PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Februar 2016

Frankfurt am Main, 23. März 2016 – Im Februar geraten gleich mehrere russische Banken ins Visier von Hackern. Mit Norwegen beschuldigt der erste NATO-Staat die chinesische Regierung offiziell Cyber-Attacken durchzuführen. Angriffe auf Plattformen wie Skype, Spotify, Wordpress, das Linux Mint Forum und die Online-Dating-Plattform mate1.com dienen dagegen in erster Linie des Diebstahls von sensiblen Daten der jeweiligen User.

Die Cyberkriminalitätsabteilung des russischen Innenministeriums gibt bekannt, dass es unbekannten Hackern durch internationale Visa- und MasterCard-Zahlungen bei mehreren **russischen Banken** im Jahr 2015 gelungen ist, eine sehr große Summe Geld zu stehlen. Die Hacker erbeuteten insgesamt 1,5 Milliarden Rubel (ca. 18 Millionen Euro).

General Lt. Morten Haga Lunde, Chef des norwegischen Nachrichtendienstes, beschuldigt die chinesische Regierung offiziell Cyber-Attacken gegen **Norwegen** durchzuführen. Das norwegische Verteidigungsministerium hat sich aus Sicherheitsgründen dagegen entschieden, die Konsequenzen der Hacks zu veröffentlichen. Hackerangriffe aus China sind schon lange die Norm. Mit Norwegen beschuldigt jedoch der erste NATO-Staat öffentlich die chinesische Regierung hinter Cyber-Attacken zu stecken.

Cyclance deckt Details der "Operation Dust Storm" auf, eine über mehrere Jahre durchgeführte Attacke auf **japanische Unternehmen**. Es wird vermutet, dass die unbekannten Hacker mit einer Regierung zusammenarbeiten. Betroffen sind japanische Firmen aus den Bereichen Strom, Öl, Gas, Finanzen, Transport und Bau.

Nutzer von **Skype** bekommen Malvertising angezeigt, die in Verbindung mit der Ransomware Locky steht. Die Hacker nutzen den Angler-Exploit, um unauthorisiert Ransomware auf dem PC der Opfer zu installieren.

Ein unbekannter Hacker behauptet, Zugriff auf die User-Daten der Online-Dating-Seite **Mate1.com** gehabt zu haben. Angeblich wurden über 27 Millionen E-Mail-Adressen sowie die dazugehörigen Passwörter gestohlen und verkauft. Der unbekannte Hacker hat sich im Dark-Web-Forum Hell zum Hack geäußert. Um seine Behauptungen zu beweisen, hat er Redakteuren 500 der gestohlenen User-Daten zur Verfügung gestellt.

Hunderte User-Daten von **Spotify** Premium Nutzern werden veröffentlicht. Es ist nicht das erste Mal, dass Spotify User-Daten geklaut werden. Bereits im November 2015 wurden mehr als Tausend Account-Informationen veröffentlicht.

Snapchat gibt bekannt, dass Gehaltsinformationen von aktuellen und ehemaligen Mitarbeitern gestohlen wurden. Die Hacker gelangen an diese Daten über eine Scam Mail, in der sie sich als CEO von Snapchat ausgeben.

Der Twitter-Account von Beatles-Drummer **Ringo Star** wird von Hacker "af" gehackt. Es werden mehrere Posts mit ironischem Inhalt veröffentlicht. Darüber hinaus wird auch ein Screenshot mit privaten Daten in Umlauf gebracht. Hacker "af" gibt über einen verschlüsselten Chat bekannt, dass er durch einen einfachen Passwort-Reset die Kontrolle über Ringo Stars Twitter-Account übernehmen konnte. Die Antworten zu den mit dem Passwort-Reset verbundenen Sicherheitsfragen waren allesamt auf Facebook zu finden.

Unbekannte Hacker platzieren eine Phishing Version des Darknet Marktplatzes **AlphaBay** im WorldWideWeb. Die Hacker arbeiten mit einer Phishing-Seite, die ähnlich wie das gewöhnliche Login-Seminar aussieht. Gehostet wird diese Seite in Deutschland. Die Phishing-Kampagne richtet sich bewusst gegen Kriminelle, die den Darknet-Schwarzmarkt verwenden.

Chilenische Hacker hacken die E-Mail-Server des **bolivianischen Militärs**. Es gelingt ihnen, E-Mails vom Server der bolivianischen Armee zu downloaden. Einen Teil ihrer Beute veröffentlichen sie im Netz. In einer öffentlichen Stellungnahme nennen die chilenischen Hacker die "wuchernde Korruption" innerhalb der bolivianischen Armee als Grund für den Angriff.

Lokale Medien in China berichten über einen Angriff auf die E-Commerce Website **TaoBao**, die Teil der Alibaba Group ist. Unbekannte Hacker verschaffen sich per Account Hijacking Zugang auf mehr als 20 Millionen aktive Accounts. Der Cloud Service der Alibaba Group ist nur einer von vielen Angriffen auf chinesische Firmen in letzter Zeit. Experten rechnen mit weiter steigenden Angriffszahlen.

Anonymous erbeuten sensible Daten von über 1.000 Mitarbeitern der **südafrikanischen Regierung**. Die Hacker veröffentlichen Namen, Telefonnummer, E-Mail-Adressen und Passwörter der Mitarbeiter. Die #OPAfrica ist eine weitere Hacktivism-Kampagne von Anonymous. Diesmal prangern die Hacker Korruption sowie soziale Ungleichheit in Afrika an.

Zahlreiche Websiten, die das **Content-Management-System WordPress** verwenden, werden gehackt. Über die gehackten WordPress-Websiten wird Ransomware an unwissende User verteilt. Es ist noch immer unklar, über welche Schwachstelle die Hacker Zugang zu den Seiten erlangt haben.

Ein Hacker, der sich "Peace" nennt, behauptet die Daten aller 70.000 User des **Linux Mint Forums** gestohlen zu haben. Darüber hinaus hat der Hacker eine Linux Version mit Backdoor auf der Website zum Download angeboten und sich damit Kontrolle über die Rechner verschafft.

Unter der Parole #OPGreenRights hat Anonymous Italia die Websiten der beiden **italienischen Regionen Apulien und Basilikata** vom Netz genommen. Die Hacker wollen auf diese Weise ihren Unmut über die Teilnahme der beiden italienischen Regionen am Trans Adrianic Pipeline (TAP) Projekt zum Ausdruck bringen.

Qadmon, Teil der Hisbollah, gibt bekannt, die Kontrolle über Überwachungskameras der **israelischen Regierung** erlangt und damit Zugriff auf das Bildmaterial der Kameras in mehreren israelischen Regierungsgebäuden zu haben. Dieser Angriff ist der erste, der vom Hisbollah-nahen Sender al-Manar offiziell bestätigt wird.

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

(5.656 Zeichen)