On the Potential of Proactive Domain Blacklisting

Márk Félegyházi, Christian Kreibich and Vern Paxson

ICSI, Berkeley
Spam domain registrations

Kreibich et al., “Spamcraft: An inside look at spam campaign orchestration” LEET 2009 (CCIED: The Collaborative Center for Internet Epidemiology and Defenses)
Spam domain registrations

- domains dropped soon after blacklisted

Kreibich et al., “Spamcraft: An inside look at spam campaign orchestration” LEET 2009
( CCIED: The Collaborative Center for Internet Epidemiology and Defenses)
Spam domain registrations

- domains dropped soon after blacklisted
- domains registered in batches

Kreibich et al., “Spamcraft: An inside look at spam campaign orchestration” LEET 2009 (CCIED: The Collaborative Center for Internet Epidemiology and Defenses)
Proactive domain clustering

name server properties + registration information

1

buypills.com

2

pillsmeds.com
rxbesthealth.com
rxpharma.com
vgrpills.com

INFERENCE
Proactive domain clustering

name server properties + registration information

1. buypills.com

2. pillsmeds.com
   rxbesthealth.com
   rxpharma.com
   vgrpills.com

INFERENCEx

known bad
suspected bad
unknown

3. pillsmeds.com
   rxbesthealth.com
   rxpharma.com
   vgrpills.com

VALIDATION
Name server features

.COM zone file - NS records

buypills.com
Name server features

.COM zone file - NS records

buypills.com

01/10/2010

FRESH

ns1.canadian.com (registered within 1 year)
Name server features

.COM zone file - NS records

buypills.com

01/10/2010

FRESH

ns1.canadian.com (registered within 1 year)

pillsmeds.com
rxbesthealth.com
besthealthpills.com
rxpharmacy.com
Name server features

.COM zone file - NS records

buypills.com

01/10/2010

FRESH

ns1.canadian.com (registered within 1 year)

pillsmeds.com
rxbesthealth.com
besthealthpills.com
rxpharmacy.com

01/17/2010

SELF-RESOLVING

ns1.buypills.com
Name server features

.COM zone file - NS records

buypills.com

01/10/2010

FRESH

ns1.canadian.com
(represented within 1 year)

pillsmeds.com
rxbesthealth.com
besthealthpills.com
rxpharmacy.com

01/17/2010

SELF-RESOLVING

ns1.buypills.com

vgrpills.com
ns.vgrpills.com
bookstores.com
ns.bookstores.com
## Registration features

**WHOIS registry records**

| buypills.com       | 01/09/2010 - Enom |
Registration features

WHOIS registry records

- buypills.com: 01/09/2010 - Enom
- pillsmeds.com: 01/09/2010 - Enom
- rxbesthealth.com: 01/09/2010 - Enom
- besthealthpills.com: 12/20/2009 - Enom
- rxpharmacy.com: 01/09/2010 - Enom
- vgrpills.com: 01/09/2010 - Enom
- bookstores.com: 01/01/2010 - GoDaddy
Registration features

WHOIS registry records

- buypills.com 01/09/2010 - Enom
- pillsmeds.com 01/09/2010 - Enom
- rxbesthealth.com 01/09/2010 - Enom
- besthealthpills.com 12/20/2009 - Enom
- rxpharmacy.com 01/09/2010 - Enom
- vgrpills.com 01/09/2010 - Enom
- bookstores.com 01/01/2010 - GoDaddy
Evaluation

INFERENCE

name server properties + registration information

1. joewein.net blacklist
   Jan 2010 (3653 domains)

2. (11053 domains)

3x
Evaluation

name server properties + registration information

joewein.net blacklist
Jan 2010 (3653 domains)

(11053 domains)

INFERENCE

joewein.net black, URIBL black
McAfee SiteAdvisor, URIBL gold
unknown

VALIDATION
Evaluation

**INFERENCE**

1. name server properties
2. registration information

**VALIDATION**

- joewein.net blacklist, URIBL black
- McAfee SiteAdvisor, URIBL gold
- unknown

joewein.net blacklist
Jan 2010
(3653 domains)

(11053 domains)

3x

+ 48.7 %
Evaluation

**Inference**

1. Name server properties + registration information
2. joewein.net blacklist, Jan 2010 (3653 domains)
3. INFERENCES (11053 domains)

**Validation**

1. joewein.net black, URIBL black
2. McAfee SiteAdvisor, URIBL gold
3. unknown

Total increase: +48.7% +19.7%
Evaluation

1. **name server properties**
   - joewein.net blacklist
   - Jan 2010
   - (3653 domains)

2. **registration information**
   - (11053 domains)

3. **INFERENCEx3**

4. **VALIDATION**
   - joewein.net black, URIBL black: +48.7%
   - McAfee SiteAdvisor, URIBL gold: +19.7%
   - unknown: 6.6%
Prediction accuracy
Prediction accuracy

- good true positive rate, only few false positives
- # of false positives vary across clusters
  - 84% of clusters have no potential FPs (unknown)
A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains
A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains

  skatesynthesize.com
  sodamonitor.com
  sofapin.com
  soulvisionmedia.com
  suggestioneject.com
  thrillcrash.com
  thunderjudge.com
  treeturn.com
  wristprogram.com
  dockundertake.com
  wrenchimprove.com
  queensnoot.com

(51 rows)
A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains

<table>
<thead>
<tr>
<th>skatesynthesis.com</th>
<th>blue-tooth-shop.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>sodamonitor.com</td>
<td>blue-towel.com</td>
</tr>
<tr>
<td>sofapin.com</td>
<td>blue-trails.com</td>
</tr>
<tr>
<td>soulvisionmedia.com</td>
<td>blue-trumpet.com</td>
</tr>
<tr>
<td>suggestioneject.com</td>
<td>blue-tux.com</td>
</tr>
<tr>
<td>thrillcrash.com</td>
<td>blue-twin.com</td>
</tr>
<tr>
<td>thunderjudge.com</td>
<td>blue-up-parfum.com</td>
</tr>
<tr>
<td>treeturn.com</td>
<td>blue-vet.com</td>
</tr>
<tr>
<td>wristprogram.com</td>
<td>blue-view-sak.com</td>
</tr>
<tr>
<td>dockundertake.com</td>
<td>blue-walking-stick.com</td>
</tr>
<tr>
<td>wrenchimprove.com</td>
<td>blue-skyblue.com</td>
</tr>
<tr>
<td>queensnnoop.com</td>
<td></td>
</tr>
</tbody>
</table>
(51 rows)           | (72 rows)           |
A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains

<table>
<thead>
<tr>
<th>skatesynthsize.com</th>
<th>blue-tooth-shop.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>sodamonitor.com</td>
<td>blue-towel.com</td>
</tr>
<tr>
<td>sofapin.com</td>
<td>blue-trails.com</td>
</tr>
<tr>
<td>soulvisionmedia.com</td>
<td>blue-trumpet.com</td>
</tr>
<tr>
<td>suggestioneject.com</td>
<td>blue-tux.com</td>
</tr>
<tr>
<td>thrillcrash.com</td>
<td>blue-twin.com</td>
</tr>
<tr>
<td>thunderjudge.com</td>
<td>blue-up-parfum.com</td>
</tr>
<tr>
<td>treeturn.com</td>
<td>blue-vet.com</td>
</tr>
<tr>
<td>wristprogram.com</td>
<td>blue-view-sak.com</td>
</tr>
<tr>
<td>dockundertake.com</td>
<td>blue-walking-stick.com</td>
</tr>
<tr>
<td>wrenchimprove.com</td>
<td>blue-skyblue.com</td>
</tr>
<tr>
<td>queensnoop.com</td>
<td></td>
</tr>
</tbody>
</table>

(51 rows) (72 rows)
A note on false positives

- some other clusters (example: 123 domains, 119 FP)
  - many noun-noun domains
    - skatesynthesize.com
    - sodamonitor.com
    - sofapin.com
    - soulvisionmedia.com
    - suggestioneject.com
    - thrillcrash.com
    - thunderjudge.com
    - treeturn.com
    - wristprogram.com
    - dockundertake.com
    - wrenchimprove.com
    - queensnoop.com
    - blue-tooth-shop.com
    - blue-towel.com
    - blue-trails.com
    - blue-trumpet.com
    - blue-tux.com
    - blue-twin.com
    - blue-up-parfum.com
    - blue-vet.com
    - blue-view-sak.com
    - blue-walking-stick.com
    - blue-skyblue.com

- large cluster: 1746 domains
  - part of a set of 80k domains
  - registered under a single name in Albania in Jan and Feb 2010
Time to blacklisting

The graph shows the percentage of events over time until blacklisting. The x-axis represents the time in hours, days, weeks, and months, while the y-axis represents the percentage. The data trend indicates an increase in the percentage of events as the time until blacklisting increases.
Time to blacklisting
Time to blacklisting

![Graph showing time to blacklisting](image-url)
Summary

- domains registered and used in clusters
Summary

- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information
Summary

- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information
- good accuracy
  - 73% of inferred domains on blacklists
  - 93% of domains are suspicious
  - false positives are often true positives
Summary

- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information
- good accuracy
  - 73% of inferred domains on blacklists
  - 93% of domains are suspicious
  - false positives are often true positives
- faster than blacklists for 92% of the inferred malicious domains
Summary

- domains registered and used in clusters
- more malicious domains based on a few seeds and domain registry information
- good accuracy
  - 73% of inferred domains on blacklists
  - 93% of domains are suspicious
  - false positives are often true positives
- faster than blacklists for 92% of the inferred malicious domains

early response to spam
Spam and click volumes

Kanich et al., “Spamalytics: An empirical analysis of spam marketing conversion” CCS 2008
(CCIED: The Collaborative Center for Internet Epidemiology and Defenses)
Spam and click volumes

Kanich et al., “Spamalytics: An empirical analysis of spam marketing conversion” CCS 2008
(CCIED: The Collaborative Center for Internet Epidemiology and Defenses)
Name server ages
NS features

- 82.2% of domains encounter fresh name servers
Registration clusters
McAfee SiteAdvisor

rxbesthealth.com

McAfee TrustedSource web reputation analysis found potential suspicious behavior on this site which may pose a security risk. Use with caution.

Are you the owner of this site? Leave a comment
What is TrustedSource™?

AUTOMATED WEB SAFETY TESTING RESULTS FOR RXBESTHEALTH.COM

E-MAIL TESTS FOR RXBESTHEALTH.COM: ?

DOWNLOAD TESTS FOR RXBESTHEALTH.COM: ?

ONLINE AFFILIATIONS FOR RXBESTHEALTH.COM: ?

ANNOYANCES FROM RXBESTHEALTH.COM: ?

REVIEWER AND WEB SITE OWNER COMMENTS

USER REVIEW SUMMARY FOR RXBESTHEALTH.COM ?

This site is good (0)       Excessive popups (0)
This site spans (0)        Phishing or other scams (2)
Adware, spyware, or viruses (0)  Bad shopping experience (0)
Browser exploit (0)