SUCHMASCHINE TUNINGEN

Informationen und Bilder aus Tuningen

10. Jahrgang | Schwarzwald-Baar-Kreis

Kategorie: Kriminalität | Datum: Samstag, 26. Oktober 2013 | Artikel: Cookies/Trojaner

Verteilung von Schadprogrammen über Werbebanner

Einschleusung von Trojanern durch Akzeptieren von Cookies?

Um die epaper-Ausgabe einer regionalen Tageszeitung lesen zu können, müssen Cookies akzeptiert werden, sobald man die Cookies aktiviert hat und die Anmeldung erfolgt ist, meldet der auf dem Rechner installierte Virenscanner einen Trojaner. Ohne eine aktuelle Internet Security Software sollte ein durch Cookies unterstützer Login somit nicht mehr erfolgen.

Tuningen. (ms) Online-Kriminelle kompromittieren dabei in grossem Umfang OpenX-Server bei der Auslieferung von Werbebannern, darauf wies schon im Januar 2013 das BSI (Bundesamt für Sicherheit in der Informationstechnik) hin. Dies ist kein Einzelproblem der hiesigen Regionalzeitung, viele deutschsprachige Webseiten wie Nachrichten-, Politik-, Lifestyle- und Fachmagazine sowie Tageszeitungen, Flirt- und Partnerbörsen sind betroffen. Für eine Infektion eines Windows-Rechners reicht schon der Besuch der Webseite mit manipulierten Werbebannern aus, ein Anklicken von Werbung ist dabei nicht nötig.

Ad Server

Dabei wird versucht, die Trojaner über einen Ad Server einzuschleussen. Der AdServer regelt und protokolliert die Einblendung, Auswertung und Abrechnung der Werbebanner (Webmaster-Vermarkterabrechnung).

HEUR:Trojan-Downloader.Script.Generic

Wichtig: Die Heuristik vermutet einen Virus auf der Seite der aufgerufenen Regionalzeitung bzw. beim entsprechenden Werbeanbieter. Vorerst ist nur diese Seite betroffen, nicht ihr Rechner!

Ob ohne einen aktuellen Virenscanner auf ihrem Rechner, ein entsprechender z.B. Online-Banking Trojaner auf ihrem System installiert würde ist nicht bekannt, da der Scanner einen Virus vermutet und diesen blockieren würde.

Künstliche Intelligenz

Bei der künstlichen Intelligenz, der Heuristik-Technologie wird aufgrund von existierenden Viren auf noch nicht existierende Viren geschlossen und bei einer entsprechenden Ähnlichkeit das entsprechende Objekt als vertrauensunwürdig eingestuft, auch wenn es vertrauenswürdig ist.

Tipp

Löschen sie z.B. in Firefox über Chronik - **Neueste Chronik löschen**, den aktuellen Browser Cache. Wir empfehlen auf jeden Fall auch alle Cookies nach dem Besuch der entsprechenden Seite(n) zu löschen. In Firefox über Einstellungen - Datenschutz - Cookies anzeigen - **Alle Cookies löschen.**

Onlinewerbung

Mit der Onlinewerbung werden Milliarden verdient, durch die akzeptierten Cookies wird jeder Klick analysiert und die bei ihnen auftauchende Werbung personalisiert. Wenn Sie sich zum Beispiel bei einem sehr bekannten Onlineversand für ein entsprechendes Produkt interessieren, ist es sehr gut möglich - dass sie dieses oder ein ähnliches Produkt als hochformatige Werbefläche neben einem redaktionellen Content am rechten Rand der Website der Regionalzeitung wiederfinden (Skyscraper-Werbebanner).

PopUnder Werbefenster

Die besagte Online-Ausgabe der Regionalzeitung verwendet auch sogenannte PopUnder, dabei öffnet sich ein Fenster mit Werbung und versteckt sich sofort hinter dem gerade geöffneten Browserfenster des Nutzers. Nach dem schliessen des aktuellen Browserfensters wird das Werbefenster dann erst sichtbar, viele wundern sich woher dieses Fenster herkam.

MP NEWMEDIA GmbH in Stuttgart

Der User kann normalerweise die Ursprungsseite der Werbung nicht nachvollziehen, da nur die URL des AdServers im versteckten Werbefenster angezeigt wird, in unserem Fall war die Ursprungsseite die besagte Regionalzeitung. Die URL im Werbefenster mit www1.mpnrs.com oder auch mp-success.com ist der Ad Server der MP NEWMEDIA GmbH in Stuttgart, mit dem Angebot von Performance Marketing, hier die Onlinekampagne eines Weinversand mit einem 800px x 600px PopUnder (Vicampo.de).