

## NEUER SCHADCODE: BANK-TROJANER FÄLSCHT KONTOAUSZÜGE

Die Sicherheitsexperten des Anbieters Finjan haben einen Trojaner identifiziert der sich nicht nur mit dem Anwender in einen Online-Banking-Account schleicht, sondern auch gleich noch dessen Umsätze fälscht, damit der Diebstahl nicht sofort bemerkt wird.

Der Schädling wird URLzone genannt und kann gut rechnen. Wird er eines Kontos habhaft, dann kalkuliert er durch wie hoch der Dispo ist und wie viel Geld sich auf dem Konto befindet, um dann den maximalen Betrag abbuchen zu können.

Der Trojaner hatte einige Kunden von verschiedenen deutschen Banken im Visier. Die Namen der Banken teilte Finjan indes nicht mit.

Inzwischen, so Finjan, seien die deutschen Behörden informiert.

Finjan spricht jetzt von einem Trojaner der nächsten Generation. Infiziert wurden die Rechner über eine Webseite. Rund 90.000 Nutzer besuchten diese Seite und etwa 6400 von ihnen wurden infiziert. Bei einigen Hundert Banknutzern wurde dann tatsächlich Geld gestohlen. Die Sicherheitsexperten von Finjan schätzen den Schaden auf etwa 438.000 Dollar.

Die Schadsoftware wurde über Mail, über Links in Webseiten oder über manipulierte Webseiten über ein Leck, das in den wichtigsten Browsern vorhanden ist, verbreitet. Dann schlummert der Trojaner vor sich hin. Erst wenn das Opfer eine bestimmte Bankseite, PayPal, Facebook oder Google Mail aufruft, wird der Schadcode aktiv.

Der Trojaner loggt sich dann mit dem Nutzer in seinen Online-Banking-Account ein. Dann wird kalkuliert, wie viel Geld von dem Konto abgehoben werden kann, ohne dass es ein spezielles Programm gestartet wird, das eine Notbremse zieht, wenn das Konto leer geräumt wird. Danach überweist der Trojaner den ausgerechneten Betrag, ohne dass der Nutzer das merkt. Denn der Trojaner schickt Anfragen an die Bank und bekommt Antworten, die vom Browser aber nicht dargestellt werden.

Das Geld wird dann an den Account einer dritten Person überwiesen. Der Trojaner aber manipuliert die Seite, auf der die Kontobewegungen dargestellt werden. Zu sehen ist da der Betrag, den der Anwender erwarten würde. Den tatsächlichen Kontostand sieht er erst dann, wenn er ihn mit einem Rechner betrachtet, der nicht von dem Trojaner befallen ist, natürlich auf dem Ausdruck von der Bank, am Automaten, oder wenn eine Überweisung mit dem Hinweis abgelehnt wird, dass das Limit bereits überschritten sei.

Für die Forscher ist es das erste Mal, dass ein Schädling in Echtzeit in der Lage ist, dem Opfer falsche Bankdaten vorzugaukeln.

Sichern Sie Ihr Netzwerk und Ihre PCs vor Schadcode durch eine zentrale Sicherheitslösung direkt am Internet-Anschluß, lassen Sie Viren und Trojaner erst gar nicht in Ihr Netzwerk.