

PacNOG 10

Nouméa - New Caledonia

Nov 21, 2011

ccTLD security



These materials are licensed under the Creative Commons *Attribution-NonCommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Overview

- ccTLDs operate DNS infrastructure (but not only!)
- Fundamentally not more complicated than most other DNS operations
- But there is **added responsibility** in being at the apex
 - If they fail in some way, many are affected
- Need for reliable infrastructure AND data integrity
 - Doesn't help to have stable DNS serving bogus data

Overview (2)

- Multiple areas of focus
 - Operational stability
 - Data security & integrity
 - Redundancy & diversity

Risk areas - Accidents

- Server crashes
- Loss of backup
 - backup seems to work
 - ... but did you **actually** test restore ?
- Natural disasters
- All of the above point to one thing
 - No disaster recovery / continuity planning !

Risk areas – Combined factors

- Accidents induced by application weaknesses
 - Insufficient error checking
 - Insufficient validation (invalid DNS data)
- This has hit well known, well run TLDs with many years of operational experience :
 - .DE incident (undetected out-of-diskspace condition)
 - .SE incident (missing dot after a name – a classic DNS manual error!)


Risk areas – Targeted attacks

- Denial of Service
- Exploiting application weaknesses
 - Insufficient data validation
 - Buffer overflows, SQL injections
 - Bugs
- Social engineering attacks
 - Pretend to be an employee to a customer
 - ... or vice versa
 - « Hello, I'm Mr. Smith, I called you yesterday... »

Attacks : why are ccTLDs targets ?

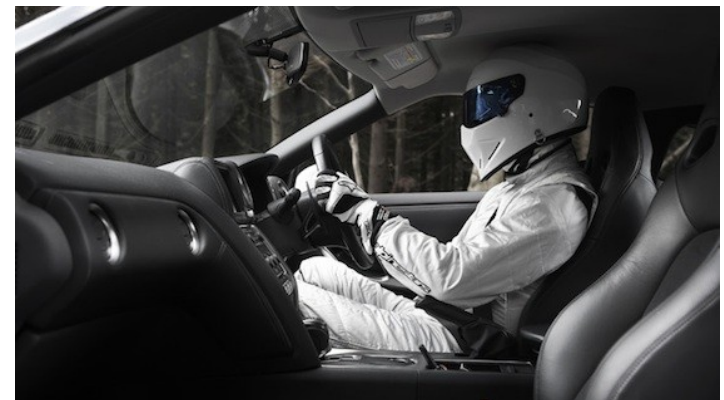
- Various reasons...
- Business (underground economy) :
 - New domains to send spam/malware / mount attacks from
 - So called fast flux networks
 - Conficker worm
 - Extortion via DoS or redirections as a business model
 - « We'll take down your domain if you don't pay »
 - Social engineering
 - Impersonation to gain privileges
 - Espionage – man in the middle : intercept & relay

Attacks : why are ccTLDs targets ?

- Social
 - Revenge
 - Vandalism / political activism (protesting, political hacking)
 - Showing off
 - Teenagers with too much testosterone
 - Also known as a  contest
 - Often manifested as « defacement »
 - « Yo d4wg, I 0wn3d your site – I rul3z »
 - <http://www.zone-h.org/archive/notifier=TiGER-M@TE/page=1>
 - <http://www.zone-h.org/archive/notifier=turkguvenligi.info/page=1>

Risk areas - Mitigation

- Note that security doesn't only mean « hackers »
- Data security – backup ?
- Data integrity – change management, verification of the output
- Think «airbag, seatbelt and crash helmet»
 - Need to protect against attacks, accidents, and incompetence



Mitigating these risks

- A combination of operational best practices :
 - Service availability
 - Geographical and software diversity
 - Redundancy (multiple DNS servers, Anycast)
 - Data integrity & protection
 - Backups
 - Verifications
- Need to implement monitoring to detect problems early on !
 - Preferably **before** your users find out
 - ... or the press

Best practices

- Keep configurations and zone files under revision control
 - Or maintain a transaction log
- Generate, don't edit zone files by hand
 - DB backends, automated zone edition and validation
 - Multiple existing free solutions for this nowadays
- Monitoring your zones, periodically
 - Many tools for this, including Nagios, DSC, Smokeping

Best practices (2)

- Diversify OS and software
 - BIND, NSD
- Log monitoring
 - Keep an eye on what your services are telling you !
- Arrange for off-site backup of your data
- Make sure you have geographically diverse DNS secondaries
 - Haiti (.HT)
 - Thailand (.TH)
- Have a disaster recovery plan
 - What happens when everything fails ?



Questions?

Thank you

Reference

- <http://www.icann.org/en/topics/ssr/dns-ncsirt-survey-results-22dec10-en.pdf>
- <http://www.securityweek.com/content/reports-massive-dns-outages-germany>
- <http://news.softpedia.com/news/Secure-SE-Zone-Goes-Down-Due-to-Missing-Dot-124268.shtml>
- <http://operations.afnic.fr/en/2011/02/18/study-and-action-plan-following-the-incident-with-validating-resolvers-on-12-february-2011.html>
- <http://www.internetblog.org.uk/post/890/ht-domain-still-operational-after-earthquake/>
- <http://www.aptdld.org/pdf/DNS%20Operational%20Guidelines%20White%20Paper%20-%20Version%201.1.pdf>
- <http://aptdld.org/ADRP/files/ACRP-Cyber%20Threats.pdf>
- <http://brussels38.icann.org/meetings/brussels2010/presentation-ccnso-tech-day-secure-cctld-registry-bartosiewicz-21jun10-en.pdf>
- <https://www.icann.org/en/security/sa-2009-0001.htm>
- <http://www.credentia.cc/research/dns/cctlds/report-2003-Oct.html>