APT (Advanced Persistent Threats)
Les menaces persistantes avancées

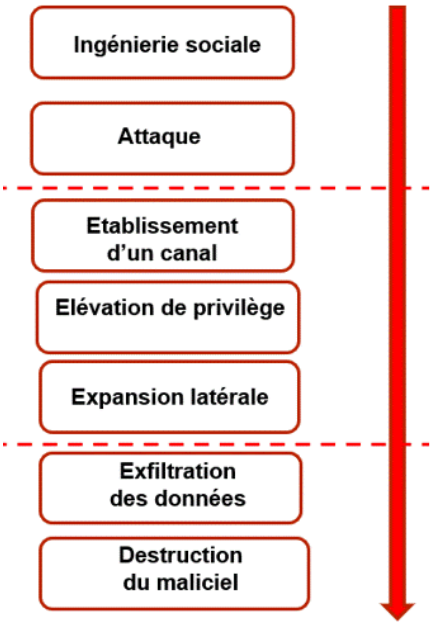
Pourquoi deux lettres des « Lundi de la Cybersécurité » 81 et 82, pour un évènement sur les APT ?

Depuis notre « Lundi de la Cybersécurité » mensuel, celui du mois d'avril, le 7 avril, avec Keren BISMUTH sur le **DLP** (Data Loss Prevention) et notre prochain Lundi, celui de mai, le 19 mai, sur les **APT**, dans la continuité du DLP, de nombreux jours se seront écoulés. Un sujet aussi important que les APT (**A**dvanced **P**ersistent **T**hreats) méritait une deuxième lettre d'information, la voici.

Au « Lundi de la Cybersécurité » du mois de mai, j'aurai le plaisir de traiter ce sujet avec une manière très insolite qui vous étonnera... Ces attaques en APT sont redoutables et très sophistiquées. Elles sont menées par des experts, souvent à la solde d'Etats dans leurs pratiques du cyber-espionnage. Elles peuvent s'étaler sur plusieurs années sur les cibles qui les intéressent. Vous ne les voyez pas arriver, mais l'un d'entre vous a commis l'erreur de cliquer sur un hyperlien ou sur un fichier PDF attaché à un email, qui, vous ne vous en êtes pas doutés, contenait un code malveillant.

Et là commence l'attaque qui va siphonner les données qui intéressent les cyberprédateurs, comme des projets d'entreprises, des secrets de fabrication, voire des secrets d'Etat quand les cibles sont des institutions

gouvernementales et militaires. Et ce vol de données va s'étaler sur plusieurs mois, parfois sur plusieurs années.



Pour faire bien passer, de manière pédagogique et sans vous barber, les explications techniques sur le déroulement de ces attaques redoutables, qui vous guettent car elles se multiplient actuellement avec l'instabilité du monde, et les conseils pour en diminuer les risques, nous essaierons d'en faire **un grand spectacle et je ne serai pas seul** (pour une fois que j'interviens pour traiter un sujet dans un de nos « Lundi »).

Nous verrons le cheminement de l'attaque, depuis la prise de renseignements pour obtenir une connaissance approfondie de votre organisation, de son personnel, de ses données sensibles, et de ses systèmes d'information, jusqu'au déclenchement de l'agression. Nous parlerons du passage du logiciel malveillant en mode administrateur de votre poste de travail, jusqu'à son élévation en privilèges, puis à l'expansion latérale qui contaminera celles et ceux qui sont impliqués dans le même secteur, ou sur le même projet que vous.

Nous parlerons de l'exfiltration des données que recueillent les prédateurs, et qui peut durer plusieurs mois ou plusieurs années avant que vous vous aperceviez qu'il y a un problème avec votre système d'information. Et quand vous et votre organisation ne les intéressent plus, ces prédateurs effacent toutes les traces de leur « visite » et disparaissent, jusqu'à leur retour quand votre organisation détient à nouveau des secrets auxquels ils vont avoir accès.

Je vous parlerai ensuite des contre-mesures qui peuvent tout de même être installées pour diminuer les risques liés à chaque phase d'une attaque en APT. Elles ne permettent pas, malheureusement, d'annuler ces risques, le « Risque 0 » n'existant pas, mais au moins elles peuvent permettre de les maîtriser en partie.

Qui suis-je ?

Je me présente : **Gérard Peliks** a travaillé plus de 40 ans dans l'industrie (Thomson, Digital Equipment, EADS puis AIRBUS Cybersécurité) dont plus de 25 ans dans la sécurité du numérique.

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

Il coanime, avec Béatrice Laurent et le Pr Ahmed Mehaoua, les « Lundi de la cybersécurité » sur une base mensuelle.

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 (surtout celui-là et je m'y emploierai personnellement). Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien pour entrer dans 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.

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 que nous partageons 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.

Orange Cyber Task Force

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

Avec 30 ans d'expérience dans les réseaux et la cybersécurité, **Claire** 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 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** les comptes rendus écrits par Clarisse Véron, élève du master2 « Cybersécurité et e-Santé » de l'Université Paris Cité, et parfois tous les slides, et les enregistrements.

Pour le « Lundi de la Cybersécurité » du mois d'avril :
La lettre d'invitation est **disponible ici**.
Les slides de la présentation des activités de l'ARCSI de Didier LOOTEN sont **disponibles ici**.
Le compte-rendu est **disponible ici**.
La rediffusion est **disponible ici**.

Keren n'a pas souhaité que ses slides soient diffusés, donc nous ne diffusons pas non plus la retransmission complète de cet évènement qui montre bien sûr ses slides.

Donc attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos futurs lundis. Il est conseillé d'être présents et 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 que j'ai posé à Gemini (l'IA Générative de Google) :

Quels sont les groupes APT connus ?

Voici une partie de la réponse de cette IA générative :

Voici une liste de quelques groupes APT (Advanced Persistent Threat) connus, classés par affiliation supposée ou zone d'activité :

Chine :

- **APT1 (Comment Crew, PLA Unit 61398)** : Un des groupes les plus anciens et notoires, connu pour des attaques d'espionnage économique à grande échelle.
- **APT3 (Gothic Panda, Buckeye)** : Ciblant les secteurs de l'aérospatiale, des communications et de la technologie.
- **APT10 (MenuPass, Stone Panda)** : Vise les secteurs de la technologie, de l'automobile et de la pharmacie.
- **APT17 (Deputy Dog, Elderwood)** : Impliqué dans de nombreuses campagnes d'espionnage.
- **APT19 (Deep Panda, C0d0so0)** : Connu pour cibler les entreprises et les cabinets d'avocats.
- **APT27 (Emissary Panda)** : Vise divers secteurs, y compris le gouvernement et la défense.
- **APT31 (Judgment Panda, Zirconium)** : Ciblant les secteurs de l'aérospatiale, des télécommunications et le gouvernement.
- **APT41 (Winnti)** : Mêle espionnage et activités de cybercriminalité financière.
- **Volt Typhoon** : Se concentre sur les infrastructures critiques aux États-Unis et en Asie-Pacifique.
- **Flax Typhoon** : Ciblant des organisations aux États-Unis.
- **Salt Typhoon (GhostEmperor, FamousSparrow)** : Ciblant les réseaux de communication critiques.

Russie :

- **APT28 (Fancy Bear, Sofacy)** : Lié au renseignement militaire russe (GRU), connu pour cibler des gouvernements, des organisations militaires et politiques.
- **APT29 (Cozy Bear, The Dukes)** : Associé au service de renseignement étranger russe (SVR), ciblant des gouvernements et des organisations diplomatiques.
- **Sandworm (Voodoo Bear)** : Lié au GRU, connu pour des attaques destructrices contre des infrastructures critiques.
- **Turla (Snake, Venomous Bear)** : Groupe sophistiqué ciblant des entités gouvernementales et diplomatiques.
- **Gamaredon (Primitive Bear)** : Ciblant principalement l'Ukraine.

Iran :

- **APT33 (Elfin, Refined Kitten)** : Vise les secteurs de l'aérospatiale et de l'énergie.
- **APT35 (Charming Kitten, Phosphorus)** : Ciblant la recherche médicale, les infrastructures et les élections.

- **APT39 (Chafer, Remix Kitten)** : Ciblant les télécommunications et d'autres secteurs au Moyen-Orient.

Corée du Nord :

- **Lazarus Group (APT38)** : Connu pour des vols financiers, des cyberattaques destructrices et des opérations d'espionnage.
- **Kimsuky** : Se concentre sur la collecte de renseignements en Corée du Sud et dans la région.
- **APT43** : Mène des activités d'espionnage et de cybercriminalité pour soutenir les intérêts nord-coréens.

Autres groupes notables :

- **Equation Group** : Un groupe très sophistiqué, dont certains liens suggèrent une affiliation avec les États-Unis.
- **APT40 (TEMP.Periscope)** : Un groupe chinois ciblant divers secteurs, notamment l'ingénierie et la marine.
- **Blind Eagle (APT-C-36)** : Un groupe d'espionnage ciblant principalement la Colombie.
- **Bahamut** : Un groupe de mercenaires cybernétiques.

Il est important de noter que l'attribution des attaques à des groupes spécifiques peut être complexe et sujette à des incertitudes. Les noms et les affiliations des groupes APT peuvent également évoluer avec le temps. De plus, de nouveaux groupes sont découverts régulièrement.

Cette liste n'est pas exhaustive, mais elle donne un aperçu des groupes APT les plus connus et de leurs activités. N'hésitez pas si vous avez d'autres questions.

Mon appréciation :

Très instructif. Bravo à ce logiciel d'Intelligence Artificielle Générative dopé aux réseaux de neurones et qui a été entrainé sur des milliards de données. Mais le lundi 19 mai, vous aurez, connecté, un vrai être humain sur Zoom, et non seulement je vous en dirai plus, mais je répondrai aussi à vos questions, après l'intervention de Claire ALBERIO, Directrice Cybersécurité d'Orange Ile de France, qui nous aura parlé de ses actions dans les Réserves Citoyennes et Opérationnelles de la Gendarmerie nationale.

A lundi 19 mai pour les inscrites et les inscrits.

Gérard

Vous pouvez accéder à la lettre précédente no 81 en :

https://www.arcsi.fr/doc/Lettre-Lundi-Cyber-No81.pdf