

Emotet ist zurück

Zusammenschluss von mehr als 60 internationalen Technologieunternehmen, um Menschen und Unternehmen vor Cyberkriminalität zu schützen.

Bochum (Deutschland), 16. November 2021

Nach einem koordinierten Takedown durch Strafverfolgungsbehörden im Januar 2021 wurden jetzt erstmals wieder neue Varianten der Emotet-Schadsoftware gesichtet – wie eine aktuelle Analyse von G DATA zeigt. Emotet war über Jahre hinweg eine Allzweckwaffe des Cybercrime.

Emotet gilt als eine der gefährlichsten Malware-Familien, weil sie insbesondere als Brückenkopf für Cyberangriffe auf Unternehmen aller Größen genutzt wird. Nach einer initialen Infizierung mit dem Schadprogramm folgte in der Vergangenheit oft eine Erpressung des kompromittierten Unternehmens mit einem Verschlüsselungstrojaner.



„Der international koordinierte Takedown von Emotet hat über viele Monate Wirkung gezeigt und viele Opfer vor Schaden bewahrt. Dazu gratulieren wir allen beteiligten Behörden. Unsere aktuellen Analysen zeigen gleichwohl, dass Emotet jetzt zurückgekehrt ist – das zeigt die manuelle Analyse aktueller Schadsoftware-Samples“, sagt Dr. Tilman Frosch, Geschäftsführer der G DATA Advanced Analytics.

Das neue Emotet-Sample fällt durch mehrere technische Ähnlichkeiten zu der ursprünglichen Schadsoftware auf. Insbesondere ein Vergleich des Quellcodes zeigt ähnliche Strukturen. Es gibt aber auch Unterschiede: Im Gegensatz zu den früher bekannten Emotet-Varianten wird der Netzwerkverkehr zwar weiterhin verschlüsselt, es wird jedoch nun HTTPS mit einem selbst-signierten Zertifikat genutzt.

Bisher sind keine nennenswerten Spam-Aktivitäten im Zusammenhang mit Emotet aufgefallen. Emotet nutzt nach derzeitigen Erkenntnissen die Infrastruktur der Trickbot-Malware, das eigene Botnetz wurde im Zuge des Takedowns offenbar nachhaltig zerstört. G DATA Kunden sind vor den neuen Emotet-Varianten geschützt.

UPDATE: Die ersten Spamaktivitäten sind angelaufen - derzeit wird Emotet in *.docm und *.xlsm- sowie passwortgeschützten ZIP-Anhängen verteilt.

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

Pressemitteilung

Ein detaillierter englischsprachiger Blogpost mit Indicators of Compromise findet sich im Blog unserer Tochtergesellschaft G DATA Advanced Analytics: Guess who's back – cyber.wtf



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