Understanding the Domain Registration Behavior of Spammers

Shuang Hao, Matthew Thomas, Vern Paxson, Nick Feamster, Christian Kreibich, Chris Grier, Scott Hollenbeck
Domain Abuse

- Domain names represent valuable Internet resources

- Domain abuse
  - Spam contains URLs leading to scam sites

Hello, By visiting this site you can decide any watch that you like http://www.bad-domain.com/qjkx

- Top-level domain name: com
- Second-level domain name: bad-domain.com
- Host name: www.bad-domain.com
Spammers Exploit Domains

- More agile and reliable for attacks
  - Domain space is very big
  - Domain cost is small
  - Not easy to detect
Motivation: Early Detection

- Most research focuses on activities after spam is sent

**Problem**: Window left for spam dissemination and monetization

- **Ultimate goal**: Detect spammer domains at *time-of-registration* rather than later at *time-of-use*
Talk Outline

• Motivation

• *Registration Process and Data Collection*

• DNS Infrastructure Used for Spammer Domains

• Detecting Registration Spikes

• Domain Life-cycle Role Analysis

• Summary
Domain Registration Process

Registry (e.g., Verisign) manages registration database

Registrar (e.g., GoDaddy) brokers registrations

Registrant

Top-level nameservers

Update
Background

Life Cycle Chart

- **Active (1-10 years)**
- **Auto-Renew Grace (45 days)**
- **Redemption Grace (30 days)**
- **Pending Delete (5 days)**

**Renew**

**Available**

**Re-registration**
Data Collection

1. What domains newly registered in .com zone
2. Whether the domains were used in spamming activities after registration
Verisign .com domain registrations over 5 months
  – Epoch: Zone file updates every 5 minutes
  – Registration information
    • Registrars
    • Nameservers
    • Registration history

Spammer domains
  – 134,455 new .com domains were blacklisted later
  – Spam trap, URIBL, and SURBL during March – October, 2012 (8 months)
Talk Outline

- Motivation
- Registration Process and Data Collection
  - DNS Infrastructure Used for Spammer Domains
    - Registrars and Authoritative Nameservers
- Detecting Registration Spikes
- Domain Life-cycle Role Analysis
- Conclusion
Registrars Hosting Spammer Domains

**Question**: What registrars do spammers choose to register domains?

The registrars ranked by the percentages of spammer domains:

<table>
<thead>
<tr>
<th>Registrar</th>
<th>Spam %</th>
</tr>
</thead>
<tbody>
<tr>
<td>eNom, Inc.</td>
<td>27.03%</td>
</tr>
<tr>
<td>Moniker Online Services, Inc.</td>
<td>19.01%</td>
</tr>
<tr>
<td>Tucows.com Co.</td>
<td>4.47%</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>OnlineNIC, Inc.</td>
<td>2.13%</td>
</tr>
<tr>
<td>Center of Ukrainian Internet Names</td>
<td>2.07%</td>
</tr>
<tr>
<td>Register.com, Inc.</td>
<td>1.89%</td>
</tr>
</tbody>
</table>

**Confirmation**: A handful of registrars account for the majority of spammer domains

Spam Proportions on Registrars

- **Question**: Do registrars *only* host spammer domains?

- **Finding**: Spammer primarily use popular registrars.
Authoritative Nameservers

- **Question**: Do spammers use particular nameservers?

Example DNS server hosting the greatest number of spammer domains

*ns1.monikerdns.net*

But 99.77% of **all** domains were registered through the same registrar *Moniker Online Services, Inc*

- **Finding**: Spammers often use the nameservers provided by the registrars
Talk Outline

• Motivation

• Registration Process and Data Collection

• DNS Infrastructure Used for Spammer Domains

• Detecting Registration Spikes

• Domain Life-cycle Role Analysis

• Summary
An Example of Bulk Registration

- Question: Do spammers register domains in groups?

- Domains registered by *eNom* every 5 minutes in March 5\(^{th}\), 2012
Spike Pattern

Distribution of Spammer Domain Registration

- Distribution of the number of spammer domains registered within the same registrar and epoch

Only 20% of the spammer domains got registered in isolation

Finding: Spammers perform registrations in batches
Question: How to identify “abnormally large” registration batches?

- Build hourly model to fit diurnal patterns
- Compound Poisson to represent the customer purchase behaviors

*eNom, Inc.*, hourly window, 10AM–11AM ET
Registrations in Spikes

- Spammer domains in spikes: 42%
- All domains in spikes: 15%

**Finding:** Spammer domains appear in spikes with a much higher likelihood.
Talk Outline

• Motivation

• Registration Process and Data Collection

• DNS Infrastructure Used for Spammer Domains

• Detecting Registration Spikes

• *Domain Life-cycle Role Analysis*

• Conclusion
Life Cycle Categories

- **Brand-new**
  - The domain has never appeared in the zone before
- **Re-registration**
  - The domain has previously appeared in the zone
    - *Drop-catch*: re-registered immediately after its release
    - *Retread*: some time elapses between a domain’s prior deletion and its re-registration
Prevalence of Different Categories

• **Question**: What type of domains is more likely being used in spam?

Conditional probability of being a spammer domain

<table>
<thead>
<tr>
<th>Category</th>
<th>Prevalence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brand-new</td>
<td>1.01%</td>
</tr>
<tr>
<td>Drop-catch</td>
<td>0.33%</td>
</tr>
<tr>
<td>Retread</td>
<td>1.34%</td>
</tr>
<tr>
<td>In spikes</td>
<td>2.61%</td>
</tr>
<tr>
<td></td>
<td>0.37%</td>
</tr>
<tr>
<td></td>
<td><strong>4.48%</strong></td>
</tr>
</tbody>
</table>

• **Finding**: Spammers commonly re-register expired domains, especially when performing bulk registrations.
Malicious Activities before Retread

- **Question**: Do spammers re-register previous spammer domains?

- Introspect with spam trap and blacklists before the re-registration time (October 2011 – February 2012)
  - Only 6.8% had appeared in a blacklist before re-registration

- **Finding**: Spammers re-register expired domains with clean histories
Life Cycle

Dormancy before Retread

- **Question**: How long is between deletion and re-registration?

![Graph showing cumulative percentage of domain deletions over time]

- **Finding**: Spammers have a trend to re-register domains that expired more recently.

65% of retread spammer domains were deleted less than 90 days before.
Takeaways

• Positive actions from specific registrars could have significant impact in impeding spammer domain registrations

• Pay attention to bulk registrations: spammers find economic and/or management benefit to register domains in large batches

• In addition to generating names, spammers take advantage of re-registering expired domains, that originally had a clean history
Summary

• We studied the fine-grained domain registration of .com zone over a 5-month period

• Registration patterns have powers for distinguishing spammer domains, but no striking signal that separates good domains from bad ones

• Next steps
  – Develop a detector against spammer domains at registration time
  – Investigate further the reasons of spammer registration strategies

http://www.cc.gatech.edu/~shao