

G DATA Bedrohungsreport: Qbot löst Emotet ab

Cyberattacken auf Unternehmen steigen stark an

Bochum (Deutschland), 11. Mai 2021

Der aktuelle Bedrohungsreport von G DATA zeigt, dass Cyberkriminelle bereits einen Nachfolger für Emotet gefunden haben: Qbot. Bei fast jedem vierten abgewehrten Angriff war die Schadsoftware mit von der Partie. Die Zahlen belegen, dass im ersten Quartal besonders Unternehmen im Fokus von Cyberkriminellen standen. Binnen Jahresfrist stieg die Zahl der abgewehrten Attacken um mehr als 60 Prozent.



Der aktuelle Bedrohungsreport von G DATA CyberDefense zeigt, dass Unternehmen stärker im Visier von Cyberkriminellen stehen. Während sich die Zahl der abgewehrten Cyberangriffe auf Privatanwender nur leicht verändert hat – ein Anstieg um 1,9 Prozent im Vergleich vom ersten Quartal 2020 zum ersten Quartal 2021 – hat sich die Zahl der Attacken auf Unternehmen deutlich erhöht. Um 61,7 Prozent lag die Zahl der abgewehrten Attacken zwischen Januar und März dieses Jahres im Vergleich zum Vorjahreszeitraum. In diesen Zeitraum fallen auch die zahlreichen Angriffe auf Exchange-Server, die viele Unternehmen vor Probleme gestellt haben – und noch stellen werden.

„Im zweiten Jahr der Corona-Pandemie haben Unternehmen immer noch gewaltigen Nachholbedarf bei der Absicherung ihrer IT. Cyberkriminellen spielt die weiter anhaltende Homeoffice-Situation in die Karten und sie schlagen daraus Kapital. IT-Verantwortliche müssen endlich handeln und sich von den schnell aufgesetzten, provisorischen Home-Office-Strukturen verabschieden und eine sichere IT-Infrastruktur schaffen“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Emotet ist tot! – Lang lebe Qbot!

Als Ende Januar Emotet durch eine international koordinierte Aktion abgeschaltet wurde, stand schnell eine Frage im Raum: Welche Schadsoftware beerbt die Allzweckwaffe des Cybercrime? Die Antwort lautet: Qbot. Aktuelle Zahlen zeigen, dass bei 22 Prozent aller abgewehrten Angriffe Qbot beteiligt ist. Der ursprüngliche Bankingtrojaner wurde von den Angreifern nach und nach modular weiterentwickelt, besitzt jetzt zusätzliche Wurmelemente und ist als Credential Stealer und als Loader aktiv. Zurzeit nutzen die Kriminellen bestehende Mail-Konversationen aus und fügen eine neue Nachricht hinzu, die einen Link auf eine kompromittierte Webseite mit einem .zip-Archiv enthält. Diese .zip lädt Qbot nach und installiert die Malware auf dem Rechner. Aktuell stehen neben Gesundheitsorganisationen, Regierungsbehörden, Finanzinstitutionen, auch Einzelhandelsunternehmen auf der Angriffsliste von Qbot.

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

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

Fax: +49 (0) 234 9762-299

Angriffe werden immer professioneller

Neben Qbot sind zurzeit auffällig viele Remote Access Trojaner (RAT) aktiv. Mehr als 30 Prozent der abgewehrten Angriffe wurden mit AveMariaRAT oder njRAT ausgeführt. 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.

Insbesondere die aktuellen RAT-Kampagnen zeigen, dass der Trend hin zu immer professionelleren Cyberangriffen geht. Kriminelle agieren dabei verstärkt arbeitsteilig und bauen einzelne Bausteine als Malware-as-a-Service zu einer modularen Infektionskette zusammen. Eine genaue Analyse einer aktuellen Kampagne der Aggah-Gruppe zeigt, dass die Angreifer versuchen, Schutz- und Erkennungsmechanismen auf dem infizierten Rechner zu deaktivieren, nachdem der Nutzer ein schadhaftes Makro in einer Phishing-Mail aktiviert hat. Das initiale Skript schaut, welche Endpoint-Protection-Lösung auf dem System installiert ist und wählt dann das nächste Skript aus, um die Schutzlösung auszutricksen. Hinzu kommt, dass die Angreifer auch ihre Infrastruktur modularisieren, indem sie schädlichen Code auf der Text-Sharing-Plattform Pastebin speichern und von dort aufrufen.

„Gerade jetzt müssen sich Unternehmen verstärkt um den Faktor Mensch in der IT-Sicherheit kümmern. Die Homeoffice-Situation und die Pandemie setzen Mitarbeitende unter Stress und macht sie anfälliger für Angriffsversuche. Durch die Gleichzeitigkeit von Arbeit- und Privatleben ist die Konzentration bei vielen Angestellten geringer, sodass sie schneller eine gefälschte Mail anklicken. Auch, weil der direkte Austausch mit den Kollegen fehlt, die man um Rat fragen könnte“, 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

E-Mail: presse@gdata.de

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

Fax: +49 (0) 234 9762-299