# Rätsel um Infektion zehntausender Webseiten gelöst

**Die Sicherheitsexperten des Internet Storm Center haben das Rätsel gelöst, wie Anfang des Jahres Zehntausende von Webseiten, die anschließend Besuchern Schadcode unterzuschieben versuchten, mit infektiösem Code verseucht werden konnten.**

Anfang des Jahres wurden mehrere tausend harmlose Webseiten manipuliert, um Besucher der Seiten mit Trojanern und anderem Schadcode zu infizieren. Die Sicherheitsexperten des Internet Storm Center (ISC) haben jetzt herausgefunden, wie es zu dieser Masseninfektion kam.

Bei der Untersuchung eines Servers, der schädlichen JavaScript-Code für die Angriffe ausliefert, sind die ISC-Experten auf eine ausführbare Datei gestoßen, mit der sich die Angriffe auf Webseiten durchführen lassen. Das Windows-Werkzeug mit chinesischer Bedienoberfläche sucht mit der Google-Suchmaschine nach verwundbaren Servern und kann dann eine SQL-Injection-Attacke ausführen, die in den aus der Datenbank generierten Webseiten einen iframe einfügt, der den Code zum Angriff auf die Webseitenbesucher nachlädt.

Der voreingestellte iframe in dem Tool enthält denselben Link, der Anfang des Jahres auf zahlreichen der manipulierten Webseiten auftauchte. Die Angriffe scheinen auf den Microsoft-SQL-Server sowie den Internet Information Server zugeschnitten zu sein. Das Werkzeug kontaktiert den Analysen des ISC zufolge vor der Nutzung auch einen weiteren Server in China, um offenbar einen Bezahlvorgang anzustoßen.

Die Analyse des Tools sei jedoch noch nicht vollständig abgeschlossen und werde fortgesetzt. Das ISC rät Webseitenbetreibern, die Sicherheit ihrer Webanwendungen zu überprüfen, da die Angriffe auf Webserver nach wie vor stattfänden. Die Artikel Schwachstellensuche mit Fuzzing oder Grundsicherung für PHP-Software auf heise Security können erste Hilfestellungen und Anregungen zu einer Sicherheitsüberprüfung des eigenen Webauftritts liefern.