Was tun bei einer Infektion durch den BKA-Trojaner?

Vorbeugung und Schutz – Eine aktuelle Avira Information

Inhalt:

1. Potenzielle Gefahr und Übertragungswege

Angriffe durch den BKA-Trojaner haben sich in Europa zu einer wachsenden Bedrohung ausgeweitet, nicht zuletzt, weil der Einsatz dieser Malware für seine Autoren höchst rentabel ist und enorme Profite verspricht. Vor diesem Hintergrund ist ein Wettstreit zwischen Antivirensoftware-Herstellern und Malwareautoren in Bezug auf Erkennung bzw. Nicht-Erkennung entbrannt. Die Malwareschreiber versuchen permanent, die Erkennungen durch neue Varianten „zu durchbrechen" – und somit wird die Malware für den Kunden wieder potenziell gefährlich.

Zumeist infizieren sich die betroffenen Kunden über zwei Wege: Einmal durch das Besuchen einer unseriösen bzw. illegalen Website wie zum Beispiel Filmstreaming-Websites oder sog. Warez-Websites. Hier wird die Malware mittels einer Sicherheitslücke in einer Werbe-Einblendung heruntergeladen und ausgeführt. Die wechselnden Werbe-Einblendungen werden zufällig angezeigt. Somit wird nicht jeder Besucher einer entsprechenden Webseite mit der Malware infiziert, sondern die Infektion erfolgt lediglich dann, wenn der Malware-Werbebanner mit der entsprechenden Sicherheitslücke in diesem Augenblick dargestellt wird.

Die weitere Möglichkeit ist eine Infektion über boshafte Dateianhänge von Spam-Mails, dem sogenannten Rechnungstrojaner. Durch das Öffnen und Ausführen dieser Anhänge, welche sich gern als PDF oder Word-Dokument tarnen, installiert sich die Malware und sorgt dafür, dass der Computer Bestandteil eines Bot-Netzwerks wird. Wenn dies geschieht, verbindet sich die Malware direkt zu einem Server, von welchem sie nun bestimmte Befehle entgegennimmt.

Dies versetzt sie in die Lage, weitere Spam-Emails zu verschicken, neue Malware nachzuladen oder die Routine des BKA-Trojaners mit dem bekannten Lockscreen auszuführen.

Zum Schutz vor dem BKA-Trojaner ist die Aktualität der installierten Software wichtig, ebenso wie eine aktuelle Avira Installation.

2. Schutz durch Avira Produkte

Avira ist in der Lage, den infizierten Computer automatisch zu bereinigen. Dazu muss gewährleistet sein, dass der Kunde die aktuellste Virendefinitionsdatei (VDF) und Engine installiert hat. Startet der Kunde den Computer im abgesicherten Modus, kann er über das Avira Center einen vollständigen Systemscan starten und die Malware entfernen lassen.

3. Lösung durch Avira Rescue CD

Eine weitere Möglichkeit, die Malwaredatei/en auf dem infizierten Computer zu löschen, bietet die Avira Rescue CD. Diese kann der Kunde kostenfrei von der Avira Webseite laden und sich automatisiert eine Boot-CD erstellen lassen. Die auf der Webseite angebotene Rescue CD enthält immer die aktuellste Virenerkennung von Avira. Nach dem Neustart des Rechners muss der Kunde ggf. noch die Bootreihenfolge seines Computers ändern. Zu finden ist die aktuellste Version auf der Homepage von Avira: http://www.avira.com/de/downloads#tools

4. Vorbeugung vor weiteren BKA-Trojaner-Angriffen

Um den Computer vor weiteren Infizierungen zu schützen, müssen alle verfügbaren Sicherheitsupdates des Betriebssystems sowie die Updates des Browsers und des Avira Produkts installiert sein. Ebenso sollte die Software für Adobe Flash-Plugins und PDF-Reader immer auf dem aktuellsten Stand sein.

Für das Surfen im Internet sollte ein sicherer Browser wie *Google Chrome* oder *Mozilla Firefox* verwendet werden. Ebenfalls empfehlen wir einen Blocker für unnötige Werbungeinblendungen und Skripte wie zum Beispiel das bekannte Plugin „Adblock plus“, das als Add-on zu installieren ist.

Avira GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de