Hackers, Etats et Dark Web : le marché des failles Zero Day incontrôlable ?

Le nec plus ultra, le Saint Graal du hacking est **la faille Zero Day**, une vulnérabilité inconnue et surtout non corrigée dans les logiciels. Les éditeurs, les Etats et bien évidemment les cybercriminels sont, pas nécessairement pour les mêmes raisons, à la recherche de ces failles avec à la clé des questions d'argent (ventes, récompenses via des *Bug Bounty* ou investissement dans la R&D). Tout cet intérêt crée **un marché** dont la dynamique a fait l'objet d'une recherche par plusieurs experts et universitaires qui vient d'être présentée à la RSA Conference. L'équipe est composée de Katie Moussouris de la société HackerOne (qui organise des programmes de recherche de failles), du Dr Michael Siegel et de James Houghton du MIT, ainsi que du Dr Ryan Ellis de Harvard.

Des programmes incitatifs et des gouvernements avides

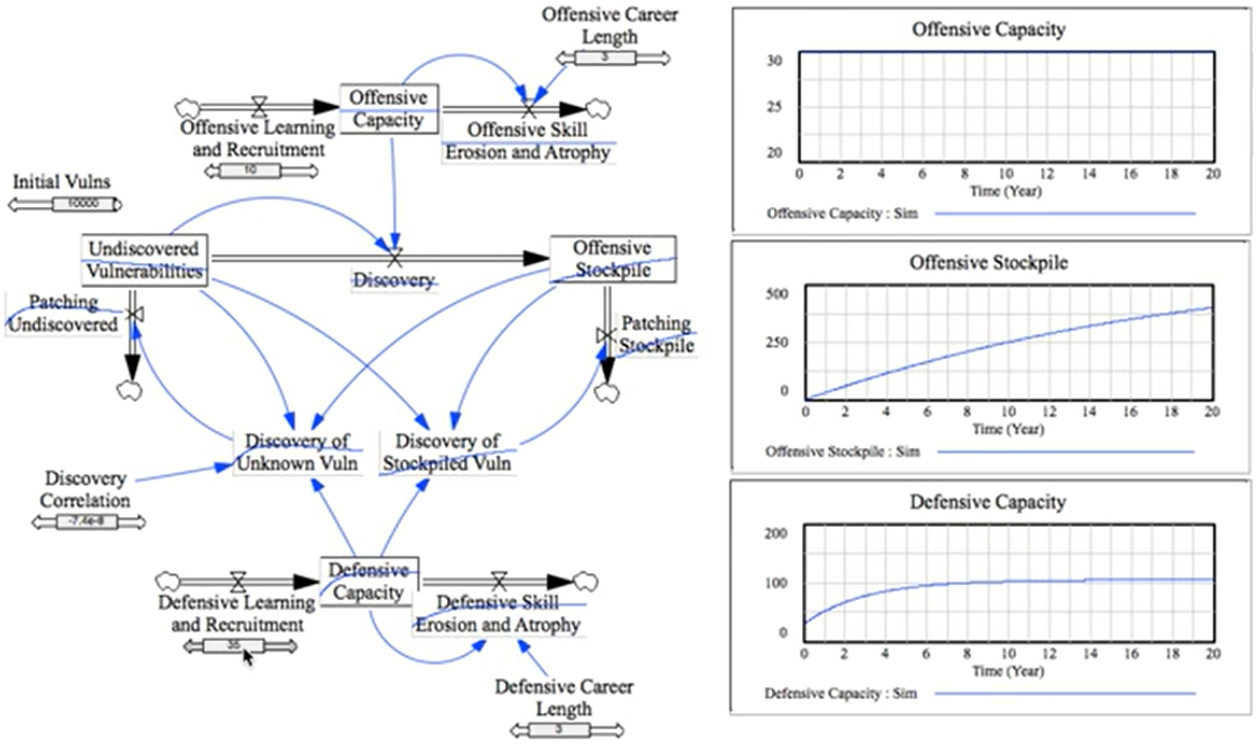
Dans un post intitulé « Wolve of The Vuln Street », Katie Moussouris a donné quelques résultats de cette étude. En premier lieu, le prix des vulnérabilités ne découle pas uniquement de l'offre et de la demande. Ainsi, **les hackers** ne sont **pas seulement intéressés par les récompenses** promises par les Bug Bounty (programme de recherche de failles), la publicité autour de leur découverte procure des **opportunités de business supplémentaire**, assure la responsable. Elle cite l'exemple du programme de Microsoft lors du lancement de la version Preview d'IE 11 qui a totalisé 28 000 dollars de primes pour la découverte de failles Zero Day. En échange, la firme de Redmond a mis en avant plusieurs chercheurs pour leur apport à la sécurité des produits. Ces hackers auraient certes pu gagner plus d'argent en revendant les failles sur le marché gris, mais avec l'inconvénient de rester dans l'ombre.

Par ailleurs, les Bug Bounty permettent dans certains cas d'**assécher les échanges de vulnérabilités non corrigées** quand elles sont rares sur les marchés souterrains. Dans cette bataille, on peut évoquer les différents projets des éditeurs comme Google avec Project Zero ou des sociétés comme Vupen qui vend des vulnérabilités aux plus offrants parmi les nations membres de l'Otan.

Un cercle vertueux qui est malgré tout fragile. En effet, le rapport rappelle que lors de la dernière Black Hat à Las Vegas, Dan Geer, RSSI du fonds d'investissement In-Q-Tel créé et géré par la CIA, a déclaré que le gouvernement américain devait s'accaparer le marché des vulnérabilités en proposant **des prix à 6 chiffres**. Cette approche risque de déséquilibrer le marché, car les hackers pourraient ne cibler que les plateformes récentes et moins matures en matière de sécurité plutôt que de travailler sur des solutions plus anciennes et donc plus stables. Il faut donc trouver un juste équilibre pour récompenser justement et suffisamment les chercheurs en sécurité afin de les inciter à trouver et à diffuser leurs découvertes.

Autre point, les éditeurs doivent travailler sur l'automatisation de la recherche de failles en proposant des outils ad hoc, plutôt que de laisser se constituer un stock de Zero Day sur les

marchés souterrains. C'est d'autant plus vrai que la stratégie des éditeurs est d'accélérer la mise sur le marché de leur produit (par exemple Microsoft avec Windows 10) les rendant au passage plus vulnérable. Les économistes du MIT et de Harvard ont essayé de modéliser (cf schéma ci-dessous) ces différentes combinaisons entre les incitations, les risques de collusions de découverte de bugs sur le marché souterrain et par les hackers, etc., pour optimiser le contrôle du marché des failles Zero Day.



La menace du Dark Web émerge

Il ne faut pas sous-estimer le marché souterrain et plus encore le Dark Web. En effet, depuis quelques mois, une place de marché nommée **TheRealDeal**, disponible via Tor, commence à faire parler d'elle. En plus d'être un magasin du vice (identifiant bancaire, drogues, etc.), TheRealDeal met en avant une boutique dédiée aux failles « rares et exclusives ». Nos confrères de *Wired* constatent que pour l'instant l'achalandage de la boutique est encore limitée, mais la liste proposée donne le ton. **Un Zero Day pour iCloud** se monnaierait l'équivalent de 17 000 dollars en bitcoin. L'annonce prévoit de faire une démonstration sur n'importe quel compte avant d'acheter la faille. Parmi les autres vulnérabilités, **les cibles sont WordPress, Android ou Windows et IE** à des tarifs pouvant aller jusqu'à 8000 dollars en bitcoin.

Il est impossible de savoir si ce site est valable ou s'il s'agit d'une arnaque. Sur une foire aux questions, les créateurs du site revendiquent une longue expérience dans la sécurité informatique. *Wired* souligne que la faille sur iCloud se révèle être une (trop) bonne affaire pour être réelle. En 2012, un exploit de ce type se marchandait 250 000 dollars et en 2013, le *New York Times* rapportait qu'une faille touchant iOS avait été vendue un demi-million de dollars au gouvernement américain. Reste que TheRealDeal pourrait connaître une fin similaire à Silk Road ou Evolution, mais le Dark Web a horreur du vide et d'autres sites devraient fleurir en promettant à leur tour la disponibilité de failles Zero Day.

A lire aussi :

Project Zero : Google lâche du lest sur les failles Zero Day
Bugzilla : une faille zero day révèle les bugs des logiciels

Crédit Photo : Releon8211-Shutterstock