ZeuS-Trojaner zielt auf mobileTAN ab: Variante des ZITMO-Trojaners für Volks- und Raiffeisenbanken im Umlauf

Eine Variante des ZeuS/ZITMO-Trojaners ist inzwischen auch für Volks- und Raiffeisenbanken im Umlauf. Ziel ist es, neben dem PC auch das Smartphone zu infizieren und somit die Sicherheit der zwei Kanäle und damit der mobileTAN auszuhebeln.

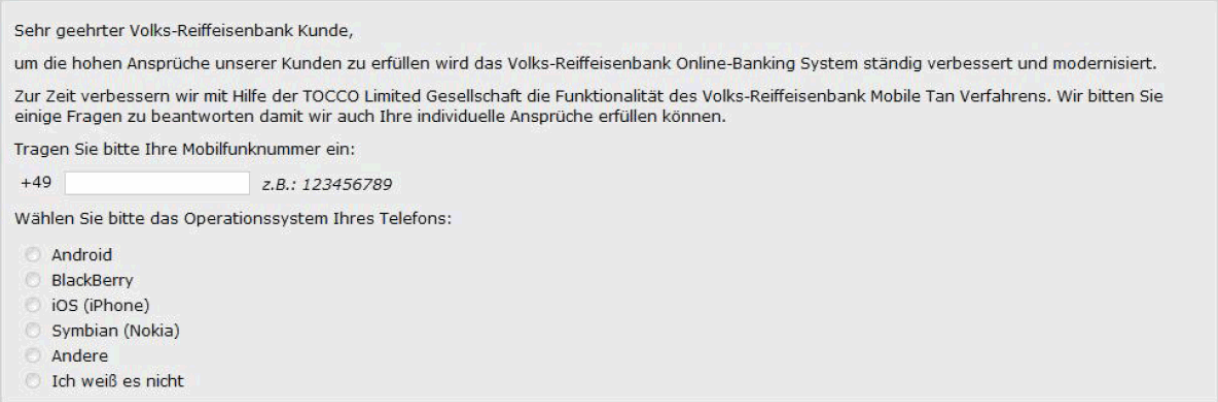
Ist der PC eines Benutzers mit dem eBanking-Trojaner ZeuS infiziert erscheint nach der Anmeldung am Online-Banking unter einem "Vorwand" (z.B. zur Verbesserung der Sicherheit oder Qualität) eine Abfrage von Handynummer und Smartphone-Betriebsystems ab:

- Gibt der Benutzer die Daten ein erhält er eine SMS mit Download-Link.
- Folgt er diesem Link und bestätigt anschließend die Software-Installation (Malware) infiziert er sein Smartphone, das mobileTAN-Verfahren ist ausgeheblt.

Die Kombination aus Trojaner, der den PC befällt (z. B. ZeuS), und anschließendem Social Engineering-Angriff zur Infektion des Smartphones(z. B. ZITMO) wurde bereits 2010 beobachtet. Damals wurden die Betrugsversuche primär außerhalb Deutschlands unternommen, beispielsweise in Spanien.

Inzwischen sind neben anderen deutschen Banken auch die Online-Banking-Seiten von Volks- und Raiffeisenbanken Ziel der Angreifer. Zu erfolgreichen Angriffen auf Kunden von Volks- und Raiffeisenbanken liegen uns bisher keine Informationen vor.

Nach der Anmeldung am eBanking von einem mit entsprechender Schadsoftware infizierten PC aus wird vom Trojaner (Man-in-the-Browser-Angriff) folgende Abfrage eingeblendet:



Gibt der Benutzer die Daten ein, bekommt er eine SMS auf sein Smartphone gesendet, in der ein Downloadlink zu angeblicher Sicherheitssoftware / Verschlüsselungssoftware hinterlegt ist:

Tatsächlich handelt es sich aber hier um den Schadcode zum Übernehmen des Smartphones. Ein infiziertes Smartphone meldet dies per SMS an den Angreifer. Ab diesem Zeitpunkt stehen sowohl der PC als auch das Smartphone unter Kontrolle des Angreifers. Dadurch ist neben dem PC auch der zweite Kanal kompromittiert - die Vertraulichkeit der übertragenen mobileTAN ist nicht mehr gesichert.

Nach unseren Informationen funktionieren die Angriffe derzeit nur für Blackberry und Geräte mit Android. Smartphones mit dem Google-Betriebssystem Android geben zusätzlich beim Installieren des Schadcodes eine Warnmeldung aus, da die Software nicht aus dem Google Appstore stammt.

Es ist aber damit zu rechnen, dass künftig auch weitere Smartphone-Betriebssysteme wie iOS betroffen sein werden. Auch sind Varianten bei der Formulierung und ein besseres Deutsch jederzeit möglich und zu erwarten.