A Case Study on Asprox Infection Dynamics

Youngsang Shin¹, Steven Myers², Minaxi Gupta¹

¹ School of Informatics and Computing, Indiana University
{shiny, minaxi}@cs.indiana.edu
² School of Informatics and Computing, Indiana University
samyers@indiana.edu

This work is supported in part by Indiana University’s Center for Applied Cybersecurity Research.
Asprox Overview

- Brief History
  - Asprox botnet has been around since 2007
  - Initially used exclusively for sending phishing emails
  - Around May 2008, a new update was pushed to Asprox bots
    - an attempt to grow the size of the botnet
    - SQL injection vector
  - A significant number of web servers have since been attacked and their unsuspecting visitor machines turned into Asprox bots
Multistep Life Cycle of Asprox

1. SQL injection
2. Web surfing
3. Infected Web page
4. JavaScript download
5. Malware download

Asprox bot
Vulnerable Web server
Vulnerable Visitor
Outline

- **Introduction**
- **Data Collection & Overview**
- **Analysis of Asprox Infection Dynamics**
  - Asprox Bots
  - Infected Web Servers
  - JavaScript-Delivery Hosts
- **Concluding Remarks**
Data on SQL-injecting Asprox Bots

- Information about Asprox bots that attacked web servers at Indiana University in August 2008
  - SQL-injection attacks

<table>
<thead>
<tr>
<th></th>
<th>8/9/2008 ~ 8/25/2008 (17 days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Period</td>
<td></td>
</tr>
<tr>
<td>Unique IP addresses of attacking bots</td>
<td>57,419</td>
</tr>
<tr>
<td>Autonomous systems attackers belonged to</td>
<td>1,847</td>
</tr>
<tr>
<td>Web servers targeted</td>
<td>581</td>
</tr>
</tbody>
</table>
# Data on JavaScript-Delivery Hosts

## JavaScript-delivery hosts

<table>
<thead>
<tr>
<th>Collection Period</th>
<th>10/26/2008 ~ 1/31/2009 (98 days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique Hostnames</td>
<td>324</td>
</tr>
<tr>
<td>With gTLDs</td>
<td>151 (.com: 105, .name: 28, .mobi: 11, .net: 4, .org: 3)</td>
</tr>
<tr>
<td>With ccTLDs</td>
<td>173 (.ru: 127, .cn: 34, .jp: 4, .cc: 4, .tk: 1, .kz: 1, .eu: 1, .me: 1)</td>
</tr>
</tbody>
</table>

## JavaScript-delivery hosts

<table>
<thead>
<tr>
<th>Resolved hostnames</th>
<th>55</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses</td>
<td>2,214</td>
</tr>
<tr>
<td>ASes</td>
<td>308</td>
</tr>
<tr>
<td>BGP prefixes</td>
<td>898</td>
</tr>
<tr>
<td>Countries</td>
<td>64</td>
</tr>
</tbody>
</table>

## DNS servers for JavaScript-delivery hosts

<table>
<thead>
<tr>
<th>Resolved hostnames</th>
<th>619</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses</td>
<td>147</td>
</tr>
<tr>
<td>ASes</td>
<td>67</td>
</tr>
<tr>
<td>BGP prefixes</td>
<td>115</td>
</tr>
<tr>
<td>Countries</td>
<td>11</td>
</tr>
</tbody>
</table>
Data on Infected Web Servers (1/2)

- Data collection
  - Searched web pages containing the URLs pointing to the malicious JavaScript delivery hosts
    - Used Google and Yahoo search APIs
  - Examined web pages in search results, including the cached pages

- Web-server classification in the search results
  - Infected but unreachable
  - Infected, reachable, but undecidable
  - Infected, reachable, and identifiable
**Data on Infected Web Servers (2/2)**

- **Data collection period**
  - 11/01/2008 ~ 01/31/2009 (92 days)

<table>
<thead>
<tr>
<th>Class</th>
<th># of Servers</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # of infected web servers</td>
<td>8,926</td>
<td>100%</td>
</tr>
<tr>
<td>Infected but unreachable</td>
<td>2,751</td>
<td>30.82%</td>
</tr>
<tr>
<td>Infected, reachable, but undecidable</td>
<td>1,141</td>
<td>12.78%</td>
</tr>
<tr>
<td>Infected, reachable, and identifiable</td>
<td>5,034</td>
<td>56.40%</td>
</tr>
</tbody>
</table>
Outline

- Introduction
- Data Collection & Overview
- Analysis of Asprox Infection Dynamics
  - Asprox Bots
  - JavaScript-Delivery Hosts
  - Infected Web Servers
- Concluding Remarks
Analysis of Asprox Bots

- The number of attacking bots is lesser on weekdays than weekends
  - Artifact of the fact that many bots are residential machines
- New bots are added to the pool as the week progresses, with peaks on Saturdays
- Modest number (up to 3,000) of bots are being reused
  - More bots are reused on weekend like the trend of the new bot addition
Attack Times by Asprox Bots

- Asprox bots attacking on a **weekend** day (8/9)
- Asprox bots attacking on a **weekday** (8/20)
Active Lifetime and Repeated Attacks

- Around 95% of attacking bots were observed for less than 2 days
  - Helps avoid any IP blacklisting
- Over 50% of web servers were continuously attacked for 8 days
- 90% of the bots attacked the same web server about 10 times
  - In some cases, one attacker hit the same target over 500 times
Geographical Distribution of Asprox Bots

36.68% of the attacking bots
JavaScript-Delivery Hosts

- Only 27 out of 55 JavaScript delivery hosts were actively used during our data collection period.
- Among the 27 JavaScript delivery hosts, 58% of them appear to be actively fluxing.
- One example, www.berkje.ru
  - 1,542 IP addresses
  - Geographically spread through 60 countries
# of IP addresses and IP diversity for www.berkje.ru
Geo. Dist. of IPs of JavaScript-Delivery Hosts

Legend: # of IPs
- : 1
- : 2 ~ 100
- : 101 ~ 1000

65.9% of JavaScript-Delivery hosts
## Infected Web Servers

- **TLDs of infected web servers**

<table>
<thead>
<tr>
<th>TLD</th>
<th>Number of web servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>2,307</td>
</tr>
<tr>
<td>.pl</td>
<td>341</td>
</tr>
<tr>
<td>.net</td>
<td>313</td>
</tr>
<tr>
<td>.org</td>
<td>294</td>
</tr>
<tr>
<td>.cn</td>
<td>242</td>
</tr>
<tr>
<td>.kr</td>
<td>201</td>
</tr>
<tr>
<td>.uk</td>
<td>125</td>
</tr>
<tr>
<td>Other gTLDs</td>
<td>105</td>
</tr>
<tr>
<td>Other ccTDLs</td>
<td>1,070</td>
</tr>
<tr>
<td>No server name, just IP address</td>
<td>36</td>
</tr>
</tbody>
</table>

**Total Number of web servers** 5,034
Infected Web Servers

- 77% of the servers were cleaned and the rest stayed infected during our collection period.

- Cleaned web servers
- Still infected web servers
Conclusion

- Asprox botnet continues to grow and infect web servers around the world

- Passive monitoring such as Honeypot is not sufficient
  - to understand the attack in its entirety or
  - to detect changes or modifications to the final vulnerabilities used to attack users’ machines or the malware payload delivered

- Adopting the mitigation for the SQL injection attacks would take a long education cycle
Questions?
shiny@cs.indiana.edu