Fuites subies par Anthem : une attaque lente et silencieuse

L'attaque menée contre Anthem, le second plus grand assureur aux États-Unis dans le domaine de la santé, qui a exposé les données personnelles identifiables de dizaines de millions d'assurés, n'était probablement pas un simple raid rapide mais plutôt un détournement continu et discret d'informations sur une période de plusieurs mois. L'attaque était conçue pour ne pas être détectée par les équipes informatiques et de sécurité de l'entreprise, et reposait sur un mécanisme d'infection par bot pour exfiltrer les données, explique Thierry Karsenti, Directeur Technique Europe de Check Point Software Technologies. Voici son analyse.

Selon les déclarations d'Anthem, les premiers signes de l'attaque sont apparus au milieu de la semaine dernière, lorsqu'un administrateur informatique a remarqué qu'une requête de base de données était exécutée à l'aide de son identifiant sans qu'il ne l'ait déclenchée. L'entreprise a déterminé qu'une attaque avait eu lieu, a informé le FBI et a engagé un consultant externe pour mener une enquête de sécurité.

Les enquêteurs ont constaté qu'un logiciel malveillant personnalisé a été utilisé pour infiltrer les réseaux d'Anthem et dérober des données. Le type exact de logiciel malveillant n'a pas été communiqué, mais il semble être une variante d'une famille connue d'outils de piratage. Un rapport de sécurité indépendant signale que l'attaque a pu commencer trois mois auparavant. Le consultant a remarqué une « activité de type botnet » dans des entreprises affiliées à Anthem en novembre 2014.
Ce n'est pas surprenant car les activités de bot à long terme sont courantes dans les entreprises. Le Rapport Sécurité 2014 de Check Point, basé sur la surveillance d'événements dans plus de 10 000 entreprises dans le monde entier, a constaté qu'au moins un bot a été détecté dans 73% des entreprises, contre 63% l'année précédente. 77% des bots étaient actifs pendant plus de quatre semaines, et communiquaient généralement avec leur « centre de commande et de contrôle » toutes les trois minutes.
Les bots sont capables d'échapper à toute détection car leurs développeurs utilisent des outils d'offuscation pour leur permettre de contourner les solutions antimalwares traditionnelles reposant sur des signatures. En tant que tel, l'émulation des menaces, également appelée « émulation en bac à sable », devrait être utilisée comme couche de défense supplémentaire pour stopper les bots avant qu'ils n'infectent les réseaux. Des solutions antibots devraient également être déployées pour faciliter la découverte des bots, et empêcher d'autres fuites en bloquant leurs communications.
Il est également important que les entreprises segmentent leur réseau, en séparant chaque segment par des couches de sécurité pour empêcher les infections de bot largement répandues. La segmentation peut restreindre les infections à une zone particulière du réseau pour atténuer les risques et empêcher les infections d'accéder à des données confidentielles dans d'autres segments du réseau.
Avec ces trois approches préventives, les entreprises peuvent réduire considérablement leur exposition au type d'attaque lente et furtive qui semble avoir frappé Anthem, et éviter de devenir la victime de fuites à grande échelle.

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

Source : http://www.itrmanager.com/articles/154049/fuites-subies-anthem-attaque-lente-silencieuse.html