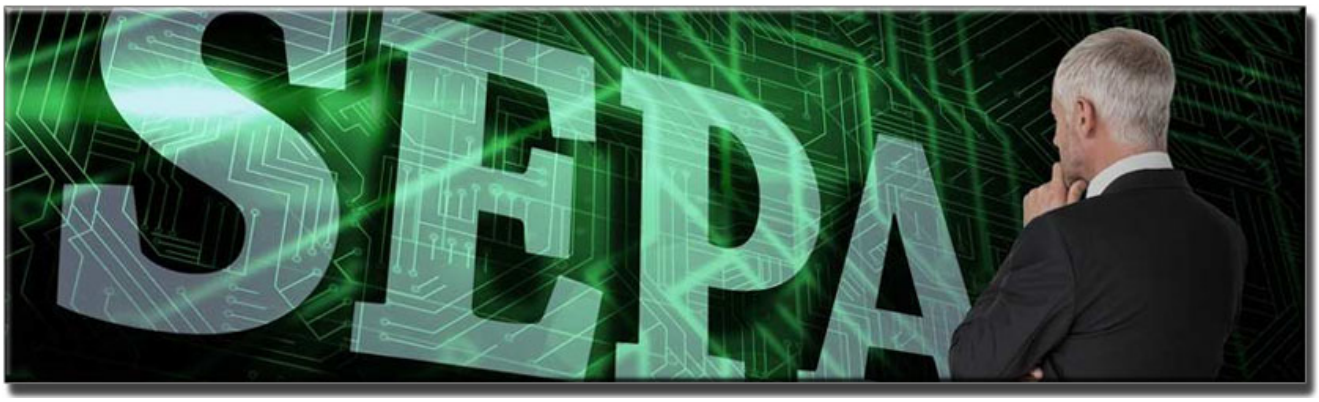
Près de 20% des entreprises sont victimes d’escroqueries bancaires. La dernière ruse en vigueur est celle qui profite de la norme SEPA



Près de 20% des entreprises sont victimes d’escroqueries bancaires. La dernière ruse en vigueur est celle qui profite de la norme SEPA

Les entreprises font de plus en plus l'objet d'escroqueries bancaires avec un préjudice estimé à ce jour à environ 250 millions d'euros.
Les organisations professionnelles et les pouvoirs publics s'émeuvent de ce phénomène croissant qui montre l'ingéniosité de ces escrocs de plus en plus pointus en terme de détournement d'informations saisies en entrant dans les systèmes informatiques et réseaux.
Une entreprise sur six reconnait avoir été victime d'au moins une tentative de fraude en 2013. Les grandes PME sont les cibles préférées des escrocs.
Ce chiffre est le résultat d'une étude interne au secteur bancaire publié par la Fédération Bancaire Française.

Une entreprise sur deux comptant entre 500 et 1.000 salariés avec un chiffre d'affaires supérieur à 75 millions d'euros a déclaré avoir été visée par une tentative de fraude.

Ce chiffre descend entre 10 et 15% pour les plus petites entreprises.
Si ces fraudes touchent tous les secteurs d'activité sans exception, elles concernent plus fréquemment le commerce, compte tenu du grand nombre de transactions réalisées dans ce secteur.
Trois types de fraude à souligner :
Les fraudes aux virements internationaux peuvent se présenter sous plusieurs formes, selon une note d'information publiée par le Service Régional de Police Judiciaire de Clermont-Ferrand (SRPJ).

1. La première d'entre elles est baptisée «escroquerie à la nigériane», en raison de l'origine des escrocs qui opèrent depuis l'Ouest africain.
Ceux-ci détournent des transactions entre les entreprises françaises et leurs fournisseurs asiatiques.
Leur méthode consiste à envoyer des courriels aux entreprises en se faisant passer pour le fournisseur. Les fraudeurs parlent alors de «dysfonctionnements bancaires» et souhaitent que le prochain virement soit réalisé sur un compte «plus sécurisé» et …qui va donc tout droit chez eux !
2. Une autre technique de fraude est celle de l'«escroquerie au président » ou arnaque «au faux patron».
Selon le SRPJ, cette méthode est «la plus redoutable». Les escrocs exigent des virements des responsables d'une entreprise, en se faisant passer pour leur PDG.
Ce genre d'escroquerie nécessite selon les auteurs de l'étude «une autorité naturelle, un certain aplomb et, un don pour la comédie» pour duper le comptable qui exécutera servilement les instructions écrites du « faux patron ».Ceci passe par plusieurs ruses:
La première ruse consiste à insister sur le caractère urgent de la requête dans le cas d'un futur contrôle fiscal, ou autre évènement perturbateur annoncé.
La seconde catégorie, dite de «l'ingénierie sociale», est d'effectuer une collecte d'informations sur l'entreprise via les réseaux sociaux pour en adopter les codes.
Cette méthode qui touche un nombre restreint d'entreprise est de loin la plus redoutable car elle émane de bandes parfaitement organisées.
Pour les petites entreprises, les méthodes de fraude les plus répandues restent toutefois les plus banales, comme la fraude à la carte bancaire volée ou usurpée.
3. Enfin la dernière ruse en vigueur est celle qui profite de la norme SEPA, l'espace de paiement unique européen :Les escrocs se font passer pour le responsable informatique de la banque qui gère les comptes de l'entreprise ciblée. Ils arrivent alors à convaincre l'interlocuteur de la société d'effectuer une série de tests et, à distance, ils prennent le contrôle de l'ordinateur et effectuent des virements directement sur leur compte en banque.
Cette technique est rendue possible par le système SEPA grâce auquel la banque n'a plus à se soucier de l'accord du client avant d'effectuer un virement.
Le client peut toutefois contester l'opération dans le cas où il constate un virement anormal.
60% des entreprises sont satisfaites de la réaction de leur banque.
4. Enfin, il existe aussi un dernière fraude, plus automatisée, moins humaine car basée sur le principe de fonctionnement des virus : Les ransomwares.Un ransomware, ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
Un ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent. Les modèles modernes de rançongiciels sont apparus en Russie initialement, mais on constate que le nombre d'attaques de ce type a grandement augmenté dans d'autres pays, entre autres l'Australie, l'Allemagne, les États-Unis.
Malheureusement, cette stratégie criminelle s'est avérée rentable et c'est pourquoi de nouvelles versions de cheval de Troie plus puissantes sont apparues en 2014. Nous souhaitions vous avertir contre le ransomware « Onion » (aussi connu sous le nom de CTB-Locker) qui utilise le réseau anonyme TOR (The Onion Router) et les Bitcoins pour mieux protéger des autorités, les criminels, leurs fonds et leurs clés d'accès aux fichiers des victimes.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
https://www.aiservice.fr/News/2014/Septembre/depannage-informatique-domicile-paris-2014-429-entreprises-sont-victimes-escroqueries-bancaires-derniere-ruse-norme-sepa-espace-de-paiement-unique-europeen
http://blog.kaspersky.fr/ransomwares-tor-cryptolocker/
http://fr.wikipedia.org/wiki/Ransomware
http://acteursdeleconomie.latribune.fr/finance-droit/2014-06-26/kpmg-les-dessous-d-une-escroquerie-record-a-7-6-millions.html