Agenda

- About SGNIC
- Types of Abuse
- Measures (AMS)
- Statistics and Experiences (AMS)
- Conclusion
About Us

- SGNIC - National domain name (.sg) registry for Singapore
- Wholly-owned subsidiary of IDA Infocomm Development Authority of Singapore
- Interact with external organizations (ICANN, IANA, APTLD, ccTLDs, APNIC, SingCert, APWG, etc)
- ~155,000 .SG domain names (in Dec 2013)
- ~7% annual increase
About Us

- 10 employees (3 technical)
- Shared Registry-Registrar System – SGR2R
  - Outsourced service
  - HA setup (x2 servers for critical applications, RAID 1, Redundant Power, Load Balancer, etc.)
  - Solaris and Linux Operating System
  - SPARC and Intel CPU
  - Java Web Application, Oracle Database
  - ~10 servers (will soon be virtualized to 3, 1 for DR)
- Monitoring Systems + NOC (SGR2R vendor and in-house)
  - Monitor uptime, performance and incident correlation.
- 4 secondary nameservers
Types of Abuse

- Abuses that SGNIC is concerned about
- In some areas we feel more effective measures can be done

Registration Abuse
- Objectionable Domain Names
- Sale of Domain Names
- Identity Theft or Fake Identity
- Registration in Wrong Category
- Incomplete or Incorrect registration details

Usage Abuse
- Cybersquatting
- Pornographic
- Copyright violations
- Scam
- Spam
- Malware
- Phishing
- Socially or politically sensitive
- Fake Drugs
Measure #1 - Detection and Tracking

- Abuse Management System (AMS)
  - Software developed in-house
  - LAMP stack (Linux, Apache, MySQL, PHP)
  - Operational in 2011 (after 3-4 months of development)
  - Detects and tracks some domain name abuses (e.g. malware/phishing, incorrect/suspicious registration information, bulk registration, DNS wildcard usage)
  - Provides statistics for tracking and to better understand the nature of some abuses.
Detection and Tracking

- Automated scanning of domain name against third party website scanner / reputation databases for malware distribution/phishing activities.
- Manual verification of flagged domains to confirm abuses.
- Send notification and continuous reminder to community (i.e. Registrant, Admin, Hosting Provider) for confirmed cases.
Detection and Tracking

- AMS operations view
- Lists relevant information on suspicious domains

<table>
<thead>
<tr>
<th>Domain name</th>
<th>Status</th>
<th>Application or System Used</th>
<th>Type of Attack</th>
<th>Third-party results</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com.sg</td>
<td>Malwarephishing checked - possible abuse (OPEN)</td>
<td>Application: ... Running on: Apache</td>
<td>HTTP request attack details</td>
<td>Clean (01-Feb-2014 01:42:58)</td>
</tr>
</tbody>
</table>
Detection and Tracking

- Providing inaccurate registration information is often a precursor to domain abuse
- Provides early warning by checking the accuracy and completeness of new registrant information
  - E.g. Checks for address completeness based on postal code
Detection and Tracking

ACRA Database
(registry of companies)

ABC Pte Ltd [Com No.: 200709805A]
79, ROBINSON RD, ABC BUILDING #03-00
Singapore 111111
+65.22223333
buy@abccompany.sg

Postal code
Database

“Postal code” must be valid
“Address” must be 70% ‘similar’ with
Singapore phone number must start with ‘2’, ‘3’, ‘8’ or ‘9’.
Highlight if it looks fake:
+65.2221234 +65.98765432

Does email contain ‘suspicious’ words? (e.g. ‘buy’, ‘sale’)
Detection and Tracking

- Checks suspicious registrations in bulk registrations (i.e. from same registrant, email, telephone number).
  - e.g.
    - > 10 domains (all different registrant name) using same email in 1 day
    - > 50 domains (all different registrant name) using same email in 30 days

Example of cases detected:

<table>
<thead>
<tr>
<th>Bulk Registration Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BR4-1</td>
<td>66 registrations in 30 days using the email <a href="mailto:ben.xxx@hotmail.com">ben.xxx@hotmail.com</a>.</td>
</tr>
<tr>
<td>BR4-2</td>
<td>54 registrations in 30 days using the phone no. +65.9872XXXX</td>
</tr>
</tbody>
</table>
Detection and Tracking

- AMS continually monitors all domain names
  - All new names are scanned weekly for 3 months, then monthly scans
- Abuse statistics (in Jan 2014)
  - \(~156,000\) - Domain names scanned by AMS
  - \(~30\) – confirmed abuses per month
Detection and Tracking

- AMS gathers data over time
  - Attacks found on abused websites
  - Applications found on abused websites (usually plugins are insecure rather than the application)

![Pie charts showing the distribution of attacks and applications found on abused websites.]

**Attacks found on abused websites**
- Javascript Injection: 64%
- iFrame Injection: 22%
- .htaccess (or Backdoor conditional) redirect: 9%
- Others: 2%
- Others: 3%

**Applications found on abused websites**
- Uncategorized: 76%
- Wordpress: 14%
- Others: 2%
- Zen Cart: <1%
- ECShop: <1%
- Drupal: <1%
- OpenX: <1%
- OsCommerce: 1%
- Microsoft: 2%
- Joomla: 5%
Measure #2 - Enforcement

- Actively enforce against all other types of abuses.
- For malware and phishing:
  - “Time is of the essence” hence it's critical to send quick and timely advices to parties who may be involved (ISP, website hosting provider, registrant, admin and tech contact) for them to take action
  - Formalised collaboration with SingCERT who can provide expert opinion
  - For serious breaches: suspend or delete based on violations from registrant agreement
Success Stories

- In July 2012, a vulnerability in a popular web hosting panel was found.
  - Multiple .sg websites were affected
  - Contacted hosting provider to patch the vulnerability
  - Affected websites were cleaned
- Shorten the life of malicious domains on the internet
- ~80% resolution rate per month.
Challenges

- “Conditional redirects/.htaccess” malware
  - It only works based on certain conditions (i.e., Search engine based, IP-based, etc.)
  - Registrants and hosting providers are unaware of this hence they think it’s a false detection.

- Some miscommunication…
  - SGNIC notified registrant and hosting provider
  - Hours after, hosting provider has acted but did not update SGNIC
  - Then registrant checks the issue and thinks its false-positive
Conclusion

- Be more proactive and informed, time is of the essence
  - More sources for more detection, work with local CERT for expert opinion, continuous reminders

- Registrant’s domain name is critical to their business
  - Be mindful of your actions (e.g. domain suspension)

- Most registrants and hosting providers are keen to work with us

- Our efforts only help mitigate some abuses and may not solve the real issue which is to prevent abuse….

- But… at the end of the day, everyone seems to be happy with our efforts of taking harm away from the Internet
Any Questions?

Thank you!

Mon-Loi Perez