Tracking DDoS Attacks
Insights into the Business of Disrupting the Web

Armin Buescher, Websense Security Labs
Thorsten Holz, Ruhr University Bochum
DDoS in today's Internet landscape

• Instruments
  o *Botnets (Cybercrime)*
  o Volunteers (Hacktivism)

• Attacked technologies
  o Network layer
  o Transport layer
  o *Application layer*

• Impacts of service downtime
  o Business - Revenue loss
  o Information - Silence
Motives for DDoS attacks

- Blackmail service operators
- Disrupt the competition
- Disrupt adversaries
- Manipulate services
- Political protest
Automated C&C monitoring

1. VirusTotal
2. Database
3. Protection Proxy
4. Sandbox
5. Emulated bot

C&C Server

Victim
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

Dirt jumper v3

Time: 17:15:32
Today: 1
Online: 1

URLs:
https://www.usenix.org/conference/leet12

Flows: 0
HTTP flood
Stop
Save
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
  o 465 samples
  o 274 samples showed DJ C&C traffic
• 68 unique C&C URLs
  o 35 URLs responded at least once w. valid command
• 1,968 unique URL targets
DJ Monitoring - C&C Lifetime

![Graph showing the C&C Lifetime of servers over time.](image-url)
DJ Monitoring - Categories (WBSN)

Games
Forums
Auctions
News
Financial
Malicious
Business
Vehicles
Educational
Entertainment
Security
Illegal
Social
Phishing
Hosted
Government
Blog
Webmail
Storage
Pay-to-Surf
Tobacco
Adult
Freeware
Health
Chat
DDNS
Portals
Questionable
Advertisements
Militancy
Travel
Hacking
Hosting
Lifestyle
Gambling
Sex
Shopping
DJ Monitoring - Financial

• 17 Online banking portals
• 9 Online stock brokerage portals
  o etrade.com.au
    ▪ 5 day attack in December 2011
DJ Monitoring - Attack length

![Graph showing the decrease in attacks over time (in hours).]
DJ Victim Logs - VirusTotal

- 12,686 unique IP addresses
DJ Victim Logs - Krebs on Security

- 21,293 unique IP addresses
Conclusion

• DDoS malware…
  o is readily available in the Underground

• DDoS botnets…
  o are used as a monetization strategy by Cybercriminals
  o can ruin Internet-centric businesses
  o are used to attack adversaries in the IT Security Community
Acknowledgments

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