Measures to Protect (University) Domain Registrations and DNS Against Attacks

Dave Piscitello, ICANN
dave.piscitello@icann.org
Why are we talking about...

Domain names and DNS?

- Domain names and URLs define your Internet presence
  - If the DNS does not resolve your domain, visitors can’t find you
  - If the DNS is subverted, visitors are at mercy of criminals or other bad actors
- These are not solely attacks against DNS
  - Similar outcomes if attackers compromise domain registration accounts
Criminals Need Domain Names

Criminals register new domains for

- Spam relays
- Hosting domains for “ecrime DNS” and fast flux proxies
- Phishing and malware hosting sites

Criminals seek legitimately registered domains for redirection and phishing

- These are harder to suspend

Other threats

- Domain name hijacking
- Squatting
Threat Landscape:
Domain Name Registrations

• Unauthorized access to registration accounts
• Unauthorized domain transfer
• Malicious or unintentional alteration of NS info
• Malicious alteration of contact information
• Renewal issues (lapses)
• “Rightful” registrant issues
Threat Landscape: DNS

Protocol threats
- Cache poisoning attacks
- Denial of Service attacks
- DNS response rewrites
- DNS hijacking
- DNS Blocking
- Operator threats

DNS hosting
- Unauthorized access
- Malicious/unintentional alteration of zone data
- Technical/business failure
Take Inventory

- What domain names has your institution registered?
  - Do affiliated parties use your “brand”?
- Which registries? Which registrars? Who is hosting DNS?
  - Do you know how to contact these operators?
- Who is the recognized registrant?
- What information is used for points of contact (registrant, tech, admin)?
- When do registrations expire? Hosting contracts?

How confident are you that you have a complete and accurate understanding of your portfolio?
Manage DNS

- Document your DNS architecture and operations.
- Design for resiliency.
- Harden name server infrastructure
- Actively manage DNS information.
- Protect domain registration and hosting accounts against attack.
- Develop a continuity plan.
- Plan carefully, provision accordingly.
Manage Domain Registrations

- Protect account credentials
- Use registrar correspondence to trigger internal checks and actions
- Maintain proof of ownership
- Manage (diversify) identities used as points of contact
- Implement change controls
- Maintain accurate external points of contact
Proactively Monitor DNS

- Track operational statistics and trends.
- Routinely query your authoritative name servers
  - Are all name servers operational?
  - Do all name servers return complete and correct zone information?
- Develop response plan and escalation procedures for exception conditions
Proactively Monitor Domain Registrations

- Use WHOIS proactively
  - Maintain copies of WHOIS records for your domains
  - Routinely query WHOIS for all domains to detect change activity
- Develop response plan and escalation procedures for reporting and recovery
Continuity considerations

- Build diversity into DNS hosting
- Implement a zone retrieval and archival process
- Develop contingency plans for all business disruption scenarios
  - Internal DNS operations
  - Outsourced DNS operations
  - Registration services
  - Maintain proof of ownership
  - Maintain accurate external points of contact
Make informed decisions

Questions to ask prospective registrars

• Account management features
• Correspondence
• Security measures
• Reputation, track history, references
Make informed choices

Questions to ask DNS Hosting Providers

• How are zone data managed?
• Hosting footprint (sites, geography)?
• Capacity?
• Security measures?
• Monitoring? Can I integrate with my own?
• Communication: reports, alerts, alarms?
• Service level agreements?
Questions?
The following photos were used under a Creative Commons non-commercial attribution license:

- Slide 2: CyboRoZ, ToastyKen
- Slide 3: Alan Cleaver
- Slide 4, Andrea Pipa.
- Slide 5, RaGardner4
- Slide 6, Fernando Gregory
- Slide 7, checklist_pjguyton
- Slide 8, problem_Lst1984
- Slide 9, 10, fioze
- Slide 11, Derek Gates

Photo Credits