

**Stonesoft : un outil de test Anti-Evasion Readiness**

**S curit **

Post  par : JPilo

Publi e le : 6/6/2011 11:30:00

Les derniers incidents de s curit  ont largement d montr  le r le fondamental de la s curit  r seau. **Stonesoft**,  diteur de solutions de s curit  r seau int gr es et de continuit  de lâ activit , annonce le lancement de son **service global de test Anti-Evasion Readiness **.

  Le but de ce service ? Montrer aux entreprises si leurs donn es critiques sont vuln rables aux Advanced Evasion Techniques (AET = techniques d  vasion avanc es).

Ce service sera assur , dans le monde entier, par des soci t s informatiques ind pendantes et soigneusement s lectionn es.

**Le service de test Anti-Evasion Readiness** s appuie sur le logiciel de test des  vasions int gr  aux produits StoneGate et d velopp  au sein des laboratoires Stonesoft. Il permet d  valuer et de g n rer des rapports sur les capacit s de protection des dispositifs de s curit  contre les Advanced Evasion Techniques (AET). Les AET permettent de dissimuler ou de modifier une attaque r seau afin de contourner les m canismes de d tection et de blocage assur s par les syst mes de s curit  r seau. Pratiquement parlant, les  vasions permettent aux cybercriminels confirm s de d poser des contenus malveillants, des exploits, ou des attaques dans un syst me vuln rable sans laisser aucune trace. Les derni res recherches ont prouv  que les AET peuvent contourner la majorit  des dispositifs de s curit  actuels.

# STONESOFT

## Secure Information Flow

**Ce service a  t  d velopp  dans le but de r pondre** aux besoins des entreprises  quip es de dispositifs de s curit  R seau tels que les Next Generation Firewalls et les syst mes de pr vention des intrusions faisant de la deep packet inspection. Ces dispositifs de s curit  assurent la protection des r seaux informatiques critiques, des donn es sensibles, des applications strat giques comme les CRM ou les ERP, ainsi que des r seaux SCADA. Tous

ces évolutions du système informatique sont une manne pour les cybercriminels et les AET représentent un moyen efficace de mener à bien des attaques lourdes de conséquences. Par ailleurs, pour beaucoup d'entreprises, la sécurité de ces évolutions est essentielle notamment pour tout ce qui touche à la conformité.

Pour **Lionard Dahan**, Country Manager de [Stonesoft France & Benelux](#) : « Les récents incidents de sécurité ont bel et bien démontré le rôle fondamental de la sécurité réseau. Pour réduire les risques, il est important, dans un premier temps d'être en savoir davantage sur le niveau de sécurité de son réseau. Le pire serait de penser que l'on est totalement protégé ou de ne jamais questionner et de dépendre de votre fournisseur de sécurité. [Le test d'Anti-Evasion Readiness](#) donne aux entreprises une vision réaliste, indépendante et définitive sur les capacités de protection contre les techniques d'évasion de leurs solutions de sécurité réseau. »

**Le service de test Anti-Evasion Readiness** sera proposé par des sociétés informatiques indépendantes et compétentes, dans le monde entier. A mesure que des acteurs majeurs intégreront ce service à leur offre, il sera de plus en plus accessible.

« Nos clients sont très intéressés par ce service. Il existe actuellement un certain nombre d'informations contradictoires sur les évasions, et les clients ont désormais besoin de données purement factuelles. Savoir si le bastion de sécurité d'une entreprise sait ou ne sait pas protéger contre les évasions est une donnée essentielle pour l'administration des systèmes informatiques. Ce service donne de la valeur ajoutée aux audits de sécurité : il permet de mettre à jour les processus d'évaluation ou de reconfigurer les systèmes en place pour y ajouter une protection contre les AET. Ce test permettra aux entreprises d'optimiser les politiques de sécurité mises en place », continue **Lionard Dahan**.

Ce logiciel de test des évasions est le plus complet du marché, à ce jour. Il intègre les dernières techniques d'évasion mises à jour par Stonesoft, qui ont été rapportées aux autres constructeurs via les procédures de coordination du CERT. Ce qui différencie le test Anti-Evasion Readiness des méthodes de tests utilisées par les éditeurs et les laboratoires ? Le test Anti-Evasion Readiness est réalisé dans des environnements de production et en fonction des configurations en place au sein de l'entreprise.

A l'issue du test, les clients se verront remettre un rapport de test complet sur la détection des évasions et les taux de blocage sur différents protocoles. Ce rapport comprend également des recommandations pratiques et des conseils visant à réduire les risques. Ce test ne nécessite aucune expertise en interne ou investissement.