Blog Attacke: Nachtrag

Die Logfiles sind ausgewertet und das Ergebnis steht fest. Es war keine DDOS Attacke welche den Blog lahmgelegt hat, sondern eine Kommentarspam Attacke.

Innerhalb von 8 Minuten wurde die Webseite von 179 verschiedenen Adressen beglückt. Der Grossteil der „Besucher“ sind Systeme mit offenen Proxies drauf die ausserdem richtig potent sind (verglichen mit Proxies die man sonst so auf Online Listen findet). Die eine hälfte dieser Zugriffe waren reine Aufrufe von Artikeln, die andere hälfte versuchte sich im platzieren von Kommentaren. Wahrscheinlich wollte der Spammer durch die normalen Zugriffe ein gewisses „rauschen“ erzeugen.

Der Grund waum das ganze diesem Ansturm nicht standgehalten hat, waren falsche Settings in der Mysql sowie Apache Konfiguration. Da mein System lediglich 512MB hat wurden zuviele Apache Instanzen geöffnet, welche nach und nach den ganzen RAM weggefressen haben. Ich hoffe nun, dass die gemachten Änderungen das nächste mal mehr als 8 Minuten durchhalten.

Und weg war der Blog: DDOS

10:25 Uhr. Ich will mich auf dem Blog einloggen und den Spam löschen, als ich stutzig werde. Die Verbindung ist heute aber auch lahm… komisch. Als ich nach vollen zwei Minuten immer noch keine Verbindung habe, versuche ich es über einen Anonymisierer. Und siehe da, auch der kriegt keine Verbindung.

10:32 Uhr. Irgendwas ist in der Zwischenzeit passiert. Ich

komme auf die Hauptseite, kann da aber den Blog auch nicht anwählen.

10:33 Uhr. Jetzt passiert schon mehr. Sobald ich den Blog anwähle erscheint die Fehlermeldung, dass keine Verbindung zum Datenbankserver hergestellt werden konnte. Und so bleibt es dann auch den ganzen Tag.

19:00 Uhr. Eine erste Analyse zeigt, dass irgendwas (Apache? Mysql?) gehörig Cores erzeugt hat und der Datenbank Server nicht mehr läuft. Hurtig alles wegdumpen um es später in ruhe anschauen zu können, dann werden die Dienste wieder aktiviert.

19:10 Uhr. Aha. Hunderte von Zugriffen auf so ziemlich alle verfügbaren Artikel dieses Blogs innerhalb von Sekunden. Da kann der Server nur in die Knie gehen. Es was also eine Distributed Denial of Service (DDOS) Attacke irgend eines Bot Netzes. Die Hauptfrage ist nun, wozu? Wollte jemand ein neues Bot-Netz ausprobieren, bevor er „richtig“ zuschlägt? Hat man während der Attacke versucht den Server zu kompromitieren (Loganalyse am Weekend, sigh!) und die Attacke genutzt um Hinweise darauf im Rauschen untergehen zu lassen? Oder ist der Egger Blog für gewisse Kreise ene Bedrohung

Updates werden folgen…

Kseniya Simonovas fantastische Sandbilder

Nicht nur in unseren Beritengraden gibt es sogenannte Talentshows. Doch während bei uns Hauptsächlich nach gesanglichen Fähigkeiten gesucht wird (und meiner Meinung nach selten gefunden werden!), haben die Ukrainer eine echte Talentshow gemacht. Die Gewinnerin der 2009er Version von Ukraine's Got Talent ist eine junge Frau mit dem Namen Kseniya Simonova.

Was diese Frau beherrscht ist die Kunst der Sandanimation. Dabei verteilt die Künstlerin auf einer hell erleuchteten Plexigalsplatte (ähnlich einem Röntgenfilmbetrachter beim Arzt) Sand. Danach malt Sie mit den Fingern in den Sand, wobei sich das Bild stetig wandelt (daher wohl Animation).

Ich wäre ja schon froh, wenn ich innerhalb eines Tages auch nur eines der Bilder hinkriegen würde! Wer das noch nie gesehen hat, soll sich einfach einmal die beiden nachfolgenden Videos zu Gemüte führen.

Please enable JavaScript

Please enable JavaScript

Wo ist der Preis heiss?

Es gibt ja zwei Arten von Käufern. Diejenigen die zwar wissen dass Sie z.B. einen Monitor für den Computer wollen, sich aber bisher keine Gedanken darüber gemacht haben welches Modell, welche Auflösung, wieviel Zoll oder welche Attribute der Monitor sonst haben soll. Solche Leute lassen sich am besten in einem Fachgeschäft beraten oder nehmen den Computerversierten Nachbarsjungen mit.

Dann gibt es die Gruppe von Käufern, welche bereits im Vorfeld das Internet nach Modellen, Testberichten, Positiv-/Negativlisten etc. durchforsten und mit der Zeit ganz genau

wissen, dass Sie z.B. den Samsung SyncMaster 2243EW und nicht etwa den 2243BW wollen. Diese wenden sich dann entweder direkt an die Geschäfte in unmittelbarer Umgebung oder grasen ihre Stamm-Web-Shops ab. Meistens werden diese dort dann auch fündig.

Mühsam ist es dann nur, wenn man zwei Tage danach von einem Bekannten erfährt, dass genau der selbe Monitor beim Händler XYZ ganze 80 CHF günstiger zu haben gewesen wäre.

Um diesem Problem vorzubeugen gibt es seit ettlichen Jahren Webseiten, welche die Preise der einzelnen Shops vergleichen. Eine Seite die ich immer wieder einmal besuche ist http://www.toppreise.ch. Sucht man dort z.B. nach oben genanntem Monitor, dann findet man Shoppreise die sich zwischen 296 CHF und 605 !! CHF bewegen. Angesichts der Tatsache, dass man beim billigsten Händler gleich zwei Samsung Monitore zum Preis eines Samsung Monitors beim teuersten Händlers bekommt, lohnt sich der Blick in die Vergleichsseite allemal!

Ausserdem ist die Seite ganz praktisch um vielleicht den einen oder anderen neuen Webshop kennenzulernen oder um mit dem eigenen Händler mal über die Rabattstufe zu diskutieren