SONICWALL

PRÉSENTATION : COMMENT LES CYBERCRIMINELS PEUVENT CONTOURNER VOTRE SYSTÈME DE RÉPUTATION

L'évolution de la gestion de réputation pour la sécurité de la messagerie

Résumé

Au fil des avancées technologiques, les cybercriminels développent de nouvelles tactiques pour procéder à de nouvelles attaques. Établie en 1997, la liste RBL (Real-time Blackhole List) a été utilisée pour créer le format DNSBL actuel, basé sur le système DNS. Mais les cybercriminels réalisent des attaques qui compromettent et contournent les systèmes de gestion de la réputation IP. Il est donc important que les professionnels de la sécurité puissent évoluer et garder une longueur d'avance sur les attaques afin de pouvoir les éviter.

Comment les cybercriminels contournent votre système de réputation IP

Tandis que les systèmes de réputation IP gagnent en popularité, les pirates consacrent de plus en plus de ressources à les neutraliser. Les auteurs des menaces préfèrent de plus en plus le phishing au spam afin de se travestir en source de confiance et retourner le système de messagerie et les employés de l'entreprise contre elle-même. Les phishers se dissimulent derrière l'identité d'amis ou de partenaires fiables ; leurs e-mails visent à compromettre les authentiques serveurs de messagerie des entreprises possédant une bonne réputation ou à pirater les comptes de messagerie Web de fournisseurs de services ISP et ASP tels que Yahoo® ou Gmail®. Cela permet aux cybercriminels d'éviter ou de retarder le processus d'identification sur les systèmes classiques de réputation IP en envoyant une combinaison d'e-mails indésirables et légitimes à partir des serveurs exposés des entreprises.

Même si les cybercriminels manipulent leurs adresses IP, ils ne manipulent pas tous les aspects d'un message de phishing ou de spam de manière uniforme. À l'instar d'autres entités à but

Pour vous préparer aux futures menaces véhiculées par e-mail, vous devez tirer les leçons du passé.

lucratif, les cybercriminels réduisent les coûts en réduisant la complexité des opérations. Ils ont tendance à réutiliser les adresses IP, ainsi que le contenu, la mise en page, les liens hypertextes et les images. Cela constitue une opportunité : une couche de protection supplémentaire pour l'identification et la gestion de la réputation au-delà des seules adresses IP.

Comment en sommes-nous arrivés là : L'évolution de la gestion de réputation

Le système initial de gestion de la réputation des systèmes de messagerie a vu le jour avec la liste RBL (Real-time Blackhole List). La toute première liste RBL a été développée en 1997 par Paul Vixie pour le système MAPS (Mail Abuse Prevention System). Sur la base d'une liaison réseau qui se coupe au lieu d'acheminer le trafic entrant, P. Vixie a ainsi développé le concept du « trou noir » pour rejeter les e-mails provenant de sites qui envoyaient directement des spams ou les autorisaient. La liste RBL initiale qui comportait les sites suspects était transmise aux administrateurs des systèmes abonnés via le protocole BGP (Border Gateway Protocol). Les abonnés pouvaient alors appliquer la liste pour bloquer le trafic TCP/IP provenant de ces sites.

Si la liste RBL des réputations a constitué un pas en avant important en termes de gestion des spams, elle s'est également accompagnée de défis. Le MAPS s'est méticuleusement attaché à vérifier l'exactitude des informations sur les sites avant de les publier sur la liste. Si cela a permis de réduire le nombre de faux positifs, cela a également considérablement retardé la capacité des abonnés à répondre rapidement aux attaques. Au fil du temps, le MAPS a développé des clients RBL intégrés aux logiciels de messagerie afin de permettre aux administrateurs de personnaliser leur propre liste RBL et ainsi de refuser les e-mails entrants, serveur par serveur.

La liste MAPS RBL a jeté les fondations nécessaires au développement du format DNSBL, basé sur le système DNS. Le service Internet DNS (Domain Name System) convertit les noms de domaines/hôtes en adresses IP (résolution DNS) et les adresses IP en noms de domaines/hôtes associés (DNS inverse), avec l'aide d'un serveur DNS. La liste DNSBL ne se contente pas d'être une liste discrète ; elle a inclus plusieurs normes permettant d'ajouter et de retirer dynamiquement les adresses IP. Les fournisseurs de services DNSBL pouvaient alors communiquer des listes actualisées via le service IDNS (Internet Domain Name Service), selon un format standardisé. Les premiers développeurs des listes DNSBL ont ajouté certains critères : par exemple si un serveur de messagerie expéditeur a utilisé des relais ouverts ou des proxys potentiellement exploitables ou bien si un serveur de messagerie a envoyé des spams à un système « pot de miel » conçu pour attirer et rassembler les spams en vue de leur identification et de leur analyse.

Aujourd'hui, il existe des dizaines de services DNSBL et la plupart des serveurs de messagerie peuvent interroger ces services pour vérifier la réputation des adresses IP. Ces services appliquent toutefois des normes différentes pour l'ajout, le retrait ou le maintien des adresses IP dans leurs listes. Par conséquent, il est possible que certaines listes ne contiennent pas d'adresses IP potentiellement dangereuses ou bien incluent par erreur des adresses valides.

Conclusion

Les e-mails constituent un vecteur de menaces redoutable que les cybercriminels ne cessent d'utiliser pour mener à bien leurs attaques. Les messages de phishing ont été identifiés comme étant l'épicentre de la plupart des attaques réussies sur les réseaux des entreprises. Avec la croissance du spear phishing et du whaling, les e-mails indésirables sont de plus en plus difficiles à distinguer des authentiques messages. Il est par conséquent impératif d'évaluer votre système de gestion de la réputation afin de vous assurer qu'il est en mesure de vous protéger de manière efficace contre les menaces émergentes véhiculées par e-mail.

En savoir plus. Lisez notre dossier La gestion avancée de la réputation face aux menaces véhiculées par e-mail.

À propos de SonicWall

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com