

## **G DATA Bedrohungsreport: Angriffe ohne Schadsoftware nehmen zu**

Cyberkriminelle greifen weiterhin verstärkt Unternehmen an

Bochum (Deutschland), 06. September 2021

**Der aktuelle Bedrohungsreport von G DATA CyberDefense verzeichnet einen deutlichen Rückgang der abgewehrten Angriffsversuche im ersten Halbjahr 2021 im Vergleich zum Vorjahreszeitraum. Der Grund dafür ist, dass für Angriffe nicht mehr nur Schadsoftware zum Einsatz kommt. Die Gefahr für Unternehmen bleibt unverändert hoch.**



Um mehr als 40 Prozent ist die Zahl der abgewehrten Cyberattacken im Vergleich zum ersten Halbjahr 2020 zurückgegangen. Das belegt der aktuelle Bedrohungsreport von G DATA für das erste Halbjahr 2021 im Vergleich zum Vorjahreszeitraum. Der starke Rückgang hängt auch mit den extrem hohen Zahlen im Jahr 2020 zusammen. Gerade im zweiten Quartal 2020 hatten Cyberkriminelle die Verunsicherung der Menschen infolge der Corona-Pandemie besonders stark ausgenutzt, was damals zu einer massiven Zunahme der abgewehrten Angriffe führte (plus 156 Prozent). Vom ersten zum zweiten Quartal 2021 beträgt der Rückgang 15,6 Prozent. Die aktuellen Zahlen bestätigen aber auch den Trend, dass Unternehmen weiterhin verstärkt im Fokus der Angreifer sind. Während die Zahl abgewehrter Attacken auf Privatkunden um fast 20 Prozent gesunken ist, beträgt der Rückgang im Unternehmensumfeld nur knapp drei Prozent.

*„Die Zeit der großflächigen Angriffe ist vorbei. Cyberkriminelle gehen bei Attacken auf Unternehmen zunehmend gezielt vor. Wir gehen davon aus, dass gerade im vergangenen Jahr viele Unternehmen auf Grund des hastigen Umzugs ins Homeoffice einer Cyberattacke zum Opfer gefallen sind, das aber noch nicht gemerkt haben“,* sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

### **Gezieltes Vorgehen**

Für gezielte Attacken nutzen Cyberkriminelle weiterhin bestehende Schwachstellen aus. Gerade in den ersten sechs Monaten des Jahres haben verschiedene kriminelle Gruppierungen mehrere größere Sicherheitslücken in Microsoft Exchange Servern aktiv ausgenutzt und die Netzwerke von Unternehmen infiltriert.

Ein weiteres Beispiel für das Vorgehen von Cyberkriminellen ist der sogenannte AMSI-Bypass. Immer wieder versuchen Angreifer, das von Microsoft entwickelte Antimalware Scan Interface (AMSI) zu umgehen. Eigentlich scannen Sicherheitslösungen dank AMSI Anwendungen auf ihre Schadhaftheit. Allerdings versuchen Malware-Autoren mit automatisierten Tools, diese Schnittstelle auszuschalten oder einen Weg an ihr vorbeizufinden – insbesondere, um dateilose Schadsoftware einzusetzen.

### **G DATA CyberDefense AG Unternehmenskommunikation**

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

[www.gdata.de](http://www.gdata.de)

E-Mail: [presse@gdata.de](mailto:presse@gdata.de)

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

## **Malware Top 10: Remote Access Trojaner in der Überzahl**

Nach wie vor zählt QBot nicht nur zu den aktivsten, sondern auch den gefährlichsten Schadprogrammen. Bei einem Großteil der aktuellen Angriffe im ersten Halbjahr kam der Emotet-Nachfolger zum Einsatz. Der ursprüngliche Bankingtrojaner wurde von den Angreifern nach und nach ebenfalls zu einer Allzweckwaffe für Cyberkriminelle weiterentwickelt. Weiterhin sind viele Remote Access Trojaner (RAT) aktiv. Sieben der zehn aktivsten Schadprogramme zählen zu dieser Gruppe. RATs ermöglichen eine vom Nutzer unbemerkte Fernsteuerung und administrative Kontrolle eines fremden Rechners. So können Angreifer unter anderem den Desktop des Opfers einsehen, Tastatureingaben protokollieren, auf die Kamera zugreifen sowie die in Browsern gespeicherte Anmeldeinformationen kopieren oder Dateien hoch- bzw. herunterladen.

## **Malware-as-a-Service: Gootloader**

Wie trickreich Cyberkriminelle ihre Angriffsbemühungen weiterentwickelt haben, verdeutlicht ein Blick auf die aktuelle Angriffswelle der Gootloader-Malware-Familie. Die Malware-Autoren haben Gootloader so weiterentwickelt, dass sie verschiedene Malware nachladen und installieren kann. Dabei pushen die Angreifer\*innen ihre eigenen Seiten mit Search-Engine-Poisoning nach oben. Diese sehen aus wie legitime Seiten, sodass auch technisch versierte User einer derartigen Täuschung zum Opfer fallen.

*„Trotz der sinkenden Zahlen kann von Entspannung keine Rede sein. Unternehmen sollten vielmehr ihre Hausaufgaben erledigen und ihre IT absichern. Technische Maßnahmen sind wichtig, aber mindestens genauso wichtig ist es, die Belegschaft im Umgang mit Gefahren zu schulen – denn längst nicht alle Risiken bestehen nur aus Schadsoftware“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.*



## **G DATA CyberDefense AG Unternehmenskommunikation**

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

[www.gdata.de](http://www.gdata.de)

E-Mail: [presse@gdata.de](mailto:presse@gdata.de)

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299