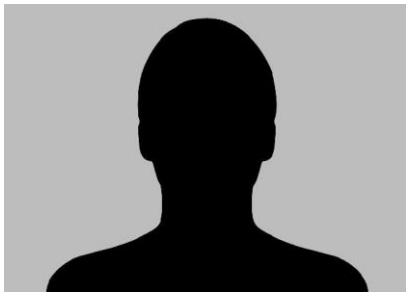
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

Persistenztechniken von Malware

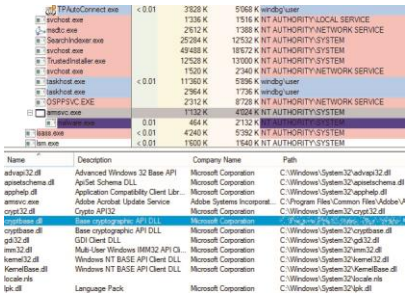
Das Aushorchen und gegebenenfalls Beeinflussen und Stören von hochrangigen Zielen wie Betreiber von kritischen Infrastrukturen, Regierungsstellen oder Industriekonzernen durch hochentwickelte Malware, sogenannte Advanced Persistent Threads, ist spätestens nach der NSA-Affäre bestätigt und wird als reales Szenario angesehen. Damit solche für spezifische Ziele professionell entwickelte Malware-Systeme identifiziert, analysiert und abgewehrt werden können, müssen entsprechende Fachkräfte ausgebildet werden.
Um die Ausbildung möglichst praxisnah zu gestalten, entwickelte das InIT in Zusammenarbeit mit der Security Competence GmbH ein Multi-Purpose APT Malware Framework, das konfigurierbare, synthetische Malware für verschiedene Sicherheitsszenarien in Trainingsumgebungen erstellen kann. Eine der dem Framework noch fehlenden elementaren Fähigkeiten von APT Malware ist das Entfernen oder Deaktivieren der Malware mittels Persistenzmechanismen zu erschweren oder zu verhindern. Eine weitere Fähigkeit ist die Aufteilung der Malware in einen mit normalen Benutzerrechten funktionierenden Teil und einen Teil mit erhöhten Rechten.
Diese Arbeit präsentiert Lösungen und deren Integration in das Framework für beide dieser noch fehlenden Fähigkeiten. Für die Persistenz ist dies ein neu entwickeltes, intelligentes Auswahlverfahren, das unter anderem auch Systeminformationen wie die installierten Softwarepakete ausliest, um für die jeweilige Systemkonfiguration geeignete Mechanismen zu installieren und zu verwalten. Für die Aufteilung der Malware ist dies ein neues Modularisierungskonzept und ein Konzept und Protokoll für die Kommunikation zwischen den beiden Teilen. Eine Analyse verschiedener Persistenzmechanismen auf Eigenschaften wie Detektierbarkeit oder der Komplexität der Umsetzung, liefert zudem sowohl die Grundlage für die Selektion der ins Framework eingebauten Mechanismen als auch Einsichten in was heute bezüglich Persistenz machbar ist.
Eine Prüfung der Sichtbarkeit der integrierten Persistenzmechanismen mit hierauf spezialisierter Tools wie HijackThis am realen System zeigt, dass es je nach verwendetem Mechanismus zumindest eine Herausforderung sein kann, die Malware auf diesem Weg zu finden.



Diplomierende
Daniel Jampen
Simon Lukes

Dozent
Bernhard Tellenbach

Code Injection in Dropbox.exe als Malware Persistenzmechanismus.



Durch ausnützen von DLL Search Order Hijacking mit erhöhter Berechtigung gestartete Malware Instanz auf einem infizierten System.