News Release

For Immediate Release

Une étude indépendante de Georgia Tech révèle les meilleures façons d'informer les clients d'une « infection »

SAN FRANCISCO, Californie--(Marketwire - February 21, 2013) - Un robot, qui aurait défalqué 14 millions de dollars de bénéfices illicites, a permis d'apprendre une leçon d'importance. La situation est exemplaire de la façon dont la communauté en ligne peut alerter et aider au mieux les clients dont les systèmes sont infectés. Lors d'une présentation à la 27e réunion générale du M[3]AAWG à San Francisco, les chercheurs de Georgia Tech ont annoncé mardi les résultats d'une étude basée sur les réponses apportées par l'industrie au cheval de Troie DNS Changer. Ils ont également proposé des recommandations communes pour aider à freiner les épidémies de futurs programmes malveillants.

Parmi les méthodes les plus efficaces pour informer les clients de l'infection de leurs systèmes, l'étude sur l'éradication de DNS Changer a recensé des appels téléphoniques, des affichages et la redirection des utilisateurs vers des pages Web personnalisées. Les chercheurs Wei Meng et Ruian Duan, travaillant sous la supervision du professeur Wenke Lee à la Georgia Tech School of Computer Science, ont également constaté que les avertissements « actifs » via les médias sociaux étaient utiles à l'éradication. Grâce à cette approche, des sites comme Google ont directement informé les utilisateurs de leur infection par le biais de leur navigateur, une méthode qui s'est révélée plus efficace pour les inciter à désinfecter leurs systèmes que les avertissements passifs émis dans des messages généraux ou des articles de presse sur les plateformes de médias sociaux.

« Les médias sociaux peuvent jouer un rôle essentiel en signalant aux utilisateurs que leurs systèmes sont infectés et en endiguant les épidémies de programmes malveillants. Nous savons qu'il est essentiel de mettre en œuvre des notifications directes et actives, plus tôt dans la procédure », a expliqué Wenke Lee.

Les chercheurs ont étudié les divers types d'alertes aux utilisateurs finaux et les efforts des opérateurs de réseau pour aider les clients à désinfecter leurs systèmes, notamment à l'aide de domaines privés, de redirections DNS, de logiciels anti-virus et d'outils de suppression des logiciels malveillants. Selon le co-président du M[3]AAWG, Michael O'Reirdan, le défi auquel l'industrie est confrontée en matière de robots consiste notamment à déterminer comment informer les utilisateurs que leurs systèmes ont été infectés, de façon opportune et crédible, puis à aider les clients non techniciens à désinfecter leurs machines.

Michael O'Reirdan l'explique : « La réponse de l'industrie au logiciel malveillant DNS Changer a clairement montré comment concurrents et fournisseurs peuvent collaborer lorsque la sécurité des utilisateurs est en jeu. L'occasion était formidable d'étudier objectivement les différentes approches développées par les sociétés pour aider les clients et comprendre le rôle majeur que chacun de nous joue dans la sauvegarde de l'expérience en ligne. L'implication active des fournisseurs d'outils de sécurité et de lutte contre les logiciels malveillants, des plateformes de médias sociaux, de la police, des fournisseurs de systèmes d'exploitation et des fournisseurs de technologie de réseaux domestiques a été jugée cruciale. Au final, l'ensemble de l'écosystème Internet doit collaborer pour protéger les utilisateurs finaux. »

Les données utilisées dans cette étude pour déterminer les taux d'infection et de nettoyage étaient anonymes. Elles ont été fournies par les principaux FAI du monde entier à l'équipe de recherche du Georgia Tech Information Security Center (GTISC), par l'intermédiaire du groupe de travail sur DNS Changer (DCWG). Pour identifier les

différentes techniques de notification et de médiation utilisées, les chercheurs ont envoyé des questionnaires aux opérateurs de réseau pour leur demander comment ils avaient alerté leurs clients infectés par DNS Changer et quels furent les efforts de réparation employés pour les aider à nettoyer leurs machines. Un FAI qui n'a engagé aucune mesure pour corriger la situation est devenu la référence selon laquelle mesurer l'efficacité des autres approches, selon Wenke Lee.

Entre 2007 et 2011, le cheval de Troie DNS Changer a détourné des recherches sur Internet et redirigé les navigateurs Web des ordinateurs infectés vers des sites frauduleux en utilisant les serveurs DNS malveillants exploités par le réseau publicitaire Rove Digital. Toutefois, si les serveurs DNS malveillants avaient été éteints lors de l'arrestation des Estoniens soupçonnés d'être responsables, les utilisateurs infectés n'auraient pas pu accéder au Web. Le groupe du DCWG a été constitué pour aider la police à faire face aux éventuels problèmes des utilisateurs finaux suite à l'action répressive. Le DCWG a également contribué à exploiter et surveiller les serveurs DNS « propres », gérés légalement par l'Internet Systems Consortium (ISC) entre novembre 2011 et juillet 2012, en vertu de l'ordonnance d'un tribunal américain. En conséquence, au lieu de perdre brusquement leur accès à Internet, des millions d'utilisateurs ont été informés qu'ils étaient infectés et qu'ils devaient nettoyer leurs machines.

L'étude complète sur le nettoyage de DNS Changer est disponible sur le site Web du M^{3}AAWG, à l'adresse https://www.maawg.org/sites/maawg/files/news/GeorgiaTech_DNSChanger_Study-2013-02-19.pdf.

À propos du groupe de travail M^{3}AAWG (Groupe de travail portant sur la messagerie, les logiciels malveillants et la lutte contre l'abus mobile)

Le Groupe de travail portant sur la messagerie, les logiciels malveillants et la lutte contre l'abus mobile (M3AAWG) rassemble l'industrie pour lutter ensemble contre les robots, les logiciels malveillants, les spams, les virus, les attaques par déni de service et d'autres interventions malveillantes en ligne. Le M^{3}AAWG (www.M3AAWG.org) représente plus d'un milliard de boîtes de réception de certains des plus grands opérateurs de réseau du monde. Le groupe s'appuie sur le sérieux et l'expérience mondiale de ses membres pour s'attaquer aux abus sur les réseaux existants et dans les nouveaux services émergents en exploitant la technologie, la collaboration et les politiques publiques. Il se consacre également à la sensibilisation des décideurs mondiaux aux questions techniques et opérationnelles liées à l'abus en ligne et à la messagerie. Basé à San Francisco, en Californie, le M^{3}AAWG est axé sur les besoins du marché et soutenu par des opérateurs de réseau et des fournisseurs de messagerie de premier plan.

Conseil d'administration du M^{3}AAWG : AT&T (au NYSE: T), Cloudmark, Inc., Comcast (au NASDAQ: CMCSA), Constant Contact (au NASDAQ: CTCT), Cox Communications, Damballa, Inc., Eloqua, Facebook, France Telecom (au NYSE et à Euronext : FTE), Google, PayPal, Return Path, Symantec, Time Warner Cable, Verizon Communications et Yahoo! Inc.

Membres à part entière du M^{3}AAWG : 1&1 Internet AG, Adaptive Mobile Security LTD, Adobe Systems Inc., AOL, BAE Systems Detica, Cisco Systems, Inc., Dynamic Network Services Inc., Email Sender and Provider Coalition, Genius, iContact, Internet Initiative Japan (IIJ NASDAQ : IIJI), Mailchimp, McAfee Inc., Message Systems, Mimecast, Nominum, Inc., Proofpoint, Scality, Spamhaus, Sprint et Twitter.

Une liste complète des membres est disponible à l'adresse http://www.m3aawg.org/about/roster.

Contact auprès des médias :
Linda Marcus, APR, 1+714-974-6356, LMarcus@astra.cc, Astra Communications