The Relationship of DDoS and Top Level Domain Name Registries

Edward Lewis
Neustar, Inc.
Presentation to the ccNSO Tech Day at ICANN 43
March 12, 2012

© Neustar, Inc.

neustar.

Threats to Registries

- Much has been made of DNSSEC and its contribution to securing the domain name system
  - But the role of DNSSEC is limited
  - And registries have a lot of other concerns
  - One is a class of attacks known as Distributed Denial of Service (DDoS)
- This presentation will cover DDoS attacks and the implications for registries

© Neustar, Inc.

Agenda

- What is a "DDoS" in a few words?
- How a DDoS attack might hit a registry?
- How a registry may become an unwitting participant?
- How a registry can play a role in issuing warnings?

© Neustar, Inc.

What is "DDoS"?

- Let's break this down a bit
  - DoS is denial of service
  - DDoS is a Distributed DoS
- Denial of service might mean "crashing the server/ application" or "block access to the server"
- Distributed DoS means doing a DoS from sources spread out over the Internet, making it harder to observe and stop
- The first "D" in DDoS makes addressing a DDoS much harder than a simple DoS

© Neustar, Inc.

Why can a DDoS exist?

- The Internet has two fundamental characteristics that allow DDoS attacks to exist
  - The use of client-server, where the server does more work than the client
    - E.g., the web, good old HTTP
  - The use of lightweight "send and forget" protocols
    - E.g., the User Datagram Protocol necessary for DNS to exist
- If the "fertile ground" for DDoS were engineered away, we'd kill the Internet

© Neustar, Inc.

Why does DDoS exist?

- Some interests are motivated to stop other interests
- Sometimes the motivation is money
  - Extortion
  - Enabling a "break-in" to steal other asset information
- Sometimes the motivation is an ideology
  - Anti-government protests
  - Protesting any other organization's decision
- There is much focus on motivation, but the answer to DDoS really isn't there. Understanding the motivation will help address the attack, but there will always be a motivation

© Neustar, Inc.

For registries...so what?

- Where are domain name registries, ccTLD and others exposed?
  - Public services like DNS, WhoIs (etc.), Registration
  - Business services like Web, eMail
- And there's one more "exposed surface"
  - Being "tuned" to what is happening "on the street"
- How are registries involved with a DDoS?
  - The victim, the target of the attack
  - An unwitting accomplice of the attack
  - A forecaster of attacks

© Neustar, Inc.

Narrowing this discussion

- The most exploited service of a domain name registry is the DNS
  - DDoS used to be primarily a web problem
  - Now increasingly a DNS problem
- Registries tend to be good at DNS and don't often show signs of being targets
  - Lots of capacity, anycast, monitoring

- But registries are "used" in DDoS, increasingly so
- And registry operators are more aware of DDoS activity than registrants

© Neustar, Inc.

If you are a target

- Simple - throw away the attack queries faster than they arrive
  - Hard - know what is an attack query
- There are many techniques to do this
  - Having capacity above peak loads
  - Anycast helps localize DDoS (most bots are regional)
  - Scrubbing, filtering packets that fit certain profiles
- Registries will do some of this on their own or outsource to DNS service providers that do

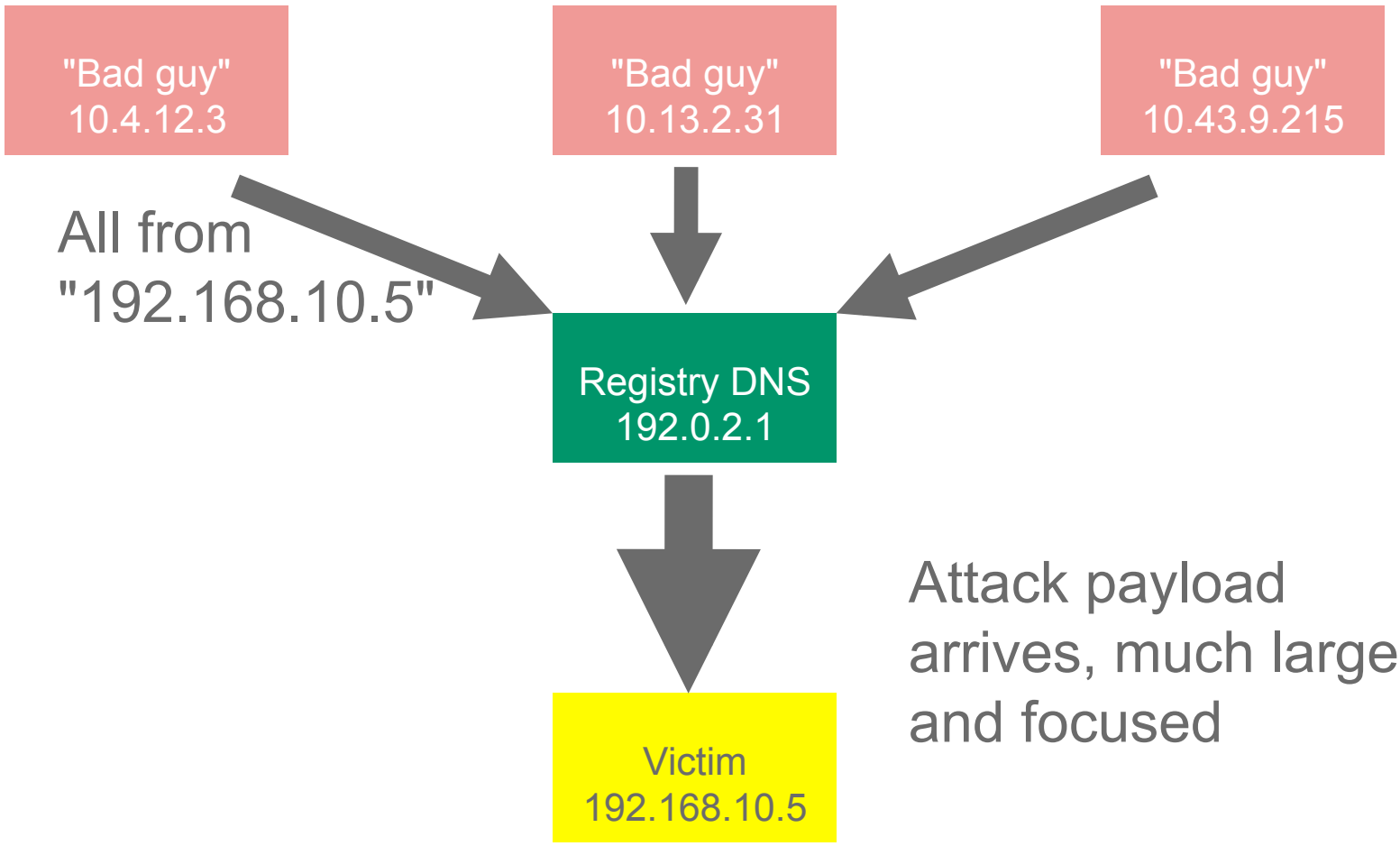
© Neustar, Inc.

Unwitting accomplices

- Reflection attacks work on the basis of
  - The malicious source sends a small query with a false return address
  - The DNS server responds with a larger response to the return address
  - The return address is the victim
- To the registry it seems that the victim is asking for this
- The paths into the registry are "D"istributed and therefore undetectable

© Neustar, Inc.

Reflection Attack



© Neustar, Inc.

An example

- One observed attack used queries for isc.org's information in bulk
  - Such a query is not that unusual
- A query might take about less than 24 bytes
- The full response is 3961 bytes
- The attacker sees the registry send 165 times as much data to the victim as the attacker ever sends
- This is not uniquely a registry problem, but registries are great places to get size amplifications like this

© Neustar, Inc.

The value of non-existence

- With DNSSEC, the size of a NXDOMAIN response is much larger than the query
  - A large amplification in bytes
- There are many non-existent names
  - In any registry, more don't exist than do
- With so many possible names to use
  - The protocol cannot distinguish between a true and a malicious query
- But in logging, you can see if a (falsified) source is "scanning" unallocated names

© Neustar, Inc.

What can a Registry do?

- First, be on the watch for this activity
  - Look for certain characteristics that identify the malicious traffic
  - This is increasingly difficult as attacks get better
- Second, filter traffic that is suspicious
  - Once identified, the attack may persist for some time
  - It helps to "scrub" it away, a term for filtering
- Third, remove filters when the attack stops
  - These attacks do end, or shift their target
  - Really want to limit false positives

© Neustar, Inc.

DDoS Forecasters

- Sometimes a registry will learn of future bad activity via their contacts
- When a registry tells the intended victim "watch out"
  - You might think the victim would be thankful
  - But, this has happened, the victim might be even more suspicious of the registry
- In this case, the registry might appear to be a blackmailer themselves!

© Neustar, Inc.

This has happened...

- A hacker group made plans to attack an organization and this was intercepted by security groups
- The local ccTLD learned of this not-so-closely held secret and tried to warn the target
- The some operating members of the target responded to the information with "and who are you?"
- The attack went ahead as planned

© Neustar, Inc.

What happened afterward

- The registry made greater efforts to "socialize" and gain the confidence of key elements in the local industry
  - This is more valuable than all the formalized, engineering-based security tools available

© Neustar, Inc.

Winding up

- Registries have a number of security headaches that are not solved by DNSSEC
- For DDoS, a registry is involved three ways
  - Victim, which can be treated through operational practices
  - Unwitting accomplice, which can be abated
  - Forecaster, "knowing" the state of the Internet
- The most important steps an registry can take, that are often overlooked
  - Monitor its operations (see if it is being scanned)
  - Develop out-of-band ties to appropriate entities (LE, gov, ...)

© Neustar, Inc.

Thanks for your time...

- Questions?
- My contact information: ed.lewis@neustar.biz

© Neustar, Inc.