

Das Hacker-Kartell

Trojaner, Datenklau, Geldwäsche: Wie Internetbetrüger nichts ahnende Nutzer ausrauben

Unter Hackern stellen sich viele Laien immer noch pfiffige Computerkids vor, die sich in ihrer Freizeit übers Netz Zugang zu anderen Rechnern verschaffen. Aber aus der romantischen Hobbyhackerei ist längst eine milliardenschwere, international organisierte Betrugsindustrie geworden, die arbeitsteilig vorgeht. Insbesondere das Geschäft mit infizierten Websites floriert – fast ein Prozent aller Seiten im Netz verbreitet inzwischen ohne das Wissen ihrer Besitzer Trojaner-Software, oft

trifft es auch populäre Adressen wie die Fan-Sites von Paul McCartney und Britney Spears oder die Homepage von *Business Week*. Trojaner, die auf diese Weise auf den Computer gelangen, sind kleine Meisterwerke. Sie modifizieren sich selbst automatisch, damit Antivirensoftware sie nicht aufspüren kann. Dass die Kontozugangsdaten dann bei Betrügern landen und nicht bei der Hausbank, können auch versierte Surfer kaum erkennen, die auf eine plumpere »Phishing«-Attacke (siehe Fall Nr. 2) nicht mehr hereinfallen würden.

Durch die Aufklärungsarbeit von Sicherheitsexperten, die das Treiben in den Hackerforen beobachten, weiß man, wie die Cyberkriminellen Daten zu Geld machen. Die Geldwäscheexperten in der Branche (die sich die Einkünfte im Verhältnis 80 zu 20 mit den Trojaner-Programmierern teilen) rekrutieren mit Tricks wie gefälschten Jobangeboten Dumme, die das Geld aus betrügerischen Transaktionen über internationale Transferdienstleister wie Western Union an Hintermänner schicken. In Onlinejobbörsen etwa werden Geldboten rekrutiert, die glauben,

dass sie im Namen einer Hilfsorganisation Geld von einem Konto aus den USA in die Ukraine schicken oder einem Maler aus Europa helfen, seine Bilder in Übersee zu verkaufen. Ende November meldete das Bundeskriminalamt die Festnahme von Mitgliedern einer Cybercrime-Bande namens Elite Crew in Deutschland und Österreich. Doch trotz solcher Fahndungserfolge läuft das Geschäft weiter – und längst braucht man keine Programmierkenntnisse mehr, um bei den dunklen Machenschaften dabei sein zu können.

1. Trojaner-Opfer Ellen

Hacker 1 programmiert Trojaner und schleust sie in Internetseiten ein – ein Fall war zum Beispiel die Homepage von Paul McCartney



Ellen ist ein Fan von **Paul McCartney**, deshalb besucht sie seine Website. Dort fängt sie sich ohne ihr Zutun einen **Trojaner** ein, der sich nun auf ihrem Computer eingenistet hat

2. Phishing-Opfer Klaus



Klaus bekommt eine **E-Mail**, die scheinbar von seiner Bank stammt. Er klickt auf einen Link in der Mail, der ihn zu einer gefälschten Version der Website von »Deine Bank« führt

Hacker 2 verschickt **Massen-E-Mails**, die so aussehen, als kämen sie von einer Bank



Ein **Trojaner** ist ein kleines Computerprogramm, das ohne Wissen der Nutzer selbstständig auf ihren Computern läuft. Er kann die befahlenen Rechner nach interessanten Daten durchsuchen oder eine Hintertür für Hacker öffnen



Ellen möchte **Geld überweisen**. Der Trojaner manipuliert die Seite der Bank, ergänzt sie zum Beispiel um Eingabefelder, in die Ellen ihre Bankdaten einträgt. Der Trojaner leitet diese Daten sowie andere, die er auf Ellens Rechner gefunden hat, weiter an den Hacker



Klaus denkt, er befände sich auf der Website seiner Bank, und gibt nichts ahnend seine **Zugangsdaten** ein: Kontonummer, Passwort, eine Transaktionsnummer (TAN) für die Überweisung – alle Daten landen beim Hacker, Klaus' Überweisung wird nicht ausgeführt

Hacker 3 hat die **Website** gebaut, die der echten Bankseite täuschend ähnlich sieht

Das **Golden Cash Network** ist ein Marktplatz für Cyberkriminelle jeder Art. Hier kann man gestohlene **Bankdaten** en masse kaufen oder auch den direkten Zugriff auf Hunderte infizierte Computer (**Botnet**) mieten

Geldwäscher 1 überweist mit den gestohlenen Daten von Ellen oder Klaus Geld auf das Konto des arglosen Geldboten



John ist auf **Jobsuche** und findet im Netz ein Angebot der Firma »AutoPay«. Er soll im Auftrag der Firma Geld ins Ausland weiterleiten

John erhält eine **Überweisung** von Ellens oder Klaus' Konto, die Geldwäscher 1 getätigt hat, und leitet sie mit dem Transferdienst »Eastern Union« an eine ausländische Adresse weiter. Er ahnt nicht, dass er an einem Betrugsdelikt beteiligt ist



Geldwäscher 2 geht zu einem »Eastern-Union«-Büro irgendwo in der Welt und hebt das Geld bar ab. Dazu muss er nur einen (meist gefälschten) Ausweis vorlegen. Die Spur des Geldes ist damit verwischt

3. Geldbote John