PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights August 2015

Frankfurt am Main, 21. September 2015 – Im August 2015 werden das Internetunternehmen Yahoo! und Microsofts Webportal MSN.com Opfer von Malvertising-Attacken. Ebenfalls ins Visier von Hackern geraten das Pentagon und die amerikanische Fluggesellschaft American Airlines Group Inc.

Das Internetunternehmen **Yahoo!** wird Opfer eines Hackerangriffs. Unbekannte Hacker greifen das Netzwerk mit Hilfe einer Malvertising-Attacke an. Bei einer Malvertising-Attacke verbergen sich Schadcodes hinter Werbebannern. Sobald ein solches Banner angeklickt wird, installieren sich die Schadcodes auf dem heimischen Computer. Alternativ wird auf eine Seite weitergeleitet, die den Nutzer dazu auffordert, eine Datei runterzuladen, um einen „sicheren" Zugriff bzw. eine „sichere" Installation auszuführen.

Microsofts Webportal **MSN.com** wird Opfer einer Malvertising-Attacke. Entdeckt wird diese Attacke von Malwarebytes. Es wird davon ausgegangen, dass der Angriff vom gleichen Hacker ausgeführt wurde, der auch Yahoo! angegriffen hat.

Nach Angaben von U.S. Offiziellen wird das **Verteidigungsministerium der USA** von russischen Hackern angegriffen. Der Angriff gilt dem E-Mail-System des Pentagons. Es ist daraufhin zwei Wochen lang down.

Die **American Airlines Group Inc.** mit Sitz in Texas meldet einen Angriff von unbekannten Hackern auf die eigenen Computer. Welche Schäden der Angriff hinterlässt, ist noch unklar.

Die Hacker-Gruppe Emissary Panda Threat Group 3390 spioniert im großen Stil gleich mehrere internationale **Unternehmen und Organisationen** aus. Die Hacker infizieren hierzu Webseiten, die ihrer Meinung nach von potentiellen Mitgliedern des eigentlichen Zielnetzwerks aufgerufen werden könnten. Mehr als hundert Websiten dieser Art, die als „Wasserlöcher" bezeichnet werden, soll die Gruppe entsprechend präpariert haben. Dabei nutzen die Hacker eine seit fast einem Jahr bekannte Java-Sicherheitslücke mit dem Ziel zu „exfiltrieren" und nicht zu infiltrieren, also unbemerkt Informationen herunterzuladen. Es wird vermutet, dass der Angriff aus China stammt. Dafür spricht zumindest die Wahl der Opfer, denn neben Unternehmen aus beinahe jeder Branche werden vor allem auch Organisationen angegriffen, die sich für ethnische Minderheiten in China einsetzen.

Der Online-Service der **Royal Bank of Scotland Group** wird von Hackern mit Hilfe eines DDoS-Angriffs gestört. Der Online-Service ist nicht mehr möglich.

Im Namen #OperationSA und #OpMonsanto stehlen die Hacktivisten von Anonymous mittels einer SQL-Injection die gesamte Datenbase der **staatlichen Behörde für Informationstechnologie der südafrikanischen Regierung**. Die Daten werden im Internet veröffentlicht.

Die Hacktivisten von Anonymous greifen unter dem Namen #OpTaiwan mehrere Webseiten der **Regierung Taiwans** mittels DDoS-Attacken an. Die Seiten sind down.

Der iranische Hacker Mr.Xpr! von der Hacker-Gruppe Iran Hack Security Team greift die **Royale Saudi Air Force** an. Die offizielle Seite der saudi-arabischen Luftwaffe wird dabei defaced.

Der Filehosting-Dienst **GitHub Inc**. mit Sitz in San Francisco, wird von unbekannten Hackern angegriffen. Eine massive DDoS-Attacke zwingt eine Hosting-Seite des webbasierten Filehosting-

Dienstes für Software-Entwicklungsprojekte in die Knie.

Die **NGO Electronic Frontier Foundation (EFF)** ist ins Visier von unbekannten Hackern geraten. Die Targeted Attack wird vom Google Sicherheitsteam bemerkt. Vermutlich wurde versucht, eine Malware zu platzieren.

Der saudische Hacker Cyber of Emotion (@Cyber_Emotion) gibt an, mehr als 24 Seiten der **saudi-arabischen Regierung** defaced zu haben.

Kelvinsecurity AKA KelvinSecTeam hackt die Webseite des **Instituts für wissenschaftliche Forschung der Regierung Venezuelas** mittels SQL-Injection und lässt dabei Benutzernamen und Passwörter von mindestens 60 Mitarbeitern mitgehen.

Malwarebytes entdeckt eine Malvertising-Attacke auf das **Dating Portal PlentyOfFish (POF)**. Wer die Angreifer sind und welche Schäden verursacht wurden, ist unbekannt.

Unbekannten Angreifern gelingt es sich in das System eines Infoscreens an einer Bushaltestelle in der **brasilianischen Stadt Curitiba** zu hacken. Statt Ankunfts- und Abreisezeiten der Busse, werden Hardcore Pornos angezeigt.

Die Hacktivisten vom MexicanH Team greifen das **mexikanische Ministerium für Kommunikation und Transport** an. Die Websiten werden defaced.

Medienkontakt:

QGroup GmbH
Phoenix Haus
Berner Straße 119
60437 Frankfurt am Main
www.qgroup.de/presse

Dirk Kopp
Tel.: +49 69 17 53 63-014
E-Mail: d.kopp@qgroup.de

(4.281 Zeichen)