Toby Lauinger, Abdelberi Chaabane, Ahmet S. Buyukkayhan, Kaan Onarlioglu, William Robertson

Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers

Usenix Security 2017
Internet Domain Names

- Used in many, often security-critical ways

**WHOIS Lost in Translation Domain Name Expiration**

Tobias Lauinger  
Northeastern University  
toby@ccs.neu.edu

Kaan Onarlioglu  
Northeastern University  
onarliog@ccs.neu.edu

William Robertson  
Northeastern University  
wkr@ccs.neu.edu

- Typically, assumption of constant ownership
- However, hundreds of thousands of domains expire *every day*
Attacks Involving Expired Domains

• Abuse of residual trust

• Schlamp et al., “The Abandoned Side of the Internet” (2014)
  – Re-register domains to take over email addresses used to manage critical resources (e.g., IP prefix or AS)

• Lever et al., “Domain-Z” (2016)
  – Take over software update/repository servers
  – Take over name servers used by non-expired domains
Attacks Involving Expired Domains

• Abuse of residual trust

• Schlamp et al., "The Abandoned Side of the Internet" (2014)
  – Re-register domains to take over email addresses used to manage critical resources (e.g., IP prefix or AS)

• Lever et al., "Domain-Z" (2016)
  – Take over software update/repository servers
  – Take over name servers used by non-expired domains
Also, Undesirable Behaviour

- When re-registered, domains often not what visitors expect
  - E.g., formerly useful website turned into spam page

- ICANN:
  - “(...) websites featuring nothing but advertisements, thus leading to a form of Internet graffiti.”
  - “(...) profit-making abuse of the domain name system”
  - https://www.icann.org/news/announcement-2009-08-12-en
Also, Undesirable Behaviour

- When re-registered, domains often not what visitors expect
  - E.g., formerly useful website turned into spam page
- ICANN:
  - "(…) websites featuring nothing but advertisements, thus leading to a form of Internet graffiti."
  - "(…) profit-making abuse of the domain name system"

https://www.icann.org/news/announcement-2009-08-12-en
Contribution: The Big Picture

• Attack potential known, but how many opportunities?
• Quantification of domain name “recycling”; two scenarios:
  – Drop-catch: Re-registered instants after general availability
  – Pre-release: Sold by registrar before general availability

• Frequent and competitive domain takeovers
• Impact of this practice on domain registration ecosystem
• After expiration, two grace periods allow recovery before deletion
• See “Whois Lost in Translation” (IMC 2016) for the details of domain expiration states
• Re-register immediately when deleted (drop-catch)
• Old registrar: sell before deletion (pre-release)
Data Collection Overview

- Drop-catch services and pre-release platforms promote lists of available domains → use as seed for measurement
- Whois lookups every 14 days to detect status changes
- All listed domains during 4 weeks in July/August 2016

<table>
<thead>
<tr>
<th></th>
<th>com</th>
<th>net</th>
<th>org</th>
<th>biz</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-release total</td>
<td>1.2M</td>
<td>135k</td>
<td>116k</td>
<td>21k</td>
<td>182</td>
</tr>
<tr>
<td>Median/day</td>
<td>43.5k</td>
<td>4.9k</td>
<td>4k</td>
<td>710</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>com</th>
<th>net</th>
<th>org</th>
<th>biz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending delete total</td>
<td>2.1M</td>
<td>255k</td>
<td>169k</td>
<td>51k</td>
</tr>
<tr>
<td>Median/day</td>
<td>76.4k</td>
<td>9.2k</td>
<td>6.1k</td>
<td>1.7k</td>
</tr>
</tbody>
</table>
Expiration, Pre-Release and Drop-Catch

• August 2016:
  – 131M .com domains registered
  – 2.2M .com domains deleted after expiration (1.7% of zone)
  – 2.6M .com domains created (new & re-registrations)

• Measurement (28 days):
  – 1.2M .com domains available pre-release; 71k sold
  – 10.1% of deleted .com domains re-registered as drop-catch

• Domain reuse is a frequent phenomenon
Re-Registrations During the Drop

- The “drop”: Domains deleted (and re-registered) during same daily time span
- Re-registration as early as possible hints at significant competition

60% daily re-registrations done by 14:31

Drop begins at 14:30
Drop-Catch Registrars

- Registries impose rate limits on each registrar
- Drop-catch services use multiple registrars to increase success rates
  - “DropCatch.com n LLC”
  - “Charlemagne 888, LLC”, “George Washington 888, LLC”, “Napoleon Bonaparte, LLC”, ...
Top 3 clusters are well-known drop-catch services
They account for over 75% of all accredited registrars
(but only 8% of monthly domain creations)
These clusters have been growing in size
Significant resources are deployed to compete in the drop
• Large cluster not necessary to create many domains
• 99.9% of domain creation attempts fail; drop-catch responsible for at least 80%
• Drop-catch has large impact on domain registration ecosystem
Discussion & Recommendations

• Results show frequent, professionally organised “recycling” of domains, expending significant resources

• Security consequences of domain “recycling”:
  – Attacks related to residual trust abuse
  – Annoyance (“Internet graffiti”)
  – Pre-release risks (potential to evade registration-time detection)

• Recommendation: “Domain Transparency”
Conclusion

• Take-away points:
  – *Domain-based trust mechanisms should anticipate ownership changes as a common, expected event.*
  – *Anti-abuse tools may need improved detection of ownership changes that are not re-registrations.*

• Paper-exclusive material:
  – Drop-catch domain tasting, auctions and prices, age and traffic
  – More on pre-release, drop-catch registrar characteristics & arms race...