Evaluation von OS X AV Produkten

Fachgebiet: Informatik
Betreuer: Dr. Endre Bangerter
Experte: Dr. Igor Metz (Glue Software Engineering AG)
Industriepartner: Compass Security Schweiz AG, Jona

Das Betriebssystem OS X hat in den letzten Jahren einen bedeutenden Aufschwung erlebt und bietet dadurch zunehmend ein attraktiveres Ziel für Cyberkriminelle. Damit die Sicherheit des Systems gewährleistet ist, wird eine effektive AV-Lösung benötigt. Es stellt sich die Frage, wie effizient aktuelle OS X AV-Produkte diese Aufgabe bewältigen. Unsere Resultate zeigen, dass die getesteten Produkte ein grosses Defizit im Bereich der Detektion unbekannter Malware aufweisen.

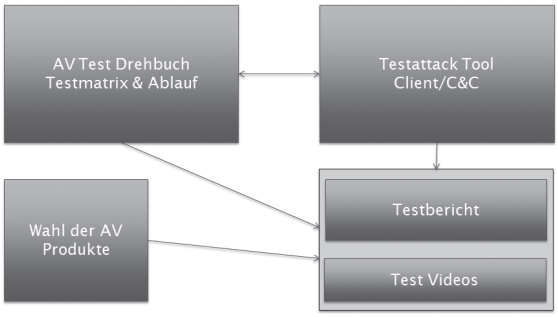
AV-Produkte verfügen über Techniken, verschiedene Arten von Malware aufzuspüren, zu blockieren und unschädlich zu machen. Dabei prüfen sie Dateien gegen bekannte Malware Signaturen, die im Voraus erstellt sein müssen. Nebst der Malware, welche AV-Unternehmen bereits analysiert haben, gibt es immer wieder neue Abwandlungen bekannter Schadprogramme und auch Neuentwicklungen. Diese Programme können nicht durch eine Signaturenprüfung erkannt werden. Um auch unbekannte Malware zu erkennen, wenden die AV-Hersteller sogenannte heuristische Analysen an.

Unter OS X sind uns keine Untersuchungen zur heuristischen Detektion von Malware bekannt. Somit können wir nicht beurteilen, ob und in welchem Ausmass ein OS X System mit installierter AV-Software vor unbekannter Malware geschützt ist.

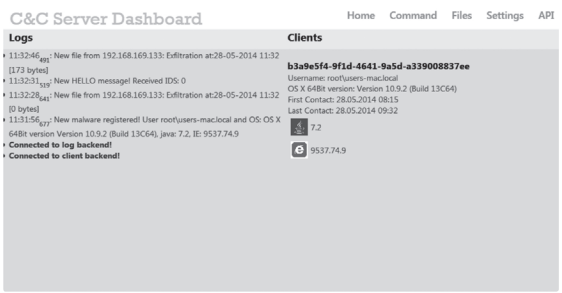
Mithilfe eines selbst entwickelten Testattack-Tools (TaT) testen wir die Fähigkeiten einer AV-Software, neue, unbekannte Bedrohungen mittels heuristischer Analyse zu erkennen. Das Testattack-Tool ist modular aufgebaut, so dass wir in den AV-Tests beliebige Kombinationen von Funktionen gegen AV-Produkte testen können. Der TaT Client verübt auf dem Testsystem sicherheitskritische Funktionen und sendet Resultate an den Command & Control Server, welcher die Steuerung des TaT ausserhalb des Testnetzwerkes ermöglicht. Durch definierte Drehbücher, bestehend aus TaT-Konfigurationen und exakt definierten Abläufen, testen wir die anhand ihres Funktionsumfangs ausgewählten AV-Produkte in einer einheitlichen Testumgebung.
Der Test hat gezeigt, dass die OS X AV-Produkte in der Detektion von unbekannter Malware noch ein grosses Defizit aufweisen. Keines der getesteten Produkte erkennt das Testattack-Tool als Bedrohung. Jedoch muss erwähnt werden, dass die integrierten Firewalls die Netzwerkkommunikation des TaT teilweise unterbinden konnten, sofern diese nicht getarnt war. Um sich effektiv gegen unbekannte und bekannte Schadprogramme zu schützen, ist es sinnvoll, sich nicht nur auf die Zuverlässigkeit eines AV-Produkts zu verlassen, sondern vor allem auch einen aufmerksamen und skeptischen Umgang im Internet zu pflegen. Durch wohlüberlegtes Surfen lassen sich sehr viele Infektionen vermeiden.

Stefan Schmid

Adrian Schwendimann



Grafische Veranschaulichung des Testkonzepts



Webinterface des Command & Control Servers mit Log Nachrichten eines Clients