Malware Classification with Machine Learning

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Dr. Endre Bangerter, Jonas Wagner
Experte: Armin Blum

Massive Malware- und Hackerangriffe gehören mittlerweile zur Tagesordnung. Solche Angriffe verursachen finanzielle und ideelle Schäden in Milliardenhöhe. Da sich Malware ständig weiterentwickeln, können in der Erkennung und Bekämpfung dieser Angriffe neue Techniken von Nutzen sein: zum Beispiel die Malware Klassifizierung mittels Machine Learning.

Relevanz

Staaten, Unternehmen und Einzelpersonen wollen sich vor diesen Angriffen und den daraus resultierenden Schäden schützen. Dies kann unter anderem durch die Analyse der Malware geschehen: so wird sie erkannt, klassifiziert und entsprechende Schutzmassnahmen können getroffen werden. Für solche Analysen sind Experten mit viel Erfahrung und Know-how notwendig. Pro Tag erscheint aber eine Unmenge an neuen Malware-Dateien. Im 2017 waren es zwischen 285'000 und 360'000 pro Tag. Meist sind es zwar nur kleine Modifikationen zu früheren Versionen, jedoch macht diese immense Anzahl eine Automatisierung der Analyse zwingend. Machine Learning kann bei Klassifizierungsaufgaben sehr effizient und effektiv sein und selbst mit grossen Datenmengen umgehen. Daher bietet es sich an, Malware-Klassifizierung mit Machine Learning zu automatisieren.

Hintergrund

Es werden die dynamische und die statische Analyse unterschieden, um aus der Malware Informationen zu gewinnen. Bei der dynamischen Analyse wird die Malware in einer sicheren Umgebung ausgeführt.
Es werden dabei alle Aktivitäten aufgezeichnet, um Rückschlüsse auf das Verhalten der Malware und die Absicht des Angreifers zu gewinnen. Diese Analyse liefert gute Resultate, ist aber selbst mit Automatismen zeit- und ressourcenaufwendig und für die tägliche Verarbeitung von hunderttausenden von Exemplaren nur sehr teuer realisierbar.
Bei der statischen Analyse wird mit der Malware-Datei an sich gearbeitet, ohne sie auszuführen. Dabei werden Strings oder Ressourcen wie Bilder ausgelesen oder der Maschinen Code in den für Menschen lesbaren Quellcode übersetzt. Diese Prozesse sind weniger aufwendig als die der dynamischen Analyse und selbst bei vielen Dateien effizient. Wird bei der Malware-Datei den Code verschleiert indem es verschlüsselt wird, kann dieser Ansatz aber auch an seine Grenzen kommen.
Um der täglichen Flut an Malware-Dateien Herr zu werden und die wenigen Experten zu unterstützen, sollten beide Ansätze automatisiert und kombiniert werden. Die statische Analyse wird verwendet, um schnell eine Vielzahl an Dateien zu klassifizieren. Diejenigen Dateien, welche bei dieser Analyse nicht genügend sicher einer Klasse zugeordnet werden konnten, werden dann mit der dynamischen Analyse genauer untersucht.

Ziele

Im Rahmen dieser Arbeit soll nun die Klassifizierung basierend auf Attribute der statischen Analyse automatisiert werden. Mussten vorher diese Attribute von Hand interpretiert und analysiert werden, übernimmt das nun ein Machine Learning Algorithmus. Dieser Algorithmus erstellt mit den Daten ein Modell, welches die verschiedenen Malware-Dateien unterscheiden kann.
Es soll dabei untersucht werden, wie effektiv und effizient der Machine Learning Ansatz im Kontext der Malware Klassifizierung funktioniert und welche Vor- und Nachteile daraus resultieren. Ausserdem soll geklärt werden, welche Attribute einer Malware-Datei sich besonders für den Machine Learning Ansatz eignen und in welchen Fällen und warum Machine Learning an seine Grenzen kommt.

Resultate

Während der Arbeit wurden gut 200'000 Samples von rund 80 verschiedenen Malware-Familien analysiert. Die Ergebnisse zeigen auf, dass sich Machine Learning gut für die Malware-Klassifikation eignet. Es wurde eine Genauigkeit von 94.3% erreicht.
Die Extraktion der Attribute aus den Samples gelingt in nützlicher Frist. Das Trainieren des Modells und der Klassifizierung der Samples kann in wenigen Minuten durchgeführt werden. Somit kann die Anzahl, welche durch die dynamische Analyse untersucht werden sollte, auf einen Bruchteil reduziert werden. Dies betrifft insbesondere Malware-Familien, die sich an Verschleierungstechniken bedienen.
Dieser Ansatz der Malware-Klassifizierung mit Machine Learning kann somit als Teilstück einer umfassenden Malware Analyse und Klassifikationsumgebung eingesetzt werden.

Matthias Frederic Sidler