# Tendances et prévisions en cybercriminalité pour 2015 | Le Net Expert Informatique


## Tendances et prévisions en cybercriminalité pour 2015

**Augmentation des attaques ciblées** En 2015, les attaques ciblées deviennent encore plus sophistiquées. Souvent appelées APT (Advanced Persistant Threats), elles sont différentes des cyberattaques traditionnelles. Conçues pour attaquer des victimes spécifiques et pour être silencieuses, les attaques ciblées peuvent être cachées et non détectées dans des réseaux insuffisamment sécurisés.
"Le vecteur des attaques ciblées profite généralement des attaques d'ingénierie sociale", explique Pablo Ramos, chef du laboratoire de recherche ESET en Amérique Latine. "C'est alors que la manipulation psychologique est utilisée pour pousser les victimes potentielles à commettre certaines actions ou à divulguer des informations confidentielles. Les attaques peuvent également prendre l'apparence d'exploits jour-zéro, où elles profitent de vulnérabilités nouvellement découvertes dans un système d'exploitation ou une application particulière."
Au cours de 2014, le blog WeLiveSecurity d'ESET a publié un certain nombre d'analyses approfondies concernant les attaques ciblées, telles que BlackEnergy campaign et Operation Windigo .

**Les systèmes de paiement en ligne attirent plus de malware**
Alors que toujours plus de personnes adoptent les systèmes de paiement en ligne pour des biens et des services, ces systèmes deviennent encore plus attrayants pour les concepteurs de malware intéressés par les gains financiers.
2014 a vu la plus grande attaque connue à ce jour en matière de paiement digital, quand un pirate a récolté plus de 600.000 dollars US en Bitcoins et Dogecoins en utilisant un réseau de machines infectées.
ESET a signalé les attaques effectuées en mai contre Dogevault site , où les utilisateurs du très populaire portefeuille électronique ont signalé des retraits non autorisés de leurs comptes avant que le site ne soit obligé d'être déconnecté suite à la destruction des données du site par les attaquants. On estime que 56.000 dollars US ont été volés aux utilisateurs du portefeuille en ligne.
Nous avons aussi vu des attaques de force brute telles que Win32/BrutPOS , qui ont essayé d'accéder aux comptes protégés par un mot de passe en les bombardant de mots de passe populaires afin d'avoir un accès à distance – un rappel général en faveur de l'utilisation de mots de passe forts et uniques.

**L'internet des choses – nouveaux jouets pour pirates**
Alors que de nouveaux appareils se connectent à internet et stockent plus de données, ils deviennent un vecteur d'attaque attrayant pour les cybercriminels. Au cours de 2014, nous avons trouvé plus de preuves de la hausse de cette tendance. Lors de la conférence Defcon, on a vu les attaques sur les voitures en utilisant le dispositif ECU, ou sur la voiture Tesla qui a été piratée afin d'en ouvrir les portes alors qu'elle roulait.
Des attaques et des concepts ont aussi été montrés dans le secteur de la télévision sur différents systèmes, systèmes biométriques sur smartphones, routeurs – pour ne pas mentionner Google glasses.
C'est un domaine émergent pour la cybercriminalité et il restera un secteur de concentration pour l'industrie de la sécurité. Alors que cela pourrait prendre des années avant de devenir une menace grave, il faut agir dès à présent afin de mieux prévenir ce type d'attaques.
Plus d'information
Le rapport complet est disponible sur WeLiveSecurity.com.

---



---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14be54fe5faeb40f?compose=14be53ae312f08d7