Proofpoint : liste des menaces informatiques les plus dangereuses
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 9/1/2014 15:00:00

Proofpoint, Inc., lâ□□un des principaux prestataires de solutions de sÃ©curitÃ©-service (SaaS), dresse une liste des menaces informatiques les plus dangereuses dans le but de protÃ©ger les utilisateurs. Proofpoint fait donc le point sur les attaques via courrier Ã©lectronique les plus frÃ©quentes et les plus destructrices envers les entreprises.

On apprend Ã©galement quâ□□au Royaume-Uni, le coÃ»t total moyen des atteintes Ã la sÃ©curitÃ© des donnÃ©es s'Ã©lÃ¨ve Ã plus de 2 millions de livres sterling1 â□□ soit plus de 2, 4 millions dâ□□euros â□□ par cyber-attaque.
Proofpoint a menÃ© une Ã©tude Ã l'Ã©chelle mondiale dans plusieurs secteurs dont la finance, la santÃ© et l'industrie pharmaceutique. Les chercheurs en sÃ©curitÃ© de Proofpoint ont analysÃ© le volume des attaques, et notamment les attaques via courrier Ã©lectronique, rÃ©seaux sociaux et d'autres types d'attaques perpÃ©trÃ©es par le biais de logiciels malveillants.

Les rÃ©sultats de cette Ã©tude permettent de dÃ©tailler les techniques d'attaques ciblÃ©es les plus efficaces auxquelles les pirates informatiques ont recours. Lâ□□Ã©tude montre en effet que ces hackers ciblent principalement les VIP des entreprises et exploitent certains grands Ã©vÃ©nements mÃ©diatiques (comme la naissance du bÃ©bÃ© Royal en Angleterre) afin de les inciter Ã cliquer sur des URL pointant vers des sites Web malveillants.

Â« *Le tÃ©lÃ©travail et les connexions Ã distance sur des smartphones et autres tablettes sont devenus le quotidien de nombreux salariÃ©s. En effet, prÃ¨s dâ□□un clic sur cinq est effectuÃ© hors rÃ©seau et Ã©chappe ainsi aux contrÃ´les de sÃ©curitÃ© traditionnels, comme les passerelles Web, les systÃ¨mes de dÃ©tection des intrusions et les pare-feu. Les pirates informatiques profitent de la difficultÃ© des Ã©quipes IT Ã assurer la sÃ©curitÃ© hors du rÃ©seau de l'entreprise et nâ□□hÃ©sitent pas Ã intervenir sur ce terrain en envoyant des courriers Ã©lectroniques le vendredi soir sachant pertinemment que certaines des cibles visÃ©es3, notamment les VIP des entreprises, vÃ©rifieront leurs mails pendant le week-end* Â», ajoute **Ismet GÃ©ri,** Directeur France et Europe du Sud chez Proofpoint.

Voici les 5 attaques les plus dangereuses identifiÃ©es par Proofpoint :

1. Phishing multimÃ©dia : un groupe d'employÃ©s ciblÃ© reÃ§oit un courrier Ã©lectronique concernant un sujet liÃ© Ã lâ□□entreprise. Le courrier Ã©lectronique provient d'une personne se faisant passer pour un collaborateur. Le lien envoyÃ© pointe vers un vÃ©ritable site d'actualitÃ©s, dont la page Web a Ã©tÃ© infectÃ©e par un programme malveillant.

2. Attaque de masse Ã partir d'une transaction de paiement : des clients reÃ§oivent les dÃ©tails d'une commande qu'ils auraient soi-disant passÃ©e de la part d'une source de confiance, ce qui provoque chez eux une rÃ©action de panique. Ils cliquent sur un lien qui pointe vers un vÃ©ritable site de paiement en ligne, dont la page Web a Ã©tÃ© infectÃ©e par un programme malveillant.

3. Attaque de masse sur fond d'actualitÃ©s : les pirates informatiques exploitent un Ã©vÃ©nement mÃ©diatique en envoyant par courrier Ã©lectronique des informations exclusives Ã son sujet Ã des employÃ©s. Si le lien figurant dans le courrier Ã©lectronique pointe effectivement vers un vÃ©ritable site prÃ©sentant l'actualitÃ©, les employÃ©s sont en rÃ©alitÃ© dirigÃ©s sur une page infectÃ©e par un programme malveillant. Les plus vastes campagnes de phishing par logiciel malveillant de toute l'histoire ont Ã©tÃ© lancÃ©es suite aux attentats Ã la bombe qui ont eu lieu lors du marathon de Boston en avril 2013. Quelque 28,7 millions de messages ont Ã©tÃ© envoyÃ©s Ã partir de 249 257 adresses IP et seulement 46 domaines4.

4. Attaque de type Â« Watering Hole Â» : ces attaques infectent dans un premier temps des sites officiels, que les employÃ©s consultent rÃ©guliÃ¨rement, de faÃ§on Ã pouvoir accÃ©der Ã leurs systÃ¨mes. Les pirates utilisent ensuite des courriers Ã©lectroniques ciblÃ©s pour inciter les employÃ©s Ã consulter les pages infectÃ©es, ce qui entraÃ®ne leur contamination par des programmes malveillants.

5. Attaque de masse sur les rÃ©seaux sociaux : des sources crÃ©dibles, comme LinkedIn, sont utilisÃ©es par les pirates informatiques pour exploiter la volontÃ© des utilisateurs d'Ã©tendre leur rÃ©seau professionnel. Bien que le nombre de courriers Ã©lectroniques reÃ§us par les entreprises pour chaque attaque reste faible, ils reposent sur des techniques de personnalisation agressives, ce qui les rend particuliÃ¨rement difficiles Ã dÃ©tecter.
Proofpoint dresse ainsi la liste des diffÃ©rentes menaces auxquelles sont exposÃ©s quotidiennement les employÃ©s, et indirectement leurs employeurs dans une plus large mesure. Les experts Proofpoint soulignent notamment la nÃ©cessitÃ© de prendre davantage conscience de ces menaces qui pÃ¨sent sur les entreprises et de trouver des solutions de dÃ©tection plus efficaces.

En guise de conclusion, **Ismet GÃ©ri** ajoute :

Â« *Des Ã©tudes menÃ©es suite Ã la divulgation d'atteintes Ã la sÃ©curitÃ© des donnÃ©es indiquent que 66 % d'entre elles restent inconnues pendant plusieurs mois5. En moyenne, un pirate informatique passe en effet 8 mois sur le rÃ©seau d'une victime avant d'Ãªtre dÃ©couvert6. Les rÃ©percussions dâ□□une telle atteinte sâ□□avÃ¨rent particuliÃ¨rement importantes lorsquâ□□il sâ□□agit de donnÃ©es personnelles ; en effet, il est aujourdâ□□hui obligatoire de dÃ©clarer a la CNIL toute atteinte Ã la sÃ©curitÃ© des donnÃ©es personnelles et le non respect de ces obligations lÃ©gales par lâ□□entreprise peut entraÃ®ner des poursuites et des sanctions pouvant aller jusquâ□□Ã une amende de 300.000 euros.*

Par ailleurs, en raison du peu de visibilitÃ© dont disposent les Ã©quipes internes en charge de la sÃ©curitÃ©, 63 % des atteintes Ã la sÃ©curitÃ© des donnÃ©es sont divulguÃ©es par des tiers, gÃ©nÃ©ralement par voie de presse, ce qui a un impact particuliÃ¨rement nÃ©gatif sur la motivation et la confiance des clients vis-Ã -vis des marques incriminÃ©es. Il est donc fortement recommandÃ© de porter tous les efforts sur la prÃ©vention et la dÃ©tection prÃ©coce des atteintes Ã la sÃ©curitÃ© des donnÃ©es. Â»
Pour en savoir plus.