PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights November 2017

Frankfurt am Main, 18. Januar 2018 – Im November gibt es wieder einige politisch motivierte Cyberattacken unter anderem gegen Neonazi-Webseiten oder die Terrororganisation ISIS. Auch werden zahlreiche Unternehmen gehackt und sensible Kundendaten erbeutet.

Unit 42, das Forschungsteam von Palo Alto Networks, hat Cyberangriffe beobachtet, die sie „MuddyWater" benannten. Es handelt sich um spionagebezogene Attacken, die auf Täuschung setzen. Die MuddyWater Angriffe richten sich gegen Ziele in verschiedenen Ländern, darunter die **Regierung Saudi-Arabiens**.

Die türkischen Hacker Akincila defaced die Webseiten der asiatischen und der israelischen Ausgabe der britischen Tageszeitung **The Times**. Es werden eigene Nachrichten mit Bezug zu Palästina hinterlassen.

Das Kollektiv Anonymous führt wegen vermehrter Vorfälle rechtsradikaler Gruppen in den USA eine Hacking-Kampagne unter dem Banner #OpDomesticTerrorism. 12 **Neonazi-Webseiten** werden in diesem Zusammenhang von Anonymous geschlossen.

Das Kommunikations-System der Terrororganisation **ISIS** wird von irakischen Hackern gestört. Die Gruppe, die sich Daeshgram nennt, platziert pornografische Inhalte im System.

Das US-amerikanische Web-Hosting Unternehmen **SchoolDesk** wird von Team System Dz infiziert, eine Hackergruppe, die den IS unterstützt. Das hat fatale Folgen. Denn SchoolDesk ist für knapp 800 Webseiten von Schulen verantwortlich. Die Angreifer hinterließen auf mehreren Hundert Schulwebseiten pro-islamistische Propaganda mit einem Rekrutierungsvideo und einem Bild von Saddam Hussein.

Der vermeintliche Kryptotrojaner Ordinypt, dem **mehrere Personen** zum Opfer gefallen sind, hat sich als Fail entpuppt. Aus Sicht der Drahtzieher hinter Ordinypt waren die Voraussetzungen zunächst alles andere als schlecht. Denn der Erpressungstrojaner wird über gut angelegte Phishing-Mails verbreitet, die auf den ersten Blick erstmal kein Misstrauen schüren. Doch zum einen sind nur wenige dieser Phishing-Mails im Umlauf und zum anderen verschlüsselt der Trojaner die Daten des Empfängers nicht, sondern löscht sie gleich ganz. Auf dieser Basis lässt sich letztendlich nur schwer Geld von den Opfern erpressen.

Die SWIFT Saga nimmt kein Ende. Nächstes Opfer ist die **NIC Asia Bank** mit Sitz in Katmandu geworden. Die Bank beklagt einen Verlust von 4,4 Millionen US-Dollar.

Der Webhoster **Hetzner** mit Sitz in Gunzenhausen wurde Opfer eines Hackerangriffs. Die unbekannten Eindringlinge hatten unter anderem Zugriff auf sensible Kundendaten wie Passwörter und Zahlungsinformationen. Das Hosting-Management wurde mit einer SQL-Injection angegriffen.

Bereits lange vor seiner Kandidatur für das Amt des amerikanischen Präsidenten gerieten der amtierende Präsident **Donald Trump und seine Trump Organization** ins Visier von Hackern. Die Spur führt nach Russland. Im Jahr 2013 gab es einen Cyberangriff auf rund 200 Webseiten Trumps, seiner Familie und seines Wirtschaftsimperiums. Als Folge der Hacks wurden die Nutzer wohl beim Aufrufen der Seiten zu Servern in Sankt Petersburg weitergeleitet.

Der amerikanische Vermittler für Personenbeförderung **Uber** ist 2016 gehackt worden und hat versucht dies zu verheimlichen. Dank Mitarbeitern gelangte die Nachricht nun doch an die Öffentlichkeit. Die Angreifer fanden offenbar in einem privaten Github-Repo von Uber-Entwicklern Zugangsdaten für den vom Unternehmen genutzten AWS-Speicher. So hatten sie Zugang zu fast 60 Millionen Kundendaten mit E-Mail-Adressen, Telefonnummern, Namen und von einigen Kunden wurden zusätzlich die Führerscheininformationen komprimiert. Die Angreifer melden sich daraufhin bei Uber und fordern ein Lösegeld in Höhe von 100.000 Dollar, welches sofort gezahlt wird. Nachdem die Sache erst ein Jahr später öffentlich wird, ermittelt nun die New Yorker Staatsanwaltschaft gegen das Unternehmen.

Bitdefender hat eine bereits seit Mitte 2016 aktive Maleware entdeckt, der vornehmlich **Bankkunden** zum Opfer fallen. Es handelt sich dabei um eine neue Variante des Banking-Trojaners Terdot, einem Ableger der Zeus-Familie. Dieser verfügt über zusätzliche Spionagefunktionen, die die Überwachung und Veränderung von Einträgen in sozialen Medien wie Facebook und Twitter erlauben. Zusätzlich verschafft die Malware den Angreifern einen Zugriff auf den E-Mail-Verkehr der Opfer.

Die Trojaner Qakbot und Emotet sind schon mehrere Jahre alt und hauptsächlich auf das Stehlen von **Zugangsdaten für das Online-Banking** spezialisiert. Die Erfinder der Malware arbeiten jedoch stetig weiter an dem Code. Um eine weite Verbreitung der Malware zu gewährleisten, werden die beiden Trojaner meist über groß angelegte Spam-Kampagnen mit infizierten Anhängen verteilt.

Experten bemerken eine Phishing-Kampagne gegen **Netflix-Nutzer** mit dem Ziel ihren Account zu kapern.

Forever 21, ein amerikanisches Textilhandelsunternehmen mit zahlreichen Ladengeschäften, wird gehackt. Die Angreifer erbeuten die Bezahlinformationen der Kunden.

Der Fotodienst **Imgur** hat mitgeteilt, dass im Jahr 2014 etwa 1,7 Millionen Nutzer von einem Hack betroffen waren. Die Angreifer hatten Zugriff auf die Passwörter und E-Mail-Adressen der betroffenen Nutzer.

Der australische Second-Hand-Händler **Cash Converters** gibt bekannt, gehackt worden zu sein. Die Hacker erbeuten Nutzerdaten wie Namen, Nutzernamen mit Passwörtern und Adressen.

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

(5.250 Zeichen)