Kreditkartendaten als heiße Ware

Von Klaus Jetter

Virtuelle Währungen mögen nicht für kriminelle Zwecke erdacht worden sein, sie werden aber gerne für sie genutzt – etwa zur Bezahlung gestohlener Kreditkartendaten. Der Markt mit ihnen ist mittlerweile millionenschwer. Und mobile Endgeräte, die von Banken verstärkt für neue Sicherheitsanwendungen genutzt werden, könnten eben dadurch zum Einfallstor für neue Angriffszenarien werden. Red.

Raffinierter, gefährlicher, professioneller – so könnte man die Entwicklung der Schadsoftware-Branche beschreiben. Waren die Programmierer der sogenannten Malware bis zu den frühen 2 000er Jahren noch von Ruhm und Anerkennung getrieben, geht es heute vielmehr um Profit, Diebstahl und Manipulation. Da das Geschäft mit Viren, Trojanern und Co. sehr lukrativ ist, weiten die Online-Schurken ihre Attacken kontinuierlich aus. Ein beliebtes Ziel: Kreditkartendaten. Dahinter steckt eine komplette Industrie, die mit ausgeklügelten Geschäftsmodellen und Infrastrukturen arbeitet. Über die Größe dieses Marktes lässt sich nur spekulieren. Experten gehen aber davon aus, dass er millionenschwer ist.

Der zweifelhafte Aufstieg der professionellen Malware-Branche begann 2002, als Hacker eine Schadsoftware mit dem konkreten Ziel entwickelten, Daten zu stehlen. Seitdem wachsen die Angriffe stetig und damit auch die Zahl der Hacker sowie der Abnehmer. Heute sind rund 70 Prozent aller Malware-Einsätze profitorientiert. Andere Motive sind beispielsweise Rache oder Abenteuerlust.

Das Geschäft mit der Malware

Den Schaden dieser Attacken beurteilen die Sicherheitsexper-ten mit Hilfe der „Payload": Je größer diese ist, desto höher der Schaden, den eine Software hinterlässt. Dabei unterscheiden sie vornehmlich vier Kategorien: harmlos, zerstörerisch, betrügerisch und manipulativ. Je mehr die Angreifer aufrüsten, desto besser werden auch die Schutzmaßnahmen. Das bedeutet für die Malware-Programmierer, dass sie wiederum mehr Arbeit und Energie in neue, komplexere Schadsoftware investieren müssen, um zum Ziel zu gelangen. Dieses Wettrüsten ist für beide Seiten mit einem immensen Aufwand und häufig mit hohen Kosten verbunden. Daher stellt sich die Frage: Wieso lohnt sich dieses Geschäft überhaupt für die Programmierer?

Zum Autor

Klaus Jetter ist Country Manager DACH der F-Secure GmbH, München.

Damit aus der Entwicklung von Schadsoftware ein Geschäft wird, müssen einige Bedingungen erfüllt sein. Neben dem Produzenten, der Zeit und Geld aufwendet, braucht es einen Abnehmer und die Möglichkeit zur Skalierung.

Über den Verkauf von Diebesgut wie E-Mail-Adressen oder Kreditkartennummern hinaus ist inzwischen eine klassische Wertschöpfungskette entstanden: Entwickler erschaffen die Malware, verkaufen diese an andere, die damit Infrastrukturen aufbauen, um sie dann wiederum an Endabnehmer zu vermieten oder zu verkaufen.

Bezahlung über virtuelle Währungen

Zu den kniffligsten Aspekten im Geschäftsmodell der Internetbetrüger gehören der Vertriebsweg und die Bezahlung. Denn ein indirekter Vertrieb oder gar Serviceleistungen wie der Kundendienst sind nicht möglich. Spezielle Foren – zum Beispiel als Gamer-Portal getarnt, oder Chat-Kanäle, sogenannte Internet Relay Chats (IRC) – vermitteln die digitale Hehlerware direkt an den Käufer. Online-Bezahlsysteme wie Paypal oder die klassische Banküberweisung kommen hierfür kaum in Frage, da sie eine Identitätsprüfung erfordern und die Hacker anonym bleiben wollen.

Aus diesem Grund nutzen sie Bezahlsysteme mit virtuellen Währungen wie Webmoney oder Bitcoins, bei denen die bloße

Anmeldung für die Registrierung ausreicht. Das Geld, das über die Online-Dienste transferiert wird, ist in der Regel eine Gegenleistung für E-Mail-Adressen, Wirtschaftsspionage und virtuelle Online-Güter oder stammt von Erpressungsopfern.

Handel mit Kreditkarten-„Dumps" und Hologrammen

Ein weiterer Grund, die oben genannten Bezahlsysteme zu nutzen, ist der Handel mit gestohlenen Kreditkartendaten. In einschlägigen Foren und IRC-Kanälen sind sie inzwischen bereits ab zwei US-Dollar pro Stück erhältlich und werden in der Regel in sogenannten Dumps angeboten. Diese beinhalten die Informationen auf dem Magnetstreifen, also Name, Nummer, Ablaufdatum und Prüfnummer.

Kriminelle stehlen die Daten über Trojaner, die die Nummern auf den PCs der Opfer ausspähen, oder durch gezielte Angriffe auf Kreditkarteninstitute, Online-Shops und Banken. Neben den Kreditkartendaten wechseln auf den einschlägigen Marktplätzen auch Informationen den Besitzer, die zur Herstellung einer gefälschten Kreditkarte nötig sind – etwa holografische Logos der Banken oder Kreditinstitute.

Ausgeklügelte Betrugsmodelle

Um das Geld einer gestohlenen Kreditkarte zu „waschen", bedienen sich die Angreifer häufig einer trickreichen Methode:

- Zuerst versteigert der Angreifer eine nicht vorhandene Ware, etwa eine hochwertige Kaffeemaschine, zu einem günstigen Preis bei einem Online-Auktionshaus. Mit dem Käufer vereinbart er, dass die Ware erst nach Eingang bezahlt werden muss. Als Zahlungsmethode wird die Zahlung über eine Online-Währung wie Webmoney vereinbart.

- Nun bestellt der Angreifer die Kaffeemaschine bei einem Online-Händler und zahlt dort mit den gestohlenen Kreditkartendaten. Als Lieferadresse gibt er die Adresse des Käufers an. Da der Käufer die ersteigerte Ware nun ordnungsgemäß und zu einem guten Preis erhält, ist die Wahrscheinlichkeit hoch, dass er den außergewöhnlichen Zahlungsweg über Webmoney akzeptiert und den Betrag überweist.

- Wenn dann der Kreditkarteninhaber den nicht autorisierten Umsatz auf seiner Kartenabrechnung bemerkt, beginnt die Rückabwicklung über das Kreditinstitut, den Online-Händler und den Käufer. In der Regel ist der Angreifer zu diesem Zeitpunkt schon längst mit dem Geld auf und davon.

Im Visier: mobile Helfer

Die Malware-Industrie nutzt nicht nur neue Bezahlmöglichkeiten wie Online-Währungen für ihre Zwecke, sondern auch technologische Trends. So verwundert es nicht, dass Mobiltelefone immer stärker

ins Visier der Angreifer rücken. So stieg etwa der Anteil von Android-Malware am gesamten mobilen Malware-Markt von 66 Prozent 2011 auf stolze 79 Prozent im letzten Jahr. Seit geraumer Zeit registrieren die Sicherheitsexperten auch vermehrt mobile Schadsoftware-Programme, welche die Drive-by-Download-Methode nutzen. Dabei infizieren Anwender ihren Rechner oder eben ihr mobiles Gerät unwissentlich durch den bloßen Besuch einer manipulierten Internetseite.

Selbst neue Verfahren von Banken, die Kunden bei Transaktionen besser absichern sollen, sind nicht vor Angriffen der Hacker gefeit. MTANs (mobile TANs) beispielsweise, die nur für eine Transaktion gültig sind und dem Nutzer pro Anfrage auf sein Mobiltelefon zugesendet werden, sollen besser schützen als die bisher genutzten TAN-Listen auf Papier. Doch dem ist leider nicht so, denn Cyberkriminelle haben auch hier bereits Wege gefunden, an diese Codes zu kommen und sie für ihre Zwecke zu missbrauchen.

Dabei wird mit dem Vertrauen der Bankkunden gespielt. Einer der aktuellen Fälle ist etwa ein Trojaner, der dem Kunden vorgaukelt, seine Bank hätte eine neue mobile Banking-App für ihn. Beim Herunterladen wird auf dem Mobiltelefon der Trojaner installiert, durch den dann die mobile TAN abgefangen und die Überweisung auf ein anderes Konto umgeleitet werden kann.

Noch haben die Angreifer ein relativ leichtes Spiel: Laut aktuellen Studien sind gerade einmal fünf Prozent der weltweit im Einsatz befindlichen Smartphones und Tablets mit einer Sicherheitssoftware geschützt. Besonders problematisch daran ist, dass das Handy zunehmend für eine sichere Verifizierung zum Beispiel bei der Wiederherstellung von E-Mail-Accounts oder bei TANs für das Online-Banking zum Einsatz kommt.

Mobile Malware könnte also die bisherigen Sicherheitsmechanismen ins Gegenteil verkehren und das Handy zum größten Einfallstor für Angreifer in die IT-Infrastruktur machen. Daher gilt es, den Hackern mit Wissen und Wachsamkeit zu begegnen.

Wer grundsätzlich versteht, wie die Angreifer arbeiten, kann mögliche Fallen oder auffälliges Verhalten seines Rechners schneller erkennen und Schäden minimieren. Umfangreiche Aufklärung und regelmäßige Schulungen für die Mitarbeiter sowie regelmäßige Updates und Aktualisierungen aller eingesetzten Anwendungen und Betriebssysteme senken die Gefahr von nicht identifizierten Sicherheitslücken. Unternehmensnetzwerke lassen sich effizienter und mit höherem Sicherheitsstandard verwalten.