Mobile et systèmes industriels : les chantiers du framework ATT@CK

CaddyWiper, HermeticWiper, Cyclops Blink… Autant de *malwares* qui ont jalonné le volet cyber du conflit russo-ukrainien. On les retrouve aujourd'hui tous trois dans la matrice Entreprise d'ATT@CK, à la faveur de la dernière mise à jour semestrielle du *framework*.

Cet *update* a aussi élargi l'éventail des techniques d'attaque. Avec, notamment, le *spoofing* DHCP et l'évasion de débogueur. Des ajouts, il y en a également sur la matrice dédiée au mobile : résolution dynamique, détournement du contrôle d'élévation de privilèges, etc.

On en est désormais à la v11 d'ATT@ACK. Mais seulement en bêta sur la matrice Mobile. Le temps d'expérimenter une nouveauté importante : l'intégration des sous-techniques, comme sur la matrice Entreprise.

Autre chantier qui avance : la conversion des éléments du *framework* en objets interopérables. Avec la v5, le cap avait été franchi pour les méthodes de contournement. Ce qui a, notamment, facilité le repérage des techniques dont elles pouvaient empêcher l'exploitation. Avec la v10, ce sont les sources de données qui sont devenues des objets. La v11 étend la démarche aux détections. Objectif : permettre de décrire, pour chaque technique, les données à collecter ; et comment analyser ces données pour identifier la technique.

Les campagnes dans ATT@CK pour octobre

Il faudra attendre la mise à jour d'octobre 2022 pour l'extension des *assets* de la matrice ICS (systèmes de contrôle industriel). Ces *assets* sont des catégories d'actifs qu'on retrouve généralement dans ces environnements : interfaces homme-machine, serveurs d'entrée-sortie, relais de protection… Aux techniques s'ajouteront par ailleurs des méthodes de détection.

Rendez-vous également en octobre pour l'intégration des campagnes. Les unités de ce type regrouperont des activités malveillantes conduites sur une période donnée, avec des cibles et des objectifs communs. Peu importe qu'elles soient ou non liées à un acteur spécifique.
Pour le moment, en l'absence d'une telle liaison, ces activités n'entrent pas dans le *framework*. En outre, les activités liées à un même acteur font forcément l'objet d'une entrée unique.

MITRE promet aussi, à l'horizon octobre, de faciliter le croisement des matrices.

Photo d'illustration © pinkeyes – Adobe Stock