Les malwares les plus menaçants de 2015

Les malwares les plus menaçants de 2015

Hexis Cyber Solutions Inc (Hexis) vient de publier une forte mise en garde sur les outils les plus sophistiqués et automatisés que les cyber-criminels utilisent pour attaquer toutes organisations.

Voici ci-dessous les attaques 2015 de logiciels les plus menaçants jusqu'ici.

Sakula – Cette famille de malwares sophistiqués a été développée contre le Bureau de la Gestion du personnel américain et de l'assurance santé, Anthem.
Cela représente l'une des plus grandes cyber-attaques dans son genre ayant été utilisé avec succès ouvrant une brèche de plus de 100 millions de dossiers. Cette menace agit comme rappel que toute organisation possédant des informations personnelles ou financières représente une cible de grande valeur pour des attaquants déterminés qui souhaitent obtenir une information spécifique.

Kjw0rm – Des attaques parrainées par les Etats continuent à émerger avec celles de cyber-terroristes, groupes criminels organisés voir même des gouvernements étrangers qui développent des logiciels malveillants conçus pour prendre le contrôle des systèmes et des opérations.
Ce qui est important de retenir est que ces techniques, tactiques et procédures utilisées par les Etats Nations – qu'elles soient avancées ou non – font leur chemin dans l'arsenal de cette large communauté établie des cybers hackers.

Dridex – En tant que cybercriminel, les organisations doivent répartir leur temps, leur argent et leurs ressources de manière efficace afin de rester « dans le jeu ».
Dridex a été développé par des cyber-criminels qualifiés qui utilisent les e-mails pour déliver des documents Microsoft Word infectés qui capturent des informations bancaires en ligne. Cette méthode d'attaque représente un moyen rapide et facile de pénétrer un réseau pour le gain financier et souvent avec très peu d'investissement pour l'exploitant.

Dyre – A l'ère du numérique, la majorité des programmes de type « exploit » viennent d'attaques de type « livraison de contenu » avec des tactiques comme le phishing, spear phishing et whaling on the rise.
Le cas de Dyre est un exemple parmi d'autres où les clients de certaines des plus grandes banques du Royaume-Uni ont été ciblés dans le cadre de grandes campagnes de phishing utilisant des logiciels malveillants réputés, et conçus pour voler des données financières.
Les organisations doivent se rendre responsables de l'éducation de leurs clients et également de la promotion des meilleures pratiques et approches à avoir à l'égard d'emails et liens web inattendus d'utilisateurs familiers ou non.

Ransomware – Les entreprises et les consommateurs ont été tous les deux victimes de cette souche de malwares qui empêche les utilisateurs d'accéder aux informations, habituellement par chiffrement.
Les hackers demandent ensuite une rançon en échange du déchiffrement de ces informations et de rendre le contrôle aux utilisateurs légitimes de telle sorte qu'ils puissent accéder à nouveau au système.
Pour éviter que les administrateurs réseaux aient à payer les pirates pour avoir l'accès à leurs propres systèmes, une combinaison de la sécurité des postes de travail et de surveillance du réseau est nécessaire afin d'identifier et d'isoler toute activité suspecte avant que les cybercriminels prennent le contrôle.

Ghost Push – La hausse des applications malveillantes disponibles sur les boutiques en ligne d'applications mobiles montre que près d'un million d'appareils Android ont été infectés et souligne la nécessité pour les organisations ayant des politiques sur l'utilisation d'appareils mobiles d'être vigilants tout en rappelant que la gestion de l'accès demeure de la plus haute importance.
Les entreprises ont besoin de savoir quels appareils ont accès au réseau, qui en est responsable, et doivent introduire une couche supplémentaire dans la sécurité du réseau qui surveillerait l'activité de chaque terminal identifiant tous signes d'alertes malveillantes.
« L'ère de la Seule prévention est révolue depuis longtemps. En 2015 seulement, les entreprises françaises ont subi en moyenne 21 incidents de cyber sécurité par jour. C'est 51% de plus qu'il y a un an selon une étude mondiale du cabinet PwC. » reflète Denis Gadonnet, Directeur Sud Europe d'Hexis Cyber Solutions.
« Au lieu de cela les entreprises ont besoin d'être préparées pour une attaque en faisant en sorte d'être en mesure de réagir rapidement.
L'Investissement dans les technologies qui permettent de détecter rapidement et répondre aux attaques les plus sophistiquées, et ciblées doivent maintenant être une priorité.
Alors seulement, les organisations seront en mesure de jouer à jeu égale et de rivaliser avec succès contre les attaquants. "
