Savoir profiter des erreurs des Cybercriminels | Le Net Expert Informatique

Savoir profiter des erreurs des Cybercriminels

L'affaire Ashley Madison semble le prouver une fois de plus, les cybercriminels commettent des erreurs qui peuvent leur nuire. Détecter ces fautes et savoir les utiliser sont des éléments essentiels dans la gestion des crises cyber.

DES ATTAQUES DONT LES OBJECTIFS SONT SOUVENT DIFFICILES À CERNER

L'actualité le montre trop régulièrement, les actes cybercriminels se multiplient et visent tous types d'organisation. Certains sont revendiqués et leurs objectifs sont rapidement connus. C'est le cas pas exemple de l'attaque visant le site Ashley Madison où les motivations sont explicites.

Mais dans la plupart des cas, les objectifs de l'attaquant sont beaucoup plus difficiles à identifier ! Il est pourtant crucial de le faire pour pouvoir réagir au mieux et protéger rapidement ce qui n'a pas encore été touché par l'attaque.

Une des clés pour mieux comprendre une attaque consiste à exploiter les erreurs des attaquants. En effet, malgré leur niveau de compétences potentiellement élevé, les pirates restent des humains et commettent souvent des erreurs. Des fautes qu'il est possible d'exploiter pour mieux comprendre l'attaque et la contrer, mais aussi pour identifier ceux à son origine.

UTILISER LES ERREURS DES ATTAQUANTS POUR MIEUX LES COMPRENDRE

Le cas récent d'Ashley Madison semble être un bon exemple, même s'il faudra attendre les investigations complètes pour confirmer tous les éléments. Les attaquants auraient diffusé les données volées via BitTorrent en utilisant un serveur loué chez un hébergeur aux Pays Bas. Ils auraient cependant oublié de sécuriser ce serveur, en particulier ils n'ont pas mis de mot de passe sur les interfaces d'administration web. Même si cela ne permet pas de les identifier directement, il s'agit d'une piste de premier choix pour les forces de l'ordre en charge des investigations. Il faut cependant rester prudent car cela peut aussi être une forme de diversion réalisée par les attaquants. Affaire à suivre !

Autre exemple, le cas « Red October ». C'est l'affaire d'une vaste opération de cyber espionnage qui a commencé en mai 2007 et qui a été découverte par le cabinet Kaspersky quelques années plus tard. Le cabinet a réussi à identifier, bloquer et neutraliser le logiciel malveillant en utilisant une faille de l'attaque. En effet, les noms de domaines pour les serveurs d'exfiltration qui étaient utilisés dans le code malveillant n'avaient pas été réservés par les attaquants. Cela a permis à Kaspersky de simuler un de ces serveurs et de voir qui était infecté et quelles données étaient capturées.

Parfois, ces erreurs permettent même d'identifier les auteurs de l'attaque, comme ce fut le cas avec la traque de la personne derrière le malware PlugX.

Nos consultants ont d'ailleurs eux aussi rencontré ce genre de situation dans le cadre d'une attaque ciblée chez un de nos clients. Les pirates avaient en effet « oublié » la présence d'un keylogger sur les serveurs internes utilisés pour l'exfiltration des données, ce qui a permis à nos experts d'identifier quelles données étaient ciblées et où elles étaient envoyées. Nous avons même pu récupérer le login et le mot de passe utilisés par les attaquants. Le concept de « l'arroseur arrosé » remis au goût du jour.

SAVOIR TIRER PARTI DE CES INFORMATIONS POUR MIEUX GÉRER LA CRISE

Les informations obtenues grâce à ces erreurs sont très précieuses, elles permettent ensuite d'adapter la réponse à l'incident. D'autant plus que les attaquants utilisent parfois des mécanismes de diversion « bruyants » (redémarrage de machines, effacement de fichiers, forte activité CPU, voir déni de service…) afin de détourner l'attention des vrais données qu'ils visent. Une compréhension « métier » des objectifs de l'attaque permet d'éviter de se focaliser sur ces pièges.

Il est même souvent intéressant de laisser l'attaque se dérouler pour mieux la comprendre.

Les réflexes face aux incidents de sécurité « classiques » (déployer des signatures antivirales, réinstaller des serveurs…) sont donc aujourd'hui largement révolus. Il faut adopter une approche dynamique de la crise, s'intéresser à son objectif métier et utiliser les erreurs des attaquants pour être plus pertinent, en pouvant même envisager des réponses « actives » à l'attaque. Un challenge pour les équipes de réponses à incidents, qui doivent adapter leurs méthodologies et leurs réflexes, mais un objectif crucial pour lutter contre ces attaques

---

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Source :

http://www.solucominsight.fr/2015/08/attaques-ciblees-profiter-des-erreurs-des-attaquants-pour-mieux-les-comprendre-et-les-contrer/