



.SE Registry - Abuse

- Abuseansvarig maj 2011, men jobbat med abuse sedan affärsmodellsbytet mars 2009

Bakgrund:

- 94-02 Datautbildning/Mjukvara/Hårdvara
- 02-09 Domäner/Hosting/E-handel
- 09- .SE

.se

Mitt fokus på .SE Registry



Registrantnivå:

- Snabbt stoppa, försvåra och vara besvärlig för "busar"
 - Få dem att välja andra TLDer för sin verksamhet

Registrarnivå:

- Granska, utreda "brott mot avtalet"
 - tillhandahålla underlag för andra att bedöma.

.se

..det sura äpplet



.se

Rollen i sig är ganska "fyrkantig"
(tak, väggar och golv)

- Det finns klara gränsdragningar för vad jag får och kan göra i rollen på .SE.
- Så mycket jag ser, **kan** och **vill** agera mot, behöver jag låta bli..

".. verka för en positiv utveckling av användandet av .se-domäner och användandet av (främst) den svenska delen av Internet i enlighet med .SE's urkund och .SE's vision."

Varför?

.se



..jag behöver bla ta hänsyn till

- .SE är en **privat** allmännyttig stiftelse
- Topppdomän**lagen** SFS 2006:24
- Registrar**avtalet**
- Registrerings**villkoren**
- Registrarers **olika modeller**

.se



Vad gör en Abuseansvarig på .SE?

.se

Rollen som ansvarig för abuse i .se-zonen



- Registrarärenden
- Registrantärenden
- *"Hybridärenden"*

Proaktivt:

- Sociala medier, forum mm
- Publika varningar mm
- Jobbar för bättre samarbeten
- Jobbar **FÖR** en nationell varningslista

.se



Registrarärenden

Utredningar / kartläggningar / kontroller av:

- misstänkt warehousing / bulvanverksamheter
- misstänkt manipulering av .SE:s system
- att avtal efterföljs (villkor mm).
- bevakar "varningsklockor"
(bolagsförändringar, företrädare, uppköp, F-skatt mm)
- avvikelser från registreringsmönster

.se

Registrantärenden



- Manuellt granskar registrantdata - ögnar igenom registreringsflöden. Backar till Registrar -> sen registrant.
- Hanterar slutkunders "svårare" klagomål och anmälningar mot registrarer.
- Utredningar kring domäner som registrarer "supit bort", åsamkat registrant skada.

.se

Hybridärenden



- Internetkataloger/bluffakturor
 - Bluffshoppar / Phishing
 - SERP-hijacking (SQL-injections)
 - Allehanda annan abuse
-
- Samarbetar med för incidenten, en lämplig organisation.

Samarbeten



- Andra domänregister
- Registrarer
- Svensk Handel mfl.
- CERT SE (fd. SITIC)
- Polis – alla nivåer
- Skatteverket / Ekobrottsmyndigheten
- Konsument Europa (Konsumentverket)
- APWG, Anti-Phishing Working Group

.se



Domän - övrigt

- Subregistrarer – vilken registrar tillhör de?
- Sv. skojare med utländsk målgrupp.
- Utl. skojare med .se-innehavare som målgrupp.

.se



Domänskojare i Sverige

Då och nu

Lugnet före stormen?

.se

iis.se 2009-01-20



Exempel på oseriös metod via e-post

Säljaren hävdar att de har en "annan kund" som är intresserad av domännamnet men att de är skyldiga att först erbjuda dig domännamnet eftersom du har samma domännamn under .se.

VARNINGSLISTA JUST NU

De företagsnamn som för närvarande är kända för oss, och som använder sig av oseriösa metoder är:

- Domänregistreringar Europa
- Webadministratörn
- System Solutions
- IT-Verket
- Svenska IT Registret AB
- Colvento IT

.se



..visade inte hela bilden

- iis.se:s lista var dels lite inaktuell och det fanns även ca 10 andra aktiva verksamheter som utnyttjade att de inte fanns med på listan:
- ..titta: – *vi finns inte med, så vi är seriösa..*

.se

Under 2½ års tid



- Löpande uppdateringar av listan
 - Snabbt informerat registrarer om tillhörighet.
 - **Mycket arbete utanför** rollen som .SE-anställd.
 - Publika varningar – (allmänheten)
 - Samarbeten..
-
- Lagt till rekommendationer från .SE och Registrars.se för registrarer att inte samarbeta med verksamheter som listas.

.se

Vi är för närvarande medvetna om följande verksamheter

Det är .SE:s rekommendation att .SE:s ackrediterade registrarer, även dennes återförsäljare, inte samarbetar med företag som namnges nedan på denna sida, med hänvisning till .SE:s registraravtal punkt 2.6, https://www.iis.se/docs/registraravtal_sv2.pdf.

Denna rekommendation görs även av registrarsföreningen för .SE-ackrediterade registrarer; registrars.se, med hänvisning till föreningens etiska regler.

http://www.registrars.se/wp-content/uploads/2007/05/etikregler_registrars.pdf

De företagsnamn som för närvarande är kända för oss, och som använder sig av oseriösa metoder är:

Nordisk Domänhantering / NDH Sweden AB / Nordic Domain Hosting / "Domainshop"

Texten på verksamhetens hemsida är i sin helhet kopierad från en av .SE:s registrarer. Telefonförsäljning mot innehavare av .se-domäner (Sverige) och .no-domäner (Norge) enligt den "vanliga" hotbilden, "vi har en kund som har beställt ert domännamn under andra toppdomäner, men vi ger er förtur..". Sedan april 2011 så betyder NDH numera "Nordic Domain Hosting", istället för som tidigare "Nordisk Domänhantering" och de senaste anmälningarna vittnar om att de blivit fakturerade för domännamn som de redan är innehavare av och även för domäner som alltså är oregistrerade. Sedan oktober 2011 presenterar de sig även som "Domainshop" i telefonsamtalen och att de "tar hand om alla domäner i Norden". De erbjuder en engångssumma för ett "varumärkesskydd" som påstås innebära att ingen kan registrera ett domännamn (som kundens) under någon toppdomän, pga av deras "varumärkesskydd" - **Detta är ren och skär bluff!**



iis.se nov 2011

.se



Förväntad utveckling av domänbusar

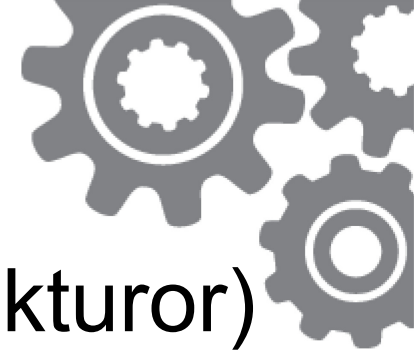
- Nya gTLDer kommer att skapa nya busar som utgår från .se-innehavare..
- Redan nu kommer anmälningar om försäljare för toppdomäner som ännu inte finns.

.se



Istället för domänskojare..

.se



Störst problem idag

Internetkatalogskojare (telefon/bluffakturor)

–Yrkeskriminella har hittat Internet

- Använder Internet (bla .se-domäner) som begräferiförstärkare.
- Kallringer och lurar näringsidkare att ingå avtal
- **Polisen förstår inte, utreder inte..lagstöd?**
- Skatteverket/EBM agerar – men för långsamt.

.se

Ökända Hittaföretagen får domäner stängda

Skojaföretaget bakom Hittaföretagen och Inspelningscentralen har fått sina svenska webbadresser stängda av stiftelsen som ansvarar för den svenska toppdomänen .se. Men verksamheten fortsätter under hittaforetagen.com och allaforetagen.com.

Sedan förra veckan går den aggressiva telefonskojaren Hittaföretagens adress www.hittaforetagen.se inte längre att nå. Domänen inspelningscentralen.se dit offren hänvisas för "bevis" på ingånget avtal ligger också nere, liksom kopian allaforetagen.se.

Gemensamt för adresserna är att de registrerats av den avregistrerade ideella föreningen Svarta Pärlor, med boxadress i Malmö. Vem som ligger bakom den går inte att få fram, vilket fått .SE Registry, som är ansvarig för de svenska domännamnen, att reagera. Peter Forsman, abuseansvarig, svarar Driva Eget:

- Jag kan bekräfta att .SE Registry den 18/8 deaktiverade ett 60-tal domännamn, för att registrant som trots upprepade begäran ej uppdaterat registrantdata med valida uppgifter. Domänerna kommer fortsatt att vara deaktiverade fram till att vidimerade uppgifter inkommit till .SE.

Företaget bakom Hittaföretagen, Företagslansering Sverige AB, har raskt bytt till domäner som slutar på .com, som Hittaforetagen.com. Den första fakturan med den nya adressen kom i veckan, rapporterar Svensk Företagsförening.

Fler artiklar om fakturaskojarna

→ Se upp för fyra nya fakturaskojare

→ Kreditföretagen till attack mot fakturaskojarna

→ Se upp för dessa tre nya fakturaskojare

→ Värsta fakturaskojaren till varningslistan

→ Fakturaskojare fick tre års fängelse

→ Riksdelen stämmer skojare

→ Nu åter skojarna dit

→ Så lurar bluffföretagen Driva Egets besökare

→ Konflikt bland fakturaskojare slutade med mord

→ "Det blir automatisk förlängning för 23 000 när du inte sagt till"

→ Riv eller bestrid för att slå mot skurkarna

→ Fakturaskojare anklagar Driva Eget för "fult trick"

→ Nytt bluffföretag försöker lura din

bakom den går inte att få fram, vilket fått .SE Registry, som är ansvarig för de svenska domännamnen, att reagera. Peter Forsman, abuseansvarig, svarar Driva Eget:

- Jag kan bekräfta att .SE Registry den 18/8 deaktiverade ett 60-tal domännamn, för att registrant som trots upprepade begäran ej uppdaterat registrantdata med valida uppgifter. Domänerna kommer fortsatt att vara deaktiverade fram till att vidimerade uppgifter inkommit till .SE.

.se



Framtid av abuse i Sverige

- Nya varianter av Telefonskojare / bluffakturor
- Bluffbutiker, värderingssiter – falsk/stulen registrantdata
- Nya gTLDer = mycket nya "busar", manipulation
- TM-intrång, scraping, FB/Googleannonser (svårare att avgöra seriösa aktörer)
- Spam via SMS/MMS med koppling till web allt vanligare.

.SE Registrys "röst" i Sociala medier



- Twitterkontot @seregistry (främst för registrarer)
- Närvaro på Webmaster Network, wn.se
- Närvaro på Twitter, Facebook, LinkedIn, Google+ mm
- Bloggar på iis.se/blogg (och internetsweden.se)
- Föreläser om "buset" och "nätgräv"

.se



Peter Forsman

- peter.forsman@iis.se
- 08-452 35 66
- 070-713 42 00
- twitter.com/internetsweden
- facebook.com/internetsweden

.se