Update on DNS hijackings

Maarten Van Horenbeeck
Security Program Manager
Google, Inc
Chronology

2010
Uganda, Puerto Rico, Denmark

2011
Suriname, Malawi, Congo, Guadeloupe, Fiji, Bangladesh

2012
Nepal, Iran, Turkey, Thailand, Guadeloupe, Ireland, Algeria, Pakistan, Romania, Serbia, Indonesia

2013
Uganda, Morocco, Saint Helena, Kyrgyzstan, Turkmenistan, Malawi, Fiji, Kenya, Bosnia and Herzegovina, Oman, Malaysia
Impact

The impact of these incidents is that **all domains** can be subverted and redirected to a server of the attacker's choosing:

Potential goals of the attacker:

- Defacement and reputation loss
- HTTP authentication token theft
- Hosting of exploit kits; botnet creation

Impact of a hijack is difficult to assess. An apparent defacement may still lead to theft of authentication tokens.
Kankalarım hep yanında arkadaş içinde
Yanimda ölmeyen mı var geçmişlik her nefeste

Pakistan Downed

trabzon 2012
Dostlara seslen artık hala yaşyoruz?
Google AND Yahoo! hijacked in Ireland after domain namespace grab

Human error or something more sinister?

By Kelly Fiveash, Networks Correspondent, 10th October 2012

Customer Success Testimonial: Recovery is Everything

Google and Yahoo!'s Irish domains were briefly hijacked on Tuesday afternoon, the IE Domain Registry (IEDR) has confirmed.
Recovery

Various complexities:

- Hijacks often happen after the end of the business day
- Average time to address an issue often 6+ hours
- Registry's first focus is often to protect additional domains
  - No response plan to recover existing users
  - Restoring previous settings is error-prone
- Once recovered, clients and intermediate service providers will cache the poisoned results

- Not always clear when incident is contained
  - Several registries have been hijacked more than once
  - Recently hijacked registries are visible targets
Top issues: (1) authorization schema

- Attacker creates account
- Attacker logs in, id value is carried forward in requests
- Attacker changes ID value, gains access to additional resources, e.g. the account of another registrar

```
GET /changeregistration.php?u=user123?domain=example.com
Session-ID: 3f0830bc30989de
```

Mitigations:

- Configure appropriate roles and privileges for each domain-name
- Ensure the access control mechanism is enforced when a new domain is being accessed
Top issues: (2) SQL Injection

The attacker is able to execute database queries allowing him to modify attributes of a domain name.

GET /query.php?name=google.com'; UPDATE nameserver SET ns='rogueserver.example.com' WHERE name='example.com''

SELECT * FROM domainnames WHERE name = 'google.com'; UPDATE nameserver SET ns='rogueserver.example.com' WHERE name='example.com';

Mitigations:

- Sanitize information from external sources
- Use prepared statements or stored procedures
- Deploy a web application firewall (mod_security, ...
Top issues: (3) registrar account compromise

Attacker attempts to authenticate using a list of frequent passwords, or using password stolen from another registry authentication database.

Mitigations:

- Properly hash passwords using a salt value
- Two factor authentication
- IP address restrictions for registrar accounts
- Lock out accounts after unsuccessful authentication
- Implement password strength requirements
Recommendations

- Deploy **registry lock** as an option for domain names
  - Disables modification of high value domain names without a specific outside protocol in place
  - Helps protect against registry portal compromises

- Provide **emergency contact information** to registrars and high traffic domain names
- Send **notification e-mails** to registrant, admin and registrar when a domain name is modified
- Consider **high traffic domains** useful canaries
Recommendations

- Develop a security management framework for the registry, which includes at minimum:
  - Selection of supported software for registry operations
  - Regular third party security testing
  - Develop a proper understanding of the weaknesses of the infrastructure, and ensure these weaknesses are tracked and remediated
  - Develop an incident response plan.
- Reach out to your local Computer Security Incident Response Team, and partner with them on understanding the threat environment
Thank You
(and we're here to help!)

Maarten Van Horenbeeck
Security Program Manager
Google, Inc

maartenvh@google.com