toute structure, qu'elle soit grande ou petite. Les APT sont persistantes car le vol de données peut s'étaler sur une très longue période. Elles sont avancées par la phase d'ingénierie sociale qui précède l'attaque qui est souvent très sophistiquée. Elles sont furtives car vous ne les voyez pas venir, et vous ne les voyez pas agir.

Une attaque en APT débute par une prise de renseignements pour obtenir une connaissance approfondie de la victime et de son système d'information. Que racontent les employés de l'organisation ciblée, et leurs amis, sur les réseaux sociaux ? Qu'écrivent-ils sur leurs conditions de travail, sur leurs projets, sur les outils et les applications qu'ils utilisent ? Cela peut durer des jours, des semaines, des mois et l'attaquant a constitué une image très précise du système d'information et des vulnérabilités de sa future victime.



Et vient l'attaque...

La victime reçoit un courriel de sa direction avec un fichier PDF attaché. Le courriel ne vient pas de la direction mais de l'attaquant qui a usurpé l'adresse, et le fichier PDF attaché est contaminé. L'ouverture du fichier PDF permet à l'amorce du vecteur d'attaque, contenu dans le fichier attaché, d'entrer dans le poste de travail de l'employé inconscient. L'attaque a réussi, le ver est dans le fruit.

Il faut se méfier de tout courriel qui semble bizarre, car un petit clic peut se traduire par une grande claque.

L'amorce du vecteur d'attaque se met en rapport, par l'Internet, en traversant coupe-feux et routeurs de l'organisation sans se faire remarquer, avec le serveur du prédateur pour télécharger ce qui va constituer le vecteur d'attaque complet. Il cherche et découvre le mot de passe administrateur et acquiert tous les droits. Il existe des applications de contrôle qui surveillent les augmentations de privilèges et détectent ainsi les débuts d'attaques en APT. Si on ne détecte pas l'attaque à ce moment-là, après il est trop tard.

Le vecteur d'attaque se répand par l'Intranet sur les postes des autres employés qui travaillent sur le même projet, ou dans le même secteur qui intéresse le prédateur, et exfiltre les données sensibles.

Les dispositifs de DLP (prévention de la fuite de données) peuvent s'apercevoir de l'existence de fonctionnements anormaux, comme le déplacement, sans raisons, de gros volumes de données. Les applications de SIEM, couplées à des applications faisant appel au Big Data et à l'Intelligence Artificielle, et interprétées dans un SOC, peuvent se révéler très utiles pour s'apercevoir à temps que l'organisation est sous une attaque en APT.

Et quand l'attaquant a suffisamment sévi sur le système de sa victime, il détruit, à distance, le vecteur d'attaque et tout ce qui pourrait constituer une preuve. Il ne laisse aucune trace de son passage, L'organisation ne saura jamais qu'elle a été attaquée.

Des contre-mesures existent pour diminuer les risques liés à toutes les phases d'une attaque en APT. Nous allons, dans ce « Lundi de la Cybersécurité » explorer les différentes phases d'une attaque en APT et indiquer ce qu'il aurait fallu faire pour diminuer les risques, sachant que le risque zéro ne sera hélas jamais atteint.

Qui est Gérard PELIKS ?

Gérard Peliks a travaillé plus de 40 ans dans l'industrie **(**Thomson, Digital Equipment, AIRBUS Cybersecurity) dont plus de 20 ans dans la sécurité du numérique.

Aujourd'hui retraité, il s'implique dans des associations comme l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information). Il est chargé de cours sur la cybercriminalité/cybersécurité/cryptologie dans des mastères et MBA d'écoles d'ingénieurs et d'universités.

Il anime les « Lundi de la cybersécurité ».

Demande d'inscription au lundi 19 mai, par visio-conférence à partir de 18 h 00.

Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à Béatrice Laurent co-organisatrice de nos évènements :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 19 mai, dès 18 h 00.** La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. C'est toujours un agréable moment avant 18 h 00.

Quelques minutes avec Claire ALBERIO

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence du « Lundi de la Cybersécurité » de février sera animée par **Claire ALBERIO.**

Avec 30 ans d'expérience dans les réseaux et la cybersécurité, **Claire Alberio** a évolué du consulting à l'architecture et la stratégie, jusqu'à la **direction de la cybersécurité chez Orange**. Elle vient d'entrer au Conseil d'Administration de la prestigieuse ARCSI. En parallèle, elle poursuit un doctorat à **l'Université Paris-Saclay**, explorant la gestion des risques perçus ou ignorés. Toujours animée par la diversité des défis, elle conjugue expertise technique, stratégie et transmission avec passion.

Pour le prochain lundi cyber, elle nous parlera des **réserves citoyennes et opérationnelles de la Gendarmerie nationale**. Aujourd'hui **lieutenant-colonel de la réserve Spécialiste du Comcyber-MI**, elle accompagne les collectivités nationales sur la gouvernance et la prévention des risques numériques, tout en coachant gendarmes et ingénieurs.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez, sur le web de l'ARCSI en **https://www.arcsi.fr/evt_passes.php** tous les détails, slides, parfois aussi les enregistrements et des comptes rendus écrits par Clarisse Véron, élève du master2 « Cybersécurité et e-Santé » de l'Université Paris Cité.

Par exemple, pour le « Lundi de la Cybersécurité » du mois de mars :

La lettre d'invitation est **disponible ici**.
Les slides de la présentation de Pierre-Marie Lore sont **disponibles ici**.
Les slides du quart d'heure cyber sont **disponibles ici**.
Le compte-rendu est **disponible ici.**
La rediffusion est **disponible ici**.

Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos futurs lundis. Donc il est conseillé d'être connectés pour les suivre par Zoom.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?
Prompt posé à Gemini (l'IA Générative de Google) :

Comment une attaque en APT peut-elle réussir à voler des données sensibles ?

Une attaque APT (Menace Persistante Avancée) est une opération complexe et ciblée qui vise à infiltrer un système informatique et à y rester indéfiniment, dans le but de voler des données sensibles. Voici les étapes typiques d'une telle attaque :

1. **Reconnaissance :**
   - Les attaquants recueillent des informations sur la cible (employés, technologies, partenaires, etc.) pour identifier les vulnérabilités.
2. **Intrusion initiale :**
   - Ils exploitent ces vulnérabilités pour accéder au réseau, souvent via des techniques d'ingénierie sociale (hameçonnage ciblé), des logiciels malveillants ou des failles de sécurité.
3. **Établissement d'un point d'ancrage :**
   - Une fois à l'intérieur, ils installent des portes dérobées et des outils pour maintenir leur accès et se déplacer discrètement dans le système.
4. **Mouvement latéral :**
   - Ils se déplacent à travers le réseau pour atteindre les systèmes contenant les données sensibles, en utilisant des privilèges volés et des outils de piratage avancés.
5. **Exfiltration des données :**
   - Ils collectent, compressent et cryptent les données volées, puis les envoient vers des serveurs contrôlés par les attaquants.
6. **Dissimulation :**
   - Ils effacent les traces de leur activité pour éviter d'être détectés et maintenir leur accès à long terme.

Caractéristiques clés d'une attaque APT :

- Persistance : Les attaquants restent cachés pendant des mois, voire des années.
- Ciblage : Les attaques sont spécifiquement conçues pour une cible précise.
- Sophistication : Elles utilisent des outils et des techniques avancés pour contourner les mesures de sécurité.
- Motivation : Les attaquants sont souvent motivés par l'espionnage, le vol de propriété intellectuelle ou le sabotage.

Comment se protéger :

- Mettre en place une stratégie de sécurité multicouche (pare-feu, antivirus, détection d'intrusion, etc.).
- Former les employés à reconnaître les tentatives d'hameçonnage et autres attaques d'ingénierie sociale.
- Surveiller en permanence le réseau et les systèmes pour détecter les activités suspectes.
- Mettre à jour régulièrement les logiciels et les systèmes d'exploitation pour corriger les vulnérabilités.
- Établir une stratégie de sauvegarde et de récupération de données.

Bien écrit pour un logiciel d'Intelligence Artificielle dopé aux réseaux de neurones à qui on a fait parcourir des milliards de lignes de textes. Le lundi 19 mai, vous aurez un être humain sur Zoom (moi), et non seulement je vous en dirai plus, mais je répondrai aussi à vos questions. Et il y aura aussi une intervention de Claire ALBERIO, Directrice Cybersécurité d'Orange Ile de France.