



DNS Spoofing

Have fun with
domain name

George Chou

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center



What is DNS spoofing?

- DNS spoofing is simply tricking the DNS system into believing your domain name is something other than it really is.

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center



Why do we care about it?(1)

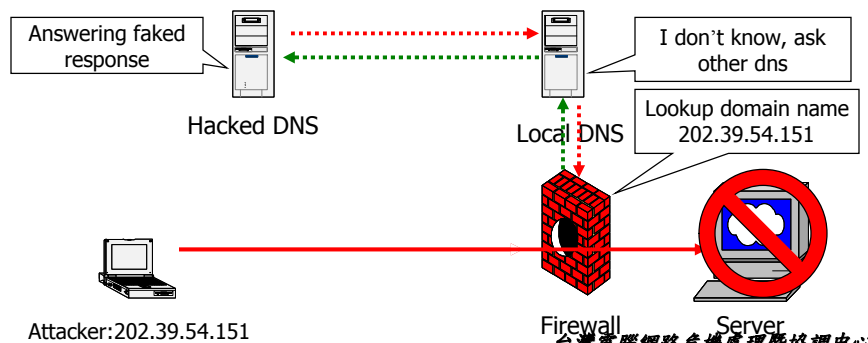
- Bypass your domain name based ACLs, including firewalls.
- Redirect your email, or send a faked email using your domain name.
- Redirect your website to an other, or simply denied.
- Redirect your browser, possible attack and gain access.

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center



Why do we care about it?(2)

- Bypass your domain name based ACLs?

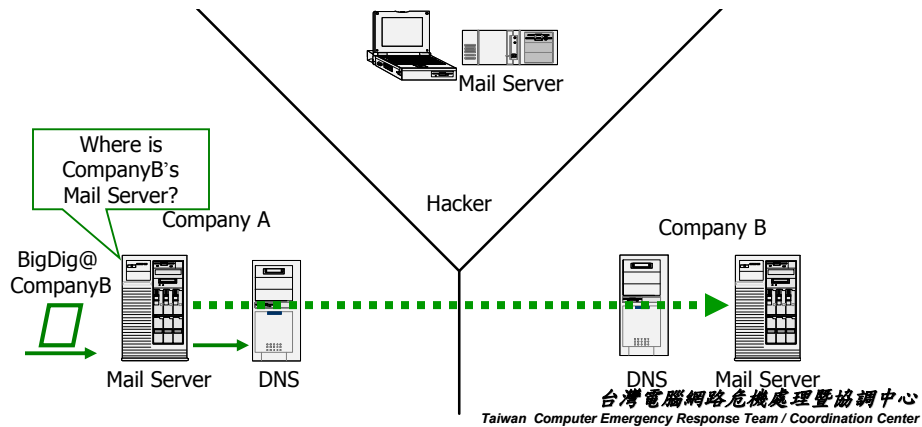


台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center



Why do we care about it?(3)

■ Redirect email?



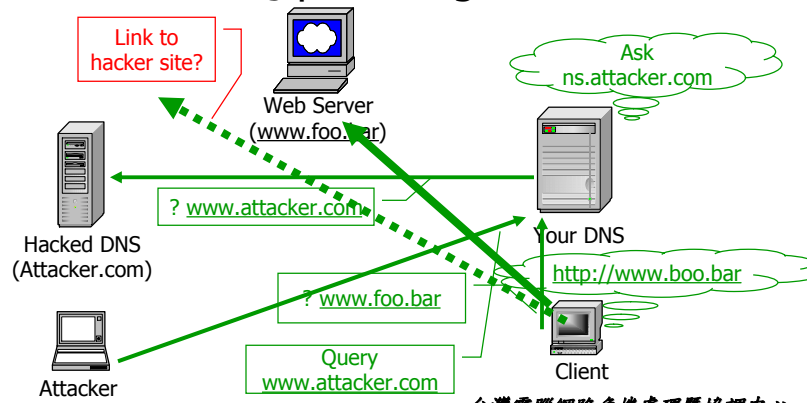
How is DNS spoofing done?

- DNS caching poisoning (additional data)
- DNS caching poisoning (related data)
- DNS ID Prediction
- DNS ID Prediction - Flooding
- Pass through BIND

TW CERT Coordination Center DNS caching poisoning(1)



■ DNS caching poisoning



台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center

TW CERT Coordination Center DNS caching poisoning(2)



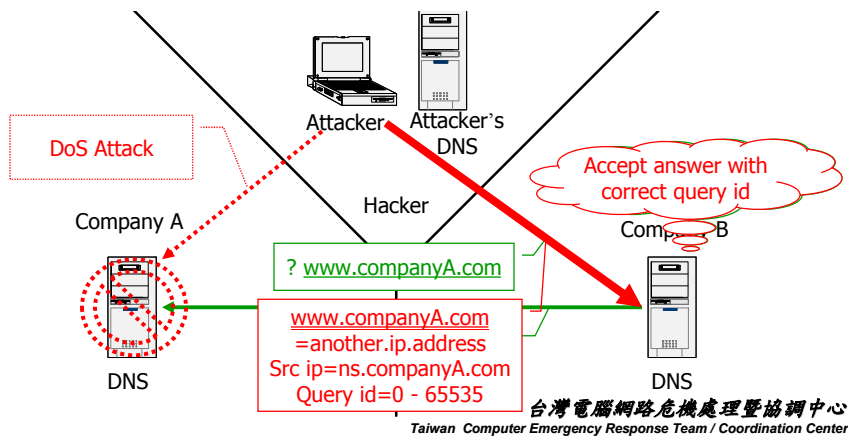
- By additional data
 - A record
- By related data
 - NS record
 - CNAME record
 - MX record

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center

TW CERT DNS ID Flooding

CERT
Coordination Center

■ DNS ID Flooding



TW CERT DNS ID Prediction & Flooding

CERT
Coordination Center

- Use latest version of bind
- Bind already patch with randomizes query id
- (Query ID is ONLY 16-bit)
- Enable DNSSEC (bind 9)?
- Use NIDS to detect abnormal DNS queries

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center

TW CERT Coordination Center Pass through the BIND(1)



- Direct CRACK the target DNS Server
- Modify the record you want to response
- Bad information will not be cached by server, but still passes to client

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center

TW CERT Coordination Center Pass through the BIND(2)



- Use latest version of bind
- Config your bind carefully
- Secure you name server (chroot...etc)

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center



No discourse with AD?

```
aegis [etc/named]# host -l dellirinaetech.com.tw
dellirinaetech.com.tw. A      61.218.23.2
dellirinaetech.com.tw. A      61.218.23.1
dellirinaetech.com.tw. NS     tiger.dellirinaetech.com.tw.
dellirinaetech.com.tw. NS     dragon.dellirinaetech.com.tw.
gc._msdcs.dellirinaetech.com.tw. A      61.218.23.1
!!! gc._msdcs.dellirinaetech.com.tw A record has illegal name
gc._msdcs.dellirinaetech.com.tw. A      61.218.23.3
!!! gc._msdcs.dellirinaetech.com.tw A record has illegal name
gc._msdcs.dellirinaetech.com.tw. A      61.218.23.2
!!! gc._msdcs.dellirinaetech.com.tw A record has illegal name
Ben.dellirinaetech.com.tw. A      10.1.4.205
chichung.dellirinaetech.com.tw. A      10.1.4.64
dailup.dellirinaetech.com.tw. A      230.31.226.19
dragon.dellirinaetech.com.tw. A      61.218.23.1
eryung.dellirinaetech.com.tw. A      61.218.23.69
Jinay.dellirinaetech.com.tw. A      10.1.4.104
michaelna.dellirinaetech.com.tw. A      163.31.25.25
SEBASTIAN-570E.dellirinaetech.com.tw. A      61.218.23.67
SMITH-X20.dellirinaetech.com.tw. A      61.218.23.68
tiger.dellirinaetech.com.tw. A      61.218.23.1
www.dellirinaetech.com.tw. A      282.381.238.245
aegis [etc/named]#
```

Taiwan Computer Emergency Response Team / Coordination Center



Questions?

台灣電腦網路危機處理暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center