Alexander Josef Steiner

Sacha von Känel

Graduate Candidates	Alexander Josef Steiner, Sacha von Känel
Examiner	Ivan Bütler
Co-Advisor	Dr. Benjamin Fehrensen, Group Security Services UBS AG, Zürich, ZH
Subject Area	Security

MITB - Man in the Browser

Introduction: As security measures in web technologies improve, hackers responded with a highly specialised "Man in the Browser" attack. An attacker may intercept and modify e-business transactions or use the victim's application on behalf of the victim's by infecting the victim browser with such malware. TLS/SSL does not protect, as the malware intercepts prior to network encryption.

The "Man in the Browser" attack is hardly detectable by web application firewalls. There is no distinguishing characteristic between the intruder and the victim, as the IP address or browser UserAgent, since the malware runs on the victim's computer.

A fully working prototype of an E-Banking "Man in the Browser" attack was developed to raise awareness and elaborate future defence strategies.

Approach: In the first stage of the project, the team analysed different techniques to hook and remotely control the victim browser. As the malware must not require local admin privileges, the team decided to implement a Google Chrome Extension. The installation of the malware is not part of the project. Second, several open-source C2 Frameworks (Command & Control Frameworks) were analysed, and Mythics has been chosen for this work. The combination of the Google Chrome Extension, remotely controlled by Mythics C2 framework was then tested against two E-banking systems. Furthermore, the report outlines essential defence strategies and mitigation techniques against this kind of attack.

Result: As a result of this project, a Google Chrome Extension, named Areion, was developed. Areion is a remote-controlled application supporting the C2 framework Mythic. It is fully extendable and allows users to add modules for specific websites dynamically. Two e-banking modules were developed, and Areion was extensively tested against these websites as part of the project. From the knowledge gained, the team created security measures to protect one's websites against this form of attack. The results will be showcased at the two banks, and our knowledge hopefully will improve the overall security of their e-banking system.