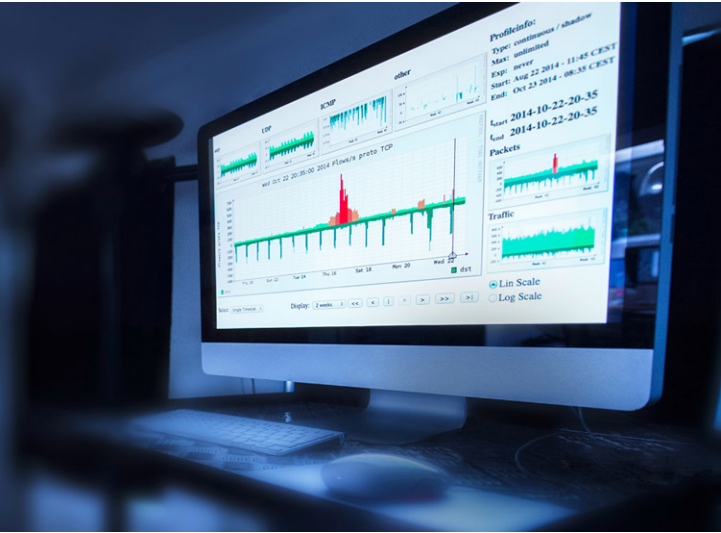


Breaking security controls using domain hijacking



SWITCH

Daniel Stirnimann
daniel.stirnimann@switch.ch

Zürich, 23. September 2017

Enterprise vs. small shops domains



abb.com
swissre.com
siemens.com
clariant.com
microsoft.com
hsbc.com
ft.com
lufthansa.com
swiss.com
...



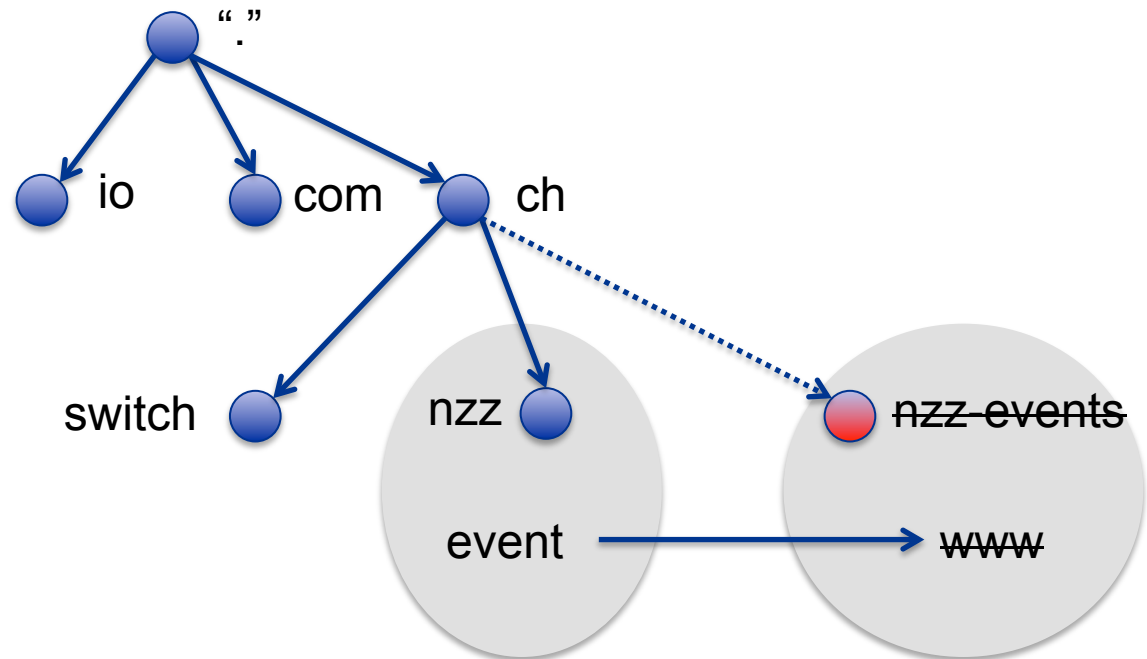
<https://event.nzz.ch/>

How does it work?

Root

TLD

(User) Domain



```
dig event.nzz.ch
```

```
;; status: NXDOMAIN
```

```
event.nzz.ch.      CNAME      www.nzz-events.ch.
```

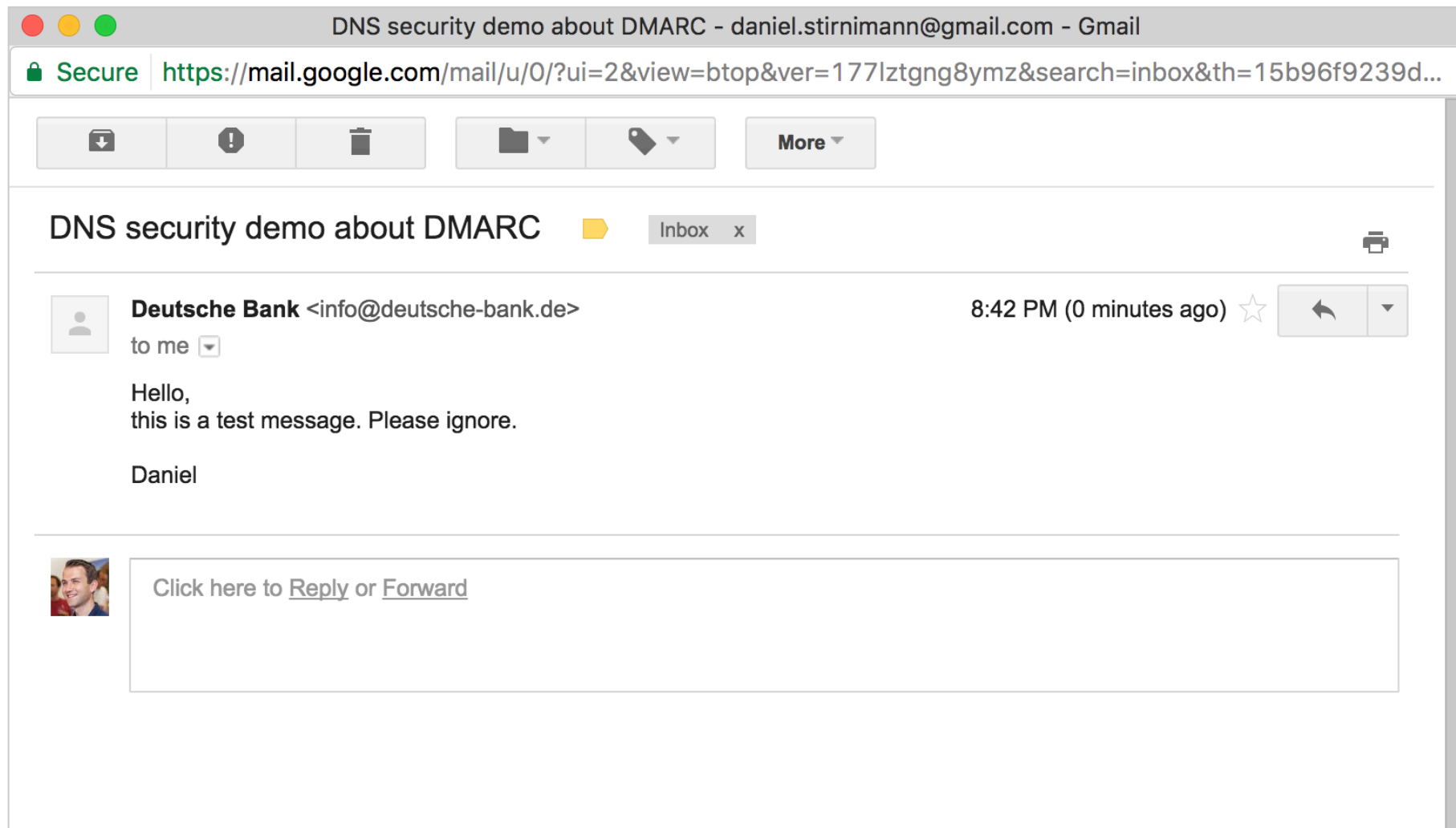
Abandoned subdomain!

- Trick/mislead user - social engineering
- Circumvent anti-mail spoofing protection such as DMARC

Sabotage:

- Use HTTP Public Key Pinning (HPKP) to render the subdomain unusable

Circumventing DMARC



The screenshot shows a Gmail interface in a browser window. The title bar reads "DNS security demo about DMARC - daniel.stirnimann@gmail.com - Gmail". The address bar shows a secure connection to "https://mail.google.com/mail/u/0/?ui=2&view=bttop&ver=177lztgng8ymz&search=inbox&th=15b96f9239d...". Below the address bar are navigation icons for download, warning, trash, folders, tags, and a "More" dropdown. The email header shows the subject "DNS security demo about DMARC" with a yellow envelope icon, the folder "Inbox", and a close button. The sender is "Deutsche Bank <info@deutsche-bank.de>" with a profile picture icon, and the recipient is "to me" with a dropdown arrow. The time is "8:42 PM (0 minutes ago)" with a star icon and a reply dropdown. The email body contains the text: "Hello, this is a test message. Please ignore. Daniel". At the bottom, there is a reply box with a profile picture icon and the text "Click here to [Reply](#) or [Forward](#)".

Circumventing DMARC

Original Message

Message ID	<20170422204241.006499@dnsresolver.novalocal>
Created at:	Sat, Apr
From:	Deutsch
To:	daniel.s
Subject:	DNS security d... DMARC
SPF:	PASS with IP 86.119.38.239 Learn more
DMARC:	PASS Learn more

```
dig bildung.deutsche-bank.de TXT +short  
"v=spf1 ip4:86.119.38.239/32 -all"
```

```
dig _dmarc.deutsche-bank.de TXT +short  
"v=DMARC1\  
p=reject\  
rua=mailto:deutsche-bank@rua.agari.com\  
ruf=mailto:dmarc.reports@db.com\  
ri=3600  
"
```

If you have a security control
which relies on DNS, then it's only
as secure as your DNS!



Hostnames in Amazon AWS

myname-25189607.eu-west-1.elb.amazonaws.com



CNAME target is NXDOMAIN:

- test.swisstopo.admin.ch CNAME
ses-test-elasticlo-13sc845pxkywd-1713101147.eu-west-1.elb.amazonaws.com
- www1011.stage.e.abb.com CNAME
xc-elb-library-stage-1510629574.eu-west-1.elb.amazonaws.com

Hostnames in Microsoft Azure

myname.cloudapp.net.

myname.azurewebsites.net.

myname.azure-api.net.



CNAME target is NXDOMAIN:

- workspaces.microsoft.com CNAME workspaces.azurewebsites.net.
- yourperfectday.hsbc.com CNAME shoot228.cloudapp.net.

Careful with Hostnames!

QTYPE with possible out-of-bailiwick hostnames

- CNAME
- NS
- MX
- DNAME
- SRV
- TXT (SPF, DMARC)

Domain Take Over

The Hacker Blog

Home sonar.js xssless wmap FlashHTTPRequest Cloudflare Subdomain Enumerator

The .io Error – Taking Control of All .io Domains With a Targeted Registration

📅 July 10, 2017

In a [previous post](#) we talked about taking over the *.na*, *.co.ao*, and *.it.ao* domain extensions with varying levels of DNS trickery. In that writeup we examined the threat model of compromising a top level domain (TLD) and what some avenues would look like for an attacker to accomplish this goal. One of the fairly simple

The Author



Source: <https://thehackerblog.com/the-io-error-taking-control-of-all-io-domains-with-a-targeted-registration/>



io. failure – what happened?

```
dig @a.root-servers.net io. NS
;; AUTHORITY SECTION:
io.          172800 IN  NS  a0.nic.io.
io.          172800 IN  NS  b0.nic.io.
io.          172800 IN  NS  c0.nic.io.
io.          172800 IN  NS  ns-a1.io.
io.          172800 IN  NS  ns-a2.io.
io.          172800 IN  NS  ns-a3.io.
io.          172800 IN  NS  ns-a4.io.
```

```
dig @a0.nic.io. io. NS
;; ANSWER SECTION:
io.          86400  IN  NS  b0.nic.io.
io.          86400  IN  NS  c0.nic.io.
io.          86400  IN  NS  a0.nic.io.
```



(In)active domain registration

whois blogwerk.com | avantcredit.ch | ...

Name Server: NS0.DNSMADEEASY.COM

Name Server: NS1.DNSMADEEASY.COM

Na

Na

Na

Na

FUSED

Don't point your inactive domain to a DNS hoster/registrar!

**Don't leave "open"
name servers for
unused domains**

Mail take over

```
dig mac.ch MX +short
```

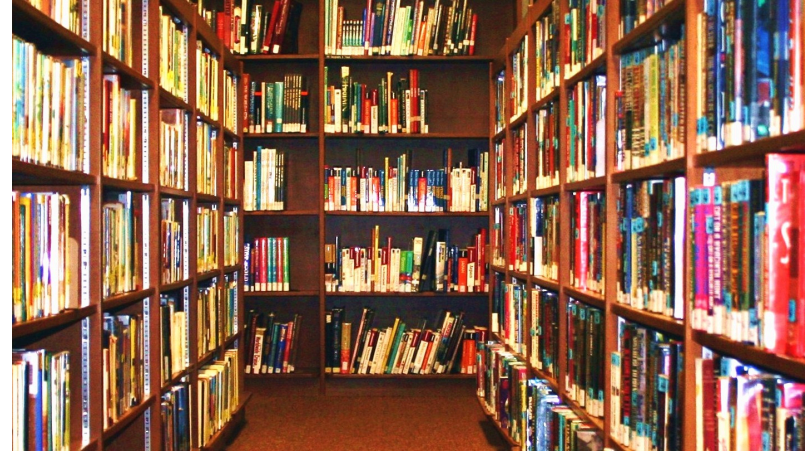
```
10 thisdomainisnotvalidformx.info.
```

```
whois thisdomainisnotvalidformx.info.
```

```
NOT FOUND
```

**Don't use domain names
you don't own!**

Data sources for hostnames



- Internet wide scanning data <https://censys.io/>
- Certificate Transparency <https://crt.sh/>
- ~~Passive DNS~~ <https://www.dnsdb.info>
- (Free) access PassivTotal, VirusTotal

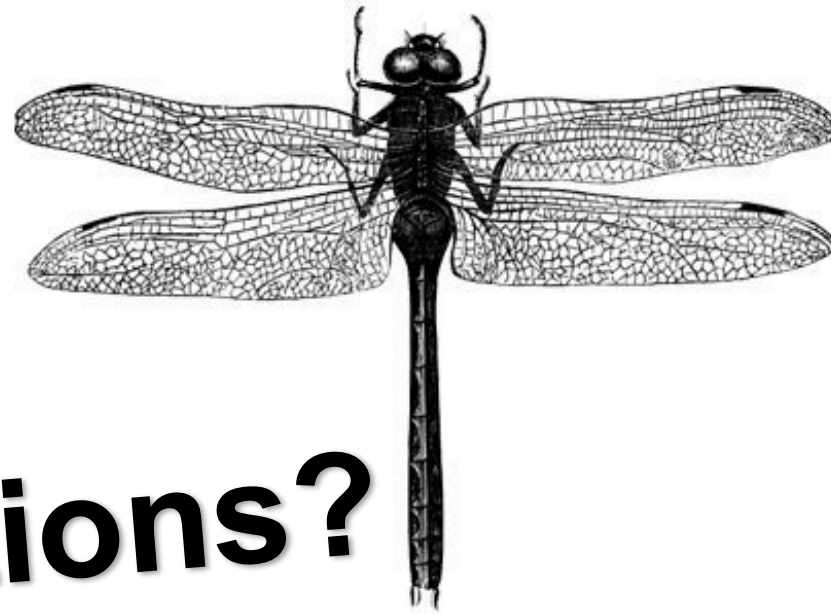
Recommendations

- Never use domain names you don't own or which don't exist in the DNS tree (e.g. .local, .corp)
- Regularly check your zone for hostnames which don't resolve (NXDOMAIN)
- DNSSEC sign your zone and use DANE

Out-of-bailiwick hostname checker

<https://github.com/stirnim/hostname-check>





Questions?

Everything is a
Fucking DNS Problem

The Definitive Guide