Stonesoft : Une menace de sÃ©curitÃ© affecte les PME du monde
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 18/10/2010 13:40:00

Stonesoft, fournisseur innovant de solutions de sÃ©curitÃ© rÃ©seau intÃ©grÃ©es et de continuitÃ© de lâ□□activitÃ© annonce aujourdâ□□hui avoir dÃ©couvert une **nouvelle forme de techniques avancÃ©es dâ□□Ã©vasion** (AET = Advanced Evasion Techniques) qui menacent trÃ¨s sÃ©rieusement les systÃ¨mes de sÃ©curitÃ© du monde entier.

Cette dÃ©couverte vient complÃ©ter et renforcer ce qui est dÃ©jÃ connu des techniques dâ□□Ã©vasion dites plus classiques. Lâ□□information a Ã©tÃ© remontÃ©e au CERT et aux ICSA Labs qui ont Ã©galement validÃ© son sÃ©rieux et son fondement.

Les AET sont lâ□□Ã©quivalent dâ□□un passe-partout permettant aux cybercriminels dâ□□ouvrir les portes de tout systÃ¨me vulnÃ©rable comme un ERP ou un CRM. Elles sont en effet capables de contourner les systÃ¨mes de sÃ©curitÃ© rÃ©seau sans laisser aucune trace. Pour les entreprises, cela signifie quâ□□elles risquent de perdre des donnÃ©es confidentielles. Par ailleurs, on peut tout Ã fait imaginer que des cyber terroristes sâ□□appuient sur ces AET afin de mener des activitÃ©s illÃ©gales pouvant avoir des graves consÃ©quences.

STONESOFT

Secure Information Flow

La dÃ©couverte a eu lieu dans les laboratoires de recherche de Stonesoft basÃ©s Ã Helsinki. Les experts ont ensuite envoyÃ© des Ã©chantillons et remontÃ© lâ□□information Ã lâ□□organisme de sÃ©curitÃ© nationale finlandais le CERT ainsi quâ□□aux laboratoires ICSA (division indÃ©pendante de Verizon Business) qui testent et dÃ©livrent des certifications aux solutions de sÃ©curitÃ© et aux Ã©quipements connectÃ©s au rÃ©seau. Le CERT-FI, chargÃ© coordonner au niveau mondial les parades aux vulnÃ©rabilitÃ©s identifiÃ©es, en collaboration avec les Ã©diteurs de sÃ©curitÃ© rÃ©seau, a publiÃ©, le 4 octobre quelques informations sur ces techniques avancÃ©es dâ□□Ã©vasion et les mettront Ã jour, aujourdâ□□hui mÃªme.

Les vulnÃ©rabilitÃ©s identifiÃ©es par Stonesoft touchent un grand nombre de technologie

dâ□□inspection du contenu. Pour contrer ces vulnÃ©rabilitÃ©s, une collaboration permanente du CERT-FI de Stonesoft et des autres Ã©diteurs de sÃ©curitÃ© rÃ©seau est absolument essentielles. Le CERT-FI sâ□□efforce de faciliter cette coopÃ©ration Â» explique Jussi Eronen, Ã la tÃªte du dÃ©partement Coordination sur les VulnÃ©rabilitÃ©s.

Juha Kivikoski, COO chez Stonesoft explique : Â« *Beaucoup de facteurs nous poussent Ã croire que nâ□□avons dÃ©couvert que la partie Ã©mergÃ©e de lâ□□iceberg. La nature dynamique et indÃ©tectable de ces techniques avancÃ©es dâ□□Ã©vasions peut potentiellement bouleverser lâ□□ensemble du paysage de la sÃ©curitÃ© rÃ©seau. Le marchÃ© rentre dÃ©sormais dans une course sans fin contre ce nouveau type de menaces avancÃ©es et il semblerait que seules les solutions dynamiques pourront tirer leur Ã©pingle du jeu.* Â»

Â« *Stonesoft a dÃ©couvert de nouvelles techniques de contournement des systÃ¨mes de sÃ©curitÃ© rÃ©seau. Les laboratoires ICSA ont validÃ© les recherches et la dÃ©couverte de Stonesoft. Par ailleurs, nous pensons que ces techniques avancÃ©es dâ□□Ã©vasion peuvent avoir des consÃ©quences pour les entreprises touchÃ©es, comme entre autres la perte de donnÃ©es stratÃ©giques et confidentielles* Â» dÃ©clare **Jack Walsh**, directeur des programmes IPS (SystÃ¨me de PrÃ©vention des Intrusions) chez ICSA Labs.

Les AET Â« dans la nature Â»

Câ□□est Ã lâ□□occasion du test de leurs propres solutions de sÃ©curitÃ© rÃ©seau StoneGate face Ã des nouvelles attaques Ã©laborÃ©es que les experts de Stonesoft ont dÃ©couvert cette nouvelle catÃ©gorie de menaces. Les tests en conditions rÃ©elles et les donnÃ©es recueillies lors de lâ□□expÃ©rience dÃ©montrent que la plupart des solutions de sÃ©curitÃ© rÃ©seau nâ□□ont pas su dÃ©tecter ces AET et nâ□□ont, par consÃ©quent, pas pu les bloquer.

Stonesoft soutient lâ□□idÃ©e que des pirates du monde entier sont peut-Ãªtre dÃ©jÃ en train dâ□□exploiter ces AET pour lancer des attaques Ã©laborÃ©es et trÃ¨s ciblÃ©es. Seuls quelques produits sont Ã mÃªme de fournir une protection contre ce phÃ©nomÃ¨ne, les entreprises doivent donc mettre en place un moyen de dÃ©fense trÃ¨s rapidement. **Quel est le meilleur moyen de se protÃ©ger contre une AET ?**

Pour se protÃ©ger de ces techniques dâ□□Ã©vasion dynamiques et en constante Ã©volution, il est nÃ©cessaire de sâ□□Ã©quiper de systÃ¨mes logiciels de sÃ©curitÃ© capables de se mettre Ã jour Ã distance et dâ□□Ãªtre administrÃ©s de faÃ§on centralisÃ©e. Ces systÃ¨mes possÃ¨dent un avantage indÃ©niable en termes de protection contre des menaces aussi dynamiques que les AET.

Stonesoft fait partie des acteurs dÃ©livrant ce type de solutions, via sa gamme StoneGate.

Cependant, la grande majoritÃ© des Ã©quipements de sÃ©curitÃ© rÃ©seau dans le monde sont des solutions matÃ©rielles, pour lesquelles il est difficile voire impossible de se mettre Ã jour au mÃªme rythme que ces techniques dâ□□Ã©vasion, qui mutent en permanence.

Pour en savoir plus sur les techniques dâ□□Ã©vasion et participer au dÃ©bat sur la faÃ§on de les combattre. Pour plus dâ□□informations sur les **solutions StoneGate de Stonesoft**