PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Mai 2017

Frankfurt am Main, 01. August 2017 - Im Mai rücken neben der Energieversorgung in Lettland, Estland und Litauen auch das US-Verteidigungsunternehmen und das britische Parlament in den Fokus von Cyberkriminellen. Aber auch zahlreiche Hackerangriffe sind rein wirtschaftlich motiviert und zielen auf Privatpersonen und Unternehmen ab.

Drei baltische Staaten geraten ins Visier von russischen Hackern, die wohl von der Regierung unterstützt werden. Vorübergehend wird die aus Russland kommende **Energieversorgung in Lettland, Estland und Litauen** getrennt.

Ein Reporter der Times deckt auf, dass vermutlich russische Hacker Twitter genutzt haben, um die Accounts von Mitarbeiters des **US-Verteidigungsministeriums** durch das Versenden von infizierten Nachrichten mit Malware zu infizieren.

Unbekannte Hacker versuchen die Online-Accounts von Mitgliedern des **britischen Parlaments** zu kapern.

Unbekannte hacken sich in die Webseite der staatlichen Nachrichten-Agentur **Qatar News** (QNA) und veröffentlichen einen angeblichen Fake-Bericht, in welchem der Emir Qatars die anderen Golf-Staaten kritisiert, aber den Iran und Terrorgruppen wie die Hamas lobt. Auch der Twitter-Account von QNA wurde gekapert und Fake-Tweets verbreitet.

Der amerikanische Medienkonzern **Gannet Company, Inc.** wird von Hackern ins Visier genommen. Mittels einer Phishing-E-Mail-Attacke komprimieren die Angreifer 18.000 Accounts von aktuellen und ehemaligen Mitarbeitern.

Hacker versuchen an Login Informationen von **britischen Bankkunden** zu kommen, indem sie mit ähnlichen Domains die Webseiten der UK-Banken nachahmen. Dort werden auch die Anmeldedaten zum Onlinebanking abgefragt, jedoch gelangt man nach der Eingabe nicht auf den eigenen Account, sondern schickt die Daten an die Hacker.

Die Banque de France warnt Kunden vor Phishing-E-Mails von Hackern, die Adresse, Logo und den Namen der Bank nutzen, um die **Kunden der Banque de France** zu täusche

Hacker haben Konten von deutschen Bankkunden über Sicherheitslücken im Mobilfunknetz von **O2 Telefonica** leer geräumt. Dies gelang ihnen wohl, indem sie Mobil-TANs, die für die Geräte der Kunden bestimmt waren, umleiteten und so die Überweisungen autorisieren konnten. Die Sicherheitslücken im SS7-Protokoll des UMTS-Netzes sind seit Jahren bekannt.

Experten von CitizenLab berichten von einer Spionage-Kampagne gegen etwa **200 Privatpersonen**, die in der Energie-Branche beschäftigt sind. Aber auch Russland-kritische Journalisten und Ukraine-Offiziere geraten dabei in den Fokus der Hacker. Vermutlich kommt der Angriff aus Russland von APT28.

Eine groß angelegte Phishing-Kampagne wird gegen **Gmail Nutzer** gestartet. Dabei wurden etwa eine Million Accounts komprimiert.

Es handelt sich um eine der größten Malware-Kapagnen im Google Play Store. Die Experten von Check Point berichten über eine Kampagne gegen **Android Nutzer**, in der mindestens

40 Apps mit Malware infiziert wurden. Die meisten Apps stammen von südkoreanischen Entwicklern.

Filialen des US-amerikanischen Herrenausstatters **Brooks Brothers** werden mit einer Malware infiziert, die Kreditkarteninformationen der Kunden komprimiert.

Das Lernnetzwerk **Edmodo** ist Ziel von Hackern geworden. Die Angreifer erbeuten bei der Cyber-Attacke Millionen Nutzeraccounts, die im Dark Web zum Verkauf angeboten werden.

Der Hacker "TheDarkOverlord" erbeutet bei drei verschiedenen Angriffen auf **Schönheitskliniken** vertrauliche Informationen von 180.000 Patienten. Die attackierten Kliniken sind die Aesthetic Dentristy, OC Gastrocare und Tampa Bay Surgery Center.

Eine Malware trifft die britische Kaufhauskette **Debenhams**. Nachdem die Systeme komprimiert wurden, erbeuten die Angreifer persönliche Informationen von bis zu 26.000 Kunden.

Unbekannte haben den Quelltext von mehreren Apps des Entwicklerstudios **Panic** kopiert, nachdem sie sich Zugang zum Versionsverwaltungssystem der Entwickler verschafft hatten. Dies gelang ihnen, weil ein CEO (Steven Frank) des Unternehmens die im Video-Encoder Handbrake für wenige Tage versteckte Malware Proton auf seinem Arbeits-Mac installiert hatte. Die Angreifer versuchen, unter Androhung einer Veröffentlichung des Codes Lösegeld zu erpressen.

Ein Hacker hat es geschafft, bei **OneLogin** verschlüsselte Daten auszulesen. Das räumte der Single-Sign-on-Dienst ein und benachrichtigte umgehend seine Kunden. Diese sollen deshalb neue API-Schlüssel und OAuth-Tokens, neue Sicherheits-Zertifikate und Anmeldedaten generieren und Mitarbeiter dazu auffordern, neue Kennwörter zu setzen. Der Angreifer konnte sich wohl sieben Stunden frei im System bewegen, bis Mitarbeiter den Eindringling bemerkten.

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

(4.576 Zeichen)