RSA rapport des fraudes, attention au Tchat sur Internet
Internet
PostÃ© par : JerryG
PubliÃ©e le : 10/11/2009 15:00:00

Le mois dernier, les experts RSA nous faisaient part des **utilisations faites par les fraudeurs des messageries instantanÃ©es**. Si toutes les messageries instantanÃ©es ne sont pas Ã incriminer, **il convient de respecter certaines rÃ¨gles Ã©lÃ©mentaires** lors de leur utilisation.

Ce mois ci, ce sont les banques et institutions financiÃ¨res qui sont la cible des fraudeurs. Ces derniers redoublent dâ□□ingÃ©niositÃ© pour obtenir les identifiants bancaires des clients et emploient une technique de piratage informatique inÃ©dite : **lâ□□utilisation de systÃ¨me de chat** au sein de lâ□□opÃ©ration de phishing ou Â« chat-in-the-Middle Â».

ConcrÃ¨tement, le systÃ¨me mis en place par les fraudeurs est le suivant :

Lâ□□attaque commence comme une attaque classique de phishing1 oÃ¹ la victime est invitÃ©e Ã se connecter sur son site bancaire pour une opÃ©ration de mise Ã jour dâ□□informations ou autre. Un lien contenu dans lâ□□invitation reÃ§ue la dirige vers un site factice ressemblant en tout point au site de sa banque. Lorsque la victime se connecte sur cette page factice pour accÃ©der Ã ses comptes, le fraudeur rÃ©cupÃ¨re les identifiants de la victime.

Habituellement, Ã lâissue de cette premiÃ¨re manipulation, la victime est redirigÃ©e vers une nouvelle page du site frauduleux ou vers le vÃ©ritable site de sa banque.

Or, dans la forme dâattaque rÃ©cente dÃ©tectÃ©e par RSA, les fraudeurs utilisent une nouvelle technique, le chat, pour obtenir des informations additionnelles sur leurs victimes. Ainsi au lieu dâÃªtre dirigÃ©e vers un nouvelle page ou vers le site lÃ©gitime de la banque, la victime voit apparaÃ®tre une fenÃªtre lâinvitant Ã dÃ©marrer un chat. De lâautre cotÃ©, le fraudeur se fait passer pour un reprÃ©sentant du dÃ©partement fraude de la banque.

Sous prÃ©texte de lui assurer un maximum de sÃ©curitÃ©, le fraudeur lui soutire alors un maximum dâinformations critiques : E-mail, tÃ©lÃ©phone, date de naissanceâ¦, autant dâinformations prÃ©cieuses et monnayables, quâil pourra ensuite utiliser pour commettre des fraude par tÃ©lÃ©phone, ou en ligne, voire mÃªme pour contacter la victime plus tard.

Il est important de noter que la fenÃªtre de Live Chat est lancÃ©e par le fraudeur, et quâelle nâa aucune relation avec toute messagerie instantanÃ©e ou application hÃ©bergÃ©e sur le PC de la victime.

Il sâagit dâune attaque de phishing normale, lancÃ©e Ã partir dâun site de phishing ne faisant pas intervenir de messagerie instantanÃ©e sur le PC attaquÃ©.

RSA recommande nÃ©anmoins la plus grande vigilance aux internautes ainsi quâaux institutions financiÃ¨res. De nombreuses attaques peuvent en effet Ãªtre Ã©vitÃ©es en sâassurant que le site est

conforme et que les informations demandÃ©es sont absolument nÃ©cessaires.

Il peut par exemple sâavÃ©rer utile quâune banque informe ses clients des derniÃ¨res techniques de fraude utilisÃ©es, telle que celles Ã©voquÃ©es dans ce rapport.

Lâarme la plus efficace contre les attaques de phishing reste bien, encore et toujours, la perspicacitÃ© et la vigilance de lâhumain.

Quâest ce que le RSA Anti Fraud Command Center ?

Le RSA Antiâ Fraud Command Center (AFCC) est le Â« quartier gÃ©nÃ©ral Â» de lutte contre la fraude de RSA, la division sÃ©curitÃ© dâEMC. Il surveille et analyse lâactivitÃ© de la fraude en ligne chaque mois et dÃ©veloppe une intelligence sur la fraude unique sur le marchÃ©. Chaque mois ce centre rÃ©capitule dans un rapport ses principales dÃ©couvertes et tendances. Le rapport de Septembre 2009 rÃ©capitule et analyse les mouvements et attaques de nuisibles dÃ©tectÃ©s sur la pÃ©riode de Septembre 2009.

â Le crime en ligne Ã©volue constamment et les criminels nâÃ©cartent aucune organisation ou personne de leur cible. Ils disposent de nouveaux outils et sont capables de les adapter plus rapidement que jamais pour contourner et dÃ©jouer les mesures de sÃ©curitÃ© les plus sophistiquÃ©es mises en place par les entreprises. Ils travaillent jour et nuit pour voler des identitÃ©s, des habilitations, des donnÃ©es de cartes de crÃ©dit ou toute information quâils pourraient monÃ©tiser.

â Le centre de commandement antifraude RSA est au coeur du service dâintelligence et lutte contre la fraude mise en place par RSA pour aider ses clients Ã toujours avoir un pas dâavance sur les criminels.

Actif 24h/24 et 7j/7, le RSA AFCC emploie une Ã©quipe dâanalystes de fraude expÃ©rimentÃ©s travaillant Ã stopper les sites frauduleux, dÃ©ployer des contreâmesures et conduire des

analyses poussÃ©es pour arrÃªter les criminels et prÃ©venir les futures attaques de type phishing, pharming, chevaux de Troie, etc. Lâ□□AFCC a Ã©tabli des canaux de communication directs et ouverts avec des centaines dâ□□ISPs Ã travers le monde et utilise plus de 200 langues pour amÃ©liorer sa capacitÃ© Ã dÃ©tecter, bloquer et arrÃªter les attaques informatiques Ã lâ□□Ã©chelle mondiale.

â□□ Lâ□□AFCC a dÃ©jÃ contrecarrÃ© plus 210 000 attaques.