PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Dezember 2015

Frankfurt am Main, 17. Februar 2016 – Im Dezember geraten laut Association Banks in Singapore etliche Banken des Inselstaates ins Visier von Hackern. Auch mexikanische Drogenkartelle nutzen die Möglichkeiten der Cyberkriminalität immer dreister für ihre Zwecke. Darüber hinaus fallen wieder zahlreiche Kunden- und Nutzerdaten verschiedenster Unternehmen in die Hände von Hackern.

Die **Association of Banks in Singapore (ABS)** informiert ihre Mobile-User darüber, dass eine neue Malware im Umlauf ist, die gezielt sensible Daten wie Kreditkarten-Details und one-time Passwörter (OTPs) im Visier hat. Sowohl Android- als auch iOS-Geräte sind hiervon betroffen.

Der Hacker Ropertus hackt im Juni 2015 die Website der britischen Pub-Kette **JD Wetherspoon**. In einem Interview zu diesem Hack gibt Ropertus keine genauen Details über die verwendete Methode bekannt, sagt aber, es wäre „lachhaft einfach" gewesen und er hätte nicht länger als 15 Minuten dafür gebraucht. Die Datensätze von insgesamt 656.723 Nutzern der Seite stehen seitdem auf einer russischen Datenbörse zum Verkauf.

Anonymous ruft unter dem Hashtag #OpTrump zu Attacken auf die Website **Trump Towers** in New York auf. Daraufhin wird die Seite des weltbekannten Wolkenkratzers in Manhatten per DDosS-Attacken lahmgelegt. Ein Twitter-Account der Gruppierung nennt diese Tat ein „Statement gegen Rassismus und Hass".

Mexikanischen Drogenkartellen gelingt es durch das Senden von unechten GPS-Daten, dem sogenannten „GPS-Spoofing", unbemannte Drohnen des **US Department of Security (DHS) sowie des US Customs and Border Protection (CBP)** zu umgehen. Auf diese Weise passieren sie unentdeckt die amerikanische Grenze. Zahlreiche teure Drohnen mussten daraufhin ausgetauscht werden.

Mittels DNS-Hijackings gelingt es unbekannten Hackern die Besucher der offiziellen Seite der **Universität von Connecticut** auf einen von ihnen kontrollieren Server weiterzuleiten. Dort wird eine als Flash Player Update getarnte Malware zum Download angeboten.

Der Whitehat-Hacker Chris Vickery macht darauf aufmerksam, dass eine Datenbank der **US Voter Registration** mit Wahldaten von 191 Millionen Amerikanern jahrelang ungeschützt verfügbar war. Bisher hat niemand Verantwortung für diesen enormen Leak übernommen. Informationen in der Datenbank weisen auf den Wahlkampagnenservice NationBuilder hin. Dieser weist jedoch jegliche Verantwortung von sich.

Die **Hyatt Hotels Corporation** gibt bekannt, dass kürzlich Malware auf Computern der Hotelgruppe gefunden worden sind, welche das Bezahlsystem der Hyatt-Hotels ausführen. Es sind insgesamt 627 Häuser in über 50 Ländern betroffen.

Dem Hacker Freedom Cry, der Teil des Anonymous R4BIA Kollektivs ist, gelingt es mit Hilfe von Social-Engenieering die Kontrolle über **400 Webseiten** zu erlangen. Die Webseiten zeigen statt ihrer eigenen Inhalte nun eine Pro-Islam-Nachricht. Außerdem ist nicht auszuschließen, dass der Hacker auch die Datenbanken der Webseiten downgeloaded hat.

Die indische Polizei gibt bekannt, dass eine Zahlung, die eigentlich an ein **ungenanntes Unternehmen in Delhi** gerichtet war, an ein mit der Terrormiliz IS in Verbindung stehendes Konto weitergeleitet wurde.

Der Cyberwar zwischen Pakistani und Indern geht in die nächste Runde: Mr. 4nOnymOus (Teil der 034th adr355 Cr3w) defaced die Website des indischen Nachrichtenportals **kasganjilive.in** im Distrikt Kasgani.

Eine DDos-Attacke durch unbekannte Hacker veranlasst **Steam**, eine Internet-Vertriebsplattform für Computerspiele und Software, eine neue Caching-Konfiguration anzuwenden, die sich noch in der Entwicklung befindet. Daher ist diese noch nicht voll funktionstüchtig und veröffentlicht ungewollt Daten von über 34.000 Usern.

Der zu Microsofts Spielkonsole Xbox zugehörige Dienst **Xbox Live** hat über die Weihnachtsfeiertage mit Problemen zu kämpfen. Gleichzeitig twittert die Hacker-Gruppe PhantomSquad, dass sie den kostenpflichtigen Dienst so lange per DDoS-Attacken angreifen werde, bis dieser das eingenommene Geld in Sicherheitsmaßnahmen investiere.

Unbekannte Hacker greifen die Webseiten des Nachrichtensenders **BBC** mittels DDoS-Attacken an. Die Seiten des Senders sind temporär nicht erreichbar. Das löst genervte Reaktionen sowie Spott auf Twitter aus.

Auf dem Twitter Account des WWE-Stars **Jim Ross** erscheint im Dezember 2015 eine Todesanzeige, die angeblich von seiner Familie verfasst worden sein soll. Über 1,3 Millionen Twitter Follower lesen die falsche Todesanzeige. Die Nachricht löst eine Welle der Betroffenheits- und Beileidsbekundungen auf Social-Media-Plattformen aus. Jim Ross muss seinen Account löschen und zumindest temporär auf einen neuen Account ausweichen.

Die Hacker-Gruppe Comcastkids gelingt mit Hilfe von SQL-Injection der Zugriff auf Daten der Website **agpestores.com**. Als Folge dieses Angriffs werden 120.000 Benutzernamen und Passwörter zurückgesetzt.

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

(4.794 Zeichen)