Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

# Security Training- und Testing Framework: Konfigurations- und Kampagnenmanagement

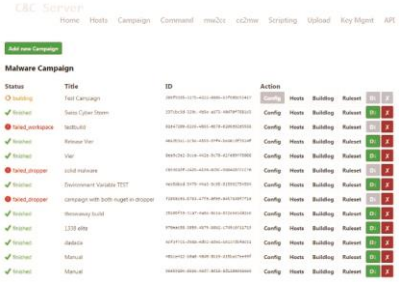
Für eine praxisnahe Ausbildung im Bereich Malware braucht es realitätsnahe und an das jeweilige Ausbildungsziel anpassbare Schadprogramme. Das InIT in Zusammenarbeit mit der Security Competence GmbH hat zu diesem Zweck ein Framework entwickelt. Um die Malware des InIT einzusetzen, muss diese, Kenntnisse des Quellcodes vorausgesetzt, auf einem entsprechend eingerichteten Entwicklungssystem erstellt werden. Die Distribution der Malware ist somit zeitaufwändig und fehleranfällig. Das Hauptziel dieser Bachelorarbeit besteht darin, die Konfiguration und das Deployment der Malware für verschiedene Einsatzszenarien weitgehend zu automatisieren und als komfortables Webinterface bereitzustellen.

Im Rahmen dieser Arbeit wurde ein Distributionsystem für Malware, bestehend aus einem Command-and-Control-Server mit Kampagnenverwaltung und einem Dropper, konzipiert und implementiert. Der bestehende Command-and-Control-Server wurde um ein Webinterface zur Kampagnenverwaltung erweitert, durch das die Malware-Konfiguration benutzerfreundlich vorgenommen werden kann. Ein neu entwickeltes, automatisiertes Buildsystem kompiliert die Malware passend zur per Webinterface spezifizierten Konfiguration. Ausgehend von einem manuell platzierten Dropper kann damit auf einem System die dafür vorgesehene Malware geladen, installiert und gestartet werden. Mittels einem per GUI konfigurierbaren Filter kann zudem sichergestellt werden, dass Malware nur an Systeme ausgeliefert wird, die bestimmte Bedingungen erfüllen, z.B. nur an Systeme in einem bestimmten Netzwerk oder an Systeme, die ein bestimmtes Softwarepaket installiert haben.

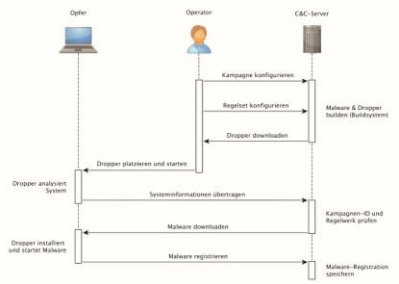
Durch die neu entwickelten Softwarekomponenten konnte der Prozess des Malware-Deployments massgeblich vereinfacht und beschleunigt werden. Das geschaffene Distributionssystem ermöglicht neu auch den Einsatz des Frameworks durch Betreuer, die keine Programmiererfahrung mitbringen und ohne aufwändige Installation einer Softwareentwicklungsumgebung.

Diplomierende
Simon Aebersold
Florian Gehring

Dozent
Bernhard Tellenbach


Übersichtsseite der Kampagnenverwaltung mit Statusinformationen zum Build-Prozess




Malware-Deployment Prozess (vereinfacht)