



# Registrar Phishing Threat

Nov 3, 2008

# SSAC Reports on Registrant Protection

- SAC 007 – Domain Name Hijacking Report (2005)
- SAC 010 – Renewal Considerations for Domain Name Registrants (2006)
- SAC 011 – Problems Caused By Non-Renewal of a Domain Name associated with a DNS Name Server (2006)
- SAC 024 – Domain Name Front Running (2008)
- SAC 025 – Fast Flux Hosting & DNS (2008)
- SAC 028 - Registrar Impersonation Phishing Attacks (2008)

# Recent Phishing Attacks aimed at Registrars

- Oct 29, 2008:
  - Network Solutions Reports Large-scale phishing attacks
  - ENOM targeted in a phishing attack
  - Moniker targeted in a phishing attack
- Oct 30, 2008:
  - Registrars, Registries take concerted action to take down most of the identified phishing domains

# Content of Network Solutions Lure

- Email Subject Line: “Attention: domain will be expired soon”
- Email Body says: “Renew your domain now”
- Link says <http://www.networksolutions.com> but actually points to <http://www.networksolutions.com.com42.asia>

Source: <http://blog.networksolutions.com/2008/phishing-alert-please-watch-for-this-email/>

# Content of ENOM Lure

- From : [support@enom.com](mailto:support@enom.com)
- Subject Line: Warning: Inaccurate whois information
- Message Body: “PLEASE VERIFY YOUR CONTACT INFORMATION”
- Link says <http://www.enom.com> but actually points to <http://www.enom.com.com62.biz>

# What Happens When You Click The Links

- Takes you to a fake site, dressed up to look like the actual registrar
- Requires you to type in  
UserName/Password combination
- Returns error code, and (in some instances) asks for more identifying information

**Effect: Compromised Domain Accounts**

# Recommendations for Registrars & Resellers

- Upgrade Registrant & Reseller account access methods
  - Consider two-factor authentication
  - Create a “3 strikes & locked out” systems
- Create an emergency action channel
  - 24x7 ability to provide intervention
- Acquire emergency contact information and validation criteria for Registrants
- Consider implementing digital signatures for your emails

# Recommendations for Registrars & Resellers (cont.)

- Train Support staff on dealing with Social Engineering efforts
- Define & communicate procedures for restoring Compromised Domain Accounts
- Implement suggestions in SSAC “[Registrar Impersonation Phishing Attacks](#)” and APWG’s “[Anti-Phishing Best Practices](#)” report

[http://www.antiphishing.org/reports/APWG\\_RegistrarBestPractices.pdf](http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf)

# Recommendations for Domain Registrants

- Do not click on web site links in your email – instead type in the web site address in your browser
- Ensure your email software can automatically identify phishing links
- Ensure that registrar website is protected by SSL (lock icon in your browser)



# Recommendations for Domain Registrants (cont.)

- Do not store your credit card information at your registrar or reseller
- Identify your “Mission Critical Domains” – names that would seriously harm you or your business if you lost them or your access to them – and protect them
  - Renew ahead of time
  - Ask your Registrar to LOCK these domains for you
- Select a reputable registrar or reseller

# Summary

Phishing is not new, but the impact of losing your domain registration account can be devastating

Exercise care in the registration and renewal of domain names

Exercise care in disclosing access credentials to your registrar or reseller accounts