PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Juli 2017

Frankfurt am Main, 21. September 2017 – Den größten Coup in Punkto Medienwirksamkeit erlangen im Juli die Hacker des amerikanischen Pay-TV-Senders HBO mit der Vorab-Veröffentlichung der 4. Folge der 7. Staffel von „Game of Thrones". Doch auch zahlreiche Regierungen, Unternehmen und Privatpersonen werden wieder Opfer von Cyberkriminalität.

Der amerikanische Pay-TV-Sender **Home Box Office (HBO)** bestätigt, Opfer einer Cyberattacke geworden zu sein. Die Hacker erbeuten von internen Servern des Senders 1,5 Terabyte Material und stellen eine Lösegeldforderung in Millionenhöhe. Kurz darauf stellt die Erpressergruppe, die sich „Mr. Smith" nennt, vorab die 4. Folge der 7. Staffel von „Game of Thrones" online. Neben der Veröffentlichung weiterer Folgen und Drehbücher der Erfolgsserie sowie anderer Serien drohen sie mit der Veröffentlichung von Informationen über Verträge, personelle Ressourcen, Geschäfts- und Marketingstrategien, IT-Infrastrukturen, Film- und Serienproduktionen, internen Briefen, vertraulichen E-Mails und Beweisen für Steuerflucht. Teile des Materials schicken die Cyberkriminellen an die Presse.

Informationen von knapp 40 Millionen **US-Wählern** stehen in einem Untergrund-Forum zum Verkauf. Ein Szenario, das von vielen Experten vorhergesagt wurde und nun Realität geworden ist. Die Informationen über Wähler aus acht verschiedenen Bundesstaaten beinhalten volle Namen, Wähler IDs, Adressen und die Information, welche Partei die Person gewählt hat.

Trend Micro berichtet von einer groß angelegten Cyberspionage-Kampagne der mit dem Iran in Verbindung gebrachten Gruppe CopyKittens. Die Kampagne richtet sich gegen **verschiedene Regierungen**, darunter auch die Deutschlands, Israels, Saudi-Arabiens, Jordaniens und die der Türkei.

Securworks berichtet von einer Cyber-Kampagne, die sich gegen hohe Funktionäre **saudi-arabischer Organisationen** richtet. Die Mitglieder der Gruppe CobaltGipsy, die mit der iranischen Regierung in Verbindung gebracht wird, geben sich im Internet als junge attraktive Frauen aus, um das Vertrauen ihrer Opfer zu gewinnen und sie so auf mit Malware infizierte Webseiten zu locken. Auf diese Weise erlangen sie die volle Kontrolle über die Computer ihrer Opfer.

Die **CIA** hat ein Hacking-Problem. Denn weitere geheime Hacking-Tools der CIA wurden von Hackern über die Enthüllungsplattform Wikileaks veröffentlicht.

Veritaseum hat ein Datenleck. Das Unternehmen, das basierend auf der Ethereum blockchain eine Software-Plattform für smart contracts-gesteuertes peer-to-peer-Trading entwickelt hat, beklagt einen Schaden von 8,4 Millionen US-Dollar.

Über ein Partner-Unternehmen schaffen es unbekannte Hacker Daten von etwa 400.000 Kunden der **UniCredit Bank** zu erbeuten.

Betrüger versuchen **Kunden der Bank of America** auszutricksen, indem sie sich in E-Mails an die Kunden als Mitarbeiter der Bank ausgeben.

Der Guardian berichtet, dass bei **Medicare** eine unbekannte Sicherheitslücke im System ausgenutzt wurde und nun im Darknet Informationen zu Patienten verkauft werden.

Das Buchungssystem Sabre kompromittiert Zahlungsdaten von Hotelkunden, nachdem Hacker sich in das System gehackt haben. Das System ist weltweit in 32.000 **Hotels** installiert, jedoch sind nicht alle betroffen. Zu den betroffenen Hotels gehören beispielsweise die Hard Rock Hotels & Casinos, Loews Hotels und Four Seasons Hotels.

Laut dem Sicherheitsanbieter CheckPoint sind 14 Millionen **Android-Smartphones** von der Malware CopyCat infiziert. Bei acht Millionen Geräten wurde die Firmware geändert. Ziel der Hacker ist es, durch Werbung Geld zu verdienen.

Und auch die Android-Malware SLocker verbreitet sich über das chinesische Social Network QQ. Die Ransomware tarnt sich als Schummel-Tool für das in China beliebte Spiel King of Glory. Die neue Variante verschlüsselt nicht nur alle Dateien auf einer SD-Karte, sie kann auch **Android-Nutzer** aus dem eigenen Gerät aussperren.

Der **Snapchat Account** eines Promis wurde mal wieder gehackt: Diesmal hat es Kylie Jenner erwischt. Die Hacker hatten Zugriff auf private Fotos und drohen mit einer zeitnahen Veröffentlichung von Nacktfotos des Stars.

Ebenfalls wird wieder ein **Twitter Account** eines Promis gehackt. Das Opfer ist die Schauspielerin Victoria Justice, die nun der Tatsache ins Auge sehen muss, dass die Hacker Bilder von ihr veröffentlichen werden.

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

(4.264 Zeichen)