Advanced Persistent Threat

Définitions :

Advanced Persistent Threat (APT) : Ou en français, Menace Persistante Avancée, est une stratégie d'attaque informatique sophistiquée et persistante. C'est-à-dire que l'attaque est susceptible de se maintenir sur de longues périodes. Ces attaques sont menées par différents groupes, le plus souvent liés à une entité étatique, ciblant d'autres états à des fins d'espionnage industriel ou de guerre économique. Cela dit, certains experts considèrent que la divulgation des outils de groupes APT tout au long de l'histoire a pu permettre l'émergence de groupes APT criminels indépendants.

Cyber Threat Intelligence (CTI) : Cette discipline a pour but de collecter et d'analyser toutes les informations liées aux menaces du cyberespace afin de brosser un portrait des attaquant, leurs techniques, tactiques et procédures.

Histoire :

Le terme d'Advanced Persistent Threat a été mis au jour aux alentours de 2005, à la suite de l'opération Titan Rain (attaque informatique visant des systèmes d'information américain et attribué sans certitude à la Chine. Cette opération aurait duré plus de 3 ans). Ce type d'attaque a été popularisé à la suite de différentes affaires, comme l'attaque contre le journal « The New York Times », attribué à un groupe chinois qui sera appelé par la suite APT1.
Attention, une idée fausse, communément répandue serait que les APT ne ciblent que des gouvernements occidentaux. Il est vrai que les APT contre les gouvernements occidentaux sont très publicisés, cela dit, il existe de nombreux groupes APT attribués à ces pays-ci, comme Equation Group, faction de la NSA spécialisée dans le cyber renseignement et opérant pour le gouvernement américain.

Les groupes APT :

Voici une liste non exhaustive de différents groupes APT ;

APT25 (aka Uncool, Vixen Panda, Ke3chang, Sushi Roll, Tor) [Chine] : Ce groupe a pour but principal le vol de données, et ont opéré dans les secteurs de la défense, des médias, de la finance et du transport. Notamment en Europe et aux États-Unis.

Equation Group (aka Shadow Brokers) [USA] : Ce groupe, lié à la NSA et de ce fait au gouvernement américain est connu pour avoir ciblé depuis 2001 des infrastructures de l'industrie nucléaire en Iran. Ses autres cibles connues sont la Syrie, l'Afghanistan et le Mali.

Unit 8200 [Israël] : L'unité 8200 a été suspectée par plusieurs médias et experts d'avoir créé le virus Stuxnet, celui-ci ayant été déployé sur des infrastructures nucléaires en Iran.

APT28 (aka Fancybear) [Russie] : Ce groupe, actif depuis 2004, lié aux renseignements Russe (GRU), est connu pour des opérations telles que la cyberattaque contre TV5 monde ou encore le piratage du Comité National Démocrate.

Les acteurs du CTI :

De nombreuses entités travaillent sur le sujet des APT, que ce soient des vendeurs de solutions de cybersécurité, le NIST, le CERT, la NSA, le FBI, la DGSE, la DGSI, l'ANSSI ou encore le MITRE, étant une base de connaissances accessible à l'échelle mondiale sur les tactiques, techniques et procédures des adversaires, fondée sur des observations du monde réel.

MITRE | ATT&CK™

Mots Clés :

- APT
- Advanced Persistent Threat
- Piratage
- Espionnage Industriel
- Guerre Économique
- Malware

Bibliographie :

Mitre Att&ck : https://attack.mitre.org/
CERT : https://cert.europa.eu/
NIST: https://www.nist.gov/
ANSSI : https://www.ssi.gouv.fr/

INFORMATION SÉCURITY IS THE IMMUNE SYSTEM IN THE BODY OF BUSINESS.

(KEVIN MITNICK, INFORMATION SECURITY RESEARCHER, UNIVERSITY OF TORONTO)