

G DATA Bedrohungsanalyse: Weitere Verdopplung der Cyberattacken im dritten Quartal

Angreifer nutzen immer noch die Corona-Pandemie aus, um Unternehmen und Privatanwender zu attackieren

Bochum (Deutschland), 19. November 2020

Im dritten Quartal des Jahres mussten die Cyber-Defense-Spezialisten aus Bochum fast doppelt so viele Cyber-Angriffe wie im zweiten Quartal 2020 abwehren. Mit großen Kampagnen attackieren Angreifer sowohl private Rechner als auch Firmennetzwerke. Besonders aktiv: Malware wie Emotet, Agent Tesla, Gozi oder RanumBot. Die Verunsicherung der Menschen in der Corona-Krise sowie die weiterhin hohe Zahl an Mitarbeitern im Homeoffice lassen Cybercrime boomen.



Die aktuelle Bedrohungsanalyse von G DATA CyberDefense zeigt, dass die Zahl der Cyberattacken auch im dritten Quartal weiter angestiegen ist. So hat sich die Zahl der abgewehrten Angriffsversuche innerhalb von drei Monaten fast verdoppelt – ein Plus von 99,1 Prozent zwischen dem zweiten und dritten Quartal.

„Die Corona-Krise hat den digitalen Wandel massiv beschleunigt. Aber bei diesem hohen Tempo hält die IT-Sicherheit in vielen Fällen nicht Schritt. Mittlerweile arbeiten viele Angestellten schon seit mehr als sechs Monaten im Homeoffice. Firmen haben am Anfang der Pandemie den Fokus auf die Funktionalität gelegt. Business Continuity hatte zunächst verständlicherweise oberste Priorität. Jetzt muss aber die IT-Sicherheit in den Fokus der Verantwortlichen rücken und umfassende Maßnahmen zur Abwehr von Cyberangriffen in Angriff genommen werden“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense.

Cyberkriminalität ist ein Saison-Geschäft

Insbesondere im Juli 2020 waren Cyberkriminelle sehr aktiv. Gegenüber Juni stieg die Zahl der Angriffsversuche um 176,1 Prozent – der höchste Zuwachs innerhalb von vier Wochen während des aktuellen Jahres. Nach dem starken Anstieg im Juli hat sich die Lage im August und September etwas beruhigt. So verzeichneten die Security-Analysten in Bochum zuletzt einen Rückgang der Cyberattacken. Von August auf September sank die Zahl um 27,5 Prozent.

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

Von Entspannung kann aber keine Rede sein: Die Zahlen bewegen sich weiterhin auf einem hohen Niveau und sind gerade im Vergleich zum Jahresanfang extrem hoch. Der Rückgang an Angriffen zeigt: Cyberkriminalität ist auch ein saisonales Geschäft. Gerade zu Beginn der Urlaubszeit im Sommer steigt die Zahl der Angriffsversuche traditionell an. So versenden Kriminelle beispielsweise Massenmails mit vermeintlich günstigen oder gefälschten Urlaubsangeboten. In diesem Jahr war auch das Versenden falscher Warn-Hinweise in Bezug auf Reisen und Corona eine Masche der Täter. Ein weiterer Grund für den Rückgang: Immer wieder nehmen Angreifer Anpassungen an der Schadsoftware oder ihrer IT-Infrastruktur vor, bevor sie eine nächste Angriffswelle starten. Ihr Ziel: Die Effizienz zu verbessern, um den Profit zu steigern.

Altbekannte Schadprogramme

Insgesamt konnten die Analysten bei G DATA 200 aktive Malware-Familien im dritten Quartal identifizieren. Besonders aktiv waren Gozi, Agent Tesla, Emotet sowie Ranumbot/Glupteba. Schadsoftware, die bereits seit längerem ihr Unwesen treibt und hohe Schäden verursacht.

So existiert **Gozi** bereits seit 2006. Gozi dringt in der Regel über Phishing-Mails in die Systeme der Opfer ein und verfügt über Screen-Capture- und Keylogging-Funktionen. So leitet die Schadsoftware Anmeldedaten, die in Browsern und Mail-Programmen gespeichert sind, ab.

Nach einer Pause im Frühjahr dieses Jahres hat **Emotet**, die Allzweckwaffe der Cyberkriminellen, wieder Fahrt aufgenommen. Das Schadprogramm ist mittlerweile sehr komplex. Von seiner ursprünglichen Funktion – dem Manipulieren von Onlinebanking-Transaktionen – ist mittlerweile nichts mehr übrig. Dafür hat sich Emotet auf andere Bereiche verlegt. Vom Abgreifen von Mailkontakten zur Erstellung detaillierter Kommunikationsprofile von Angriffsopfern bis hin zur Rolle als Türöffner für andere Schadprogramme.

Agent Tesla ist seit mehr als sechs Jahren aktiv und ein ausgeklügelter Keylogger und Informationsstealer, der Tastatureingaben aufzeichnet, Daten mitliest, Screenshots erstellt und Zugangsdaten abfängt. Zurzeit verknüpfen Angreifer diese Attacken mit aktuellen Social-Engineering-Methoden und nehmen in Phishing-Mails Bezug auf Covid-19, sodass sie immer noch großen Schaden anrichten.

RanumBot deaktiviert auf einem infizierten System alle Sicherheitsdienste und die Windows-Firewall und öffnet so eine Tür für weitere Schadsoftware wie etwa den Trojaner Glupteba. Darüber hinaus ändert die Malware die Standardeinstellungen in der Windows-Registry, um bei jedem Neustart von Windows automatisch aktiviert zu werden.

„Die IT-Sicherheitslage bleibt weiterhin kritisch. Cyberkriminelle entwickeln immer wieder neue Angriffsszenarien, mit denen sie auch versuchen, Schutzmaßnahmen zu umgehen. Es reicht heute nicht mehr aus, sich nur auf technologische Schutzmaßnahmen zu verlassen. Damit lassen sich insbesondere Angriffe durch Social Engineering kaum verhindern. Daher müssen Firmen ihre Mitarbeiter in die Lage versetzen, Cyberattacken frühzeitig zu erkennen. Security Awareness Trainings und Phishing-Simulationen sind ein guter Weg, die IT-Sicherheit ganzheitlich anzugehen und zu verbessern“, sagt Tim Berghoff.

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