05/07/2012

EPR07/2012
www.enisa.europa.eu

L'agence européenne ENISA pour la sécurité sur Internet : les braquages de banques en ligne "High Roller" révèlent des failles dans la sécurité

Beaucoup de systèmes bancaires en ligne se fient à tord aux ordinateurs considérés comme sécurisés, mais les banques devraient plutôt prendre le parti pris que les ordinateurs de leurs clients sont infectés, déclare l'agence européenne ENISA en réponse à des rapports au sujet de l'attaque informatique nommée "High Roller".

Les récentes attaques informatiques "High Roller" de comptes bancaires de riches sociétés qui brassaient des dizaines de millions de dollars ont été analysées dans un rapport récemment publié par McAfee et Guardian Analytics. Le rapport décrit les détails techniques et l'impact de la série d'attaques en ligne. Le vieil adage qui dit que «les criminels vont là où l'argent est" pourrait être traduit aujourd'hui par "les braqueurs de banque vont sur internet", comme a déclaré le Directeur exécutif de l'ENISA, le professeur Udo Helmbrecht. Il ne faut donc pas s'étonner que les grands groupes de crime organisé ciblent les sites bancaires en ligne. Pourtant, les attaques ont attiré l'attention pour trois raisons :

1. Hautement automatisées : Les hackers ont réduit l'intervention manuelle au minimum, en s'appuyant principalement sur l'automatisation. Les attaques ont également été rapides et sont facilement passées inaperçues pour l'utilisateur.

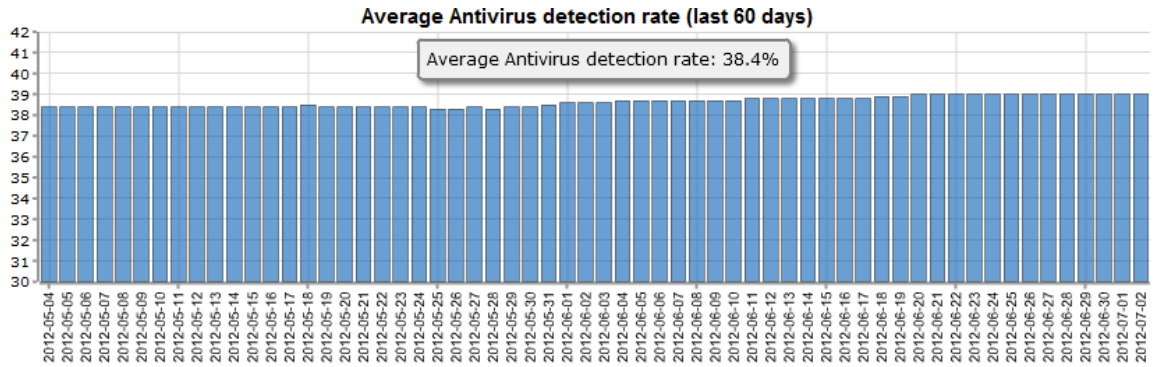
2. Sophistiquées : Les mesures de protection des banques, comme l'authentification à deux facteurs et la détection des fraudes, ont été contournées. Les utilisateurs n'ont pas remarqué immédiatement puisque les transactions frauduleuses ont été cachées par des logiciels malveillants (insérant un code JavaScript dans les pages).

3. Ciblées : Seuls les ordinateurs des utilisateurs ayant un solde élevé ont été ciblés (par exemple, environ 5000 ordinateurs aux Pays-Bas).

Les cyber-attaques se sont déroulées en trois phases. Tout d'abord, les cibles ont été identifiées à l'aide de la reconnaissance en ligne et du hameçonnage. Les victimes ayant accès à des comptes à solde élevé (d'où le nom de « High Rollers ») ont été choisies. Ensuite, les logiciels malveillants (SpyEye, Zeus et Ice 9) ont été installés sur l'ordinateur de la victime, le logiciel étant personnalisé selon les sites bancaires en ligne de cette dernière. Le programme se déclenchait lorsque la victime commençait une nouvelle session bancaire en ligne. SpyEye, Zeus et Ice 9 sont des logiciels malveillants courants et ont été formatés sur mesure pour cette attaque. Plus tard, les transactions frauduleuses automatisées étaient effectuées au nom de l'utilisateur et dissimulées par des messages d'avertissement et des messages en attente. Le logiciel malveillant transférait ensuite des sommes provenant des comptes épargne vers les comptes courants, puis à des mules à l'étranger qui retiraient l'argent en liquide et l'envoyaient ensuite, utilisant un système de transfert d'argent de particulier à particulier (tels que Western Union). Une analyse technique détaillée et une série de recommandations de McAfee et de Guardian Analytics peut être consultée en ligne.

Recommandations

1. Supposer que tous les ordinateurs sont infectés : Les attaques utilisaient Zeus, un kit pour virus Do-It-Yourself disponible pour environ un millier d'euros. Zeus est un virus prêt à l'emploi disponible comme tel depuis environ 2007 ayant un faible taux de détection.[1]Dans la conjoncture actuelle, il est plus sûr pour une banque de supposer que tous les ordinateurs de ses clients sont infectés, et les banques devraient ainsi prendre des mesures de protection pour faire face à cette situation.



Chiffres concernant Zeus: Seulement 40% environ des logiciels malveillants Zeus sont détectés.

2. Sécuriser les dispositifs de services bancaires en ligne : de nombreux systèmes bancaires en ligne, certains avec des codes de transaction à usage unique, les calculatrices ou des lecteurs de cartes à puce, se basent sur l'hypothèse que l'ordinateur du client ne contient pas de virus. Compte tenu de l'état actuel de la sécurité informatique, cette hypothèse est dangereuse. **Les banques devraient plutôt supposer que les PC sont infectés, et toujours prendre des mesures pour protéger les clients contre les transactions frauduleuses.** Par exemple, une authentification à deux facteurs de base n'empêche pas que « l'attaque de l'homme du milieu » ou celle de « l'homme dans le navigateur » n'attaque[2] les transactions. Par conséquent, il est **important d'effectuer une vérification croisée** avec l'utilisateur concernant la valeur et la destination de certaines opérations, par l'intermédiaire d'un canal de confiance, sur un **dispositif de confiance** (par exemple, un SMS, un appel téléphonique, un lecteur de carte à puce autonome avec écran). Même les smartphones pourraient être utilisés ici, à condition que la sécurité du smartphone soit ad hoc.

3. Une étroite coopération était nécessaire pour déjouer des centres de commandement mondiaux : La cyber-attaque a été lancée en utilisant de manière dynamique des serveurs de commande et de contrôle situés à travers le monde, en utilisant par exemple des botnets (ou réseaux zombies) en flux rapides et des fournisseurs d'hébergement bulletproof (sécurisés). Les criminels utilisent ces ruses pour rendre l'application de la loi et la

---

[1] Le taux de détection antivirus des codes binaires de Zeus (detection rate for Zeus binaries) est en moyenne de 38,4%. En d'autres termes, même si vous possédez des programmes antivirus à jour, il y a toujours une grande chance d'être infecté.

[2] Même si l'utilisateur doit taper un nouveau code secret à chaque fois pour authentifier la transaction sur le serveur, le hacker peut toujours intercepter le code et le retranscrire sur le serveur pour exécuter une transaction frauduleuse.

procédure de démantelage plus compliquées. **Par conséquent, une forte collaboration mondiale, tant en termes de prévention qu'en termes de réponse est nécessaire.** L'ENISA travaille sur le resserrement des liens et l'échange de plus d'informations entre les équipes nationales d'intervention d'urgence informatique (CERT), sur les applications de la loi et sur les relations entre les pays de l'UE pour améliorer la réponse aux incidents par-delà les frontières géographiques.

La prévention des attaques en ligne est primordial, mais il est aussi nécessaire d'être prêt lorsque des attaques se produisent. L'ENISA a collaboré avec les différents Etats membres de l'UE pour veiller à ce que chaque pays dispose de CERTs (équipes nationales d'intervention d'urgence informatique) efficaces pour gérer les incidents de cyber-sécurité. L'ENISA organise des exercices internationaux de cyber-sécurité à grande échelle (par exemple Cyber Europe 2010, Cyber Atlantic 2011, et très prochainement Cyber Europe 2012) pour accroître la collaboration internationale en matière d'incidents de sécurité à grande échelle. L'ENISA travaille aussi avec les États membres à l'amélioration des bilans d'incidents afin d'assurer une plus grande transparence sur les causes, la fréquence et l'impact des incidents passés. Actuellement les consommateurs, les entreprises et les autorités sont dans l'obligation de faire des estimations approximatives. La Commission européenne a récemment annoncé une stratégie prochaine pour la sécurité sur Internet, expliquant la possibilité d'étendre l'Article 13a (bilan des incidents obligatoires et mesures de sécurité) au-delà du simple secteur des communications électroniques.

A l'avenir, la sécurité du navigateur et celle des smartphones va jouer un rôle toujours croissant étant donné que plus en plus de transactions sont réalisées sur des smartphones ou des tablettes. L'adoption rapide des smartphones offre une occasion en or d'améliorer la sécurité dernier-cri (par exemple en utilisant des appstores examinés de près ou en utilisant les smartphones comme des facteurs secondaires), sans pour autant prendre pour acquis la sécurité des smartphones.[3]

Pour plus d'informations: Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Mobile: + 30 6948 460 143, ou cert-relations@enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu

[3] *Notez que même si nous voyons que beaucoup de vendeurs de smartphones ont profité de l'occasion pour améliorer la sécurité des ordinateurs, nous devrions rester sur nos gardes : il y a déjà eu des cas où les criminels ont infecté l'ordinateur et le smartphone de la victime afin de contourner les systèmes d'authentification à deux facteurs basés sur les SMS, à l'aide de Zitmo.*