PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Februar 2018

Frankfurt am Main, 20 April 2018 - Im Februar sind auffällig viele Hackerangriffe wirtschaftlich motiviert. Neben harten Devisen stehen auch Kryptowährungen bei Cyberkriminellen hoch im Kurs. Doch auch sensible Unternehmens- oder Kundendaten lassen sich zu Geld machen.

Das bislang als „sicher" eingestufte Datennetz der **Deutschen Bundesverwaltung** – der Informationsverbund Berlin-Bonn (IVBB) – wurde von Hackern infiltriert. Mutmaßlich soll es sich dabei um die russischen Hacker Fancy Bear handeln. Die Angreifer könnten ein gesamtes Jahr lang unbemerkt im Netz gewesen sein und wären somit in der Lage über den gesamten Zeitraum Informationen des Innenministeriums abgezweigt zu haben.

Pünktlich zur heißen Phase der Parlamentswahlen 2018 wurde die **italienische demokratische Partei Partito Democratico** gehackt. Die Hacker von AnonPlus veröffentlichten ihre Beute in Form von internen Informationen der Partei und ihres Politikers Matteo Renzi.

Forscher von McAfee haben eine Phishing-Kampagne aufgedeckt, die es auf **Bitcoin**s abgesehen hat. Drahtzieher ist die berüchtigte Lazarus Gruppe, die es in der Vergangenheit vor allem auf Rüstungskonzerne abgesehen hatte. Die Gruppe versucht durch täuschend echt aussehende E-Mails, Besitzer von Bitcoin dazu zu bringen, ihnen diese anzuvertrauen oder Informationen preiszugeben.

Ukrainische Cyberkriminelle haben mit einer Phishing-Kampagne über 50 Millionen Euro erbeutet. Mit Google AdWords wurden **Bitcoin Interessenten** betrügerische Seiten angeboten, welche den Originalseiten extrem ähnelten. Versucht nun sich ein Besitzer eines Bitcoin-Kontos auf der falschen Seite anzumelden, gelangen seine Login-Daten direkt zu den Hackern. Mit diesen melden sich dann die Hacker an und räumen das Konto leer. Die zuständige Polizei in der Ukraine konnte zusammen mit Cisco Talo die Kriminellen ausmachen.

Auf der Webseite der **Los Angeles Times** haben Hacker in dem Bereich, in dem über Morde berichtet wird, einen Kryptowährung schürfenden Code eingeschleust. Die Rechenkapazität der Server der Los Angeles Times wurde daraufhin für das Schürfen der Monero Währung missbraucht.

Die russische Zentralbank gibt im Februar bekannt, dass im vergangenen Jahr eine namentlich nicht genannte **russische Bank** Opfer eines Hackers wurde. Dieser hatte das SWIFT Bezahlsystem manipuliert. Der Schaden für die Bank beläuft sich wohl auf sechs Millionen Dollar.

Und schon wieder gelang es Hackern, das Zahlungssystem SWIFT zu manipulieren. Unbekannte Hacker erbeuteten über die Bezahlplattform zwei Millionen Dollar von der indischen **City Union Bank**.

Western Union, ein US-amerikanischer Anbieter von weltweitem Bargeldtransfer, gab bekannt, über einen externen Dienstleister gehackt worden zu sein. Dabei haben sich die Unbekannten Zugang zum Western Unions System verschafft und Kundeninformationen mitgehen lassen. Der Funfaktor dabei: Besagter externer Dienstleister wurde mit der Sicherung aller Datensätze betraut.

BitGrail, ein italienischer Exchange mit Fokus auf Nano (ehemals RailBlocks), wurde

gehackt. Es ist ein Schaden in Höhe von 195 Millionen US-Dollar entstanden. Das Unternehmen gab am 9. Februar den Verlust von 17 Millionen XRB bekannt. Der Nano-Kurs ist nach der Meldung von $ 11,5 auf $ 9,12 gefallen.

Nach einem Hackerangriff auf zwei Datenbases der **Sacramento Bee**, einer lokalen Tageszeitung, sah sich die Zeitung gezwungen, die beiden Datenbases zu vernichten, um weiteren Schaden zu verhindern. Hacker hatten die Datenbases mit Malware infiziert und Daten von 19,5 Millionen Wählern und 53.000 Abonnenten geraubt. In einem Video auf Facebook hatten die Angreifer ein Lösegeld für die Daten gefordert und gedroht, andernfalls weiteren Schaden anzurichten. Da sich die Sacramento Bee nicht erpressen lassen und weitere Schäden vermeiden wollte, wurden die infizierten Datenbases vernichtet.

Das Schweizer Telekommunikationsunternehmen **Swisscom** ist Opfer eines großen Datendiebstahls geworden. Wie nun bekannt wurde, hatten unbekannte Täter im Herbst 2017 800.000 Datensätze entwendet. Darunter befinden sich sensible Kundendaten wie Namen, Adressen, Telefonnummern und Geburtsdaten. Angeblich habe sich niemand in das System gehackt, sondern es seien Zugriffsrechte missbraucht worden.

Eine neue aggressive Malware kursiert im Internet und hat enormen Schaden bei zahlreichen **Einzelpersonen** angerichtet. Black Ruby ist ihr Name. Die Ransomware tauscht die Namen der sich auf dem infizierten PC befindenden Dateien und verschlüsselt diese. Zusätzlich installiert die Malware einen Monero Miner. Einen Hinweis auf die Herkunft gibt eventuell die Tatsache, dass die Malware Systeme aus dem Iran ignoriert.

Der amerikanische Anbieter für Mobile Monitoring **Retina-X-Studios** wurde anscheinend gehackt. Hacker haben nämlich behauptet, ein Terabyte mit Daten des Unternehmens zu besitzen. Das Unternehmen verkauft unter anderem Technologie, mit der sich Telefongespräche und SMS-Verkehr aufzeichnen lassen.

Eine Phishing-Kampagne vom Juli 2017 wurde nun aufgedeckt. Kriminellen war es damit gelungen, **Snapchat** Konto-Informationen von 50.000 Nutzern zu erbeuten.

Die Amazon-Cloud-Umgebung des E-Autobauers **Tesla** wurde gehackt. Die Angreifer hatten es jedoch nicht auf geheime Unternehmensdaten abgesehen, sondern nutzten die Rechenkapazität der Server für Crypto-Mining aus.

Die Coding-Plattform **GitHub** hat den bislang stärksten verzeichneten DDoS-Angriff überstanden. Der Angriffstraffic hatte eine Bandbreite von insgesamt 1,35 Terabit/s, berichtet Wired. Der bis dahin stärkste Angriff hatte eine Stärke von 1,2 Terabit/s.

Sonstige

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

(5.520 Zeichen)