PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights August 2016

Frankfurt am Main, 6. September 2016 – Auch im August sind zahlreiche Cyberangriffe wieder politisch motiviert. Daneben gibt es wieder vermehrt Angriffe auf Banken und auf große Plattformen und Unternehmen wie Yahoo, Instagram, Playstation Network, Telegram, Bitfinex und damit auch deren Nutzer.

Südkorea wird erneut Opfer einer Attacke aus Nordkorea. Die Nachbarnation greift 56 Diplomaten und Sicherheitspersonal aus Südkorea an. Dabei erbeuten die Hacker aus Nordkorea E-Mails und Passwörter.

Citizen Lab berichtet von einer Cyber-Spionage-Gruppe aus dem Iran, die **syrische Dissidenten** ausspioniert. Die Gruppe hat demnach eine Malware-Kampagne gestartet.

Intsights, ein israelisches Cyber Intelligents Unternehmen gibt bekannt, ein **Forum des IS** im Dark Web erfolgreich angegriffen und dabei wertvolle Informationen erbeutet zu haben.

Am indischen Unabhängigkeitstag greifen die Kerala Cyber Warriors 50 **pakistanische Webseiten** per DDoS Attacken an.

Die brasilianische Sparte von Anonymous greift mehrmals **verschiedene Ziele in Brasilien** per DDoS-Attacken an. Damit wollen die Hacker ihren Protest gegen die Olympischen Spiele in Rio de Janeiro 2016 zum Ausdruck bringen und auf Ungerechtigkeiten aufmerksam machen. Zusätzlich werden pikante Details über Funktionäre und Offizielle der Spiele veröffentlicht.

Nach dem Cyberangriff auf die Zentralbank von Bangladesch hat es weitere Attacken auf Geldinstitute gegeben. Dabei haben Banken erneut Geld verloren, teilt der internationale Zahlungsdienstleister **Swift** in einem Brief an seine Mitglieder mit. Die Bedrohung sei nicht nur temporär und die Täter passten sich an neue Gegebenheiten an, warnt die in Brüssel ansässige Genossenschaft.

Die Webseite der **Bank of Israel** wird von den Ghost Squad Hackers per DDoS Attacke lahmgelegt.

Nachdem etwa 10.000 ATMs im südostasiatischen Raum von Cyberkriminellen ausgebeutet wurden, warnt die Zentralbank von Thailand, die **Government Savings Bank**, vor den Hackern, welche bisher schon 350.000Euro erbeutet haben.

Symantec berichtet von einer Hacking-Kampagne, bei der **Instagram**-Usern mit einer gewissen Anzahl an Followern der Account gestohlen wird. Auf den Accounts wird nach der Übernahme durch die Hacker nur noch Spam in Form von pornografischen Inhalten veröffentlicht.

Der Hacker „Peace“, der in der Vergangenheit bereits LinkedIn und Myspace gehackt hat, greift nun **Yahoo** an und veröffentlicht Login-Daten von Nutzern im Internet.

Die Hacker-Gruppe PoodleCorp gibt an, dass sie die Server von **PlayStation Network** zum Erliegen gebracht haben.

Die Bitcoin-Tauschbörse **Bitfinex** wird Opfer einer heftigen Hacker-Attacke. Die Angreifer erbeuten Bitcoins im Wert von rund 58 Millionen Euro. Nach dem Angriff bricht der Bitcoin-Kurs an der Bitcoin-Tauschbörse um etwa 20 Prozent ein.

Hacker, die in Verbindung zur iranischen Regierung stehen, greifen die iranische Bevölkerung an. Demnach wurden 15 Millionen **iranische Accounts der Messenger App Telegram** gehackt. Erbeutet wurden dabei persönliche Daten wie Namen und Nummern.

Die **Leoni AG**, ein führender deutscher Hersteller in den Produktgruppen Drähte, Kabel und Bordnetz-Systeme, wird von Unbekannten gehackt. Unter Verwendung gefälschter Dokumente und Identitäten sowie der Nutzung elektronischer Kommunikationswege schaffen es die Hacker, 40 Millionen Euro auf ein ausländisches Konto zu überweisen.

In Texas erlebt eine Frau den Albtraum einer jeden Mutter. Unbekannte hacken die **Webcam** der Texanerin, die auf das Zimmer ihrer beiden Töchter gerichtet ist. Doch es bleibt nicht nur bei dem fremden Zugriff, der Hacker veröffentlicht den sehr privaten Stream der Webcam auch noch für jeden sichtbar im Internet.

Eine von der russischen Regierung finanzierte Hacker-Gruppe greift Reporter der **New York Times** und anderen Nachrichtenorganisationen an.

Baris Pehlivan ist ein türkischer Journalist – einer, der sich wie viele seiner Kollegen und Kolleginnen nicht von dem türkischen Regime mundtot machen lassen wollte. Entsprechend gerät er ins Visier der türkischen Regierun. Sein Computer wird konfisziert und es werden auf diesem E-Mails und Dokumente gefunden, die ihn mit dem Putschversuch in der Türkei in Verbindung bringen. Schon viel weniger hätte gereicht, um ihn in der Türkei ins Gefängnis zu bringen. Nachdem der Journalist schon einige Zeit in Haft sitzt, wird bekannt, dass ein Hacker diese Informationen auf seinen PC platziert hat. Dabei habe man sich sogar sehr Mühe gegeben, dass das auch nach einer Untersuchung des PC's nicht auffällt.

Die polnische Sparte des Anonymous-Kollektivs greift die **Welt-Anti-Doping-Agentur (WADA)** an und veröffentlicht gekaperte E-Mail-Accounts.

Der Account der Russin **Yulia Stepanova** bei der Welt-Anti-Dopin-Agentur (WADA) wird gehackt. Sämtliche Informationen werden veröffentlicht.

Kaspersky Lab berichtet von einem Trojaner (mobile Malware), der **Android-Smartphones** bedroht.

Eddie Bauer, das US-amerikanische Einzelhandelsunternehmen für Freizeitbekleidung, bemerkt einen Angriff auf das Bezahlsystem, bei dem jede Transaktion aus sämtlichen 370 Shops komprimiert wird.

Wieder werden **Straßenverkehrsschilder in den USA** gehackt. Statt wichtiger Verkehrsinformationen werden darauf Statements veröffentlicht, die sich vor dem Hintergrund, dass es in der Vergangenheit zu tödlichen Schüssen auf wehrlose schwarze US-Bürger gab, gegen die Polizei richten.

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

(5.295 Zeichen)