Detection and Mitigation of Fast-Flux Service Networks

Thorsten Holz, Christian Gorecki,
Felix Freiling, Konrad Rieck
Motivation

- Yesterday: presentation by Dagon
  - “Corrupt DNS Resolution Paths”
- Today: How attackers use DNS for malicious purposes, e.g., scam hosting
Motivation

• Yesterday: presentation by Dagon
  • “Corrupt DNS Resolution Paths”

• Today: How attackers use DNS for malicious purposes, e.g., scam hosting

$ dig isoc.org

;; ANSWER SECTION:
isoc.org. 38679 IN A 206.131.241.137
$ dig dadusual.com

;; ANSWER SECTION:
dadusual.com.   300 IN A 125.59.103.156
dadusual.com.   300 IN A 218.254.9.205
dadusual.com.   300 IN A 62.65.233.109
dadusual.com.   300 IN A 76.181.194.207
dadusual.com.   300 IN A 77.41.18.139
dadusual.com.   300 IN A 78.84.69.132
dadusual.com.   300 IN A 78.106.115.147
dadusual.com.   300 IN A 78.106.180.151
dadusual.com.   300 IN A 78.106.200.47
dadusual.com.   300 IN A 78.106.224.174
dadusual.com.   300 IN A 79.120.43.191
dadusual.com.   300 IN A 80.222.32.58
dadusual.com.   300 IN A 84.62.186.63
dadusual.com.   300 IN A 85.177.42.179
dadusual.com.   300 IN A 85.181.225.55
dadusual.com.   300 IN A 89.112.4.172
Motivation

$ dig dadusual.com

;; ANSWER SECTION:

cm125-59-103-156.hkcable.com.hk. 300 IN A 125.59.103.156

cm218-254-9-205.hkcable.com.hk. 300 IN A 218.254.9.205

cp109.host41.starman.ee. 300 IN A 62.65.233.109

cpe-76-181-194-207.columbus.res.rr.com. 300 IN A 76.181.194.207

host-77-41-18-139.qwerty.ru. 300 IN A 78.84.69.132

dadusual.com. 300 IN A 78.106.115.147

dadusual.com. 300 IN A 78.106.180.151

dadusual.com. 300 IN A 78.106.200.47

dadusual.com. 300 IN A 78.106.224.174

dadusual.com. 300 IN A 79.120.43.191

dadusual.com. 300 IN A 80.222.32.58

dadusual.com. 300 IN A 84.62.186.63

dadusual.com. 300 IN A 85.177.42.179

dadusual.com. 300 IN A 85.181.225.55

dadusual.com. 300 IN A 89.112.4.172
Motivation
Outline

- Introduction
- Automated identification fast-flux domains
- Measurement results
  - Two month period in July / August 2007
- Mitigation (briefly)
- Conclusion
Introduction

• *Availability* is important for commercial services

• Techniques from the area of reliability engineering help to achieve availability

• RAID or failover systems

• Methods using DNS
  • Round-robin DNS
  • Content distribution networks (CDNs)
Introduction

- Availability is important for commercial services
- Techniques from the area of reliability engineering help to achieve availability

$ dig myspace.com

;; ANSWER SECTION:
myspace.com.             3410    IN      A       216.178.38.104
myspace.com.             3410    IN      A       216.178.38.121
myspace.com.             3410    IN      A       216.178.38.116
• **Availability** is important for commercial services

• Techniques from the area of reliability engineering help to achieve availability

```
$ dig myspace.com

;; ANSWER SECTION:
myspace.com.       3409 IN  A   216.178.38.116
myspace.com.       3409 IN  A   216.178.38.104
myspace.com.       3409 IN  A   216.178.38.121
```
• **Availability** is important for commercial services

• Techniques from the area of reliability engineering help to achieve availability

$ dig myspace.com

;; ANSWER SECTION:
myspace.com.       3408 IN A 216.178.38.121
myspace.com.       3408 IN A 216.178.38.116
myspace.com.       3408 IN A 216.178.38.104
Introduction

• *Availability* is important for commercial services

• Techniques from the area of reliability engineering help to achieve availability

• RAID or failover systems

• Methods using DNS
  • Round-robin DNS
  • Content distribution networks (CDNs)
Introduction

- Note: illegal commercial organizations also need high availability
- Scammer only earns money if pharmacy shop is online
- Phisher needs to have phishing site online
- Our starting point:
  - How do attackers achieve high availability?
• If scammers could advertise multiple IP addresses for a given domain, shutdown would be harder
• Botherder could use idea behind RRDNS to split botnet across multiple C&C server
• Technique used: Fast-flux service networks
  • Fast change in DNS answers
  • Recent paper by Honeynet Project
• Given fast-flux domain returns few IP addresses from large pool of compromised machines ("flux agents")

• After the (low) TTL expired, return different subset
• Given fast-flux domain returns few IP addresses from large pool of compromised machines (“flux agents”)

• After the (low) TTL expired, return different subset

<table>
<thead>
<tr>
<th>Host Name</th>
<th>TTL</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>69.183.26.53</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>76.205.234.131</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>85.177.96.105</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>217.129.178.138</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>24.98.252.230</td>
</tr>
</tbody>
</table>
FFSNs

• Given fast-flux domain returns few IP addresses from large pool of compromised machines ("flux agents")

• After the (low) TTL expired, return different subset

<table>
<thead>
<tr>
<th>Host</th>
<th>TTL</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>69.183.26.53</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>76.205.234.131</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>85.177.96.105</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>217.129.178.138</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>24.98.252.230</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Host</th>
<th>TTL</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>213.47.148.82</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>213.91.251.16</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>69.183.207.99</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>91.148.168.92</td>
</tr>
<tr>
<td>thearmynext.info.</td>
<td>600</td>
<td>IN</td>
<td>195.38.60.79</td>
</tr>
</tbody>
</table>
**FFSNs**

- Given fast-flux domain returns few IP addresses from large pool of compromised machines ("flux agents")
- After the (low) TTL expired, return different subset

<table>
<thead>
<tr>
<th>IP address returned in A record</th>
<th>Reverse DNS lookup for IP address</th>
<th>ASN</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>69.183.26.53</td>
<td>69.183.26.53.adsl.snet.net.</td>
<td>7132</td>
<td>US</td>
</tr>
<tr>
<td>76.205.234.131</td>
<td>adsl-76-205-234-131.dsl.hstntx.sbcglobal.net.</td>
<td>7132</td>
<td>US</td>
</tr>
<tr>
<td>85.177.96.105</td>
<td>e177096105.adsl.alicedsl.de.</td>
<td>13184</td>
<td>DE</td>
</tr>
<tr>
<td>24.98.252.230</td>
<td>c-24-98-252-230.hsd1.ga.comcast.net.</td>
<td>7725</td>
<td>US</td>
</tr>
</tbody>
</table>
FFSNs

1) HTTP GET
host: thearmynext.info

2) GET redirected

3) Response

4) Response

"mothership"

flux agent

thearmynext.info

flux agent

UNIVERSITÄT MANNHEIM
1) HTTP GET
host: thearmynext.info

2) GET redirected

3) Response
thearmynext.info

4) Response

"mothership"

flux agent

flux agent

flux agent

Thorsten Holz • NDSS’08 - “Detection and Mitigation of Fast-Flux Service Networks”
FFSNs

Proxy network on top of compromised machines

1) HTTP GET
   host: themynext.info

2) GET redirected

"mothership"

3) Response
   themynext.info

4) Response

flux agent

flux agent
Automated Identification
Finding Fast Flux Service Networks
• Attacker’s restrictions in establishing FFSNs
  • IP address diversity
  • No physical agent control
Metric

- Attacker’s restrictions in establishing FFSNs
  - IP address diversity
  - No physical agent control
- Possible distinguishing parameters
  - Number of unique A records $n_a$ in all lookups
  - Number of NS records in single lookup $n_{NS}$
  - Number of unique ASNs for all A records $n_{ASN}$
Flux-Score

- Vector $x = (n_A, n_{NS}, n_{ASN})$, weight vector $\omega$
- Linear decision function

$$F(x) = \begin{cases} 
    w^T x - b > 0 & \text{if } x \text{ is a fast-flux domain} \\
    w^T x - b \leq 0 & \text{if } x \text{ is a benign domain}
\end{cases}$$

- Use corpus of FF and benign domains to derive values for $\omega$ and $b$
- Compute optimal hyperplane
- Efficient computation with linear programming
Flux-Score

- Obtain scoring metric $f$
  
  $$f(x) = w^T x = w_1 \cdot n_A + w_2 \cdot n_{ASN} + w_3 \cdot n_{NS}$$

- Instantiate model with weights

- 128 manually verified FF domains and 5,803 benign domains

- 10-fold cross validation using different parameters

  $$f(x) = 1.32 \cdot n_A + 18.54 \cdot n_{ASN} + 0 \cdot n_{NS}$$
  
  with $b = 142.38$

  detection accuracy 99.98%, standard deviation 0.05%
Empirical Results

Measuring FFSNs in July / August 2007
Scam Hosting

- Spamscatter (USENIX’07, Anderson et al.)
- No FFSNs identified
- 6% of scams hosted on multiple IPs (45 IPs max)
- Spamcorpus with 22K mails from August 2007
- Contained 7,389 unique domains
- Based on flux-score, 2,197 (29.7%) are FFSNs
  - 563 unique fast-flux domains (w/o wildcards)
  - 1,737 unique IP addresses
• 33 FFSNs were tracked for 7 weeks every 300s
• 18,214 unique IP addresses monitored
  • Does not take churn by DHCP into account
  • NAT is no problem since machines need to be reachable
• 818 unique AS (43.3% in top 10 AS)

<table>
<thead>
<tr>
<th>Rank</th>
<th>ASN</th>
<th>Name</th>
<th>IPs</th>
<th>Top 10 AS%</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7132</td>
<td>(AT&amp;T Internet Services, US)</td>
<td>2,677</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4766</td>
<td>(Korea Telecom, KR)</td>
<td>590</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>8551</td>
<td>(Bezeqint Internet, IL)</td>
<td>445</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>8402</td>
<td>(Corbina telecom, RU)</td>
<td>397</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>9304</td>
<td>(Hutchison Global, HK)</td>
<td>1,797</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3320</td>
<td>(Deutsche Telekom, DE)</td>
<td>500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>12322</td>
<td>(Proxad/Free ISP, FR)</td>
<td>418</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1680</td>
<td>(NetVision Ltd., US)</td>
<td>361</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cumulative number of distinct ASNs observed for 33 FFSNs (15 days)
Other Abuses

- Storm Worm uses fast changing DNS entries to host web site with malware binary
  - Observed more than 50K IP addresses in four week period
- Rock Phish, a large phishing group, uses FFSNs to host phishing site
  - Observed 1,121 unique IP addresses in 4 days
- FFSNs could be used to host IRC, SMTP, ...
Mitigation

Stopping the Threat
Mitigation

- Domain blacklist
  - Collaboration with registrar / monitoring DNS
  - Content-based spam filtering
- Identifying control node
- Tracing in proxy network is hard
- Mark specific request and trace it through network (needs ISP collaboration)
Conclusion

- First empirical study of FFSNs, a new and emerging threat
- Developed a metric to automatically identify fast-flux domains
- Empirical measurement results
- Future work
  - Improve flux-score
  - Estimate size of FFSN based on capture-recapture methods
Acknowledgments:
Thanks to anonymous reviewers and Fabian Monrose

Data available:
http://pi1.informatik.uni-mannheim.de/fast-flux
Fluxiness

- Metric to distinguish FFSNs from benign domains can be defined as function of $n_a$, $n_{NS}$, and $n_{ASN}$

- Fluxiness: $\varphi = \frac{n_a}{n_{single}}$

  - $n_{single}$ is number of A records in single lookup
  - $\varphi = 1.0$: constant set of A records returned
  - $\varphi = 2.0$ in previous example
  - Implicitly contained in $n_A$ and $n_{ASN}$
Cumulative number of distinct A records observed for 33 FFSNs (15 days)

Thorsten Holz • NDSS’08 - “Detection and Mitigation of Fast-Flux Service Networks”
VeriSign Implements Rapid Updates to Domain Name System Files

News & Events

VeriSign Implements Rapid Updates to Domain Name System Files
.com and .net Domain Name Changes Now Functional for Viewing on the World Wide Web within Minutes of New Registration or Modifications

Mountain View, CA September 9, 2004 - VeriSign, Inc. (Nasdaq: VRSN), the leading provider of intelligent infrastructure services for the Internet and telecommunications networks, today announced that it has implemented a major enhancement, called "rapid updates," to its .com and .net Domain Name System (DNS) servers. With rapid updates, it is now possible for domain registrants to launch Web sites more quickly and to experience greater continuity in service when changing hosting providers or modifying their domain name registrations.

Previously, VeriSign updated DNS servers for .com and .net twice each day by generating a file from its .com and .net Registry database and globally distributing it to all 13 of the .com and .net DNS servers.

With new, rapid updates, VeriSign distributes updates every few seconds accommodating all changes that affect any of the more than 35 million domain names for .com or .net. With the new update process, domain registrants are now able to add a new domain name, change their hosting provider or make other changes to their domain name, and see those changes reflected in the .com and .net DNS servers within a matter of minutes.

"Companies that bundle Web and e-mail services with a domain name, can now provide their customers with the ability to see their new Web sites almost immediately," said Elliott Noss, CEO of Tucows Inc. "Rapid updates enables us to provide our customers with better levels of service."

"In a very short time, the Internet has become an indispensable communications tool of businesses and consumers, so much so that even a very short disruption in service can have a significant impact on those conducting commerce and communications," said Raynor Dahlquist, acting vice president of VeriSign's