# Domeinnaambewaking, een must-have voor steeds meer organisaties

## Analyse van 65 merk- en handelsnamen laat de omvang van het probleem zien

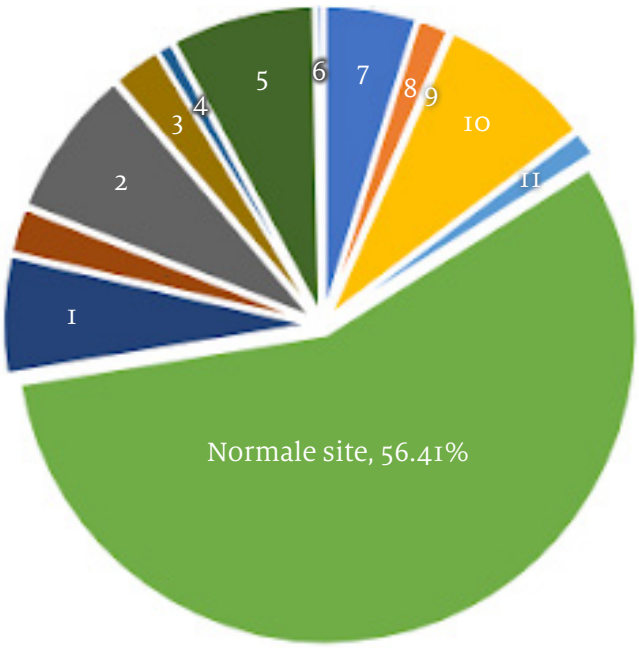
Nederlandse organisaties hebben vaak weinig zicht op het online gebruik van hun merknaam. Dat blijkt uit eigen onderzoek dat wij in september uitvoerden. SIDN onderzocht een selectie van 65 bekende merken en handelsnamen en ontdekte meer dan 10.000 .nl-registraties die niet aan de organisatie zelf toebehoorden. Bij 2,5% daarvan is waarschijnlijk sprake van malafide intenties (phishing), maar dat lijkt het topje van de ijsberg: een veel groter deel van de registraties kan onder water gebruikt worden om mailadressen van merken of organisaties na te bootsen.

## 10.269 resultaten, meer dan 150 domeinnamen per merk

Voor organisaties lijkt het monitoren van het internet soms onbegonnen werk. De analyse van 65 merken laat zien waarom: met 150 resultaten per merk die regelmatig veranderen zie je soms door de bomen het bos niet meer. Wanneer wij de resultaten van onze analyse grafisch weergeven ziet dat er als volgt uit, zie afbeelding 1.

## 2,5% in lijn met eerdere metingen

Het percentage phishingsites is daarbij al jaren stabiel tussen de 2 en 4%, maar wel met een kanttekening: phishingwebsites worden steeds sneller offline gehaald. Mede dankzij het door SIDN geïnitieerde programma Abuse204.nl drongen we samen met de .nl-registrars de gemiddelde uptime van phishingsites en malware enorm terug van gemiddeld 144 uur in 2017 naar 21 uur dit jaar. Wanneer het percentage gevonden phishingsites in 2021 gelijk is aan dat in 2017, betekent dit dus dat het aantal malafide registraties fors is toegenomen. Ze worden bovendien steeds sneller gedetecteerd.




*Afbeelding 1: De analyse van 65 grote merken op hoofdlijnen*

1. Ongebruikt - 6.15%
2. Reageert niet - 7.18%
3. Reclamenetwerk - 2.54%
4. Redirect naar originele domeinnaam - 0.82%
5. 'Te koop' site - 7.52%
6. Verwijderd - 0.32%
7. Adult - 4.83%
8. Alleen e-mail - 1.63%
9. Domein vrij - 0.08%
10. Geparkeerde site - 8.14%
11. Niet van toepassing - 1.36%

## Cybercriminelen verbreden en specialiseren

De betere tegenmaatregelen betekenen dus niet dat cybercriminelen de handdoek in de ring gooien. Integendeel. Ze richten zich op een bredere groep doelwitten. Vooral in het mkb. Afgelopen jaar zagen wij voorbeelden van domeinnaammisbruik bij een **groothandel in Aziatische snacks** en een **transportbedrijf**. Veel mkb'ers verkeren nog steeds in de veronderstelling dat zij geen interessant doelwit zijn. Cybercriminelen profiteren daarvan. Mede daarom koos SIDN dit keer voor een analyse van 65 geselecteerde merken en niet alleen voor de 50 bekendste.

## Meer dan één dreiging

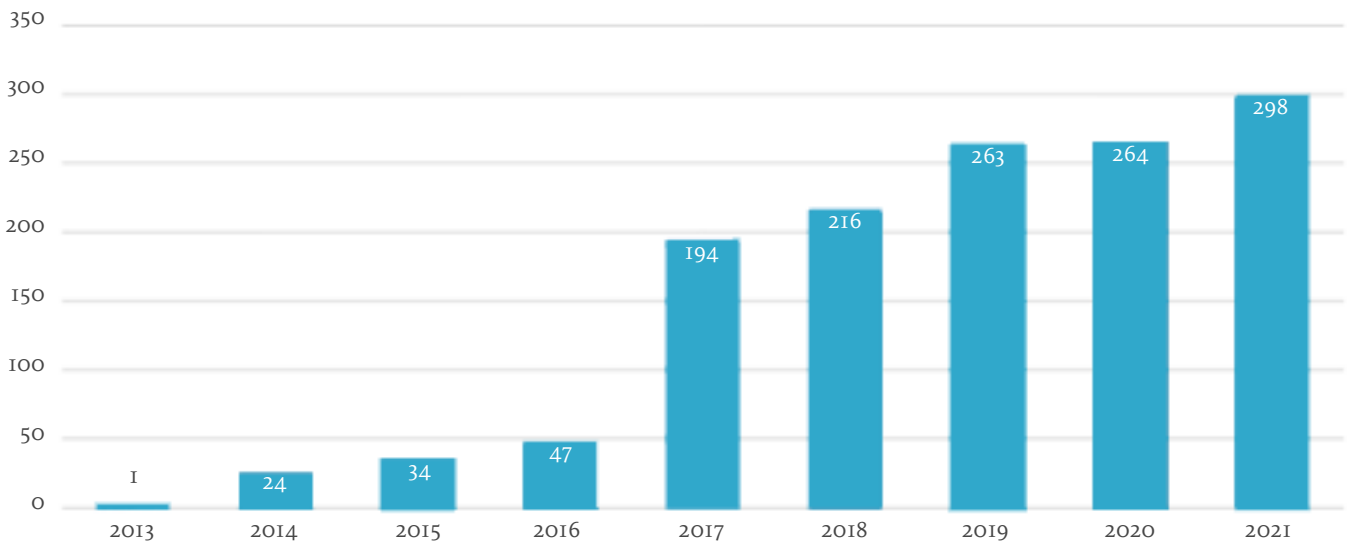
Zonder tooling kan het dus een hele klus zijn om de phishingsites (2,5%) eruit te halen. Er zijn bovendien meer aandachtspunten. Zo gebruiken spammers vaak een redirect naar de originele bedrijfswebsites, om bij ontvangers de indruk te wekken dat ze bij dat bedrijf horen. Ook het te koop aanbieden van domeinnamen met de merknaam erin is, hoewel niet illegaal, wel in strijd met het intellectueel eigendomsrecht.

## Naast malafide is er ook ongewenst 'bonafide gebruik'

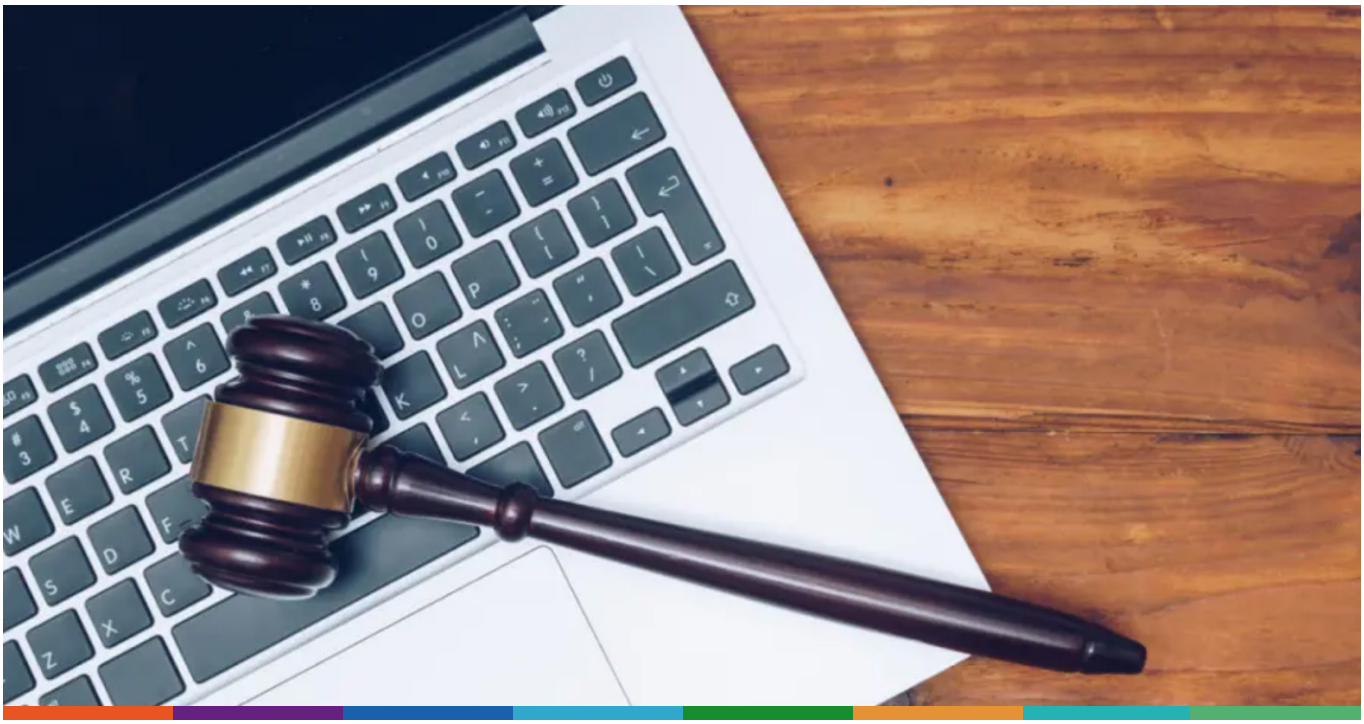
Veel bedrijven zijn zich er niet van bewust maar ook bonafide gebruik van hun domeinnaam is soms ongewenst. Tal van domeinnamen van een merk staan op naam van (ex-)medewerkers, partners of leveranciers. Vaak vinden registraties met goede bedoelingen plaats, maar raken ze uit beeld als bijvoorbeeld de relatie met de leverancier verbroken wordt. Ook bedrijven die een marketingprogramma bieden, waarbij ze derde partijen betalen voor verkeer naar hun site (zgn. affiliate marketing) moeten oppassen: sommige partijen registreren typo's op hun merk en laten het merk zo betalen voor verkeer naar de eigen site. Vooral bij loterijen komt dit veel voor. Een voorbeeld uit onze analyse is de domeinnaam saatsloterij.nl.

## Tools ontwikkelen mee

Steeds meer organisaties gebruiken domeinnaambewakingstools. Zo wordt SIDN Merkbewaking in Nederland al gebruikt om 300 grote merken te bewaken. Om cybercriminelen nog beter op te sporen moeten de tools die hiervoor gebruikt worden beter worden. Gelukkig is dat het geval. Zo gaat SIDN Merkbewaking vanaf 2022 ook logo's op mogelijk malafide websites detecteren en komt er een nieuwe crawler, waarmee zoekresultaten nauwkeuriger geclassificeerd worden. Dit verkleint de kans dat een phishingwebsite door de mazen van het net glipt.




*Afbeelding 2: Aantal merken bewaakt door SIDN Merkbewaking*



### Wat te doen als je merkinbreuk spot?

Veel bedrijven zijn zich er onvoldoende van bewust dat ze ook zonder tussenkomst van de rechter tegen online merkinbreuk kunnen optreden. Dat is meestal goedkoper, makkelijker en sneller dan naar de rechter. Voor .nl is die geschillenregeling te vinden op **sidn.nl**. De registry's voor .com en andere niet-landgebonden extensies vind je op de website van de verantwoordelijke registry of op **ICANN.org**.

### Bewaak je merk online!

Aandacht voor online gebruik van de eigen merk- of handelsnaam blijft dus belangrijk. Het voeren van een actief domeinnamenbeleid en regelmatig domeinnaamregistraties monitoren die lijken op de naam van je bedrijf horen daarbij. Ook het beveiligen van mail met veilige internetstandaarden zoals DMARC zou steeds meer prioriteit moeten krijgen. Mkb'ers moeten zich realiseren dat elk bedrijf, ook de kleinere, een interessant doelwit kunnen zijn voor cybercriminelen en zich hierop voorbereiden.

| | .nl | .com (en andere niet-landgebonden extensies) |
|---|---|---|
| Inbreuk op intellectueel eigendomsrecht | • Geschillenregeling voor .nl-domeinnamen<br>• Rechter | Uniform Domain Name Dispute Resolution Policy (ICANN.org) |
| Onrechtmatige content | • Notice-and-Take-Down-procedure (EU) | Notice-and-Take-Down-procedure (US) |
| Klacht over registrar | • Geschillencommissie | Uniform Domain Name Dispute Resolution Policy (ICANN.org) |

*Tabel 1: De opties voor een geschil rond domeinnamen*

## Wat is SIDN Merkbewaking?

SIDN Merkbewaking is een **monitoringservice** met als doel typosquatting en merkinbreuk op het internet op te sporen. Typosquatting is een vorm van internetmisbruik gebaseerd op het feit dat internetgebruikers zich wel eens vergissen bij het intypen van een website- of mailadres. Deze vorm van misbruik kan schade toebrengen aan de betrouwbaarheid van jouw merk en vormt vaak het begin van gerichte phishingaanvallen, waarbij (persoons)gegevens worden geconfisqueerd via een valse website.

SIDN Merkbewaking maakt gebruik van een rechtstreekse koppeling met de database van alle .nl-domeinnamen, waardoor alle .nl-typosquats rondom jouw merknaam realtime worden gecontroleerd. Voor andere top level domeinen (o.a. .com) downloadt SIDN Merkbewaking iedere 24 uur de database met alle domeinnamen of doorzoeken wij deze met een zogenaamde 'domain name spinner'. Wij bieden je via een webinterface inzage in de resultaten, daarnaast bieden wij een API die geïntegreerd kan worden met jouw systemen (XML).

**SIDN Merkbewaking is een monitoringservice met als doel typosquatting en merkinbreuk op het internet op te sporen.**

## Meer informatie

Wil je meer weten over SIDN Merkbewaking of over wat SIDN nog meer voor je kan betekenen, neem dan contact op met Peter Rotgans, specialist domeinnaammonitoring, via de onderstaande gegevens of kijk op de website **www.sidn.nl/sidn-merkbewaking**.

**Neem contact op met:**

Peter Rotgans
peter.rotgans@sidn.nl
+31 26 352 55 55