PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights April 2017

Frankfurt am Main, 27. Juni 2017 – Im April werden neben dem französischen Präsidentschaftskandidaten Emmanuel Macron unter anderem auch die Deutsche Bundeswehr und das dänische Militär zum Ziel von Hackerangriffen. Doch auch zahlreiche wirtschaftlich motivierte Angriffe werden gemeldet.

Der unabhängige französische Präsidentschaftskandidat **Emmanuel Macron** ist Opfer eines "massiven und koordinierten" Hackerangriffs geworden. Eineinhalb Tage vor der entscheidenden Stichwahl zwischen ihm und Marine Le Pen sind Mails und Dokumente in einer Größenordnung von neun Gigabyte im Internet aufgetaucht. Der Angriff wird dem russischen Hacker Fancy Bear zugeschrieben.

Nach Angaben des Verteidigungsministeriums gab es allein in den ersten neun Wochen dieses Jahres rund 284.000 Angriffsversuche auf die Netzwerke der **Deutschen Bundeswehr**.

Der dänische Verteidigungsminister Claus Hjort Frederiksen von der Partei Venstre hat gegenüber der Zeitung Berlingske dahingehend geäußert, dass Russland das **dänische Militär** gehackt und sich 2015 und 2016 Zugang zu E-Mails von Mitarbeitern verschafft haben soll. Laut Frederiksen soll hinter dem Angriff die Hackergruppe APT28 stecken, auch bekannt als Fancy Bear. Die gleichen Hacker hatten sich im vergangenen Jahr ebenfalls unerlaubt Zugang zu den E-Mails der Demokraten in Amerika verschafft.

Eine Untersuchung von Experten von Interpol und sieben Ländern aus der **südostasiatischen Region** hat ergeben, dass diese Länder Cyber-Kriminellen schutzlos ausgeliefert sind. Knapp 9.000 mit Malware verseuchte Server und tausende komprimierte Webseiten soll es demnach geben.

Das United Cyber Caliphate veröffentlicht mal wieder eine "kill list", in der 8.786 Namen von **Personen** inklusive Adressen und weiterer Informationen genannt werden.

Der Hacker EauchulaGhost defaced 250 **Twitter Accounts**, welche in Verbindung mit dem IS stehen. Es werden pornografische Inhalte auf den Seiten platziert.

Mehrere Medien berichten, dass sich nordkoreanische Hacker Zugang zu Kriegsplänen von den **Regierungen der USA und Südkoreas** verschafft haben. Diese sollten zum Einsatz kommen, wenn es in der Region zu einem Krieg kommen sollte. Mögliche Angriffsziele werden darin wohl auch genannt.

Der oder die Hacker von Fancy Bear greifen den **Weltleichtathletikverband International Association of Athletics Federations (IAAF)** an und komprimieren medizinische Informationen zu Athleten.

Die Hacker-Gruppe Shadow Brokers hat ein verschlüsseltes Archiv samt Passwort veröffentlicht, das Tools und Exploits des **NSA**-Teams Equation Group enthalten soll. 2016 hatte sie das Archiv zum Verkauf angeboten, doch nun soll jeder zugreifen können. Anfangs hatte die Gruppe noch eine Million Bitcoins für das Archiv verlangt, umgerechnet etwa 568 Millionen US-Dollar. Die Auktion scheiterte jedoch. Die Gruppe bot die Exploits daraufhin direkt zum Kauf an, nun soll jedoch jeder auf die Daten zugreifen können.

Kaspersky berichtet von einer Malware, die es auf ATM's **russischer Banken** in Russland und Kasachstan abgesehen hat und Geld abhebt.

Ein unbekannter Hacker kapert den **LinkedIn Account** des Herstellers für Antivirussoftware **McAfee**.

Es soll es in der Nacht vom 22. April 2017 zwischen 2 und 3 Uhr einen Angriff auf die Bitcoin Börse **Yapizon** gegeben haben. Dabei wurden 3.831 Bitcoins im Wert von rund 4,5 Millionen Euro gestohlen.

Der Videospiele Riese **Gamestop** gibt bekannt, dass Hacker mit einer Malware Kreditkarteninformationen abgezapft haben.

Über eine Sicherheitslücke wird der Banking Trojaner Dridex über **Microsoft Office** verbreitet. Betroffen ist das Textverarbeitungsprogramm Word. Millionen Nutzer sind bereits Opfer geworden, indem sie verdächtige E-Mails mit Schadsoftware im Anhang geöffnet haben.

Nordkoreanische Hacker sollen 2015 erfolgreich die **Union Bank of India** mit einer Malware angegriffen und dabei wohl 170 Millionen Dollar erbeutet haben.

Unbekannte Hacker kapern **Amazon** Accounts von Verkäufern und erstellen falsche Angebote.

Hacker kapern Accounts bei **Airbnb** und mieten sich über diese Wohnungen und räumen sie leer.

Die Hacker von OurMine komprimieren mehrere beliebte **Youtube**-Kanäle.

Wieder veröffentlicht ein Hacker private Bilder von **mehreren Celebrities**, darunter auch viele Nacktbilder. Wie der Hacker an die Bilder gekommen ist, bleibt unklar.

In Litauen sind Hacker in die Server **von Grozio Chirurgiija**, ein Betreiber von Schönheitskliniken, eingedrungen. Wie die Polizei in Vilnius berichtete, erbeuteten sie dabei persönliche Patientendaten, darunter etwa 25.000 Fotos. Wie die Beamten laut "AP" mitteilten, handelte es sich bei den Cyberkriminellen um eine Gruppierung namens "Tsar Team". Mit dem Material erpressen die Hacker nun die Patienten und die Klinik für plastische Chirurgie. Unter den Betroffenen sind auch Deutsche.

Unbekannte Hacker habe die Kontrolle über die App der **New York Post** übernommen und verbreiten Falschmeldungen.

Der Hacker TheDarkOverlord veröffentlicht noch bis dahin unveröffentlichte Episoden der **Netflix** Serie "Orange is the new Black".

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

(4.966 Zeichen)