McColo goes offline – Meilenstein in der Spamvermeidung

Wie bereits an vielen Stellen beschrieben, wurde am Dienstag, den 11.11.2008 das Unternehmen McColo (AS26780) vom Internet getrennt. Die beiden größten Upstream-Provider von McColo kappten die Internet-Verbindung – McColo war damit praktisch offline. McColo ist bekannt für seine fragwürdigen Aktivitäten. Dementsprechend wurden die Auswirkungen vielerorts deutlich. Manche Quellen sprechen davon, dass McColo für bis zu 3/4 des gesamten Spamversands im Internet verantwortlich sei (http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html). Darüber hinaus beobachteten andere, dass Bots in Richtung McColo nach Hause telefonierten oder von dort kontrolliert wurden (http://asert.arbornetworks.com/2008/11/third-bad-isp-dissolves-mccolo-gone/).

Diese Aktivitäten wurden mit dem Abschalten plötzlich eingestellt – dies ist unter anderem an unserem Blacklist-Slave der NiX-Spam-Blacklist sichtbar. Seit Dienstagabend etwa 22:00 Uhr CET liegt die Gesamtanzahl an Anfragen an die Blacklist deutlich unter den Werten der vorherigen Tage. Auch die relativen Werte von positiven zu negativen Antworten haben sich etwas zugunsten der negativen verschoben.

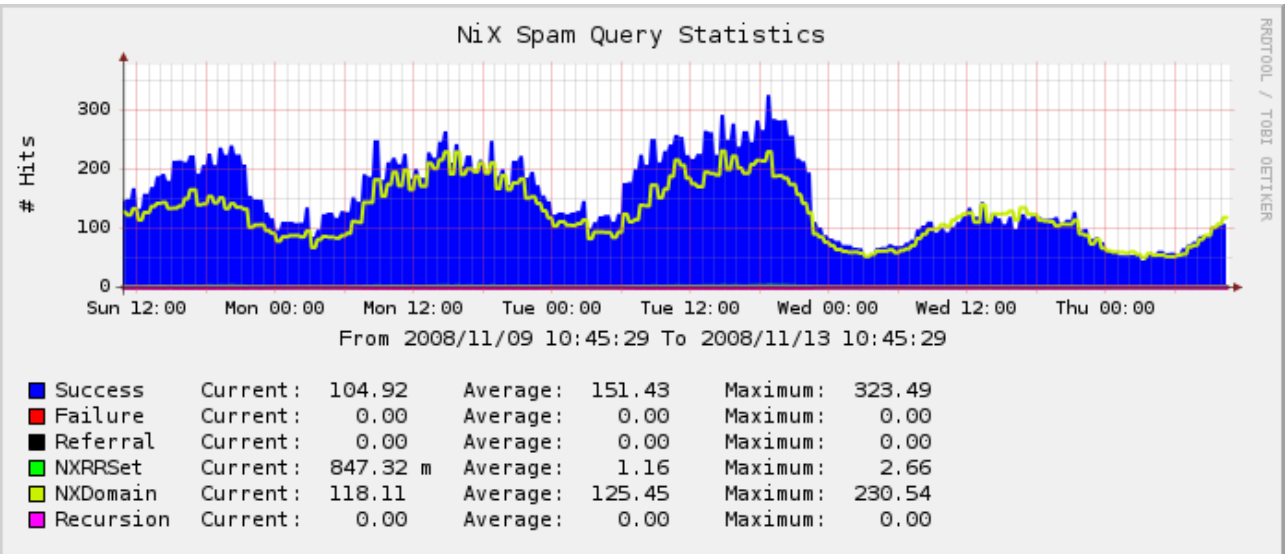

Abbildung 1: Anzahl an positiven und negativen Antworten an unserem NiX Spam Slave

Der Traffic, der durch die Abfragen verursacht wird hat sich sogar im Vergleich zu Spitzenzeiten innerhalb eines Tages nahezu halbiert.

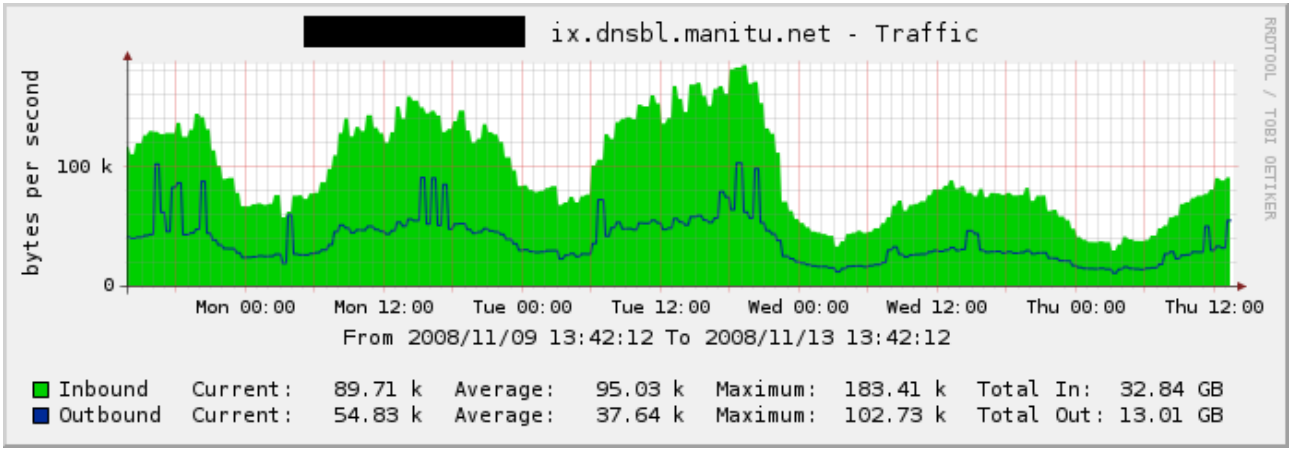

Abbildung 2: Traffic an unserem NiX Spam Slave

Darüber hinaus ist zu beobachten, dass die Anzahl an spammenden IP-Adressen deutlich zurückgegangen ist. Vergleicht man die Zahlen des 12.11.2008 (~1.5 Mio. spammende IPs alleine auf unserem Slave) mit denen des 10.11.2008 (~1 Mio. spammende IPs), so reduzierte sich die Anzahl an spammenden IP-Adressen um rund ein Drittel.

Üblicherweise wurden von McColo Bots instruiert, die dann wiederum Spam versendet haben (oder diverse andere Dinge). Aus dem Netz von McColo (AS26780) selbst konnten wir jedoch auch Spam feststellen, allerdings verhältnismäßig wenig und eher unregelmäßig.

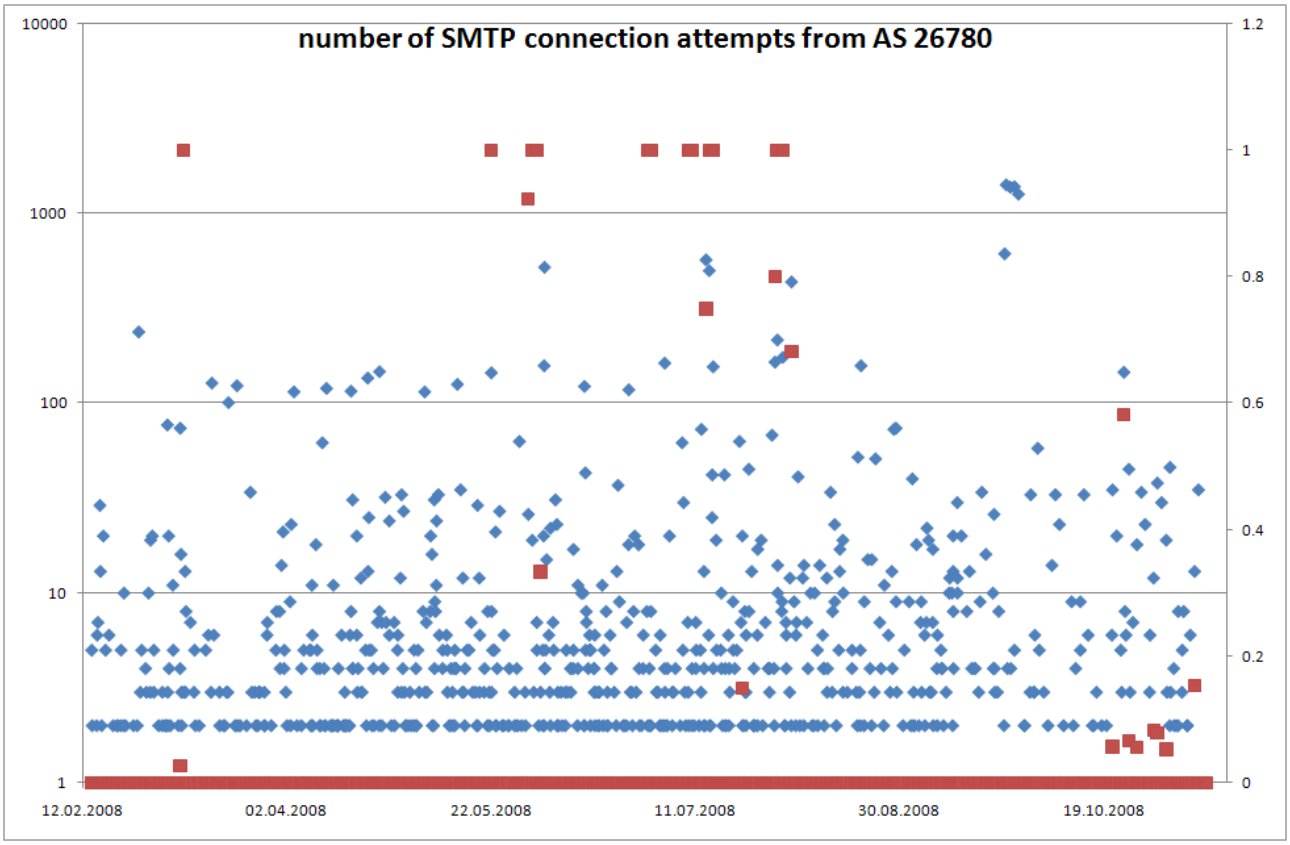

Abbildung 3: Anzahl an SMTP-Verbindungsaufbauten pro Tag aus dem Netz von AS 26780. In rot ist die Hit Rate (abzulesen an der rechten y-Achse) dargestellt.

Es bleibt offen, ob damit ein Großteil an Spamquellen langfristig aus dem Internet verschwindet. Fälle aus der Vergangenheit haben gezeigt, dass sich durchaus andere "kooperative" ISPs finden lassen, mit Hilfe derer der Spamversand weitergeht.

Kontakt

Christian J. Dietrich

Institut für Internet-Sicherheit

http://www.internet-sicherheit.de/wir-ueber-uns/team/mitarbeiter/mitarbeiter-detail/Dietrich/

Vielen Dank an unseren Hoster Dr. Bülow & Masiak GmbH (http://www.buelow-masiak.de/).