Acknowledgements

• Dave Piscitello
  – Vice President, Security and ICT Coordination – ICANN
1. Brief Overview of DNS
2. Defining Badness in the DNS
3. Identifying Badness and Abuse Sources
4. Tools for Handling DNS Abuse or Misused Domains
5. Importance of WHOIS
6. Summary / Demo
Brief Overview of DNS
DNS Recap

• **A domain** is a node in the Internet name space
  – A domain includes all its descendants

• Domains have names
  – Top-level domain (TLD) names are generic or country-specific
  – TLD *registries* administer domains in the top-level
  – TLD registries *delegate* labels beneath their top level delegation

Names in generic Top Level Domains

<table>
<thead>
<tr>
<th>org</th>
<th>gov</th>
<th>com</th>
<th>AF</th>
<th>ZW</th>
</tr>
</thead>
<tbody>
<tr>
<td>icann</td>
<td>ncfta</td>
<td>irs</td>
<td>ftc</td>
<td>google</td>
</tr>
<tr>
<td>www</td>
<td>ssac</td>
<td>co</td>
<td>google</td>
<td></td>
</tr>
</tbody>
</table>
DNS Recap

- DNS is a distributed database
- Types of DNS servers
  - DNS Authoritative
    - Master
    - Slaves
  - DNS Resolver
    - Recursive
    - Cache
    - Stub resolver
Operational elements of the DNS

• Authoritative Name Servers host zone data
  – The set of “DNS data” that the registrant publishes

• Recursive Name Resolvers ("resolvers")
  – Systems that find answers to queries for DNS data

• Caching resolvers
  – Recursive resolvers that not only find answers but also store answers locally for “TTL” period of time

• Client or “stub” resolvers
  – Software in applications, mobile apps or operating systems that query the DNS and process responses
Domain name “directory assistance”

How does a resolver find the IP address of ICANN.ORG?

- Resolvers find answers by asking questions iteratively.

Ask root name servers for IPv6 address of ICANN.ORG

Ask a0.org.afilias-nst.info for IPv6 address of ICANN.ORG

Ask ns.icann.org for IPv6 address of ICANN.ORG

m.root-servers.net

Here’s a list of ORG TLD name servers. Ask one of these.

NS .org

Here’s a list of ICANN name servers. Ask one of these.

The IPv6 address of www.icann.org:
2001:500:88:200::7
How to register a domain:
- Choose a string e.g., example
- Visit a registrar to check string availability in a TLD
- Pay a fee to register the name
- Submit registration information
- Registrar and registries manage:
  - “string” + TLD (managed in registry DB)
  - Contacts, DNS (managed in Whois)
  - DNS, status (managed in Whois DBs)
  - Payment information
What is a DNS zone data?

- DNS zone data are hosted at an **authoritative name server**
  - Each “cut” has zone data (root, TLD, delegations)
- DNS zones contain **resource records that describe**
  - name servers,
  - IP addresses,
  - Hosts,
  - Services
  - Cryptographic keys & signatures...

Only US ASCII-7 letters, digits, and hyphens can be used as zone data.

In a zone, IDNs strings begin with XN--
Common DNS Resource Records

- **Time to live (TTL)**
  - How long RRs are accurate

- **Start of Authority (SOA) RR**
  - Source: zone created here
  - Administrator’s email
  - Revision number of zone file

- **Name Server (NS)**
  - IN (Internet)
  - Name of authoritative server

- **Mail Server (MX)**
  - IN (Internet)
  - Name of mail server

- **Sender Policy Framework (TXT)**
  - Authorized mail senders

```
$TTL 86400; 24 hours could have been written as 24h or 1d
$TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@ IN SOA ns1.example.com. hostmaster.example.com. ( 2002022401 ; serial 
3H ; refresh 
15 ; retry 
1w ; expire 
3h ; minimum 
)
IN NS ns1.example.com. ; NS in the domain bailiwick
IN NS ns2.smokeymcge.com. ; NS external to domain
IN MX 10 mail.another.com. ; external mail provider

; server host definitions
ns1 IN A 192.168.0.1 ; name server definition
www IN A 192.168.0.2 ; web server definition

; web and ftp server on same address
ftp IN CNAME www.example.com. ; ftp server definition

; endpoint or non server domain hosts
mikeslaptop IN A 192.168.0.3
fredsipad IN A 192.168.0.4
```
Common DNS Resource Records

$TTL 86400 ; 24 hours could have been written as 24h or 1d
$TTL used for all RRs without explicit TTL value
$ORIGIN example.com.
@ 1D IN SOA ns1.example.com. hostmaster.example.com. ( 2002022401 ; serial 
3H ; refresh 15 ; retry 1w ; expire 3h ; minimum 
)
IN NS ns1.example.com. ; NS in the domain bailiwick
IN NS ns2.smokejce.com. ; NS external to domain
IN MX 10 mail.another.com. ; external mail provider
;
; Sender policy framework with hard fail
; Use A and MX resource records for verification and google too
; example.com. IN TXT "v=spf1 a mx include:google.com -all"
;
; server host definitions
;
nsl IN A 192.168.0.1 ; name server definition
WWW IN A 192.168.0.2 ; web server definition
;
; web and ftp server on same address
; ftp IN CNAME www.example.com. ; ftp server definition
;
; endpoint or non server domain hosts
; mikeslaptop IN A 192.168.0.3
fredsipad IN A 192.168.0.4

Name server address record
- NS1 (name server name)
- IN (Internet)
- A (IPv4) * AAAA is IPv6
- IPv4 address (192.168.0.1)

Web server address record
- www (world wide web)
- IN (Internet)
- A (IPv4) * AAAA is IPv6
- IPv4 address (192.168.0.2)

File server address record
- FTP (file transfer protocol)
- IN (Internet)
- CNAME means “same address spaces and numbers as www”
Where can I get root zone data?

- IANA Root Zone Management
  - http://www.iana.org/domains/root/files
Registration Data Directory Services

Whois

Databases containing records of registrations

- **Domain Whois**
  - Sponsoring Registrar
  - Domain Name Servers
  - Domain Status
  - Creation/Expiry dates
  - Point of Contact
  - DNSSEC data

- **Address Whois**
  - Regional Internet Registry
  - IPv4/v6 address allocation
  - ASN allocation
  - Creation/Expiry dates
  - Point of Contact
Abuse investigations typically involve collection of most/all of these identifiers

- Domain Names
- Name Servers
- IP networks and addresses
- Autonomous Systems
- Registration data
Defining Badness in the DNS
Common Uses for Maliciously Registered Domains

- Counterfeit goods
- Data exfiltration
- Exploit attacks
- Illegal pharma
- Infrastructure (ecrime name resolution)
- Malware C&C
- Malware distribution (drive-by pages)
- Phishing
- Scams (419, reshipping, stranded traveler…)

[Images related to malicious domains]
Abuses of other peoples’ Domains & DNS

- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Tunneling (covert communications)
- Attack obfuscation
- Host file modification (infected devices)
- Changing default resolvers (DNSChanger)
- Poisoning (resolver/ISP)
- Man in the Middle attacks (insertion, capture)
How Abusers acquire DNS resources

- Purchase using stolen credit cards, compromised accounts
- Abuse “free” services
- Leverage bullet-proof or grey hat hosting/domain providers
- Hack and exploit legitimate hosts
- Phish registration account credentials and use to modify domain zone data or buy domains
Abuse (Malicious) Domain or a Misused (Exploited) Domain?

• *Not always easy to differentiate*
Collecting Evidence of DNS Abuse/Misuse

- Recent domain registration creation date
- Questionable Whois contact data
- Privacy protection service
- Suspicious values in DNS Zone data (e.g., TTL)
- Spoofing or confusing use of a brand
- Known DGA or malware control point
- Hosted on suspicious (notorious) name servers
- High frequency/volume of name errors
- Suspicious (notorious) hosting location
- Suspicious (notorious) service operator
- Base site content is non-existent or bad
- Linked content is suspicious or bad
- Suspicious mail headers, sender, or content
Not always easy to identify badness

- Abusers Use Obfuscation
  - Redirection: hacked sites use URL shorteners
  - Recursion: Shortened URLs are shortened
  - One-time use URLs
  - Add subdomains to zone at a hacked DNS server
  - Country- or script-specific content; non-visible content
  - Privacy-protected domain registrations or bogus Whois

- Abusers use ACLs
  - Prevent registrars, Google, LE, investigators from seeing sites
  - “Abuse” behaviors can emulate legitimate behavior
  - EXAMPLE: Fast flux versus adaptive networking (e.g., CDNs)
What is Fast Flux Hosting?

• An evasion technique

• Using fast flux hosting, an attacker
  – Hosts illegal content at a web site
  – Sends phishing email containing URLs that point to compromised computers he commands
  – Commands the compromised computers (proxies) to forward user requests to the attacker’s web site
  – Rapidly changes the IP addresses of the proxies to avoid detection and takedown

• Several variants
  – Double flux changes addresses of name servers as well as proxies
  – Domain names are key element of FF attacks
Steps to investigate & suspend domains

1. Collect evidence of abuse
   A. The purpose of this course is to show ways to do this
2. Determine registrar
   A. Is there a reseller of that registrar involved?
3. Contact registrar abuse desk
   A. Provide evidence of abuse
   B. Point out registration problems
   C. Ask if TOS, ICANN, ccTLD registry domain suspension policy applies
4. No success? Contact registry
   A. Same supporting info as registrar
5. Escalate
   A. Sharing/intel networks
   B. National CERT or local LE
   C. ICANN compliance

If you are looking at a suspicious domain, someone else is, too.
Collecting Evidence of Abuse/Misuse

- Domain names
- Name servers, resolvers
- DNS zone data
- DNS traffic
- Name registration data
- Registry
- Registrar

- Host IP addresses
- IP networks
- Address registration data
- Autonomous systems
- Service providers
- Hosting providers
- Content
Tools for Identifying Badness and Abuse Sources
Tools for Abuse Handlers

• Many tools to help you identify the abused or malicious resource
  – Domain names, host names, IP addresses, ASNs
  – Hosting location (web, DNS, mail) or origin
  – Content (URL, file, email, attachment)

• Many tools to identify whom to contact or report the resource
  – Databases of domain registrants, operators, ISPs
  – Block list and analysis sites and data providers

SAVE A COPY OF EVERYTHING YOU VISIT OR QUERY
WHOIS Database

• Internet Protocol you can use to search registry and registrar databases and discover who registered a domain name or IP address

• Includes contact information for registrant
A typical WHOIS entry

- Registrant name
- Street address
- Email
- Telephone number
- Creation date
- Expiration date
Why is WHOIS important?

• Helps network administrators find and fix system problems and maintain Internet stability
• Manages registration status of domain names
• Assists in fighting abusive use of Internet
Accuracy of WHOIS data is important

• WHOIS records are created when a domain name is registered
• Information changes over time and should be updated so that registrants can be easily contacted
• Inaccurate records can lead to the domain name’s cancellation
Who do I tell if WHOIS information is wrong or missing?

- Send complaint to ICANN about inaccurate or missing WHOIS data

What if I don’t want to share my personal information in the WHOIS database?

• ICANN requires all accredited registrars and registries to provide contact information for registrants and managers via WHOIS.

• Some registrars offer privacy or proxy services that show the contact information of the service instead of the registrant’s.

• These are not truly anonymous. A registrar may be legally compelled to release information in some cases or will voluntarily release information in accordance with its policies.
WHOIS may change dramatically in future

- An Expert Working Group has proposed a complete overhaul to how registrant information is provided to users.

- Next Generation gTLD Directory Services Model would streamline the way data is retrieved and validated.

- It would also help safeguard data against illegitimate uses.
Delegation Records for new TLDs

- [https://newgtlds.icann.org/newgtlds.csv](https://newgtlds.icann.org/newgtlds.csv)
Tools for Investigating DNS

- nslookup (Win), host
  http://support.microsoft.com/kb/200525

- dig (Linux, BSD, MacOS),
  https://library.linode.com/linux-tools/common-commands/dig

- Robtex
  http://www.robtex.com/dns/

- Passive DNS at BFK.DE
  http://www.bfk.de/bfk_dnslogger.html

- Passive DNS at DNSDB
  https://www.dnsdb.info/
Using dig (Linux, BSD)

Last login: Wed Aug  8 17:13:30 on console
Daves-MacBook-Pro:~ davepiscitello$ man dig
Daves-MacBook-Pro:~ davepiscitello$ dig icann.org

; <<<< DiG 9.8.1-P1 <<>> icann.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7037
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;icann.org.

;; ANSWER SECTION:
icann.org. 600 IN A 192.0.43.7

;; Query time: 67 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Aug 21 12:24:26 2012
;; MSG SIZE  rcvd: 43

Daves-MacBook-Pro:~ davepiscitello$
Using `dig` (Linux, BSD)

```
Daves-MacBook-Pro:~ davepiscitello$ dig -t MX icann.org +noquestion +nocomments +nostats

; <<>> DiG 9.8.1-P1 <<>> -t MX icann.org +noquestion +nocomments +nostats
;; global options: +cmd
icann.org.  536    IN    MX 10 pechora1.icann.org.
icann.org.  536    IN    MX 10 pechora2.icann.org.
icann.org.  536    IN    MX 10 pechora3.icann.org.
icann.org.  536    IN    MX 10 pechora4.icann.org.
icann.org.  536    IN    MX 10 pechora5.icann.org.
icann.org.  536    IN    MX 10 pechora6.icann.org.
icann.org.  536    IN    MX 10 pechora7.icann.org.
icann.org.  536    IN    MX 10 pechora8.icann.org.
Daves-MacBook-Pro:~ davepiscitello$
```

ask for mail servers

```
Daves-MacBook-Pro:~ davepiscitello$ dig -t NS icann.org +noquestion +nocomments +nostats

; <<>> DiG 9.8.1-P1 <<>> -t NS icann.org +noquestion +nocomments +nostats
;; global options: +cmd
icann.org.  22412  IN    NS  a.iana-servers.net.
icann.org.  22412  IN    NS  b.iana-servers.net.
icann.org.  22412  IN    NS  c.iana-servers.net.
icann.org.  22412  IN    NS  d.iana-servers.net.
icann.org.  22412  IN    NS  ns.icann.org.
Daves-MacBook-Pro:~ davepiscitello$
```

ask for name servers
Using `dig` (Linux, BSD)

```
Daves-MacBook-Pro:~ davepiscitello$ dig amazon.com txt

;; DiG 9.8.5-P1 <<>> amazon.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24679
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 2

;; QUESTION SECTION:
;amazon.com.

;; ANSWER SECTION:
amazon.com. 749 IN TXT "spf2.0/prf include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
amazon.com. 749 IN TXT "v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"

;; AUTHORITY SECTION:
amazon.com. 98561 IN NS pdns6.ultradns.co.uk.
amazon.com. 98561 IN NS pdns1.ultradns.net.

;; ADDITIONAL SECTION:
pdns1.ultradns.net. 87809 IN A 204.74.108.1
pdns1.ultradns.net. 87809 IN AAAA 2001:502:ff00:1

Query time: 82 msec
;; SERVER: 10.32.11.34#53(10.32.11.34)
;; WHEN: Mon Dec 08 10:48:45 EST 2014
;; MSG SIZE  rcvd: 413
```

```
Daves-MacBook-Pro:~ davepiscitello$ dig amazon.com txt +short
"v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
"spf2.0/prf include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all"
Daves-MacBook-Pro:~ davepiscitello$
```
Using nslookup

basic nslookup
ask for name servers
ask for IPv6 addresses
ask for mail servers

Also try:
“q=any”
“q=“txt”

Name system lookup
Passive DNS Replication (PDNS)

• **What does Passive DNS do?**
  – Shows query and response traffic, i.e.,
    • The DNS records clients are asking to resolve and
    • The Responses resolvers receives back from authoritative servers

• **How does Passive DNS work?**
  – Monitor DNS queries & responses (near recursive servers)
  – Put all of the data you monitor into a database

• **Query the database to extract behavior**

• **Best results at big ISPs**
  – Physical network location with visibility
  – Filter down to just the DNS queries/responses
Command line Whois

Windows Sysinternals

Linux, BSD have it:

Use `whois domain.tld > domainwhois.txt` to save output

Download for DOS here:

Web based Whois tools

- **Domain Tools**
- **http://domaintools.com**
- **Domain Dossier**
  - [http://centralops.net/co/DomainDossier.aspx](http://centralops.net/co/DomainDossier.aspx)
Identifying IPs and ASNs

Address Whois:
• AfriNIC.net
• APNIC.net
• ARIN.net
• LACNIC.net
• RIPE.net

• Shadowserver Whois

• Team Cymru
  – https://asn.cymru.com/

• Robtex (Share Tab)
  – http://robtex.com

• DNSSTuff
  http://www.dnsstuff.com
Reputation services, Block lists, Malware Analysis

<table>
<thead>
<tr>
<th>Reputation services</th>
<th>Block lists</th>
<th>Malware Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spamhaus</td>
<td>Google</td>
<td></td>
</tr>
<tr>
<td>SURBL</td>
<td>VirusTotal</td>
<td></td>
</tr>
<tr>
<td>ZeusTracker</td>
<td>Anubis</td>
<td></td>
</tr>
<tr>
<td>Team Cymru</td>
<td>ThreatExpert</td>
<td></td>
</tr>
<tr>
<td>Alexa</td>
<td>URLquery</td>
<td></td>
</tr>
<tr>
<td>Clean MX</td>
<td>SiteVet</td>
<td></td>
</tr>
<tr>
<td>CBL</td>
<td>Wepawet</td>
<td></td>
</tr>
<tr>
<td>Stopbadware</td>
<td>MalwareTracker</td>
<td></td>
</tr>
</tbody>
</table>
Reputation Services

- Organizations that classify
  - IP address allocations,
  - Domain names,
  - hosting providers,
  - ISPs,
- As legitimate or malicious using a scoring system

- URLQuery.net
- sitevet.com
- HOSTexploit.com
- Spamhaus.org
- ProjectHoneypot.org
- MalwareDomainList
I’ve got what I think is malware
  – How do I figure out if it’s a malware?
  – How do I figure out if it’s controlled via a domain or host?

• Malware analysis methodologies include:
  – Grab a sample: fingerprint files, dissect, disassemble…
  – Run wireshark to capture traffic
  – Catalog the IPs and ASNs of hosts exchanging traffic with my botted machine
  – Passively map DNS
  – Share what I find with other skilled white hats

• Not your day job? Consider publicly available tools

• Web based malware analysis tools
  – Virustotal, for malware analysis
    • http://www.virustotal.com
Summary

1. Brief Overview of DNS
2. Defining Badness in the DNS
3. Identifying Badness and Abuse Sources
4. Tools for Handling DNS Abuse or Misused Domains
5. Importance of WHOIS
6. Summary / Demo
Questions?
Thank You!

<champika.wijayatunga@icann.org>