Neuer Geldautomat-Trojaner: Und plötzlich ist die Karte weg

Sicherheitsexperten warnen vor einer neuen Masche von Hackern: Mit manipulierten Geldautomaten können die Kriminellen Geldkarten klauen und das Konto leerräumen.

Hacker haben es auf Geldautomaten abgesehen © Only5/iStockphoto


Christoph Fröhlich

Gefälschte Bahn-Tickets, manipulierte Werbebanner, verseuchte Whatsapp-Links: Hacker lassen sich viel einfallen, um die privaten Daten ihrer Opfer auszuspähen. Besonders begehrt sind die Konto- und Kreditkartendaten. Doch während viele Nutzer beim Online-Banking extreme Vorsicht walten lassen, agieren sie am Geldautomaten vergleichsweise unbedarft. Solange niemand die PIN ausspäht, ist schon alles in Ordnung - oder? Diese Leichtgläubigkeit könnte bald teuer werden, glauben Experten: Die Sicherheitsforscher von FireEye haben eine neue Schadsoftware entdeckt, mit der gezielt Geldautomaten angegriffen werden sollen.

Geld weg, Karte weg

Der neuartige Trojaner hört auf den Namen "Backdoor.ATM.Suceful", der auf einen Schreibfehler (Suceful statt Successful) innerhalb des Programmcodes zurückgeht. Der Schädling ist äußerst mächtig: Wurde ein Geldautomat infiziert, können sämtliche Daten aus den eingeführten Karten ausgelesen und die Konten vollständig leergeräumt werden. Bei Bedarf werden die Karten sogar direkt vom Automaten eingezogen. In

solch einen Fall dürften Nutzer zunächst wohl eher von einer technischen Panne als von einer gezielten Attacke ausgehen. Das verschafft den Kriminellen mehr Zeit.

Kontrolliert wird die Schadsoftware über das Zahlenfeld am Geldautomat, schreiben die Experten. Außerdem legt der Trojaner die internen Schutz-Mechanismen des Geldautomaten lahm, damit diese keinen Alarm schlagen.

"Schockierend"

Entdeckt wurde der Geldautomat-Trojaner eher durch einen Zufall, weil die Kriminellen die Software bei "Virus Total" hochgeladen haben, einer Art Online-Virenscanner, mit der man Dateien überprüfen kann. So wollten die Hacker vermutlich überprüfen, ob ihre Software von den einschlägigen Virenwächtern erkannt wird.

Die Masche ist nicht neu, bereits in den Jahren 2013 und 2014 wurden manipulierte Geldautomaten in Russland und Mexiko endeckt. Der Zeitstempel der neuen Software ist auf den 25. August datiert, fertig ist die Software laut "FireEye" noch nicht. Derzeit befindet sich "Backdoor.ATM.Suceful" noch in der Entwicklung. Doch schon jetzt sei der Trojaner "schockierend" und biete Features, die "noch nie zuvor in einer Geldautomaten-Schadsoftware" auftauchten.

Mit dem Trojaner können Geräte verschiedener Hersteller angegriffen werden, etwa von Diebold und NCR. Von beiden stehen auch in Deutschland Automaten.