# Emotet, Trickbot, Ryuk – ein explosiver Malware-Cocktail

By Thomas Hungenberg

Published: 2019-11-06 · Archived: 2026-04-06 00:32:02 UTC

Emotet hat in den vergangenen Monaten für viele Schlagzeilen gesorgt. Infektionen mit Emotet und insbesondere darüber nachgeladene weitere Schadprogramme wie Trickbot oder die im Anschluss in den Netzwerken der Opfer ausgerollte Ransomware Ryuk führten bereits weltweit und auch in Deutschland zu enormen finanziellen Schäden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte mehrfach vor Emotet; das US-CERT bezeichntete Emotet als eines der "kostenträchtigsten und zerstörerischsten" Schadprogramme.

Thomas Hungenberg studierte Angewandte Informatik und Kommunikationstechnik und verfügt über mehr als 20 Jahre Berufserfahrung im Bereich IT-Sicherheit. Seit 2003 ist er als Incident Handler und Security Analyst im Referat CERT-Bund des Bundesamts für Sicherheit in der Informationstechnik (BSI) tätig und arbeitet mit Analysten weltweit bei der Analyse von Schadprogrammen und Botnetzen zusammen.

In einer Vielzahl von Unternehmen, Krankenhäusern, Einrichtungen der kommunalen Verwaltungen und anderen Organisationen kam es zu großflächigen oder kompletten Ausfällen der IT-Infrastruktur. Dies hatte vieltägige Produktionsausfälle zur Folge, Dienstleistungen konnten über einen längeren Zeitraum nicht erbracht werden und Mitarbeiter mussten in den Zwangsurlaub geschickt werden. Nicht berichtet wird üblicherweise über die Schäden bei tausenden ebenfalls von Emotet betroffenen Privatnutzern durch den Missbrauch ausgespähter Zugangsdaten oder Online-Banking-Betrug.

## Wie alles begann

Emotet basiert auf einer Weiterentwicklung des Online-Banking-Trojaners Cridex (auch Bugat oder Feodo genannt). Der Name Emotet wurde von dem IT-Sicherheitsdienstleister Trend Micro geprägt, der im Juni 2014 als Erster dazu berichtete. Verbreitet wurde die erste Version von Emotet – auch als Geodo bezeichnet – über Spam-Kampagnen mit gefälschten Rechnungen oder angeblichen Mitteilungen von Banken. Die Spam-Mails enthielten dabei das Schadprogramm entweder direkt im Dateianhang (teilweise in ein ZIP-Archiv verpackt) oder die Spam-Mails enthielten einen Link, über den der Empfänger die angebliche Rechnung bzw. Mitteilung herunterladen sollte. Durch doppelte Dateiendungen wie ".pdf.exe" wurde verschleiert, dass es sich bei dem Anhang beziehungsweise der heruntergeladenen Datei um ein ausführbares Programm handelte.

Geodo führte sogenannte "Man-in-the-Browser"-Angriffe auf das Online-Banking der Opfer durch, indem es sich in den Webbrowser einklinkte und vom Nutzer eingegebene Anmeldedaten ausspähte. Dabei standen Kunden deutscher und österreichischer Banken im Fokus der Angreifer, die deshalb ihre Spam-Mails primär an E-Mail-Adressen mit den Endungen .de und .at versendeten. Zusätzlich spähte Geodo auf den Opfersystemen Zugangsdaten für E-Mail-Konten aus, um über diese anschließend weitere Spam-Mails zur Verbreitung des Schadprogramms zu versenden. Dabei verwendete es – wie auch heutige Emotet-Versionen noch – eine mitgelieferte Kopie des Passwort-Recovery-Tools Mail PassView des Herstellers NirSoft, um in E-Mail-

Programmen wie Microsoft Outlook, Windows Mail oder Mozilla Thunderbird gespeicherte Zugangsdaten zu extrahieren.

## Die weitere Entwicklung

Die zweite Generation von Emotet – welche von den Tätern ab Herbst 2014 in Umlauf gebracht wurde – hatte einen neuen, modularen Aufbau. Eine Infektion installierte zunächst nur eine Kernkomponente des Schadprogramms, welche dann Module für verschiedene Schadfunktionen nachladen konnte. Dies umfasste Module für Angriffe auf das Online-Banking, das Ausspähen von Zugangsdaten aus E-Mail-Clients und Webbrowsern, das Auslesen von Outlook-Adressbüchern, den Spam-Versand und zur Durchführung von DDoS-Angriffen. Das Banking-Modul nutzte jetzt (wie bereits einige andere Banking-Trojaner-Familien) sogenannte Web-Injects. Diese fügten während des Online-Bankings im Webbrowser des Nutzers unter anderem dynamisch zusätzliche Eingabefelder zur Abfrage von TANs ein, um damit im Hintergrund Überweisungen auszuführen. Außerdem unterdrückten sie Sicherheitswarnungen der Bank.

Mit der dritten Version von Emotet – welche ab Januar 2015 verbreitet wurde – gerieten auch Kunden Schweizer Banken in den Fokus der Täter, die deshalb ihre Spam-Kampagnen auf Schweizer Nutzer ausweiteten. Zusätzlich wurden die Schutzfunktionen des Schadprogramms gegen Detektion und Analyse verbessert.

---