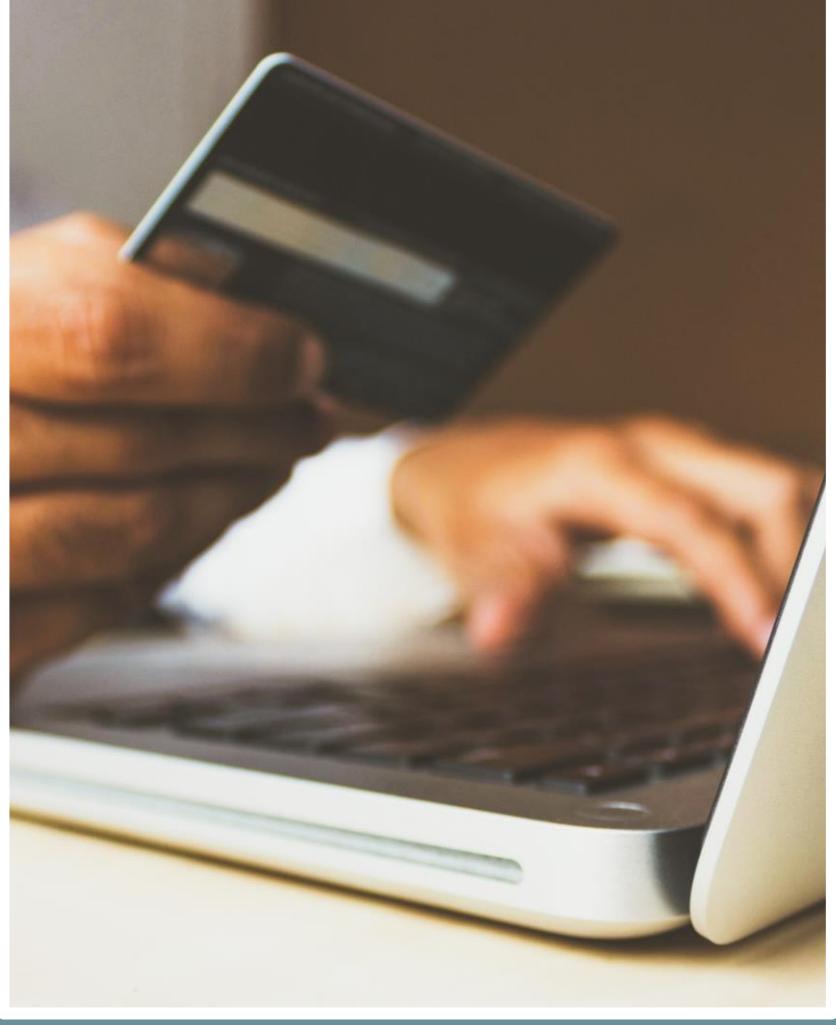


Fake-Shops

Der systematische Betrug mit abgelaufenen .de-Domains

November 2019

wdp wachter digital partners

Inhalt

wdp

Summary

1

Betrügerbanden übernehmen systematisch auslaufende deutsche Domains, um deren SEO-Power und Direct-Traffic für ihre Fake-Shops nutzen zu können.

Sie bieten Markenprodukte weit unter regulären Marktpreisen an, um Zahlungsdaten auszuspionieren

2

Das Ausmaß des Betruges ist gigantisch.

Schätzungsweise über 16.000 deutsche sogenannte Expired Domains sind aktuell betroffen.

3

Auch Domains bekannter Institutionen sind darunter.

Dies sind z. B. politische Parteien oder auch die Deutsche Annington.

4

Die DENIC weist jede Verantwortung von sich.

Die DENIC liefert weder Hilfe für Betrugsopfer, noch bekämpft sie die Ursache des Problems - obwohl die Shops mit hoher Wahrscheinlichkeit mit Fake-Daten registriert wurden.

wdp

Hintergründe der Untersuchung

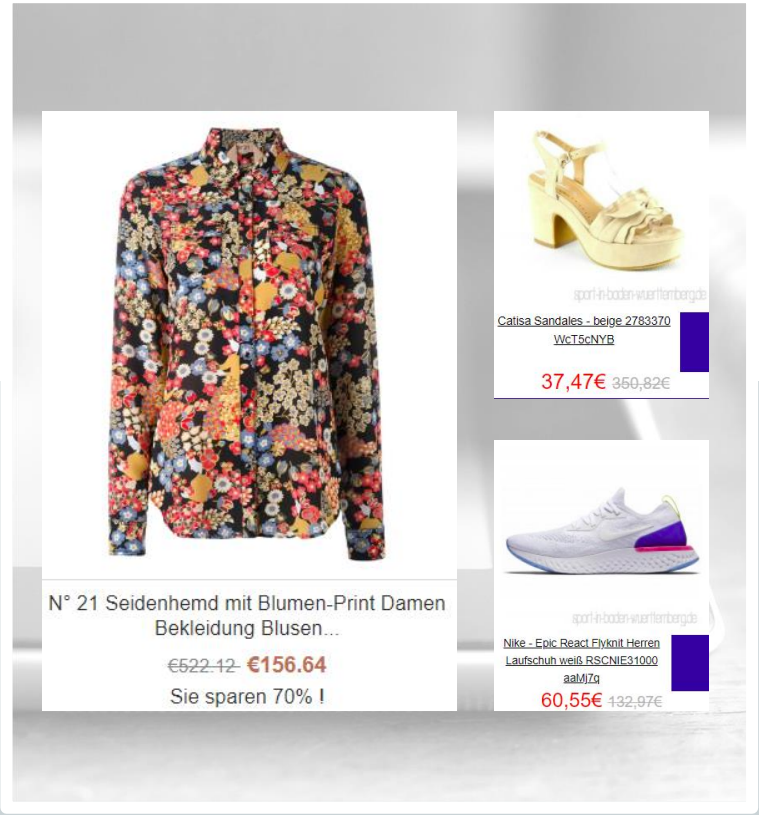
Bei einer Marktanalyse zu Onlineshop-Software fiel auf, dass neben den populären Systemen wie Magento, Shopware und Shopify auch einige weitere, den wdp Digitalexperten unbekannten Technologien überraschend große Marktanteile verzeichneten. Konkret waren dies Opencart, osCommerce und Zen-Cart. Beim stichprobenartigen Aufrufen von Shop-Seiten, die eine dieser Technologien nutzten, entstand der Eindruck, dass sich zahlreiche dieser Shops in vielerlei Hinsicht ähneln und von allgemein schlechter Qualität sind.

Es ergab sich der Verdacht, dass diese Shops zu Betrugszwecken aufgesetzt wurden – und dass es sich nicht um Einzelfälle handelt, sondern dahinter systematischer Betrug in großem Stil steckt.

wdp führte daraufhin eine Untersuchung zum Umfang dieser sogenannten „Fake-Shops“ auf den drei verdächtigen Shop-Systemen durch.

Insgesamt wurden 29.406 Domains betrachtet, die mindestens eine der drei Technologien nutzen. Eine Stichprobe von 280 Shops wurde von wdp-Experten auf Anzeichen von Fake-Shops manuell überprüft. Das Ergebnis: 159 Shops (57 %, also hochgerechnet über 16.000) Onlineshops zeigten die typischen Anzeichen für Fake-Shops. Dabei fiel eine weitere Besonderheit auf: Die URLs dieser Shops standen in keinerlei Zusammenhang mit den angebotenen Waren. Die Fake-Shops waren alle auf vormals seriösen, abgelaufenen Domains deutscher Internetseiten errichtet.

Was sind Fake-Shops?



Fake-Shops sind unseriöse Onlineshops, deren Ziel es ist, Bestellungen zu generieren, keine oder minderwertige Produkte zu versenden und die vorab geleistete Zahlung zu behalten. Im schlimmsten Fall werden auch die persönlichen Daten und Zahlungsdetails zu betrügerischen Zwecken weiterverwendet.

„Fake-Shops sind auf den ersten Blick schwer zu erkennen. Teilweise sind sie Kopien real existierender Websites, sie wirken auf den ersten Blick seriös und lassen daher beim Käufer selten Zweifel an ihrer Echtheit aufkommen. Mit gut kopierten Produktbildern und Informationen aus dem Internet sowie einem professionellen Erscheinungsbild gewinnen Fake-Shops das Vertrauen der Online-Käufer und verleiten sie dadurch zum Kauf. Ein weiteres Lockmittel ist der scheinbar besonders günstige Preis des gesuchten Produkts.“*

* www.verbraucherzentrale.de/wissen/digitale-welt/onlinehandel/abzocke-online-wie-erkenne-ich-fakeshops-im-internet-13166

So erkennt man Fake-Shops

1

Ungewöhnlich hohe Rabatte & krumme Preise

Die Preise der Produkte auf nahezu alle betrachteten Webseiten sind grundsätzlich sehr hoch und stark rabattiert. Zusätzlich ergibt sich kein konkretes Schema bei der Preiserstellung, es gibt viele „krumme“ Preise, was wahrscheinlich aus einer automatisierten Kursumrechnung resultiert.

2

Markenprodukte

Sehr häufig werden in Fake-Shops ausschließlich Markenprodukte zu viel zu niedrigen Preisen angeboten. Dies ist nicht nur bei Schuhen (Nike, Adidas etc.) der Fall, jedoch hier am auffälligsten.

3

Schlechte Übersetzungen, fehlende & falsche Inhalte

Anstelle des Impressums findet man oft eine Datenschutzerklärung. Beim Lesen fallen Fehler auf, die auf eine automatisierte Übersetzung schließen lassen. Es tauchen immer wieder die gleichen Formulierungen auf, wie:
„Der Schutz Ihrer Privatsph?re ist uns wichtig . Diese Politik erkl?rt, wie wir sammeln, verwenden und weitergeben der pers?nlichen Informationen, die Sie zur Verfügung stellen , w?hrend die Nutzung dieser Website . Es ist immer die Wahl, ob sie pers?nliche Daten über das Web zu erstellen.“*

* z. B. auf www.bmwstammtischstuttgart.de/datenschutz-bestimmungen.html

4

Fehlendes Impressum

Bei allen untersuchten Seiten gab es kein Impressum und keinen Hinweis auf den Betreiber der Seiter. Ein Impressum ist nach § 5 Telemediengesetz (TMG) vorgeschrieben für „geschäftsmäßige Online-Dienste“. Daher ist dessen Fehlen ein starkes Zeichen für einen nicht seriösen Anbieter.

5

Kein SSL-Zertifikat

Gegen die seit 2015 bestehende Pflicht*, personenbezogene Daten gegen Zugriffe Dritter zu schützen, verstoßen alle betrachteten Fake Shops.

6

Keine Übereinstimmung von URL und Seiteninhalt

Geht man normalerweise davon aus, dass die Domain eines Shops einen Hinweis auf den Inhalt der Seite liefert, so ist dies bei den betrachteten Shops selten der Fall.

* www.werbeagentur-wicker.de/ssl-verschluesselung-fuer-unternehmen-pflicht

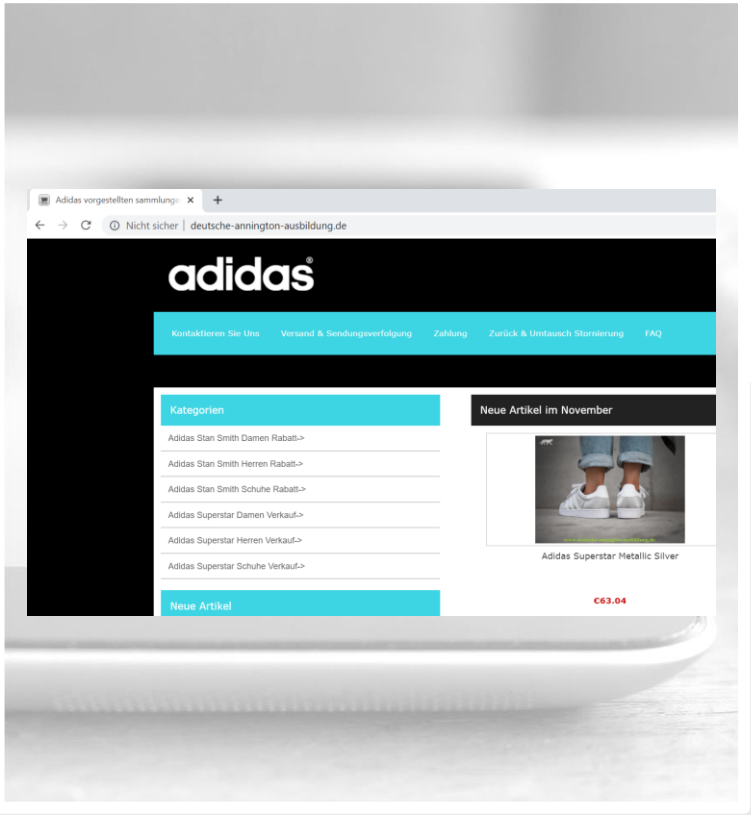
Das Vorgehen
Schritt 1: Shop-Technologien

Mithilfe von builtwith.com wurden 29.406 deutsche Domains extrahiert, auf denen (mindestens) eine der verdächtigen drei Shop-Technologien läuft. Bei allen drei Systemen können Onlineshops kostengünstig und ohne großen Aufwand aufgesetzt werden.

Für Fake-Shop-Betreiber sind einfache, kostengünstige Shop-Technologien deshalb wichtig, weil Fake-Shops in Massen aufgesetzt werden und häufig nur wenige Wochen online sind, bevor sie geschlossen und an anderer Stelle (Domain) neue Fake-Shops geöffnet werden. Damit diese kurzlebigen Shops sich schneller rentieren, gilt es, die Kosten für Software und Implementierung möglichst gering zu halten.

Shop-System	Anzahl gesamt	Anzahl Stichprobe	Anteil verdächtiger Shops
Zen-Cart	13.212	101	71%
OpenCart	6.628	73	44%
osCommerce	5.138	67	28%
Zen-Cart und osCommerce	4.428	39	92%
Gesamt-summe	29.406	280	57%

Schritt 2: Stichprobe



In einer Stichprobe (siehe Tabelle Seite 8) wurden 280 Shops einzeln betrachtet und manuell auf Auffälligkeiten hin untersucht. 43 Domains (15%) waren nicht vergeben oder endeten in einer Fehlermeldung.

Von den restlichen 237 wiesen 159 (57%) starke Indizien für Fake-Shops auf. Hochgerechnet ergaben sich daraus insgesamt 16.761 verdächtige Shops.

Bei der Prüfung der Stichprobe fiel eine Besonderheit auf: Die URLs der mutmaßlichen Fake-Shops standen in keinerlei Zusammenhang mit den angebotenen Waren.

Die Shops waren auf vormals seriösen, abgelaufenen Domains deutscher Internetseiten errichtet.

Da eine finale Verifizierung des Verdachts aus der Stichprobe nur durch umfangreiche Testbestellungen erfolgen kann, wurde nach weiteren technischen Gemeinsamkeiten in der Stichprobe gesucht.

* CPanel: SSL Zertifikat, welches einfach und kostenlos zu installieren ist. Daher scheint es bei den Betreibern solcher Webseiten beliebt zu sein.

Schritt 3: SSL-Zertifikate

Für Fake-Shop-Betreiber ist ein kostenpflichtiges SSL-Zertifikat[1] ein zusätzlicher Kostenfaktor, der die Rentabilität des kurzlebigen Fake-Shops negativ beeinträchtigt. Naheliegend daher: Wie auch schon bei der Shop-Technologie setzen Fake-Shop-Betreiber auf kostenlose Lösungen – oder verzichten komplett auf SSL-Zertifikate.

Das Resultat unserer Untersuchung bestätigt dies: Domains ohne SSL-Zertifikat bzw. mit einem kostenlosen Zertifikat von CPanel[2] wiesen zu einem sehr hohen Anteil starke Anzeichen von Fake-Shops auf.

SSL-Zertifikat	Anzahl gesamt	Anzahl Stichprobe	Anteil verdächtiger Shops
Keins	19.897	128	70%
CPanel SSL	4.861	66	91%
SSL by Default	3.259	65	8%
LetsEncrypt	975	24	13%
Cloudflare SSL	790	8	13%

[1] SSL bezeichnet ein Verschlüsselungsprotokoll zur sicheren Datenübertragung. Eine Domain kann mehrere SSL-Zertifikate nutzen.
[2] CPanel: SSL Zertifikat, welches einfach und kostenlos zu installieren ist. Daher scheint es von den Betreibern von Fake-Shops häufig verwendet zu werden.

Schritt 4: Nameserver

Anschließend wurde die Stichprobe auf die verwendeten Nameserver* untersucht. Zu Grunde legten wir die 5 am häufigsten verwendeten Nameserver-Varianten. Auch hier zeigte sich bei zwei ganz konkreten Nameservern eine auffallend hohe Anzahl potentieller Fake-Shops.

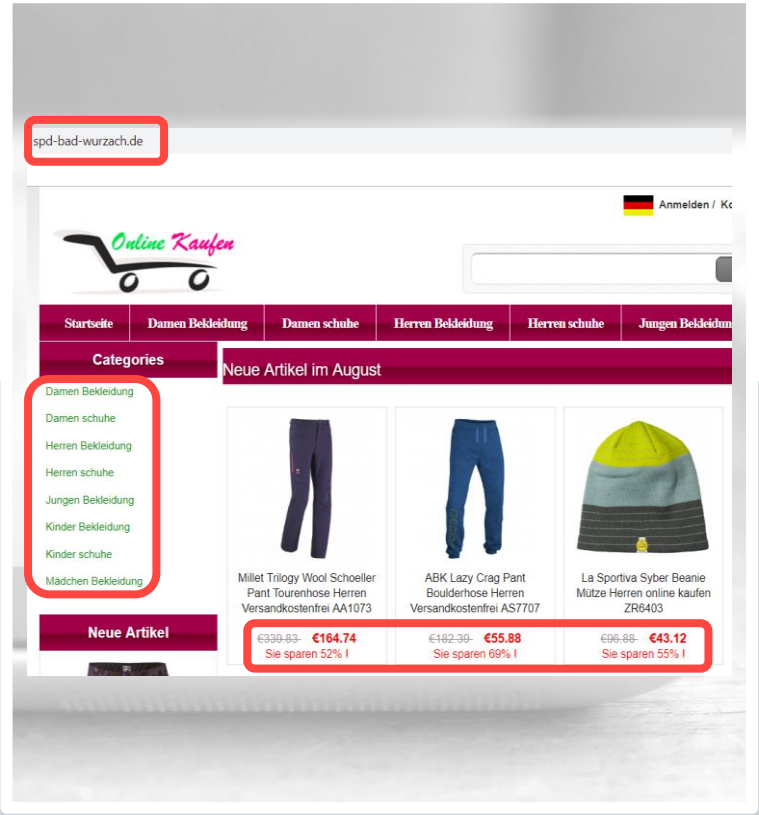
Nameserver	Anzahl gesamt	Anzahl Stichprobe	Anteil verdächtiger Shops
Keiner	12.181	122	48%
Logic Boxes DNS	10.793	78	**95%**
InterNetX DNS	1.699	14	**100%**
Cloudflare DNS	1.607	11	36%
Bodis DNS	691	8	(-)

* Nameserver verwalten die Zuordnung von Domain-Namen zu IP-Adressen

Ergebnis

Aus den betrachteten 29.406 Domains sind nach Hochrechnung der Ergebnisse aus der manuellen Stichprobe von 280 Domains **16.761 der Onlineshops, die eine der drei verdächtigen Shop-Technologien nutzen, mit hoher Wahrscheinlichkeit als Fake-Shops einzuordnen.**

Inwiefern alle diese potentiellen Fake-Shops wirklich betrügerische Absichten verfolgen, ließe sich nur durch Testkäufe bei jedem einzelnen Shop final verifizieren. Auch eine Einsicht bei der DENIC in die Informationen zu den Seiten-Betreibern ist seit der DSGVO nur noch aufgrund „berechtigten Interesses“ möglich, und kann von wdp nicht beantragt werden.*



Die inhaltlichen Indizien jedenfalls liefern klare Hinweise auf ungeahnte Dimensionen beim Online-Betrug mit ausgelaufenen deutschen Domains.

* Siehe Seite 21. Die Beispiele ab den Seite 16 sind daher alle von älteren DENIC-Einträgen, die vor der Einführung der DSGVO erstellt wurden.

Bei dem Versuch, die ohnehin große Wahrscheinlichkeit auf Betrug noch weiter technisch zu verifizieren, wiesen in der wdp-Untersuchung verschiedene Technologie-Kombinationen in der Stichprobe sogar zu 100 % starke Indizien für Fake-Shops auf.

SSL	Nameserver	Shop-Software	Anzahl Stichprobe	Anteil Fake	Anzahl Hochrechnung
CPanel SSL oder Kein SSL	DNS Pod, InterNetX DNS, Logic Boxes DNS oder NameSilo DNS	OpenCart oder Zen-Cart + osCommerce	40	100%	4.761
CPanel SSL oder Kein SSL	DNS Pod, InterNetX DNS, Logic Boxes DNS oder NameSilo DNS	andere	52	92%	7.247
CPanel SSL oder Kein SSL	andere	OpenCart oder Zen-Cart + osCommerce	35	69%	4.233
CPanel SSL oder Kein SSL	andere	andere	69	55%	8.577
andere	DNS Pod, InterNetX DNS, Logic Boxes DNS oder NameSilo DNS	OpenCart oder Zen-Cart + osCommerce	3	100%	313
andere	DNS Pod, InterNetX DNS, Logic Boxes DNS oder NameSilo DNS	andere	1	100%	416
andere	andere	OpenCart oder Zen-Cart + osCommerce	34	3%	1.844
andere	andere	andere	48	8%	2.211
		Gesamt	280	57%	29.406

Systematischer Betrug mit Expired Domains

Es ist grundsätzlich ein weit verbreitetes und normales Vorgehen, hochwertige existierende Domains zu übernehmen und sie für den eigenen Zweck zu verwenden. Der Vorteil gegenüber der Registrierung einer neuen Domain: Man profitiert vom Google Ranking der existierenden Domain, welches dafür sorgt, dass die Seite in Suchresultaten gut platziert ist und organischen Traffic liefert. Zudem kann man von noch vorhandenem Direct Traffic profitieren, also den direkten Zugriffen auf die Domain ohne Umweg über eine Suchmaschine. Mittlerweile ermöglichen viele Dienste die Suche nach Expired Domains[1].

Die Untersuchung von wdp zeigt: Dass dieses Vorgehen von Betrügern verwendet wird, ist kein Einzelfall.

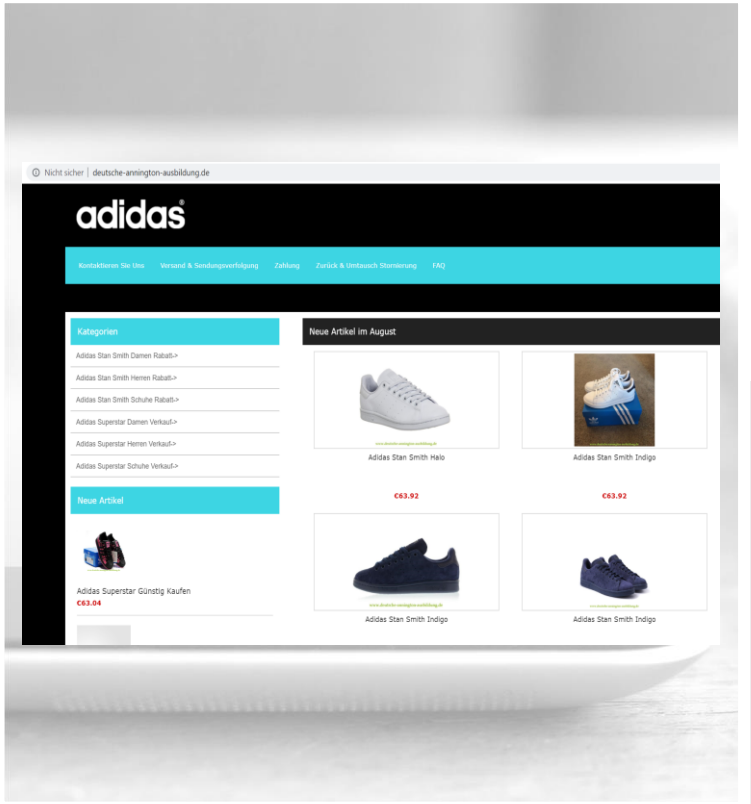
Betrügerbanden übernehmen systematisch auslaufende deutsche Domains, um deren SEO-Power und Direct-Traffic für ihre Fake-Shops nutzen zu können.

Bei Fake-Shops werden keine einzelnen, hochwertigen Domains gekauft, sondern pauschal alle Domains, die zu einem günstigen Preis verfügbar sind. Somit lässt sich der Gesamtpreis eines Fake-Shops deutlich reduzieren und der Shop rechnet sich schon nach wenigen eingegangenen Bestellungen.

Expired Domains sind solche Domains, die „abgelaufen" sind, also bereits bei der jeweiligen Registrierungsstelle gelöscht wurden oder bald werden. Damit sind Expired Domains ehemalige Projekte anderer Webmaster, die sie nicht weiterhin betreuen wollten oder konnten. Nach einer gewissen Ablauffrist kann eine Expired Domain erneut registriert werden - inkl. der Eigenschaften, die sie bis dahin gewonnen hat.[2]

[1] beispielsweise www.expireddomains.net
[2] www.ranksider.de/talk/seo-trick-expired-domains

Beispiel:
deutsche-annington-ausbildung.de



Diese Domain gehört(e) der Deutschen Annington, mittlerweile Vonovia. Im WebArchive* findet sich ein Screenshot mit dem ursprünglich seriösen Inhalt der Seite.

Mittlerweile werden hier Adidas-Schuhe verkauft. Im Report von Domaintools findet sich als Inhaber der Domain die Person „Alex Richards“. Auffällig: im Whois Record findet sich eine unseriöse E-Mailadresse eines chinesischen Mailproviders.

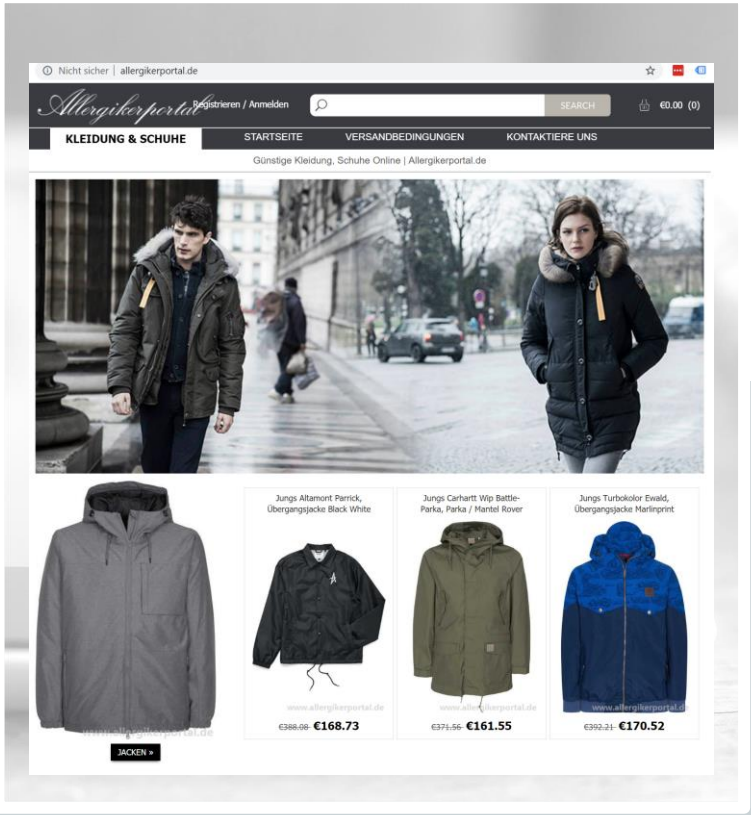
Whois Record on Jul 30, 2017

```
Domain: deutsche-annington-ausbildung.de
Nserver: ken.ns.cloudflare.com
Nserver: venus.ns.cloudflare.com
Status: connect
Changed: 2017-07-28T10:33:32+02:00

[Tech-C]
Type: PERSON
Name: Alex Richards
Address: Forggenseestr. 85
PostalCode: 87645
City: Schwangau
CountryCode: DE
Phone: +49.083628233
Email: arandalld01@163.com
Changed: 2016-08-30T02:55:03+02:00
```


* web.archive.org/web/20181123223317/http://deutsche-annington-ausbildung.de

Beispiel:
AllergikerPortal.de



Auch allergikerportal.de wurde offensichtlich für Betrugszwecke recycelt. Hier liegt nun ein Shop, welcher Jacken mit großen Rabatten anbietet.

Im Whois Record findet sich -wie beim vorherigen Beispiel auch- eine unseriöse E-Mailadresse des gleichen chinesischen Providers.

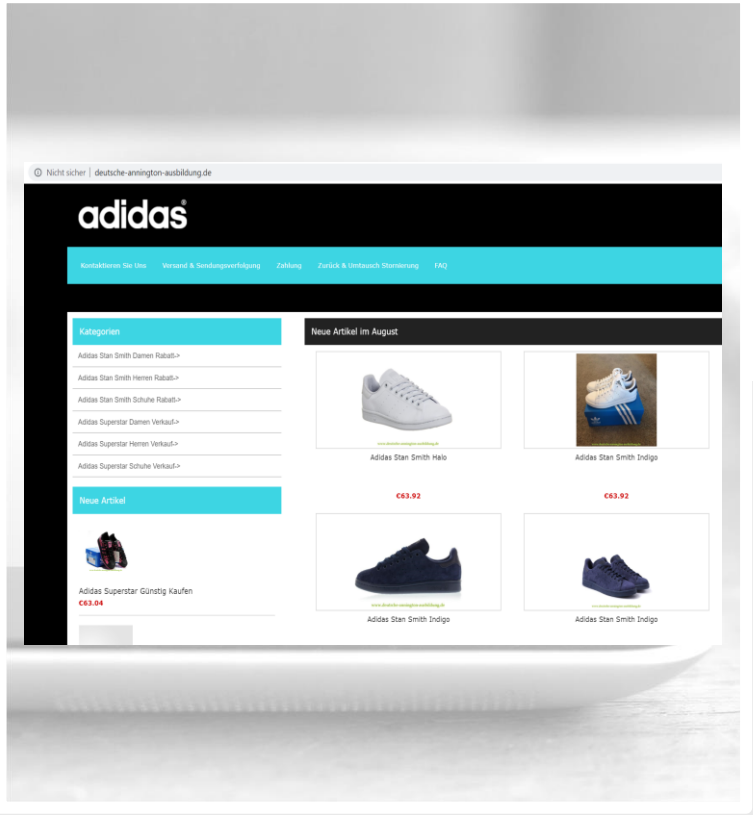
Whois Record on Nov 24, 2017

```
Domain: allergikerportal.de
Nserver: ns.gransy.com
Nserver: ns2.gransy.com
Nserver: ns3.gransy.com
Nserver: ns4.gransy.com
Nserver: ns5.gransy.com
Status: connect
Changed: 2017-11-20T07:08:10+01:00

[Tech-C]
Type: PERSON
Name: Henrik Wallin
Address: 7 rue du Fosse des Tanneurs
PostalCode: 53225
City: Bonn
CountryCode: DE
Phone: +49.03649206092
Fax: +49.03649206092
Email: wvsi18314690@163.com
Changed: 2017-11-20T04:15:07+01:00
```


wdp

Beispiel:
afroamericanhair-passau.de



Im Whois Record dieser Seite gibt es zwei Auffälligkeiten:

- Die registrierte Person „Erika Gabler“ ist die weibliche Variante des „Max Mustermanns“[1]
- Zudem ist der Provider „hxmail“ bei vielen Fakeshops im Gebrauch[2]

Whois Record on Feb 10, 2018

```
Domain: afroamericanhair-passau.de
Nserver: or.earth.orderbox-dns.com
Nserver: or.mars.orderbox-dns.com
Nserver: or.mercury.orderbox-dns.com
Nserver: or.venus.orderbox-dns.com
Status: connect
Changed: 2018-02-08T11:41:12+01:00

[Tech-C]
Type: PERSON
Name: Erika Gabler
Organisation: Erika Gabler
Address: Heidestr.17
PostalCode: 50670
City: Cologne
CountryCode: DE
Phone: +49.68949396938
Fax: +49.68949396938
Email: deysbh@hxmail.com
Changed: 2017-08-15T22:49:11+02:00
```

[1] de.wikipedia.org/wiki/Mustermann
[2] verbraucherschutz.de/tag/hxmail-com

wdp

Weitere Beispiele betroffener ausgelaufener Domains

Domains von **Parteien** auf Stadt- oder Kreisebene:
- spd-auersmacher.de
- spd-bad-wurzach.de
- cdu-bad-freienwalde.de
- cdu-bad-gandersheim.de
- cdu-beeden.de
- fdp-kreisborken.de
- fdpkverft.de
- fdpmoelln.de

Domains diverser **Vereine**:
- angelsportverein-salzwedel.de
- angelverein-rossdorf.de
- reiterverein-dahn.de
- schuetzenverein-borgholz.de

Domains eingetragener **Firmen**:
- aksel-gmbh.de
- alpha-tec-gmbh.de
- amestec-gmbh.de
- aztec-gmbh.de
- backstudio-dahlke-gmbh.de
- bege-gmbh.de
- compartgmbh.de
- doelger-foto-gmbh.de
- dogan-gmbh-ulm.de
- eyo-gmbh.de

Weitere Domains:
- akademie-verkehrundwirtschaft.de
- alesol.de

Und die DENIC?

Es dürfte rechtlich gar nicht erst möglich sein, auf diese Art Fake-Shops aufzuziehen, denn für die Registrierung einer Domain bei der DENIC gelten Voraussetzungen[1]:

- „Sie müssen rechtsfähig sein, d. h. Sie können Träger von Rechten und Pflichten sein, UND voll geschäftsfähig sein.
- Die Daten für den Domaininhaber müssen korrekt und vollständig sein.
- Sie sind dafür verantwortlich, dass Ihre Domain keine Rechte Dritter verletzt, so z. B. Namens- und Markenrechte Dritter.
- Um von vorneherein für Klarheit zu sorgen, ist bei juristischen Personen darauf zu achten, dass keine Person als Domaininhaber eintragen wird, sondern das Unternehmen."

Registrierungen unter falschem Namen sind also nicht zulässig, aber offensichtlich geduldet. Es scheint bei der Registrierung keine Verifikation stattzufinden.

Die DENIC weist offiziell die Verantwortung von sich. Auf der offiziellen Seite findet sich folgender Passus:

„Einen Zugriff auf die Inhalte von Webseiten, auf die eine Domain verweist, hat DENIC nicht. Deshalb kann DENIC auch nicht gegen Fake-Shops vorgehen oder die Inhalte einer Fake-Shop-Seite löschen."[2]

Die DENIC bietet zudem nur wenig hilfreiche Ratschläge, die im Betrugsfall kaum weiterhelfen und die Ursache des Problems nicht lösen.

Die Fake-Shops verstoßen offensichtlich nicht nur gegen die DENIC-Richtlinien, sondern kollidieren oft auch mit dem **Markenrecht,** der **Impressumspflicht** und der **DSGVO** aufgrund fehlender SSL-Verschlüsselung.

[1] www.denic.de/domains/de-domains/registrierung
[2] www.denic.de/aktuelles/informationen-zu-fake-2 shops

Durch Einführung der DSGVO ist es wesentlich schwieriger geworden, einen Fake-Shop zu identifizieren.

Vor Einführung der DSGVO hat der Domainname noch Aufschluss über betrügerische Absichten geben können.[1] Nun erhält man als Außenstehender über diverse WHOIS-Datenbanken keine Informationen mehr über den Inhaber einer Domain:

„The DENIC whois service on port 43 doesn't disclose any information concerning the domain holder, general request and abuse contact.“[2]

Auch die Politik fordert mittlerweile einen Identitätsnachweis für .de-Domains[3], um so die Erstellung von Fake-Shops zu erschweren. Warum jedoch die DENIC keine Verifikation der Registrierungsdaten durchführt und Domains mit offensichtlichen Verstößen (z. B. gegen die Impressumspflicht) nicht kündigt, lässt sich nur vermuten. Möglicherweise spielt hier eine Rolle, dass sie an jeder Registrierung verdient.

[1] webschauder.de/die-denic-und-fakeshops-sorry-aber-da-kann-man-echt-nichts-machen
[2] z. B. whois.domaintools.com
[3] www.sueddeutsche.de/wirtschaft/fake-shops-liste-politik-1.4459589

Über wdp

wdp ist eine Beratungsgesellschaft mit Spezialisierung auf digitale Geschäftsmodelle und digitale Transformation. Bei einer Due Diligence Prüfung einer Shop-Technologie erstellte wdp im Rahmen von Marktanalysen eine Übersicht über Marktanteile verschiedener Shop-Technologien, die überraschende Resultate hervorbrachte. Basierend darauf untersuchte wdp die auffälligen Shop-Technologien im Detail und identifizierte eine sehr große Anzahl an mutmaßlichen Fake-Shops. Das Resultat der Untersuchung ist Gegenstand dieses Reports.

Autoren: Christoph Nichau, Oliver Niehues
wdp GmbH // Wachter Digital Partners
Friesenwall 5-7
50672 Köln
www.wdp.de