Masterproef industriële ingenieurswetenschappen 2019-2020

Het gebruik van machine learning voor het detecteren en genereren van DGA-domeinnamen

Denzel Vanrompay

Master industriële ingenieurswetenschappen elektronica-ICT

PROBLEEMSTELLING

INTRODUCTIE

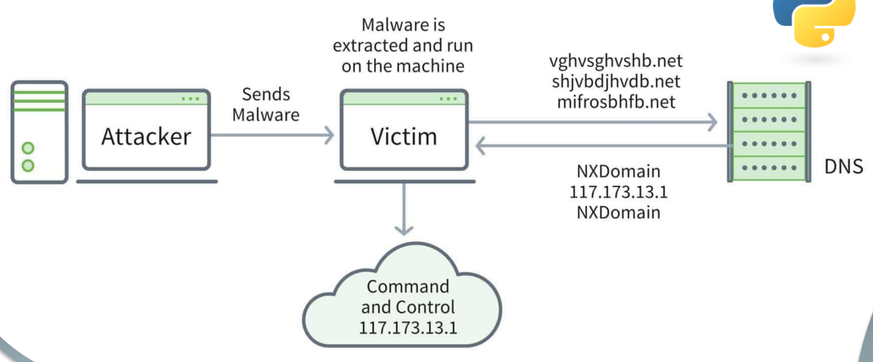
Een Domain Generation Algorithm (DGA) wordt gebruikt door malware. Een DGA genereert honderden of duizenden domeinnamen waarvan de aanvaller er maar enkele registreert om verbinding te kunnen maken met de Command & Control (C&C) server van de aanvaller. Een C&C server kan gebruikt worden door een aanvaller voor het aansturen van een botnet.

- **DETECTEREN**

Machine learning-model trainen om door DGA gegenereerde domeinnamen te detecteren via Splunk.

- **GENEREREN**

Opzetten van machine learning om domeinnamen te genereren die detectiesystemen proberen te ontwijken.



[1] - Een voorbeeld van hoe DGA gegevens van een doelwit exfiltreert

MATERIAAL & METHODE

- **DETECTEREN**

In Splunk met Machine Learning ToolKit (MLTK) een detectiesysteem opzetten waarin de passivedns index wordt ingeladen en er een classificatie gebeurt op basis van de domeinnaam. Een dashboard voor aanpassen van vals positieven is voorzien.

- **GENEREREN**

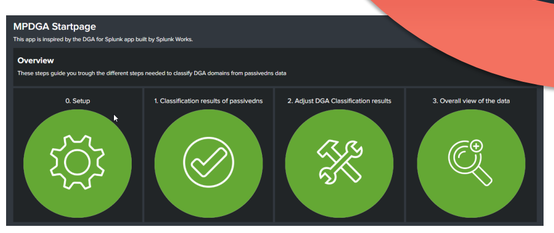
Opzetten van een Generative Adversarial Network (GAN) voor het genereren van DGA-domeinnamen met behulp van Python en Anaconda Spyder.

Het GAN gebruikt verschillende functies uit de TensorFlow-gpu bibliotheek voor Python. Deze bibliotheek wordt ondersteund door NVIDIA CUDA en cuDNN.

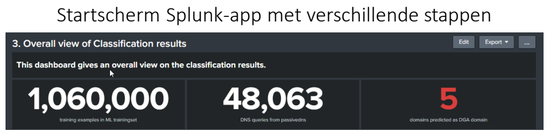
RESULTATEN

- **DETECTEREN**

Voor detectie werd een app in Splunk ontwikkeld. Deze app laat toe een passivedns log in te laden en hierop een analyse te maken. Random Forest is het algoritme achter deze classificatie. Meerdere stappen gebouwd voor setup, analyse, bijsturen van vals positieven en een algemeen overzicht van de data.



Startscherm Splunk-app met verschillende stappen



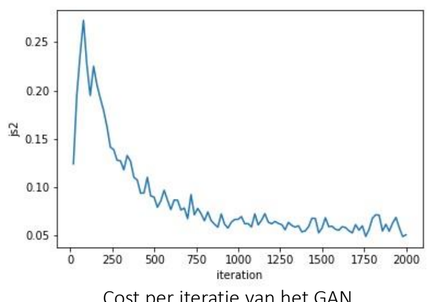
Overzichtsdashboard met algemene analyseinformatie

Classificatieresultaten	Predicted dga	Predicted legit
dga	56575 (94,3%)	3425 (5,7%)
legit	3385 (5,6%)	56615 (94,4%)

Confusion matrix voor Random Forest classificatie

- **GENEREREN**

Het GAN werd ingesteld om 2000 iteraties uit te voeren voor het genereren van DGA-domeinnamen. Deze domeinnamen werden niet gedetecteerd door het detectiesysteem. Na voldoende training op dit type gaf dit een recall van 89,5%.



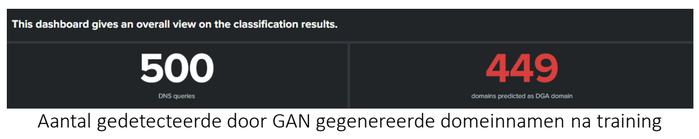
Cost per iteratie van het GAN

CONCLUSIE

- **DETECTEREN**

Detectie van DGA-domeinnamen met behulp van machine learning werkt vrij goed maar is niet foutloos. Ongeziene types kunnen moeilijk gedetecteerd worden waardoor het model hertraint moet worden op nieuwe types. Het zal daarom eerder een ondersteunende rol hebben waar manuele bijsturingen van vals positieven en vals negatieven indien gekend nodig zijn in plaats van het systeem autonoom te laten werken.

- **GENEREREN**



Aantal gedetecteerde door GAN gegenereerde domeinnamen na training

DGA-domeinnamen genereren met een GAN is zeker mogelijk maar zeer rekenintensief. De lijst kan ook ingebouwd worden in malware om zo synchrone lijsten te gebruiken. Random extensie wordt achteraf toegevoegd.

20 iteraties	mx	0e	te	t9
100 iteraties	tooooooo	aotootooioo	oottotto	ootototooo
500 iteraties	unaores	bamtbo	itscas	tapubics
2000 iteraties	buhetorn.sa	teikrotoge.pe	papnimor.me	camustoc.tg

Voorbeeld van opbouw domeinnamen door GAN telkens na aantal iteraties

Promotoren / Copromotoren: Andy Geraerts, Cegeka

ing. Frank Appaerts, UHasselt

[1] - https://www.exabeam.com/information-security/domain-generation-algorithm-t1483-mitre-attck-framework/

cegeka IN CLOSE COOPERATION

UHASSELT

KU LEUVEN