A Case Study on Asprox Infection Dynamics

Youngsang Shin[1], Steven Myers[2], Minaxi Gupta[1]

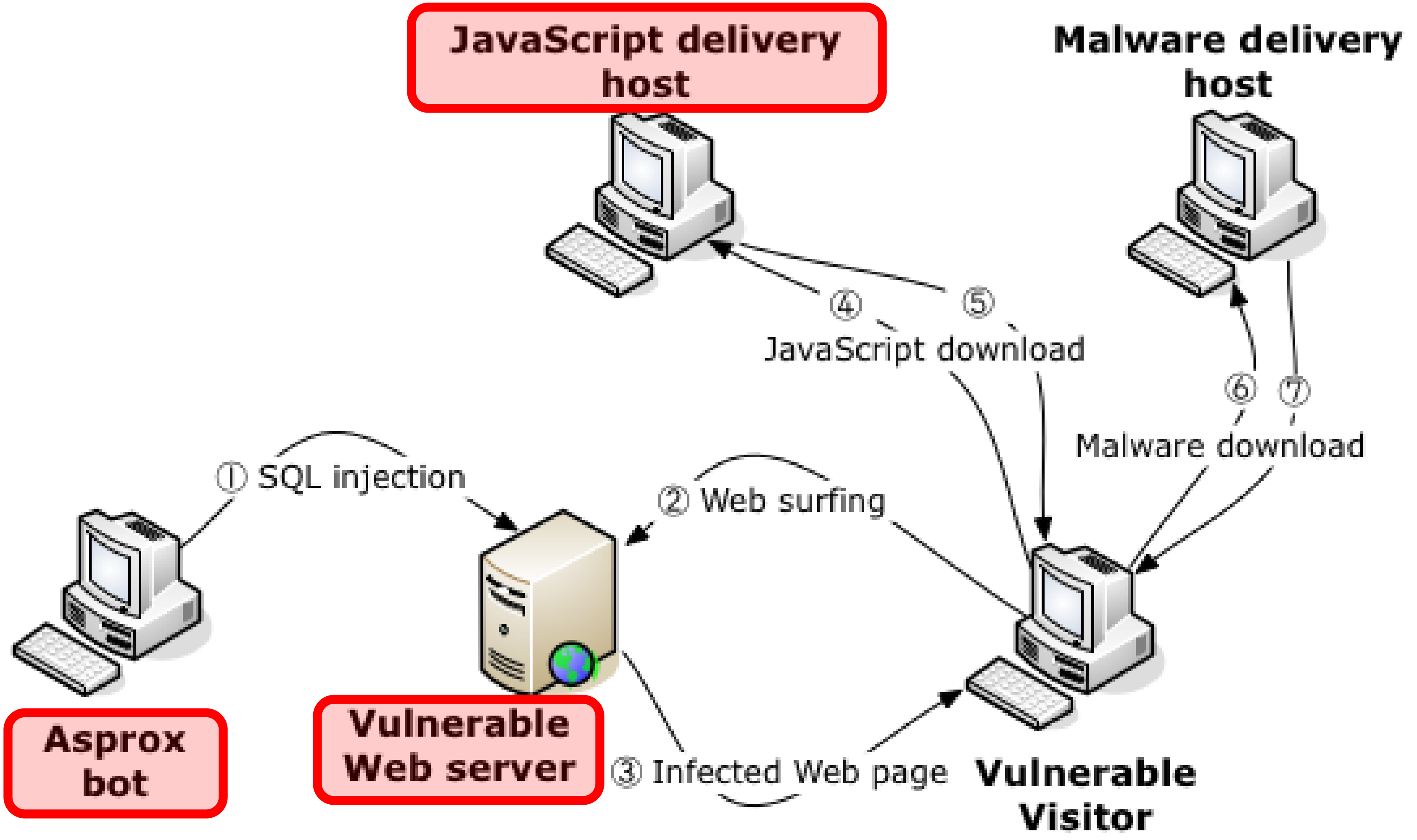
[1] School of Informatics and Computing, Indiana University
{shiny, minaxi}@cs.indiana.edu
[2] School of Informatics and Computing, Indiana University
samyers@indiana.edu

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



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

Collection Period	8/9/2008 ~ 8/25/2008 (17 days)
Unique IP addresses of attacking bots	57,419
Autonomous systems attackers belonged to	1,847
Web servers targeted	581

Data on JavaScript-Delivery Hosts

- JavaScript-delivery hosts

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

- JavaScript-delivery hosts

Resolved hostnames	**55**
IP addresses	**2,214**
ASes	308
BGP prefixes	898
Countries	64

- DNS servers for JavaScript-delivery hosts

Resolved hostnames	**619**
IP addresses	**147**
ASes	67
BGP prefixes	115
Countries	11

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)

Class	# of Servers	%
Total # of infected web servers	8,926	100%
Infected but unreachable	2,751	30.82%
Infected, reachable, but undecidable	1,141	12.78%
Infected, reachable, and identifiable	**5,034**	**56.40%**

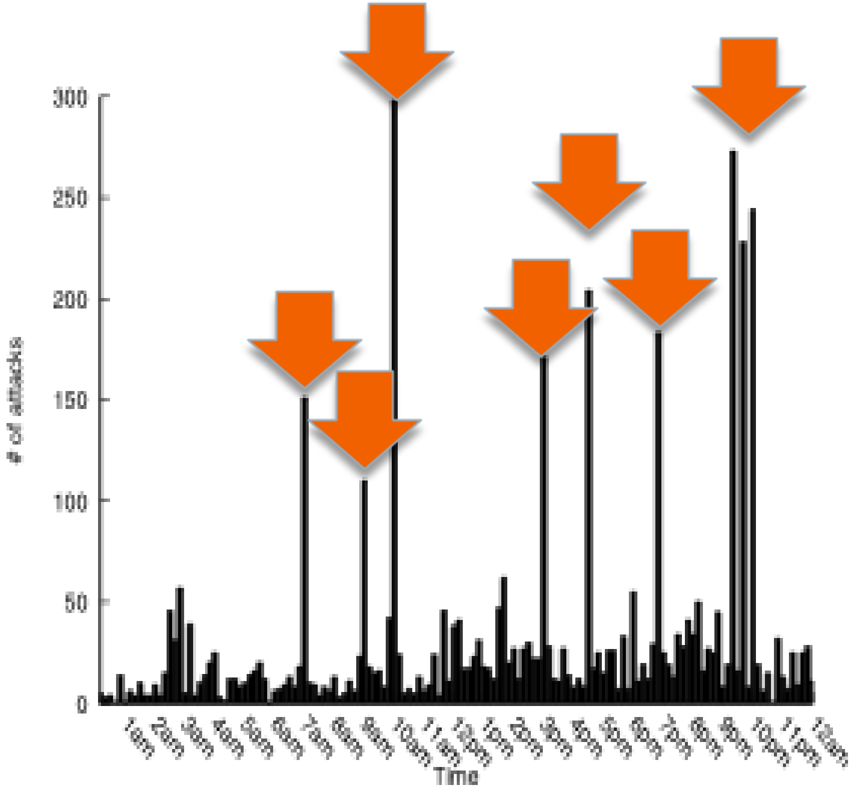
Outline

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

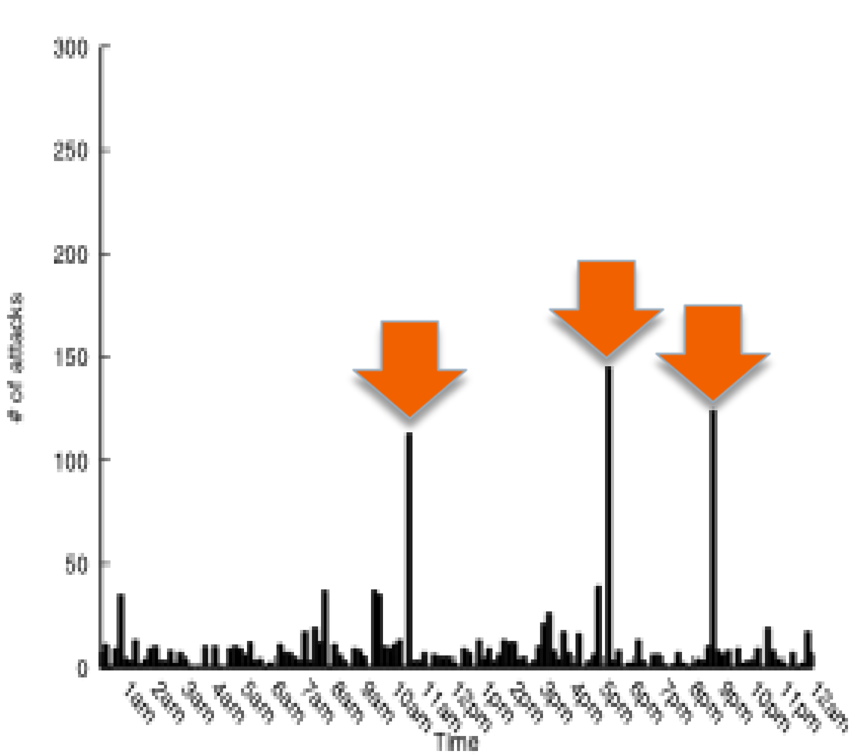
Analysis of Asprox Bots

- 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)

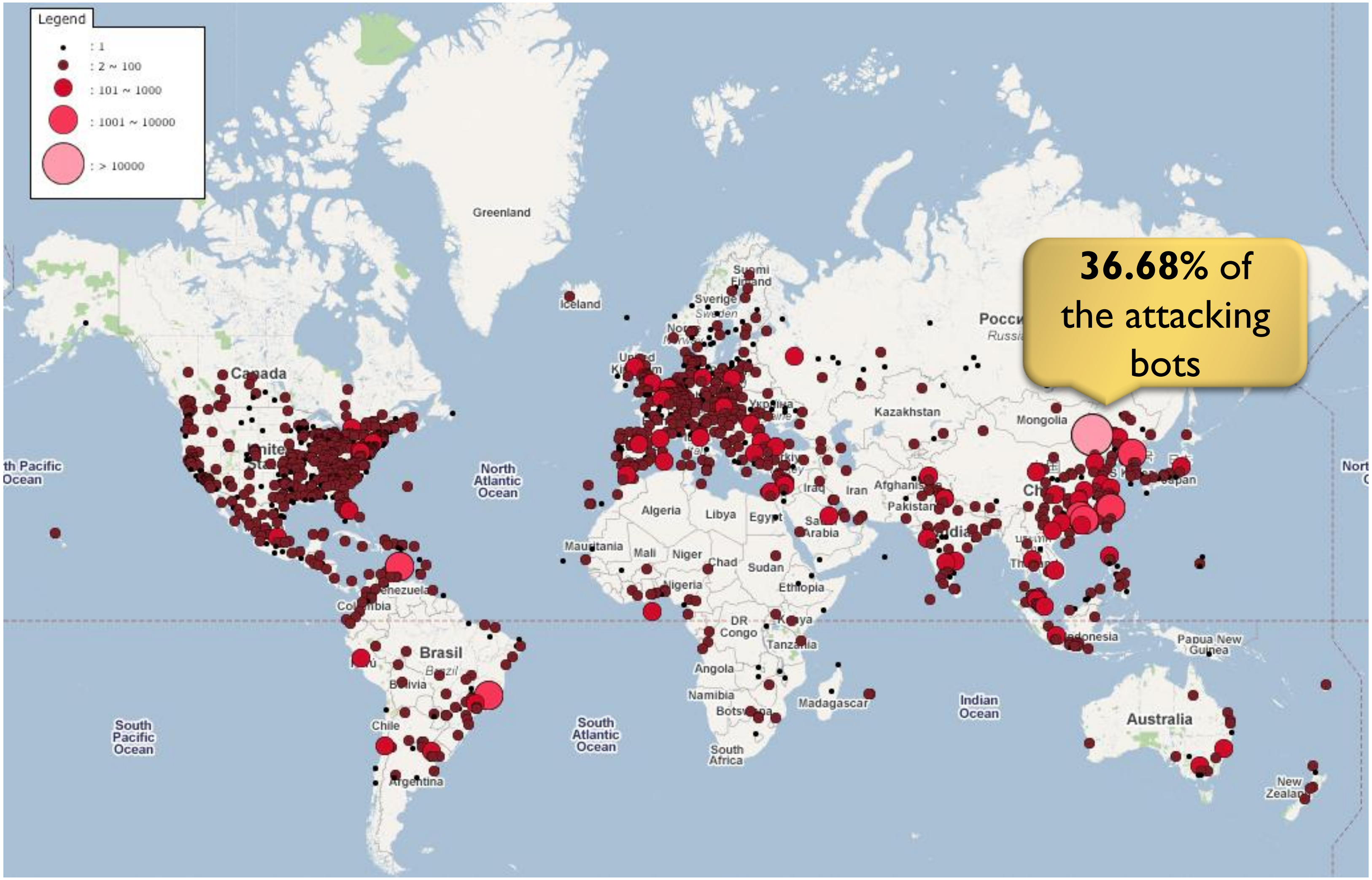


- Asprox bots attacking on a **weekday** (8/20)

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

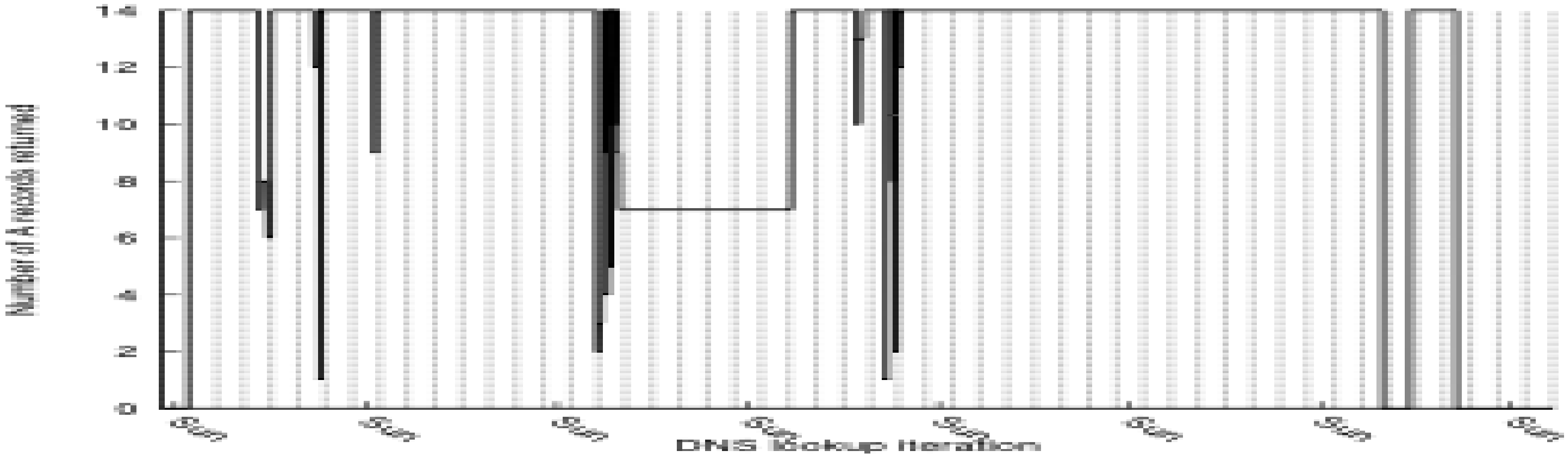


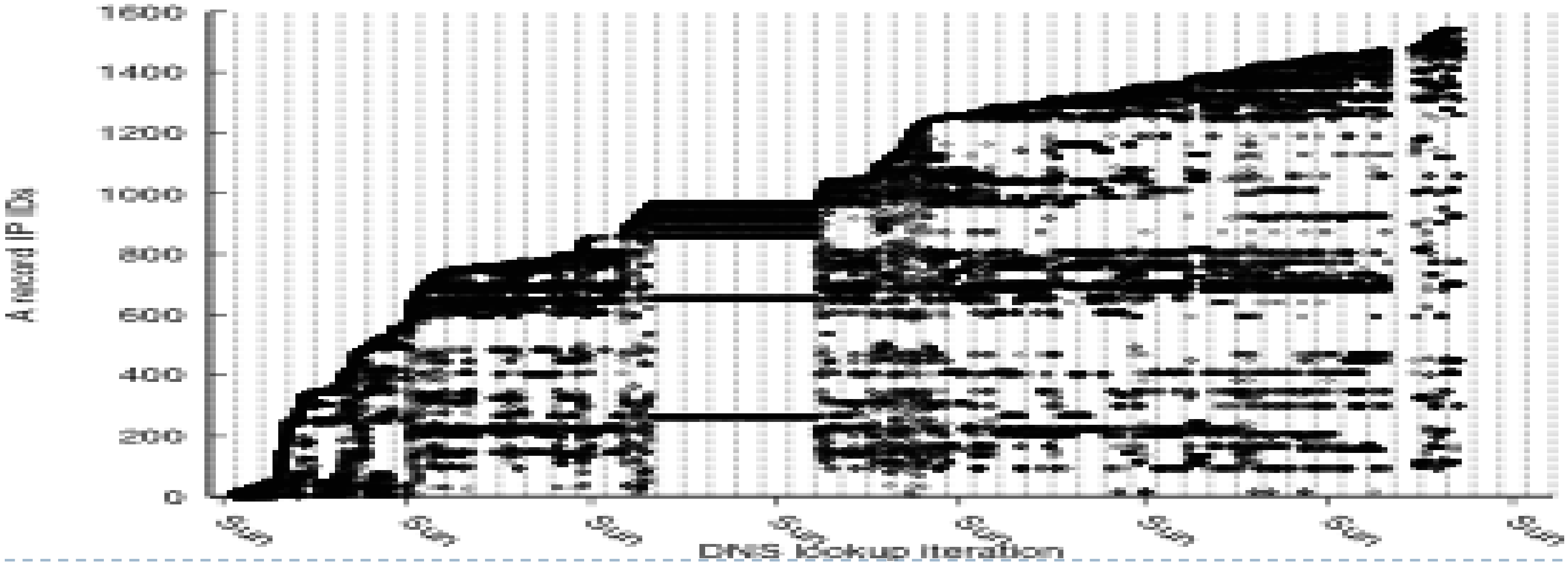
36.68% of the attacking bots

JavaScript-Delivery Hosts

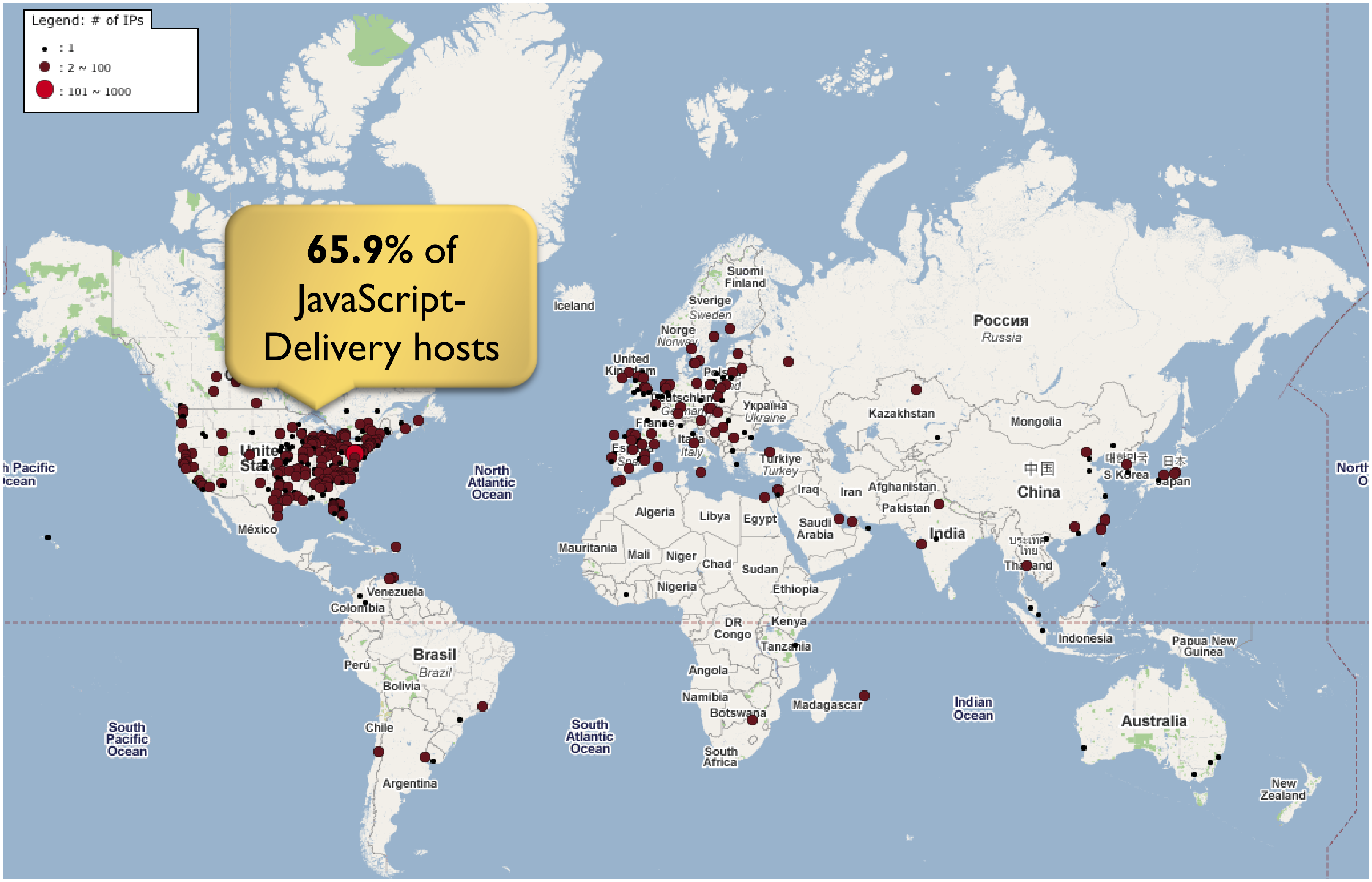
- Only 27 out of 55 JavaScript delivery hosts were actively used during our data collection period
- Among the 27 JavaScript delivery hosts, 58% of them appear to be actively fluxing.
- One example, **`www.berkje.ru`**
  - 1,542 IP addresses
  - Geographically spread through 60 countries

# of IP addresses and IP diversity for `www.berkje.ru`





Geo. Dist. of IPs of JavaScript-Delivery Hosts



65.9% of JavaScript-Delivery hosts

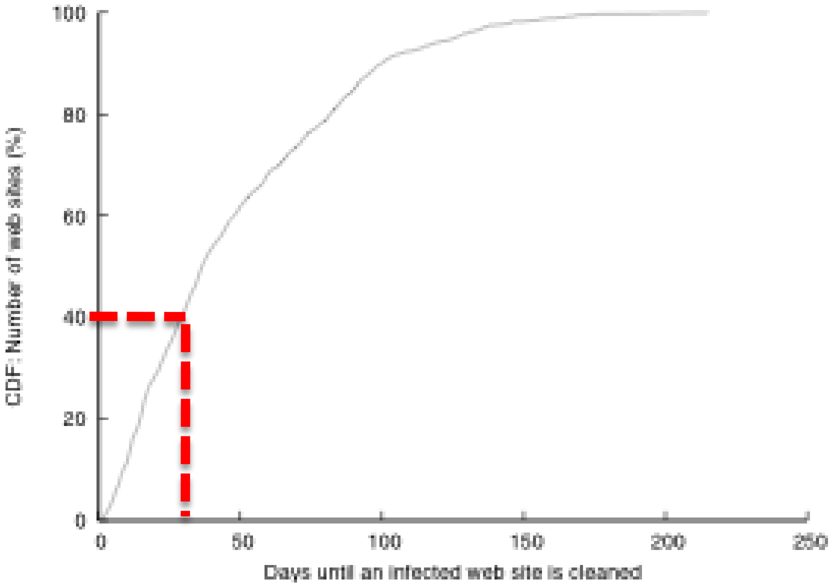
Infected Web Servers

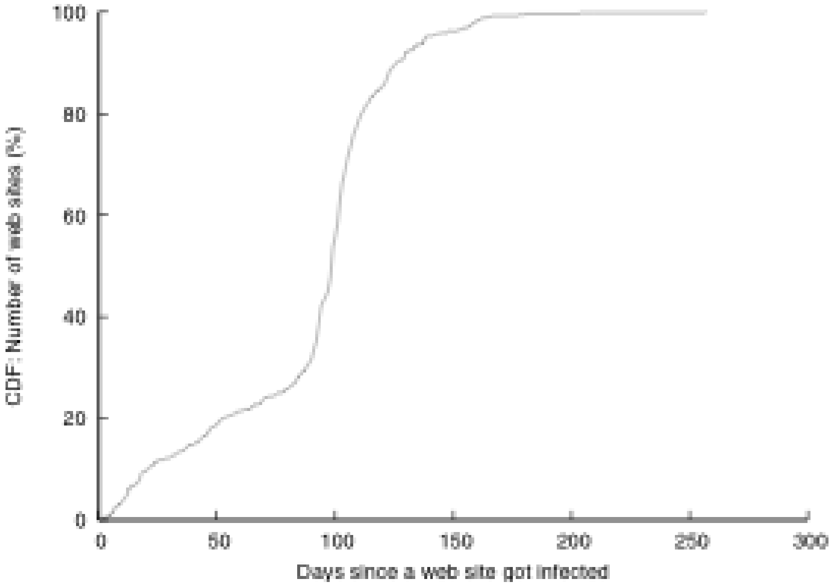
- TLDs of infected web servers

TLD	Number of web servers
.com	**2,307**
.pl	341
.net	313
.org	294
.cn	242
.kr	201
.uk	125
Other gTLDs	105
Other ccTDLs	1,070
No server name, just IP address	36
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