KILL 'EM ALL

DDoS Protection Total Annihilation

Network Threats
Information Sharing and Analysis Center

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab
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 defense community.
AGENDA

- DDoS Relevance, Attack Categories, Detection & Mitigation
- Source Host Verification: Authentication Methods
  - TCP SYN Auth
  - HTTP Redirect Auth
  - HTTP Cookie Auth
  - JavaScript Auth
  - CAPTCHA Auth
- PoC Tool
  - TCP Traffic Model
  - HTTP Traffic Model
SHOW ME THE $!

Size
Bandwidth > 20Gbps

Complexity
Layer 7 > 30%

Frequency
Attack > 2.5mil per year

Cost
Lost > US$6M per hour!!

OMGWTFFBBQ?!

ATTACK CATEGORIES

Volumetric

Semantic

Blended
MITIGATIONS

Traffic Policing

Proactive House Keeping

CDN / Clean Pipe

Black- / Whitelisting

Traceback
DETECTIONS

Rate Measurement
Baseline Enforcement
Protocol Sanity Checking
Protocol Behavior Checking
Protocol Pattern Matching
Big Data Analysis
Malicious Source Intelligence
Source Host Authentication
TCP SYN AUTH (FORCEFUL RESET)

SYN
SYN ACK
ACK
RST
SYN
SYN ACK
ACK

WTF?!
RETRY

✔

Bloodspear Laboratories
Nexusguard
DDoS Mitigation Lab
TCP SYN AUTH (OUT-SEQ REPLY)

1. SYN
2. SYN ACK
3. RST
4. SYN
5. SYN ACK
6. ACK
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

Valid path
HTTP COOKIE AUTH

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

Valid Connection
HTTP COOKIE AUTH (HEADER TOKEN)

GET /index.html

HTTP 302 redir to /index.html
[X-Header: foo=bar]

GET /index.html
[X-Header: foo=bar]

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!!
JAVASCRIPT AUTH

GET /index.html

HTTP 302 redir to /index.html

ans=16

POST /auth.php

7+nine=?

GET /index.html

HTTP 302 redir to /index.html

GET /index.html
CAPTCHA AUTH

GET /index.html

ans="overlooks inquiry"
POST /auth.php

HTTP 302 redir to /index.html

GET /index.html

GET /index.html
POC

Kill 'em All 1.0

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
Custom header: 

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspear 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

Number of Connections

Connections Interval

Connections Interval
HTTP TRAFFIC MODEL
## AUTHENTICATION BYPASS

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

Testing results under specific conditions, valid as of Jul 13, 2013
# POST-AUTHENTICATION ATTACK

<table>
<thead>
<tr>
<th>Detection Techniques</th>
<th>Arbor Peakflow SP TMS</th>
<th>NSFocus ADS</th>
<th>Cloudflare</th>
<th>Akamai</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Measurement / Baseline Enforcement</td>
<td>✓ (Zombie Removal, Baseline Enforcement, Traffic Shaping, Rate Limiting)</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Protocol Sanity &amp; Behavior Checking</td>
<td>✓ (HTTP Countermeasures)</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Proactive Housekeeping</td>
<td>✓ (TCP Connection Reset)</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Testing results under specific conditions, valid as of Jul 13, 2013
## POST-AUTHENTICATION ATTACK

<table>
<thead>
<tr>
<th>Detection Techniques</th>
<th>Arbor Peakflow SP TMS</th>
<th>NSFocus ADS</th>
<th>Cloudflare</th>
<th>Akamai</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Big Data Analysis</strong></td>
<td>✓ (GeoIP Policing)</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Not implemented in ADS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Malicious Source Intelligence</strong></td>
<td></td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>✓ (Black White List, IP Address Filter List, Global Exception List, GeoIP Filter List)</td>
<td>(Not implemented in ADS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol Pattern Matching</strong></td>
<td>✓ (URL/DNS Filter List, Payload Regex)</td>
<td>✓</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Testing results under specific conditions, valid as of Jul 13, 2013*
NEXT-GEN MITIGATION
THANK YOU!

tony.miu@nexusguard.com
waileng.lee@bloodspear.org