Wild Card Report
(Redirection in the COM and NET Domains)

Steve Crocker, Jaap Akkerhuis

SSAC

July 21, 2004

www.icann.org/committees/security/ssac-report 09jul04.pdf

SSAC: Security and Stability Advisory Committee

- An advisory committee to the ICANN board
- Volunteers individual, technically competent, unpaid
- SSAC operates semi-independently
  - Does not speak for ICANN
  - Focuses on security and stability, not politics or contracts

Background

- 15 Sept 2003 VeriSign changed COM and NET domain registries
- Queries of uninstantiated names usually typographical mistakes were redirected to VeriSign s servers instead of receiving the standard error code.
- Community response was swift and vocal
- VeriSign suspended the change
- SSAC held meetings in October

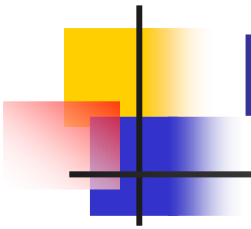
Findings 1-4

VeriSign changed the registry; caused harm

The Change violated engineering principles, blurred architectural layers

VeriSign s Change put itself in the loop for all current and future protocol changes

The Change was abrupt despite long internal development



Findings 5-8

- Quick reactions yielded more changes and counterpatches
- Email senders and receivers were ingested into VeriSign servers
- Web redirection program collected information associated with users
- The collective events reduced trust overall

Recommendations

No new wild cards in TLDs

Roll back wild cards in existing TLDs

Clean up specs

Enforce proper discipline, including open notice and consensus, for registry changes

Counter Measures

- Delegation only
  - Assumption
    - All TLDs only delegate
    - Block in-zone Authoritative answers
    - Few exceptions documented
      - DE, LV, US, MUSEUM
  - Worked, but ...

Delegation only

- Who still runs the hack?
- Why?

Problems

- TLD name server changes
  - name compression, IPV6 support
    - a.ns.se, b.ns.se etc.
- TLDs name servers ***not*** delegation only
- breaks end to end model
- Other various tricks with nameservers

(More) Questions???