Vorsicht: Ungeprüfte Links oder Anhänge mit ZIP-Dateien können Schadsoftware enthalten.

Schädliche Anhänge

Laut einer Analyse des Softwareherstellers Kaspersky Lab waren zwei Drittel aller 2014 versendeten E-Mails Spam. Viele davon enthielten schädliche Beilagen.

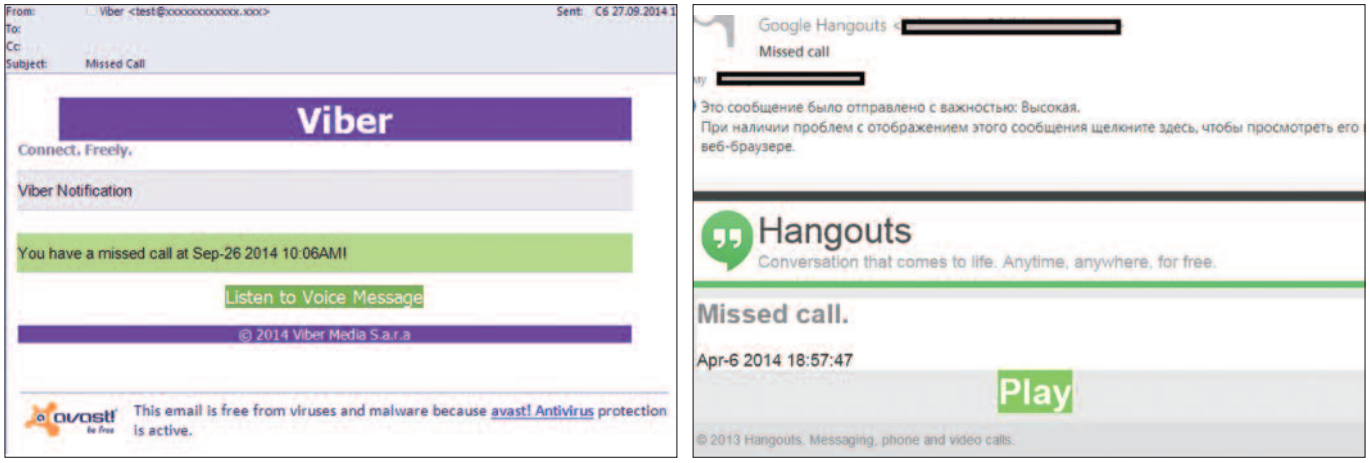
Der Spam-Anteil am E-Mail-Gesamtaufkommen ist laut einer Analyse von *Kaspersky Lab* 2014 leicht rückläufig. Die Zahl unerwünschter, aber ungefährlicher Werbe-E-Mails hat abgenommen. Während es Cyber-Kriminelle mit Phishing-Angriffen vorwiegend auf Kunden von Online-Dienstleistern wie *Yahoo, Facebook* oder *Google* abgesehen haben, stehen bei den E-Mails mit Schadprogrammen im Anhang die Finanzen der Nutzer im Fokus der Kriminellen.

Gefälschte Nachrichten. Immer mehr E-Mails geben vor, von einem Smartphone aus versendet worden zu sein. Neben der typischen Signatur wie zum Beispiel „Von meinem i-Phone gesendet“ und einem schädlichen Anhang oder Link enthalten sie kaum Text. Cyber-Kriminelle gehen davon aus, dass eine E-Mail mit angehängter Datei und der entsprechenden Signatur, die angeblich von einem *i-Phone* verschickt wurde, einen vertrauenswürdigen Eindruck macht. Sie nutzen das aus und versenden daher vermehrt gefälschte Nachrichten von mobilen Kommunikationsplattformen wie *WhatsApp* oder *Viber*. In diesen E-Mails wird auf vermeintliche Bilder oder Sprachaufzeichnungen verwiesen, die die Anwender über diese Dienste erhalten haben sollen. Viele Nutzer bemerken nicht, dass diese Hinweise niemals von den genannten Plattformen stammen können, da diese nicht mit den E-Mail-Accounts des Anwenders verbunden sind.

Von *WhatsApp* kann niemand ein Bild per E-Mail erhalten, da bei der Registrierung von *WhatsApp* die E-Mail-Adresse nicht verlangt wird. Im Anhang der Mail befindet sich statt dem vermeintlichen Bild eine Zip-Datei, in der ein Schadprogram verborgen ist. Oder die Benachrichtigung über eine angeblich über *Hangouts* verschickte Sprachmitteilung enthält einen Hyperlink, der wie eine „Play“-Schaltfläche (Oberfläche eines Musik-Players) gestaltet ist. Klickt der Empfänger darauf, hört er nicht die erwartete Voicemail ab, sondern landet über den Link auf einer gehackten legitimen Webseite, von wo aus das integrierte JavaScript ihn auf eine Werbeseite umleitet.

An der Spitze von E-Mails mit schadhaften Programmen stehen jene, die auf den Diebstahl vertraulicher Zugangsdaten ausgelegt sind. In erster Linie geht es dabei um die Anmeldedaten zu Online-Banking, Online-Shopping oder für Bezahlsysteme. Die Spam-Mails werden häufig als Benachrichtigungen von Banken und anderen Finanzdienstleistern getarnt. „Dabei ge-

FOTO: ALEXSKOPJE/FOTOLIA



Von mobilen Kommunikationsplattformen wie Viber oder Hangouts kann man keine Bilder oder Sprachnachrichten erhalten.

hen Cyber-Kriminelle immer raffinierter vor und bestücken ihre E-Mails mit zahlreichen echten Links auf Dienstleistungen der Institute“, erklärt Maria Vergelis von *Kaspersky Lab*. „Damit erhöhen sie deren Glaubwürdigkeit. Der Empfänger fällt so leichter auf den einzigen schadhaften Link in der E-Mail herein.“

In der Absicht, die Spam-Filter auszutricksen, versuchen die Spammer nicht selten auch die technischen Header („Kopfzeilen“) der E-Mails so zu fälschen, dass sie aussehen, als wären sie von mobilen Geräten gesendet worden. Der „Header“ einer E-Mail enthält die Absenderadresse.

Nutzer mobiler Geräte sind bereits an die Synchronisation von plattformübergreifenden Anwendungen gewöhnt und an verschiedene Benachrichtigungen von diesen Apps. Daher kommt es vielen Usern auch nicht verdächtig vor, wenn sie per E-Mail darüber informiert werden, dass sie irgendeine Mitteilung in einer mobilen Messaging-App erhalten haben. Und es macht auch nichts, dass diese mobilen Anwendungen nicht mit dem E-Mail-Account des Anwenders verbunden sind und die Illegitimität dieser E-Mails ganz offensichtlich ist.

Die Ukraine-Krise. Eine instabile politische Situation und Kriegshandlungen sind Quellen der Inspiration für Spammer. Früher hatte man es regelmäßig mit E-Mails zu tun, die sich Konflikte in verschiedenen Ländern zunutze machten, hauptsächlich im Nahen Osten. 2014 konzentrierte sich die Aufmerksamkeit der Spammer auf die Situation rund um die Ukraine. Die Autoren der betrügerischen E-Mails gaben sich als in Ungnade gefallene ukrainische Politiker und Unternehmer aus, die versuchten, Millionenbeträge auszuführen. Es gab auch E-Mails im Namen russischer Geschäftsleute, die unter den Sanktionen leiden würden. Wie in solchen E-Mails üblich, wurde dem Empfänger eine hohe Summe für die Hilfe angeboten, die er dem in eine schwierige Situation geratenen Absender erweisen würde. Einem Opfer, das tatsächlich Kontakt zu den Betrügern aufnahm, wurde Geld für angeblich notwendige Ausgaben aus der Tasche gezogen, wie etwa für Zoll, Steuern, Transaktionsgebühren, Flugtickets und Hotelzimmer.

Die Ebola-Epidemie wurde ebenfalls von Spammern ausgenutzt. Verschickt wurden E-Mails im Namen angeblich infizierter Afrikaner, die ihr Vermögen angeblich aus reiner Wohltätigkeit einem guten Menschen überlassen wollten.

Eine neue Idee der Betrüger war in diesem Zusammenhang eine Einladung, in der der Empfänger aufgefordert wurde, als Gast an einer Konferenz der *Weltgesundheitsorganisation (WHO)* teilzunehmen. Ihm wurden 350.000 Euro sowie ein Dienstwagen für die Arbeit als *WHO*-Vertreter in Großbritannien geboten. Die Verbreiter von Schadprogrammen nutzten die Angst der Menschen vor dieser lebensgefährlichen Krankheit aus und versendeten im Namen der *WHO* E-Mails, die einen Link auf Informationen über Maßnahmen zum Schutz vor einer Ebola-Infektion enthielt. Später erschienen inhaltlich ähnliche Mitteilungen, in denen die „Informationen von der WHO“ in einem Archiv (Zip-Datei) verpackt waren. Tatsächlich verbarg sich hinter dem Link ebenso wie im angehängten Archiv ein Schadprogramm, das zum Datendiebstahl verwendet wurde.

Tricks der Spammer. In den letzten Jahren setzten Spammer in der Regel Methoden zur Umgehung der Spam-Filter ein. Ein eindeutiges Beispiel für den Einsatz lange bekannter Spammer-Tricks ist der Börsen-Spam mit Werbung für Aktien kleinerer Unternehmen. Solche E-Mails sind Teil des bekannten Börsenbetrug-Schemas „pushing Penny-Stocks“. Die Betrüger kaufen günstige Aktien mit geringem Tagesumsatz und verbreiten mittels Spam falsche Angaben über die baldige Erhöhung des Preises für diese Aktien. Sie versuchen so, eine hektische Nachfrage zu provozieren und verkaufen die Aktien in den steigenden Markt.

Die Blütezeit dieser Betrugsart entfiel auf die Jahre 2006 bis 2007, doch Börsen-Spam wird auch heute noch verbreitet. 2013 kursierte im Börsen-Spam nur ein Werbetext mit einem Hinweis auf den aktuellen und den zu erwartenden Preis der Aktien des jeweiligen Unternehmens. In einigen Versendungen hatten die E-Mails eine Autosignatur, die von einem angeblich durchgeführten Antiviren-Scan zeugte. Dabei entsprach die Sprache der Signatur der geografischen Domain, in der sich die E-Mail-Adresse des Empfängers befand. Solche Ansätze finden sich häufig im Spam, um den Empfänger von der Legitimität und Sicherheit der E-Mail zu überzeugen. 2014 änderte sich die Aufmachung der betrügerischen Versendungen mit Aktienwerbung – die Mitteilungen sahen nun realistischer aus, und es wurde schwieriger, sie zu erkennen. *S. L.*

Screenshots: Kaspersky Lab