Cybercriminalité : une année 2015 sous haute tension

Les cybercriminels sont de plus en plus confiants : ils avaient auparavant tendance à attaquer les usagers de services bancaires, voyant en eux le maillon faible de la chaîne de sécurité, mais les experts de Kaspersky Lab anticipent désormais des cyber-attaques ciblées d'envergure sur les banques elles-mêmes. Et les fraudeurs ne s'arrêteront pas là ; ils devraient tenter le tout pour le tout en essayant de développer de nouveaux malwares capables de retirer du liquide directement depuis les distributeurs. Outre les cyber-crimes financiers, 2015 suscitera probablement encore plus d'inquiétudes quant à la confidentialité et à la sécurité des appareils Apple, et fera resurgir les peurs quant aux appareils connectés ; il s'agira d'empêcher les hackers d'utiliser des outils comme les imprimantes réseau pour pénétrer les réseaux d'entreprises.

1. Quand les cybercriminels s'inspirent des APT

Lors d'une étude récente, nous avons découvert une attaque dans laquelle l'ordinateur d'un comptable a été compromis et utilisé pour effectuer un transfert important avec une institution financière. Cela illustre une tendance intéressante : celle des attaques ciblées contre les banques elles-mêmes.Nous assistons à une augmentation des incidents provoqués par des malwares dans lesquels les banques sont infiltrées en utilisant des méthodes utilisées dans les APT. Une fois que les pirates ont pénétré les réseaux de la banque, ils volent assez d'informations pour pouvoir voler de l'argent directement à la banque et ce, de plusieurs manières :En prenant le contrôle des distributeurs automatiques à distance afin d'obtenir du liquideEn réalisant des transferts SWIFT depuis plusieurs comptes de clientsEn manipulant les systèmes bancaires en ligne pour réaliser des transferts en arrière-planDe telles attaques annoncent l'émergence d'une nouvelle tendance qui s'inspire des attaques APT que l'on voit dans le monde cybercriminel.

2. Les groupes se fragmentent, les attaques APT se diversifient

La révélation de l'existence de ces groupes utilisant les APT a mené à l'exposition publique et la condamnation d'un groupe de pirates qui aurait mené des actions de cyber-espionnage contre des entreprises américaines.Alors que les équipes de recherche continuent d'encourager la découverte de ces groupes ayant recours aux APT, nous nous attendons à des changements en 2015 : les groupes d'APT les plus importants et les plus connus se sépareront en plus petits groupes qui fonctionneront indépendamment les uns des autres. Les attaques deviendront plus répandues et davantage d'entreprises seront touchées car les petits groupes diversifieront leurs attaques. Cela signifie également que les entreprises les plus importantes qui ont déjà été compromises dans le passé par deux ou trois groupes d'APT importants (comme par exemple, 'Comment Crew' et 'Webky') seront la cible d'attaques plus diverses et provenant de plusieurs sources différentes.

3. Un ancien code, de nouvelles vulnérabilités (dangereuses)

De récentes accusations d'altération délibérée et de défaillances accidentelles dans des systèmes de chiffrement (« goto fail ») ainsi que des vulnérabilités critiques dans des logiciels connus (Shellshock, Heartbleed, OpenSSL) ont laissé la communauté dubitative face à ces logiciels non vérifiés. La réaction a donc été de lancer des analyses indépendantes de la clé de ces logiciels ou que des chercheurs en sécurité les dissèquent à la recherche de vulnérabilités critiques (une alternative à l'analyse non officielle). Cela signifie que 2015 sera une autre année remplie de nouvelles vulnérabilités dangereuses qui apparaitront dans des anciens codes, exposant ainsi l'infrastructure Internet à des attaques.

4. Augmentation des attaques contre les distributeurs automatiques et les points de vente

Les attaques contre les distributeurs automatiques semblent avoir explosé cette année avec plusieurs incidents publics et la vive réaction des autorités à travers le monde pour faire face à cette

crise. Une des conséquences de ces incidents est la prise de conscience que ces distributeurs automatiques sont très faciles à pirater et les cybercriminels l'ont bien remarqué. Comme la plupart de ces systèmes fonctionnent sous Windows XP et disposent d'une sécurité physique très faible, ils sont très vulnérables par défaut. Et comme les institutions financières disposent d'argent liquide, il est logique que les cybercriminels commencent par là.En 2015, nous nous attendons à observer une évolution de ces attaques contre les distributeurs automatiques grâce à l'utilisation de techniques d'APT afin d'accéder au système d'information de ces machines. On verra ensuite les pirates compromettre les réseaux des banques et utiliser cet accès pour prendre le contrôle des distributeurs en temps réel.

5. Attaques Mac : des botnets OS X

Malgré les efforts d'Apple pour verrouiller le système d'exploitation Mac, nous continuons d'observer des logiciels malveillants envoyés via des torrents ainsi que des logiciels piratés. La popularité grandissante des appareils Mac OS X fait tourner les têtes dans le monde criminel et rend très intéressante la création de malwares pour cette plateforme. L'écosystème fermé par défaut empêche les malwares d'envahir la plate-forme mais certains utilisateurs choisissent de désactiver les mesures de sécurité Mac OS X – surtout ceux qui utilisent des logiciels piratés. Cela signifie que ceux qui cherchent à pirater les systèmes OS X pour diverses raisons savent qu'ils ont juste à cacher leur malware dans un logiciel attirant (certainement en le faisant passer pour un générateur de clé) pour réussir à le diffuser. À cause des idées reçues sur la plateforme OS X, ces systèmes ont peu de chances d'avoir une solution antimalware qui détectera les infections une fois le malware installé : ce dernier passera donc inaperçu pendant très longtemps.

6. Des attaques contre les systèmes de billetterie automatique

Les incidents comme le piratage NFC contre les transports publics chiliens montre l'intérêt que les criminels ont pour les ressources publiques comme les systèmes de transports publics. Certains pirates ne chercheront même pas à obtenir de l'argent pour ce type d'attaques et seront simplement contents de voyager gratuitement et de partager leur technique avec d'autres. Bien que ces systèmes de billetterie soient vulnérables (la plupart d'entre eux fonctionnent sous Windows XP), dans de nombreuses villes, ils gèrent directement des transactions par carte bancaire. Nous nous attendons donc à voir des attaques plus violentes contre ces systèmes que cela soit pour détourner le système ou voler des données de carte bancaire.

7. Des attaques contre les systèmes de paiement virtuel

La logique veut que les cybercriminels cherchent à gagner de l'argent grâce à leurs attaques de la manière la plus efficace et la plus simple possible. Quoi de mieux que les systèmes de paiement virtuel qui n'en sont encore qu'à leurs débuts ? Nous nous attendons donc à ce que les criminels se jettent sur toutes les opportunités qu'ils trouveront pour exploiter ces systèmes. Qu'il s'agisse d'ingénierie sociale, d'attaques ciblant les appareils des utilisateurs (dans la plupart des cas, les téléphones mobiles), ou de pirater directement des banques, les cybercriminels choisiront les attaques qui pourront leur rapporter de l'argent rapidement et les systèmes de paiement virtuel finiront par en faire les frais.Ces craintes peuvent également s'appliquer à Apple Pay qui utilise la NFC (Near Field Communications) pour gérer les transactions sans fil des utilisateurs.

8. Apple Pay

De précédentes attaques se sont concentrées sur les systèmes de paiement NFC mais, grâce à son adoption limitée, ces attaques n'ont pas rapporté beaucoup. Apple Pay va certainement changer cela. L'enthousiasme pour ce nouveau système de paiement va faire exploser l'adoption de ce système et cela attirera bien évidemment les cybercriminels qui chercheront à intercepter ces transactions. Le design d'Apple se concentre principalement sur la sécurité (avec par exemple, la virtualisation des données de transaction) mais nous sommes très curieux de voir comment les pirates exploiteront les fonctionnalités de ce système.

9. Compromettre l'Internet des objets

Les attaques contre l'Internet des objets (ou objets connectés) se sont limitées aux prototypes et aux avertissements (parfois exagérés) annonçant que les smart TV et les réfrigérateurs seront ciblés par les pirates pour créer des Botnets ou lancer des attaques malveillantes.Alors que de plus en plus d'appareils connectés sont disponibles, nous nous attendons à observer un débat plus important sur

la sécurité et la confidentialité, surtout parmi les entreprises de ce secteur. En 2015, on verra certainement des attaques contre des imprimantes connectées en réseau et autres appareils connectés qui aideront les pirates expérimentés à s'infiltrer dans les réseaux corporatifs. Nous nous attendons à ce que les appareils de l'Internet des objets fassent partie de l'arsenal des groupes utilisant les APT, surtout si l'on considère que la connectivité est désormais introduite aux procédés industriels ainsi qu'aux procédés de fabrication.