Behavioral Analysis of Fast Flux Service Networks

Cyber Security and Information Intelligence Research Workshop

April 14, 2009
Oak Ridge, TN

Presentation Outline

- Fast flux botnet problem
- Data collection
- Short term behavior
- Long term behavior
- Organizational behavior
- Operational behavior
- Conclusions
News

• **Waledac botnet is active again with malicious money saving website ...**
  
  SC Magazine UK - '1 hour ago'

• **Conficker botnet ready to be split, sold**
  
  SearchSecurity.com - Feb 26, 2009

• **Malware Writers Use Multiple Botnets to Spread Valentine's Day ...**
  
  eWeek - Feb 11, 2009

Fast Flux Problem

• ICANN GNSO definition:
  – rapid and repeated changes to host and/or name server resource records, which result in rapidly changing the IP address to which the domain name of an Internet host or name server resolves

• Malicious use:
  – Spam campaigns, phishing, malware delivery, DDoS attacks

• Technical challenge:
  – monitoring changes to DNS records
  – classification of historical behavior
  – real time detection
  – differentiation from legitimate behavior
Fast Flux Behavior

- no fast flux
- fast flux

FastFlux Service Monitor

- Scheduler
  - Supports multiple concurrent processes for domain testing
- Detection and classification
  - Behavioral indicators from DNS records
  - Bayesian classifier domain IPs → single flux
  - Bayesian classifier nameserver IPs → double flux
- Application logic
  - Analytics, reporting, domain management (e.g. dead domains) ...
- Notification services
  - RSS ...
- Distributed Architecture Design
  - Support batch processing and incremental learning automation
FFM Architecture

Fast Flux Short Term Behavior

safecause.com

<table>
<thead>
<tr>
<th>Time</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:55 pm</td>
<td><img src="image1.png" alt="Graph" /></td>
</tr>
<tr>
<td>1:58 pm</td>
<td><img src="image2.png" alt="Graph" /></td>
</tr>
<tr>
<td>2:01 pm</td>
<td><img src="image3.png" alt="Graph" /></td>
</tr>
<tr>
<td>2:04 pm</td>
<td><img src="image4.png" alt="Graph" /></td>
</tr>
<tr>
<td>2:07 pm</td>
<td><img src="image5.png" alt="Graph" /></td>
</tr>
</tbody>
</table>
Lifespan Distribution of FF Botnet Domains

Lifespan: Malware vs. Phishing vs. Spam
Lifespan: Phishing Fast Flux Botnets

Size Distribution of FF Botnet Domains
Fast Flux Botnet Domains: Size vs. Lifespan

Malware FF Botnets: Size vs. Lifespan
Distribution of Shared IP Addresses

Operation in Multiple Countries
Conclusions

- Short term behavior
  - Domain fluxing every minute with sporadic idles
  - Name server fluxing every 6 hours

- Long term behavior
  - Spam and malware FF botnets live about two months
  - Phishing FF botnets live about 5 days
  - Larger networks live longer

- Organizational behavior
  - The number of IPs shared is inversely proportional to the number of domains sharing them

- Operational behavior
  - Operate in 60 countries and 300 ASNs

- Evaluate beta service: bot@milcord.com
Thank You.

Any Questions?

info@milcord.com  (781) 839-7138