APT - Advanced Persistent Threat pour menace persistante avancée

Pr Chérif DIALLO, CISSP
Professeur Titulaire des Universités
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept. Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

"Le monde est davantage menacé par ceux qui tolèrent ou encouragent le mal que par ceux qui s'emploient à le faire." Albert Einstein.

Résumé : Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui un problème crucial de cyber sécurité. Il s'agit des menaces persistantes avancées (APT). Ces dernières années, les APT ont considérablement augmenté et causé des dommages de plus en plus importants, en plus de créer davantage de discordes entre plusieurs États. Ainsi, la prise en compte des APT devient une priorité parmi les priorités dans la gestion des menaces et risques cyber. Après une brève définition, ce bulletin, donne quelques exemples d'attaques APT, leur mode de fonctionnement, et enfin les solutions à adopter pour faire face à ces menaces.

Mots clés : Vulnérabilité, Menace, APT, Hacking, Phishing, Ransomware, SIEM, SOC.

---

1. Définition

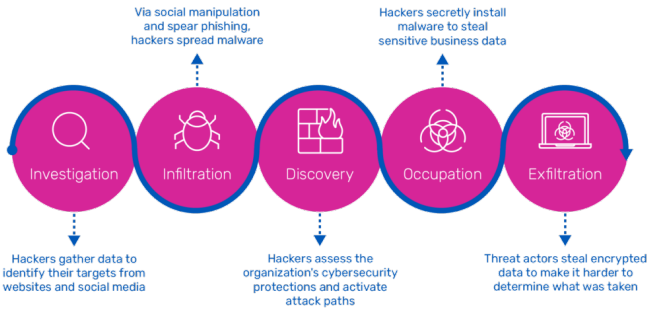
Un malware représente une cyberattaque opportuniste. Il peut être l'œuvre d'un pirate isolé. Les techniques utilisées visent souvent à implanter un logiciel malveillant dans le système ou le réseau informatique des victimes.

A l'inverse, une menace persistante avancée (APT) est une cyberattaque sophistiquée et soutenue dans laquelle un intrus établit une présence non détectée dans un réseau afin de voler des données sensibles sur une période prolongée. Une attaque APT est soigneusement planifiée et conçue pour infiltrer une organisation spécifique, échapper aux mesures de sécurité existantes et passer inaperçue.

L'exécution d'une attaque APT nécessite un degré de personnalisation et de sophistication plus élevé qu'une attaque traditionnelle. Les adversaires sont généralement des équipes de cybercriminels expérimentés et bien financés qui ciblent des organisations de grande valeur. Ils ont consacré beaucoup de temps et de ressources à rechercher et à identifier les vulnérabilités au sein de l'organisation.

Pour les APT, il s'agit donc d'un groupe agissant d'une manière non liée à une opportunité déterminée attaquant des organisations d'une manière stratégique, à long terme et avec des objectifs précis. En termes simples, les APT sont des « cyber hulks » (menaces informatiques excessivement sophistiquées) existants quelque part dans l'environnement informatique, totalement différentes des auteurs de menaces opportunistes qui, par exemple, cherchent seulement à voler quelques données de carte de crédit afin de réaliser un gain à court terme.

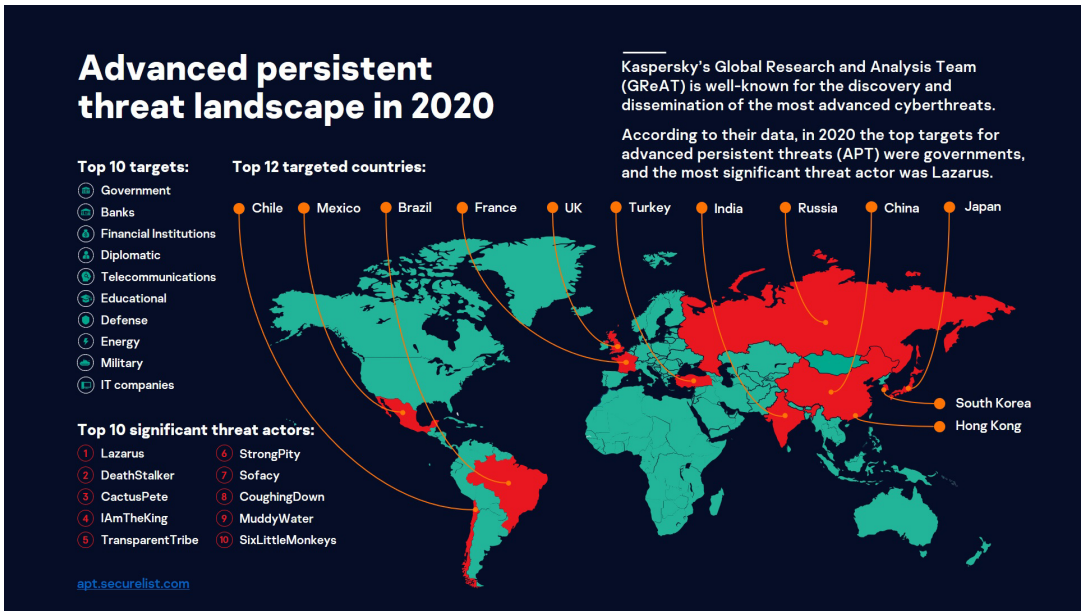
En outre, une APT n'est pas constituée seulement d'un composant d'un malware même s'il utilise parfois un logiciel sophistiqué spécifiquement développé pour mener à bien des attaques ciblées. Les APT sont dangereuses en raison des personnes qui sont à l'origine de l'opération, celles qui planifient, exécutent les campagnes APT et exercent un contrôle sur les outils. La figure ci-dessous illustre un exemple cycle de vie d'une APT en 5 phases.



2. Quelques exemples d'APT

Les victimes d'une Advanced Persistent Threat représentent des cibles de grande valeur : économique, politique, sociale. Ce sont souvent aussi des organisations à importance vitale (OIV) dans des secteurs stratégiques : énergie, transport, santé, militaire, etc. Les APT peuvent déstabiliser également la vie publique d'un pays : infiltration d'un parti politique ou de médias avant des élections.

Les APT sont donc portées principalement par des groupes de pirates financés par les États. La Russie, la Chine, l'Iran et la Corée du Nord sont souvent cités, mais, les États occidentaux financent eux aussi des groupes de hackers comme, par exemple, le groupe Animal Farm piloté par la DGSE et celui de l'Equation Group par la NSA (National Security Agency). La figure ci-dessous est le paysage des APT dressé en 2020 par Kapersky.



- ***Conti Ransomware (Russie) :*** Le groupe Ransomware-as-a-Service (RaaS), Conti, est devenu célèbre pour ses méthodes énergiques et ses vastes attaques contre des entités des secteurs public et privé. Avec d'autres groupes de malwares notoires, Conti a souligné la nécessité d'une réaction bien planifiée pour se prémunir contre des pertes potentiellement catastrophiques de biens, de personnel et de réputation. Le ransomware Conti, basé en Russie, est apparu en février 2020 et est rapidement devenu l'un des groupes de ransomware les plus actifs. En août 2020, ils ont créé un site de fuite de données et ont divulgué les données de plus de 150 entreprises à la fin de l'année, ce qui en fait le troisième groupe de fuites le plus actif, derrière Maze et Egregor. Le ransomware Conti est devenu un groupe incontournable d'acteurs de cybermenaces. Cependant, en août 2021, un ancien associé de Conti a révélé les tactiques et le cadre de Conti en matière de ransomware et l'a accusé d'utiliser ses partenaires pour une main d'œuvre à faible coût avec une rémunération minimale. Et puis, en 2022, des fuites de conversations privées entre membres ont suscité des spéculations sur son avenir.
- ***Kimsuky (Corée du Nord) :*** Kimsuky (alias Velvet Chollima, Thallium, TA406), un gang de cybercriminalité soutenu par la Corée du Nord, est actif depuis 2017 mais existe depuis 2012. Le groupe de hackers mène des opérations d'espionnage contre des groupes de réflexion sud-coréens, des sociétés d'énergie nucléaire et le Ministère de l'Unification, qui fait partie du gouvernement sud-coréen et œuvre à la réunification de la Corée. Le groupe de menaces persistantes avancées a utilisé les informations d'identification d'hébergement Web volées à d'autres victimes pour héberger leurs scripts et outils malveillants. Ces informations d'identification ont probablement été obtenues grâce à des scripts de spearphishing et de collecte d'informations d'identification. De faux sites et services ressemblant à Google ou Yahoo Mail ont été créés sur les domaines des victimes, mais l'approche la plus courante consiste à envoyer un e-mail avec une pièce jointe malveillante.
- ***Charming Kitten, APT35 (Iran) :*** Charming Kitten (également connu sous le nom de Phosphorus) est un groupe de cyberespionnage iranien de premier plan depuis 2014, lorsqu'il a orchestré une opération complexe d'espionnage sur Internet via les réseaux sociaux. Depuis lors, ces acteurs malveillants ont été à l'origine de nombreuses cyberattaques à l'échelle mondiale. En 2019, il a ciblé des universités aux États-Unis, en France et au Moyen-Orient. Fin 2020, il a frappé des organismes de recherche médicale en Israël et aux États-Unis. Depuis 2021, il exploite les vulnérabilités du serveur Microsoft Exchange via ProxyShell. En 2022, Charming Kitten avait adapté de nouvelles tactiques pour frapper plusieurs cibles.

Des renseignements ont été collectés grâce à une nouvelle souche de malware, et ils ont commencé à utiliser l'outil Hyperscrape pour voler subrepticement des e-mails dans les boîtes aux lettres.

- ***Wicked Panda, APT41 (Chine) :*** En 2020, Wicked Panda (alias Winnti, Barium ou Wicked Panda) était devenu un « cheval de bataille » des cyberopérations qui aident le gouvernement chinois, selon les cyberspécialistes et les autorités de diverses agences. Les services secrets américains ont déclaré que Wicked Panda est un « groupe de cybermenace parrainé par l'État chinois » qui est très doué pour commettre des actes d'espionnage et des délits financiers pour le bénéfice personnel et gouvernemental. Les experts décrivent le modèle de piratage chinois comme un système de groupes d'espionnage semi-autonomes sous le contrôle de l'État, le gouvernement chinois orchestrant les cyberattaques.
- ***OceanLotus Group, APT32 (Vietnam) :*** L'unité de cyberespionnage, OceanLotus Group, pirate des entreprises du secteur privé dans de nombreux secteurs, des gouvernements étrangers, des dissidents et des journalistes. Il utilise de puissants logiciels malveillants et des outils disponibles dans le commerce pour exécuter des opérations conformes aux objectifs de l'État vietnamien. En 2020, Bloomberg a déclaré qu'OceanLotus visait à accéder aux données concernant la pandémie de COVID-19 auprès du ministère chinois de la gestion des urgences et des autorités de Wuhan. Le ministère vietnamien des Affaires étrangères a rejeté ces affirmations comme étant sans fondement. Kaspersky a découvert qu'OceanLotus distribuait des logiciels malveillants via Google Play en 2020, et plus tard cette année-là, Volexity a découvert que le groupe avait créé de faux sites d'information/pages Facebook pour le profilage et la diffusion de logiciels malveillants.
- ***Sofacy ou FANCY BEAR, APT28 (Russie),*** utilise des attaques de phishing et des sites Web falsifiés qui ressemblent beaucoup à des sites légitimes afin d'accéder à des ordinateurs et appareils mobiles conventionnels. Les hackers de Fancy Bear (ou Sofacy autre nom attribué) seraient impliqués dans l'ingérence russe dans l'élection présidentielle américaine de 2016. Ils sont également soupçonnés dans l'espionnage du parti En Marche en France et du Bundestag allemand.
- ***HELIX KITTEN, APT34 (Iran),*** est actif depuis au moins fin 2015 et est probablement basé en Iran. Il cible les organisations des secteurs de l'aérospatiale, de l'énergie, de la finance, du gouvernement, de l'hôtellerie et des télécommunications et utilise des messages de spear phishing bien documentés et structurés qui sont très pertinents pour le personnel ciblé.
- ***L'Opération Aurora :*** l'attaque financée par la Chine ciblait 30 grandes entreprises américaines. Le gain de l'opération, c'est le vol du code source de produits commerciaux stratégiques.
- ***Le groupe Lazarus, adossé à la Corée du Nord,*** a attaqué une société d'armement polonaise entre 2020 et 2021. Il a également accédé aux données personnelles d'accès de salariés en publiant une fausse offre d'emploi de la société Boeing.
- ***DeathStalker, CactusPete, IAmTheKing, TransparentTRibe, StrongPity, CoughingDown, MuddyWater, et SixLittleMonkeys*** sont également des groups d'APT très actifs parmi plus de cent autres.

3. Comment fonctionne une APT ?

Les menaces persistantes avancées se composent de cinq étapes et se développent au fil du temps pour échapper à la découverte :

- ***Investigation (Collecte) :*** Au début, les pirates informatiques collectent des données provenant de plusieurs sources pour identifier leurs objectifs. Ils sont devenus plus compétents et peuvent utiliser les informations provenant des sites Web des entreprises et des réseaux sociaux pour cibler des personnes spécifiques dans l'entreprise.
- ***Infiltration*** : une fois à l'intérieur du réseau d'une victime, les pirates informatiques propagent des logiciels malveillants vers des systèmes et des personnes non sécurisés. Une menace persistante avancée commence par plusieurs approches de cyberattaque telles que la manipulation sociale, le spear phishing, la récupération des informations de connexion ou le téléchargement (via drive).
- ***Discovery (Découverte) :*** lors de la phase de découverte, les pirates informatiques restent silencieux et travaillent lentement pour éviter d'être découverts. Ils évaluent les protections de cybersécurité de l'organisation, créent une stratégie et activent de nombreuses voies d'attaque, dont une pour l'accès éventuel à distance.
- ***Occupation*** : Les pirates informatiques s'introduisent dans des systèmes non sécurisés pendant une longue période sans que la victime ne s'en rende compte. La menace persistante avancée installe ensuite secrètement des logiciels malveillants pour voler des informations commerciales sensibles telles que des e-mails, des documents, des plans de conceptions, des adresses IP, du code, etc.
- ***Exfiltration*** : une fois que les acteurs malveillants ont obtenu les données, ils attendent l'occasion de les transmettre au centre de contrôle de l'attaquant pour évaluation et éventuellement davantage d'abus et de tromperie. Les données peuvent être envoyées via des serveurs piratés ou cryptées pour rendre plus difficile la destination et la détermination de ce qui a été volé.

4. Solutions : comment se protéger contre les APT ?

Il existe de nombreuses solutions de cybersécurité pour aider les organisations à mieux se protéger contre les attaques APT. Voici quelques-unes des meilleures tactiques à utiliser :

- Déployer des capacités qui offrent à leurs défenseurs une visibilité totale sur leur environnement afin d'éviter les angles morts qui peuvent devenir un refuge pour les cybermenaces.
- Tirer parti des informations techniques, telles que les indicateurs de compromission (IOC), les indicateurs de performance, et intégrez-les dans un gestionnaire d'informations et d'événements de sécurité (SIEM). Cela permet d'obtenir plus d'intelligence lors de la corrélation d'événements, mettant potentiellement en évidence des événements sur le réseau qui, autrement, n'auraient pas été détectés.
- S'associer à une entreprise spécialisée en cybersécurité, parmi les meilleures du secteur, est une nécessité. Si une attaque APT se produisait, les organisations pourraient avoir besoin d'aide pour résister à ce type de cybermenace sophistiquée.
- Utiliser un pare-feu d'application Web (WAF) qui est un dispositif de sécurité conçu pour protéger les organisations au niveau des applications en filtrant, surveillant et analysant le trafic des protocoles de transfert hypertexte (HTTP & HTTPS) entre l'application Web et Internet.
- Faire régulièrement des audits de vulnérabilités et se renseigner sur les menaces facilitent le profilage des acteurs malveillants, le suivi des campagnes et le suivi des familles de logiciels malveillants. De nos jours, il est plus important de comprendre le contexte d'une attaque plutôt que de simplement savoir qu'elle a eu lieu, et c'est là que les renseignements sur les menaces jouent un rôle essentiel.
- Superviser les opérations de cybersécurité par la mise en œuvre de SOC (Centre Opérationnel de Sécurité) : de nombreuses organisations ont besoin d'une chasse aux menaces par une co-gestion automatique et manuelle 24h/24, 7j/7, pour accompagner leurs dispositifs de cybersécurité déjà en place.
- Savoir que la détection est essentielle dans la lutte contre les APT et il existe des concepts simples que de nombreuses entreprises tardent encore à mettre en œuvre systématiquement :
  - Enregistrer les événements proxy, les événements webserver, DNS, Anti-Virus (également les événements « nettoyés » et « mis en quarantaine »), les stocker tous dans un endroit centralisé et demander aux équipes de sécurité de les examiner.
  - Surveiller l'usage des outils OS natifs tels que powershell et psexec. L'utilisateur habituel n'en a généralement pas besoin.
  - Utiliser deux facteurs d'authentification dans la mesure du possible, y compris pour les comptes Active Directory hautement privilégiés.

5. En conclusion

"Les enfants ont le sens du juste milieu, ils semblent interpréter comme une menace toute dérogation à la norme." De Lise Parent / Les Îles flottantes.

En bref, pour prévenir et gérer les APT, les organisations doivent renforcer leurs procédures habituelles de sécurité informatique. La mise en place d'une bonne gouvernance de la cybersécurité permet en particulier de déployer des mesures de prévention adaptées. Enfin, la formation d'experts en cybersécurité devient indispensable pour répondre à la sophistication des APT. Aussi, il s'agit finalement de développer une véritable culture de la cybersécurité pour détecter et bloquer des menaces persistantes avancées qui s'intensifient donc de jour en jour. Aujourd'hui, on dénombre plus de 150 groupes d'APT dans le monde. Pour contrer leurs attaques, les moyens de protection doivent être à la hauteur de ceux des menaces : financement, sensibilisation, formation et expertise, etc.
