Tracking DDoS Attacks
Insights into the Business of Disrupting the Web

Armin Buescher, Websense Security Labs
Thorsten Holz, Ruhr University Bochum

5th USENIX Workshop on Large-Scale Exploits and Emergent Threats

LEET '12

Botnets, Spyware, Worms, New Emerging Threats, and More

APRIL 24, 2012
SAN JOSE, CA

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

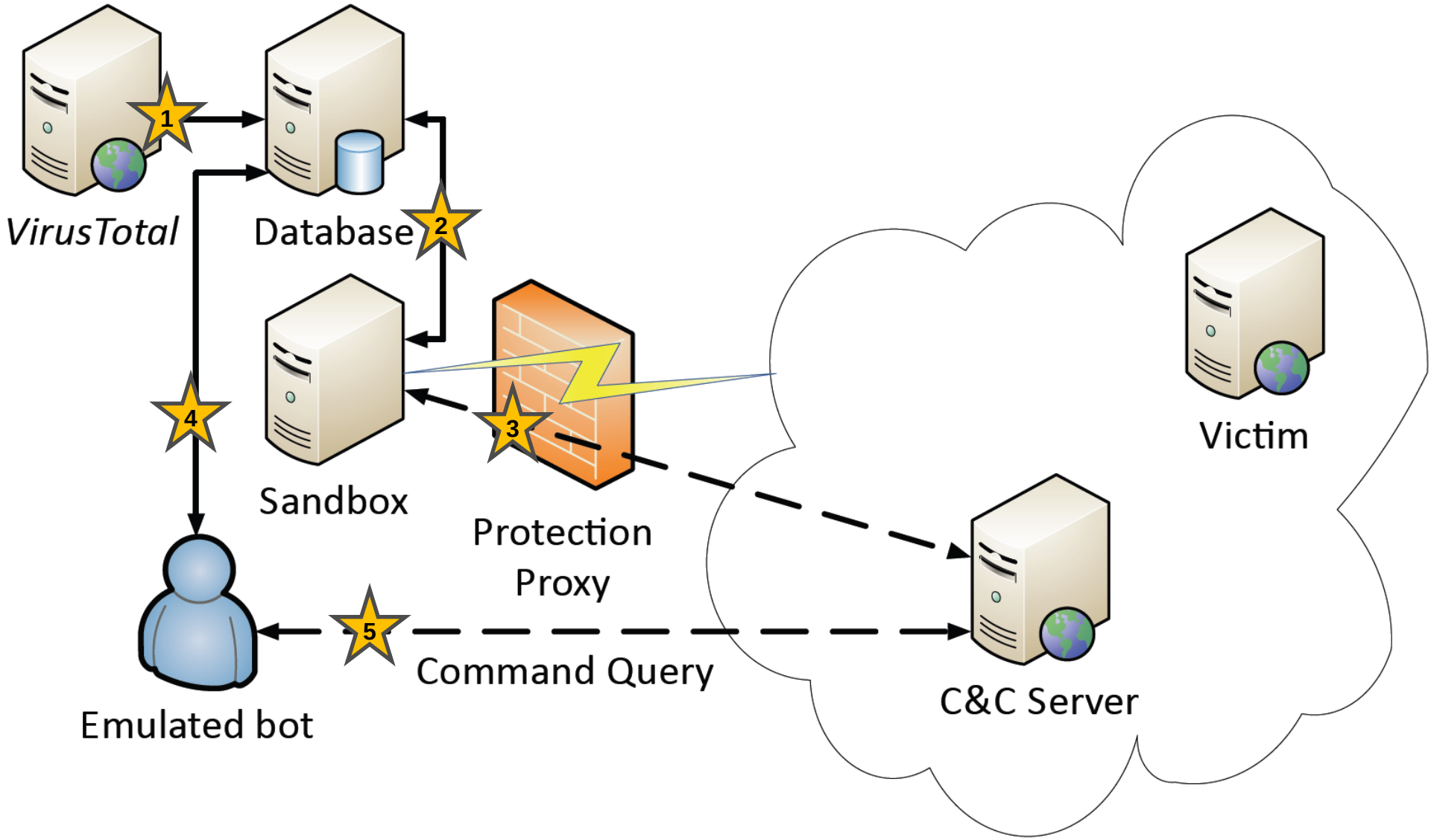
DDoS in today's Internet landscape

- Instruments
  - ***Botnets (Cybercrime)***
  - Volunteers (Hacktivism)
- Attacked technologies
  - Network layer
  - Transport layer
  - ***Application layer***
- Impacts of service downtime
  - Business - Revenue loss
  - Information - Silence

Motives for DDoS attacks

- Blackmail service operators
- Disrupt the competition
- Disrupt adversaries
- Manipulate services
- Political protest

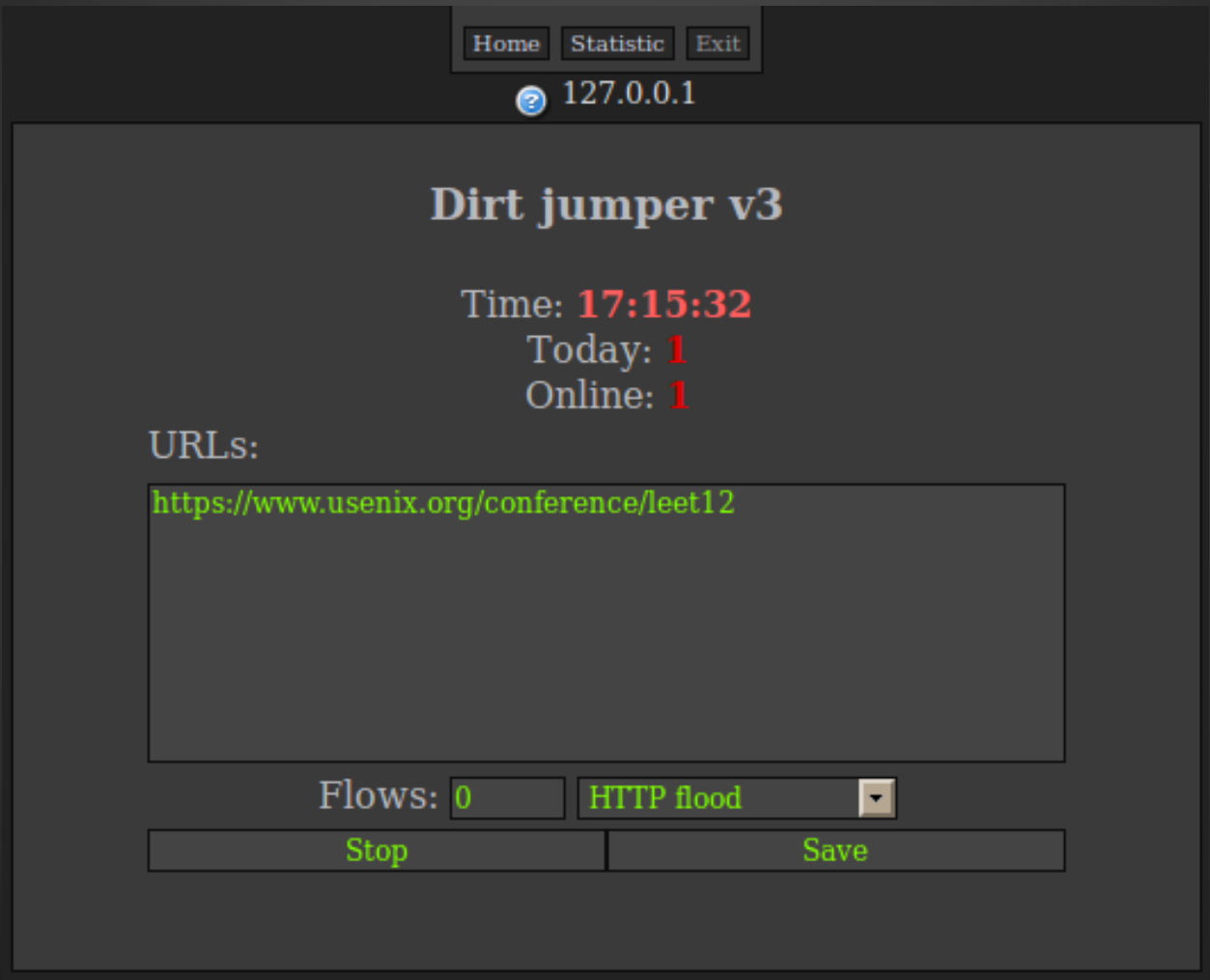
Automated C&C monitoring



Dirt Jumper (DJ)

- Crimeware Kit
  - Successor of ***Ruskill*** (2009) DDoS bot
  - Sold in Underground forums
  - Leaked/Pirated in Underground forums
  - Several versions:
    - ***DJ v1-v3***
    - ***DJ September***
    - ***DJ v5*** (first seen Oct 2011)
    - (***Pandora***)
  - Unencrypted C&C traffic

DJ Panel


Home
Statistic
Exit
127.0.0.1
Dirt jumper v3
Time: 17:15:32
Today: 1
Online: 1
URLs:
https://www.usenix.org/conference/leet12
Flows: 0
HTTP flood
Stop
Save

DJ C&C HTTP Request

```
POST /index.php HTTP/1.0
Host: ***C&C***.com
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1)
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

k=807789926667168
```

DJ C&C HTTP Response

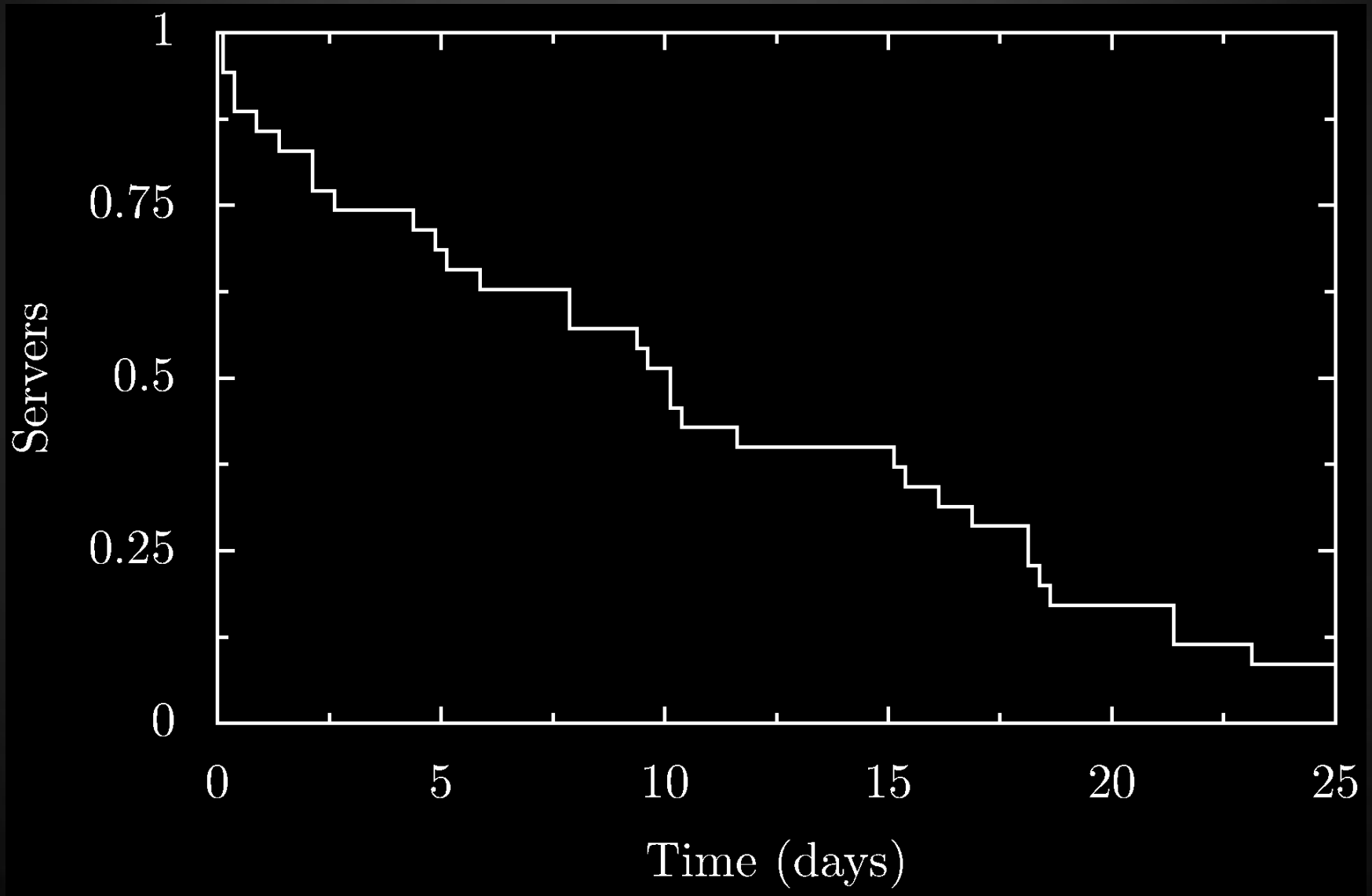
```
HTTP/1.1 200 OK
Date: Thu, 02 Feb 2012 21:33:48 GMT
Server: Apache
X-Powered-By: PHP/5.2.17
Vary: Accept-Encoding,User-Agent
Content-Length: 30
Connection: close
Content-Type: text/html

01|50|60http://***VICTIM***.com
```

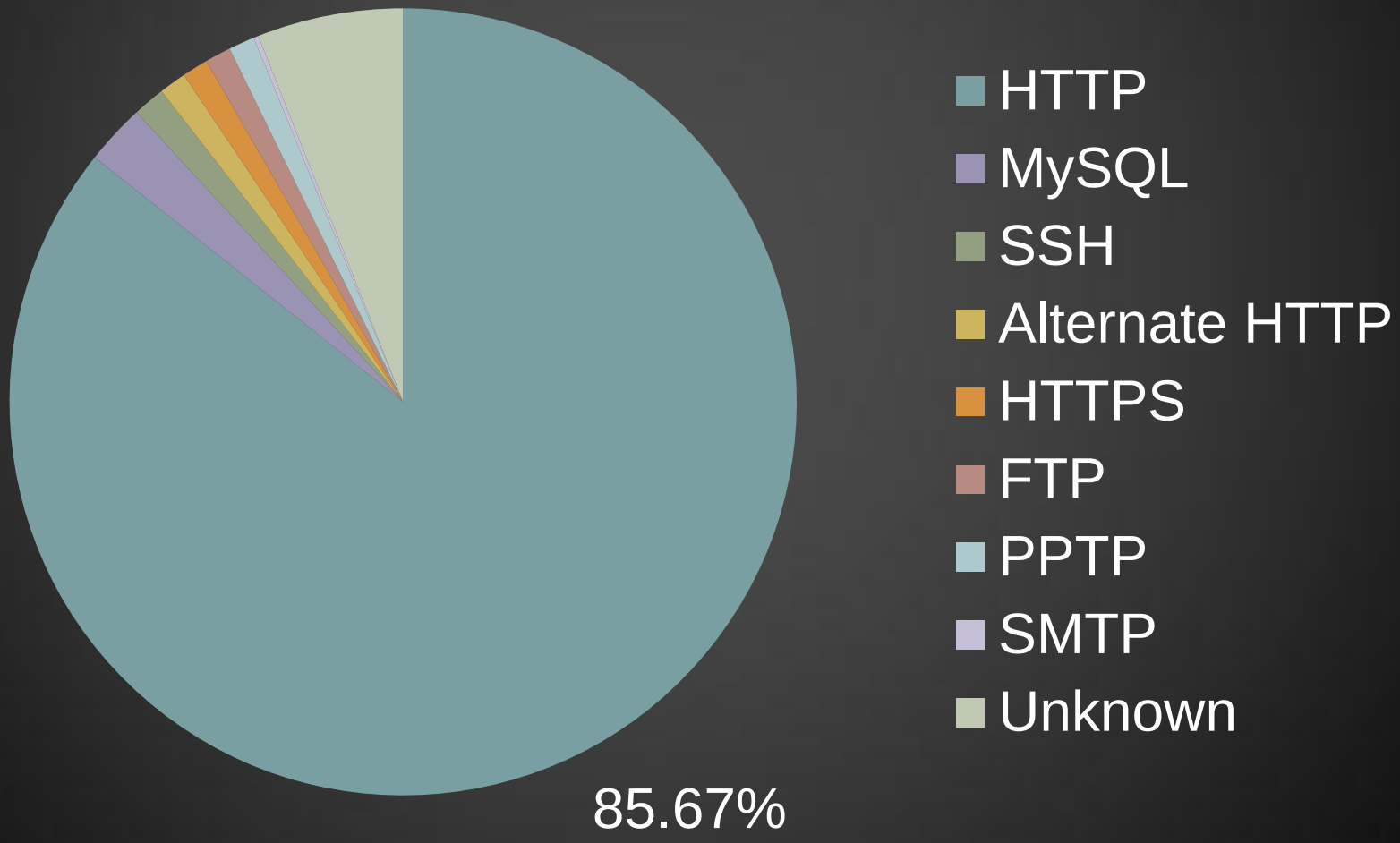
DJ Monitoring

- Monitoring C&C commands over four months (Oct '11 - Jan '12)
- Dirt Jumper malware sample set
  - 465 samples
  - 274 samples showed DJ C&C traffic
- 68 unique C&C URLs
  - 35 URLs responded at least once w. valid command
- 1,968 unique URL targets

DJ Monitoring - C&C Lifetime



DJ Monitoring - Services

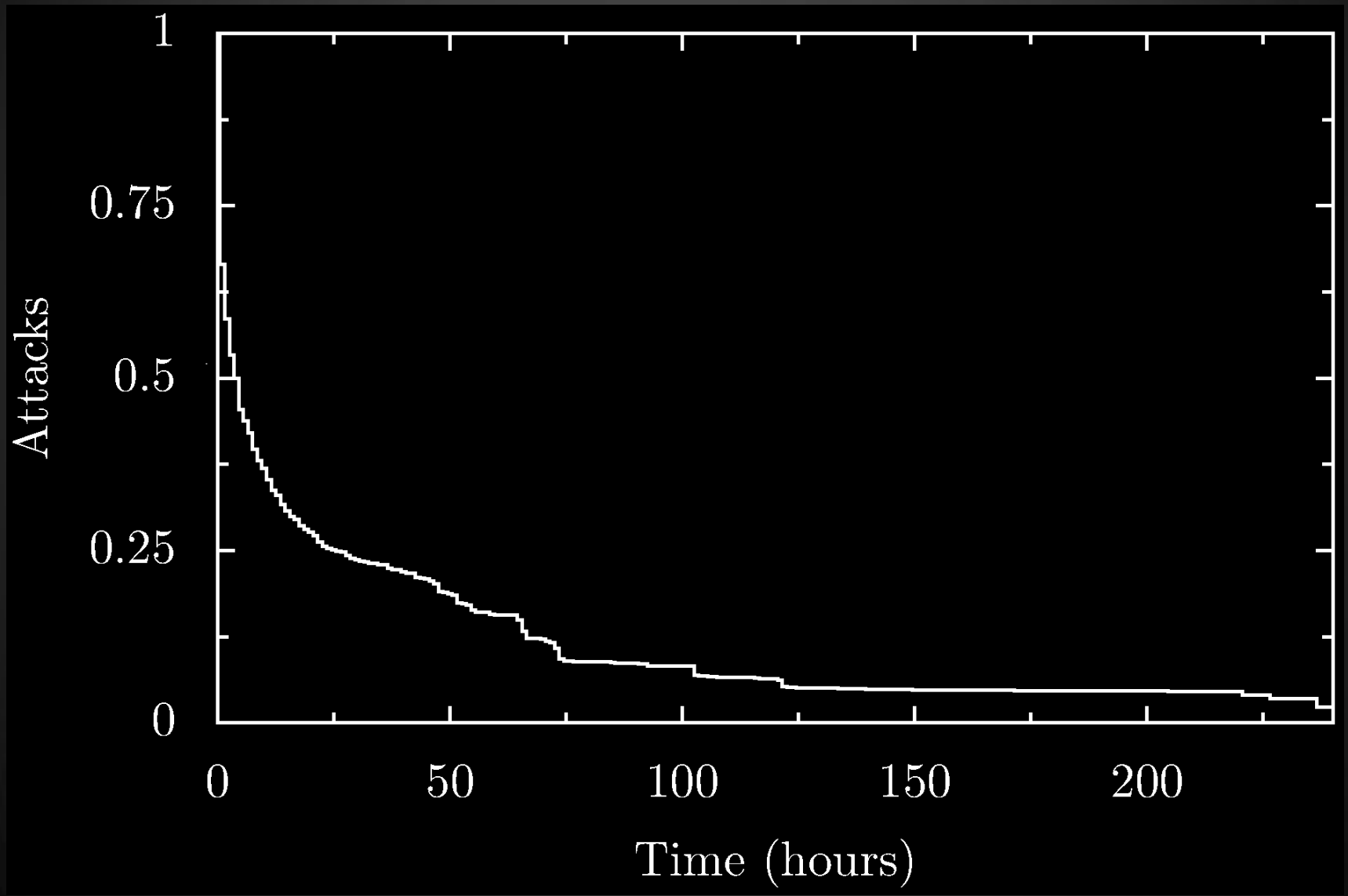


DJ Monitoring - Categories (WBSN)

DJ Monitoring - Financial

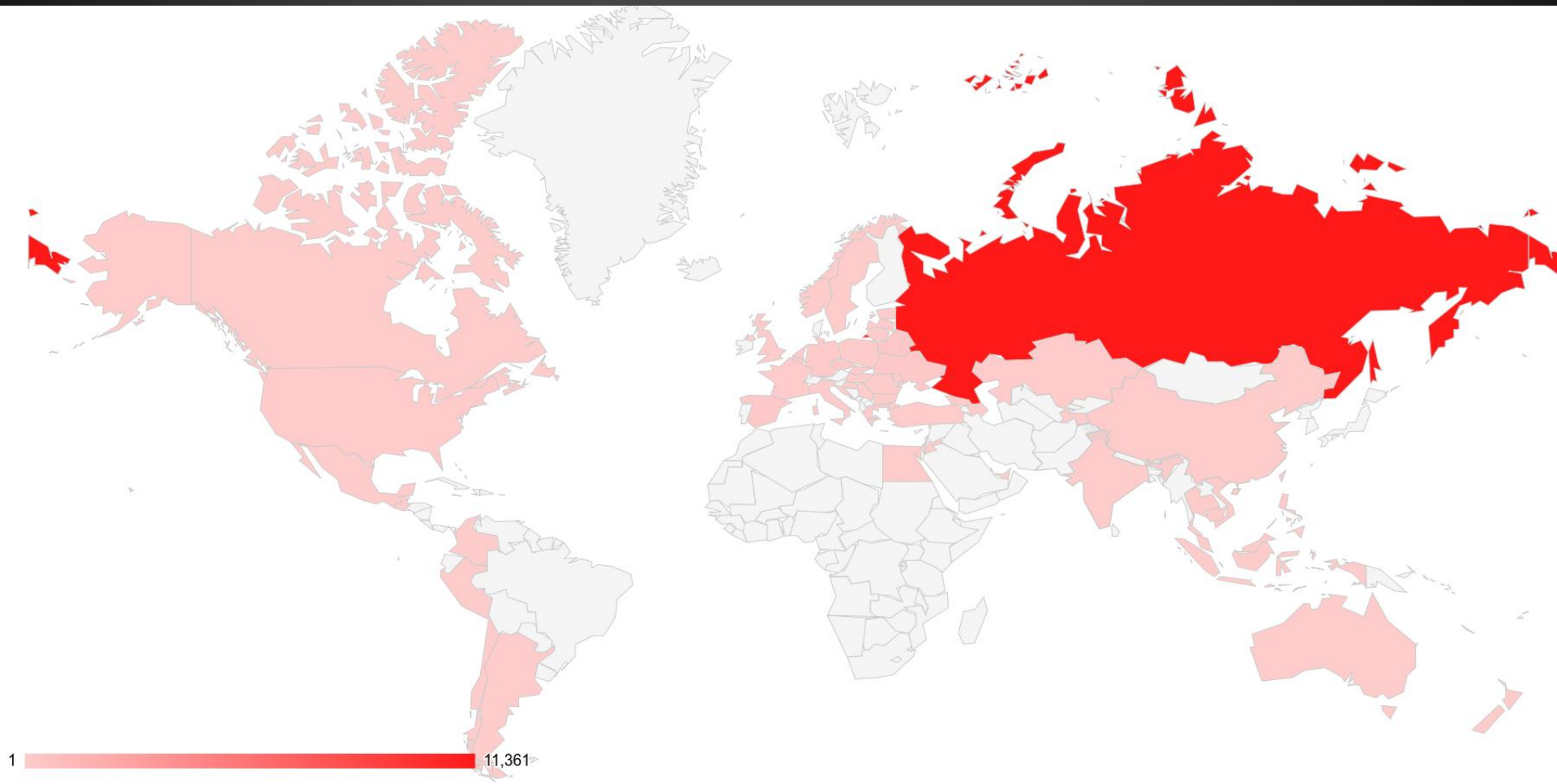
- 17 Online banking portals
- 9 Online stock brokerage portals
  - etrade.com.au
    - 5 day attack in December 2011

DJ Monitoring - Attack length



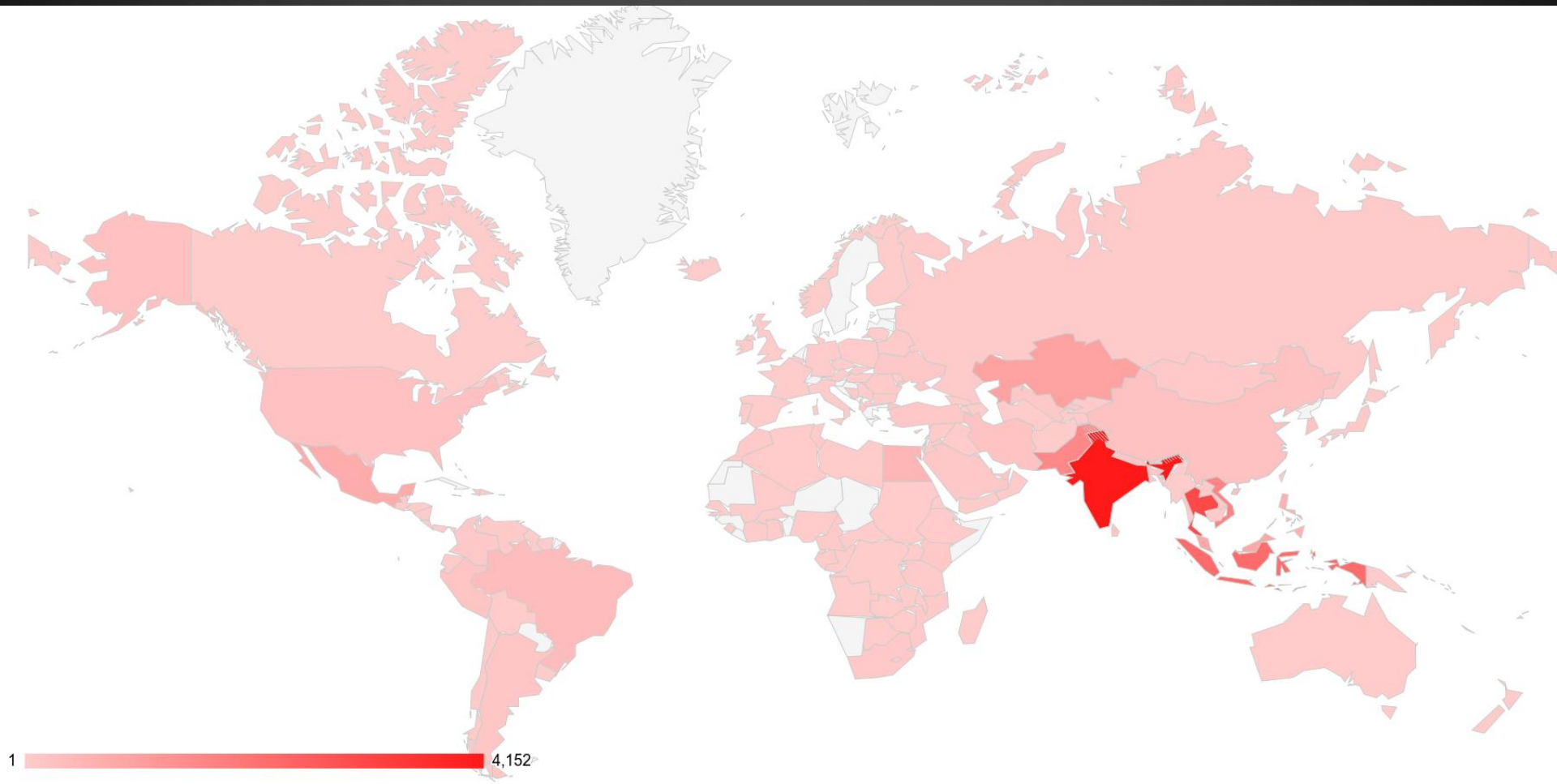
DJ Victim Logs - VirusTotal

- 12,686 unique IP addresses



DJ Victim Logs - Krebs on Security

- 21,293 unique IP addresses



Conclusion

- DDoS malware…
  - is readily available in the Underground
- DDoS botnets…
  - are used as a monetization strategy by Cybercriminals
  - can ruin Internet-centric businesses
  - are used to attack adversaries in the IT Security Community

Acknowledgments

- Francisco Santos, Julio Canto (Hispasec)
  - virustotal.com attack webserver logs
- Brian Krebs ('Krebs on Security' blog)
  - krebsonsecurity.com attack webserver logs
- Security community sharing intel
  - Andre M. DiMino (DeepEnd Research)
  - Curt Wilson (Arbor Networks)
  - Shadowserver

Thank you!
Questions?