PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights August 2017

Frankfurt am Main, 6. Oktober 2017 - Im August rücken wieder vermehrt politische Institutionen ins Visier von Cyberkriminellen. Aber auch Accounts bei Twitter, Instagram und Co werden vermehrt angegriffen, wodurch Hacker Zugriff auf allerlei geschäftliche und persönliche Daten und Informationen haben.

Die Mitteldeutsche Zeitung berichtet von einem Hackerangriff auf die **deutsche Regierung**. Mitte April wurden mehrere PCs der Landesbehörde von Sachsen-Anhalt mit Hilfe einer Erpressungssoftware verschlüsselt. Diese mussten daraufhin vom Netz genommen werden. IT-Experten entdeckten dann im Verlauf der Untersuchung einen Backdoor-Trojaner. Wie lange dieser schon im System war, ist unbekannt.

ESET-Sicherheitsforscher präsentieren Informationen zu einer Cyberspionage Kampagne. Die Experten erläutern Aktivitäten der berüchtigten Cyberspionage Gruppe Turla und einer bis jetzt unentdeckten Backdoor „Gazer“. Mit Hilfe der Hintertür spionierte die Gruppe **weltweit Konsulate und Botschaften** aus. Zahlreiche Computer seien kompromittiert worden, heißt es. Die meisten Ziele lagen wohl in Europa.

Anonymous übernimmt die Verantwortung für einen DDoS Angriff auf die offizielle Webseite der Stadt **Charlottesville** im US-Bundesstaat Virginia. #OpDomesticTerrorism läuft, nachdem es in der Stadt zu Ausschreitungen rechtsextremer Gewalttätiger gekommen ist.

Indische Hacker defacen eine Webseite der **pakistanischen Regierung**. Der Hacker Ne0-H4ck3r hinterlässt auf der Seite eine eigene Nachricht unterlegt mit indischer Volksmusik.

Unbekannte greifen per DDoS Attacke den nationalen Postservice **Ukrposhta** der Ukraine an. Die Seite ist daraufhin nicht mehr erreichbar.

Rund 40 Webseiten von **venezolanischen Institutionen** sind von einem Hackerangriff getroffen worden. Dabei wurden die Seiten defaced. Zu der Aktion bekannte sich eine Gruppe mit dem Namen "The Binary Guardians", die offenbar dem radikalen Teil der Opposition nahesteht.

Wieder werden Webseiten der **armenischen Regierung** von türkischen Hackern angegriffen. Ob die Angreifer Daten entwenden konnten, ist nicht bekannt.

Nach der **Präsidentschaftswahl 2017 in Kenia** hat Oppositionskandidat Raila Odinga seinem Konkurrenten Uhuru Kenyatta Wahlbetrug vorgeworfen. Er behauptet, die Datenbank der Wahlkommission sei gehackt worden.

Offizielle Regierungsmitglieder räumen ein, dass das **schottische Parlament** Ziel einer Brute Force Attacke geworden ist.

Indonesische Hacker defacen 22 Webseiten der **malaysischen Regierung**.

Die **Surgical Dermatology Group** muss ihren Patienten mitteilen, dass es einen Angriff auf die Server des Cloud-Providers gab. Dabei wurden Patientendaten entwendet.

Die Hackergruppe OurMine, die dafür bekannt ist, Social Media Konten zu kapern, hat sich die **Twitter Accounts von HBO und Game of Thrones** als neustes Ziel ausgesucht. Nach erfolgreicher Übernahme werden #HBOHacked Nachrichten verbreitet.

Die gleiche Hackergruppe hat auch die **Twitter Accounts des FC Barcelona und des Champions League Siegers Real Madrid** gehackt und übernommen. Die Hacker verbreiten via Twitter die Nachricht, es würden neue Spieler verpflichtet.

Instagram gibt bekannt, dass es Hackern über eine Sicherheitslücke in der eigenen API gelungen ist, Informationen wie E-Mail-Adressen und Telefonnummern von zahlreichen Instagram Accounts auszulesen. Unter den Opfern sind viele Celebrities.

The Fappening 2017: Es ist mal wieder soweit. Wie schon so oft in den letzten Monaten und Jahren kommt es zu einem riesigen Datenleak bei **mehreren Celebrities**. Hacker erbeuten äußerst private Fotos von Stars wie Tiger Woods, Miley Cyrus, Kristen Stewart und vielen mehr. Es dauerte nicht lange, bis die Hacker die gestohlenen Bilder und Videos veröffentlichten.

Unbekannte hacken die Website Domain von **Enigma Blockchain Project** und stehlen eine Mailing Liste. Mit dieser Liste wird ein Phishing Angriff gestartet, bei dem den Empfängern suggeriert wird, einen Rabatt auf einen Presale Aktion zu erhalten, der umso höher ausfällt, wenn viele Personen daran teilnehmen. Letztendlich gingen alle Transaktionen an die Hacker, die auf diese Weise insgesamt 500.000 $ erbeuten konnten. Nachdem es eine DDoS Attacke gegeben hat, sind die Webserver von **Blizzard Entertainment** down.

Wieder einmal wurden **Android Nutzer** zum Ziel von Hackern. Kaspersky Laab berichtet von einem neuen Android-Trojaner. „Faketoken" stiehlt Zugangsdaten von mehr als 2.000 Finanz-Apps, verschlüsselt private Daten und fordert Lösegeld.

Die Hackergruppe OurMine hackt die **Wikileaks** Webseite und übernimmt die Kontrolle darüber.

Die Ransomware WannaCry hat ein weiteres Opfer ausgemacht. Der koreanische Elektronikkonzern **LG** bestätigte, dass einige seiner Systeme mit der Malware infiziert wurden. Als Folge schaltete das Unternehmen Teile seines Netzwerks für zwei Tage ab, um eine weitere Verbreitung von WannaCry zu verhindern.

Kaspersky Lab berichtet von einer elf Tage andauernden DDoS Attacke auf einen chinesischen **Telefonie-Anbieter**.

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

(4.927 Zeichen)