No 13, Q1 2014

The.nlyst

LOCAL ANYCAST: SIDN'S LATEST WEAPON AGAINST DDOS ATTACKS

SIDN becomes first registry to site DNS servers 'in the field'

Anycast is a widely used technology for boosting the availability of servers. Increasingly frequent and fierce DDoS attacks prompted SIDN to decide that DNS anycast capability should also be installed at local third-party sites, such as at large ISPs and hosting firms. SIDN is the first registry to set up a local anycast network of this kind. Erwin Heringa, Network Manager, and Marc Groeneweg, ICT-Project Leader have been sharing their inside knowledge with The.nlyst.

Marc Groeneweg,
ICT-Project Leader

No longer unwitting accomplices

SIDN has an impressive DNS infrastructure, which can handle thousands of DNS queries per second. One consequence of having such a powerful infrastructure is that trouble-makers can abuse it to amplify DDoS traffic. "We've been seeing that a lot in the gaming industry recently. Gamers launch attacks on their rivals or try to take down big gaming platforms," says Marc Groeneweg. "By response rate limiting – controlling malicious DNS traffic – SIDN can greatly reduce the impact, meaning that we are no longer unwitting accomplices in DNS amplification attacks.

As well as the problem of DNS amplification attacks on third parties, there is a risk of SIDN itself being targeted by DDoS attackers. "Until recently, we would handle DDoS attacks by deploying more DNS capacity," explains Groeneweg. "Although that remains a useful tactic, an upward spiral of capacity increases isn't ultimately a solution." SIDN therefore decided to look for another way of addressing the problem and settled on local anycast.

Global anycast: proven technology

Global anycast is a proven and very effective technology, which has been in use for the root name servers for some time. At SIDN too, global anycast has long been used to increase the availability of the .nl domain. The principle is as simple as it is effective. A number of servers share a single IP address, making routers 'think' that they are all the same server. IP packages are therefore forwarded to the 'nearest' point, with the result that the total network load is distributed across the multiple instances of the server.

Erwin Heringa,
Network Manager

Local anycast

Local anycast differs from global anycast insofar as a number of local nodes are involved. Smart routing means that the nodes can only be approached locally. As a result, worldwide DDoS traffic, cannot ever reach a local ⊖

Foreword

The internet is now the global medium for communication, information exchange, social interaction, collaboration and commerce. It has become a crucial factor in the economic and democratic development of nations, the success of businesses and the personal development of individuals. We go on line to do our work, chat with our friends, air our views and share experiences with the world. We look to the internet for news and entertainment, and we use it to manage our finances, play games and buy everything from clothes, to food or a new smartphone.

However, the internet's success has a down side. Precisely because it is so important to society and the economy, it is increasingly a medium or a target for regimes, criminals, terrorists, vandals and sad individuals who simply want to show off what they can do. In 2013, we saw more incidents than ever. The customs service, the tax service, Dutch Railways and various Dutch banks all fell victim to DDoS attacks. A large-scale attack on Spamhaus, the non-profit organisation that plays a leading role in controlling spam, even caused large parts of the internet to slow down. Worryingly, it seems that attackers and defenders are increasingly locked in an endless war.

The 'good news' is that, following the recent spate of high-profile incidents, people in government and the business community are taking much more interest in security and stability, and starting to make the necessary investments.

SIDN attaches great importance both to its own security and to the general security of the internet. Our particular role means that we too are a target for wrongdoers. We therefore have a large array of protective systems, including a local anycast network, established last year. We are the first registry to collaborate with internet service providers on such a project. More information about the initiative is provided in this edition of The.nlyst. The magazine also features news of an innovative monitoring service for .nl domain names and an article describing how registrars are joining forces to head off DDoS attacks.

The internet will realise its full potential only if its availability is stable everywhere and if users not only feel safe but are safe. At SIDN, we strive daily to secure those goals.

Roelof Meijer,
CEO

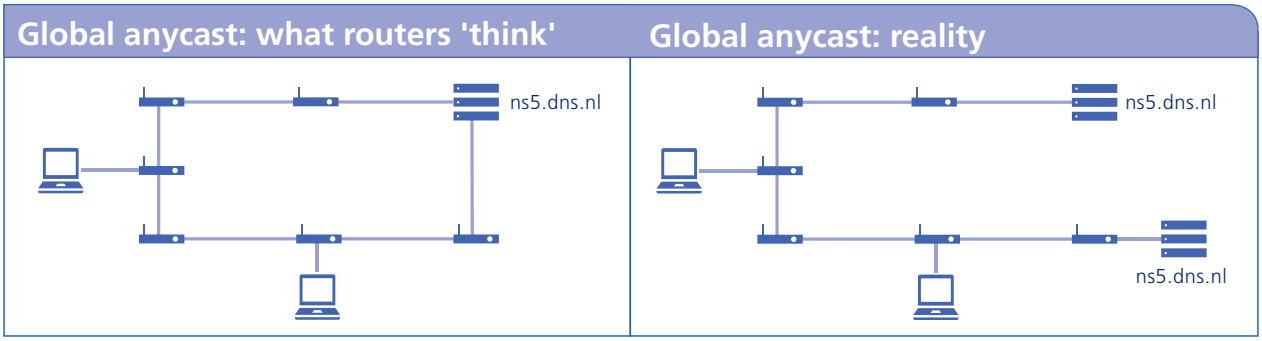
node, regardless of the traffic volume. The only DDoS traffic can reach the node is locally generated traffic, which is much easier to control. Consequently, in the event of an attack that cannot be isolated because of its size, local anycast servers provide extra capacity that can be used to fight off the assault. SIDN's local anycast set-up has been devised and built in house. And, in the course of the project, a great deal of knowledge has been built up. "We already had a lot of DNS know how," points out Marc Groeneweg, "and we've now added expertise in the field of routing. The project combines numerous interesting control features. Naturally, we will continue refining and developing the system. We are learning all the time."

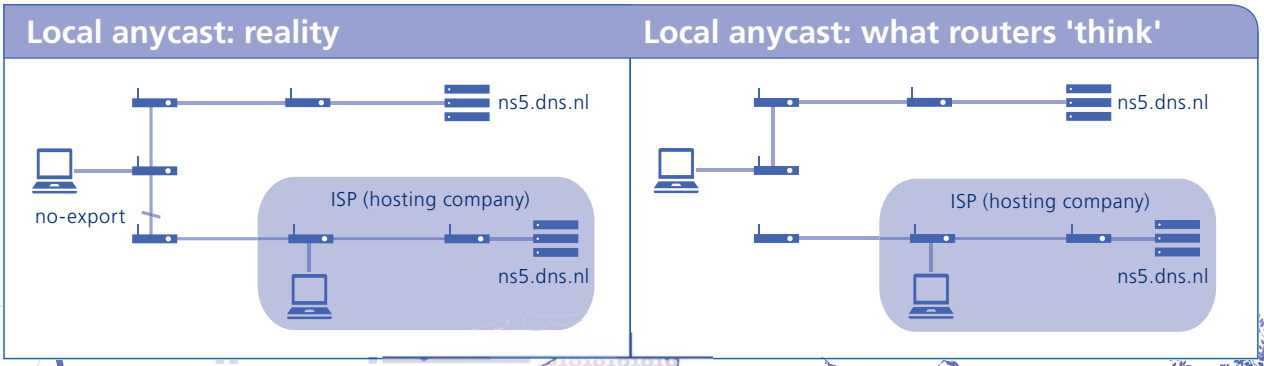
Dedicated and shared nodes

SIDN's local anycast-technology is attractive mainly to large ISPs and hosting firms. "If SIDN's .nl services were hit by DDoS attacks, the .nl domain would remain available to our anycast partners because of having their 'own' local anycast servers," explains Erwin Heringa. The first company on board was hosting firm LeaseWeb, which was enthusiastic about SIDN's vision from the start and had no hesitation about making the necessary data centre facilities available. Before long, 'dedicated nodes' were set up at various Dutch ISPs, including UPC, KPN and XS4All. SIDN also has so-called 'shared nodes' – local anycast servers that are shared by several firms – which are attractive mainly to smaller players. One of the shared nodes is housed at AMS-IX and is already being used by a number of internet firms.

Attractive for a variety of internet companies

Local anycast is relative straightforward to implement and has numerous advantages. One might therefore expect that many registries would be using it. However, SIDN is the first to introduce local anycast. "I believe that the German registry was at one stage planning to add local anycast capability," observes Erwin Heringa. "But they were reluctant to give the project participants a commercial advantage over other hosting firms. However, our technology is in principle available to any hoster that wants it, so we don't have the problem that the Germans had." SIDN therefore anticipates deploying more local anycast servers in the period ahead. Any hosting firm can ask to participate, but SIDN does attach a number of conditions to acceptance. For example, a firm must have a sound policy for tackling abuse and must be IPv6-enabled. If you would like to know more about SIDN's local anycast or to become one of SIDN's anycast partners, please contact our Account Manager Daniël Federer on daniel.federer@sidn.nl.





"NO ONE LIKES TO TALK ABOUT IT"

Two registrars discuss DDoS attacks

DDoS attacks are an increasingly common problem for hosting firms. Rob van den Nieuwelaar, CEO of Hosting2GO, and Erik Logtenberg, CEO of VEVIDA and Chair of the Registrars' Association, describe how their companies deal with the issue.

How common are DDoS attacks?

Erik Logtenberg: "In the second half of 2013, there was a big upsurge. Before that, it was mainly prominent websites that were targeted. Now it seems that the attackers are liable to pick on almost anyone."

Rob van den Nieuwelaar: "The issue hasn't received much media attention. No one wants to talk about it. Companies don't want people to think that they are vulnerable. And, if you publicise the fact that you've put all sorts of measures in place to defend yourself, you can bet that someone out there will see getting round your defences as a challenge to their ingenuity."

How much trouble do DDoS attacks cause you?

Erik Logtenberg: "We come under fire maybe a few times a month. The attacks aren't just annoying; they are costly. Defending yourself is an expensive business and you can't pass on the whole cost to your customers."

Rob van den Nieuwelaar: "Part of the problem is that customers don't always accept a DDoS attack as a valid reason for their website or e-mail going down. The situation isn't helped by the fact that some service providers use the term 'DDoS' to gloss over a technical fault or human error. So, when there's a real attack, it can be difficult to convince customers that we aren't making excuses."

Rob van den Nieuwelaar, CEO Hosting2GO

What kinds of business do the attackers tend to target?

Erik Logtenberg, CEO of VEVIDA

Rob van den Nieuwelaar: "We've certainly noticed that some sites are more likely to be targeted than others. Favourites seem to be porn sites, websites where you can download illegal software and forums where very extreme views are promoted. An attack will often begin with a row in a forum or with a period of fierce competition between rival sites. In the first of those cases it's usually fairly easy to identify the target – often the busiest forum on a server – and the attack will typically be quite short-lived. In the second case, the attack will usually be more professional, larger scale and harder to fight off. Really, it's just a form of digital terrorism."

Erik Logtenberg: "The attacks aren't just vindictive: they regularly involve extortion. A small webshop will get brought down and afterwards they'll receive an e-mail telling them that they can avoid further trouble by paying a certain amount in Bitcoins."

And do the victims pay up?

Erik Logtenberg: "Some of them must do. Otherwise the racketeers wouldn't keep doing it. But we always advise against paying. Because you might pay off the one gang, but what's to stop another coming along with the same demands? Your first extortionist can't protect you against the copycats."

Can the police do anything?
Rob van den Nieuwelaar: "Victims of DDoS attacks hardly ever report the matter to the police. After all, the police have very little expertise in this area, the culprits are hard to trace and evidence is almost impossible to obtain."

Erik Logtenberg: "Whenever I speak to people involved in law enforcement, it's clear that they're just not active in this field. When it comes to the internet, all their efforts are focused on child pornography and cybercrime against banks. The extortion of a few hundred euros apparently isn't worth their while."

What damage does a DDoS attack do?
Rob van den Nieuwelaar: "Well, there's the direct financial cost, but for companies like ours the real issue is the damage to our image. Customers get annoyed if their sites suffer problems, and the worry is that they will then take their business elsewhere. Fortunately, that hasn't really happened to us much. Our customers understand that the problem affects the whole industry."

What do you do to protect against DDoS attacks?
Rob van den Nieuwelaar: "Minor DDoS attacks can be warded off automatically by our own systems. But there isn't really an automated system that can protect against a major attack. You have to do it manually."

Erik Logtenberg adds: "The only way to defend against attacks that use up huge amounts of bandwidth is to enormously increase your capacity. Not many providers in the Netherlands have the resources to do that, so the answer has to be hiring extra capacity from an international source. That's an effective response, but also an expensive one."

The NBIP is setting up an anti-DDoS service, which enables providers to share the cost of response measures. What do you think of that initiative?
Erik Logtenberg: "I must admit I haven't heard about that, but it sounds like a good idea. The companies that offer anti-DDoS services are used to working with heavy capacity users, such as banks and government agencies, who can bear the financial cost. It's very different for a small hosting firm. Sharing the cost would certainly make a difference."

Do you foresee any end to the problem of DDoS attacks?
Erik Logtenberg: "Not really, no. The principle of a DDoS attack – swamping the infrastructure with more traffic than it can handle – is just too simple. Of course, we can address certain tricks that the attackers use, but they'll just come up with new ones."

Rob van den Nieuwelaar: "I think that there's quite a lot that we can do. The first time that it happened to us, our servers were struggling for an entire night. Now we can neutralise an attack like that within a few minutes. It's still a matter of baling while water pours in. But, for the moment at least, we're able to bale faster than we're taking on water."

Erik Logtenberg: "We can certainly fight off some attacks effectively enough. If mounting an attack costs criminals more than it earns them, they won't continue. But you'll never deter people from mounting attacks to make a statement."

SIDN STARTS TYPO HUNT

Domain Name Surveillance Service identifies typosquats

SIDN recently completed a successful pilot of the Domain Name Surveillance Service – a new product developed by the Dutch registry. The pilot was run in collaboration with a major financial services provider. Daniël Federer, SIDN's Key Account Manager, explains.

What is the Domain Name Surveillance Service?

"It's a tool for identifying cases of typosquatting: a form of abuse that takes advantage of the fact that people sometimes make slips when typing web and e-mail addresses – the so-called 'fat fingers phenomenon'. You might accidentally type 'amsterdan.nl' instead of 'amsterdam.nl', for example. Squatters register domains corresponding to common typing errors. Then, if you make a slip at the keyboard, you find yourself looking at the squatter's site – which may simply be loaded with adverts, but may also host malware. Another trick is to send e-mails that purport to come from a trusted organisation's domain, when in fact they come from a domain with almost the same name and are designed to con the recipient into revealing personal information. Phishing often begins with typosquatting."

What impact does typosquatting have?

"Websites operated by typosquatters can do a lot of damage. Considerable sums are lost to phishing scams all the time. And, crucially, abusive activities undermine user confidence, which is a serious issue for banks and other companies whose business models depend on trust. Early detection of new typosquats associated with their domain names is very important for such businesses."

How does the Domain Name Surveillance Service work?

"The Domain Name Surveillance Service is linked to the database of all registered .nl domain names. The system scans the database for names that are similar to the protected domain name. For example, a subscriber is alerted to the registration of a name consisting of 'my' plus the protected name (e.g. my-anybank.nl), or a name that is only one letter different from the protected name (e.g. anybamk.nl). Every user of the Domain Name Surveillance Service (DNSS) has access to a web interface where potentially significant recent registrations are listed. The user can also opt to receive e-mail alerts whenever the surveillance system detects a similar domain name, so that swift action can be taken if the need arises."

Daniël Federer,
Key Account Manager

What is the background to the new service?

"At the end of 2012, SIDN set up an innovation programme. The DNSS was the first new product idea developed through the programme. While we were working on it, I mentioned the project to a major financial services provider during one of our regular discussions. They liked the idea straight away, so the pilot was set up soon afterwards. The most challenging aspect of the development was not devising the technology, but deciding what data we could make available. What was permissible, what was desirable, what was possible? And, in the end, what are the benefits?"

Did the pilot throw up any surprises?

"Yes. We discovered that the service was also very useful as a compliance tool. Some large companies act as registrars themselves, because they have strict security requirements and rules on the registration of domain names – rules that not everyone in the various departments and local offices is aware of. So, if for example a marketing department registers a name for a campaign website through an outside registrar, the company gets an alert, enabling them to take the necessary internal steps."

Who is the Domain Name Surveillance Service aimed at?

"At the moment, we think it's useful mainly for a small number of large companies with strong brands, strong reputations or websites where valuable data are processed. Examples would include banks and government agencies. However, we are already working on variants of the product, which would enable other types of organisation to benefit – perhaps through an intermediary, such as the registrar that manages their domain name."

What remains to be done in terms of development?

"We'll start by talking to the Registrars' Association about the best way of tailoring the product to the market. We would like to add additional intelligence, for example, in the form of risk profiles. That would enable us to qualify typosquats, so that a company can quickly and easily see whether a registration actually represents a threat. We are also looking into the possibility of using the DNSS to additionally monitor registrations under other top-level domains besides .nl."

What are typosquats used for?

- To attract visitors. Typosquats are often used to get you to visit a squatter's website. You might find yourself looking at an on-line casino site, an advertising page or even the website of a rival of the company you were trying to reach.
- Phishing. Criminals will often create a website that looks very like the site of a well-known bank or webshop. If you make a typing error or click a link in a phishing mail, you find yourself on the look-alike website. If you don't realise that the site is a fake, you may go ahead and enter your password or your credit card details.
- Propagating malware. Domain names that are very similar to those of well-known companies are frequently used to trick people into visiting websites or opening e-mails that install harmful software – computer viruses, adware, spyware etc – on your computer.
- Satire and parodies. Some typosquats are used for websites that merely ridicule the owners of the domain names that they resemble.

"WE CAN GET THE RIGHT PEOPLE TOGETHER WITHIN TEN MINUTES"

A look at SIDN's Computer Security Incident Response Team

SIDN does all it can to make the .nl domain as secure as possible. Nevertheless, the company was the victim of a hack on Tuesday 9 July 2013, when unauthorised files were found on one of its web servers. Security Officer Bert ten Brinke immediately convened SIDN's Computer Security Incident Response Team (CSIRT), which took swift action to ensure that the impact of the hack was minimised.

Bert ten Brinke, security officer

Quick response

When a computer system is hacked or a virus is detected, it is important to respond quickly and effectively. To that end, it is helpful to have a single command and control point. Most companies of any significant size therefore have a special 'computer security incident response team' (CSIRT). SIDN's CSIRT is ready to react at any time

of the day or night. “Incidents don't only happen during office hours,” emphasises Bert ten Brinke. “And security is extremely important to SIDN. Our primary task is to resolve faults as quickly as possible. Some problems are relatively minor and can be dealt with by one CSIRT member on their own. Others require the whole team to work together. However significant an incident may be, we can get the right people together and ready for action within ten minutes.”

First contain the damage ...

The first objective is always to contain the damage. “When the hack was discovered in July, several of us worked through the night to stabilise the situation,” Ten Brinke recalls. “We isolated the compromised server as quickly as possible and reset all the accounts for our domain registration system. As an additional precaution, we delayed the publication of further updates to the zone file – the file that lists all .nl domain names – even though that is handled by a separate system. Fortunately, there was never any threat to the .nl zone and registrars were able to go on registering domain names as usual via the EPP interface.”

... then find the cause

Resolving a problem is one thing; removing the cause is another. All SIDN's systems were fully operational within two days of July's hack coming to light, but follow-up activities continued for some time. A server had to be reconfigured and various tests carried out, including a forensic analysis. “After an incident, it's important to establish exactly what happened and how it was able to happen. So every incident teaches you something,” explains Ten Brinke. On the basis of its findings, the CSIRT makes recommendations about how SIDN's security can be improved. “But we can never guarantee that nothing else will go wrong,” says Ten Brinke. “The difficulty with internet security is that you are always responding to what hackers are doing. It's an endless game of cat and mouse. We counter one threat, so the hackers look for new ways in. When they find one, we act to close it.”

Since 1988

The world's first computer incident response service was set up in 1988, following the outbreak of the Morris computer worm. This worm spread quickly across much of the internet, crippling servers and leaving many users without e-mail and other services. Because of its success with Morris, the Computer Emergency Response Team (CERT) became a model that was copied around the world. Nowadays, almost all large organisations and nations have their own CERT. In the Netherlands, the national CERT role is played by the NCSC, the National Cyber Security Centre.

Good communication

In the event of an incident such as the hack in July, good communication is vital, Ten Brinke stresses. “The best approach is to communicate openly and honestly with all stakeholders. However, there's an art to doing that without giving the hackers information that they can use to their advantage. The information we put out during the incident in July 2013 was well received by registrars. So we now update them regularly on what we are doing to make .nl and our systems even more secure.”

SIDN's CSIRT is affiliated to FIRST – an international forum in which teams from all around the world exchange technical information and share best practices.

THE RIGHT SOLUTION FOR EVERY DDOS ATTACK

NBIP makes DDoS readiness affordable for ISPs

The National Management Organisation for Internet Service Providers (NBIP) – which helps ISPs to meet their statutory obligations under the Telecommunications Act – will soon be launching an anti-DDoS service. NBIP's CEO Alex Bik has been talking to The.nlyst about the initiative.

Alex Bik, Chair of the NBIP

Fulfilment of wire-tap orders

NBIP was established a little more than ten years ago, following amendment of the Telecommunications Act in 2002. "The revised Act placed a statutory responsibility on ISPs to fulfil wire-tap orders," said Alex Bik. "If ordered to implement a wire-tap, a provider has to intercept and filter the relevant data traffic, then forward it in accordance with certain standards. That all requires special hardware and software, the cost of which is unsupportable for small and medium-sized ISPs. So a group of them decided that the way forward was to work together and share the costs. NBIP was established as a vehicle for the collective realisation of wire-tap capability." The foundation began with ten members, but now supports about a hundred ISPs.

Mandatory response to DDoS attacks

NBIP's new anti-DDoS service also has its origins in the Telecommunications Act. "The legislation has recently been amended again," explains Bik. "It now includes requirements about provider continuity as well. DDoS attacks threaten that continuity, so ISPs need to be ready to counter them. And, again, that implies expensive equipment – hundreds of thousands-worth of hardware. So, just as with the wire-tap systems, there is a big incentive for sharing the cost, and NBIP is ideally placed to enable that."

Every attack requires its own solution

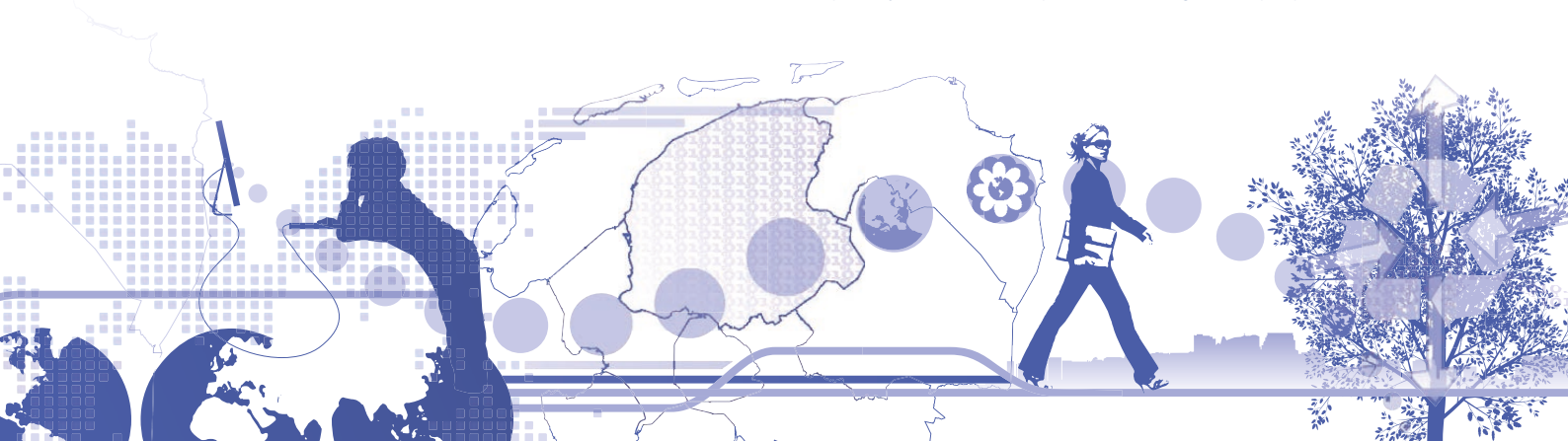
DDoS attacks are not all the same, says Bik. "Sometimes an attack is targeted on a particular part of a website, but at other times the tactic is simply to try to bring a service down by using as much bandwidth as possible. Each type of attack requires a different solution. There's no silver bullet. It's almost impossible for a small ISP to retain comprehensive response capability in house. But, as a national organisation, NBIP can maintain that kind of capability. We have brought the best solutions together at a central location connected to AMS-IX. If one of our members is attacked, all the traffic for the member in question is diverted to us. We filter out as much of the suspect traffic as possible and forward the rest. Our service works like an automated car wash for data traffic at the national level."

Successful test

Testers are currently putting NBIP's anti-DDoS service through its paces. Bik is very pleased with the way the tests are going: "The system is working exactly as we expected. Fifteen members have so far indicated that they would like to use the service, and we expect a lot more ISPs to subscribe when we roll out anti-DDoS in the near future."

Less impact, but attacks unlikely to end

NBIP's anti-DDoS service will certainly help small and medium-sized ISPs to ward off DDoS attacks more quickly. Bik nevertheless stresses that the attacks won't simply stop. "I can't imagine that our initiative will stop DDoS attacks happening. What we can do is reduce the impact. And, hopefully, that will help to discourage the perpetrators."



.NL Analysed

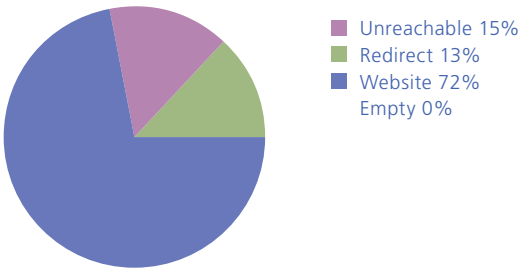
#	TLD		Count Q4	Growth	
1	.com	Generic	111,839,466	1.1%	=
2	.tk	Tokelau	21,131,593	10.2%	=
3	.de	Germany	15,592,379	0.7%	=
4	.net	Generic	15,166,881	0.4%	=
5	.cn	China	10,829,480	1.0%	↑
6	.uk	United Kingdom	10,550,763	0.7%	↓
7	.org	Generic	10,366,672	4.3%	↓
8	.info	Generic	5,836,808	-4.6%	=
9	.nl	Netherlands	5,388,364	1.0%	=
10	.ru	Russia	4,918,923	3.1%	=
11	.eu	European Union	3,709,860	-0.5%	=
12	.br	Brasil	3,310,867	2.8%	=
13	.ar*	Argentina	2,920,000	2.5%	=

#	TLD		Count Q4	Growth	
14	.au	Australia	2,754,959	1.9%	=
15	.fr	France	2,716,055	2.3%	=
16	.biz	Generic	2,632,683	1.2%	↑
17	.it	Italy	2,630,900	1.5%	↓
18	.pl	Poland	2,461,509	1.6%	=
19	.ca	Canada	2,150,831	1.5%	=
20	.ch	Switserland	1,837,020	1.2%	=
21	.us	United States	1,796,591	0.4%	=
22	.es	Spain	1,696,538	1.8%	=
23	.co*	Colombia	1,690,000	4.5%	=
24	.be	Belgium	1,433,990	1.7%	=
25	.jp	Japan	1,356,102	0.8%	=
	* estimate				

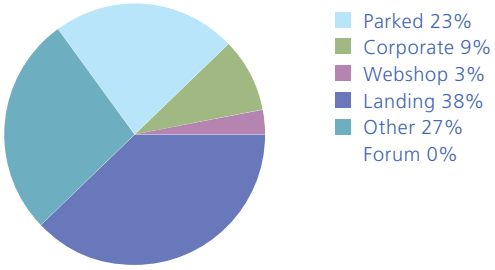
Top 25 TLDs

By the end of 2013, the total number of registered domain names was nearly 271 million – 20.5 million more than a year earlier. The growth was less than that seen in 2012 (when the total went up by 25 million names), but was up on the period 2009 to 2011. Overall growth in the number of domain names remained strong, but was driven by a smaller number of TLDs than in the past. Most extensions saw reduced rates of growth. The ccTLDs were responsible for 73 per cent of the net growth, with .tk accounting for 33 per cent of the total growth. Notably, however, .tk's growth in the final quarter of the year was the lowest recorded since records began (Q2 '12). Because of the limited horizon, it is not yet possible to identify a cause for the reduced growth rate. By contrast, China's .cn increased its rate of growth in the final quarter.

Use of .nl



Classification of websites



Use of .nl

Since the middle of 2013, SIDN has had an analytical tool, which sheds light on the way .nl domain names are used. To build understanding of the usage patterns, we now scan all active .nl domain names on a frequent basis. First, each domain name is placed in one of four general usage groups:

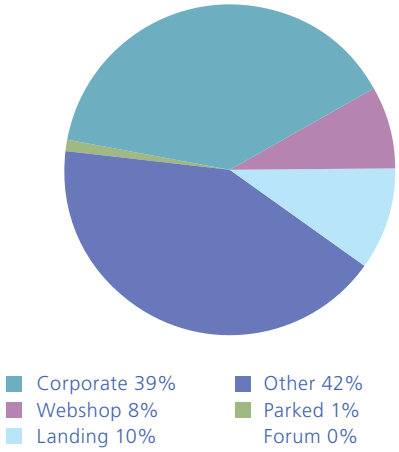
- Website: the domain name is reachable and there is a website associated with it
- Redirect: traffic is redirected to another other domain name
- Empty: the domain name is reachable but there is no website associated with it
- Unreachable: the domain name cannot be reached

Classification of websites

Domain names that have websites associated with them are then classified according to the type of site:

- Webshop: the website is an (on-line) store offering goods for sale
- Corporate: the website relates to a company or organisation, but goods are not sold via the site
- Forum: the website is a discussion platform
- Other: the website does not fall into any of the other categories
- Landing: the website consists of only a notice such as 'Website undergoing maintenance' or 'Website of XYZ coming soon'
- Parked: the website consists of a holding notice of the type often displayed by ISPs once a domain name has been registered, but before the registrant has associated a website with the name

Type of redirect



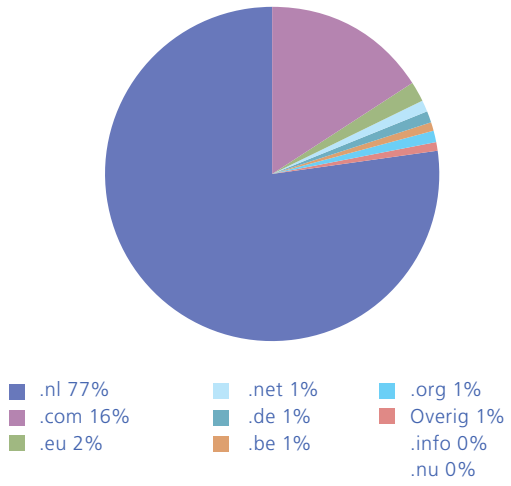
Type of redirect

We know that many domain names are registered for brand protection, for future projects, and for other similar purposes. Many such domain names have no website associated with them, but are set up as 'redirects', sending traffic to other domain names. Our analytical tool provides information about redirects as well, enabling us to classify the domain names that the redirects point to, in the same way as primary websites. Not surprisingly, most of the sites turn out to be commercial websites.

Redirect per TLD

As well as analysing the types of site the redirects point to, we can build up a picture of the TLDs involved, as illustrated below. The graph shows a clear correlation with the extensions most widely used in the Netherlands. Many redirects point to .com (globally the biggest TLD) and to the extensions of neighbouring countries: .be, .de and, of course, .eu. We have found redirects to a total of 110 different TLDs.

Redirect per TLD



Event calendar

In the coming months, SIDN plans to be represented at the following events:

Date	Event	Venue
27-02 to 28-02	13th CENTR Marketing Workshop	Frankfurt, Germany
06-03	43rd CENTR Legal & Regulatory Workshop	Rome, Italy
02-03 to 07-03	89th IETF	London, United Kingdom
12-03 to 13-03	51st General Assembly	Stockholm, Sweden
24-03 to 27-03	49th ICANN Meeting	Singapore
01-04 to 03-04	World Hosting Days	Rust, Germany
12-04	ISP Kart Competition	Maarssen, The Netherlands

SIDN supports campaign to protect children against identity hacking

Identity hacking is making unauthorised use of photos or other personal information – for creating fake Twitter accounts or fake Facebook profiles, for example. Unfortunately, the practice isn't always about the satirisation of politicians or celebrities, but can involve the victimisation of innocent children. A foundation called My Child Online has now produced a powerful video to highlight the problem of identity hacking. SIDN attaches great importance to on-line security and is therefore supporting the My Child Online initiative. By doing so, we aim to contribute to enhancing internet security for children.

Suggestions

If there is a topic that you think we should be covering in The.nlyst, please send your suggestions to: communicatie@sidn.nl.

SIDN wins Internet Innovation Award

In January, SIDN Labs received the ISOC Internet Innovation Award 2014 for the development of EPP key relay – a solution to the thorny problem of how to transfer DNSSEC-protected domain names from one DNS operator to another. In the solution developed by SIDN Labs, the registry (e.g. SIDN) plays a key role. The DNSSEC key material is relayed from the releasing DNS operator via the registry to the receiving operator, using the Extensible Provisioning Protocol (EPP), a standard for data exchange between registries and registrars. The methodology allows domain names to be transferred without any interruption to the DNSSEC protection. EPP key relay has been submitted to the IETF as internet draft and is very likely to become a new internet standard.

Colophon
The.nlyst is published by SIDN, the company behind .nl. The magazine provides information about internet-related themes and about (.nl) domain names in particular. The.nlyst is distributed free of charge to SIDN's registrars and other stakeholders.

Editorial address
SIDN
PO Box 5022
6812 AR ARNHEM, the Netherlands
communicatie@sidn.nl

Additional input
Rob van den Nieuwelaar, Alex Bik, Erik Logtenberg, Daniël Federer, Erwin Heringa, Marc Groeneweg, Bert ten Brinke, Roelof Meijer, Sean Schuurman van Rouwendal, Marnie van Duijnhoven and Martin Sluijter

Design & production
ARA, Rotterdam – www.ara.nl

Translations
G & J Barker Translations – www.gandjbarker.co.uk

Print run
Approximately 2,500

Subscriptions
The.nlyst is distributed free of charge to associates of SIDN. If you wish to be added or removed from the distribution list, please contact communicatie@sidn.nl.

ISSN: 2212-2842