Malware Demonstration Framework

Fachgebiet: Informatik
Betreuer: Dr. Endre Bangerter, Dominic Fischer
Experte: Dr. Igor Metz

Computer, Smartphones und Tables finden im Privatleben wie auch in Firmen immer neue Einsatzgebiete und sind aus unserem Leben kaum mehr wegzudenken. Wir setzen unser Vertrauen vermehrt in diese Technologien, dabei wird leicht vergessen, welche Risiken das Computerzeitalter mit sich bringt. In unserer Bachelorarbeit zeigen wir Angriffe mit dem Fokus auf das Zusammenspiel von Windows- und Androidmalware auf. Der Kern dieser Arbeit ist die Demonstration eines Malwareangriffes auf E- Banking Systeme, welche mTAN einsetzen.

Ausgangslage

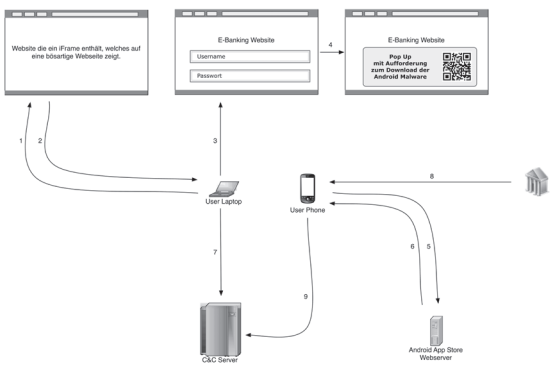
Heute sind einige Finanzinstitute auf das mTAN Verfahren umgestiegen, andere möchten dies in nächster Zeit noch nachholen. Das Verfahren ist jedoch nicht sicher genug. Die Beweise für einen Angriff halten sich in Grenzen. Lange existierten sie nur in der Theorie.

Ziel

Durch die gewonnen Erkenntnissen in den Bereichen E-Banking, mTAN und den beiden Betriebssystemen Windows und Android, haben wir uns das Ziel gesetzt, ein praxisnahes Demonstration Framework aufzubauen. Der Kern unserer Arbeit liegt eindeutig beim Aufzeigen der Unsicherheit von mTAN Verfahren.

Resultat

Das Malware Demonstration Framework beinhaltet nebst dem Angriff auf mTAN Systeme auch eine PC-Standalone Variante mit sich. Diese zeigt auf, wie Malware, insbesondere der Zeus-Bot funktioniert und wie er zu steuern ist. Zusätzlich haben wir in einer Papierstudie das Thema rund um die Sicherheit mobiler Geräte auf einer konzeptionellen Ebene untersucht.



Ablauf

Aus Platzgründen gehen wir hier nur auf die Kern-Demonstration unserer Arbeit ein.

Die angefügte Abbildung zeigt den Ablauf der Demonstration. Durch einen Besuch einer legitimen Seite (1) gelangt mittels einer «Drive-By-Infection» (2) Malware auf den Rechner des Opfers. Diese Malware gibt dem Angreifer Kontrolle über das System und manipuliert die E-Banking-Login Seite.

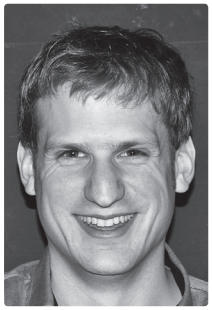
Ruft der Benutzer nun die E-Banking Seite auf (3), so wird ein zusätzliches Pop-Up eingeblendet (4), welches den Nutzer auffordert, ein «Sicherheitsapp» auf seinem Android Smartphone zu installieren. Kommt der Benutzer dieser Aufforderung nach (5), so wird die mobile Malware auf dessen Smartphone geladen (6) und durch den Benutzer installiert.

Die vorher eingegeben Daten (3) werden in regelmässigen Abständen an den C&C Server weitergeleitet (7). So ist der Angreifer nun im Besitz des Benutzernamen und des Passwortes.

Schickt die Bank nun eine zusätzliche Authentisierungsnummer in Form einer mTAN per SMS (8), bleibt diese dem Benutzer verborgen und wird stattdessen an den C&C Server geleitet (9).

Der Angreifer hat nun alle nötigen Informationen, um sich auf dem E-Banking System des Opfers einzuloggen und Zahlungen von dessen Konto zu tätigen.

Damit hätten wir aufgezeigt, dass das mTAN Verfahren als zweiter Authentisierungskanal zu unsicher ist und man besser auf andere Systeme setzt, welche ausgereifter sind.



Silas Bärtsch

Cyril Imadjane