Anti-Abuse SIDN

FIAT! 2016

5 februari 2016

Maarten Wullink & Moritz Müller, SIDN



SIDN

- SIDN = registry van .nl
- Diensten
 - Voor internetters: gebruiken van .nl domeinnamen (resolving)
 - Voor registrars: domeinnaamregistratie, met DNSSEC-support
 - Voor registries: back-end registry services (.amsterdam en .aw)
 - Voor abuse/CERT community: data en early warning services (in ontwikkeling)
- Besteding resultaat
 - SIDN Fonds: gebruik en maatschappelijke impact van de internetinfra
 - SIDN Labs: R&D voor meer veiligheid, stabiliteit en schaalbaarheid van internetinfra zelf (.nl, DNS en als geheel)
 - Registars en andere stakeholders: hulp bij technologie-adoptie (bijv. DNSSEC, AbuseHUB, Campus Challenge)
 - In the end impact op de internetgebruiker (individu of organisatie)





SIDN Labs

- Doel: ontwikkelen en evalueren van
 - Nieuwe mechanismes en systemen die de security en stabiliteit van .nl, het DNS en de internet infra vergroten
 - Nieuwe diensten voor SIDN
 - Beide zo veel mogelijk samen met de Nederlandse R&D community
- Beoogde impact:
 - Verhoogde waarde van het internet (afgeleid: versterkte reputatie van SIDN als onafhankelijk expertisecentrum)
 - Verder geïnnoveerde dienstverlening SIDN
 - Versterkte positie van onderzoek uit Nederland met toegevoegde waarde voor .nl en het internet
- Labnetwerk voor prototyping/evaluatie



Anti-Abuse





Preventie



Phishing





<complex-block></complex-block>	ANRO Extension that is being and a fact that is a	Geachte cliënt, Enge tijd geleden is het ons opgevallen dat er wat nalatigheid van uw rekening is bij Kotab. T fore is er open spoor van gebruik geweet van uw betaarkekning. Voor deze reden zijn wij at verplicht op eleoning van werkening is van de opst een verzicht van het process. Aanog gebruik willen maken van uw rekening? Manog servicedesk
<complex-block></complex-block>	ARO Update Image: I	toe is er geen spoor van gebruik geweest van uw bealarksening. Voor deze reden zijn wij al verplicht uw rekening is Annadiering uan uw rekening? Wit ua anog van beer van uw rekening? Wit ua anog van bieven bealarksening is were van uw bealkpes is semmeer van uw bealkpes is in ter van uw bealkpes is
<form></form>		Alanoi gebruik willen maken van werkening? Mit anog kan bijven bij Kog2 Oak na uiteraard. Door <u>her</u> te klikken gaat u direct door gebruik maken van werkoog beering. Met viendelike oroot. Manger Servicedesk Manger Service
<form><form></form></form>		nummer ven uw bankpes in rer van uw bankpes in rer van uw bankpes in rer van uw bankpes in
<form></form>	Advanter Voormaante Advanter Noted hummer* Extended* Obtoornotstum* Kok op Gx ander # Putzada* Obtoornotstum* Kok op Gx ander # Putzada* Obtoornotstum* Numer # Putzada* Putzada* Obtoornotstum* Putzada* Putzada* Putzada* Putzada* Putzada* Obtoornotstum* Putzada* Putzad	summer van uw bankpas in Personality (1) Personality (1
<form></form>	Atternaser* Addefinaser* Add	nummer van uw bankpas in rer van uw bankpas in
<form>Indication of the set of the</form>	Teleforstrummer* Rabobank Emailsder* Ameri* Ameri* Nutteda* Obsortelitum* Obsortelitum* Okcep DK ander # Radoo Internetinationen de lades Internetinationen de lades Stotate aleen bij het vorzenden. Zin u was dwijkunder Beil Internetinationen de lades Stotate aleen bij het vorzenden. Wagen over/ Internetinationen de lades Stotate aleen bij het vorzenden. Houdjoed Privey Exteiner Carri Name informatio Maker informatio Oddo Kotat tariet/. Name informatio Name informatio Image Statement Image Statement Image Statement Image Statement </td <td>summer van uw bankpas in Parintentin (2017) Parintentin (2017)</td>	summer van uw bankpas in Parintentin (2017) Parintentin (2017)
<form><form><form></form></form></form>	Arres" Puttada" Odosototitum" Odosototitum Odos	Aanvragen Heeft u geen toegeng tot Robo Internetbenkieren? Het Robo Steamstenkieren? Het Robo Steamstenkieren kunt u stigd vis Internet uw rekeningen inzien en transacties uitvoeren. Jer van uw bankgas in
<form><form><form><form></form></form></form></form>	Odbortdotsin* Kik sp GK ardenir Gebruik bij het inkgopen do Rabo Enternetiaerikaren de Joeds von uw Random Rasder, Gabruik de Strotta alleen bij het vorzendom. Zieder von uw Random Rasder, Gabruik de Strotta alleen bij het vorzendom. Zieder von uw Random Rekeningsummer: Unter the Hobeski > Heer informatie 1. Vul het rekening Rekeningsummer: 2. Vul het posisummer: 3. Vul je geboerted 3. Vul je geboerted 3. Vul je geboerted foort datum:	Nummer van uw bankpas in Statement of Statement wieren. In ummer van uw bankpas in Statement wieren stateme
<form></form>	I -toest van ur Random warder, Gabrik de S-toets inter informatie Vorgen over/ valgheld Proof (a belofest) staligheld Proof (a belofest) > Hear informatie Image: Staling and the sta	nommer van uw bankpas in Reinsteinen Reinsteinen reinst
<form><form><form></form></form></form>	Vrogen over Vrogen over Vroge	rekaningen inzian en tronoaties uitvieren. > Informatie over Rabo
<form><form></form></form>	Raljdad Pracy Diddimer Ceri Malifdad Pracy Diddimer Ceri Maer informatia Nul je geboorted Home'Bark	ver van uw bankpas in Diformatie over Rebo
<form><form></form></form>	Mage informatie Maser informatie Maser informatie Second address Maser informatie Second address Parsummer: U Second address Tecond address Tecond address Tecond address	L'US RELATION
<form></form>	Home'Bant	> Dakijk de demo
<form></form>		Help
Sector All representation of the sector representation of the r	ul uru namen ir	> Waarom kan ik niet
Mission where due due due due due due due due due du	elden in Home'Bank	vitiggen 7 vitiggen 7 vitig & de vitiggen 7 vitig & de vitiggen 7 vitig & de vitiggen 7 vitiggen 7 vitigg
<form>Name and a body to maxe maxe define the source source high define the source source high by by we verticate and a source high by the vertication of device define the source source high define the source source high by the vertication of device define the source source high define the source here here here here here here here h</form>	Algelopen weekend werd de laalste versie van Home Bank gelanceerd, met onder andere deze nieuwe loginpagina. Tildens het doorvoeren van deze wijzieinene ondervonden sommine cijerten moeilijkheden met het inionene Wij zijn	melding (647)?
<form>Here the probleme text throughe op Home Bank Offline C G dam name do generalizadatant on beiligk de procession. Nei D Genef win NG D D Genef win NG D D Genef win NG D D Genef win NG D D Genef win NG D D Bewaar ming opponed Genef win NG D Bewaar ming opponed Genef win NG D C and Reader on druce to Control Winter assessed I Passocid verseter? Genef win NG D Genef spatias, de opfers in die op het schem van uw NG C and Reader er schether. Nortic gegevensie Genef win nu wind-Sankkaart on van wind C and Reader er schether. Nortic gegevensie Genef wind wind W-Gankkaart on van wind NG C and Reader er schether. Adres Do ne er undig is tableper H Schetter Nortic gegevensie Genef wind wind W-Gankkaart on van wind NG C and Reader er schether. Adres Head T Sank W Home State, the schether van uw NG C and Reader er schether. Adres Head T Sank W Home State, the schether van uw NG C and Reader er schether. Adres Head T Sank W Home State, the schether van uw NG C and Reader er schether. Adres Head T Sank W Home State, the schether wan uw NG C and Reader er schether. Adres Head T Sank W Home State, the schether wan uw NG C and Reader er schether.</form>	hievan op de hoogte en namen ondertussen de endige maatregeler om onze tilehet he ondersteuene hij het gebruik war Home Bank. Kals unge vragen hetel of prochemen onderninkt. Bij het gebruik van het neuwe sokernen, kunt u steak rekense op onze huip. We verontschuldigen ons voor het tijdelijke ongemak. Wit u zien hete de nieuwe logingagins werkt, bestjor onze geme.	iat
rg ge vens NO D Gef uv Klob In Card D Card D Gef uv Card D In Bewaar mijn gegevens Passwoord D Bewaar mijn gegevens Not D Steek uw Not-banksaat in de NO Card Reader en duk op: DOTTTT Vor de pincode in van uw Not-banksaat in duk op: Optimer gasits online veligheid Vor de pincode in van uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw Not-banksaat in de NO Card Reader en duk op: Optimer gasits online veligheid Steek uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw Not-banksaat in de NO Card Reader verschijnen. Steek uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw Not-banksaat en duk op: Optimer gasits online veligheid Steek uw wonktings online veligheid Steek uw won	Hebt u problemen met inloggen op Home'Bank Offline? Ga dan naar de <u>downloadpagina</u> en bekijk de procedure.	Annularen Help
 Including of the function of the func	gegevens Bei de Home/Bank Helpdesk op	
Call of international of inte	INSID Geef uw INSID in +32 2 464 60 01 Confut Confut	
Bewaar ming gegevens Bewaar ming gegevens Peswood Intificatie Iterux passwoord Pas	Carolin Ceer ow Carolin Kaart verforen of gestolen? Bel Card	
Paswoorl I Paswoord I	Bewaar mijn gegevens Meer over online velligheid	
Interw paswoord Paswoord veroeter? Intificatie I. Steek uw ING-bankkaart in de INO Card Reader en druk op: Dibbrury 2. Voer de pincode in van uw ING-bankkaart in de invo op: OK 3. Voer, zonder spaties, de cifers in de op het scherm van uw ING Card Reader verschijnen. Adree Contendation Cap Cape Cape Cape Cape Cape Cape Cape C	Paswoord	
Intificatie I. Steek uw ING-bankkaart in de ING Card Reader en druk op: BIDTNTIF 2. Ver de pincode in van uw ING-bankkaart en druk op: OK 3. Ver zonder spalles, de cijfers in die op het scherm van uw ING Card Reader verschijnen. 4 eenvoudige stappen! Geboortedatum Dag - W - Maand - W - Jaar - W	Word cliënt bij ING Nieuw paswoord Paswoord vergeten?	
 Steek uw ING-bankkaartin de ING Card Reader en druk op: RUDNTIV Ver de pincode in van uw ING-bankkaart en druk op: OK Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw ING Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw Vind Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw Vind Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm van uw Vind Card Reader verschijnen. Ver zonder spalles, de olfers in die op het scherm verschijnen. Ver zonder spalles, de olfers in die op het scherm verschijnen. Ver zonder spalles, de olfers in die op het scherm verschijnen. Ver zonder spalles, de olfers in die op het scherm verschijnen. Ver zonder spalles, de olfers in die op het scherm verschijnen. Ver zonder spalles, de olfers in die op het scherm verschijnen. Ver zonder spalles,	Den een grats onine zichtrekening, ontvang uw	
2. Ver de pincode in van uw NIX-bankkaat en druk op: OK 3. Ver, zonder spaties, de cijfers in die op het scherm van uw NIX Card Reader verschijnen. rscontlijke gegevens ant • voorletters Adres Telefoonsummer Geboortedatum • Dag - V - Maand - V - Jaar - V	1. Steek uw ING-bankkaart in de ING Card Reader en druk op: DIDENTIFY beheer uw verrichtingen	
rsconlijke gegevens am + voorletters Adres Geboortedatum - Dag - I - Maard - I - Jaar - I	2. Voer de pincode in van uw ING-bankkaart en druk op: OK 4 eenvoudige stappen! 3. Voer, zonder spalles, de cijfers in die op het scherm van uw ING Card Reader verschijnen.	
sconlijke gegevens am + voorieters Adres Geberoonaummer Geberoonaummer Geberoonautum - Dag - V - Maand - V - Jaar - V		
Adres Celefoonsummer Geboortedatum - Dag - I - Maand - I - Jaar - I Geboortedatum - Dag - I - Maand - I - Jaar - I Solution S	rsoonlijke gegevens	
Geboortedatum - Dag - 🔍 - Maand - 🔍 - Jaar - 🔍		
Geboortedatum - Dag - I - Maand - I - Jaar - Jaar - I - Jaar - Jaar - I - Jaar	vnia2	(Streeting
	ueuourieuaium - Jag - 💌 - Maand - 💌 - Jaar - 💌	

Domeinnaambewakingsservice (DBS)

- Real-time monitoring
- Alle .nl-domeinnamen (binnenkort ook andere TLD's)
- Classificatie websites (Phishing, malware etc.)



Domeinnaambewakingsservice (DBS)



Tijd tot automatische logout 59:39 Actueel										
Domeinna	am 🔽 o	Wijzigingsdatum 📳 ^	ڻ د	Status 🕎 o	Classificatie 🕎	Actie 🔻	Doorzetten naar 😨	Verplaats naar	Opmerkin	Rabobank
tjeb.nl	0 ×	25-11-2015 10:11:15	٢	Inactive	💷 Normale site			***		
1jeb.nl	0 ··· ×	25-11-2015 10:02:38	Ö	Inactive	E Ongebruikt					
nuu.nl	0 ··· ×	25-11-2015 10:01:46	٢	Inactive	😽 Redirect naar originele domeinnaam			42		
aardappelsa	p.nl 🕕? 🗙	23-11-2015 11:23:18	٢	Inactive	Terwijderd					
midn.nl	0 ×	19-11-2015 07:53:36	Ö	Inactive	A Phishing site			-		
aidnini	e x	19-11-2015 07:51:18	٢	Inactive	Geparkeerde site			****	J	
zidn.nl	0 ··· ×	19-11-2015 07:51:11	٥	Inactive	🛅 'Te koop' site			***		Rijksoverheid
sidm.nl	0 ··· ×	19-11-2015 07:45:54	٢	Inactive	P Geparkeerde site					N. COLL
p440.nl	0 ··· ×	17-11-2015 18:47:39	٢	Inactive	🛅 Ongebruikt			40		
<u>n440.nl</u>	0 ··· ×	17-11-2015 18:40:28	٥	Inactive	A Reageert niet					Bank Name
m440.nl	0 ··· ×	17-11-2015 18:40:23	٥	Inactive	💊 Redirect naar originele domeinnaam			***		
c440.nl	6 ··· ×	17-11-2015 15:02:06	ð	Inactive	Cnoebruikt			*		1234 5678 9876 5432



.nl control

Zelf 100% controle over uw domeinnaam. Er worden geen wijzigingen doorgevoerd zonder uw nadrukkelijke toestemming.

- wijzigen gegevens domeinnaam
- (houder, admin-c, tech-c, nameserver, DNSSEC-sleutelmateriaal)
- wijzigen gegevens contactpersoon
- domeinnaam verhuizen
- domeinnaam verwijderen
- wijzigen van de glue records van de in-zone nameserver

KEEP CALM AND **STAY IN** CONTROL



Security / Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22 Email 🖶 Print

OPINION: Attack shows the potential for serious spoofing attacks that could leave end users helpless. The only real solution is DNSSEC, which will take years to implement under the best of circumstances.



DNS cache poisoning attacks exploited in the wild

HOME « NEWS « TOP SECURITY STORIES « GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING...

GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING ATTACK

ave provided more details in their "30 Days of DNS HD Moore's statement on DNS cache poisoned AT&T ces are starting to see evidence of DNS cache poisoning appears to be an attempt to take advantage of the y :" client 143.

DNS poisoning slams web traffic from millions in China into the wrong hole

ISP blames unspecified attack for morning outage

By John Leyden, 21 Jan 2014

C >> = apetris ISI per 1987

Follow via: 🥎 🖂

GMT (04:24 BST)

s of DNS Attack Activity" ed AT&T DNS servers. Numerous ng attempts on their local "recent" DNS cache poisoning Inerable[®] if any of the results below are

DNSSEC

- Incentive voor het signeren van domein namen
- 44% van alle .nl domeinnamen heeft DNSSEC support





ValiBox

- Thuis validatie test
- GL-INET device
- Gebaseerd op OpenWRT
- Aangepaste Unbound resolver



valibox.

SIDN Labs ValiBox

Probleem met www.servfail.nl

Er is een fout opgetreden bij het opzoeken van de domeinnaam www.servfail.nl.

Dit kan komen doordat de DNSSEC-validatie niet is gelukt.

Als je denkt dat het om een configuratiefout van de beheerder gaat, kun je een Negative Trust Anchor zetten, waarna dit domein alsnog te bereiken is. De NTA zal blijven staan totdat de valibox opnieuw opgestart wordt.

Doe dit NIET als je het niet vertrouwt.

Zet een Negative Trust Anchor voor www.servfail.nl

Zet een Negative Trust Anchor voor servfail.nl

ValiBox Hoofdmenu

Hier kun je de instellingen van de ValiBox wijzigen, de wachtwoorden veranderen, de logs bekijken, de software updaten, en backups maken.



Ċ



DNSSEC validatie

- SIDN validerende resolver
 - Pilot bij een educatieve instelling
- stats.sidnlabs.nl

DNSSEC validerende resolvers

Afgelopen maand





Wetenschappelijk onderzoek

- REMEDI3S for TLDs (REMEDI3S-TLD)
 - Ontwikkelen van security metrics for top-level domains (TLDs)
 - Universiteit Delft, NCSC en SIDN
- The Open INTernet Evolution Library (OpenINTEL)
 - Platform waarmee de evolutie van het internet geanalyseerd wordt, door continue DNS metingen uit te voeren.
 - Universiteit Twente, SURFnet en SIDN
- Self-managing Anycast Networks for the DNS (SAND)
 - Bepalen optimale plaatsing van gevirtualiseerde DNS anycast nodes, voor een zelfsturende DNS anycast dienst
 - Universiteit Twente, NLnet Labs en SIDN



UNIVERSITY OF TWENTE.





Nationaal Cyber Security Centrum Ministerie van Veiligheid en Justitie





Detectie



Waar zoeken we naar?

- Domeinnamen die gebruikt worden voor:
 - Phishing
 - Webshops met namaakproducten
 - Distributie van malware
- Botnet clients





ENTRADA

ENhanced Top-level Domain Resilience through Advanced Data Analysis

- 'DNS big data' systeem
- **Doel**: ontwikkelen van toepassingen welke de veiligheid en stabiliteit van .nl, DNS en het Internet verhogen
- ENTRADA hoofd componenten
 - Applicaties en services
 - Platform en data bronnen
 - Privacy framework
 - Platform + privacy framework = ENTRADA





Security Intelligence for Top-level Domain Operators (SITO)

Herkenning van verdachte nieuwe domeinnamen





Botnet client detectie



Malafide activiteiten:

Spam-runs





Botnet client detectie – koppeling met AbuseHUB



Mitigatie



Actionable intelligence

- AbuseHub
 - Nederlandse ISPs tegen internet-abuse
 - Informatie van "Reliable notifiers"
- SIDN
 - Reliable notifier van NL infecties
 - 5-10 per dag





Abuse204.nl

- Verminderen van phishing en malware in de .nl zone
- Gebaseerd op Netcraft
- In samenwerking met registrars en hosting provider



DNS Anycast – Wat routers denken

- Hogere beschikbaarheid van DNS
 - Tegen DDOS
 - Tegen netwerk storing
- Wat denken de routers?





DNS Anycast – Hoe het werkelijk is





Het werkt!



AMS-IX storing Woensdag 13-05-2015



SAND – Onderzoek: Waar plaatsen wij onze servers?





Vragen?

Maarten Wullink Research Engineer maarten.wullink@sidn.nl

9 @wulliak

Moritz Müller Research Engineer moritz.muller@sidn.nl

www.sidnlabs.nl



