NOTE D'INFORMATION

26/05/2023

WASHINGTON ATTRIBUE DES CYBERATTAQUES À LA CHINE

Le 24 mai 2023, le gouvernement Américain a publiquement attribué à la Chine une série d'attaques ciblant des infrastructures critiques situées aux États-Unis ainsi que sur l'île de Guam. Un groupe d'attaquants qui serait piloté par Pékin a été identifié par Washington. Il s'agirait du groupe APT (Advanced Persistent Threat) **Volt Typhoon** suivi par Microsoft et actif depuis 2021 d'après Secureworks (AKA BRONZE SILHOUETTE). Pour renforcer la légitimé de cette attribution, les pays membres des *Five Eyes*[1] sont venus appuyer les propos de Washington.

Le terme APT, *Advanced Persistant Threat*, désigne un type d'attaque perpétré par des groupes professionnels, opérant dans des structures banalisées et financées par des États. À cet égard, les groupes qui conduisent ces APT sont **une famille de cybercriminels qui dispose de moyens financiers et techniques très importants**. Ces groupes sont capables de conduire des attaques présentant souvent un haut niveau de sophistication, préparées pendant plusieurs mois. Ces groupes APT poursuivent des objectifs précis sur le long terme en pénétrant un réseau pendant plusieurs mois voire plusieurs années, notamment en matière d'espionnage politique et/ou industriel.

Les différentes publications mettent en avant **l'usage des outils natifs Windows** par les attaquants pour s'introduire dans un système d'information. Il s'agit d'une technique intitulée « *Living off the Land* » (LotL) qui consiste à utiliser les **ressources d'ores-et-déjà disponibles sur un système**, tels que des outils d'administration standard, afin d'éviter le déploiement d'outils de piratage connus et **augmenter leurs chances de passer inaperçus**. Bien que cette technique soit répandue, ce témoignage offre un élément de contexte supplémentaire et doit pousser les défenseurs à appliquer une surveillance accrue des outils natifs Windows utilisables[2] dans ce cadre.

Sur le plan technique, il est difficile d'attribuer avec certitude l'origine d'une attaque à un groupe APT. Toutefois, certains États font le choix de désigner les pays auxquels les groupes seraient affiliés. Ce type de manœuvre s'intègre dans une stratégie de communication politique visant à afficher publiquement les activités d'un pays en utilisant le "*naming and shaming*". Dans le cas des États-Unis, leur politique étrangère **cible particulièrement la Chine**. Le concept de ***Chinese Threat*** structure notamment tout un pan de leur politique étrangère. Ainsi, selon le FBI, « *the Chinese government is seeking to become the world's greatest superpower through predatory lending and business practices, systematic theft of intellectual property, and brazen cyber intrusions*[3] ».

Il est utile de préciser qu'il ne s'agit pas de la première attribution réalisée par le gouvernement américain concernant des attaques perpétrées par la Chine sur des infrastructures situées aux Etats-Unis. A titre d'exemple, le 27 avril 2017, le CISA[4] a publié une alerte concernant une **campagne de cybervol[5] sophistiquée d'origine chinoise** visant des fournisseurs mondiaux de services technologiques et leurs clients.

[1] Les *Five Eyes* désignent un ensemble d'États alliés, principalement issus du Commonwealth dont les États-Unis, le Royaume-Uni, le, Canada, la Nouvelle-Zélande et l'Australie, dont les agences de renseignement sont en coopération étroite.
[2] LOLBAS-PROJECT. Living Off The Land Binaries, Scripts and Libraries. https://lolbas-project.github.io/
[3] FBI. *The China Threat.* https://www.fbi.gov/investigate/counterintelligence/the-china-threat
[4] L'agence pour la cybersécurité et la sécurité des infrastructures (CISA) est une agence du ministère américain de la sécurité intérieure (DHS) chargée de renforcer la cybersécurité et la protection des infrastructures.
[5] CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. 27/04/2017. *Intrusions Affecting Multiple Victims Across Multiple Sectors.* https://www.cisa.gov/news-events/alerts/2017/04/27/intrusions-affecting-multiple-victims-across-multiple-sectors

WASHINGTON ATTRIBUE DES CYBERATTAQUES À LA CHINE

Tout comme le gouvernement Américain, selon le ministère des Armées, « la France se réserve le droit d'attribuer publiquement, ou non, une cyberattaque dont elle aurait été victime, et de porter cette information à la connaissance de sa population, d'États tiers ou de la communauté internationale[1] ». Comme les États-Unis, **la France fait parfois le choix de désigner publiquement certains États**. Ainsi, en juillet 2021, les autorités françaises ont attribué une attaque au groupe chinois APT31 (AKA ZIRCONIUM)[2].

Sur le plan de la cyberdéfense, l'attribution d'une attaque peut permettre de mettre fin à une attaque de grande ampleur mais peut être aussi défavorable à la lutte contre les activités malveillantes menées par d'autres États. En effet, mettre en lumière des attaquants ainsi que les campagnes qu'ils ont menées peut les conduire à **revoir leur méthodologie d'attaque**. Ainsi, le traçage des groupes devient plus complexe, notamment pour les services de renseignement car les attaquants sont susceptibles de **modifier leurs méthodologies** (TTP [3]), or celles-ci aident parfois à les identifier[3]. Toutefois, cela n'est pas valable pour tous les groupes car certains continuent d'utiliser les mêmes techniques.

[1] MINISTÈRE DES ARMÉES. Droit international appliqué aux opérations dans le cyberespace, p.11.
[2] CERT-FR. Indicateurs de compromission du CERT-FR. https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003/
[3] Les TTP (techniques, tactiques, procédures) désignent l'ensemble des comportements observés d'un groupe cybercriminel permettant de l'identifier.

Sources :

CERT-FR. *Indicateurs de compromission du CERT-FR*. https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003/

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. 24/05/2023. *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. *China Cyber Threat Overview and Advisories.* https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. 27/04/2017. *Intrusions Affecting Multiple Victims Across Multiple Sectors.* https://www.cisa.gov/news-events/alerts/2017/04/27/intrusions-affecting-multiple-victims-across-multiple-sectors

FBI. *The China Threat.* https://www.fbi.gov/investigate/counterintelligence/the-china-threat

MICROSOFT THREAT INTELLIGENCE. 24/05/2023. *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.* https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

MINISTÈRE DES ARMÉES. Droit international appliqué aux opérations dans le cyberespace, p.11

SECUREWORKS COUNTER THREAT UNIT. 24/05/2023. *Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations.* https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations

LOLBAS-PROJECT. *Living Off The Land Binaries, Scripts and Libraries*. https://lolbas-project.github.io/