Malware classification based on network protocol similarities

Studiengang: BSc in Informatik | Vertiefung: IT Security
Betreuer: Prof. Dr. Endre Bangerter
Experte: Andreas Fischer
Industriepartner: Threatray, Biel

Schadsoftware oder sogenannte Malware verursacht jährlich einen weltweiten Schaden von mehreren Milliarden Franken. Damit sich die Betroffenen gegenüber dieser Flut von Malware zur Wehr setzen können, ist es wichtig die entsprechende Malware zu klassifizieren. Durch gute Klassifizierung der Malware können resultierende Risiken abgeschätzt und entsprechende Abwehr-Massnahmen getroffen werden!

Vorgehensweise

In dieser Arbeit wurde ein System entwickelt, um eine Klassifikation der Malware anhand ihrer Netzwerkkommunikation zu erreichen. Es wurde eine virtualisierte LAB-Umgebung aufgebaut, welche die einzelnen Malwaresamples automatisiert abspielt und deren Netzwerkverkehr aufzeichnet. Diese Lab-Umgebung erlaubt Masssubmissions von Malwaresamples. Dabei wird ein TLS Interceptor eingesetzt, damit die verschlüsselte TLS Kommunikation entschlüsselt werden kann. Um die Effizienz bei der Prüfung der einzelnen Netzwerkaufzeichnungen zu verbessern und zusätzliche sogenannte False Positive zu vermeiden, werden die „known good“ Traffic Elemente aus den Netzwerkaufzeichnungen gefiltert.

Die Klassifikation anhand des Netzwerktraffics der einzelnen Aufzeichnungen erfolgt sowohl automatisiert durch statische Suricata Regeln, wie auch mittels Machine Learning (ML). Suricata ist ein open source Network Intrusion Detection System. Die Auswertung durch Suricata wurde mit dem ETOpen Regelset und mit einem Set aus selbst erstellten Regeln vorgenommen. Bei der Klassifikation durch ML wurden verschiedene ML Algorithmen getestet und geeignete Features ermittelt. Abschliessend wurden die Resultate der einzelnen Klassifikationsmethoden verglichen um zu bestimmen, welche Klassifikationsmethode die besten Resultate erzielen konnte und um die unterschiedlichen Stärken dieser Methoden zu zeigen.

Resultate

Im Rahmen dieser Arbeit wurden insgesamt 6878 Malware Samples, aus 10 verschiedenen Malware-Familien, über eine Dauer von 3 Minuten auf der virtuellen Umgebung abgespielt und deren Netzwerktraffic aufgezeichnet. Das ergibt eine Aufzeichnungsdauer von 20634 Minuten oder 343.9 Stunden beziehungsweise etwas über 14 Tage. Nach dem Studieren vieler dieser Aufzeichnungen (PCAP-Dateien) konnten die „known good“ Traffic-Pakete isoliert und herausgefiltert werden. Dabei haben 4884 PCAP-Files keine Malwaretraffic verursacht. Die restlichen 1994 Aufzeichnungen bestehend aus 8 Malware-Familien haben insgesamt 2‘791‘822 Pakete gesendet und 3‘145‘333 Pakete empfangen, welche zur Klassifikation verwendet werden konnten.

Eine erste Prüfung mit Suricata und dem ETOpen Regelset fiel mit einer Klassifikation von 19% relativ schlecht aus. Nach dem Analysieren des gefilterten Traffics und dem Schreiben eigener Suricata Regeln, lag das Resultat bei 76,5% und in Kombination mit dem ETOpen Regelset sogar bei 81,5% richtig klassifizierter Malware Samples. Anschliessend wurden die PCAP-Dateien geparst und Features extrahiert um mittels supervised ML eine Klassifikation der Samples vorzunehmen. Bereits mit wenigen Features konnten gute Resultate erzielt werden. Die finale korrekte Klassifikationsrate durch die ML Methode lag bei 97,29%.

Der Vergleich dieser Methoden zeigt, dass der Einsatz von ML zum Erkennen von Malware-Familien mittels Netzwerktrafficanalyse sehr gute Resultate liefert. Die Machine Learning Methode konnte im Vergleich zur Suricata Methode mehr Malware-Samples richtig klassifizieren, wobei Suricata den Vorteil einer beinahe perfekten Präzision ihrer Klassifikation bietet.

Das Ergänzen weiterer Malware-Familien wäre mit der ML Methode wesentlich einfacher als mit Suricata. Im Gegensatz zu den individuell pro Malware-Familie definierten Regeln von Suricata, sind die gewählten Features der ML Methode für jede Malware-Familie gleich. Zudem zeigen die Experimente, dass durch ML im Gegensatz zu Suricata auch eine Klassifikation ohne TLS Interception möglich wäre.

Patrick Sandro Wyss