

Holger Bleich

# Angriff der Blog-Kloner

## Unbekannte spiegeln deutsche Blogs zu ähnlich lautenden Domains

Was tun, wenn plötzlich eine perfekte Kopie des eigenen Blogs unter einer .net- oder .com-Adresse auftaucht? Mit diesem Problem sehen sich momentan deutsche Food-, Reise- und Lifestyle-Blogger konfrontiert. Noch ist nicht ganz klar, was die mysteriösen Blog-Kloner bezwecken.

Egal ob große Verlage oder private Blogger: Alle, die im Web publizieren, haben hin und wieder damit zu kämpfen, dass andere ihre Inhalte ungeniert abkupfern. Gegen derlei Verstöße gegen das Urheberrecht kann man meist wirksam vorgehen, weil sich der Content-Kopierer zu erkennen gibt.

Doch was tun, wenn Unbekannte das gesamte Blog eins zu eins zu einer anderen Web-Adresse spiegeln? Mitte August bemerkten die ersten Blogger, dass ihre Inhalte im identischen Layout unter denselben Domain-Namen, aber anderen Top-Level-Domains zu lesen sind. So fand „Elbköchin“ Bianca Matthée ihr Blog elbcuisine.de auch unter elbcuisine.com. Bloggerin Stefanie Bamberg reagierte stinksauer, als sie ihre schoen-und-fein.de-Küchentipps auch unter schoen-und-fein.com las – eine Domain, die Unbekannte registriert hatten.

Wie viele Blogs derzeit gespiegelt werden, ist unklar. 25 Betreiber von gekaperten Blogs tauschen sich bereits in einer Facebook-Gruppe aus. Sie besprechen dort ihre Recherche-Fortschritte und koordinieren mögliche Gegenmaßnahmen. Wer herausfinden möchte, ob er selbst Opfer der Blog-Kopierer geworden ist, kann das über Recherche-Tools von Registraren tun. So listen etwa United-Domains.de oder Checkdomains.de auf, unter welchen anderen Top-Level-Domains eingeebene .de-Name frei oder vergeben sind.

Die Fake-Domains laufen allesamt über das US-amerikanische Unternehmen GoDaddy. GoDaddy ist der weltgrößte Registrar und gestattet Domain-Registrierungen ohne jede Prüfung der Kunden-Identität. Bei allen bisher bekannten Fake-Registrierungen waren die Kontaktdaten der Blogger eingetragen. Allerdings unterschied sich die Kon-

takt-Mailadresse von der des echten Blog-Betreibers.

### Affiliate-Betrug

Offensichtlich wollen die Blog-Kloner mit den fremden Inhalten Kasse machen. Wie das mit dieser Masche funktioniert, darüber lässt sich momentan nur spekulieren. Fest steht, dass auf den in Echtzeit gespiegelten Klon-Blogs andere Werbung auftaucht als auf den Originalen. Diese Banner spielen Partner-Werbenetzwerke zu.

Bespricht der Blogger beispielsweise ein Buch, blendet Amazons Werbenetzwerk Partner einen Werbelink ein. Wenn ein Blog-Besucher über diesen Link in den Amazon-Shop kommt und dort das Buch ordert, erhält der Blogger eine Provision. Im Affiliate-Jargon spricht man von der Conversion, also der Weiterführung einer Werbeblendung zu einem Klick und schließlich zu einem Kauf.

Monatsbeginn bis heute ▼

Letzte Aktualisierung: 26 August 2014

**Gewinnaufstellung**

Versandte Artikel -- gesamt	611
Werbekostenerstattungsrate	6,50%
Erhöhen Sie Ihre Empfehlungsrate auf 7,00% durch Empfehlung 419 weitere Artikel	
<b>GESAMT *</b>	<b>EUR 687,95</b>
<a href="#">Details anzeigen</a>	

**Zusammenfassung der Bestellungen**

Bestellte Artikel	562
Klicks	28911
Ihre Conversion	1,94%
<a href="#">Details anzeigen</a>	

\* Kombiniertes Bericht für alle Tracking-Ids.

**Ein Blick in den Amazon-Account der unbekanntenen Blog-Kloner offenbart, dass über die Fake-Domain viel Umsatz und Provision durch Banner-Klicks generiert wird.**

dieser fälschlicherweise dem simulierten Klick zugeordnet – die Provision gelangt zu einem anderen Account. In seinem Blog seohelfer.de berichtete Fachmann Timo Fach im vergangenen Jahr über eine ähnliche Welle von Blog-Spiegelungen, bei der Cookie-Dropping zum Einsatz kam, wie er herausgefunden hatte.

### Lukrative Klicks

Alex Mirschel, Betreiber des ebenfalls gekaperten Reiseblogs niedblog.de, hat es als erster geschafft, GoDaddy von dem Blog-Missbrauch zu überzeugen. Als er dem Registrar seine Identität nachgewiesen hatte, bekam er die Klon-Domain zugesprochen. Weil er dadurch die zugehörigen Mail-Accounts kontrolliert, konnte er Mails abfangen, die an die Betrüger gerichtet waren. Unter anderem erhielt er damit Zugang zu einem Amazon-Partner-Netzwerk-Account, den die Betrüger für die Klon-Domain eingerichtet hatten.

Ein Blick in den mittlerweile von Amazon gesperrten Account, den Mirschel uns gewährte, förderte Erstaunliches zutage: Im Zeitraum vom 1. bis 18. August liefen über den Klon niedblog.com knapp 30 000 Klicks auf Amazon-Anzeigen ein. Mehr als 12 000 Euro Umsatz mit bestellten Waren brachten über 650 Euro Provision in nicht einmal drei Wochen. Geht man nun davon aus, dass die Betrüger



**Missbrauch / Abuse**

Sehr geehrte Betrüger,

wir haben uns nun in Ihr illegales Vorhaben darzwischen gefickt. Der beliebte Reiseblog www.NIEDBlog.de wurde auf rechtswidrige Weise gespiegelt und unter der gleichnamigen ".com" Domain inhaltlich als fortwährende Kopie online bereitgestellt. Dabei wurden nicht nur die urheberrechtlich geschützten Inhalte vollumfänglich gestohlen und auf eigenen Servern bereitgestellt, sondern auch unsere Personendaten ohne Erlaubnis für die Registrierung der missbräuchlichen Domain verwendet.

Wir haben von diesem Missbrauch nun Kenntnis erlangt und bereiten rechtliche Schritte gegen die verantwortlichen Personen vor. Anhand der von Registrierungsstelle, der Provider und der beteiligten Behörden bereitgestellten Daten werden wir die handelnden Personen juristisch zur Rechenschaft ziehen.

Für den Moment erlauben wir uns jedoch, Ihre Macheschaften schlichtweg zu unterbinden. Vielen Dank für Ihr Verständnis.

**Alex Mirschel, Betreiber von niedblog.de, ist es gelungen, dem Klon niedblog.com eine Warnmeldung unterzuschreiben.**

hunderte Spiegelungen betreiben, wird deutlich, wie lukrativ die Masche ist.

Rätselhaft bleibt, woher die geklonten Blogs ihre Besuche erhalten. Mirschel hat auf die eroberte Spiegelung „jegliche Analysetools“ geschaltet, wie er sagte. Besucher hat er aber kaum registriert. Demnach können nach Meinung Mirschels die 30 000 Klicks in Wahrheit nicht über niedblog.com gekommen sein. Dies habe ihm Amazon in einem Gespräch bestätigt. Herkunft und Linktyp der Klicks und Verkäufe seien unbekannt. Mirschel vermutet daher, dass die Blog-Klone tatsächlich eher dem Missbrauch der Blogger-Identitäten dienen, um eine unbekanntere, andere Betrugsmasche zu verschleiern.

### Kloner aussperren

Hinter den Domains arbeitet offenbar eine Art Proxy-Server, der beim Abruf in Echtzeit den Original-Inhalt des Blogs zieht, durch einen Parser schickt und leicht manipuliert an den abrufenden Browser weitergibt. Im von Timo Fach aufgedeckten Fall kam im vergangenen Jahr die offensichtlich eigens für diese Masche in China entwickelte Serversoftware Mr9-SM zum Einsatz. Indizien sprechen dafür, dass dies auch bei der aktuellen Blog-Kloning-Welle der Fall ist.

Die Betrüger verstecken ihre Server hinter dem IP-Proxy-Service von Cloudflare. Zu tatsächlichen IP-Adressen der Server könnten allenfalls strafrechtliche Ermittlungen führen. Nach mehreren Strafanzeigen hat beispielsweise die Polizei Leipzig angefangen nachzuforschen. Bis es Ergebnisse gibt, bleibt betroffenen Bloggern nur, sich selbst zu helfen.

Versuche, über einen .htaccess-deny-Eintrag die Besuche der abgrasenden IP-Adresse zu sperren, brachten nur kurzfristig Erfolg, weil diese oft wechselt. Manche Blogger haben die gesamte IP-Range ausgesperrt und damit erst einmal Ruhe gehabt. Auf dem ebenfalls vom Kloning betroffenen Blog seitenwechsel.org hat der Entwickler Chris Kuhles eine Möglichkeit veröffentlicht, mit der Wordpress bemerkt, dass es gespiegelt wurde, und beim Abruf eine entsprechende Meldung ausgibt. Eine ähnliche Lösung hat Sebastian

Bauer auf Github zur freien Verwendung präsentiert ([github.com/sebauer/wp-anticlone](https://github.com/sebauer/wp-anticlone)).

Vom Kloning betroffene Blog-Betreiber sollten Beweise zu dem Fall unter Zeugen mit Screenshots sichern. Außerdem haben sie Chancen, die Fake-Domain unter eigene Kontrolle zu bringen. Dazu müssen sie unter Nachweis ihrer Identität (Personalausweiskopie) einen sogenannten Change Request beim

Registrar GoDaddy anmelden, der hierfür ein Web-Formular bereitstellt ([supportcenter.godaddy.com/ChangeRequest/](https://supportcenter.godaddy.com/ChangeRequest/)). Außerdem sollten sie Cloudflare den Missbrauch der IP-Adressverschleierung melden.

Eine Strafanzeige wegen Verdachts auf Betrug und Verstoßes gegen das Urheberrecht lohnt schon deshalb, weil Behörden oft erst dann intensive Ermittlungen einleiten, wenn eine große

Zahl von Opfern einer betrügerischen Masche bekannt ist. Der Schaden lässt sich natürlich nicht beziffern. Bislang ist nicht bekannt, dass Blogger nennenswert Besucher-Traffic an die Klone verloren haben. Allerdings könnte es sein, dass die Google-Trefferplatzierung leidet, falls die Suchmaschine Klone als Duplicate Content bewertet. Auch dafür liegen bislang aber keine Hinweise vor. (hob)

Anzeige