QGroup präsentiert »Best of Hacks«: Highlights Juli 2020

Frankfurt am Main, 28. August 2020 – Im Juli rückt Twitter in den Fokus der Berichterstattung, nachdem Konten bekannter Persönlichkeiten für die Betrugskampagne „Crypto for Health" missbraucht wurden. Darüber hinaus kam es wieder zu zahlreichen Zugriffen auf persönliche Daten von Internetnutzern.

Der US-amerikanische Mikroblogging-Dienst **Twitter** rückt mal wieder in den Fokus von Cyberkriminellen. Mehrere Twitter-Konten wurden von unbekannten Hackern gekapert. Zahlreiche der betroffenen Konten gehören bekannten Persönlichkeiten wie Elon Musk oder Barack Obama oder auch Unternehmen wie Apple oder verschiedene Bitcoin-Börsen. Auf ihnen wurden nicht autorisierte Tweets abgesetzt, in denen versprochen wurde, den doppelten Betrag übertragener Bitcoins an den Sender zurückzuschicken. Die Angreifer konnten so 118.000 US-Dollar in Bitcoins erbeuten. Mehrere Bitcoin-Börsen setzten die Bitcoin-Adresse dieser Bitcoin-Betrugswelle namens "Crypto for Health" auf eine schwarze Liste und verhinderten so nach eigenen Angaben mehr als 1.100 weitere Bitcointransfers.

386 Millionen Nutzerdatensätze wurden in einem Untergrundforum von einem unbekannten Cyberkriminellen zum Download angeboten. Die Datensätze stammen aus verschiedenen Leaks, wovon einige bereits bekannt waren und die betroffenen Unternehmen sich schon dazu geäußert hatten. Andere Datensätze stammen von Leaks, die bisher noch nicht bekannt waren. Insgesamt umfasst der Download 18 Datenleaks. 9 davon waren bisher nicht bekannt. Die angebotenen Nutzerdatensätze teilen sich wie folgt auf: 5,9 Millionen Datensätze von **Appen**.com, 2,4 Millionen von **Drizly**.com, 1,3 Millionen von **Havenly**.com, 475 Tausend von **Indabamusic**.com, 127 Tausend von **Ivoy**.mx, 444 Tausend von **Proctoru**.com, 3 Millionen von **Rewards1**.com, 5,8 Millionen von **Scentbird**.com und 4,8 Millionen von **Vakinha**.com.br.

Der Datenleck-Sammler **Data Viper** wurde Opfer eines Cyberangriffs. Eine Hackergruppe erbeutete mindestens 2 Milliarden Datensätze, die anschließend im Darknet zum Kauf angeboten wurden. Die Firma Data Viper sammelt Zugangsdaten aus Datenlecks und verkauft den Zugang zu einer Datenbank mit rund 15 Milliarden Benutzernamen, Passwörtern und weiteren Informationen an Organisationen und Strafverfolgungsbehörden.

Garmin.com und Garmin Connect wurden Ziel einer Attacke mit der Ransomware "WastedLocker". Der Ausfall betraf die Connect-Apps und auch die Garmin Express Dienste. Benutzer konnten z.B. ihr Fitnessband, die Sportuhr oder den Radcomputer nicht mehr mit der hauseigenen Datencloud von Garmin synchronisieren. Das Abrufen von E-Mails und der Online-Chat waren ebenfalls betroffen. (2.591 Zeichen)

Medienkontakt:

QGroup GmbH
Berner Straße 119
60437 Frankfurt am Main
www.qgroup.de/presse

Lars Bothe
Tel.: +49 69 17 53 63-014
E-Mail: l.bothe@qgroup.de