PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Januar 2018

Frankfurt am Main, 9. März 2018 – Im Januar werfen die Olympischen Winterspiele bereits ihre Schatten voraus. Sie werden gleich zwei Mal das Ziel von Hackerangriffen. Neben politischen Institutionen werden auch Banken vermehrt Opfer von Cyberkriminalität.

Experten von McAfee haben eine Phishing- und Malware-Kampagne gegen Organisationen aufgedeckt, die Infrastruktur und andere Dienste für die **Olympischen und Paralympischen Winterspiele** in Südkorea bereitstellen. Die Angriffe beginnen mit zielgerichteten E-Mails, die vorgeben von der südkoreanischen Behörde zur Terrorismusabwehr zu stammen.

Russische Hacker aka Fancy Bear zweigen E-Mails von Offiziellen des **Olympischen Komitees** ab. Russland ist von den Spielen in Südkorea ausgeschlossen.

Die berüchtigte Cyberspionage-Gruppe Turla greift gezielt hochrangige **Diplomaten und politische Organisationen in Osteuropa** an. Der in der Vergangenheit erfolgreiche Modus Operandi mit infizierten Flash Player Installern besitzt einen gefährlichen neuen Zusatz: Die Installationsdateien gaukeln Vertrauenswürdigkeit vor, indem sie scheinbar von der offiziellen Webseite des Software-Anbieters Adobe heruntergeladen werden.

Trend Micro berichtet von einem Hackerangriff auf den **US-Senat**. Die Angreifer sollen die berüchtigten russischen Staatshacker Fancy Bear sein. Der Angriff zielte wohl auf Spionage ab.

Trend Micro hat eine neue mobile Malware entdeckt. Das Ziel dieser Malware ist das Abfangen von Banking Informationen. Hierzu werden SMS von **Bankkunden** mitgelesen und auf TANs gewartet. Die Malware mit dem Namen FakeBank hat es auf russische Ziele abgesehen.

Die japanische Kryptogeldbörse **Coincheck** wird Opfer einer schwerwiegenden Hackerattacke. Laut der in Tokio ansässigen Kryptogeldbörse wurden bei dem Hackerangriff 500 Millionen Einheiten der Kryptowährung NEM gestohlen. Was zu dem Zeitpunkt einem Wert von rund 533 Millionen US-Dollar entsprach. Damit ist dieser Angriff der wohl größte Diebstahl im Bereich Kryptowährungen.

Hacker greifen mehrmals das Online-Banking der niederländischen **ING Bank** per DDoS-Attacke an.

Neben der ING Bank werden mit ABN Ambro und Rabobank noch mindestens zwei weitere **niederländische Banken** Opfer von DDoS-Attacken.

Hacker haben die Preise an mehreren **Tankstellen in Russland** manipuliert. Mit einer Malware wurde das entsprechende Programm der Tankstellen gehackt, so dass Kunden bis zu 7 % mehr für ihre Tankfüllung gezahlt haben.

Die neu entdeckte Android-Spyware Skygofree kann Gespräche von **Android-Nutzern** mithören, heimlich Fotos machen und liest sogar bei Whatsapp oder Facebook Messenger mit. Die Malware wurde von Kaspersky Labs Ende 2017 entdeckt. Skygofree kann den Aufenthaltsort des Smartphones mitverfolgen und sie kann sogar die Audio-Aufnahme einschalten.

Kunden des Streaming-Dienstes **Netflix** erhalten täuschend echte Spam-E-Mails von Hackern. Die Phishing-Kampagne zielt auf Kreditkarteninformationen ab.

Persönliche Informationen von **Organspendern in Malaysia** sind öffentlich zugänglich. Im Internet ist eine Liste mit Daten und Informationen von 220.000 Spendern aufgetaucht.

Medienkontakt:

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

Bela Schuster
Tel.: +49 69 17 53 63-078
E-Mail: b.schuster@qgroup.de

(3.053 Zeichen)