Livre Blanc Stonesoft

Advanced Evasion Techniques

Nouvelles méthodes et combinaisons de contournement des technologies de prévention des intrusions

Par Marc Boltz, Mika Jalava et Jack Walsh (ICSA Labs)
Stonesoft Corporation

STONESOFT

Secure Information Flow

Introduction

A mesure que les environnements réseaux se complexifient, la gestion des systèmes de sécurité des informations devient un véritable challenge. Les systèmes de détection et de prévention des intrusions offrent une protection aux architectures les plus vulnérables, notamment celles dont la mise à jour présente certains risques. Depuis que l'IPS est né, des techniques d'évasion et de contournement de ce système existent. Cependant, ces techniques utilisées par les cybercriminels et autres hackers ont rapidement été identifiées, connues et maîtrisées. Aujourd'hui, Stonesoft dévoile de nouvelles techniques qui viennent compléter celles déjà connues et qui s'y mélangent parfaitement. Combinées, ces techniques (AET) ciblent les faiblesses des protocoles. De plus, la communication réseau, par essence assez permissive, provoque une augmentation du nombre d'évasions capables de contourner les technologies IPS, même les plus à jour.

Les auteurs

Mark Boltz est Senior Solutions Architect chez Stonesoft Corporation. Il justifie de plus de 20 ans d'expérience dans le domaine des technologies de l'information, dont plus de 18 ans spécialisées dans la sécurité réseau. Titulaire des certifications CISSP et CISA, il suit actuellement un Master en technologie de l'information.

Mika Jalava est le directeur technique de Stonesoft Corporation.

Jack Walsh est Anti-SPAM and Network IPS Program Manager chez ICSA Labs, division indépendante de Verizon Business.

Sécurité réseau

La sécurité des réseaux informatiques dépend d'un nombre surprenant de facteurs. Ceci s'applique même si l'on se limite à défendre les réseaux contre les attaques actives. Le nombre de contrôles que le réseau, le serveur et l'administrateur doivent comprendre et appliquer correctement pour défendre l'entreprise contre l'ensemble des menaces, en constante évolution, peut se révéler énorme. Les dispositifs réseau, les systèmes d'exploitation serveurs et les applications doivent non seulement être correctement configurés mais également parfaitement mis à jour. Les contrôles d'accès doivent être appliqués de façon appropriée. Pour réduire les risques de dégâts et délivrer la meilleure protection possible, il est nécessaire de segmenter le réseau. Les règles intégrées au firewall ne doivent être conformes qu'aux services dont l'entreprise a besoin. Tous les logs systèmes doivent être recueillis, stockés et analysés en un point central, afin de repérer facilement toute anomalie ou comportement suspect. Les cartes de paiement et les informations personnelles doivent être protégées, dans le respect non seulement des politiques de sécurité internes, mais également des standards de conformité imposés par l'extérieur.

Les sociétés désireuses de respecter les étapes mentionnées ci-dessus ou de mettre en place des bonnes pratiques, risquent d'être freinées par la topologie de leur réseau. Des services réseaux dynamiques et mal conçus ne permettent pas de segmenter le réseau et d'y implémenter des politiques de firewall. Les entreprises, à l'instar d'une multitude de réseaux industriels, risquent de se voir limiter dans leurs possibilités de mise à jour des systèmes d'exploitation, notamment à cause des applications et protocoles déjà en place. Le nombre important de patches, de nouvelles versions des systèmes d'exploitation et d'applications, leur compatibilité mutuelle sont autant de facteurs risquant d'empêcher l'entreprise de les tester et de se maintenir parfaitement à jour.

Le rôle de l'IPS et de l'IDS

On déploie généralement un IPS (Système de Prévention Contre les Intrusions) ou un IDS (Système de Détection des Intrusions) pour offrir un complément à la protection statique, mais en constante évolution, délivrée par les firewalls réseaux. Les technologies IPS et IDS offrent un niveau de sécurité supplémentaire aux entreprises ayant à prendre en comptes les problématiques mentionnés précédemment. A l'inverse d'un firewall qui autorise ou interdit, via des politiques de sécurité, la circulation de paquets en fonction de leur source, de leur destination, du protocole ou d'autres facteurs, l'IDS et l'IPS inspectent et laissent circuler l'ensemble du trafic à condition qu'il ne renferme aucune menace. Dans le cas où une tentative de connexion malveillante est lancée, ces dispositifs alertent immédiatement l'administrateur (IDS) ou empêchent la connexion (IPS). Les techniques utilisées par ces dispositifs de sécurité sont variées mais consistent généralement en l'analyse du protocole et en des signatures d'attaques capables de déterminer des modèles d'attaques réseau, provenant des exploits identifiés ciblant des vulnérabilités dans les systèmes de communication.

Le nombre d'exploits et de vulnérabilités connus est considérable et ne cesse de croître rapidement. Fort heureusement, les capacités d'inspection des solutions IPS et IDS évoluent également très rapidement. Généralement, lorsqu'un exploit ciblant les entreprises est découvert, les méthodes pour le détecter sont intégrées aux dispositifs en quelques jours, voire quelques heures. Certains exploits, similaires à d'autres, pourront être détectés et empêchés grâce à des fonctionnalités d'analyse déjà connues.

Evasions

Que se passe-t-il lorsqu'un système est vulnérable à un exploit mais que le pirate ne parvient pas à mener à bien son attaque à cause d'un système de détection réseau ? C'est à ce moment que l'on parle d'évasion. Le développement des techniques d'évasion, ou évasions, n'est pas passé inaperçu auprès des personnes désireuses d'attaquer les réseaux. Le pirate change alors de questionnement et « comment puis-je pirater le système de destination ? » devient « comment puis-je pénétrer et pirater ce système sans être repéré ? »

Standards réseau

TCP/IP, le protocole utilisé sur Internet et la majorité des réseaux informatiques se base sur les prérequis techniques définissant la norme RFC 791, née en 1981.Entre autres choses, la norme RFC explique que : « généralement, une implémentation doit être plutôt stricte pour tout ce qui concerne les envois et plutôt permissive en ce qui concerne la réception. Ceci signifie qu'elle doit envoyer des datagrammes correctement constitués, mais doit accepter tout type de datagramme qu'elle est capable d'interpréter (ex : ne pas objecter devant des erreurs techniques alors que la signification est toujours déchiffrable) (Postel, 1981, p. 23).En d'autres termes, il existera plusieurs manières de former des messages qui seront identifiés de la même façon par l'hôte distant. Cette position permissive est adoptée pour faciliter et fiabiliser l'interopérabilité entre les systèmes, mais a, parallèlement, ouvert la voie à de nombreuses attaques et méthodes visant à empêcher des attaques d'être détectées.

Les systèmes d'exploitation et applications ne réagissant pas de la même façon à la réception de paquets, l'application de l'hôte distant verra peut-être quelque chose de différent de ce qui se trouvait initialement dans le trafic réseau. Le réseau lui-même peut tout à fait modifier le trafic entre le système de détection et l'hôte distant. En exploitant minutieusement ces différences, il est possible, dans beaucoup de cas, de construire des paquets de telle façon à ce qu'ils paraissent normaux et sans danger mais qui, au moment d'être interprétés par l'hôte distant, se transformeront en exploit, le prenant pour cible. Ces techniques sont généralement appelées évasions.

Recherches sur les évasions

Les recherches sur les évasions ont été entamées à la fin des années 1990. Dans un papier daté de 1998, Newsham et Ptacek ont présenté des techniques pouvant servir à contourner efficacement les systèmes de détection. Depuis lors, peu de nouvelles recherches ont été mises à jour et concernent soit les éditeurs de sécurité soit les membres de la « Black Hat Community ».

Une technique d'évasion élémentaire, mise à jour par Newsham et Ptacek s'articule autour des défis que représente la fragmentation IP. La fragmentation IP est spécifiée dans la RFC 791. Elle est requise afin d'assurer l'interopérabilité entre les systèmes et de gérer les différentes topologies réseaux (Postel, 1981). Lors d'une évasion de type fragmentation IP, le pirate profite, par exemple, de fragments désordonnés ou surcharge l'IPS de fragments. Newsham et Ptacek corroborent le fait suivant : « un IDS qui ne sait pas gérer correctement des fragments désordonnés devient vulnérable. Un pirate peut volontairement brouiller ses flux de fragments dans le but de contourner les IDS » (Newsham & Ptacek, 1998). Par ailleurs, les systèmes IDS doivent affronter une nouvelle problématique : en effet « ils reçoivent des fragments qui doivent être stockés jusqu'à ce que le flux de fragments puisse être réassemblé dans un datagramme IP entier ». En conclusion, les architectures IPS et IDS doivent compenser autant que possible le fait que l'hôte distant réassemblera peut-être les fragments. L'IPS doit prendre en compte toutes les possibilités. Si l'IPS ne sait pas absorber assez de fragments avant d'appliquer les signatures ou déterminer les possibilités de reséquençage, ce dernier ne dispose plus de contexte approprié, et réécrit par conséquent « le flux dans l'IDS » (Newsham & Ptacek, 1998). On appelle « désynchronisation d'état » ce changement de contexte entre l'IPS et l'hôte distant.

Newsham & Ptaceck ont également inclus dans leurs recherches de 1998 plusieurs techniques impliquant des options IP, TCP et le séquençage TCP. Ils en parlent en détails dans leur document et elles ont été consignées ici pour donner une plus grande perspective sur ces techniques d'évasion.

Les évasions dont il est question dans ce document datant de 1998 sont toujours actuellement efficaces sur les systèmes IPS. Ce fait surprenant donne une idée de l'intérêt qu'ont représenté jusqu'à aujourd'hui ces évasions pour les éditeurs de sécurité. Les laboratoires comme les ICSA labs, réalisant les tests en vue de certifications ont incorporé plusieurs évasions dans leurs tests IPS. Cependant, le nombre de nouvelles vulnérabilités et d'exploits est si conséquent que les pirates peuvent se contenter d'utiliser les derniers exploits plutôt que de conjuguer leurs attaques à des

techniques d'évasion pour contourner les remparts de sécurité en place sur les réseaux.

Normalisation

Les dispositifs de sécurité équipés de fonctionnalités d'inspection doivent faire correspondre les signatures d'attaque avec l'information que l'hôte distant perçoit. Ils ne peuvent donc pas analyser simplement le trafic réseau paquet par paquet. De la même façon, pour les dispositifs de sécurité, replacer et réassembler les paquets dans le bon ordre ne suffit pas. Les dispositifs de sécurité doivent pouvoir prendre en compte d'autres possibilités comme la non-réception des paquets par l'hôte distants ou l'interprétation multiple des protocoles.

Le mécanisme de gestion derrière ce phénomène s'appelle la normalisation. La normalisation a été suggérée par Handley et Paxson en 1999 puis étendue en 2001. Cette tâche a été fortement complexifiée par la politique fixée dans la RFC 791. Bien que le standard exige une approche plutôt prudente côté hôte émetteur, un utilisateur malveillant ne respectera jamais ce fait. De plus, la RFC exigeant que les hôtes distants soient plutôt permissifs en termes de réception, les standards plus détaillés expliquant ce que cela signifie sont souvent trop flous et permettent de trop grandes variations. Handley et Paxson ajoutent que « malheureusement, le trafic réseau comprend parfois une proportion non négligeable de trafic totalement inhabituel mais tout à fait bénin; ce qui provoque souvent des faux positifs pris pour des tentatives d'évasion » (2001). De plus, si différents systèmes d'exploitation décodent un message donné de différentes façons, il est difficile pour un dispositif de sécurité de prendre les bonnes décisions. Ceci est dû au processus de normalisation.

Advanced Evasion Techniques (AET)

L'équipe de recherches sur les vulnérabilités de Stonesoft a à cœur de constamment améliorer nos produits, dont les IPS. Des résultats décevants, notamment face à des évasions, nous ont forcés à approfondir nos recherches sur ces techniques. Composée de professionnels de la sécurité avec une solide expertise, l'équipe de recherche sur les vulnérabilités ne s'est pas contentée d'apporter des réparations de base. Elle s'est véritablement penchée sur les évasions et a été tout à fait surprise par le danger potentiel qu'impliquent ces techniques en matière de sécurité.

L'équipe a fait plusieurs découvertes : il existe beaucoup plus de façons de déconnecter un IPS du trafic réseau au moyen de techniques d'évasion que ce qui était connu jusqu'alors. L'IPS et l'hôte distant interprètent différemment l'état du protocole. Certaines méthodes découvertes étant relativement simples, Stonesoft a pensé avec inquiétude qu'elles avaient peut-être déjà été découvertes et utilisées par les cybercriminels à l'insu des dispositifs IPS et des entreprises dans lesquels ces derniers étaient déployés. Les autres évasions sont bien plus complexes mais aussi efficaces.

Les recherches sur les évasions ont probablement été ralenties par le fait que de nombreuses attaques et outils d'évasion ont été limités par les systèmes d'exploitation et leurs piles TCP/IP. Ce type de limitation s'avère plutôt logique : ces systèmes sont en effet censés se conformer aux politiques de prudence recommandées par la RFC 791. En s'affranchissant de ces limitations avec des outils de bas niveau et en incluant des piles TCP/IP moins restrictives, les chercheurs Stonesoft ont rapidement découvert des dizaines de techniques d'évasions. Les tests de ces techniques sur des IPS existants et systèmes similaires ont permis à Stonesoft de constater que les techniques permettaient effectivement d'échapper à la détection.

Les nouvelles évasions trouvent leur fondement sur le principe élémentaire de désynchronisation des systèmes de détection ayant une visibilité réseau du côté de l'hôte distant. Bien que l'objectif soit le même, les méthodes diffèrent. Les possibilités d'évasion ont été trouvées au niveau des couches IP et de transport (TCP, UDP) ainsi que dans les protocoles des couches applicatives, dont SMB et RPC, mais pas uniquement. Bien que nous ne puissions pas dévoiler les détails exacts sur les évasions au moment où le CERT-FI se trouve en pleine phase de coordination de vulnérabilité, ce dernier a vérifié et validé cette découverte. Les ICSA Labs ont également testé les évasions (voir la note des ICSA Labs à la fin de ce document, après la conclusion). Dès que le CERT-FI aura trouvé une solution au problème, Stonesoft sera à même de livrer davantage de détails.

La fiabilité des méthodes de détection, dont la normalisation, est remise en cause par la possibilité de combiner les techniques d'évasion. Les modifications ou combinaisons ne se heurtant plus aux limitations des systèmes d'exploitation lors de l'envoi de paquets malformés sur le réseau, elles ont pu être très facilement testées sur des hôtes vulnérables couplés à des IPS ou à d'autres dispositifs de sécurité (un firewall réseau par exemple) dans les laboratoires Stonesoft. Il est désormais évident que ces nouvelles techniques d'évasion, et ces nouvelles façons de les utiliser rajoutent de nouveaux prérequis au processus de normalisation. De plus en plus d'évasions apparaissant au niveau de la couche applicative et ciblant des protocoles multiples, une normalisation des couches IP et de transport ne suffit plus.

Conclusion

Les chercheurs Stonesoft ont découvert de nouvelles techniques d'évasion dans un laboratoire plutôt que « dans la nature ». Ceci ne signifie cependant pas que les cybercriminels ou autres acteurs malveillants n'ont pas déjà découvert et utilisé ces techniques contre des cibles réelles. Après tout, un grand nombre d'incidents de sécurité passent inaperçus. Selon un rapport publié par Verizon Business daté de 2010, (Data Breach Investigations Report) pour environ 20 % des incidents de sécurité impliquant la détection d'un malware le « vecteur d'infection » est inconnu (Baker, et. al., 2010). Il est impossible d'affirmer que ceci soit le résultat des AET. Cela est cependant fort probable, notamment dans le cas d'attaques plus avancées et plus ciblées. Stonesoft a découvert qu'il était possible de contourner et de traverser la plupart, si ce n'est tous, les IPS du marché. Tous été ont testés et aux vues de leur architecture, tous ne seront pas facilement réparables.

La plupart des menaces de sécurité réseau, et presque toutes celles véritablement dangereuses sont conçues par des cybercriminels motivés par l'argent. Le butin pouvant être considérable, les pirates n'hésitent pas à investir dans les attaques et les techniques d'évasion. On peut donc se poser quelques questions : pourquoi les éditeurs n'ont-ils pas continué les recherches sur les évasions ? Ce problème est-il trop grave pour être résolu par les dispositifs de sécurité actuels ?

Avec le recul, on remarque que les dispositifs de sécurité se différenciaient jusqu'alors par le prix et les débits qu'ils savaient absorber. Cependant, le critère principal actuellement pour les solutions de sécurité basées sur l'inspection reste la protection. Il est donc étonnant de voir que les éditeurs ont quelque peu négligé la précision des méthodes de détection et l'efficacité des réponses face aux attaques et évasions détectées. Si, bien entendu, le débit est un facteur important, il reste secondaire face aux fonctionnalités de sécurité pure, ou du moins devrait l'être. Certains éditeurs pensent peut-être que vendre des systèmes rapides, mais sérieusement limités en termes de fonctionnalités de sécurité, est bien plus lucratif que de mener des recherches et trouver des solutions aux techniques d'évasions découvertes par Stonesoft, puisque ces dernières ne sont pas facilement détectables par des systèmes dotés d'excellentes performances.

L'avis du département de recherches des ICSA Labs

Depuis plus de 20 ans, les ICSA Labs testent des centaines de solutions de sécurité informatique. Depuis tout ce temps, les ICSA Labs assurent aux collaborateurs des entreprises la meilleure protection via des tests rigoureux des antivirus, antispam, des IPS, des firewalls, des normes FIPS-140, USGv6, SSL, IPsec et d'une multitude d'autres produits. Il n'est pas surprenant que Stonesoft ait contacté les ICSA Labs pour corroborer ses recherches sur les AET.

Stonesoft a pu faire la démonstration de sa découverte aux ICSA Labs via un système de vidéoconférence. La société avait au préalable regroupé les évasions dans un outil appelé Predator, et a pu montrer aux ICSA Labs comment les attaques s'appuyant sur ces nouvelles techniques d'évasion traversent les IPS, IPS qui savaient auparavant détecter ces attaques. Fervents partisans de la notion du « *responsible disclosure* », Stonesoft et les ICSA Labs ont alors élaboré un projet qui permettrait aux ICSA Labs de tester les AET tout en laissant l'outil Predator et son code associé à l'abri dans le laboratoire de recherche de Stonesoft, situé en Finlande.

A l'issue de la démonstration vidéo de l'outil Predator et de sa quarantaine de techniques d'évasions, Stonesoft a pu délivrer des échantillons de paquets de trafic crées par les chercheurs à l'aide de Predator. Le CERT-FI a ensuite livré ces échantillons aux éditeurs de sécurité concernés par le problème. Les experts en vulnérabilité des ICSA Labs ont confirmé que les évasions contenues dans ces échantillons appartenaient à un nouveau type d'évasions, jusqu'alors inconnues du public. Les ICSA Labs ont ensuite confirmé que les attaques dissimulées dans les AET n'étaient pas détectées par plusieurs systèmes IPS connus.

Cependant, pour vérifier fermement que les AET savaient contourner les dispositifs de détection et corrompre les systèmes les ICSA Labs ont dû, par eux-mêmes, combiner les AET avec des attaques récentes et les lancer dans des systèmes vulnérables. Pour ce faire, Stonesoft et les ICSA Labs Labs ont construit un réseau privé virtuel (VPN) connectant les bureaux de Stonesoft situés à Helsinki avec les laboratoires de test d'ICSA situés à Mechanicsburg, en Pennsylvanie. Les ICSA Labs se sont appuyés sur la connexion VPN pour accéder à l'interface graphique de Predator. En sélectionnant parmi les nombreuses options incluses dans Predator, les ICSA Labs ont alors pu lancer des attaques couplées à des AET via plusieurs IPS et vers un système vulnérable. Parmi les dizaines de nouvelles évasions testées, les ICSA Labs ont pu confirmer qu'une multitude d'attaques furtives ont traversé un ou plusieurs dispositifs IPS sans être détectées et ont bel et bien compromis le système vulnérable.

Bibliographie

Baker, W., Goudie, M., Hutton, A., Hylender, C., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., Sartin, B., Tippett, P. (2010). Verizon 2010 Data Breach Investigations Report. Verizon Business. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Caswell, B., Moore, H. D. (2006). Thermoptic Camouflage: Total IDS Evasion. Proceedings of the BlackHat Conference. Retrieved from www.blackhat.com/presentations/bh-usa-06/BH-US-06-Caswell.pdf

Chien, E., Falliere, N., Murchu, L. O. (2010). W32.Stuxnet Dossier. Symantec Security Response. Retrieved from http://www.wired.com/images_blogs/threatlevel/2010/10/w32_stuxnet_dossier.pdf

Gorton, S. A., Champion, T. G. (2003). Combining Evasion Techniques to Avoid Network Intrusion Detection Systems. Skaion Corporation. Retrieved from http://www.skaion.com/research/tgc-rsd-raid.pdf

Handley, M., Kreibich, C., Paxson, V. (2001). Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-end Protocol Semantics. In Proceedings of the 10th USENIX Security Symposium. Vol. 10. Berkeley, CA: USENIX Association. pp. 115-131. Retrieved from http://www.usenix.org/events/sec01/full_papers/handley/handley.pdf

Jang, Jong-Soo, Jeon, Yong-Hee, Oh, Jin-Tae, Park, Sang-Kil. (2007). Detection of DDoS and IDS Evasion Attacks in a High-Speed Networks Environment. In International Journal of Computer Science and Network Security. Vol. 7, No. 6. Retrieved from http://paper.ijcsns.org/07_book/200706/20070617.pdf

Newsham, Timothy N., Ptacek, Thomas H. (1998). Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. Secure Networks, Inc. Retrieved from http://insecure.org/stf/secnet_ids/secnet_ids.html

Pazos-Revilla, M.. FPGA based fuzzy intrusion detection system for network security. M.S. dissertation, Tennessee Technological University, United States -- Tennessee. Retrieved from Dissertations & Theses: Full Text. (Publication No. AAT 1480256).

Postel, J. (1981). RFC 791: Internet Protocol. DARPA Internet Program Protocol Specification. Internet Engineering Task Force. Retrieved from http://datatracker.ietf.org/doc/rfc791/