About Us

Industry body formed to foster synergy among stakeholders to promote advancement in DDoS defense knowledge.

Independent academic R&D division of Nexusguard building next generation DDoS mitigation knowledge and collaborate with the defense community.
Outline

• DDoS Attack Categories
• DDoS Detection and Mitigation Techniques
  – How they work?
  – How to bypass / take advantage?
• DDoS Mitigation Bypass
  – How to use our PoC tool?
  – PoC tool capability
• Next-Generation Mitigation
Financial Impact

Volume: > 20GBPS

Frequency: > 2.5mil per year

Complexity: App Level > 30%

Cost: > US$6mil per hour

Volumetric Attacks

- Packet-Rate-Based
- Bit-Rate-Based
Semantic Attacks

API attacks
Hash DoS
Apache Killer
Teardrop (old textbook example)
Slowloris / RUDY
SYN Flood (old textbook example)
Smurf (old textbook example)

APPLICATION LEVEL ATTACKS!

PROTOCOL ATTACKS!
Blended Attacks

BLENDING
IT REALLY WORKS!
ADMIT IT, YOU DID NOT NOTICE HIM AT FIRST.

black hat
USA 2013
Attack Quadrant

Volume

xxx Gbps+

xxx Mbps+

Complexity

Simple

Sophisticated

Volumetric Attack

Semantic Attack
DDoS Mitigations

- Traffic Policing
- Black- / Whitelisting
- Proactive Resource Release

Volume

Complexity

xxx Gbps+

xxx Mbps+

Simple

Sophisticated
DDoS Mitigation: Traffic Policing

Source: Cisco
DDoS Mitigation: Proactive Resource Release

1. Open lots of TCP connections
2. TCP connection pool starved
3. Detect idle / slow TCP connections
   RST
4. Close idle / slow TCP connections
   With RST

Example:
Slowloris Attack

1. Open lots of TCP connections
2. TCP connection pool starved
3. Detect idle / slow TCP connections
   RST
4. Close idle / slow TCP connections
   With RST

Example:
Slowloris Attack
DDoS Mitigation: Black- / Whitelisting

1. **Black List**
   - Src: 1.2.3.4
   - Src: 5.6.7.8
   - Dropped

2. **White List**
   - Src: 5.6.7.8
   - Src: 3.4.5.6
   - Src: 6.7.8.9
   - White List = *free pass*
   - (for awhile / for x amount of volume)

3. **Backend**
DDoS Mitigation: Source Isolation

Source: http://www.cs.duke.edu/nds/ddos/
DDoS Solution: Secure CDN

1: request
2: redirect to nearest server
3: return
4: bypass distribution, attack backend!
DDoS Detection

Rate Measurement (SNMP)
Baselining (Netflow)

Big Data Analysis
Protocol Sanity (PCAP)
Protocol Behavior (PCAP)
Application (SYSLOG)

Volume
xxx Gbps+
xxx Mbps+

Complexity
Simple
Sophisticated

black hat USA 2013
Rate- / Flow-Based Countermeasures

Detection

Rate Measurement

Baseline Enforcement

Mitigation
Protocol-Based Countermeasures

Detection

Mitigation

Protocol Sanity Checking

Protocol Behavior Checking

Protocol Pattern Matching

black hat USA 2013
Blanket Countermeasures

Detection

Traffic Statistics and Behavior
Big Data Analysis

Source Host Verification

Mitigation

Malicious Source Intelligence

black hat USA 2013
# Source Host Verification

<table>
<thead>
<tr>
<th>Verifies</th>
<th>TCP SYN</th>
<th>HTTP Redirect</th>
<th>HTTP Cookie</th>
<th>JavaScript</th>
<th>CAPTCHA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Spoofed Source IP</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>HTTP Compliant Application</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Real Browser</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Real Human</td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
PoC Tool

Version 1.0 Caveat:
* Only support IPv4.
* Source IP not spoofable.
* Limited CAPTCHA cracking capability.
* Watermark embedded for easy detection.

TCP Traffic Model
- Number of connections: 10
- Connections interval (second): 5.0
- Connection hold time before first request (second): 1.0
- Connection idle timeout after last request (second): 1.0

HTTP Traffic Model
- Number of requests per connection: 10
- Requests interval (second): 5.0
- Custom header:

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspat Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

KILL 'em!!
PoC Tool Strengths

- True TCP/IP behavior (RST, resend, etc.)
- Believable HTTP headers (User-Agent strings, etc.)
- Embedded JavaScript engine
- CAPTCHA solving capability
- Randomized payload
- Tunable post-authentication traffic model

**INDISTINGUISHABLE FROM HUMAN!!**
PoC Tool: Authentication Bypass

Version 1.0 Caveat:
* Only support IPv4.
* Source IP not spoofable.
* Limited CAPTCHA cracking capability.
* Watermark embedded for easy detection.

Source IP: auto detect
Target URL:

Authentication Bypass
- [ ] HTTP Redirect
- [ ] HTTP Cookie (Header field: Cookie)
- [ ] JavaScript
- [ ] CAPTCHA

Reauth every (second): 300.0

TCP Traffic Model
- Number of connections: 10
- Connections interval (second): 5.0
- Connection hold time before first request (second): 1.0
- Connection idle timeout after last request (second): 1.0

HTTP Traffic Model
- Number of requests per connection: 10
- Requests interval (second): 5.0
- Custom header:

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspaire Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

KILL 'em !!
TCP SYN Auth (TCP Reset)

- SYN
- SYN ACK
- ACK
- RST
- SYN
- SYN ACK
- ACK
- RETRY

Red path: Failed connection
Green path: Successful connection
TCP SYN Auth (TCP Out-of-Sequence)
HTTP Redirect Auth

GET /index.html
HTTP 302 redir to /foo/index.html
GET /foo/index.html
HTTP 302 redir to /index.html
GET /index.html

✔

blackhat USA 2013
HTTP Cookie Auth (Header Token)

GET /index.html

HTTP 302 redir to /index.html

[X-Header: foo=bar]

GET /index.html

HTTP 302 redir to /index.html

[X-Header: foo=bar]

GET /index.html

[X-Header: foo=bar]

GET /index.html

[X-Header: foo=bar]

BROWSER-DEPENDENT BEHAVIOR!!

blackhat
USA 2013
JavaScript Auth

GET /index.html

HTTP 302 redir to /index.html

POST /auth.php

ans=16

JS 7+nine=?

GET /index.html

blackhat USA 2013
GET /index.html

HTTP 302 redirect to /index.html

POST /auth.php

ans="overlooks inquiry"

GET /index.html

CAPTCHA Auth
CAPTCHA Pwnage
PoC Tool: TCP Traffic Model

Version 1.0 Caveat:
* Only support IPv4.
* Source IP not spoofable.
* Limited CAPTCHA cracking capability.
* Watermark embedded for easy detection.

Source IP: auto detect
Target URL:

TCP Traffic Model
Number of connections: 10
Connections interval (second): 5.0
Connection hold time before first request (second): 1.0
Connection idle timeout after last request (second): 1.0

HTTP Traffic Model
Number of requests per connection: 10
Requests interval (second): 5.0

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspor Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

KILL 'em !!
TCP Traffic Model

Connection Hold Time
Before 1st Request

Connection Idle Timeout
After Last Request

TCP Connection

Connections Interval

Connections Interval

TCP Connection

TCP Connection

Number of Connections
PoC Tool: HTTP Traffic Model

Version 1.0 Caveat:
* Only support IPv4.
* Source IP not spoofable.
* Limited CAPTCHA cracking capability.
* Watermark embedded for easy detection.

Source IP: auto detect
Target URL:

Authentication Bypass
- HTTP Redirect
- HTTP Cookie (Header field: Cookie)
- JavaScript
- CAPTCHA
Reauth every (second): 300.0

TCP Traffic Model
- Number of connections:
- Connections interval (second):
- Connection hold time before first request (second):
- Connection idle timeout after last request (second):

HTTP Traffic Model
- Number of requests per connection: 10
- Requests interval (second): 5.0
- Custom header:

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspair Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

KILL 'em All 1.0
PoC Tool Design

• 3 tries per authentication attempt (in practice more likely to succeed)
• True TCP/IP behavior thru use of OS TCP/IP stack
• Auth cookies persist during subsequent dialogues
• JavaScript execution using embedded JS engine (lack of complete DOM an obstacle to full emulation)
CAPTCHA Bypass Design

1. Converted to black-and-white for max contrast
2. 3x3 median filter applied for denoising
3. Word segmentation
4. Boundary recognition
5. Pixel difference computed against character map
PoC Tool in Action

DEMO VIDEO
Testing Environment

Against Devices
- Direct Links
- Measure Attack Traffic

Against Services
- Measure Traffic
Mitigation Bypass (Protection Products)

### Auth Bypass

<table>
<thead>
<tr>
<th>Detection Techniques</th>
<th>Arbor Peakflow SP TMS</th>
<th>NSFocus ADS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Host Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP SYN Authentication</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTTP Redirect Authentication</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTTP Cookie Authentication</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>JavaScript Authentication</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>CAPTCHA Authentication</td>
<td>(Not implemented in TMS)</td>
<td>✓</td>
</tr>
</tbody>
</table>

Testing results under specific conditions, valid as of Jul 13, 2013

### Post-Auth

<table>
<thead>
<tr>
<th>Detection Techniques</th>
<th>Arbor Peakflow SP TMS</th>
<th>NSFocus ADS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Measurement/Baseline Enforcement</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>(Zombie Removal, Baseline Enforcement, Traffic Shaping, Rate Limiting)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Protocol Sanity &amp; Behavior Checking</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(HTTP Countermeasures)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Proactive Resource Release</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(TCP Connection Reset)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Big Data Analysis</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(GeoIP Policing)</td>
<td>✓</td>
<td>(Not implemented in ADS)</td>
</tr>
<tr>
<td>Malicious Source Intelligence</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(Black White List, IP Address Filter List, Global Exception List, GeoIP Filter List)</td>
<td>✓</td>
<td>(Not implemented in ADS)</td>
</tr>
<tr>
<td>Protocol Pattern Matching</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>(URL/DNS Filter List, Payload Regex)</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

black hat USA 2013
## Auth Bypass

<table>
<thead>
<tr>
<th>Detection Techniques</th>
<th>Cloudflare</th>
<th>Akamai</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Host Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP SYN Authentication</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP Redirect Authentication</td>
<td>✔️</td>
<td>N/A</td>
</tr>
<tr>
<td>HTTP Cookie Authentication</td>
<td>✔️</td>
<td>N/A</td>
</tr>
<tr>
<td>JavaScript Authentication</td>
<td>✔️</td>
<td>N/A</td>
</tr>
<tr>
<td>CAPTCHA Authentication</td>
<td>✗</td>
<td>N/A</td>
</tr>
</tbody>
</table>

## Post-Auth

<table>
<thead>
<tr>
<th>Detection Techniques</th>
<th>Cloudflare</th>
<th>Akamai</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Measurement / Baseline Enforcement</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol Sanity &amp; Behavior Checking</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Proactive Resource Release</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Big Data Analysis</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Malicious Source Intelligence</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol Pattern Matching</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Testing results under specific conditions, valid as of Jul 13, 2013*
Next-Generation Mitigation

- Client Puzzle – add cost to individual zombies.
DDoS is expensive to business
Existing DDoS protection insufficient
Next-Generation solution should make attack expensive
Thank You!

tony.miu@nexusguard.com
albert.hui@ntisac.org
waileng.lee@ntisac.org

http://www.ntisac.org