Volksbank-Phishing-Mails zur Verbreitung von Malware im Umlauf

Aktuell werden Phishing-Mails (Spam) im Namen der Volksbanken versendet. Ziel ist es, über eine in der Mailverlinkte Webseite per Driveby-Download Banking-Trojaner zu verbreiten.

Die E-Mails haben Betreffzeilen wie "950.00 Euro werden von Ihrem Konto in VOLKSBANK in 24 Stunden abgeschrieben" oder "Abschreibung von 950.00 Euro von Ihrem Bankkonto in VOLKSBANK" und weisen sprachliche Mängel auf.

In den Mails ist ein Link auf Schadsoftware enthalten (blauer Text im Screenshotunten).
Bitte klicken Sie keinesfalls auf einen solchen Link!

Die E-Mails zielen darauf ab, den Kunden unter dem Vorwand einer angeblich geplanten Abbuchung von seinem Konto zum Aufruf einer Web-Seite zu bewegen. Dort wird versucht, den betroffenen PC unter Ausnutzung von Sicherheitslücken miteinem Trojaner zu infizieren (Drive-by-Download):

- Der Trojaner späht zum einen die Anmeldedaten zum Internet-Banking aus und blendet zum anderen eine Meldung über eine vermeintliche "Sicherheitskontrolle" zur Untersuchung des PCs auf Schwachstellen im Browser ein. Zum Abschluss der vermeintlichen Untersuchung fordert der Trojaner den Kunden in einer Meldung auf, zur "Vollendung der Überprüfungsprozedur" eine Überweisung mit einer TAN zu bestätigen.

- Bei dem Trojaner handelt es sich um eine neue Variante der Banking-Trojaner-Familie Anserin (alias Torpig oder Sinowal).

- Zur Infektion wird ein sog. Web-Infection-Toolkit namens "Blackhole" genutzt, welches diverse Schwachstellen in Browsern,Browser-Plugins sowie weiterer Software ausnutzt.

Alle aktuell bekannten und beworbenen Phishing-Sites finden Sie im Security Portal unter:

https://www.itsec.fiducia.de/background/phishing/site_suche/request.php

Folgend sehen Sie eine exemplarische Mail: