Avis d'expert sécurité : focus sur les AET

Les Techniques d'Évasion Avancées (AET) constituent un nouveau défi pour les systèmes de sécurité réseau. Un avis d'expert de **Laurent Boutet**, CISSP, expert avant-vente de Stonesoft.

Contrairement aux moyens de contournement connus, les AET combinent et modifient des méthodes afin de déguiser une attaque ou un code malveillant. Ainsi elles infiltrent un réseau sans être détectées par les systèmes de sécurité en place. Le risque particulier associé aux AET est le nombre presque illimité d'options de combinaison qui peuvent s'effectuer. Les estimations actuelles atteignent 2^250 variantes d'AET, qui vont servir aux pirates informatiques pour déguiser une attaque. Des mécanismes de protection courants (système de prévention d'intrusion ou pare-feu) ne gèrent pas ces techniques. Il n'existe aucune protection complète contre les AET. Néanmoins il est possible de sécuriser des réseaux par des méthodes de prévention.

Décryptage du fonctionnement des AET

Pour contourner un système protégé les cyberpirates déguisent ou modifient des logiciels malveillants et les dirigent, inaperçus, vers des réseaux. Dans le cas de contournements simples et des AET, le protocole TCP/IP, utilisé sur Internet et une majorité de réseaux informatiques, joue un rôle central. Il refait appel à la norme IP RFC 791 et définit un mode de réception ouvert tandis que le mode envoi reste conventionnel. En général seuls des paquets de données sans erreur peuvent être envoyés, et le système accepte tous les paquets de données entrants qui peuvent être interprétés en bout de chaîne. Des paquets de données entrants peuvent disposer de formats différents, mais ils sont toujours interprétés de la même manière. Cette approche ouverte, basée sur la notion que l'interaction entre des systèmes différents doit être aussi fiable que possible, ouvre la porte aux attaques ou aux techniques déployées pour les déguiser.

Les différents systèmes d'exploitation et applications ne se comportent pas de la même manière en recevant des paquets de données, et il peut arriver qu'un IPS ne détecte pas le contexte original du paquet et par conséquent, interprète le flux de données différemment de l'hôte cible. On parle dans ce cas de « désynchronisation de statut ». C'est le point de départ pour des techniques de contournement, qui utilisent ce contexte pour créer les paquets de données qui apparaissent normaux et sécurisés. Ces paquets ne sont identifiés comme des attaques que quand ils sont interprétés par le système final, c'est-à-dire, quand le code malveillant est déjà installé dans le réseau.

Quel risque particulier associe-t-on aux AET ?

Jusque très récemment, on connaissant quelques techniques de contournement, qui étaient correctement gérées par les solutions de sécurité. Mais depuis la découverte de Techniques Avancées, il est évident que davantage de techniques peuvent être utilisées pour contourner des systèmes IPS. Les AET exploitent des vulnérabilités dans des protocoles et les faibles barrières de sécurité de la communication réseau. Tout comme les méthodes conventionnelles, elles commencent par « le statut désynchronisé » décrit plus haut. Or les AET font preuve de plus de finesse encore – elles varient constamment, combinent les techniques de déguisement et visent

différentes couches du réseau.

Les nouveaux champs d'attaque

Les tests de départ ont identifié la possibilité d'attaques AET au niveau de l'IP, du transport (TCP, UDP) et des protocoles de couche applicatives (SMB et RPC). Le phénomène a donc été identifié comme une menace interne. Des AET intervenant au niveau d'autres protocoles, comme IPV4, IPv6, TCP et HTTP, ont aussi fait surface en automne 2011. Si les AET visent la couche de protocole HTTP (le port 80 et donc l'Internet), elles peuvent aussi tromper les pare-feux et faire passer des logiciels malveillants dans le réseau via le trafic Web. Cela signifie que les cyberpirates peuvent utiliser les AET pour atteindre les environnements *cloud* tout comme des applications et données web. Le protocole IPv6 offre aux AET de nouvelles façons de déguiser des attaques protocolaires ou agissant au niveau du transport. En raison de la compatibilité exigée avec IPv4, les systèmes doivent faire preuve d'une plus grande tolérance lors de l'interprétation de paquets de données entrants. Cela augmente la dérive pour les AET lorsqu'il s'agit de déguiser des codes malveillants. Un facteur aggravant est notre manque d'expérience et de recul par rapport à l'IPv6.

À ce jour Stonesoft a identifié plus de 300 AET différents. Ce n'est qu'une goutte d'eau ! On peut estimer les combinaisons potentielles aujourd'hui à 2^250. Voici donc le défi auquel les systèmes de sécurité sont confrontés à présent. La protection fiable contre des attaques réseau déguisées par le biais des AET implique que les IPS doivent connaître et intégrer toutes les variantes AET utilisables par un système cible pour rassembler des fragments de données.

Comment se protéger contre les AET ?

Les dispositifs d'inspection de flux fonctionnent avec des analyses de protocole et détections de signature. Cela signifie qu'un système IPS doit déjà être familier avec un modèle d'attaque pour pouvoir l'éviter. Vu le nombre potentiel des AET la tâche est très difficile. Il est vrai que les méthodes de détection correspondantes sont généralement ajoutées aux dispositifs quelques jours après la découverte de nouvelles menaces.

En outre, il existe des fonctions analytiques qui détectent et bloquent des codes malveillants comparables à ceux qui sont déjà connus. Or, il suffit parfois d'un changement minimal dans le nombre d'octets pour que la variante AET ne ressemble à aucune des attaques répertoriées dans le système IPS. En conséquence, le système de sécurité ne reconnaît pas le code malveillant crypté avec l'AET et le laisse entrer dans le réseau sans blocage. L'attaquant peut alors librement se déplacer dans le système pour chercher une zone de faiblesse ou un serveur non-patché.

Les IPS doivent donc être à même de gérer plus d'éléments que les simples caractéristiques des codes-menaces pour décerner les attaques AET. Les applications de sécurité qui comparent des signatures d'attaque reçues par l'hôte cible avec des signatures déjà connues ne peuvent pas prendre en compte chaque paquet du trafic réseau. Il ne suffit pas de trier tous les paquets dans l'ordre et rassembler tous les fragments. C'est pourquoi les fonctions d'IPS classiques généralement utilisées pour protéger contre des *exploits* – comme la prise des empreintes digitales ou la détection à base de signature – ne protègent pas contre les AET.

La normalisation

Des options complémentaires sont nécessaires pour inspecter le flux de données, telles que des paquets de données non reçus en bout de système ou les protocoles qui peuvent être décryptés différemment. Ces contrôles supplémentaires peuvent être mis en œuvre avec un mécanisme appelé la normalisation. Les instruments de sécurité qui sont capables de mettre en œuvre des processus complets de normalisation interprètent des paquets de données et les rassemblent comme le système final. Ils prennent en compte toutes les couches pertinentes pour chaque connexion. Le risque que les paquets de données ne se comportant pas selon les règles RFC 791 puissent contourner des systèmes de sécurité sans détection est réduit.

Les réseaux devraient aussi être protégés avec des systèmes de sécurité flexibles à base de logiciel. Ils n'offrent pas la protection 100 % garantie contre les AET mais peuvent être ajustés aux modèles d'attaque changeants plus facilement et rapidement que des solutions matérielles. Contrairement aux solutions matérielles, les solutions logicielles tiennent compte de la mise en œuvre immédiate des *patchs* de sécurité et des mises à jour. La gestion centralisée est également un atout pour le traitement efficace des AET.

Quel est l'objectif des AET à présent ?

On ne peut pas mesurer avec exactitude l'utilisation actuelle des AET. Ne laissant pas de trace, ces attaques sont découvertes quand elles sont déjà entrées dans le réseau. Mais alors il n'est plus possible de dire quelle technique a été utilisée pour permettre au code malveillant de contourner les systèmes de sécurité. Des recherches actuelles indiquent que certaines AET sont relativement faciles à manipuler, et on peut supposer que les pirates informatiques les utilisent déjà.

D'autres sont très complexes et leur utilisation exige des ressources financières considérables ainsi que le savoir-faire technique. De telles ressources et savoir-faire sont du ressort des cybercriminels organisés agissant selon des intérêts économiques ou politiques. On en conclut que les attaques déguisées par les AET constituent une menace pour les données sensibles de grandes sociétés, des agences gouvernementales ou des banques.

Crédit photo : © Stonesoft