COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/spam-nimmt-wieder-zu,2501986

E-Mail-Security Report

Spam nimmt wieder zu

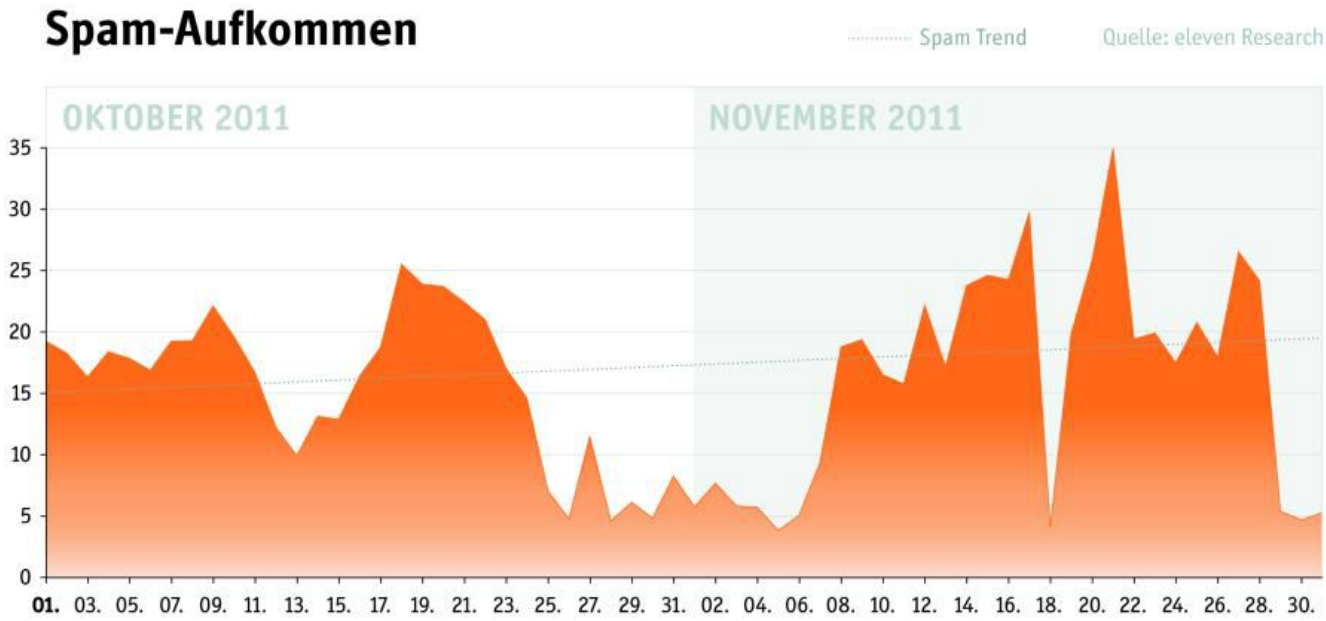
Datum: 20.12.2011
Autor(en): Thomas Pelkmann

Im November 2011 hat das Spam-Aufkommen einen neuen Höchststand seit der Abschaltung des weltgrößten Botnets Rustock im März dieses Jahres erreicht. Das berichtet der E-Mail-Security Report von Eleven.

Wieder mehr Spam im digitalen Briefkasten ermittelte der Sicherheitspezialist Eleven für den November 2011.
Foto:

Im Vergleich zum Oktober wuchs das Spam-Volumen um 6,3 Prozent und erreichte im November drei Viertel des Niveaus von Januar 2011, als der weltgrößte Versender von Spam, **Rustock**[1], noch aktiv war.

Wieder sind neun von zehn (90,3 Prozent) der weltweit versendeten E-Mails Werbemüll. Im Mai, nach der Abschaltung von Rustock, war dieser Anteil auf 78,7 Prozent gefallen. Der Anteil sauberer Mails betrug demnach ganze 6,4 Prozent, Massen-E-Mails ohne Spam-Charakter machen 2,4 Prozent aus. Der Anteil der mit Malware verseuchten E-Mails lag bei 0,04 Prozent.



Neun von zehn E-Mails sind Spam. Der Anteil "sauberer" Mails liegt dagegen bei gerade einmal 2,4 Prozent.
Foto: Eleven

Die meisten der unerwünschten Werbemails kommen aus Indien (11,6 Prozent), Brasilien (11,2 Prozent) und Vietnam (10,5 Prozent). "Gleichzeitig", berichtet Eleven, "sind die drei größten Spam-Versender näher zusammengerückt". Das sein ein Indikator dafür, dass die Spammer die Verbreitung ihrer Mailings stärker verteilten. Auf Platz vier der Versendeländer landete Indonesien mit 8, 3 Prozent, gefolgt von Russland mit 6,9 Prozent.

Damit setzt sich Eleven zufolge der Trend fort, dass die führenden westlichen Industrieländer, die vor der Rustock-Abschaltung noch eine wesentliche Rolle bei der Verbreitung von **Spam**[2] gespielt hatten, weiter an Bedeutung verlieren. Der langjährige Spitzenreiter USA lag im November 2011 mit 1,3 Prozent nur noch auf Platz 14, Deutschland belegte gerade noch Platz 30 (0,6 Prozent). Dominiert wird der Spam-Versand von Schwellenländern in Asien (sechs der Top 10). Auch osteuropäische Länder (Russland, Ukraine, Rumänien) gewinnen wieder an Bedeutung, während der Anteil Südamerikas mit Ausnahme von Brasilien wieder sinkt.

Spam-Trends

Die Monate Oktober und November gelten mit der Vorweihnachtszeit als die wichtigsten Einkaufmonate des Jahres. Kein Wunder also, dass die Zahl der versendeten Spams wieder zunimmt. Neue Höhepunkte gibt es laut Eleven im Bereich "Event-Spam", bei dem Feiertage oder andere populäre Ereignisse als Köder für Spam-, Phishing- und Malware-Kampagnen genutzt werden.

In den USA etwa wird ein Großteil des Vorweihnachtsgeschäfts in der Zeit um Thanksgiving Ende November abgewickelt. Mittlerweile haben sich Institutionen wie der **"Cyber Monday"**[3], das Online-Äquivalent zum Haupt-Shopping-Tag **"Schnäppchenfreitag"**[4], auch in Europa etabliert. Ähnliches gilt für das ebenfalls konsumfreudige Halloween (31. Oktober).

"Im Vorfeld des Kürbisfestes kursierten wie in den Vorjahren massenhaft Angebote für illegale Software", schreibt Eleven in seinem Spam-Report. Hinzu kamen 2011 eine Reihe größerer Mailings, die Sonderangebote in den Bereichen Süßigkeiten, Snacks oder Getränke anpriesen. Da das Sammeln von Süßigkeiten durch Kinder, die an die Türen ihrer Nachbarn klopfen, zu den bekanntesten und längst auch außerhalb der USA verbreiteten Traditionen gehört, erhofften sich die Spammer von dieser Masche besonders großen Erfolg.

In diesem Jahr stand vor allem der wachsende Trend, Gutscheine zu verschenken, im Fokus der Spammer und Malware-Autoren. So kursierte eine E-Mail, die angeblich einen Gutschein für Apples beliebten Musikdienst iTunes beinhaltete. Tatsächlich verbarg sich im Anhang ein Trojaner. Der gleiche Trick wurde Anfang Dezember erneut versucht, diesmal mit Gutscheinen für den Online-Versanddienst Amazon. Damit setzt sich ein Trend dieses Jahres fort: Zunehmend wird Event-Spam zusätzlich auch zur Verbreitung von Malware sowie zum Phishing eingesetzt. Das Interesse an besonderen Angeboten und Schnäppchen führt bei vielen dazu, weniger vorsichtig als sonst zu sein, wenn sie unbekannte E-Mails erhalten. Darauf spekulieren viele Spam- und Malware-Versender.

Phishing

Im Bereich **Phishing**[5] setzte sich die Regionalisierung fort. Das Research-Team von Eleven verzeichnet in seinem Report zahlreiche Kampagnen, die sich an Empfänger eines Landes oder zumindest eines Sprachraums wenden. Sie sind in der Sprache des Empfängers verfasst und geben vor, von regionalen Kreditinstituten zu stammen. Von der Lokalisierung der Mails versprechen sich die Phisher eine deutlich verbesserte Erfolgsquote, zumal sich das sprachliche Niveau der E-Mail-Texte deutlich verbessert hat.

In Deutschland stand erneut die Deutsche Bank im Fokus der Phisher. Die E-Mails waren sehr kurz gehalten und forderten dazu auf, die Website der Deutschen Bank zu besuchen. Folgt man dem in der E-Mail enthaltenen Link, wird man auf eine Seite geleitet, die zwar die URL "meine.deutsche-bank.de" enthält, aber auf einem anderen Server gehostet wird.

Die Untersuchung des Quellcodes zeigt, dass große Teile der Website tatsächlich von der Originalseite der Deutschen Bank geladen werden. Fast alle Links führen auch auf die Website der Deutschen Bank, nur der Login-Link verweist auf eine weitere Seite der Phisher. Dort werden die Besucher zu einer "Kontobestätigung" aufgefordert, über die vertrauliche Daten wie Kontonummer, Sicherheitscode, Karteninhaber und weiteres eingetragen werden sollen. Nach erfolgter Eingabe wird der Nutzer zur echten Seite der Deutschen Bank weitergeleitet. Das Abschöpfen der vertraulichen Benutzerdaten hat er in der Regel gar nicht bemerkt.

Weiterhin beobachtete Eleven Versuche, Zugangsdaten zu E-Mail-Konten abzufischen, um legale E-Mail-Accounts zum Spam-Versand zu missbrauchen. Weitere Phishing-Kampagnen betrafen Kunden der Postbank, die bereits das neue Layout der Postbank-Onlinebanking-Seiten einsetzten. Auch Mastercard-Kunden wurden in deutscher Sprache von Phishern angesprochen. Weitere Phishing-Ziele waren außerdem zum wiederholten Male der Kreditkartenanbieter Visa und der Online-Bezahldienst PayPal.

Malware

Im November stieg das Aufkommen der per E-Mail versandten Malware gegenüber dem Vormonat um 183 Prozent an. Dabei handelte es sich um einen weiteren einer ganzen Reihe massiver Sprünge, die 2011 wiederholt aufgetreten sind. Diese nach wie vor spürbare Malware-Aktivität, die zu einem Großteil aus Trojanern besteht, deutet darauf hin, dass Botnetbetreiber nach wie vor versuchen, ihre Infrastruktur zu erweitern oder neue **Botnets**[6] aufzubauen.

Größter Versender bekannter Malware war im November 2011 China mit 18,5 Prozent aller Viren-E-Mails, gefolgt von Bangladesch mit 13,9 Prozent. Mit 8,9 Prozent belegt Spam-Spitzenreiter Indien Platz 3. Im Gegensatz zum Spam-Versand spielt Deutschland bei der Malware-Verbreitung nach wie vor eine wichtige Rolle. Im November lag das Land mit 3,2 Prozent auf Platz 10.

Mit 20,8 Prozent aller Malware belegt der **Trojaner**[7] TR/Gamarue.A im November Platz 1. Getarnt war er als angebliche Nachricht über vermeintlich missbräuchliche Bewegungen auf dem Konto des Empfängers. In der Mail wurde auf einen Anhang mit weiteren Informationen verwiesen, der tatsächlich aber den Trojaner aktivierte und auf den Rechner lud.

Links im Artikel:

[1] **https://www.computerwoche.de/security/2369814/**
[2] **https://www.computerwoche.de/schwerpunkt/s/Spam.html**
[3] **https://www.computerwoche.de/schwerpunkt/c/Cyber-Monday.html**
[4] **https://www.computerwoche.de/hardware/notebook-pc/2500620/**
[5] **https://www.computerwoche.de/schwerpunkt/p/Phishing.html**
[6] **https://www.computerwoche.de/schwerpunkt/b/Botnet.html**
[7] **https://www.computerwoche.de/schwerpunkt/t/Trojaner.html**

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.