Le secteur public ciblé par la cybercriminalité | Le Net Expert Informatique

Le secteur public ciblé par la cybercriminalité

« Au cours du second trimestre, nous avons assisté à une mutation dans l'univers des menaces. Les pirates informatiques font désormais preuve de davantage de sophistication et de créativité afin de renforcer et de réinventer leurs méthodes d'attaques existantes », observe Raimund Genes, CTO de Trend Micro. « La vision éthérée de la cybercriminalité n'est plus d'actualité. Ce trimestre a démontré que les dommages potentiels des cyberattaques vont bien au-delà de simples bugs logiciels. Le piratage d'avions, de voitures intelligentes et des chaines de TV est en effet devenu une réalité. »

Les hackers identifient et affinent leurs approches de façon plus stratégique, ciblant ainsi leurs victimes de manière plus sélective afin d'améliorer le taux d'infection de leurs attaques. Une tendance qui reflète une réelle progression de plusieurs méthodes d'attaques traditionnelles, avec notamment un bond de 50% de l'utilisation du kit d'exploitation Angler et de +67% pour les menaces utilisant des kits d'exploitation en général. Les attaques ciblant les banques en ligne sont par ailleurs en forte augmentation dans l'hexagone, avec plus de 60% du nombre de PC infectés entre le premier et le second trimestre 2015. D'autre part, l'adware Opencandy et le malware Upatre ont été particulièrement actifs en France ce trimestre, avec respectivement 12 773 et 3 854 PC infectés. Le malware Dyre arrive quant à lui en 4ème position avec 1 469 infections.

De même, les administrations ont été les cibles privilégiées de cyberattaques au cours du second trimestre, avec les piratages massifs des données de l'Internal Revenue Service (le fisc américain) en mai et du système de l'U.S. Office of Personnel Management (une agence gouvernementale américaine responsable de la fonction publique) en juin. Le piratage des données de l'OPM constitue un modèle du genre avec, à la clé, la divulgation de données personnelles identifiables portant sur près de 21 millions d'individus. D'autres agences gouvernementales ont été impactées par des campagnes ciblées utilisant des macros malveillantes, de nouveaux serveurs C&C (Command & Control), de nouvelles vulnérabilités, ainsi que la faille zero-day Pawn Storm.

En se penchant sur le panorama global des menaces au cours du second trimestre, on remarque que les États-Unis jouent un rôle majeur, que ce soit en tant que pays d'origine mais également en tant que cible de nombreuses attaques. Les liens malveillants, le spam, les serveurs C&C et les ransomware y sont tous très présents.

Parmi les points essentiels du rapport :

Des attaques perturbant les services publics : réseaux de diffusion, avions, véhicules automatisés et routeurs résidentiels présentent non seulement un risque d'infection élevé par malware, mais sont également susceptibles d'avoir des répercussions sur l'intégrité physique de leurs utilisateurs.

Le succès d'attaques ransomware ou ciblant les terminaux de points de vente (PoS), aubaine pour les cybercriminels solitaires en quête de notoriété : en déployant les attaques FighterPoS et MalumPoS, ainsi que keylogger Hawkeye, les hackers solos "Lordfenix" et "Frapstar" ont démontré que la force de frappe d'individus isolés est aujourd'hui indéniable.

La lutte des gouvernements contre la cybercriminalité : Interpol, Europol, le département américain de la sécurité nationale et le FBI ont contribué à démanteler des réseaux botnets majeurs et déjà bien établis. D'autre part, l'inculpation de Ross Ulbricht, fondateur de Silk Road, a mis en lumière la nature obscure et redoutable du Dark Web.

Les impacts nationaux et politiques d'attaques ciblant des organisations gouvernementales : la redoutable attaque sur l'OPM a prouvé que la confidentialité de nos données personnelles n'est pas avérée. Les macros malveillantes, les tactiques d'island-hopping (piratage d'une entité tierce avant de remonter vers la cible finale) et les serveurs C&C comptent parmi les tactiques les plus utilisées pour cibler les informations gouvernementales lors d'attaques.

De nouvelles formes de menaces visant les sites web publics et les dispositifs mobiles : alors que les menaces ciblant les logiciels sont toujours d'actualité, les vulnérabilités des applications web se montrent tout aussi dangereuses. Les assaillants savent tirer parti de toute vulnérabilité existante, tandis que les applications personnalisées nécessitent une prise en charge toute aussi personnalisée afin de neutraliser ces passerelles potentielles d'intrusion.

Le rapport

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.globalsecuritymag.fr/Trend-Micro-identifie-de-nouvelles,20150917,55924.html