This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/

Hugo González

@hugo_glez

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

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Ataques de inclusión de archivos remotos a servidor web

Hugo Francisco González Robledo
hugo.gonzalez@ieee.org

Agenda

- Antecedentes
- Tipos de ataques
- Métodos
- Resultados
- Conclusiones
- Trabajo a futuro

Resumen

- Se analizan los ataques RFI recibidos por un servidor web universitario durante un año.
- Se presenta el comportamiento de los ataques y se situan en el mapa los atacantes.
- Se supone la organización de los ataques en botnes, que son analizadas en un trabajo posterior.

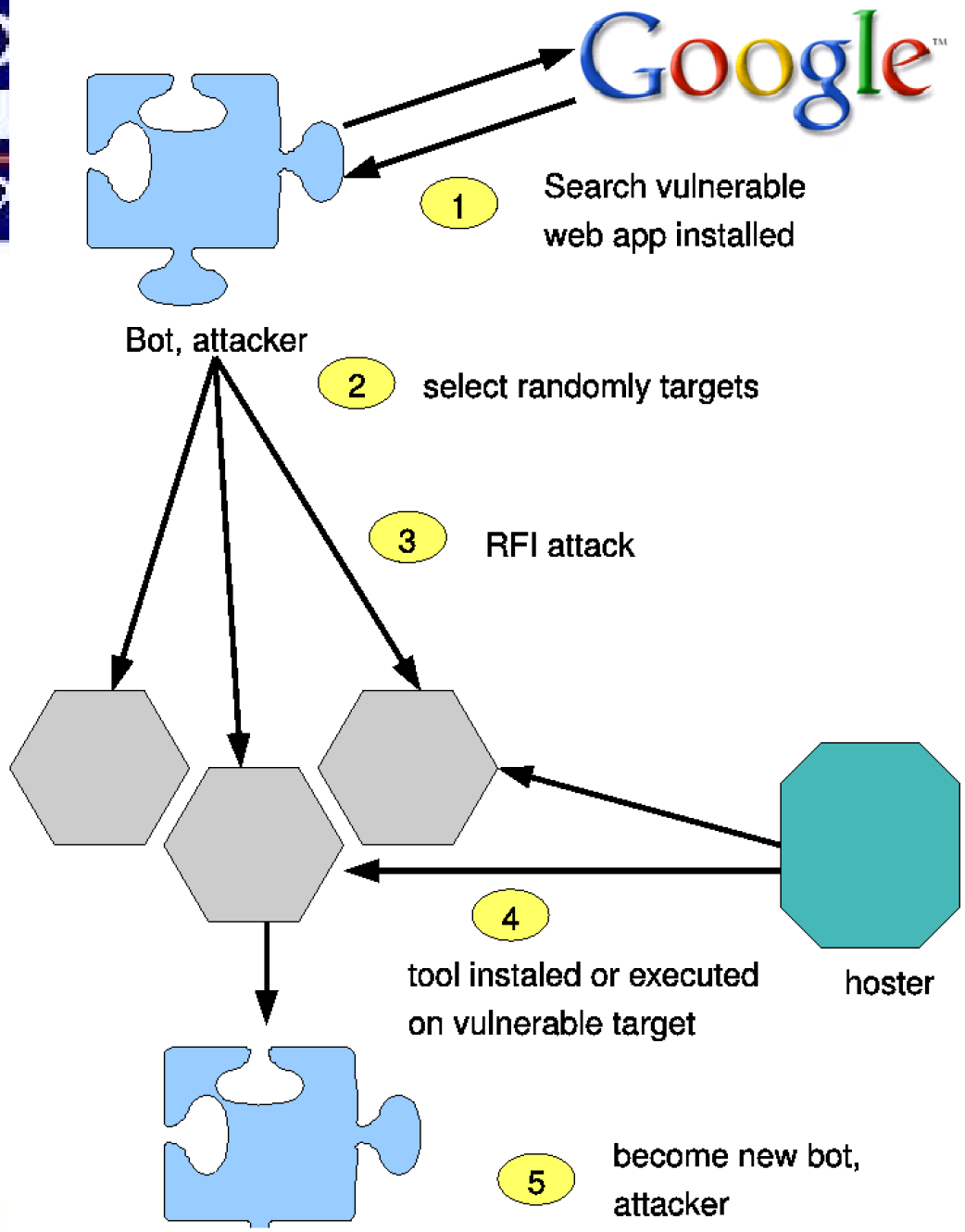
Antecedentes

- La aparición de virus, gusanos, troyanos y malware en general ha ido aumentando en los últimos años en Internet.
  - Code Red, Nimda (2001)
  - SQL Slammer (2003)
  - Otros
- Es importante conocer al enemigo para poder luchar contra él.
- La tendencia actual son los ataques a las aplicaciones web.

Tipos de ataques

- Inyección de SQL
- Inyección de código
- XSS
- Inclusión de código remoto

Behavior of a bot in RFI attacks



Comportamiento RFI

- Probar la vulnerabilidad del sitio.
- Modificar la página principal del sitio.
- Shell web para controlar el servidor.

- Suponemos organización de botnets para realizar estos ataques.
- Los ataques se realizan de manera aleatoria.

Datos

- Registros de Enero 2007 a Enero 2008

200.146.192.105 - - [13/Jan/2008:06:26:30 -0600] ”GET /index2.php?option=com rss&feed=RSS1.0&no html=1 HTTP/1.0” 200 3187 ”-” ”-”

Análisis exploratorio

1. Se extrajeron los datos de los ataques de inclusión de código remoto unicamente.
2. Se alojaron los datos en un sistema de gestión de base de datos MySQL
3. Se utilizó SQL y el paquete R para obtener la información estadística y los mapas presentados en la sección de resultados.
4. Con esta información y las graficas de los datos se exploran los hallazgos para presentar los resultados y conclusiones.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Máximos registrados

	Unicos	mensual		diario	
Hits	13296	Nov	2886	9 Dic	311
Ips	4342	Nov	952	27 Nov	112
Herramienta	1537	Nov	305	1 Sep	120
Dirección	390	Sep	143	1 Sep	114
Vulnerabilidad	791	Nov	293	6 Dic	91
Agente	56	Dic	39	5 Nov	17

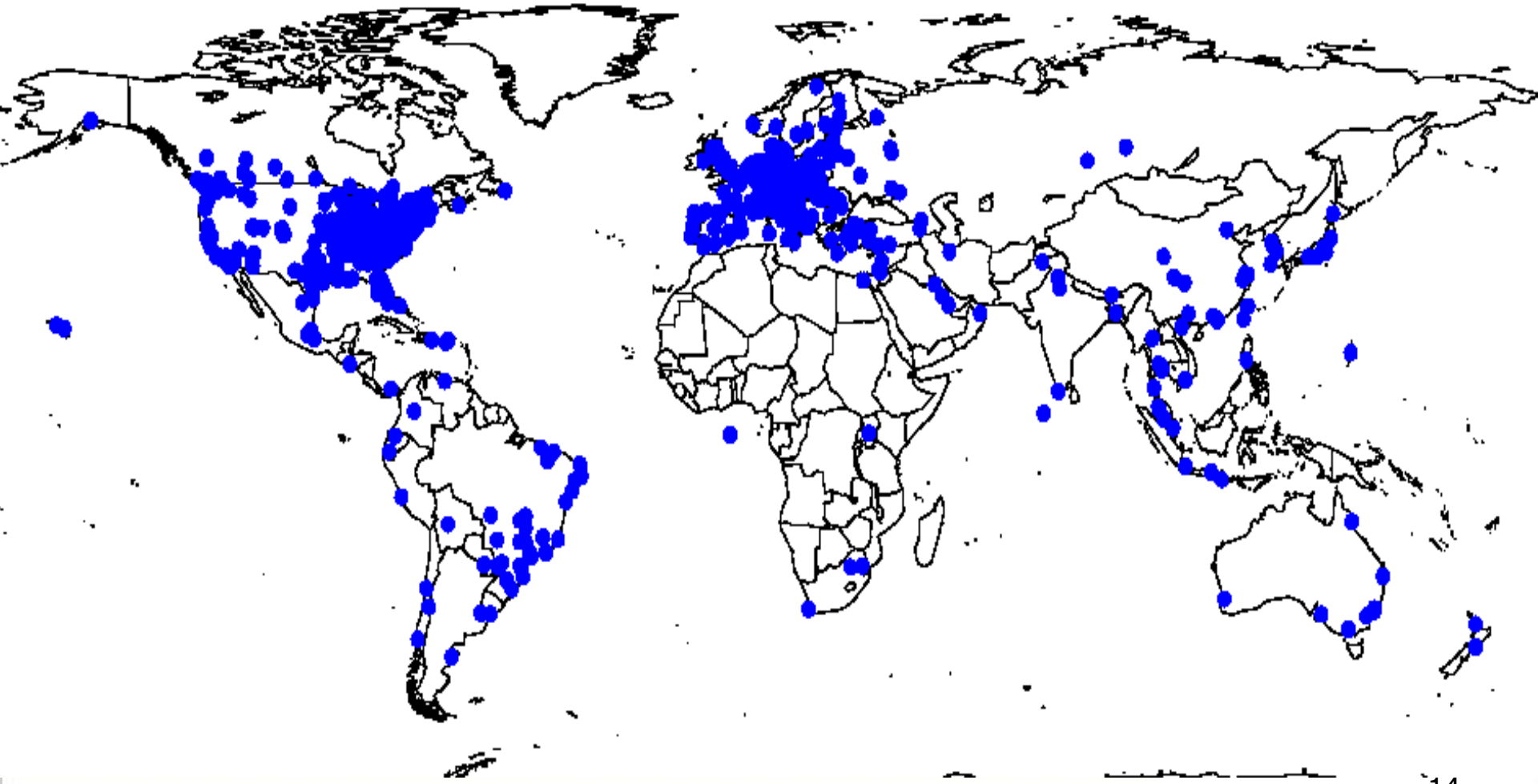
dias	herramientas	Hits/ip	hits/Ip
1	1019	108/1	26/25
2	264	260/27	90/45
3	119	108/44	
4	39	441/38	
5	20	192/19	99/37
6	23	305/64	
7	6	31/24	
8	8	178/39	
9	4	22/11	
10	6	52/11	33/22

11	4	238/18	117/57
12	1	98/22	
13	4	474/115	
14	2	61/36	54/37
15	2	35/24	
16	4	222/74	202/83
17	1	31/19	
18	2	74/55	
19	1	31/11	
20	1	110/57	

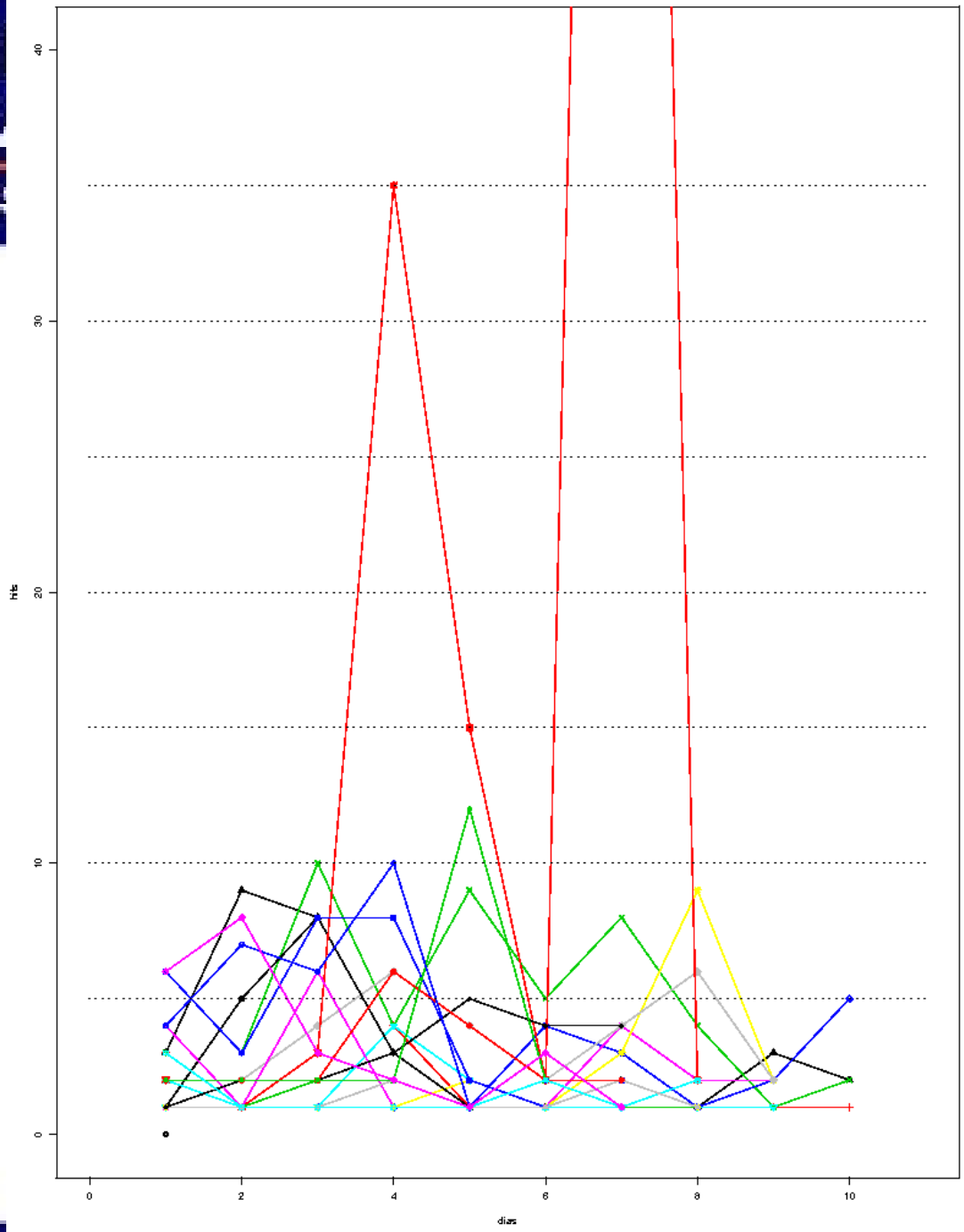
22	2	556/29	47/38
27	1	183/44	
34	1	257/56	
39	1	84/37	
68	1	332/152	
85	1	722/423	

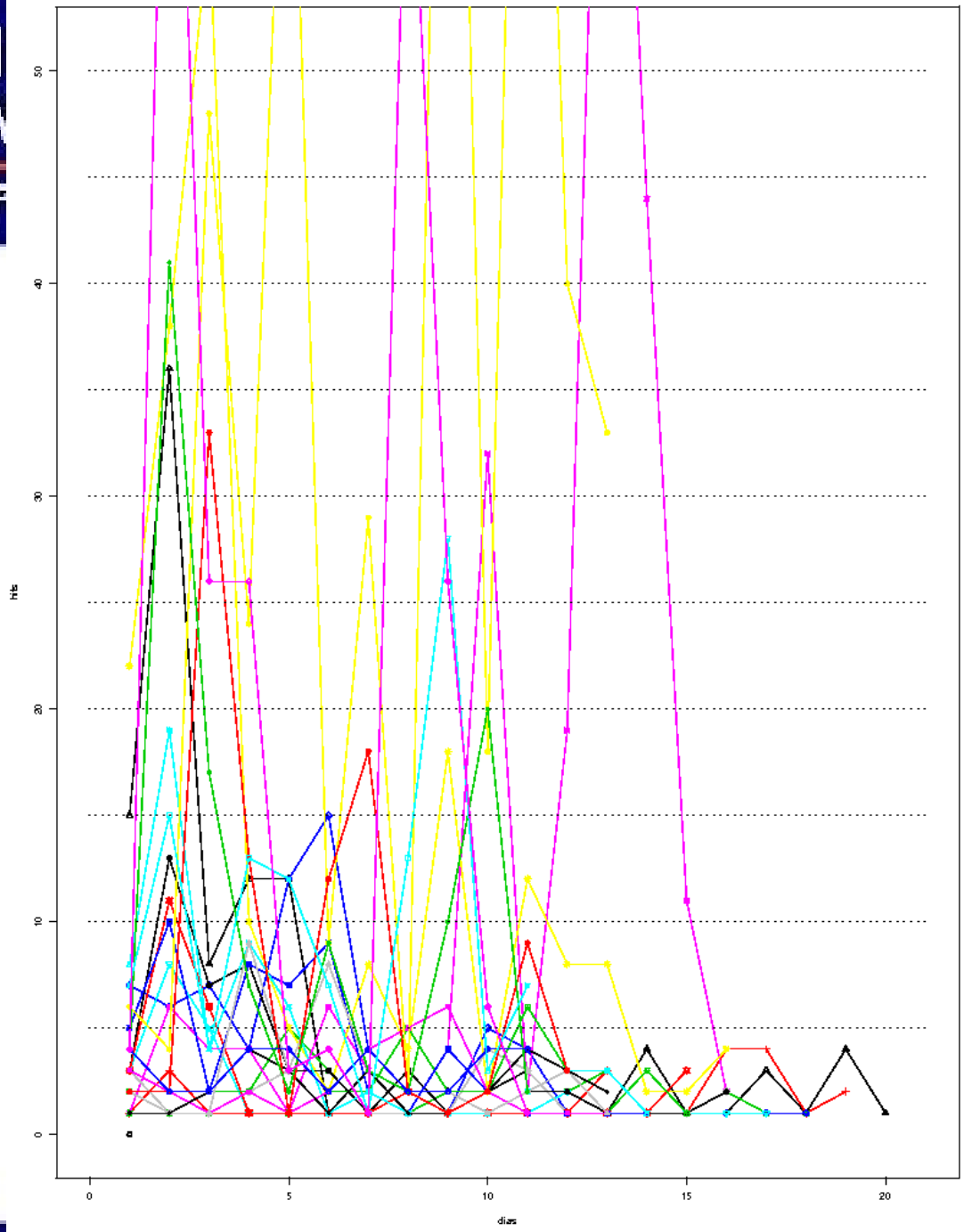
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

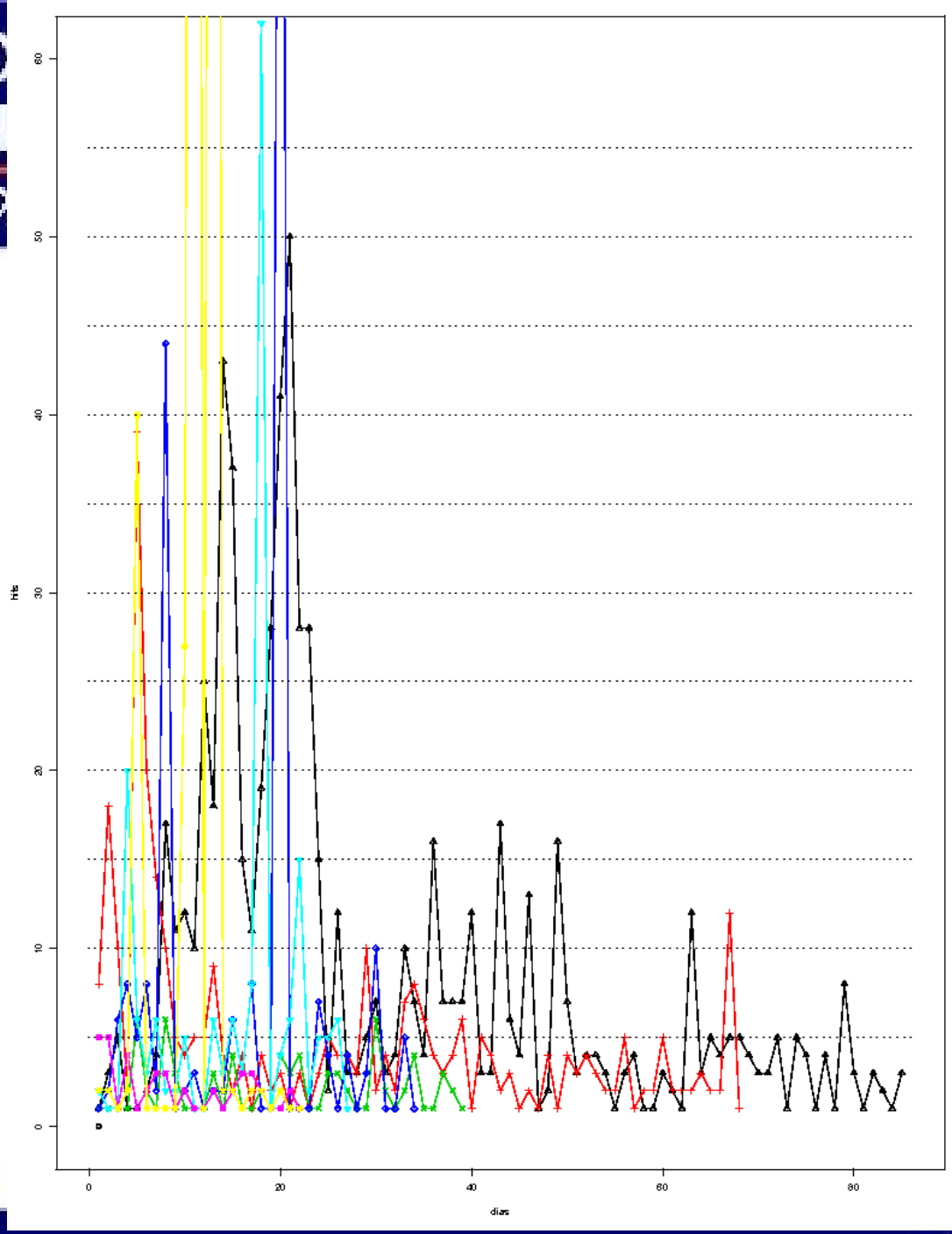
Distribución Mundial



UNIVERSIDA
POLITÉCNIC
DE SAN LUIS POTO




Hits
0
10
20
30
40
50
0
5
10
15
20
dias


Hits
0
10
20
30
40
50
60
0
20
40
60
80
dias

Conclusiones

- No hay relación directa entre fechas o ataques.
- El comportamiento es parecido, aumenta al principio y luego disminuye hasta desaparecer
- La costa este de estados unidos y europa son los lugares de donde provienen mayor cantidad de ataques.
- Tiempo de vida máximo de 5 meses.

Trabajo a futuro

- Analizar las botnets relacionadas
- Tipos de equipos pertenecientes a estas botnets
  - Resultados diversos, no solo servidores web comprometidos son atacantes
  - Metodología para detectarlos
- Analizar herramientas utilizadas en los ataques.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Preguntas

hugo.gonzalez@ieee.org