WatchGuard Technologies : Le top 8 des prÃ©visions de cyber-sÃ©curitÃ© pour 2014
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 14/1/2014 13:30:00

Un scÃ©nario catastrophe hollywoodien pourrait-il se produire ? Le portail Healthcare.gov sera-t-il attaquÃ© ? Doit-on sâ□□attendre Ã lâ□□apparition de nouveaux CryptoLocker ?. WatchGuard Technologies, leader mondial des plateformes de sÃ©curitÃ© intÃ©grÃ©es, publie ses prÃ©visions annuelles de cyber-sÃ©curitÃ© pour 2014.

Parmi les Ã©lÃ©ments listÃ©s, lâ□□Ã©quipe de chercheurs en sÃ©curitÃ© de WatchGuard sâ□□attend Ã des avancÃ©es dans le domaine des ranÃ§ongiciels (ransomware), Ã des piratages visant lâ□□Internet des objets, Ã des attaques ciblant les infrastructures stratÃ©giques et Ã une violation des donnÃ©es du portail amÃ©ricain des assurances maladie Healthcare.gov.

Â« *Entre le dÃ©veloppement de botnets par des agences gouvernementales opÃ©rant dans lâ□□ombre, les importantes failles de sÃ©curitÃ© comme celle subie par Adobe et les logiciels malveillants particuliÃ¨rement nuisibles de type CryptoLocker, 2013 aura Ã©tÃ© une annÃ©e Ã©prouvante pour les spÃ©cialistes de la cyber-sÃ©curitÃ©* Â», commente **Corey Nachreiner**, Directeur de la stratÃ©gie de sÃ©curitÃ© de **WatchGuard Technologies**.

Â« *Cependant, grÃ¢ce aux nouveaux outils de visibilitÃ© dÃ©sormais disponibles, 2014 devrait Ãªtre lâ□□annÃ©e de la visibilitÃ© en matiÃ¨re de sÃ©curitÃ©. Le paysage des menaces continue certes Ã Ã©voluer Ã un rythme effrÃ©nÃ© en raison de lâ□□apparition de nouvelles techniques Ã©voluÃ©es dâ□□exploitation des vulnÃ©rabilitÃ©s et de lâ□□orientation des criminels vers de nouvelles cibles.*

NÃ©anmoins, les professionnels de la sÃ©curitÃ© devraient pouvoir utiliser ces nouveaux outils de visibilitÃ© afin de faire, Ã nouveau, pencher la balance de la cyber-guerre en leur faveur. Â»

Les principales prÃ©visions de WatchGuard pour 2014 en matiÃ¨re de sÃ©curitÃ© :

1. Le portail amÃ©ricain des assurances maladie sera la cible de nombreuses attaques :

WatchGuard sâ□□attend Ã ce que le site amÃ©ricain Healthcare.gov subisse au moins une violation de donnÃ©es en 2014.

Du fait de sa popularitÃ© et de la valeur des donnÃ©es quâ□□il stocke, Healthcare.gov constitue une cible particuliÃ¨rement attractive pour les cybercriminels.

En rÃ©alitÃ©, cette violation a, dans une certaine mesure, dÃ©jÃ dÃ©butÃ©.

DiffÃ©rents chercheurs en sÃ©curitÃ© ont dâ□□ores et dÃ©jÃ mis en Ã©vidence plusieurs incidents mineurs (indices d'attaques avortÃ©es contre des applications Web, tentatives dâ□□attaque en dÃ©ni de service (DDoS), etc.).

2. Le dÃ©veloppement du cyber-kidnapping accroÃ®t les profits des pirates :

Les ranÃ§ongiciels, une nouvelle classe de logiciels malveillants dont le but est de prendre en otage un ordinateur, ont vu leur nombre augmenter rÃ©guliÃ¨rement ces derniÃ¨res annÃ©es, mais une variante particuliÃ¨rement nuisible a fait son apparition en 2013 : CryptoLocker.

Rien que cette annÃ©e, il a touchÃ© plusieurs millions de machines, avec un fort retour sur investissement pour les cybercriminels dâ□□aprÃ¨s les estimations. WatchGuard sâ□□attend Ã ce que de nombreux cyber-dÃ©linquants tentent dâ□□imiter en 2014 le succÃ¨s de CryptoLocker, en copiant ses techniques et son mode de fonctionnement. WatchGuard prÃ©voit ainsi une multiplication des ranÃ§ongiciels en 2014.

3. Un scÃ©nario catastrophe hollywoodien :

En 2014, une attaque majeure commanditÃ©e par un gouvernement hostile et exploitant les failles dâ□□une infrastructure stratÃ©gique pourrait bien transformer un film dâ□□Hollywood en rÃ©alitÃ© tragique. Et ce, mÃªme lorsque les systÃ¨mes ciblÃ©s ne sont pas connectÃ©s Ã un rÃ©seau.

Le ver Stuxnet, si souvent montrÃ© du doigt, a en effet prouvÃ© que des cyber-attaquants motivÃ©s pouvaient infecter une infrastructure non reliÃ©e Ã un rÃ©seau avec des rÃ©sultats potentiellement dÃ©sastreux.

Des chercheurs ont consacrÃ© plusieurs annÃ©es Ã Ã©tudier les vulnÃ©rabilitÃ©s des systÃ¨mes de contrÃ´le industriel (ICS) et des solutions de supervision et dâ□□acquisition de donnÃ©es (SCADA), et ont dÃ©couvert que ces systÃ¨mes prÃ©sentaient de nombreuses vulnÃ©rabilitÃ©s.

4. Lâ□□Internet des objets, nouvelle cible des hackers :

WatchGuard sâ□□attend Ã ce que, lâ□□an prochain, les hackers, quâ□□ils soient white ou black hat, consacrent plus de temps aux terminaux informatiques non traditionnels comme les voitures, les montres, les jouets et le matÃ©riel mÃ©dical.

Si les experts en sÃ©curitÃ© informatique insistent depuis plusieurs annÃ©es sur la nÃ©cessitÃ© de sÃ©curiser ces pÃ©riphÃ©riques, il semble que le marchÃ© nâ□□en rÃ©alise lâ□□importance que maintenant. WatchGuard sâ□□attend donc Ã ce que les hackers sâ□□attachent fortement en 2014 Ã dÃ©tecter les failles de ces objets connectÃ©s, que ce soit pour les combler ou pour les exploiter.

5. 2014 sera lâ□□annÃ©e de la visibilitÃ© :

Ces derniÃ¨res annÃ©es, les cybercriminels sont parvenus Ã pÃ©nÃ©trer les dÃ©fenses de trÃ¨s grandes entreprises malgrÃ© lâ□□utilisation de pare-feu et dâ□□antivirus. Lâ□□ancienneté des systÃ¨mes de dÃ©fense en place, la mauvaise configuration des contrÃ´les de sÃ©curitÃ© et la surabondance de journaux de sÃ©curitÃ© ne permettent pas aux professionnels de protÃ©ger efficacement leur rÃ©seau et de dÃ©tecter les Ã©vÃ©nements rÃ©ellement importants.

WatchGuard prÃ©voit quâ□□en 2014 de plus en plus dâ□□entreprises dÃ©ploieront des outils de visibilitÃ© afin de faciliter lâ□□identification des vulnÃ©rabilitÃ©s et la mise en place de stratÃ©gies de protection renforcÃ©e des donnÃ©es stratÃ©giques.

6. Attaquer la Â« chaÃ®ne de confiance Â» sera une technique de choix pour atteindre les cibles les plus difficiles :

Si les victimes les plus prestigieuses, telles que les administrations ou les entreprises du CAC 40, bÃ©nÃ©ficient dâ□□un dispositif de sÃ©curitÃ© plus important, ce nâ□□est pas pour autant quâ□□elles parviendront Ã arrÃªter les pirates motivÃ©s et patients, qui sâ□□attaqueront au maillon faible de la Â« chaÃ®ne de confiance Â» de lâ□□entreprise : les partenaires et les sous-traitants.

Les cybercriminels les plus douÃ©s visant dÃ©sormais des cibles plus complexes, il faudra sâ□□attendre en 2014 Ã une exploitation grandissante des vulnÃ©rabilitÃ©s de la Â« chaÃ®ne de confiance Â», les pirates sâ□□attaquant aux partenaires pour atteindre lâ□□entreprise.

7. Les attaques deviendront plus nuisibles :

La plupart des cyber-attaques et des logiciels malveillants ne sont pas volontairement destructeurs. En effet, lorsquâ□□un cybercriminel dÃ©truit lâ□□ordinateur de sa victime, il ne peut plus accÃ©der Ã ses ressources. Cependant, lâ□□Ã©volution du profil des pirates fait dÃ©sormais de la cyber-destruction un objectif valable dans un nombre croissant de cas.

Les cybercriminels peuvent Ã©galement se rendre compte que la menace d'une destruction imminente contribue Ã amÃ©liorer les chances de succÃ¨s de l'extorsion, comme le compte Ã rebours utilisÃ© par CryptoLocker pour effrayer les victimes et les amener Ã coopÃ©rer. WatchGuard sâ□□attend ainsi Ã observer une multiplication des vers, chevaux de Troie et virus destructeurs en 2014.

8. De technicien Ã psychologue du cybercrime :

Ces derniÃ¨res annÃ©es, les attaquants avaient clairement lâ□□avantage sur les dÃ©fenseurs, sâ□□appuyant sur des tactiques dâ□□esquive et des techniques plus sophistiquÃ©es pour pÃ©nÃ©trer des dÃ©fenses vieillissantes.

Cependant, le vent est en train de tourner. En 2014, les dÃ©fenseurs accÃ¨deront plus facilement aux solutions de sÃ©curitÃ© de nouvelle gÃ©nÃ©ration et aux fonctionnalitÃ©s de protection avancÃ©e, rÃ©Ã©quilibrant le rapport de force.

Mais les cybercriminels nâ□□abandonneront pas facilement la partie. On peut sâ□□attendre Ã une Ã©volution de leur stratÃ©gie, qui sera sans doute moins focalisÃ©e sur lâ□□avantage technique et plus sur les faiblesses de la nature humaine.

En 2014, attendez-vous Ã ce que les attaquants privilÃ©gient la psychologie Ã la technologie, en sâ□□appuyant sur la culture populaire et sur diffÃ©rentes techniques (emails dâ□□hameÃ§onnage convaincants, par exemple) pour cibler le maillon le plus faible de la chaÃ®ne : lâ□□utilisateur.