Sicherheit - Artikelübersicht, Netz - Artikelübersicht, Server - Artikelübersicht, Artikel zum tag: protokolle

Tool zur Erkennung der Infektion mit EMOTET

Der Heise-Verlag berichtete über ein nützliches Tool, welches vom CERT Japan veröffentlicht wurde https://www.heise.de/security/meldung/EmoCheck-Neues-Tool-kann-Emotet-Infektionen-aufspueren-4652554.html.

Das Tool mit dem Namen EmoCheck kann auf Github heruntergeladen werden: https://github.com/JPCERTCC/EmoCheck/releases. Es steht als ausführbare Datei (.exe) für x86 und x64 Windows Systeme zur Verfügung. Eine Installation o. Ä. ist nicht notwendig. Nach der Ausführung erstellt es ein Logfile. Der Check dauert nur einen kurzen Moment und stellt direkt klar, ob Ihr System befallen sein

Wenn das Tool anzeigt, dass ein Befall vorliegt, wenden Sie sich bitte umgehend an Ihren Administrator oder das Rechenzentrum an beratung@rz.uni-freiburg.de.

Weitere Informationen

Die Gefahr, welche von der Malware ausgeht, ist nicht zu unterschätzen. Deswegen haben Sie bitte keine Hemmung, sich an das Rechenzentrum zu wenden, auch wenn Sie sich unsicher sein sollten.

Emotet kann unbemerkt die Systeme befallen. Die häufigste Infektion geht von E-Mail Anhängen aus. Die Masche bei Emotet ist sehr heimtückisch. Betroffene können Mails mit einem .doc Anhang von einem bekannten Mailkontakt bekommen. Inhaltlich sind die Mails auch von regulären dienstlichen/geschäftlichen Mails kaum zu unterscheiden, weswegen oftmals keine Zweifel in Bezug auf die angehängten Files entstehen.

Achten Sie deswegen auch darauf, dass Sie keine .doc oder .docx Files per Mail versenden bzw. stattdessen die Dokumente als PDF versenden. Umgekehrt bitten Sie Ihren Kontakt, von welchem Sie ein .doc oder .docx File erhalten haben, dass dieser Ihnen ein PDF zusendet.