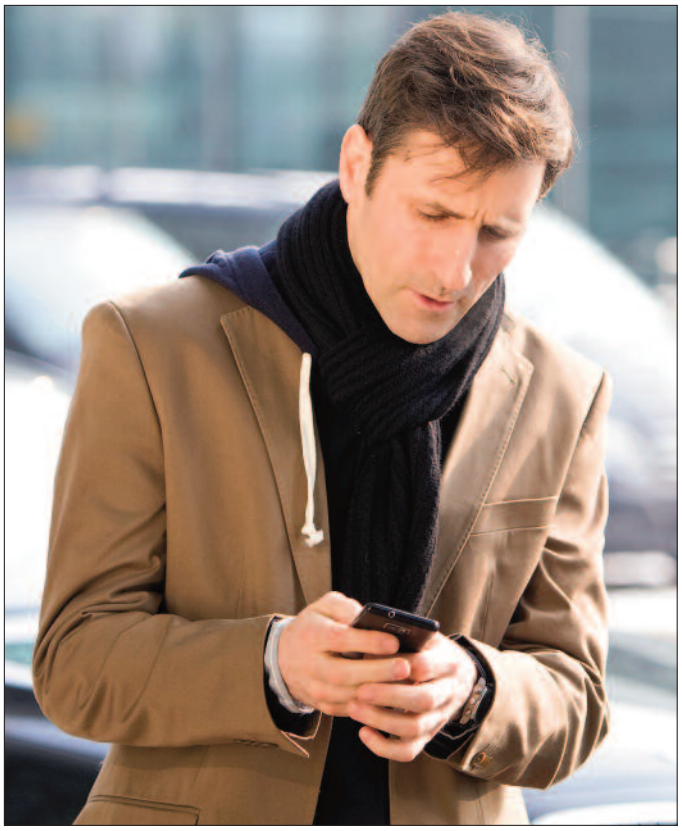
Bankkonten im Visier

Kriminelle versuchen mit Bank-Trojanern, die Konten ihrer Opfer zu plündern. Laut einer Studie von *Kaspersky Lab* und Interpol zielen drei von fünf Android-Schädlingen auf das Geld der Anwender ab.

Fast 200 Kunden einer italienischen Bank wurden innerhalb einer Woche um knapp 600.000 Euro geschädigt. Betrüger waren mit einem Onlinebanking-Trojaner an die Daten der Bankkunden gelangte und hatten unberechtigt Beträge zwischen 1.700 und 39.000 Euro von deren Konten überwiesen.

Die Cyber-Betrugskampagne mit dem Namen „Luuuk" wurde von Experten des Softwareherstellers *Kaspersky Lab* aufgedeckt. Sie entdeckten am 20. Januar 2014 den zur „Luuuk"-Kampagne gehörenden *Command-and-Control-Server (C&C)*. Zwei Tage nach Entdeckung des Servers hatten die Hintermänner von „Luuuk" sämtliche Spuren entfernt. „Wir haben die betroffene Bank sowie die Ermittlungsbehörden sofort nach Enttarnung des Servers informiert und sämtliche Hinweise zur Verfügung gestellt", sagte Vincente Diaz, Principal Security Researcher bei *Kaspersky Lab*.



Android-Nutzer werden immer öfter Opfer von Bank-Trojanern.

Die Geschädigten hatten die Schadsoftware beim Surfen auf Internetseiten heruntergeladen. Beim Onlinebanking wurde ihnen eine modifizierte Seite vorgegaukelt. Die Daten der Bankkunden wurden laut Experten vermutlich von einem Trojaner des Typs *Zeus* oder dessen Variationen *Citadel, SpyEye* oder *IceIX* automatisch beim Anmeldevorgang zum Onlinebanking abgefischt. Unbemerkt von den Kunden, konnten die Cyber-Kriminellen damit ihre betrügerischen Transaktionen abwickeln. Diese Vorgehensweise wird „Man-in-the-Browser" (MITB) genannt.

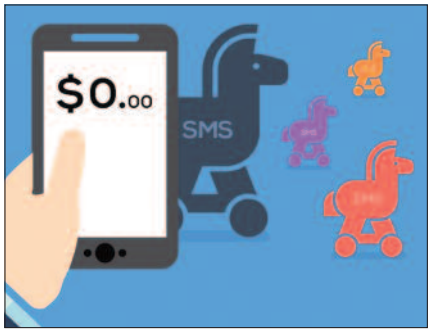
Hehlerei. Das Geld wurde auf Konten von Personen transferiert, die die Betrüger als „Finanzagenten" („Money Mules") oder dergleichen angeworben hatten. Die „Money Mules" wissen meist nicht, dass diese Uberweisungen kriminellen Hintergrund haben. Sie machen sich der Hehlerei schuldig. Die Betrüger teilten die „Money Mules" je nach Vertrauenswürdigkeit in vier Gruppen ein. Die erste Gruppe wickelte nur Zahlungen bis 2.000 Euro ab, die zweite Gruppe war für Überweisungen bis 3.000 Euro zuständig. Die dritte Gruppe für Überweisungen zwischen 15.000 und 20.000 Euro, eine vierte Gruppe für Beträge zwischen 40.000 und 50.000 Euro. Die Hintermänner der „Luuuk"-Kampagne versuchten sich mit dieser Vorgangsweise vor einem Betrug durch ihre Komplizen zu schützen. Der Betrag für die „Money Mules" wurde auf eigens eingerichtete Bankkonten überwiesen. 15 IBAN-Nummern wurden zu „Money-Mule"-Konten gefunden.

Studie. *Kaspersky Lab* und Interpol analysierten die weltweite Gefahrenlage für Besitzer mobiler Geräte mit Android-Betriebssystem.* Bei 588.000 Besitzern zwischen August 2013 und Juli 2014 Angriffe von Malware identifiziert, bei denen es Cyber-Kriminelle auf das Geld der Anwender abgesehen hatten. Damit waren sechsmal mehr Android-Nutzer betroffen als im Vergleichszeitraum 2012/13. In knapp zwei Prozent der Fälle sind Bank-Trojaner im Spiel. Der Großteil der Angriffe erfolgt mit SMS-Trojanern. Die Angriffe richteten sich mehrheitlich gegen Anwender in Russland. Es gab auch Betroffene in Deutschland, Frankreich, Spanien und Großbritannien.

Cyber-Kriminelle können mit SMS-Trojanern die Bankdaten der Anwender sowie deren Kartennummern oder Zugangsdaten für das Online-Banking erbeuten. Infizierte mobile Geräte versenden selbstständig und unbemerkt Nachrichten an kostenpflichtige Rufnummern (Premiumnummern). „Falls es einem Bank-Trojaner gelingt, auch nur ein einziges mobiles Gerät zu infizieren, erhalten Cyber-Kriminelle möglicherweise Zugriff auf das komplette Vermögen des Besitzers. Bei SMS-Trojanern müssen dagegen sehr viele Geräte infiziert werden, damit die Angreifer nennenswerte Beute machen können", erklärt Stefan Ortloff von *Kaspersky Lab*. „Außerdem nutzen noch nicht alle Besitzer ihre mobilen Geräte für Bank-Applikationen. Das ist der Grund für die großen Unterschiede bei den von uns ermittelten Angriffszahlen bei SMS- und Bank-Trojanern."

In den vergangenen Jahren konnten wir beobachten, dass mobile Cyber-Bedrohungen zunehmen und gleichzeitig immer komplexer und gefinkelter geworden sind und inzwischen auch einzelne Geräte angreifen können", berichtet Madan Oberoi, Director of Cyber Innovation & Outreach bei Interpol. „Mit dem stark wachsenden mobilen Markt wurde deutlich, dass sich Gefah-

FOTO: KASPERSKY LAB



Cyber-Kriminelle können mit SMS-Trojanern Bankdaten oder Zugangsdaten für das Online-Banking erbeuten.

ren dahingehend wandeln, dass neue Angriffsvektoren entstehen, die auf Smartphones und Tablets abzielen."

Schutz. Trojaner sind Schadprogramme, die vom Benutzer unbemerkt Aktionen auf dessen Computer oder mobilen Geräten ausführen. Dazu gehören unter anderen das Löschen, Sperren, Verändern und Kopieren von Daten. Die Opfer handeln sich Trojaner etwa durch Phishing ein, wenn sie einen Link anklicken in einer vermeintlichen E-Mail-Nachricht ihrer Bank. Im Zweifelsfall sollte man die Website der Online-Bank aufrufen, indem man deren Adresse in die Browserzeile eintippt, oder sich beim zuständigen Bankberater erkundigen. Es gibt Schädlinge, die den Browser des Opfers manipulieren, indem sie ihm eine Webseite seiner Online-Bank mit der Meldung anzeigen: Das Opfer habe irrtümlich eine Überweisung auf sein Konto bekommen und die Bank bitte um Rücküberweisung. Auch im Kontostand scheint der scheinbar zusätzliche Geldbetrag auf. Überweist der Kunde diesen Betrag auf ein angeführtes Konto, ist er das Geld los. Website-Filter erkennen betrügerische Phishing-Seiten und zeigen eine Warnung an.

Besondere Vorsicht geboten ist vor unbekannten E-Mails mit eingebetteten Links und Anhängen. Software und Dateien sollten nur aus seriösen und bekannten Quellen heruntergeladen werden. Gegen die meisten dieser Schädlinge hilft ein leistungsfähiges Antivirenprogramm. *Siegbert Lattacher*

* *Die Studie Mobile Cyber Threats: Kaspersky Lab & Interpol Joint Report kann im Internet heruntergeladen werden:http://media.kaspersky.com/pdf/-Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pd*

FOTO: KASPERSKY LAB