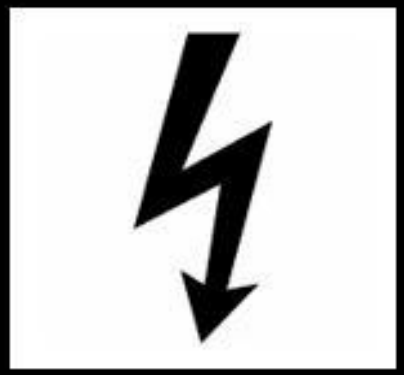
DANGER



DNS Has Been Found To Be Hazardous To Your Health

Use With Caution

Robert Stucke

bobx@rot26.net

Disclaimer: This presentation is based upon personal research that was not supported or authorized by my employer. The material being presented may be considered offensive to those with weak hearts, a sense of ethics, or those highly invested in technology funds.

About Me

Phoenix @ 90K feet!

Agenda

- DNS Bit-Squatting
- Misunderstood end-point DNS behavior
- You don’t own that domain, I do
- Abandoned Botnets and Forgotten Toys

Bit-Squatting

Presented by Artem Dinaburg at Blackhat and Defcon in 2011

- **Project Page**

  http://dinaburg.org/bitsquatting.html

- **Presentation Video**

  http://youtu.be/lZ8s1JwtNas

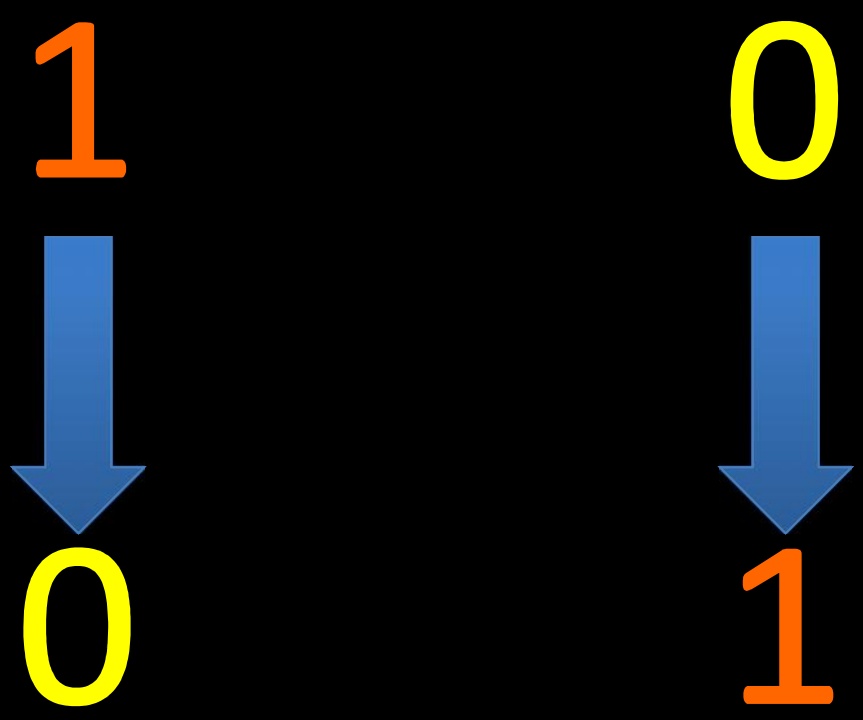
- **Presentation Slides**

  http://dinaburg.org/data/DC19_Dinaburg_Presentation.pdf

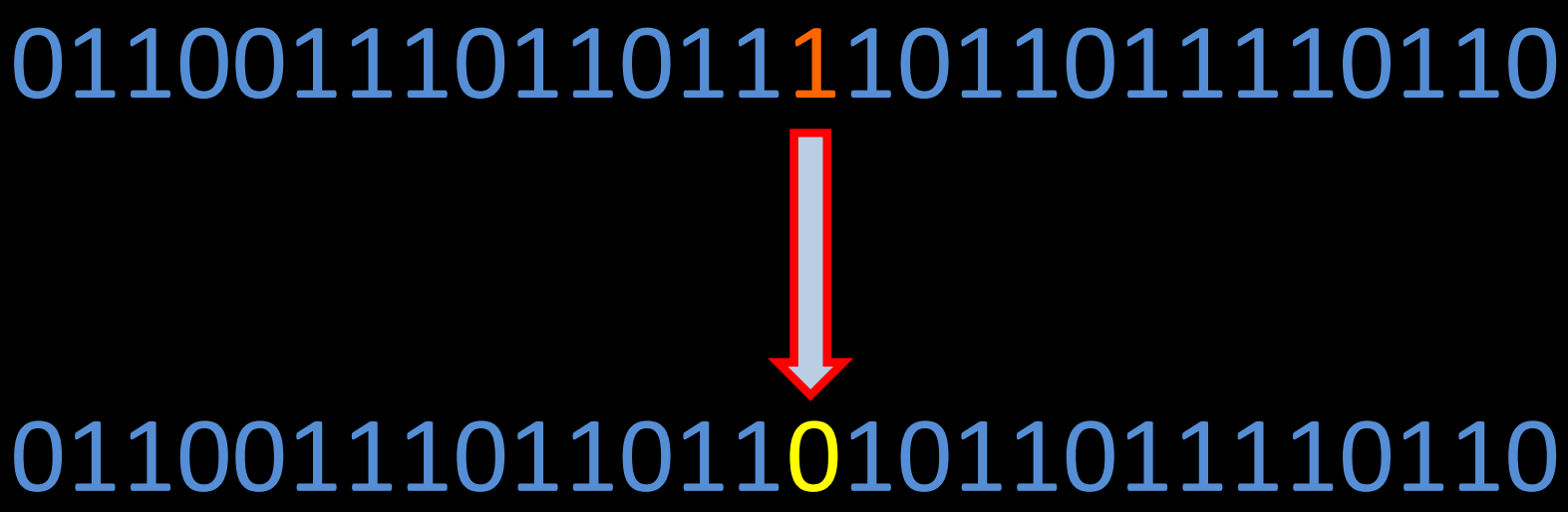
Bit-Squatting

- What is it?
- Why does it happen?
- What is the impact?

Bit-Squatting



Bit-Squatting

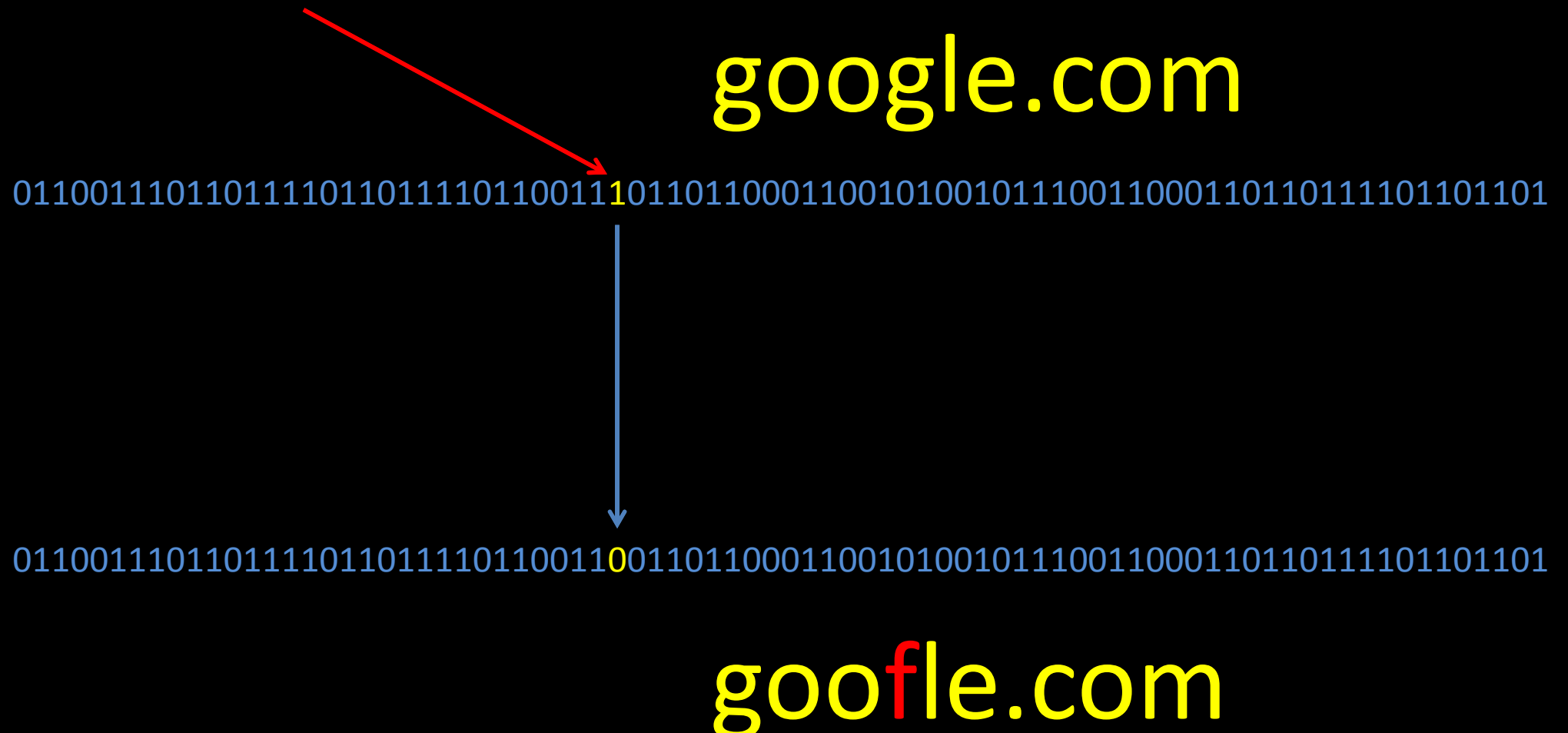


Bit-Squatting

What is Bit-Squatting?

- Anticipate the way a single bit error in memory will corrupt the DNS name
- Registering those mangled domains
- Rapture, Mayhem, Yay!

Bit-Squatting



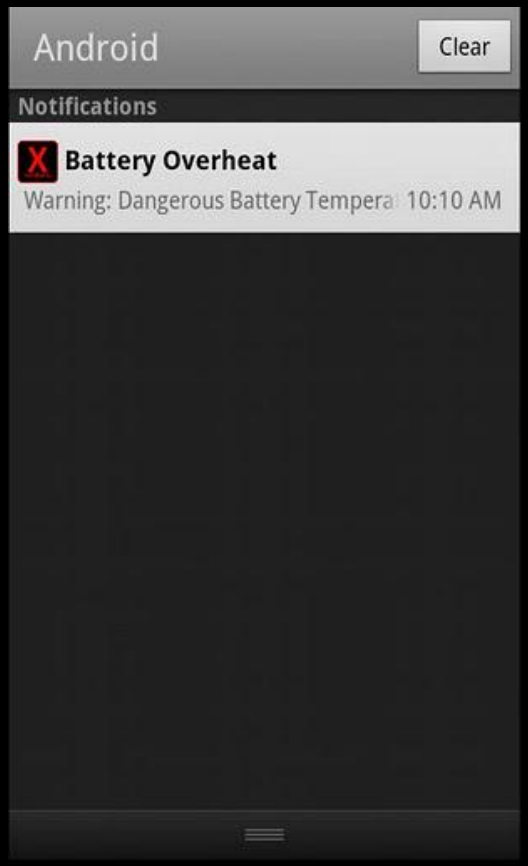
Bit-Squatting

What causes these memory errors?

- Heat
- Electrical Problems
- Radioactive Contamination
- Cosmic Rays!

Bit-Squatting

Phones



Bit-Squatting

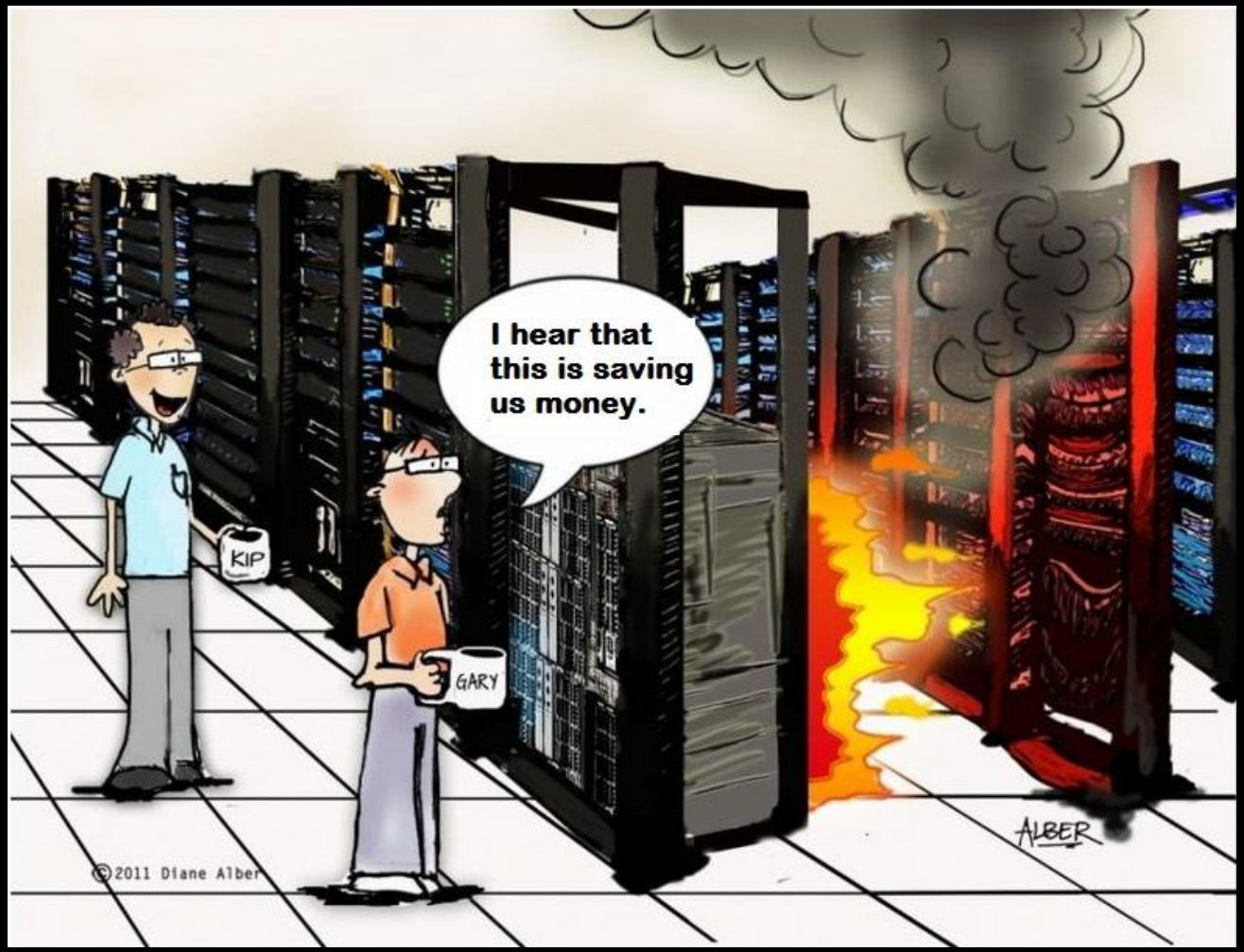
“The guidance we give to data center operators is to raise the thermostat. “

“Many data centers operate at 70 degrees or below. We’d recommend looking at going to 80 degrees”

- Erik Teetzel
Energy Program Manager at Google

The peak operating temperature Google’s Belgium data center reaches is 95 degrees Fahrenheit!

Bit-Squatting



Bit-Squatting

gstatic.com

Google domain for serving static content

CSS

Images

Javascript

XML

Bit-Squatting

gstatic.com

fstatic.com	estatic.com	cstatic.com
ostatic.com	wstatic.com	grtatic.com
gqtatic.com	gwtatic.com	gctatic.com
g3tatic.com	gsuatic.com	gsvatic.com
gspatic.com	gsdatic.com	gs4atic.com
gstctic.com	gstetic.com	gstitic.com
gstqtic.com	gstauic.com	gstavic.com
gstapic.com	gstadic.com	gsta4ic.com
gstathc.com	gstatkc.com	gstatmc.com
gstatac.com	gstatyc.com	gstatib.com
gstatia.com	gstatig.com	gstatik.com

Bit-Squatting

gstatic.com

fstatic.com	estatic.com	cstatic.com
ostatic.com	wstatic.com	grtatic.com
gqtatic.com	gwtatic.com	gctatic.com
g3tatic.com	gsuatic.com	gsvatic.com
gspatic.com	gsdatic.com	gs4atic.com
gstctic.com	gstetic.com	gstitic.com
gstqtic.com	gstauic.com	gstavic.com
gstapic.com	gstadic.com	gsta4ic.com
gstathc.com	gstatkc.com	gstatmc.com
gstatac.com	gstatyc.com	gstatib.com
gstatia.com	gstatig.com	gstatik.com

Bit-Squatting

gstatic.com

fstatic.com	estatic.com	cstatic.com
ostatic.com	wstatic.com	grtatic.com
gqtatic.com	gwtatic.com	gctatic.com
g3tatic.com	gsuatic.com	gsvatic.com
gspatic.com	gsdatic.com	gs4atic.com
gstctic.com	gstetic.com	gstitic.com
gstqtic.com	gstauic.com	gstavic.com
gstapic.com	gstadic.com	gsta4ic.com
gstathc.com	gstatkc.com	gstatmc.com
gstatac.com	gstatyc.com	gstatib.com
gstatia.com	gstatig.com	gstatik.com

Bit-Squatting

170.185.129.xx "**t1.gwtatic.com**"

GET /images?q=tbn:ANd9GcShHkx1JNpi-DLmfnciij3_3PsiBzk_Oag_ocxD9WPkcgGcZLer

http://www.google.com/search?um=1&hl=en&safe=active&biw=1024&bih=587&tbm=isch&sa=1&q=trisha+jones&oq=trisha+jones&aq=f&aqi=g1&aql=&gs_sm=e&gs_upl=6506l11170l0l11373l14l14l1l0l0l0l327l1716l2-4.2l6l0

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NE
T CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)"

Bit-Squatting

170.185.129.xx "**t1.gwtatic.com**"

GET /images?q=tbn:ANd9GcShHkx1JNpi-DLmfnciij3_3PsiBzk_Oag_ocxD9WPkcgGcZLer

http://www.google.com/search?um=1&hl=en&safe=active&biw=1024&bih=587&tbm=isch&sa=1&q=trisha+jones&oq=trisha+jones&aq=f&aqi=g1&aql=&gs_sm=e&gs_upl=6506l11170l0l11373l14l14l1l0l0l0l327l1716l2-4.2l6l0

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)"

Bit-Squatting

170.185.129.xx "**t1.gwtatic.com**"

GET /images?q=tbn:ANd9GcShHkx1JNpi-DLmfnciij3_3PsiBzk_Oag_ocxD9WPkcgGcZLer

http://www.google.com/search?um=1&hl=en&safe=active&biw=1024&bih=587&tbm=isch&sa=1&q=trisha+jones&oq=trisha+jones&aq=f&aqi=g1&aql=&gs_sm=e&gs_upl=6506l11170l0l11373l14l14l1l0l0l0l327l1716l2-4.2l6l0

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)"

Bit-Squatting

170.185.129.xx "**t1.gwtatic.com**"

GET /images?q=tbn:ANd9GcShHkx1JNpi-DLmfnciij3_3PsiBzk_Oag_ocxD9WPkcgGcZLer

http://www.google.com/search?um=1&hl=en&safe=active&biw=1024&bih=587&tbm=isch&sa=1&q=trisha+jones&oq=trisha+jones&aq=f&aqi=g1&aql=&gs_sm=e&gs_upl=6506l11170l0l11373l14l14l1l0l0l0l327l1716l2-4.2l6l0

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)"

Bit-Squatting

170.185.129.xx "**t1.gwtatic.com**"

GET /images?q=tbn:ANd9GcShHkx1JNpi-DLmfnciij3_3PsiBzk_Oag_ocxD9WPkcgGcZLer

http://www.google.com/search?um=1&hl=en&safe=active&biw=1024&bih=587&tbm=isch&sa=1&q=trisha+jones&oq=trisha+jones&aq=f&aqi=g1&aql=&gs_sm=e&gs_upl=6506l11170l0l11373l14l14l1l0l0l0l327l1716l2-4.2l6l0

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)"

Bit-Squatting

170.185.129.xx "**t1.gwtatic.com**"

GET /images?q=tbn:ANd9GcShHkx1JNpi-DLmfnciij3_3PsiBzk_Oag_ocxD9WPkcgGcZLer

http://www.google.com/search?um=1&hl=en&safe=active&biw=1024&bih=587&tbm=isch&sa=1&q=trisha+jones&oq=trisha+jones&aq=f&aqi=g1&aql=&gs_sm=e&gs_upl=6506l11170l0l11373l14l14l1l0l0l0l327l1716l2-4.2l6l0

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)"

Bit-Squatting

170.185.129.xx "**t1.gwtatic.com**"

GET /images?q=tbn:ANd9GcShHkx1JNpi-DLmfnciij3_3PsiBzk_Oag_ocxD9WPkcgGcZLer

http://www.google.com/search?um=1&hl=en&safe=active&biw=1024&bih=587&tbm=isch&sa=1&q=trisha+jones&oq=trisha+jones&aq=f&aqi=g1&aql=&gs_sm=e&gs_upl=6506l11170l0l11373l14l14l1l0l0l0l327l1716l2-4.2l6l0

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)"

Bit-Squatting

200.142.133.xx "t3.gstatmc.com“

GET /images?q=tbn:ANd9GcTpBH9vsMVT7yp6aC0-wVunxW1aIK7ICDDFjB2pMY2PKIeEOdmfNF2LpRE

"http://www.google.com.br/m/search?site=images&q=selena+gomez+photoshop&start=14&sa=N“

Bit-Squatting

200.142.133.xx "t3.gstatmc.com“

GET /images?q=tbn:ANd9GcTpBH9vsMVT7yp6aC0-wVunxW1aIK7ICDDFjB2pMY2PKIeEOdmfNF2LpRE

"http://www.google.com.br/m/search?site=images&q=selena+gomez+photoshop&start=14&sa=N“

Bit-Squatting

200.142.133.xx "t3.gstatmc.com“

GET /images?q=tbn:ANd9GcTpBH9vsMVT7yp6aC0-wVunxW1aIK7ICDDFjB2pMY2PKIeEOdmfNF2LpRE

"http://www.google.com.br/m/search?site=images&q=selena+gomez+photoshop&start=14&sa=N“

Bit-Squatting

200.142.133.xx "t3.gstatmc.com“

GET /images?q=tbn:ANd9GcTpBH9vsMVT7yp6aC0-wVunxW1aIK7ICDDFjB2pMY2PKIeEOdmfNF2LpRE

"http://www.google.com.br/m/search?site=images&q=selena+gomez+photoshop&start=14&sa=N“

Bit-Squatting

"What I want to
be when I grow up"

Bit-Squatting

But isn’t this just random noise?

Bit-Squatting

91.217.185.104 "www.g3tatic.com" GET /m/images/logo_small.gif "Nokia5130c-2/2.0 (07.91) Profile/MIDP-2.1 Configuration/CLDC-1.1“

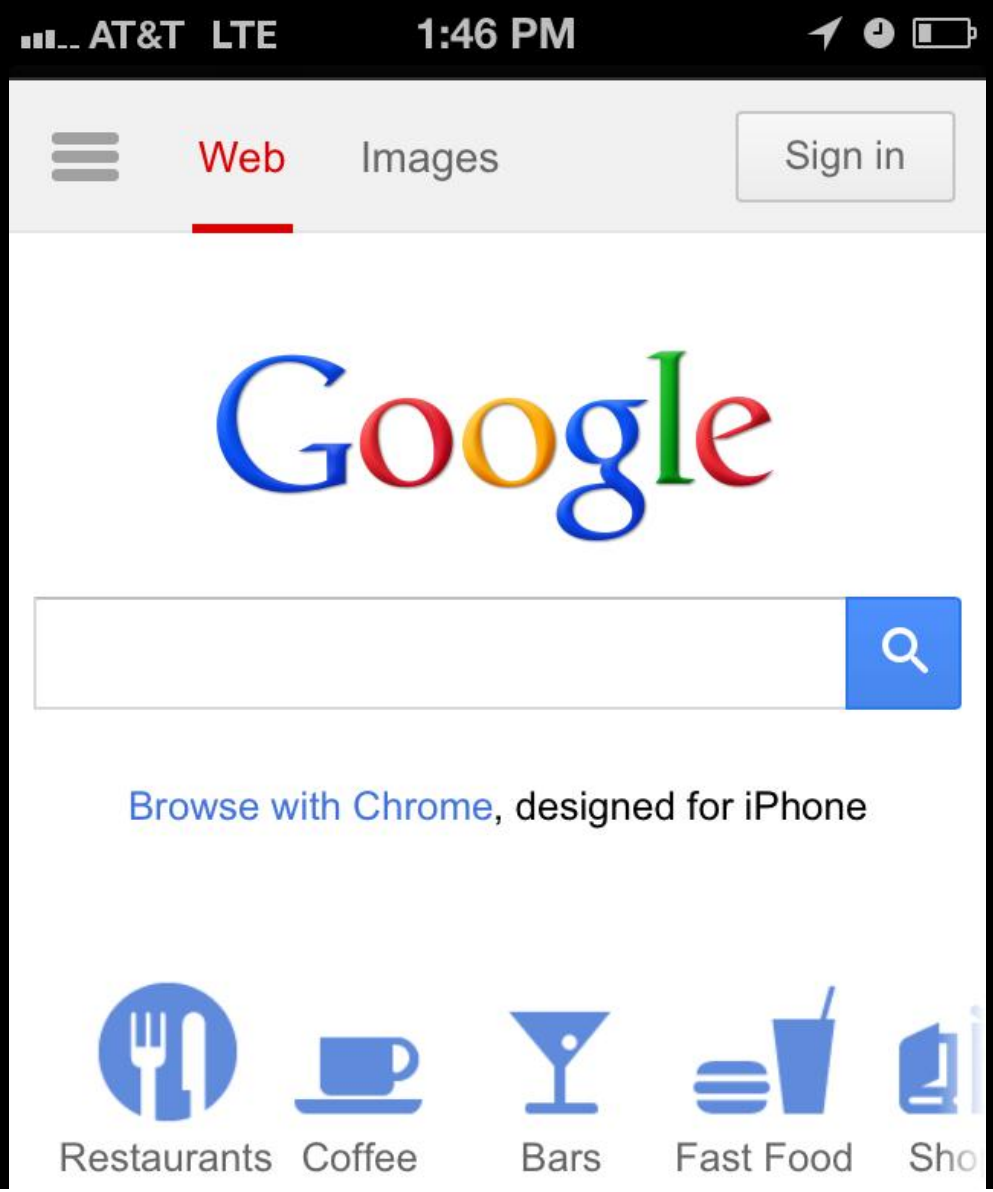
125.235.49.56 "www.g3tatic.com" GET /m/images/logo_small.gif "GIONEE-D6/SW1.0.0/WAP2.0“

196.201.208.32 "www.g3tatic.com" GET /m/images/logo_small.gif "Alcatel-OT-305/1.0 ObigoInternetBrowser/Q03C“

125.235.49.55 "www.g3tatic.com" GET /m/images/logo_small.gif "LG-GB270 Obigo/WAP2.0 MIDP-2.0/CLDC-1.1“

200.89.84.90 "www.g3tatic.com" GET /m/images/logo_small.gif "ZTE-G_R221/WAP2.0"

Bit-Squatting



Bit-Squatting

Bit-Squatting

What else is that heat doing to Google servers?

Bit-Squatting

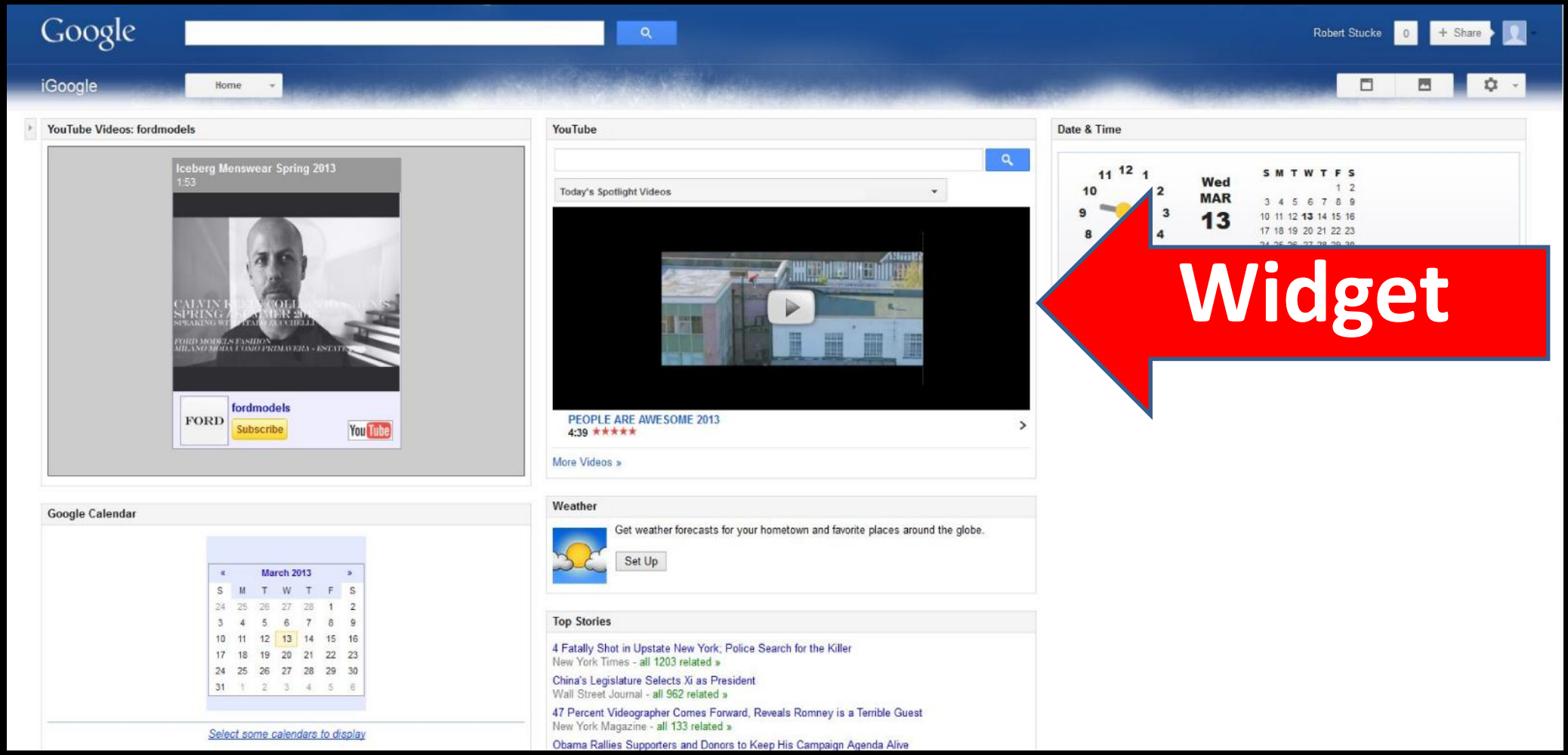
209.85.226.83 "www.gwtatic.com" /igomodules/youtube/v3/youtufe.xml "Feedfetcher-Google”

209.85.224.96 "www.gstqtic.com" /ig/modules/youtube/v3/youtube.xml "Feedfetcher-Google”

209.85.226.89 "www.gstctic.com" /ig/modules/tabnews/kennedy/tabnews.xml "Feedfetcher-Google”

209.85.228.82 "www.gstatmc.com" /ig/modules/wikipedia/kennedy/wikipedia.xml "Feedfetcher-

Bit-Squatting



Bit-Squatting

```
<?xml version="1.0" encoding="UTF-8" ?>
<Module>
    <ModulePrefs
      title="__MSG_title__"
      directory_title="__MSG_title__"
      title_url="//maps.google.com/maps?q=__UP_location__"
     description="__MSG_description__"
     author="Mark L."
     author_affiliation="Google"
     author_location="Santa Barbara, CA"
     default_value="false"/>

...

<![CDATA[
```

The goods are in here!

Bit-Squatting

```
background-image:url(‘

http://www.grtatic.com/ig/modules/gadgetfactory/v2/search-white.cache.png

’)
```

Bit-Squatting

62.30.127.40 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
62.30.90.211 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
62.31.197.88 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
77.101.112.66 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
77.101.54.41 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
77.103.212.102 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
77.96.107.165 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
77.96.68.59 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
77.96.94.150 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
77.98.65.88 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
80.195.240.134 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
80.195.240.140 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
80.195.240.66 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
80.195.28.42 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
82.38.119.43 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
82.41.181.77 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"
82.41.183.91 "www.grtatic.com" "GET /ig/modules/gadgetfactory/v2/search-white.cache.png"

Bit-Squatting

GB,	62.30.127.40,	Virgin Media
GB,	62.30.90.211,	Virgin Media
GB,	62.31.197.88,	Virgin Media
GB,	77.101.112.66,	Virgin Media
GB,	77.101.54.41,	Virgin Media
GB,	77.103.212.102,	Virgin Media
GB,	77.96.107.165,	Virgin Media
GB,	77.96.68.59,	Virgin Media
GB,	77.96.94.150,	Virgin Media
GB,	77.98.65.88,	Virgin Media
GB,	80.195.240.134,	Virgin Media
GB,	80.195.240.140,	Virgin Media
GB,	80.195.240.66,	Virgin Media
GB,	80.195.28.42,	Virgin Media
GB,	82.38.119.43,	Virgin Media
GB,	82.41.181.77,	Virgin Media
GB,	82.41.183.91,	Virgin Media
GB,	82.46.238.196,	Virgin Media

Bit-Squatting

Fun with Postini

$ **dig mozilla.org. mx +short**

400 **mozilla.com**.s5b2.**psmtp.com.**

100 **mozilla.com**.s5a1.**psmtp.com.**

200 **mozilla.com**.s5a2.**psmtp.com.**

300 **mozilla.com**.s5b1.**psmtp.com.**

Bit-Squatting

about.com.mail11.prmtp.com
aggintl.com.s9a2.prmtp.com
airties.com.s0b2.prmtp.com
amg-inc.com.s7a2.prmtp.com
ashbyco.com.s7b1.prmtp.com
atcomhq.com.s8b2.prmtp.com
bardadv.com.s5a2.prmtp.com
bbinswa.com.s6a1.prmtp.com
bc.pitt.edu.s7b1.prmtp.com
bridge.nl.s200a1.prmtp.com
bryant.edu.s10a2.prmtp.com
cableone.net.mail6.prmtp.com
cch-lis.com.s5a1.prmtp.com
cinmach.com.s8b2.prmtp.com
cvcvbc.aw46z.prmtp.com
acterna.com.s7b2.prmtp.com
ahrcnyc.org.s8a2.prmtp.com
alaska.com.mail5.prmtp.com
ams-pmt.com.s5a1.prmtp.com
ashland.com.s5a1.prmtp.com
auracom.com.s6a1.prmtp.com
baseinc.com.s8b2.prmtp.com
bbrslaw.com.s8b1.prmtp.com
bda-inc.com.s7a1.prmtp.com
brofort.com.s8b2.prmtp.com
bslogin.com.s9a1.prmtp.com
calarts.edu.s9a1.prmtp.com
charity.org.s5a2.prmtp.com
conxxus.com.s6b2.prmtp.com
cwl-inc.com.s5b2.prmtp.com
aeecorp.com.s5a1.prmtp.com
aireco.com.mail6.prmtp.com
alston.com.mail5.prmtp.com
archenv.com.s7a1.prmtp.com
asurion.com.s9a1.prmtp.com
autogas.com.s7a1.prmtp.com
b-bachs.com.s5a1.prmtp.com
bbt.co.uk.s200a2.prmtp.com
braden.com.s10b2.prmtp.com
brunico.com.s9a1.prmtp.com
bwnoise.com.s7b2.prmtp.com
capital.net.s6b2.prmtp.com
chouest.com.s5a1.prmtp.com
dbigolf.com.s6b2.prmtp.com

Bit-Squatting

dcsdk12.org.s9a2.prmtp.com
dcshoes.com.s5b2.prmtp.com
deloitte.dk.s7b1.prmtp.com
denvest.com.s9a1.prmtp.com
desales.edu.s8a2.prmtp.com
detnews.com.s7a1.prmtp.com
digitel.net.s7a1.prmtp.com
dlvbbdo.com.s7b1.prmtp.com
dnata.com.s201b2.prmtp.com
duralee.com.s7a2.prmtp.com
dvicomm.com.s9b2.prmtp.com
Ecomdss.com.s8b1.prmtp.com
ecsdnv.net.s10b1.prmtp.com
educate.com.s5a1.prmtp.com
ee.pitt.edu.s7b1.prmtp.com
eknikl.ldoy2.prmtp.com
e-m.co.uk.s200a1.prmtp.com
emerson.com.s7a2.prmtp.com
eritter.net.s6b2.prmtp.com
esedona.net.s6a1.prmtp.com
fordham.edu.s8a2.prmtp.com
futurestep.com.s8b2.prmtp.com
galileo.com.s8a1.prmtp.com
gannett.com.s7a1.prmtp.com
gdjpud.vsnad.prmtp.com
genpact.com.s8a1.prmtp.com
glcomp.com.mail6.prmtp.com
hal-pc.org.mail1.prmtp.com
herguth.com.s7a1.prmtp.com
hklaw.com.mail12.prmtp.com
hocking.net.s5b2.prmtp.com
hpdsoftware.com.s200b2.prmtp.com
ici-llc.com.s5b2.prmtp.com
infoave.net.s5a2.prmtp.com
infonxx.com.s8b1.prmtp.com
infopia.com.s7a1.prmtp.com
innovex.com.s8a1.prmtp.com
itronix.com.s8b2.prmtp.com
jaxbank.com.s5a1.prmtp.com
jcurran.com.s7b1.prmtp.com
jennmar.com.s9a2.prmtp.com
jet-web.com.s9a2.prmtp.com
jfshea.com.s10a2.prmtp.com
juniper.net.s7a1.prmtp.com
kdlegal.com.s8a1.prmtp.com
koenigs.com.s5a1.prmtp.com
kpmg.com.hk.s8a1.prmtp.com

Bit-Squatting

lakemac.net.s6a2.prmtp.com
lesspub.com.s9a1.prmtp.com
liebert.com.s7a1.prmtp.com
limitlessny.s8a2.prmtp.com
mag-ias.com.s8a1.prmtp.com
minpack.com.s5b2.prmtp.com
mq.edu.au.s200a1.prmtp.com
myexcel.com.s6a1.prmtp.com
newport.com.s8a2.prmtp.com
opm-llc.com.s8a1.prmtp.com
pacrelo.com.s8b2.prmtp.com
pickpro.com.s7a1.prmtp.com
prupref.com.s9a1.prmtp.com
regions.com.s6a1.prmtp.com
rodale.com.mail5.prmtp.com

laser27.com.s8b2.prmtp.com
lexmark.com.s8b1.prmtp.com
lifeway.com.s5a1.prmtp.com
lindal.com.s10a1.prmtp.com
markany.com.s7a1.prmtp.com
mozilla.com.s5a1.prmtp.com
mudlake.net.s8b1.prmtp.com
netptc.net.mail8.prmtp.com
nominum.com.s7a2.prmtp.com
orkla.com.s200a2.prmtp.com
pccpllc.com.s9a1.prmtp.com
pogolaw.com.s8a1.prmtp.com
qed-inc.com.s9a1.prmtp.com
remax-lx.ca.s7a1.prmtp.com
rosetti.com.s6b1.prmtp.com

lchcnet.org.s8a1.prmtp.com
lfstaff.com.s8a2.prmtp.com
limitlessny.s8a1.prmtp.com
maciejn.com.s7a1.prmtp.com
mendes.com.mail5.prmtp.com
mpitime.com.s7b2.prmtp.com
muskoka.com.s5a1.prmtp.com
netsync.net.s9a1.prmtp.com
nqlc.com.au.s9a1.prmtp.com
pacific.net.s5a1.prmtp.com
perlick.com.s8a1.prmtp.com
postini.com.s8a1.prmtp.com
re4u.net.s8a2.prmtp.com
rivkin.com.mail5.prmtp.com
route24.net.s9b2.prmtp.com

Bit-Squatting

rubloff.com.s9b1.prmtp.com
seabox.com.s10b2.prmtp.com
silanis.com.s5a1.prmtp.com
smkdlaw.com.s6b1.prmtp.com
sscotti.org.s7b2.prmtp.com
stevens.edu.s9a2.prmtp.com
stryker.com.s8a1.prmtp.com
swassoc.com.s8a2.prmtp.com
tctwest.net.s5a1.prmtp.com
undss.org.s201b2.prmtp.com
vss.fsi.com.s5a1.prmtp.com
yaskawa.com.s5a1.prmtp.com
sage.com.au.s7b1.prmtp.com
shawinc.com.s6b1.prmtp.com
seattle.gov.s8b1.prmtp.com
smythnora.com.s8a2.prmtp.com
state.pa.us.s7a1.prmtp.com
stibo.com.s200a1.prmtp.com
studeo.com.s10a1.prmtp.com
swisher.com.s8b2.prmtp.com
thomson.net.s7a2.prmtp.com
unomaha.edu.s5a2.prmtp.com
wctatel.net.s6a1.prmtp.com
zachry.com.s10b1.prmtp.com
sbolive.com.s5a1.prmtp.com
sig-ins.com.s7a2.prmtp.com
smlperu.com.s6b2.prmtp.com
solusii.com.s7a1.prmtp.com
stena.com.s200b2.prmtp.com
stroock.com.s6a2.prmtp.com
surfari.net.s8b1.prmtp.com
talent2.com.s9a1.prmtp.com
udayton.edu.s9b2.prmtp.com
uwc.ac.za.s200a1.prmtp.com
weshred.net.s8b1.prmtp.com

Bit-Squatting

Explore how this kind of thing will affect you.

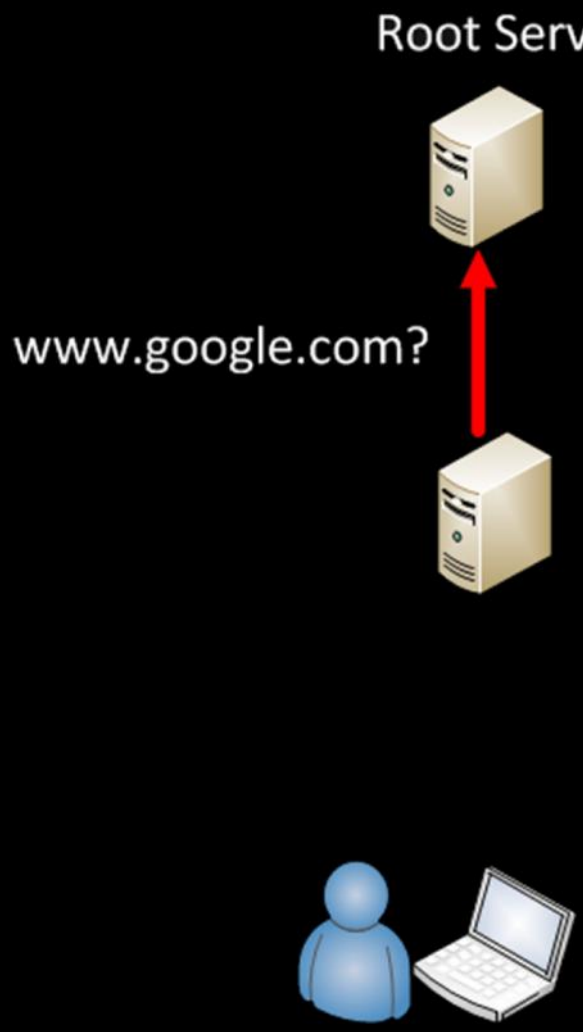
Misunderstood End-Point Behavior

Misunderstood End-Point Behavior

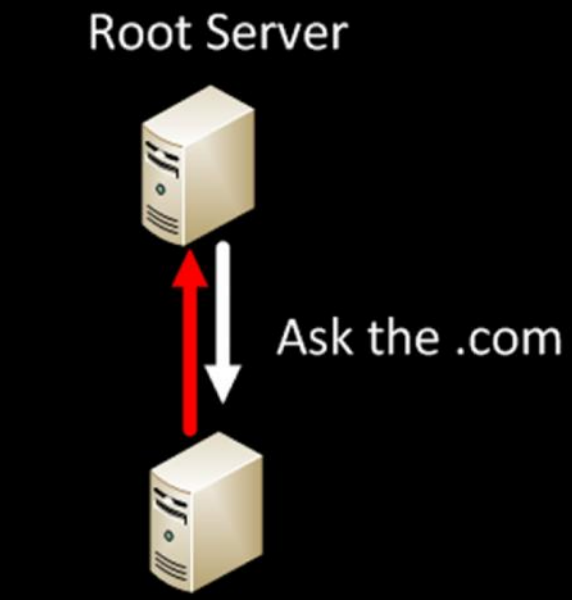
- Expected resolver behavior
- DNS suffix search paths
- Poorly documented behavior
- Observations and lessons learned

Misunderstood End-Point Behavior

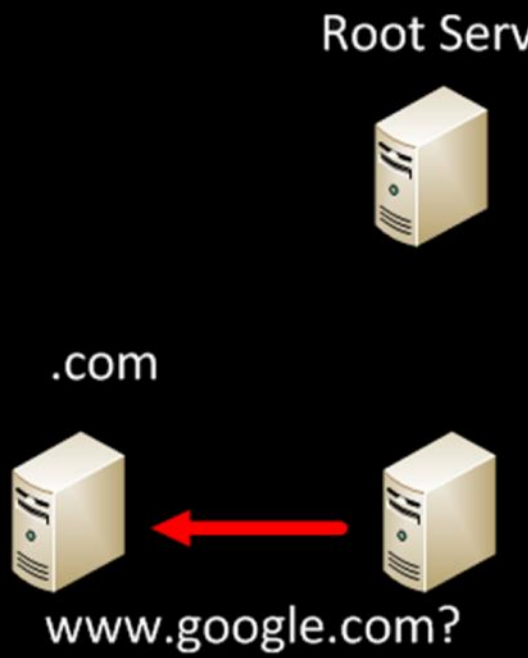
Misunderstood End-Point Behavior



Misunderstood End-Point Behavior

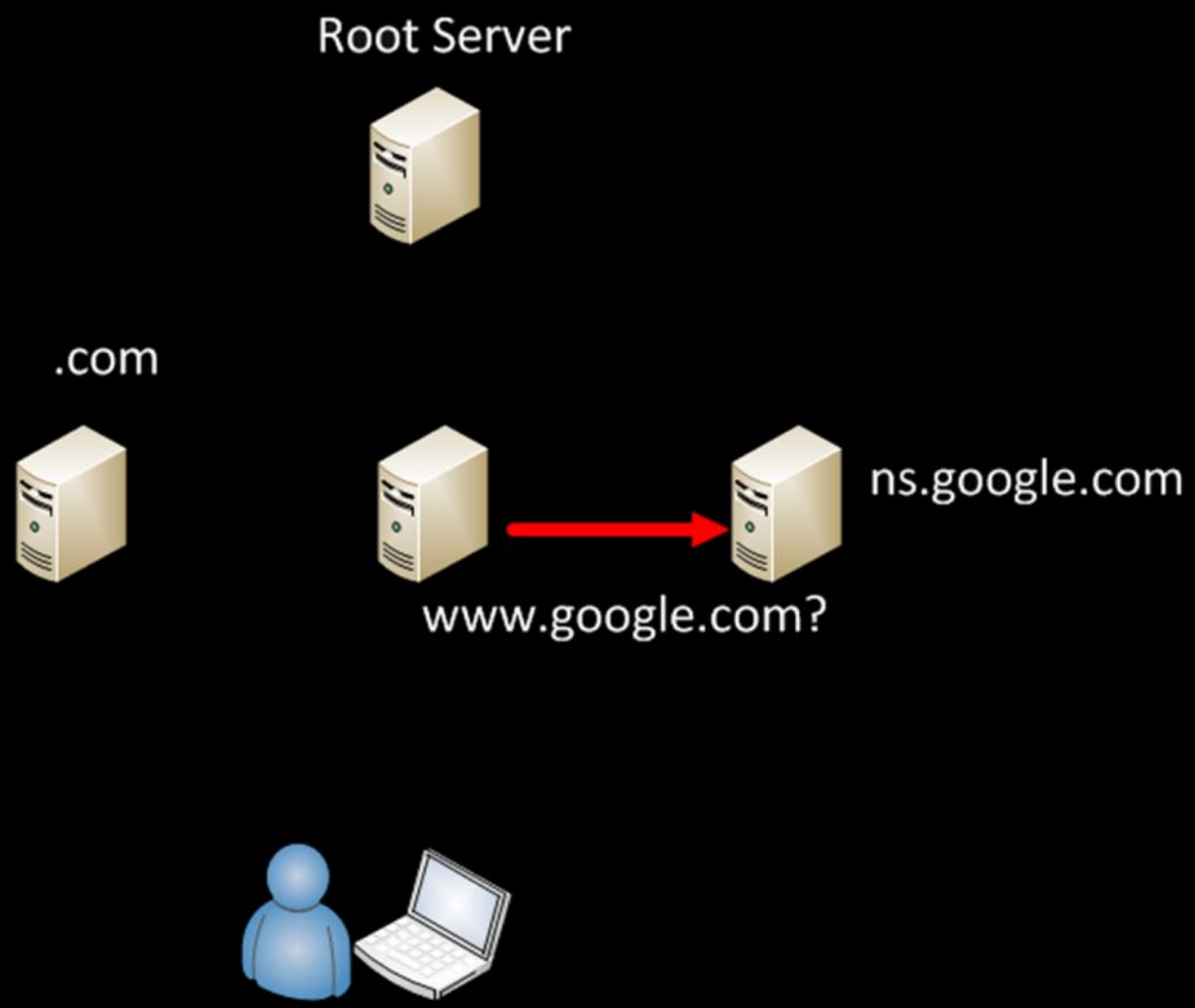


Misunderstood End-Point Behavior

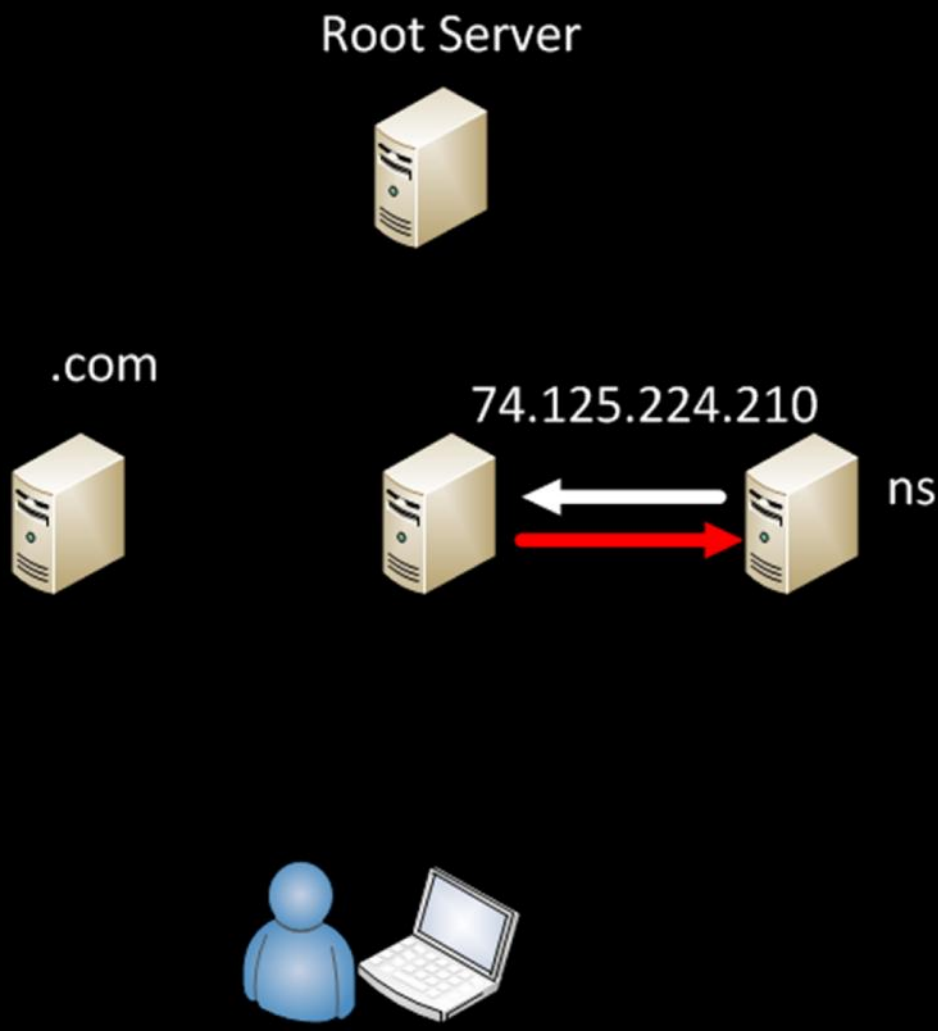


Misunderstood End-Point Behavior

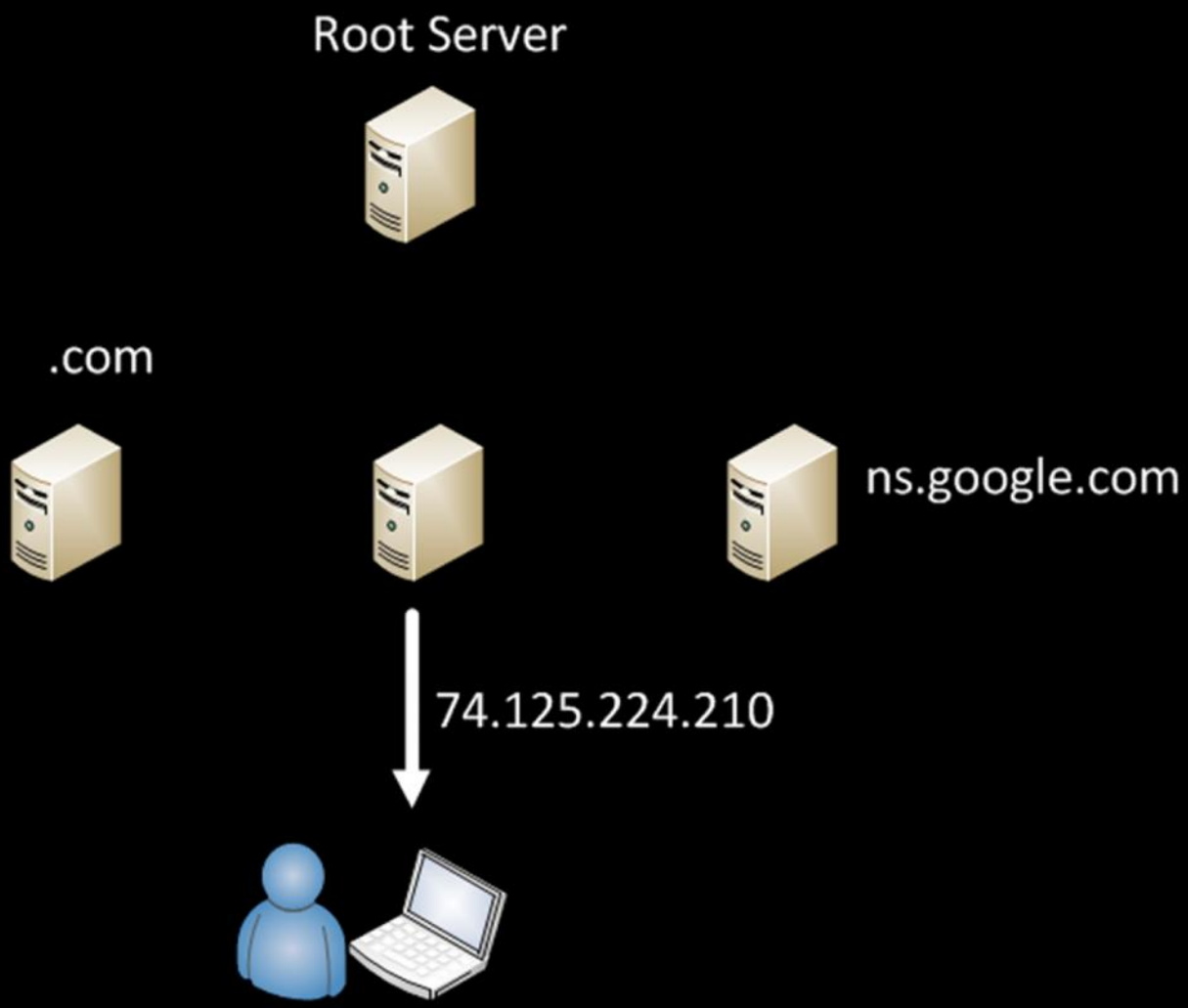
Misunderstood End-Point Behavior



Misunderstood End-Point Behavior



Misunderstood End-Point Behavior



Misunderstood End-Point Behavior

www.google.com

Misunderstood End-Point Behavior

www.google.com. 

Misunderstood End-Point Behavior

www.google.com
google.com
www
www.google.com.

Misunderstood End-Point Behavior

- Suffix Search Paths
- DNS Devolution

Misunderstood End-Point Behavior

Suffix Search Paths

Foo Inc.

- ad.foo.com
- foo.com

Misunderstood End-Point Behavior

Suffix Search Paths

XP Behavior

DNS Query -> www.ad.foo.com
DNS Query -> www.foo.com

NetBIOS Query -> www

Misunderstood End-Point Behavior

Suffix Search Paths

XP Behavior

DNS Query -> www.phx
DNS Query -> www.phx.ad.foo.com
DNS Query -> www.phx.foo.com

NetBIOS Query -> www.phx

Misunderstood End-Point Behavior

Suffix Search Paths

Post-XP Behavior

DNS Query -> www.phx

NetBIOS Query -> www.phx

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com
DNS Query –> www.foo.com

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com
DNS Query –> www.foo.com
DNS Query –> www.com

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **ad.foo.co.uk**

DNS Query –> www.ad.foo.co.uk
DNS Query –> www.foo.co.uk
DNS Query –> www.co.uk

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **ad.foo.co.uk**

DNS Query –> www.ad.foo.co.uk
DNS Query –> www.foo.co.uk
~~DNS Query –> www.co.uk~~

Misunderstood End-Point Behavior

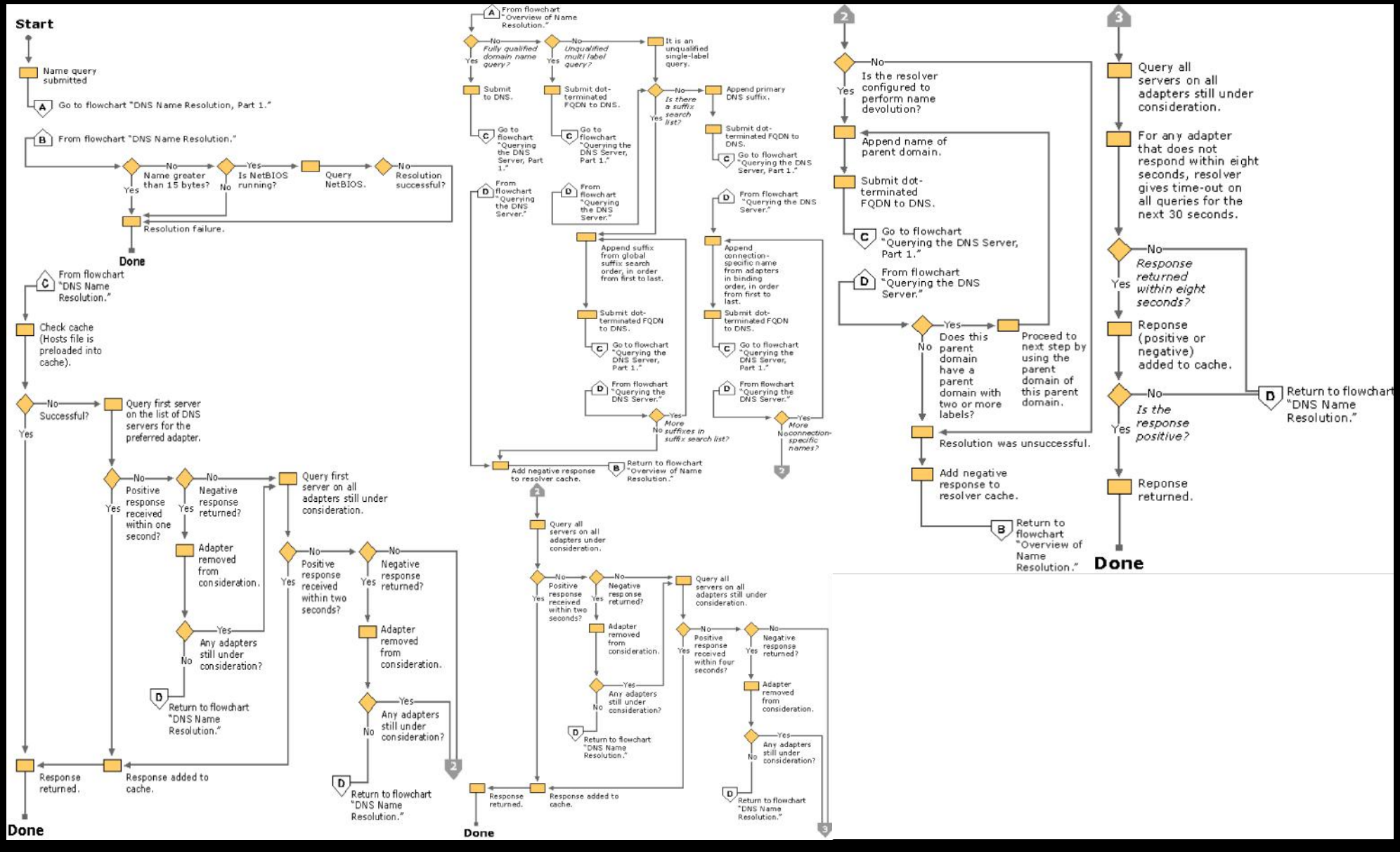
DNS Devolution

XP Behavior

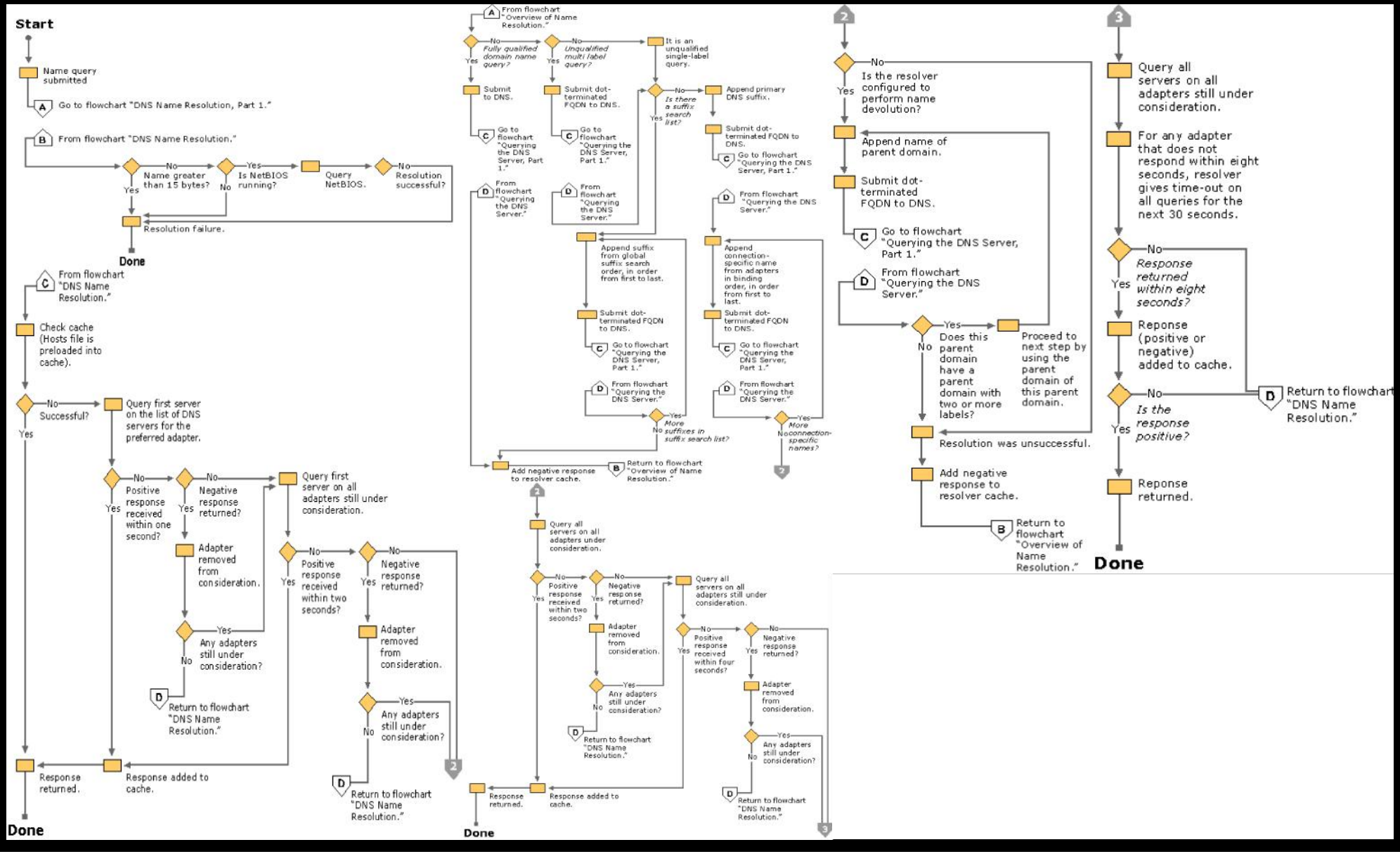
Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com
~~DNS Query –> www.foo.com~~

Misunderstood End-Point Behavior



Misunderstood End-Point Behavior



Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com
~~DNS Query –> www.foo.com~~
~~DNS Query –> www.com~~

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com
DNS Query –> www.foo.com
~~DNS Query –> www.com~~

Misunderstood End-Point Behavior

DNS Devolution

XP Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com
DNS Query –> www.foo.com
DNS Query –> www.com

Misunderstood End-Point Behavior

DNS Devolution

Windows 7 Behavior

Connection Specific Domain – **phx.ad.foo.com**

DNS Query –> www.phx.ad.foo.com
DNS Query –> www.ad.foo.com
DNS Query –> www.foo.com
~~DNS Query –> www.com~~

Misunderstood End-Point Behavior

Fixed?

Misunderstood End-Point Behavior

BYOD
Mobile
Broken XP

Misunderstood End-Point Behavior

BYOD
Mobile
Broken XP

Misunderstood End-Point Behavior

sipinternal.com

proxy-phoenix.com
set-proxy.com

Misunderstood End-Point Behavior

sipinternal.com

REGISTER sip:com SIP/2.0
Via: SIP/2.0/TCP 199.41.198.254:33663
Max-Forwards: 70
From: <sip:com>;tag=e72f0d4ce7;epid=895120c8c2
To: <sip:com>
Call-ID: 53b3ec1c2e0547ab9b72ab97ed17c8b0
CSeq: 1 REGISTER
Contact: <sip:**199.41.198.254**:33663;transport=tcp;ms-opaque=8300f99968>;methods="INVITE, MESSAGE, INFO, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER, BENOTIFY";proxy=replace;+sip.instance="<urn:uuid:D964A4BE-A17A-50DD-9D69-836911E33E95>"
User-Agent: UCCAPI/3.5.6907.221 OC/3.5.6907.221 (Microsoft Office Communicator 2007 R2)
Supported: gruu-10, adhoclist, msrtc-event-categories
Supported: ms-forking
ms-keep-alive: UAC;hop-hop=yes
Event: registration
Content-Length: 0

Misunderstood End-Point Behavior

proxy-phoenix.com

Misunderstood End-Point Behavior

set-proxy.com

170.249.6.88 "set-proxy.com" "GET /bin/setup.proxy"
170.249.6.88 "set-proxy.com" "GET /bin/setup.proxy"
170.249.6.88 "set-proxy.com" "GET /bin/setup.proxy"
170.249.6.88 "set-proxy.com" "GET /bin/setup.proxy"
170.249.6.88 "set-proxy.com" "GET /bin/setup.proxy"
170.249.6.88 "set-proxy.com" "GET /bin/setup.proxy"

NetRange:	170.249.0.0 - 170.250.255.255
OrgName:	Arthur Andersen
OrgId:	ARTHUR-15

Misunderstood End-Point Behavior

set-proxy.com

```
170.252.248.200 "GET /bin/setup.proxy" "mstreamd/1 CFNetwork/548.1.4 Darwin/11.0.0"
170.252.248.200 "GET /bin/setup.proxy" "WordsWithFriendsPaid/4.12.1 CFNetwork/548.1.4 Darwin
170.252.248.200 "GET /bin/setup.proxy" "itunesstored (unknown version) CFNetwork/548.1.4 Darwin
170.252.248.200 "GET /bin/setup.proxy" "Mail/53 CFNetwork/548.1.4 Darwin/11.0.0"
170.252.248.200 "GET /bin/setup.proxy" "GeoServices/84 CFNetwork/548.1.4 Darwin/11.0.0"
170.252.248.200 "GET /bin/setup.proxy" "Maps/1.0 CFNetwork/548.1.4 Darwin/11.0.0"
170.252.248.200 "GET /bin/setup.proxy" "itunesstored (unknown version) CFNetwork/548.1.4 Darwin
170.252.248.200 "GET /bin/setup.proxy" "dataaccessd (unknown version) CFNetwork/548.1.4 Darwin
170.252.248.200 "GET /bin/setup.proxy" "mstreamd/1 CFNetwork/548.1.4 Darwin/11.0.0"
170.252.248.200 "GET /bin/setup.proxy" "itunesstored (unknown version) CFNetwork/548.1.4 Darwin
```

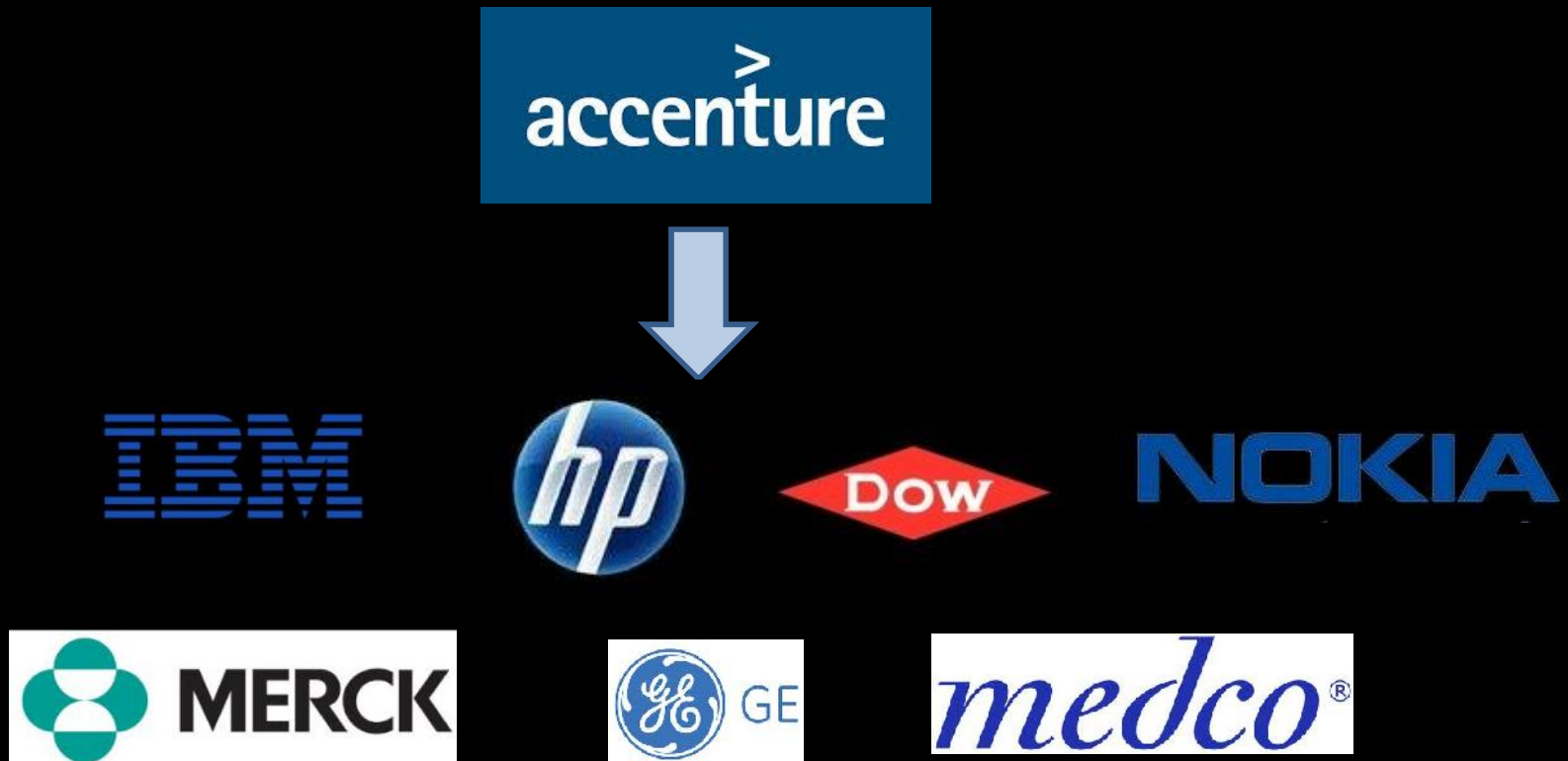
NetRange:	170.251.0.0 - 170.252.255.255
OrgName:	Accenture
OrgId:	ACCENT-10

Misunderstood End-Point Behavior

set-proxy.com

Misunderstood End-Point Behavior

set-proxy.com



Misunderstood End-Point Behavior

Don’t trust expectations based upon on how things used to work, monitor and understand what normal DNS traffic looks like on your network.

You don’t own that domain

I do >:)

You don’t own that domain

I do >:)

You don’t own that domain

“HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\SearchList”

Or

“Windows IP Configuration” + “DNS Suffix Search List”

You don’t own that domain

Windows IP Configuration

Host Name . . . . . : AN990107196
Primary Dns Suffix . . . . . : quanta.corp
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : quanta.corp

rsquanta.com

quantacn.com

You don’t own that domain

Windows IP Configuration

Host Name . . . . . : AN990107196
Primary Dns Suffix . . . . . : quanta.corp
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : quanta.corp

rsquanta.com

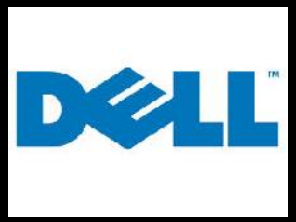
quantacn.com

You don’t own that domain

“Quanta Computer”

60,000 employees worldwide

manufactures hardware for



You don’t own that domain

myproxy.rsquanta.com
proxycn.rsquanta.com
proxy.rsquanta.com
wpad.rsquanta.com

wsus01.rsquanta.com
wsus-cq.rsquanta.com
wsus-sh1.rsquanta.com
SMS_SLP.rsquanta.com

mailbx01.rsquanta.com
mailbx02.rsquanta.com
mailbx03.rsquanta.com
mailhub04.rsquanta.com
mailhub05.rsquanta.com

FTP-CHT.rsquanta.com
ftp.rsquanta.com
nb1ftp.rsquanta.com
nb5-ftp.rsquanta.com
f1ftp02.rsquanta.com
ftp01.rsquanta.com

You don’t own that domain

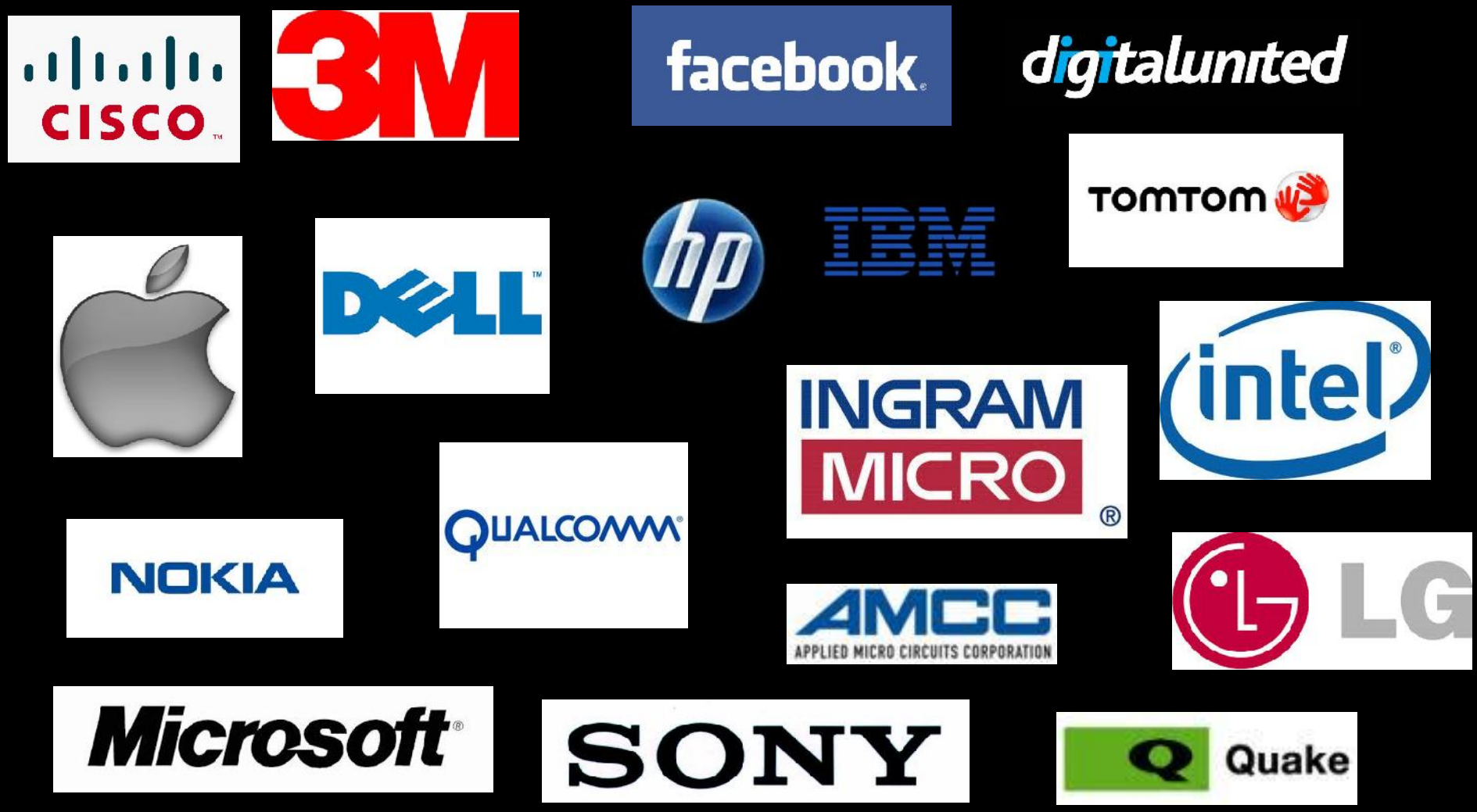
173.37.87.155: view external-in: query: **proxy.rsquanta.com**
171.70.168.155: view external-in: query: **QRDCOFC05.rsquanta.com**
171.70.168.167: view external-in: query: **wpad.rsquanta.com**

17.254.0.23: view external-in: query: **wpad.rsquanta.com**
17.254.0.23: view external-in: query: **wsus01.rsquanta.com**
17.254.0.23: view external-in: query: **proxy.rsquanta.com**

136.229.2.57: view external-in: query: **proxy.rsquanta.com**
136.229.2.56: view external-in: query: **qrdcprt02.rsquanta.com**
136.229.2.57: view external-in: query: **QRDCOFC03.quanta.corp.rsquant**

143.166.82.252: view external-in: query: **wpad.rsquanta.com**
143.166.224.3: view external-in: query: **SMS_SLP.rsquanta.com**
143.166.224.11: view external-in: query: **proxy.rsquanta.com**

You don’t own that domain



You don’t own that domain

Best Dry Cleaners	99.59.76.38: query: wpad.rsquanta.com
San Francisco International Airport	216.9.98.80: query: wpad.rsquanta.com
Venetian Resort Hotel Casino	64.79.144.10: query: wpad.rsquanta.com
MGM Mirage	69.162.4.53: query: wpad.rsquanta.com

You don’t own that domain

- Please verify your configurations
- Monitor the internet for details of your internal configuration
    - Pastebin
    - Bleeping Computer
- Monitor your DNS logs to verify your clients and the clients of your onsite partners and vendors are querying what you expect

Abandoned Botnets and Forgotten Toys

Abandoned Botnets and Forgotten Toys

- Expired Command and Control Domains
- Botnet remnants
- Abandoned Botnets
- Detection

Abandoned Botnets and Forgotten Toys

microsoft-windows-security.com

Win32:EyeStye

268 remaining infections

Uses form grabbing to steal credentials

Abandoned Botnets and Forgotten Toys

--55372666816118
Content-Disposition: form-data; name="data"

bot_guid=138BFC5C-8C31-4415-92D0B382B5550E0D
process_name=iexplore.exe
hooked_func=HttpSendRequestW
func_data=POST /login.php?login_attempt=1 HTTP/1.1

lsd=AVoCccq2&email=steve*******@yahoo.com&pass=*******&default_persistent=0&timezone=240&lgnrnd=183641_PjES&lgnjs=1363743523&locale=en_US
--55372666816118--

Abandoned Botnets and Forgotten Toys

Remaining Infections

simrako.com	14162 infected
ms-stats.info	2979 infected
myrestricted.info	2203 infected
zapalinfo.info	2111 infected
ntpupdatedomain.com	1571 infected
rapeisntfunny.info	844 infected

Abandoned Botnets and Forgotten Toys

b.354782.InfO

"POST /b/i.asp HTTP/1.1”

Content-Disposition: form-data; name="InSfo”

txtUserId::Gupta

txtPassword::*******

Content-Disposition: form-data; name="BasicSInfo”

192.168.50.26|192.168.50.26|8.0000|**00-1C-C0-EB-E9-34**|BC01-0920

Abandoned Botnets and Forgotten Toys

ET_product::**SSIM**
ET_component::**BACKEND**
ET_version::**4.8**
ET_target_version::**4.8**
ET_assigned_to::**gaurav_pratap**
ET_type::**DEFECT**
ET_state::**CLOSED**
ET_reporter::**gaurav_pratap**
ET_severity::**2**
ET_priority::**2**
ET_resolution::**SOURCE_CHANGE**
ET_user_defined_list::**FILES**
ET_user_defined_list2::**SECURITY**
ET_build::**153**
ET_target_build::**184**

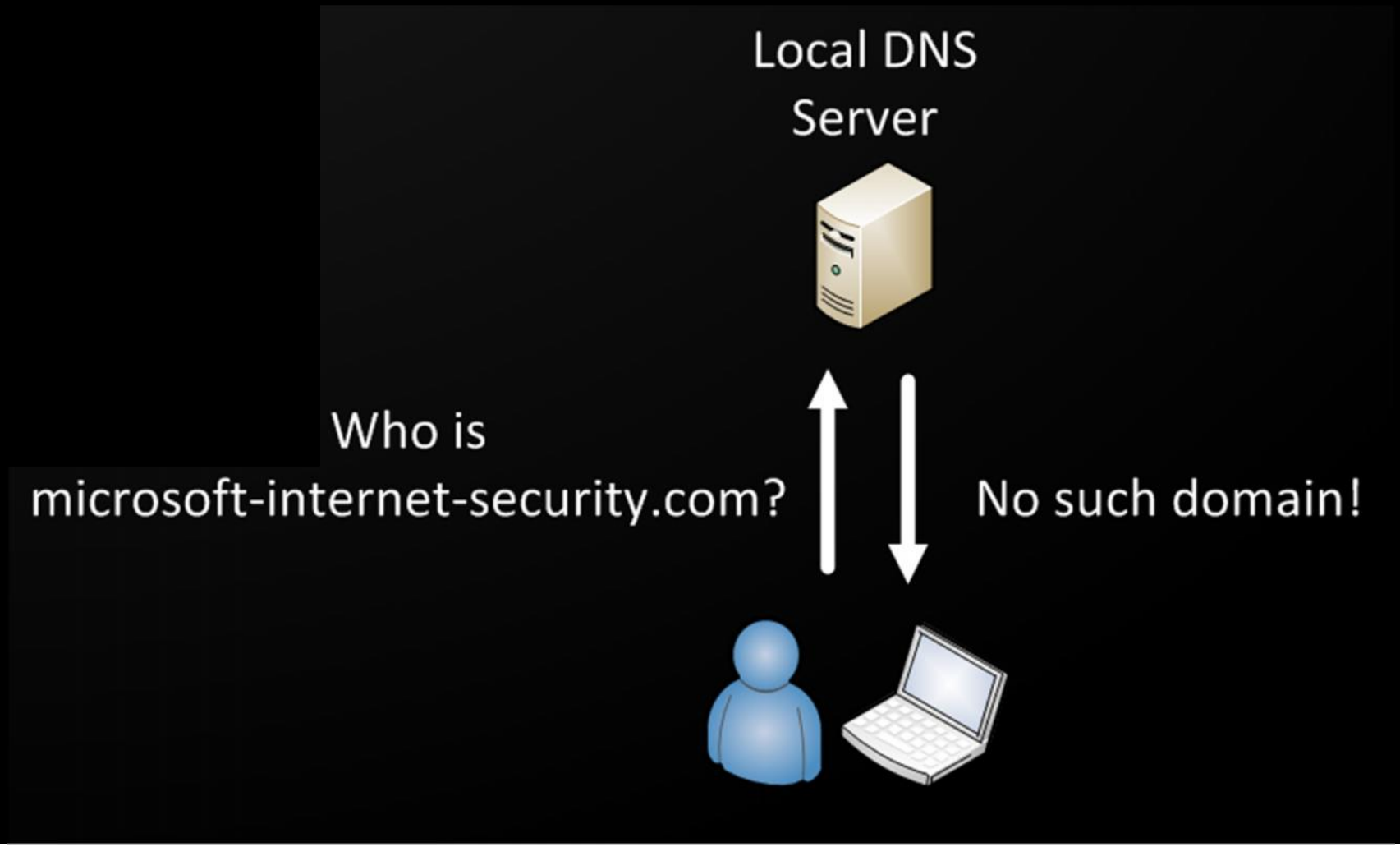
Site::**engtools.engba.symantec.com**
Mac::**00-24-E8-4A-ED-A3**
Ver::**BC01-0920**

Abandoned Botnets and Forgotten Toys

NXDOMAIN Hijacking

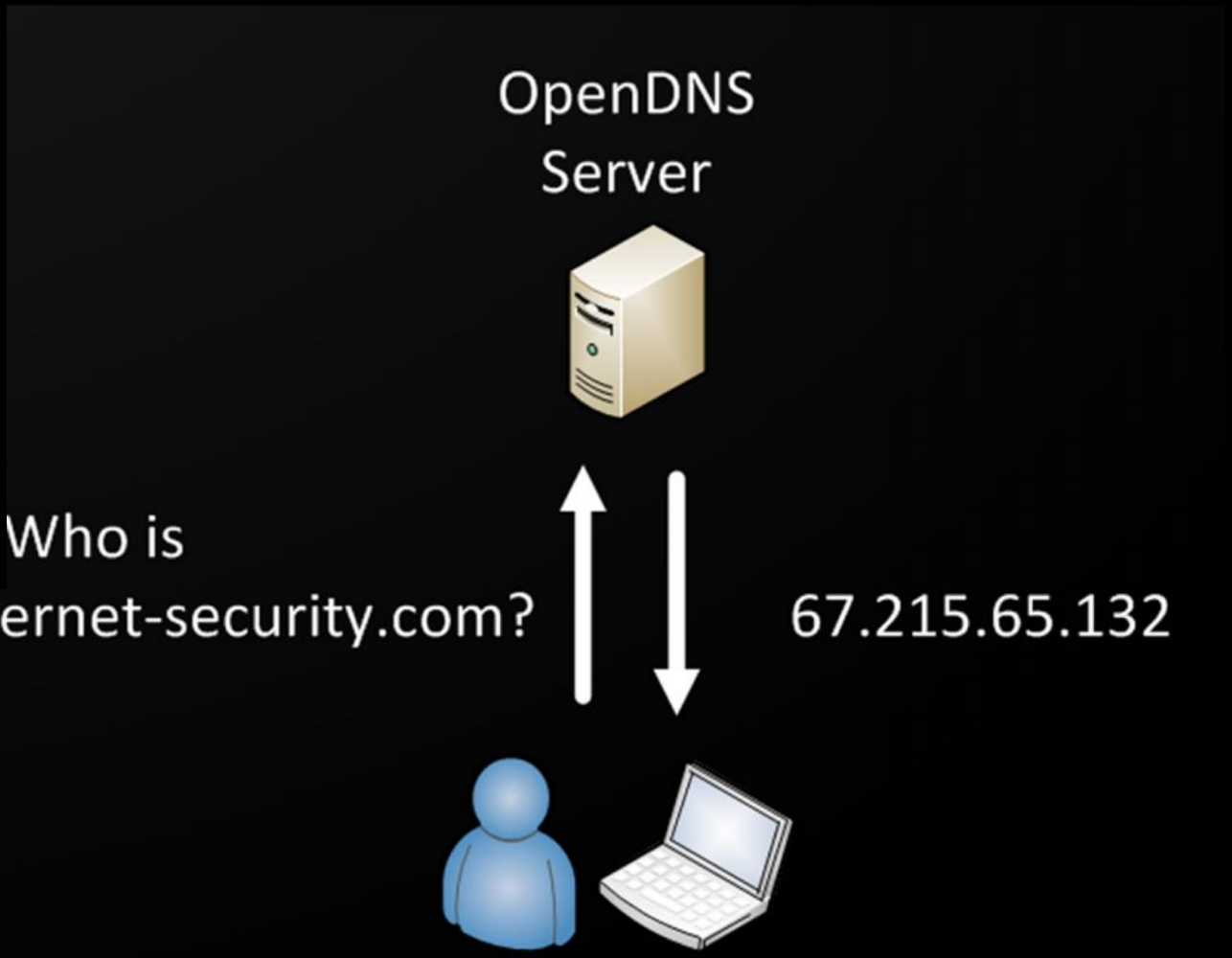
Abandoned Botnets and Forgotten Toys

NXDOMAIN Hijacking



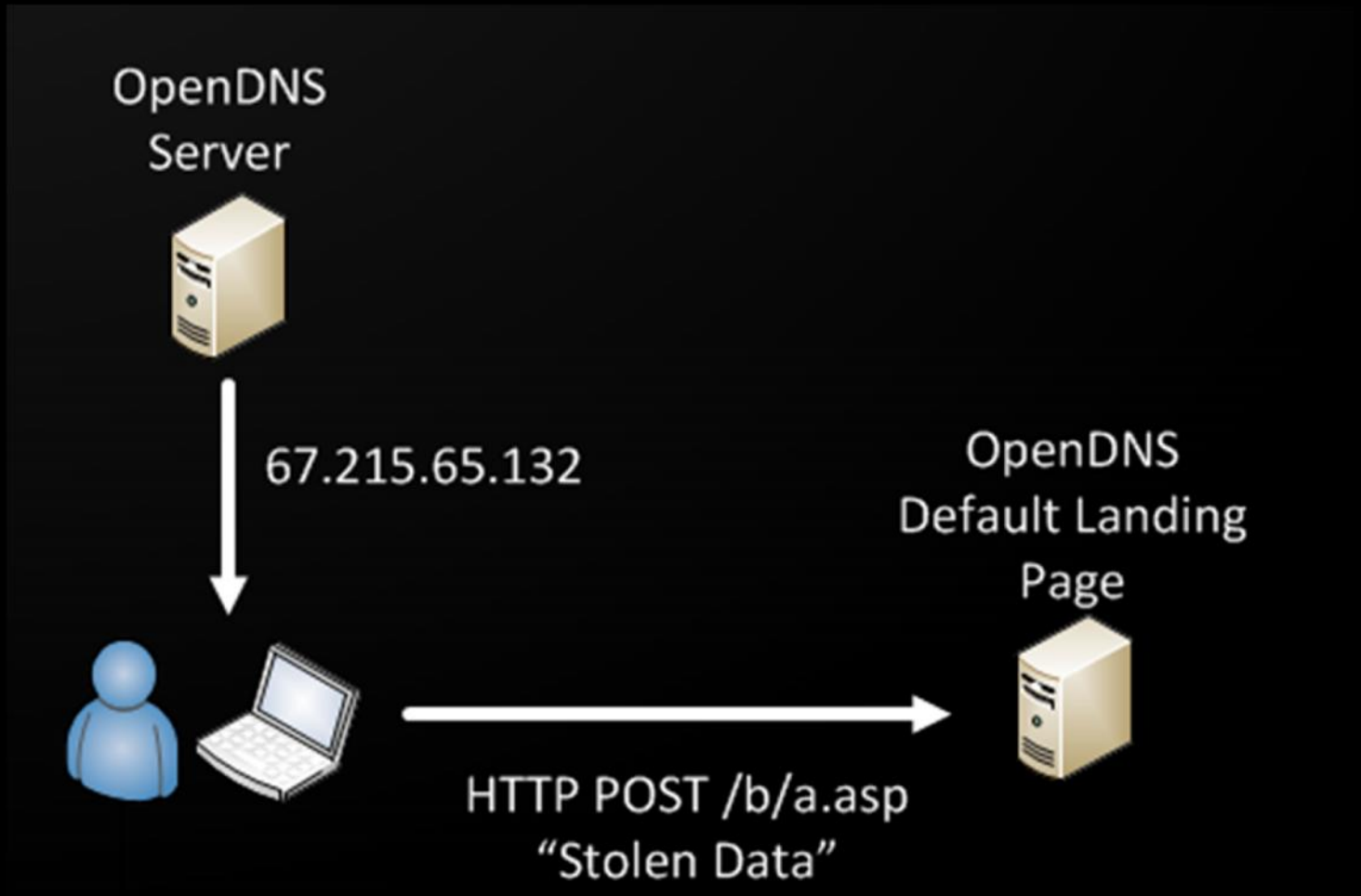
Abandoned Botnets and Forgotten Toys

NXDOMAIN Hijacking



Abandoned Botnets and Forgotten Toys

NXDOMAIN Hijacking



Abandoned Botnets and Forgotten Toys

Detection

- Collect your DNS logs into a database
- Regularly extract names being queried for the first time in your environment
- Look for names only being queried by a single client
- Look up the registration dates and owners
- Look for anything resolving to 127.0.0.1

Abandoned Botnets and Forgotten Toys

Resources

- Bro – http://www.bro.org
- DNS Anomaly Detection - http://code.google.com/p/security-onion/wiki/DNSAnomalyDetection
- Passive DNS - https://github.com/gamelinux/passivedns
- Response Policy Zones (RPZ)
- DNS Sinkholes - http://handlers.sans.edu/gbruneau/sinkhole.htm

Abandoned Botnets and Forgotten Toys

White Papers

- Passive Monitoring of DNS Anomalies

http://www.caida.org/publications/papers/2007/dns_anomalies/dns_anomalies.pdf

- Detecting Malware Domains at the Upper DNS Hierarchy

https://www.usenix.org/legacy/event/sec11/tech/full_papers/Antonakakis.pdf

- Mining DNS for Malicious Domain Registration

http://www.mcafee.com/us/resources/white-papers/wp-mining-dns-for-malicious-domain-regist.pdf

- Preprocessing DNS Log Data for Effective Data Mining

http://www.ccs.neu.edu/home/koods/papers/snyder09preprocessing.pdf

- Detecting Botnet Activities Based on Abnormal DNS Traffic

http://arxiv.org/pdf/0911.0487v1.pdf

Questions?

bobx@rot26.net

Please contact me with any questions, comments, or opportunities :)

Thank You!