PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Juni 2017

Frankfurt am Main, 18. August 2017 – Im Juni werden wieder zahlreiche politisch und wirtschaftlich motivierte Hackerangriffe durchgeführt. Aber auch Regierungen nutzen die Möglichkeiten von Spyware nicht mehr nur gegen Kriminelle, wie das Beispiel der mexikanischen Regierung zeigt, die Aktivisten bewusst ausspioniert.

Nachdem sich die **Regierung von Montenegro** dazu entschieden hat, der NATO beizutreten, erreicht sie eine Cyber-Angriffswelle.

Die New York Times berichtet von der Spyware "Pegasus", eine Malware der mexikanischen Regierung. Pegasus wird wohl von der Regierung genutzt, um **mexikanische Menschenrechtler, Aktivisten und Anwälte** zu beschatten. Gekauft wurde die Spyware ursprünglich mit dem Gedanken, Kriminelle leichter zu überführen.

Der arabische Nachrichtensender **Al Jazeera** mit Sitz in Doha wird von Hackern angegriffen. Per DDoS-Attacke bringen die Angreifer die Webseite zum Erliegen. Die Seite ist temporär nicht mehr erreichbar.

Die US-Regierung hat eine offizielle Warnmeldung herausgegeben, die auf Gefahren durch eine Hacker-Gruppe namens Hidden Cobra aufmerksam machen soll. Die Gruppe soll im Auftrag der nordkoreanischen Regierung Angriffe auf **Ziele in den USA** und weltweit ausführen.

Unbekannte hacken die Webseite des **argentinischen Militärs** und hinterlassen Bilder von Kämpfern des IS.

Das CyberTeam bringt per DDoS Attacke die Server von **Skype** zum Erliegen.

Hacker verschaffen sich Zugang zum Netzwerk von **Airway Oxygen Inc.** Sie erbeuten Daten von 500.000 Kunden und Angestellten.

Die Bitcoinbörse **Bitfinex** wird von Hackern per DDoS-Attacke angegriffen, so dass keine Aktionen mehr möglich sind.

Trend Micro berichtet von Wirtschaftsspionage im Bereich neue Technologien. Die Hacker BlackTech fokussieren sich demnach vor allem auf **Ziele in Ostasien** wie Taiwan, Hong Kong und Japan.

Homeland Security und das FBI warnen vor erfolgreichen Hackerangriffen ausländischer Hacker gegen **US-Atomkraftwerke**.

In den Netzwerken zweier **Krankenhäuser in Israel** wurde eine Malware entdeckt (WORM_RETADUP.A), die auf sehr aggressive Weise sensible Daten abzapft.

Der südkoreanische Webhoster **Nayana** wird von Cyber-Kriminellen angegriffen und mit den gestohlenen bzw. verschlüsselten Daten erpresst. Einen Image-Verlust bei seinen Kunden fürchtend, bezahlt das Unternehmen die geforderte Summe in Höhe von einer Million Dollar.

Die US-Richterin **Lori Sattler** wurde von Cyber-Kriminellen um eine Million Dollar betrogen. Die Hacker gaben sich in einer E-Mail als Agentin der Richterin aus und forderten Sattler auf, den Betrag an das in der E-Mail genannte Konto zu überweisen. Im Nachhinein stellt sich heraus, dass das Geld nicht an ihre Agentin ging, sondern an eine Bank in China.

Ein unbekannter Hacker verschafft sich Zugang und Kontrolle über die **Classic Ether Wallet** Domain und zapft Ether in Wert von 300.000 US-Dollar von gehackten Konten ab.

Bithumb, ein koreanischer Ether- und Bitcoin-Exchanger, wird Opfer von Hackern. Diese erbeuten 8.700 US-Dollar.

CD Projekt Red S. A., ein polnischer Entwickler und Publisher von Videospielen, wird erpresst. Hacker kontaktieren das Unternehmen und drohen geheime Informationen zu einem neuen Spiel zu veröffentlichen. Sie fordern die Zahlung einer unbekannten, wie das Unternehmen in einer Pressemitteilung bekannt gibt.

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

(3.238 Zeichen)