Projet oThSec

Apprend à me protéger du risque des attaques sur Internet !

Déc 2017

Samuel LEPETRE

Contexte fraude

Risques des attaques (hacking) liés à Internet en hausse

Les cas de fraudes sur Internet explosent

Généralisation du Web/Cloud

Les solutions Cloud se généralisent augmentant les flux Internet

Pas d'intelligence

L'absence d'un contrôle intelligent des flux entre son PC/Smartphone et Internet.

Les systèmes existants ne suffisent plus à protéger des nouvelles formes d'attaques

Enjeux

Renforcer la sécurité

Géolocaliser et mesurer le risque en temps réel des flux Internet et afficher une carte de l'exposition sur Internet

Améliorer la lutte contre le Hack

Réaliser un modèle de détection d'intrusions réseau afin de protéger les ordinateurs contre les activités malveillantes (signaux faibles). Construire un modèle prédictif capable de différentier les bonnes (normales) des mauvaises connexions (attaques ou intrusions)

Objectif

Gains estimés

sur une estimation (impossible à chiffrer, 1 exemple - source Equifax – 145M d'américains touchés par le piratage) de fraudes sur Internet, il est prévu de détecter 1% des flux suspects.

Dès 2018 :

- 10000 IP blacklistés
- 100 zones géographiques blacklistées
- 10 comportements blacklistés
- ...

Système oThSec temps réel

Exemple d’un simple ordinateur laissé connecté sur internet via une Freebox qui affiche 41 attaques de type SSHD après 10 jours

POC disponible à l’@ :

https://beewoo.ddns.net/TrackR

Références

- Les tentatives de phishing sont détectées par **GreatHorn** (2015, $8,83M)
- Lookout (2007, $282M) sécurise les mobiles avec un modèle prédictif.
- Les malwares sont détectés avec du machine learning par **Cylance** (2012, $177M)
- L'israélien **DeepInstinct** (2014, $32M) protège les systèmes contre les failles de sécurité récentes ("zero day threats"). Ce serait la première startup à exploiter le deep learning – avec des GPU Nvidia – tandis que la plupart utilisaient du machine learning jusqu'à présent pour faire de l'analyse multifactorielle des menaces en lieu et place de l'utilisation de bases de signatures de virus.
- **Recorded Future** (2009, $33M) utilise le machine learning pour détecter les menaces de sécurité en temps réel
- Des startups comme **Onfido** (2012, $30M) vérifient l'identité de clients de service en ligne. C'est de la détection de fraude basée sur du machine learning et du prédictif
- L'israélien **Fortscale** (2012, $32M) identifie de son côté les menaces internes dans les entreprises, avec sa solution User & Entity Behavioral Analytics (UEBA). Il a détecter des comportements suspects comme la copie de fichiers de grande taille sur des clés USB ! Dans les pays où ce genre de surveillance est autorisée !"

Conclusion

- Se protéger contre des flux Internet risqués. La protection intelligente des SI est l'une des plus grandes occupations des entreprises aujourd'hui
- Rendre intelligent la lutte contre la fraude sur Internet
- 1 plateforme BigData Machine Learning (fouille de données complexes)
- 6 mois pour un POC
- 1 équipe de 4 personnes profil IT
- POC basé sur les données http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html proposant un type de données normales et 24 types d'attaques différentes classées en 4 catégories DoS, Probe, U2R et R2L