Geodo

Der CERT-Bund hat von einer externen vertrauenswürdigen Quelle Informationen zu Systemen in Deutschland erhalten, welche mit dem Online-Banking-Trojaner "Geodo" (aka "Cridex") infiziert sind. Die Schadsoftware wird per Spam-Mail über kompromittierte Mailaccounts als angebliche Rechnung zum Beispiel im Namen von Telekommunikationsunternehmen verbreitet.

- malpedia: Emotet aka: Geodo, Heodo [1]

Links

[1] https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/geodo/