

Emotet-Takedown zeigt Wirkung - was Unternehmen jetzt tun sollten

Bochum (Deutschland), 10. Februar 2021

Der international koordinierte Takedown des Emotet-Botnetzes zeigt Wirkung: Im Emotet-Tracking von G DATA CyberDefense ist es aktuell sehr ruhig. Wie Unternehmen die Verschnaufpause jetzt nutzen sollten.



Emotet ist seit dem international koordinierten Takedown der Command- und Control-Server der Allzweckwaffe des Cybercrime vorläufig lahmgelegt - das zeigt eine aktuelle Auswertung von G DATA CyberDefense. Die Aktion der Strafverfolgungsbehörden vor zwei Wochen hatte weltweit für Aufsehen gesorgt. G DATA beobachtet Emotet seit Jahren intensiv, um seine Kunden bestmöglich zu schützen.

„Der Emotet-Takedown ist ein großer Erfolg gegen die organisierte Kriminalität, das zeigen unsere aktuellen Zahlen deutlich. Die Allzweckwaffe des Cybercrime sticht nicht mehr“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Emotet gehörte zu den aktivsten Schadsoftware-Familien - im vergangenen Jahr hatte G DATA über 800.000 Versionen der Malware identifiziert. Seit dem 27. Januar 2021 ist die Aktivität jedoch fast auf null zurückgegangen. Verbleibende identifizierte Samples stammen aus dem in der Branche etablierten Sampletausch. Neuinfektionen mit Emotet sind daher derzeit eher unwahrscheinlich.

Unternehmen sollten Emotet jagen

In vielen Unternehmen dürfte es aktuell jedoch noch stille, bislang unentdeckte Emotet-Infektionen geben. Diese sind weiterhin gefährlich, weil Cyberkriminelle darüber andere Schadsoftware wie Trickbot oder Qbot nachinstallieren können. Diese Malware wird in der Regel dazu genutzt, alle Daten im Unternehmensnetzwerk zu verschlüsseln und nur gegen Zahlung einer Erpressersumme wieder freizugeben.

Insbesondere Unternehmen, die in den vergangenen Wochen eine Warnung vom BSI erhalten haben, sollten diese unbedingt ernst nehmen und ihr Netzwerk genau prüfen. Ein guter Ansatzpunkt ist die Auswertung der Firewall-Logs – bei Bedarf mit externer Unterstützung. Zur Untersuchung der Clients selbst sollte eine Endpoint-Protection mit In-Memory-Scanner

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

eingesetzt werden. Diese bietet die beste Chance, bestehende Infektionen zu erkennen.

„Unternehmen sollten die Verschnaufpause für intensives Emotet-Hunting nutzen. Wer eine stille Infektion im Netzwerk hat, ist nach wie vor gefährdet. Gerade in der aktuellen wirtschaftlichen Lage kann sich wohl kaum ein Unternehmen eine Ransomware-Attacke wirklich leisten“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Emotet war besonders deshalb sehr gefährlich, weil die Malware sich über täuschend echte Phishing-Mails verbreitete. Dabei nutzte sie das Mailpostfach bereits infizierter Opfer, um auf bestehende Konversationen zu antworten. Zudem ist die Schadsoftware technisch in der Lage, im Browser gespeicherte Passwörter auszulesen und diese Informationen für weitere Angriffe zu benutzen.

Zu den Hintergründen von Emotet finden Sie in unseren Blogbeiträgen [Emotet: G DATA erklärt die Allzweckwaffe des Cybercrime](#) und [Emotet: Wie eine Emotet-Infektion in Unternehmen abläuft](#) weitere Informationen.



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