Presenters

- Champika Wijayatunga (ICANN)
  - Regional SSR Engagement Manager – APAC
    champika.wijayatunga@icann.org

- Kitisak Jirawannakool (EGA – Thailand)
  - Information Security Specialist
    kitisak.jirawannakool@ega.or.th
Acknowledgements

• Dave Piscitello
  – VP – Security and ICT Coordination – ICANN

• Richard Lamb
  – Senior Program Manager – DNSSEC – ICANN
Agenda

1. Threats and Risks in DNS
2. Importance of DNS Security
3. Handling DNS Abuse
4. Tools, Techniques and Policy considerations
5. Case Studies and Use cases
6. Collaboration with ICANN
Threats and Risks in DNS
DNS Resolution Recap

- Client: 10.1.2.3
- Resolver (ISP): www.example.net.
- Root Server: a.server.net.

- Example.net nameserver: ns.example.net.
- Example.net nameserver: 5.6.7.8
- Example.net nameserver: 199.7.83.42
- Example.net nameserver: 2001:500:3::42
- Example.net nameserver: 1.2.3.4
- Example.net nameserver: a.server.net.

---

- Root Server: 1.root-servers.net.
- Root Server: l.root-servers.net.
Reflection and Amplification Attack

- Attacker sends DNS messages to recursor from spoofed IP address of target.
- Recursor sends LARGE responses to targeted host.
- Amplified responses delivered to targeted host consume resources faster.
Distributed Reflection & Amplification Attack (DDoS)

- Launch reflection and amplification attack from 1000s of origins
- Reflect through open recursor
- Deliver 1000s of large responses to target

All sources spoof source IP of target: 10.0.0.1
Targeted host IP: 10.0.0.1
Basic Cache Poisoning

Attacker

– Launches a spam campaign where spam message contains http://loseweightfastnow.com
– Attacker’s name server will respond to a DNS query for loseweightfastnow.com with malicious data about ebay.com
– Vulnerable resolvers add malicious data to local caches
– The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry

My Mac

What is the IPv4 address for loseweightfastnow.com

My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO www.ebay.com is at 192.168.1.2

I’ll cache this response… and update www.ebay.com

ecrime name server
Query Interception (DNS Hijacking)

- A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forged responses
  - Can be done using a DNS proxy, compromised access router or recursor, ARP poisoning, or evil twin Wifi access point

![Diagram showing the process of query interception through DNS hijacking.]

- Evil twin AP or compromised router redirects DNS queries to attacker’s name server
- Attacker’s resolver
- Attacker’s name server returns fake bank web site address
- Redirected path
- Intended path for online banking transactions
- Bank Web Site
- Fake Bank Web Site
Importance of DNS Security
DNS: Data Flow

1. Zone administrator
   - Zone file
2. Dynamic updates
   - Primary
3. Secondary
4. Caching Servers
5. Resolvers
DNS Vulnerabilities

- Corrupting data
  - Zone file
  - Zone administrator
  - Dynamic updates
  - Unauthorized updates

- Impersonating master
  - Primary
  - Secondary
  - Caching Servers
  - Resolver

- Cache impersonation
- Cache pollution by Data spoofing
- Altered zone data
- Data protection
- Server protection
Securing DNS

• There are two aspects when considering DNS Security
  – Server protection
  – Data protection

• Server protection
  – Protecting servers
    • Make sure your DNS servers are protected (i.e. physical security, latest DNS server software, proper security policies, Server redundancies etc.)
  – Protecting server transactions
    • Deployment of TSIG, ACLs etc. (To secure transactions against server impersonations, secure zone transfers, unauthorized updates etc.)

• Data protection
  – Authenticity and Integrity of Data
    • Deployment of DNSSEC (Protect DNS data against cache poisoning, cache impersonations, spoofing etc.)
How DNSSEC Works

Client  www.example.net.

Resolver (ISP)  www.example.net.

Root Server  a.server.net.

example.net nameserver  10.1.2.3

.example.net.?

.example.net.?

.example.net.?

.example.net.?

.example.net.?

.example.net.?
DNSSEC ccTLD Map

https://rick.eng.br/dnssecstat/
DNSSEC Deployment

% of TLDs signed in root

% of TLDs signed

Approx % of 2LDs signed

Trend

https://rick.eng.br/dnssecstat/
DNSSEC: So what’s the problem?

• Not enough IT departments know about it or are too busy putting out other security fires.

• When they do look into it they hear old stories of FUD and lack of turnkey solutions.

• Registrars*/DNS providers see no demand leading to “chicken-and-egg” problems.

  *but required by new ICANN registrar agreement
Handling DNS Abuse
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...)
Abuses of other peoples’ Domains & DNS

- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Host file modification (infected devices)
- Changing default resolvers (DNSChanger)
- Poisoning (resolver/ISP)
- Man in the Middle attacks (insertion, capture)
- etc.
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
Best practices in collecting evidences when handling DNS Abuse

- Be aware of questionable WHOIS contact data (Names and IP addresses)
- Check whether privacy protection service is involved
- Check for suspicious values in DNS Zone data
- Examine the spoofing or confusing use of a brand
- Check on the name servers? Are they suspicious?
- Check for hosting locations? Are they suspicious?
- Examine the Base site content? Is it non-existent or bad?
- What about the linked content? Is it suspicious or bad?
- Analyze the mail headers, sender, or content? Are they suspicious?
Pop Quiz
Tools, Techniques and Policy considerations to Handle DNS Abuse
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
How the policies and guidelines can assist?

• When collecting abuse related evidences

• Dealing with registrars, privacy protection services, registries etc.

• Acceptable Use Policies (AUP)

• WHOIS database data accuracy

• Dealing with National CERTs

• Dealing with Law Enforcement

• ICANN Compliance
Case Studies
Collaboration with ICANN to keep Internet Secure, Stable and Resilient
Collaborative Measures at ICANN

ICANN

- Network Operators
- CERTs
- Regional Internet Registries
- Domain Operators
- Law Enforcement
- Trust-based Collaboration
- Capability Building
- Identifier SSR Analytics
- Gov
Training and Outreach

- Security, operations, DNS/DNSSEC deployment training
  - for TLD registry operators
  - Network Operators / ISPs
  - Enterprises, Corporates etc.

- Information gathering to identify Internet Identifier Systems abuse/misuse and Investigation Techniques
  - Law Enforcement Agencies
  - CERTs
  - Internet Investigators etc.
Pop Quiz
Summary

1. Threats and Risks in DNS
2. Importance of DNS Security
3. Handling DNS Abuse
4. Tools, Techniques and Policy considerations
5. Case Studies and Use cases
6. Collaboration with ICANN
Thank You and Questions

Email: <champika.wijayatunga@icann.org>

Website: icann.org

twitter.com/icann
twitter.com/icann4biz
facebook.com/icannorg
linkedin.com/company/icann
youtube.com/user/icannnews
gplus.to/icann
weibo.com/ICANNorg
flickr.com/photos/icann
slideshare.net/icannpresentations