

Modifizierter BKA-Trojaner im Umlauf

Ein aktuell im Umlauf befindlicher Trojaner sperrt infizierte Rechner angeblich im Namen der GVV und des BSI. Der Trojaner ist eine Variante des bekannten BKA-Trojaners, der Benutzern vorgaukelt, dass der Computer vom BKA untersucht worden sei und aufgrund illegaler Downloads gesperrt werde, bis ein Bußgeld bezahlt werde. Im vorliegenden Fall sollen die Benutzer 50 Euro bezahlen.

Der Trojaner gibt vor, dass der PC im Auftrag der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. (GVV) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) gesperrt werde, da sich Raubkopien auf dem Rechner befänden. Der Benutzer wird aufgefordert, mittels Paysafe*-Guthabekarten 50 Euro zu bezahlen, danach werde der Rechner wieder freigeschaltet.

Nach Recherchen von heise.de und Auskunft der GVV erfolgt auch nach Bezahlen der 50 Euro kein "Freischalten" des Rechners. Statt dessen wird der Benutzer aufgefordert, die Festplatte auszubauen und mit einem externen Virenschanner zu prüfen. Nach Meinung der Experten wird der Trojaner hiermit wahrscheinlich jedoch nicht rückstandslos vom infizierten Computer befreit, da der Trojaner sich entsprechend im System verankert.

Von der Zahlung der 50 Euro wird ausdrücklich abgeraten. Betroffene sollten ihr System entweder neu aufsetzen oder sich über die Webseite BKA-Trojaner.de informieren, wie die jeweilige Variante des Schädlings komplett vom Computer gelöscht werden kann.

*) Eine Paysafecard ist vergleichbar mit einer Prepaid-Karte. Man erwirbt das Guthaben beispielsweise an einer Tankstelle, bei einem Discounter oder bei der Post. Das Guthaben ist mit einer 16-stelligen PIN verknüpft, welche man beim Bezahlvorgang, beispielsweise in einem Online-Shop, angibt. Dieser Vorgang ist schwerer zurück zu verfolgen als beispielsweise eine Überweisung.

Quelle: heise.de