SÃ©curitÃ© : Les 5 PrÃ©dictions en matiÃ¨re de SÃ©curitÃ© pour 2014
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 3/12/2013 13:00:00

1. Les Logiciels Malveillants Android sâ□□Etendent aux SystÃ¨mes de ContrÃ´le Industriels et Ã Â Lâ□□Internet des Objets (Internet of Things en anglais)

Alors que les ventes de tÃ©lÃ©phones mobiles stagneront probablement dans les annÃ©es Ã venir, les dÃ©veloppeurs Android doivent trouver des marchÃ©s encore inexploitÃ©s pour le systÃ¨me dâ□□exploitation Google.

Ces marchÃ©s Ã©mergents incluent les tablettes, consoles de jeu portables, appareils â□□wearablesâ□□ (qui se portent sur soi), Ã©quipement domotique et systÃ¨mes de contrÃ´le industriels (ICS/SCADA). **FortiGuard** prÃ©dit que lâ□□annÃ©e prochaine, nous verrons les premiers exemples de logiciels malveillants sur ces nouveaux types dâ□□appareils, notamment autour des systÃ¨mes ICS/SCADA embarquÃ©s.

Bien que nous ne pensons pas voir un "Stuxnet mobile " en 2014, nous pensons que les cybercriminels seront attirÃ©s par les plateformes qui vont au-delÃ de la simple fraude par SMS.

Cela inclut de nouveaux appareils domotiques qui ont la mainmise sur notre consommation Ã©lectrique, la tempÃ©rature de nos rÃ©frigÃ©rateurs, etc. et sont dotÃ©s de logiciels avec des panneaux de contrÃ´le de connexion Ã distance pour voir qui peut Ãªtre Ã la maison Ã un instant T.

Cela donne aux cybercriminels de nouvelles et malsaines idÃ©es sur la maniÃ¨re et quand cambrioler la maison de quelquâ□□un.

2. La Bataille pour le Web Profond

Alors que le FBI va Ã©largir son champs dâ□□action en matiÃ¨re de cibles lâ□□an prochain, nous pensons que lâ□□agence continuera Ã surveiller les darknets Tor et services de partage de fichiers douteux tel que Mega Upload.

Depuis lâ□□apparition du premier virus informatique, les black et white hats jouent au jeu du chat et de la souris et, nous prÃ©disons que la surveillance plus minutieuse de ces services â□□anonymesâ□□ entrainera de nouvelles versions qui seront encore plus difficiles dâ□□infiltrer, de compromettre et/ou de dÃ©manteler.

Nous avons dÃ©jÃ vu que le dÃ©mantÃ¨lement de MegaUpload a donnÃ© naissance Ã Mega, une plateforme fondamentalement plus robuste. Attendez-vous Ã un dÃ©veloppement similaire autour de Silk Road (marchÃ© noir sur Internet qui utilise le rÃ©seau Tor) au cours de lâ□□annÃ©e prochaine.

3. Les Fournisseurs de SÃ©curitÃ© RÃ©seau Contraints de Devenir Plus Transparent

En Septembre, la Federal Trade Commission a sÃ©vÃ¨rement sanctionnÃ© une entreprise qui commercialisait une technologie de vidÃ©osurveillance pour les consommateurs. Dans sa documentation, elle indiquait que leur produit Ã©tait â□□sÃ©curisÃ©â□□ alors que les preuves dÃ©montraient clairement le contraire.

Ce fÃ»t la premiÃ¨re action de lâ□□agence contre un fabricant de produits de consommation quotidienne avec une interconnectivitÃ© Ã Internet et autres appareils mobiles. Lâ□□entreprise a dÃ» prendre un certain nombre de mesures. Lâ□□an prochain, nous prÃ©disons que ce niveau de responsabilitÃ©s et dâ□□examen sera renforcÃ© au niveau des fournisseurs de sÃ©curitÃ© rÃ©seau.

Les consommateurs nâ□□accepteront plus le discours marketing axÃ© sur un "OS propriÃ©taire dotÃ© dâ□□une sÃ©curitÃ© renforcÃ©e". Ils exigeront une preuve, et lorsquâ□□ils seront exposÃ©s Ã des risques injustifiÃ©s, ils exigeront des comptes.

Cela prendra la forme dâ□□une plus grande transparence autour des pratiques de gestion de la chaine dâ□□approvisionnement, de gestion des patchs et du cycle de vie de dÃ©veloppement sÃ©curisÃ© (Secure Development Lifecycle ou SDL).

4. Augmentation des Attaques ciblant Windows XP

Microsoft ne fournira plus de support Ã Windows XP le 8 Avril 2014. Cela signifie que les vulnÃ©rabilitÃ©s nouvellement dÃ©couvertes ne seront pas patchÃ©es, laissant les systÃ¨mes vulnÃ©rables. Selon NetMarketShare, en Septembre 2013, Windows XP est exÃ©cutÃ© encore sur 31.42% des PC dans le monde.

Selon Gartner, dâ□□ici le 8 Avril, il est estimÃ© que plus de 15% des moyennes Ã larges entreprises auront toujours Windows XP fonctionnant sur au moins 10 pourcent de leurs PC.

Lâ□□an prochain, nous prÃ©disons que les hackers, dÃ©jÃ en possession dâ□□exploits zero day, attendront jusquâ□□au 8 pour les vendre au plus offrant. En raison de leurs prix Ã©levÃ©s espÃ©rÃ©s, ces zero days seront probablement utilisÃ©s pour lancer des attaques ciblÃ©es contre les entreprises et individus de grande importance plutÃ´t que les dÃ©ployer par des cybercriminels ordinaires dans le but de propager des infections massives.

5. La BiomÃ©trie employÃ©e Ã des fins dâ□□authentification augmentera

Cette annÃ©e, Apple a fait preuve dâ□□audace lorsquâ□□il a annoncÃ© que son nouvel iPhone 5s intÃ©grerait lâ□□authentification par empreinte digitale. Peu importe quâ□□il ait Ã©tÃ© hackÃ©

quelques jours aprÃ¨s sa commercialisation. Les gens ont commencÃ© Ã parler de lâ□□importance dâ□□une authentification Ã deux facteurs dans un monde oÃ¹ la connexion par un seul mot de passe est de plus en plus archaÃ¯que.

En raison de ce regain dâ□□intÃ©rÃªt, nous prÃ©disons que lâ□□an prochain nous verrons plus dâ□□entreprises dâ□□appareils mobiles incluant un deuxiÃ¨me facteur dâ□□authentification dans leurs appareils. Nous verrons Ã©galement une augmentation de nouvelles formes dâ□□authentification, telles que les tatouages et pilules, scan de lâ□□iris et reconnaissance faciale.