Mitigating Cyber Crime with a DNS Emergency Alert System

OARC 2010 Prague Workshop

Rod Rasmussen
CTO, Internet Identity

ACTIVELY SECURING THE EXTENDED ENTERPRISE

The problem at hand

- Bad guys are catching on to vulnerabilities in the DNS
- Take-overs at registrars and DNS providers
- Baidu, Comcast, ICANN, Photobucket, Whois.com, Twitter…
- CheckFree hijacking injured 75% of US banks

TTL keeps attacks alive for days

The problem coming

- BGP exploits and other fun with routing/peering
- Criminals (and State actors?)
- Beijing i-root, Great Firewall leakage events
- Underground saw the reroute capabilities of the China telecom announcements
- Ability to poison DNS massively using reroutes

TTL keeps attacks alive for days

Net effect - events can last days

- After AUTH server is fixed, long TTLs mean ISPs/ resolvers can store bad values for hours/days without refreshing
- Affected organization has no way to know where the bad values persist or fix
- ISPs and enterprises exposing their users to potential harm well after the original incident handled

DNSSEC will help, but...

- TTL will still muck up the works
- Cache poisonings vs. auth take-overs - does this make a difference?
  - You bet! I can authenticate the DNSSEC to my poisoned values if I've p0wned you.
- How are people caching DNSSEC records? If I "poison" a caching server by intercepting the entire AUTH chain via BGP or other route hack, does DNSSEC gain me anything?

Solution: Cache flushing

- Contact ISPs to have them flush their caches
  - Who do I contact, do they trust me, how many ISPs are there?
  - What about all the enterprises out there?
- China told all their ISPs to set fixed entry for Baidu - it worked
- Scaling is difficult

Out-of-band DNS zones

- Third party publishes separate "real" DNS zones
- DNS resolvers consult trusted source files separately and prior to standard DNS resolution
- Typically require DNS platform hosting of the affected domains/hostnames - so not universal
- ISP has to install custom hardware and/or software
- Works well but with overhead

How about an alert system?

- Similar infrastructures exist in many fields
- Information is easy to act on, the issue today is getting it to the right people in a manner they can trust
- A well-scaled system can provide tremendous coverage to overcome the TTL affects

Goals for an alert system

- Main Goal: Organizations that have their DNS hijacked (or screw it up badly on their own) with long TTLs need to have all resolvers/caches drop the old values and use the corrected ones - very quickly.
- Needs to scale
- Easy to request a fix
- Needs to be secure - vetted inputs

Signs are already positive

- I've been socializing this idea for around a year with some of the major ISPs - definite interest
- Enterprises are starting to ask about how to react with all that's gone on of late - starting to realize they're currently exposed
- Some large enterprise customers realizing they have the same exposure ISPs do - their employees can be exposed if they don't flush/fix

How to implement?

- Central clearing house?
- Protocols and trusted signatures?
- Alert posting system - RSS? website? DNS server?
- Alert then pick-up info? Push info? Post info for automatic collection?

A role for DNS-OARC?

- Or someone else?

Discussion

Mitigating Cyber Crime with a DNS Emergency Alert System

OARC 2010 Prague Workshop

Rod Rasmussen
CTO, Internet Identity
rod.rasmussen@internetidentity.com

ACTIVELY SECURING THE EXTENDED ENTERPRISE