

## PRESSEMITTEILUNG

### QGroup präsentiert Best of Hacks: Highlights Oktober 2015

**Frankfurt am Main, 24. November 2015 – Im Oktober werden mit T-Mobile US, Vodafone, CAT Telecom Pcl und TalkTalk gleich vier Telekommunikationsanbieter Opfer von Cyberkriminalität. Zudem geraten Samsungs mobiles Zahlssystem LoopPay sowie einige deutsche Unternehmenswebsites wie ebay.de und t-online.de ins Visier von Hackern.**

Die US-amerikanische Telekom-Tochter **T-Mobile US** gibt bekannt, Opfer einer groß angelegten Cyberattacke geworden zu sein. Eigentlich galt der Angriff dem Dienstleistungs-Partner der Telekom Tochter Experian. Diese testet die Kreditwürdigkeit der Kunden, um präventiv gegen Betrüger vorgehen zu können. Bei dem Angriff werden sensible Informationen von mehr als 15 Millionen T-Mobile Kunden erbeutet – unter anderem Sozialversicherungs-, Führerschein- und Reisepassnummern. Es wird vermutet, dass der Angriff im Auftrag der chinesischen Regierung erfolgt ist.

Der deutsche Telekommunikationsanbieter **Vodafone** informiert 1.827 Kunden darüber, dass unbekannte Hacker sich Zugriff auf ihre Vodafone-Accounts verschafft haben und die Informationen eventuell für kriminelle Handlungen nutzen wollen. Die Daten seien jedoch nicht komprimiert worden.

Im Namen #OpSingleGateway greift Anonymous die Seite der staatlichen Telekommunikationsgesellschaft **CAT Telecom Pcl** ([www.cattelcom.com](http://www.cattelcom.com)) Thailands an. Dabei werden auch Daten gestohlen.

Bereits zum dritten Mal ist der britischen Mobilfunk- und Internetprovider **TalkTalk** in diesem Jahr Opfer einer Cyberattacke geworden. Diesmal sollen ein paar Teenager Daten von bis zu vier Millionen Kunden geraubt haben, welche Namen, Adressen, Kreditkarteninformationen, Geburtsdaten, Telefonnummern, E-Mail Adressen und TalkTalk Kundeninformationen enthalten. Es ist bereits zu Festnahmen durch Scotland Yard gekommen, darunter ein 15-Jähriger aus Nordirland.

**LoopPay**, das neue mobile Zahlungssystem von Samsung, wird Opfer einer Cyberattacke. Die von der chinesischen Regierung beauftragten Hacker sollten wohl die neue Technik ausspähen, die sich hinter LoopPay verbirgt. Daten konnten die Hacker, nach Angaben von Samsung, allerdings nicht stehlen.

Malwarebytes entdeckt eine Malvertising-Kampagne auf verschiedene **deutsche Unternehmenswebsites** darunter auch **eBay.de** und **T-Online.de**. Welche Schäden dabei entstanden sind, ist nicht bekannt.

Die Malvertising-Attacke, die in den vergangenen Monaten schon Yahoo! und eBay getroffen hat, trifft nun die britische Boulevardzeitung **Daily Mail**. Welche Schäden dabei verursacht wurden, ist nicht bekannt.

Ein Teen-Hacker hackt den AOL E-Mail-Account von **John Brennan**, dem Direktor der CIA. Dabei erbeutet der Hacker sensible Dokumente und fängt E-Mails ab.

Als Reaktion auf Angriffe auf indische Webseiten, greift die indische Hackergruppe Hell Shiled Hackers die Seite der **pakistanischen Regierung** an. Die Seite wird defaced.

Um gegen die Politik der eigenen Regierung zu protestieren, defacen zwei brasilianische Hacker

Seiten der **Regierung Brasiliens**.

Nordkoreanische Hacker greifen Server des **Blue House, der Residenz des Staatspräsidenten von Südkorea**, an. Betroffen sind Computer von Mitgliedern der südkoreanischen Legislative. Die Angreifer erbeuten Daten.

Die **ägyptische Regierung** wird Opfer eines Angriffs. Anonymous defaced einige Seiten der Regierung.

Anonymous Lebanon defaced mehrere Seiten der **libanesischen Regierung**.

Der Hacker Amped Attacks greift verschiedene **rassistische Seiten** per DDoS-Attacken an. Darunter sind Seiten des Ku-Klux-Klans, ein Online-Store, die Seite der Westboro Baptist Church und IS-Seiten.

Die Website der Premium-Modemarke **David Jones Limited** wird gehackt. Dabei werden sämtliche Kundendaten gestohlen.

Palästinensische Hacker, die sich selbst Anoncoders nennen, defacen die Webseite von **Radio Tel Aviv**, eines der größten Radiosender Israels. Sie hinterlassen auf der Seite die Nachricht "We are always here to punish you."

Südkorea gibt bekannt, dass Nordkorea im vergangenen Jahr eine Cyberattacke auf das **U-Bahn-System Südkoreas** gestartet hat. Das U-Bahn System wird täglich von Millionen Südkoreanern genutzt.

„Alister Maclin“, ein russischer Hacker, hackt das **Bitcoin-Netzwerk** und erstellt über eine Woche lang Duplikate von Transaktionen.

Nicht zum ersten Mal wird in den USA ein **Straßenverkehrszeichen** gehackt, diesmal in Sacramento. Es zeigt daraufhin entweder keine oder falsche Informationen an.

Laut Trend Micro wird das **internationale Untersuchungsteam von Flug MH17** von Unbekannten gehackt.

In Auckland (Neuseeland) bricht eine Person in ein **Autohaus** ein und hackt einen Jaguar XFR im Wert von 80.000 Pfund, um ihn zu stehlen.

Medienkontakt:

QGroup GmbH  
Phoenix Haus  
Berner Straße 119  
60437 Frankfurt am Main  
[www.qgroup.de/presse](http://www.qgroup.de/presse)

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

(4.534 Zeichen)