Stonesoft : ProtÃ©ger vos donnÃ©es sensibles contre les Advanced Evasion Techniques
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 25/3/2011 13:00:00

Lâ□□an dernier, **Stonesoft**, fournisseur innovant de solutions de sÃ©curitÃ© intÃ©grÃ©es et de continuitÃ© de lâ□□activitÃ© a dÃ©couvert **les Techniques dâ□□Evasions AvancÃ©es** (AET).

Depuis lors, il sâ□□est avÃ©rÃ© que la menace que reprÃ©sentent les AET pour les donnÃ©es sensibles des entreprises est non seulement dynamique, mais en constante Ã©volution. Stonesoft dÃ©voile donc six faÃ§ons de protÃ©ger les donnÃ©es contre les AET.

Une Ã©vasion permet de contourner les SystÃ¨mes de PrÃ©vention des Intrusions (IPS) ou tout autre dispositif de sÃ©curitÃ© analysant le trafic rÃ©seau. En tant que telles, les Ã©vasions sont connues et identifiÃ©es depuis longtemps.

Cependant, lorsque Stonesoft a dÃ©couvert les Advanced Evasion Techniques (un nouveau type de menace que les systÃ¨mes de sÃ©curitÃ© rÃ©seau ne savent pas dÃ©tecter) lâ□□information et les 23 premiers Ã©chantillons ont trÃ¨s rapidement Ã©tÃ© livrÃ©s au CERT-FI. Cette information a ensuite fait lâ□□objet dâ□□une annonce Ã la presse. Stonesoft a rÃ©cemment renvoyÃ© 124 nouveaux Ã©chantillons au CERT-FI. MalgrÃ© tout, ceci ne reprÃ©sente que la partie Ã©mergÃ©e de lâ□□iceberg.

STONESOFT

Secure Information Flow

Par principe, lâ□□ensemble des services ont prÃ©vu une maintenance Windows et les entreprises se sont dotÃ©es de systÃ¨mes de prÃ©vention des intrusions pour protÃ©ger leurs donnÃ©es sensibles, entre deux mises Ã jour. Ces nouvelles menaces rÃ©seau et ces restrictions sur la maintenance sont Ã©galement valables pour les rÃ©seaux SCADA, ciblÃ©s en 2010 par le ver Stuxnet.

Cependant, les Advanced Evasion Techniques savent contourner ces protections et dÃ©poser des attaques sans Ãªtre dÃ©tectÃ©es par les dispositifs de sÃ©curitÃ© en place, tels que les IPS. Tomo

Kononow, Chef de produit StoneGate IPS chez Stonesoft explique : Â« En rÃ©sumÃ©, cela signifie que chaque vulnÃ©rabilitÃ© dâ□□un systÃ¨me peut Ãªtre exploitÃ©e, et ce, Ã nâ□□importe quel moment. Pour protÃ©ger leurs donnÃ©es confidentielles contre les AET, les entreprises doivent anticiper, remettre en question leurs solutions de sÃ©curitÃ© existantes et trouver des alternatives capables de combattre les Advanced Evasion Techniques. Le paysage de la sÃ©curitÃ© rÃ©seau a changÃ© et les anciennes mÃ©thodes ne sont plus valables. Â»

Six faÃ§ons dâ□□amÃ©liorer sa protection contre les AET

1. Renseignez-vous sur les Advanced Evasion Techniques : en beaucoup de points, elles diffÃ¨rent des Ã©vasions traditionnelles. Il est important de comprendre que ce ne sont pas des attaques en tant que telles, mais des mÃ©thodes de transport des menaces indÃ©tectables par le firewall et les IPS. Il nâ□□existe donc aucune solution imparable contre les AET. Il est seulement possible de minimiser les risques dâ□□attaque en se dotant dâ□□une solution de sÃ©curitÃ© rÃ©seau capable de mener Ã bien une normalisation multi-couches du trafic et dâ□□une plateforme de sÃ©curitÃ© intelligente capable de se mettre Ã jour continuellement contre les AET.

2. Evaluez les risques : auditez vos infrastructures fragiles et Ã©valuez les Ã©lÃ©ments les plus essentiels de votre entreprise, lâ□□endroit et la faÃ§on dont ils sont stockÃ©s et si une sauvegarde de ces informations a Ã©tÃ© effectuÃ©es. Puis, Ã©tablissez des prioritÃ©s. Commencez par vous assurer que les donnÃ©es les plus sensibles et les services publics sont protÃ©gÃ©s de la meilleure faÃ§on contre les AET.

3. RÃ©evaluez la gestion de correctifs de sÃ©curitÃ© : lorsquâ□□ils existent, les correctifs de sÃ©curitÃ© dÃ©livrent une excellente protection contre les attaques rÃ©seau, quâ□□elles aient Ã©tÃ© vÃ©hiculÃ©es par des AET ou non. Les Ã©vasions aident simplement le pirate Ã contourner le systÃ¨me de prÃ©vention des intrusions (IPS) ou les NextGen Firewalls (NGFW). Elles ne servent Ã rien dans un systÃ¨me patchÃ©. Cependant, le test et le dÃ©ploiement des correctifs de sÃ©curitÃ© prennent beaucoup de temps, mÃªme dans les meilleures conditions. Pendant ce temps, les recommandations liÃ©es Ã lâ□□IPS (Ã©numÃ©rÃ©es ci-dessous) sont valables.

4. RÃ©Ã©valuez votre solution de prÃ©vention des intrusions : Ã©valuez la solution de prÃ©vention des intrusions que vous avez mise en place et votre NGFW. Assurez-vous que ces dispositifs soient capables de vous protÃ©ger contre les AET. Ayez lâ□□esprit critique, anticipez et recherchez des alternatives. Nâ□□oubliez pas que les AET ont changÃ© le paysage de la sÃ©curitÃ© de faÃ§on immuable. Câ□□est un fait : si un dispositif ne sait pas gÃ©rer les Ã©vasions, ce dernier devient quasiment inutile, et ce en dÃ©pit des certifications ou des rÃ©compenses reÃ§ues ou du taux de blocage quâ□□il affiche.

5. Repensez votre gestion de la sÃ©curitÃ© : lâ□□administration centralisÃ©e joue un rÃ´le essentiel dans la protection contre les AET. Elle permet dâ□□automatiser les mises Ã jour contre les AET et de planifier les upgrades logicielles facilement et Ã distance. Vous bÃ©nÃ©ficiez ainsi du meilleur niveau de protection contre les AET.

6. Testez les fonctionnalitÃ©s anti-Ã©vasions de vos dispositifs de sÃ©curitÃ© dans vos environnements, avec vos politiques et votre propre configuration : beaucoup dâ□□Ã©diteurs savent gÃ©rer les Ã©vasions quand elles sont bien dÃ©finies et stabilisÃ©es dans un laboratoire de test. Cependant, face Ã des Ã©vasions rÃ©elles et dynamiques transportant des exploits, ces systÃ¨mes deviennent incapables de protÃ©ger vos donnÃ©es. Si vous dÃ©sirez vraiment connaÃ®tre votre niveau de protection contre les AET, faites impÃ©rativement des tests en conditions rÃ©elles.