PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights September 2015

Frankfurt am Main, 21. Oktober 2015 – Im September geraten gleich zwei der wichtigsten italienischen Bankhäuser ins Visier von Hackern. Neben der Regierung der Vereinigten Staaten von Amerika werden auch zahlreiche andere Regierungen und regierungsnahe Institutionen ausspioniert. Ebenfalls Opfer von Hackangriffen werden der Apple App Store, Google Play, die Hilton-Hotelkette und das Wirtschaftsmagazin Forbes.

Mit der **Banca Intensa** und der **Unipol Banca** geraten gleich zwei der wichtigsten Banken Italiens ins Visier von Hackern. Im Namen #OpBankDump stehlen „Ghost Italy", eine in Italien stationierte Celle des Hacker-Kollektivs Anonymous, verschiedene Datenbases der beiden Bankhäuser sowie Informationen zu Partnerunternehmen der Banken.

Trend Micro berichtet von der Operation Iron Tiger, in welcher Hacker im großen Stil die **US-Regierung und verschiedene Firmen**, welche mit dem Verteidigungsapparat zusammenarbeiten, ausspionieren. Dabei werden mehrere Billionen Bytes an Daten gestohlen.

Großbritanniens **National Crime Agency** wird vom Hacker-Kollektiv „Lizard Squad" mit einer DDoS-Attacke angegriffen. Die Seite ist down.

Die Webseiten der **Essex Police**, der **Greater Manchester Police** und des **Manchester Airports** werden von einem Hacker per DDoS-Attacken in die Knie gezwungen. Nach eigenen Angaben übernimmt der Hacker mit dem Twitter-Account @n0w1337 die Verantwortung für diese Attacken.

Die **Regierungen Ägyptens, der Vereinigten Arabischen Emirate und des Yemen** werden scheinbar schon seit Jahren von Hackern ausspioniert. Kaspersky Lab bemerkt eine Hacker-Kampagne der sogenannten „Gaza Cybergang", welche wohl seit 2012 aktiv ist.

Die Hacker-Gruppe Turla, deren Mitglieder unbekannt sind, spionieren seit acht Jahren verschiedene Ziele aus, darunter **Regierungsbehörden, Botschaften, militärische Einrichtungen und bestimmte Industriebetriebe**. Dabei bleiben die Angreifer stets anonym und stehlen vertrauliche Informationen. Sie kapern die Verbindungen von Internet-Satelliten und halten sich im Abdeckungsgebiet des Satelliten auf, damit ihr konkreter Standort und auch ihre Identität nicht mehr nachvollziehbar sind. Es wird jedoch vermutet, dass die Hacker aus dem russischsprachigen Raum stammen und Verbindungen zu Regierungen oder hohen Behörden haben.

Nach Informationen des Telegraph spionieren jihadistische Hacker aus Syrien unbemerkt vom britischen Geheimdienst verschiedene Minister der **britischen Regierung** aus. Dafür hacken sich die Angreifer in die E-Mail-Accounts ihrer Opfer und gelangen so an vertrauliche Informationen.

Experten von FireEye entdecken im September eine Spionage-Kampagne von Hackern aus Nordkorea. Diese nutzen eine Sicherheitslücke, um in das Computersystem der **südkoreanischen Regierung** zu gelangen (Zero-Day-Exploit). Welchen Schaden sie dabei anrichten, ist nicht bekannt.

Das US-amerikanische Investmentunternehmen **Fidelity Group** wird von der Hacker-Gruppe „Hack for Trump" mittels einer SQL-Injection angegriffen. Dabei erbeuten die Angreifer

geheime Firmendaten, mit deren Veröffentlichung sie drohen, sollte nicht ein Lösegeld in Höhe von 30.000 US-Dollar gezahlt werden. Mit dem Lösegeld wollen die Hacker Donald Trump bei seiner Kandidatur für das Präsidentenamt der Vereinigten Staaten von Amerika unterstützen.

Der **Apple App Store** ist in das Visier von unbekannten Hackern geraten. Nachdem die infizierten Apps einer IT-Sicherheitsfirma aufgefallen sind, muss Apple seinen App Store reinigen. Dass gleich mehrere Dutzend infizierte Apps in den App Store gelangen konnten, soll daran liegen, dass die Entwickler eine gefälschte Version von XCode verwendet haben (XcodeGhost). Über diese Software konnte den Entwicklern die Malware untergeschoben werden.

Check Point Software entdeckt eine Malware-infizierte App in Google's Store **Google Play**. Die App tarnt sich als „Brain Test". Es könnten bis zu eine Million Androids betroffen sein. Hinter dem Angriff wird ein chinesischer Hacker vermutet.

Die **Hilton-Hotelkette** ins Visier von unbekannten Hackern geraten. Verschiedene Banken bemerken ein Muster bei Kreditkartenbetrugsfällen, das auf einen Hackerangriff auf die Kassensysteme der Geschenke Shops des Hotelkonzerns hindeutet. Mittlerweile hat die Hotelkette selbst eine Malware in den Systemen eingeräumt. Dabei wurden wohl Kreditkarteninformationen aus dem vergangenen Jahr von Kunden in den USA und Kanada gestohlen. Die betroffenen Hotels befinden sich in New York, Chicago, Honolulu, Las Vegas, Toronto und Miami.

Die Hacker von DDoS for Bitcoins (DD4BC) greifen seit April 2015 **verschiedene Unternehmen und Institutionen** per DDoS-Attacken an. Ziel der Angriffe ist es, Geld zu erpressen.

Das amerikanische Wirtschaftsmagazin **Forbes** wird Opfer einer Malvertising-Attacke. Acht Tage lang läuft eine Malvertising-Kampagne auf der Internetseite der Forbes. Folgen des Angriffs sind ein Imageschaden und nicht weiter benannte Schäden für die Nutzer. Wer das englischsprachige Magazin angegriffen hat, ist nicht bekannt.

Acht offizielle Seiten der **vietnamesischen Regierung** werden von den Hackern AntiSec und HagashTeam defaced. Die Hacker wollen mit diesem Angriff gegen die Zensur der Regierung und Menschenrechtsverletzungen protestieren.

Wie bereits im Juli greift Anonymous auch im September wieder die **kanadische Regierung**. Erbeutet werden High-Level-Dokumente.

Die pakistanischen Hacker Team „Pak Cyber Attacker" defaced zwei Seiten der **Regierung des Bundesstaates Kerela** im Süden Indiens.

Als Antwort auf das Defacement von zwei Seiten der Regierung von Kerela durch pakistanische Hacker, greift die indische Hackergruppe „The Mallu Cyber Soldiers" 46 Seiten der **Regierung Pakistans** an und defaced diese.

Unbekannte Hacker greifen die Seite der **thailändischen Regierung** mit einer DDoS-Attacke an und zwingen so die Server in die Knie.

Ein ähnlicher Malvertising-Angriff wie auf die Dating-Seite PlentyOfFish im August richtet sich diesmal gegen die britische Version von **Match.com** (uk.match.com). Welchen Schaden die unbekannten Hacker dabei verursachen wird nicht bekannt.

Gleich **neun Dating-Webseiten** werden von dem Hacker @smitt3nz mit Hilfe einer SQL-Injection gehackt. Dabei kann er auf insgesamt 7.764 Benutzerdaten zugreifen.

NetPirates hackt die polnische Mode- und Kosmetikwebsite **dresscloud.pl** per SQL-Injection und lässt 5.269 Benutzernamen und Passwörter mitgehen.

Ein unbekannter Hacker ist auf der Online-Glücksspielseite **PokerStars** aktiv. Er cheatet mit Hilfe einer Malware (Win32/Spy.Odlanor) in Online-Spielen. Die Malware erlaubt es dem Hacker, die Karten seiner Gegenspieler einzusehen. Theoretisch kann er so nie verlieren.

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)