Emotet: Was Sie über die Schadsoftware wissen sollten…

Emotet= Emotet ist ein sog. Trojaner, der vor allem über Spam-E-Mails verbreitet wird. Die infizierte Mail enthält z.B. ein bösartiges Skript, ein Dokument mit aktivierten Makros oder bösartige Links.

Kommt per E-Mail

Ob getarnt als vermeintlich harmlose Bewerbung, Nachricht von einem Ihrer privaten Kontakte oder Rundschreiben von der Firmenleitung: Startpunkt einer Infektion ist in aller Regel eine schadhafte E-Mail. Oft enthält diese z.B. eine manipulierte Word-Datei.

Kapert Ihr Adressbuch

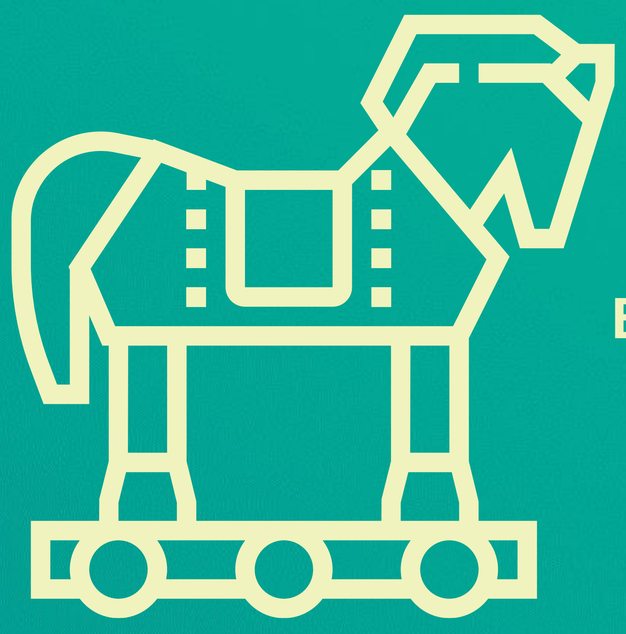
Emotet ergreift Besitz von Ihrem Adressbuch und versendet sich selbst an alle dort auffindbaren Kontakte, also z.B. Ihre Freunde, Familienangehörigen, Mitarbeiter oder Kunden.

Stiehlt Ihre Identität

In den E-Mails an Ihre Kontakte wird Ihr richtiger Name angezeigt. Da Ihr E-Mail-Konto gekapert wurde, sehen die E-Mails nicht wie Spam, sondern wie ganz normale E-Mails von Ihnen aus – dies verleitet Ihre Kontakte dazu, selbst auf den Schadcode hereinzufallen.

Installiert weitere Malware

Häufig lädt Emotet auch weitere Schad-software nach, z.B. sog. Banking-Trojaner oder auch Erpressungssoftware, die Ihren Computer sperrt bzw. Daten löscht.



Tritt in vielen Gestalten auf

Der Code von Emotet wird bei jedem neuen Abruf leicht abgeändert, um einer Erkennung durch signaturbasierte Virenscanner zu entgehen; man bezeichnet Emotet daher auch als polymorphen Schadcode.

Aktualisiert sich selbst

Emotet kann vom Angreifer „ferngewartet“ werden, d.h. es können unbemerkt Updates aufgespielt werden, die neue Befehle ausführen oder die Mechanik des Programms so verändern, dass es unentdeckt bleibt.

Breitet sich eigenständig aus

Die Schadsoftware ist vor allem auch deshalb so gefährlich, weil sie versucht, andere Rechner zu infizieren, die sich im gleichen Netzwerk befinden.

Nimmt jeden ins Visier

Egal ob Privatperson, Kleinunternehmen, Multinationaler Konzern oder Behörde: alle sind bereits Opfer von Emotet geworden. Gerade diese Vielseitigkeit macht den Virus so gefährlich und unberechenbar.

…und wie Sie sich davor schützen können.

Vorsicht bei Links oder Anhängen

Auch wenn Ihnen der Absender bekannt vorkommt: klicken Sie auf keinen Fall unbedacht auf Anhänge oder auf in Mails enthaltene Links. Bei einer verdächtigen E-Mail sollten Sie den Absender anrufen und sich die Echtheit bestätigen lassen.

Alle Systeme updaten

Halten Sie alle Betriebssysteme (z.B. Windows) und Softwareprogramme (Microsoft Office etc.) stets auf dem aktuellsten Stand. Folgen Sie hierfür den Anweisungen und Anleitungen Ihrer IT-Abteilung.

Im Ernstfall schnell informieren

Sollten Sie betroffen sein, schalten Sie den Rechner aus und informieren Sie umgehend Ihre IT-Abteilung. Auch sollten Sie alle Kontakte aus Ihrem Adressbuch über den Vorfall informieren, um diese vorzuwarnen, nicht auf „Ihre“ E-Mails zu klicken.

Weitere Information zu Phishing und Security-Awareness unter:

www.allianz-fuer-cybersicherheit.de

Allianz für Cyber-Sicherheit Partner

www.sosafe.de

SoSafe Cyber Security Awareness