Analyse von Infostealer und Trojaner

Studiengang: MAS Information Technology

Diese Masterarbeit befasst sich mit der Analyse von Infostealer und Trojaner Malware, die als Bedrohungen in der digitalen Welt auftreten. Der Fokus liegt darauf, ein tiefgreifendes Verständnis dieser Bedrohungen zu erlangen und effektive Strategien für ihre Erkennung zu entwickeln, um die digitale Sicherheit zu verbessern.

Ausgangslage

In der aktuellen digitalen Welt sind Infostealer und Trojaner Malware eine präsente Bedrohung für alle Nutzer des Internets. Durch die bekanntesten Attacken wie Phishing-Mails (Malspam) oder unkontrolliertes Installieren von Dateien gelangen solche Malware Samples auf die Computer von Privatpersonen sowie auch Institutionen. Ein Schutz vor solchen Angriffen kann auf mehreren Ebenen geschehen, beispielsweise durch Sensibilisierung der Personen oder technische Massnahmen. Damit vor allem Letzteres umgesetzt werden kann, ist es notwendig ein tiefgreifendes Verständnis für Funktions- und Verhaltensmuster von Malwarearten zu erlangen.

Zielsetzung

Das Ziel dieser Thesis ist, die am weit verbreitetsten Malwarefamilien in den Kategorien Infostealer und Trojaner zu evaluieren, ihre spezifischen Merkmale und Verhaltensweisen durch statische und dynamische Analysen zu identifizieren. Ausserdem sollen spezifische Gegenmassnahmen in Form von zwei unterschiedlichen technischen Lösungen entwickelt und verifiziert werden. Die erste Lösung ist die Erkennung und Klassifizierung von Schadsoftware durch vorgegebene Signaturen und Bedingungen. Die Zweite ist eine netzwerkbasierte Schutzmassnahme, die Netzwerkpakete erfasst und sie auf vorgegebene Signaturen nach schädlichen Aktivitäten untersucht, um mögliche Netzwerkangriffe zu detektieren.

Ergebnisse

Die Malwarefamilien AgentTesla, RedlineStealer und Formbook wurden als die aktuell verbreitetsten Infostealer und Trojaner Malware evaluiert. Die Analyse dieser drei Malwarefamilien lieferte Erkenntnisse ihrer Verhaltens- und Funktionsmuster, was Unterschiede in ihren Techniken offenbart. Es wurde festgestellt, dass Formbook und AgentTesla einen ähnlichen .Net Dropper nutzen, welcher mehrere Stufen nutzt, um den schlussendlichen Payload zu laden. Die Payloads von AgentTesla und RedlineStealer basieren auf .NET-Code, während Formbook eine Assembler Payload nutzt, was die Komplexität dieser Malwarefamilien unterstreicht. Die Aktivitäten der unterschiedlichen Malwarefamilien zeigt, dass RedlineStealer einfach strukturierte Aktionen durchführt, währenddem AgentTesla bereits komplexere Aktivitäten entfaltet und Formbook die komplexesten und am stärksten verschachtelten Aktivitäten aufweist. Diese Beobachtungen sind besonders relevant für die Entwicklung von Schutzmassnahmen, da sie aufzeigen, wie unterschiedlich die Malwarefamilien agieren. Alle drei Malwarefamilien exfiltrieren Zugangsdaten von Webbrowsern und Mail Applikationen. RedlineStealer hat zusätzlich das Ziel, Kryptowallets, spezifische Dateitypen sowie Informationen wie Sprache, Region oder installierte Programme von infizierten Systemen an den C2 Server zu senden. In Bezug auf die C2 Kommunikation stellte sich heraus, dass RedlineStealer unverschlüsselte Verbindungen und Daten nutzt, was die Analyse vereinfacht. AgentTesla hingegen verschlüsselt seine Verbindungen und kodiert die exfiltrierten Daten in Base64. Bei Formbook sind die Verbindungen nicht verschlüsselt, jedoch sind die übertragen Daten Base64 kodiert und RC4 verschlüsselt. Zudem setzt er zur Erschwerung der Erkennung der richtigen C2 Kommunikation auf eine gewisse Anzahl von Decoy Hosts.

RedlineStealer und AgentTesla können mit in dieser Arbeit entwickelten Yara und Suricata Regeln erfolgreich identifiziert werden. Für die Malwarefamilie Formbook wurde nur einer Suricata Regel erfolgreich umgesetzt. Die Implementierung der Yara Regel erfordert umfassendes Reverse Engineering der Malware, was über die Fähigkeiten der angewandten Analysemethoden hinausging. Die erstellten Schutzmassnahmen erkennen nicht nur die analysierten Malware Samples, sondern auch weitere Samples, die zu diesen Malwarefamilien verbreitet sind.

Jan Nadler
MAS Information Technology