Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Types of hosts on a Remote File Inclusion(RFI) botnet

Hugo **F**rancisco **G**onzález **R**obledo
hugo.gonzalez@upslp.edu.mx

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

About me ...

- Professor at Universidad Politécnica de San Luis Potosí
- ACM
- IEEE
- The Honeypot Project
- Free and open source software
- Security

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

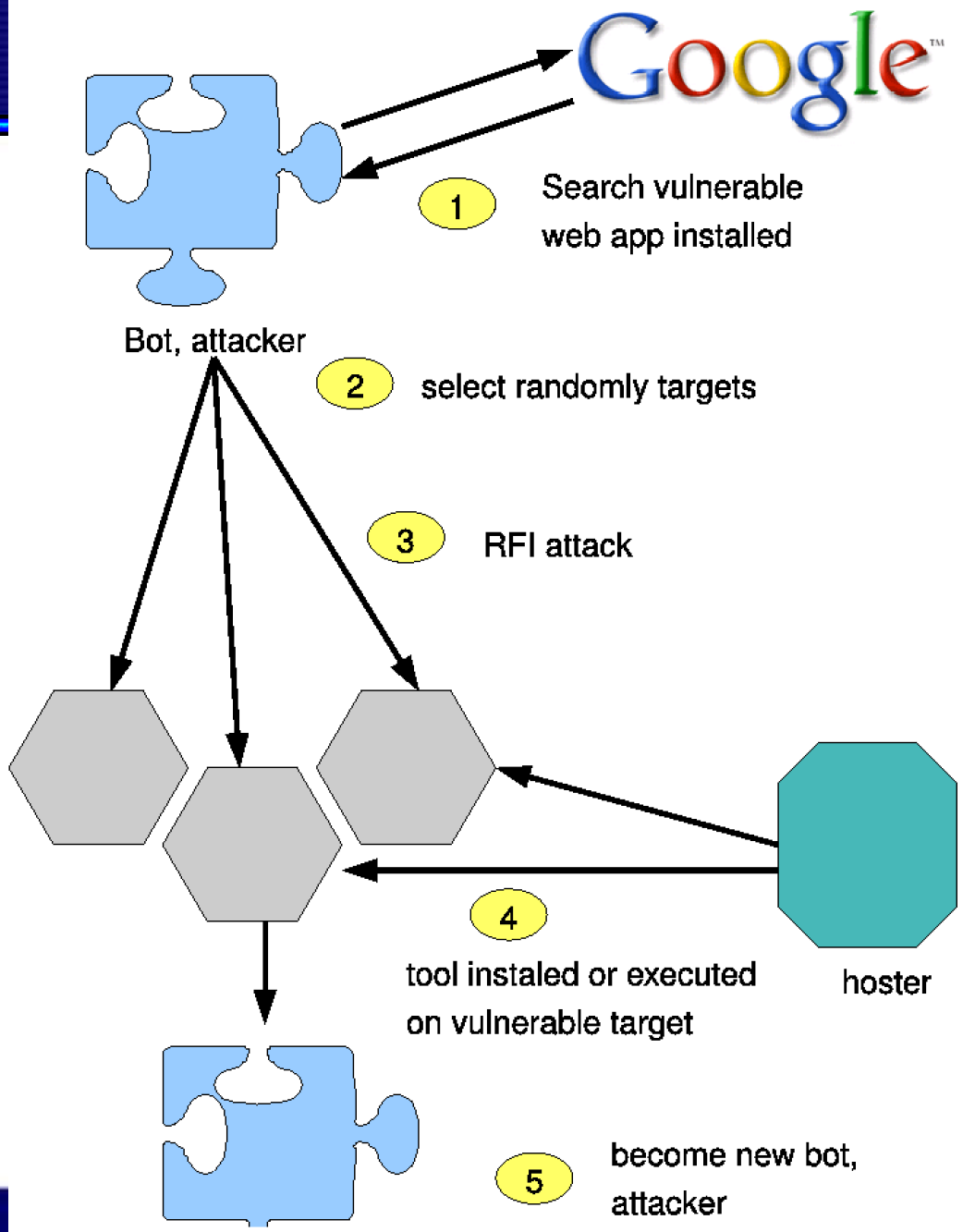
Agenda

- Context and definitions.
- Question work.
- Procedures.
- Results
- Conclusions.
- Future work

Context

- Botnets
- Web security and web attacks
  - SQL injections
  - Code inclusion
  - Cross site scripting (XSS)
  - Remote File Inclusion (RFI)

Behaivor of a bot in RFI attacks



UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Question !!!!

Are the attackers on a RFI botnet a compromised web servers ????

Procedures

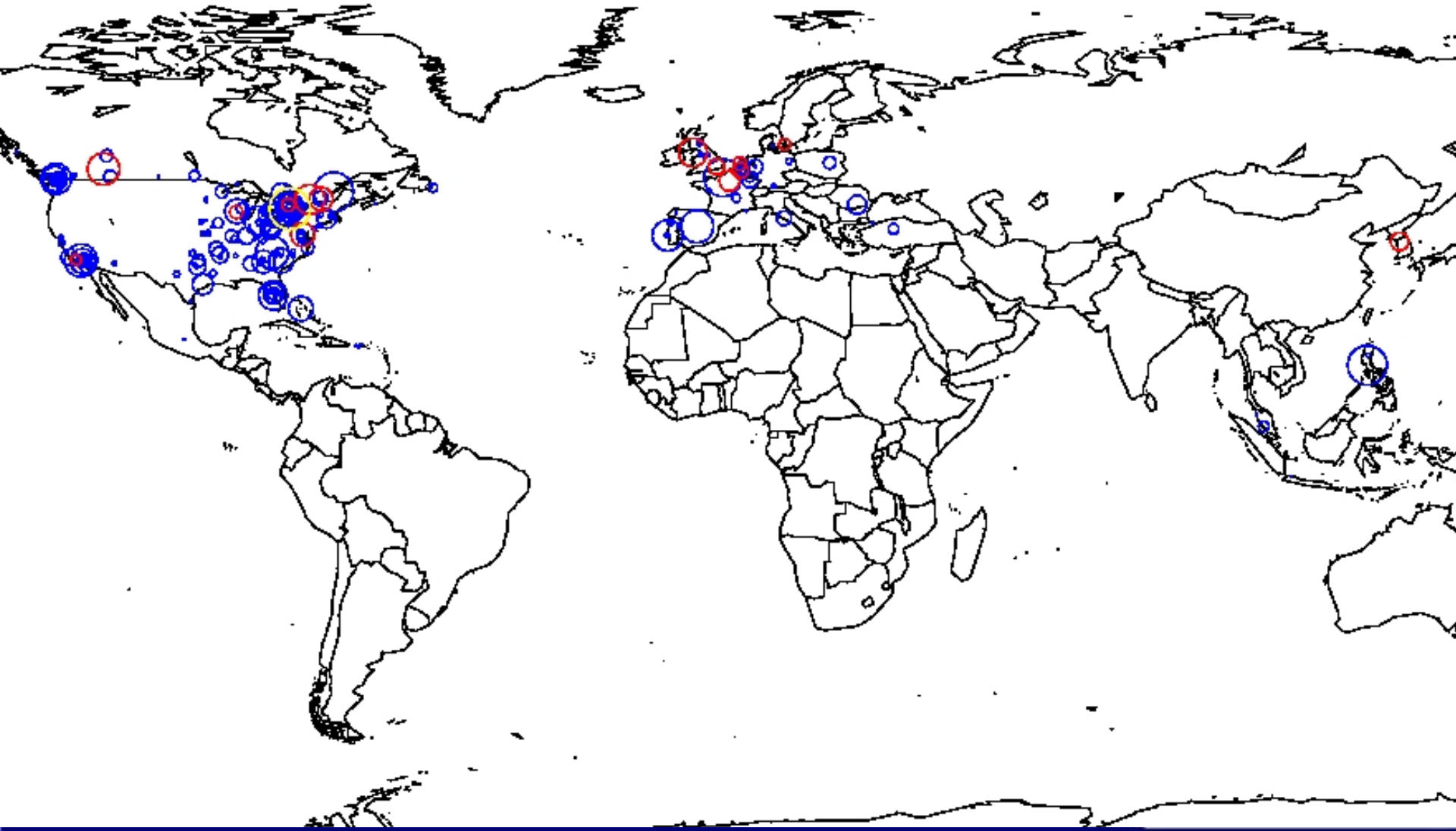
- Track the botnet trought web server logs (since 2 years ago)
- Select one of the larger botnet, by time and hosts
- Track the ip's
- Analize them by:
  - nslookup and active services

Results

- In a time slice of 100 days, 837 bots and 1628 attacks
  - Attacking and *index.php* file
  - The tool use is *cs.txt*
    - Is a php shell, using exec, shell_exec, passthru commands to execute post method instructions

UNIVERSIDAD POLITÉCNICA

DE SAN LUIS POTOSÍ



- The bots ARE NOT web servers.
- Almost all are computers connected by ADSL to Internet and NO have web, smtp or other service available.
- The hosters are public web servers, but the tool are blocked now
  - This attacks ends in noisy and unwanted traffic.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Result methodology

- Analize web server logs looking for patern of attack like =[fh]t.
- Extract the info about attacker, hoster, date and tool. Log in a database.
- Try to get the source of the tool, keep the tool and log it.
- Reverse dnslook for the attacker, log it.
- Whois for the attacker, log it.
- Search ubication in geolocation database, log it.
- Group the data about hoster and attacker, tool and ips.

Conclusion

- There are a lot of attacks
- Diferent types of botnets
- Noisy traffic
- No way to prevent the query, we can block it.

Future work

- Tracking botnets.
- Improve the methodology for do it in automatic way.
- Make it public and free to consult or add data.
- Detect and black list compromised hosts.

Questions

Questions