RSACONFERENCE ASIA PACIFIC 2013

SMILE, YOU'VE BEEN PROFILED: HOW INTRUSION DECEPTION IS SHRINKING HACKER PROFITS

Edward Roberts

Counter Security, Juniper Networks

Session ID: SPO-T05

Session Classification: Intermediate

40

Anti-virus

80

New Viruses

5%

Catch Rate

RHB
RHB
MIKASA
MIKASA
lotto
lotto
7
17
Geylang United F.C.

40

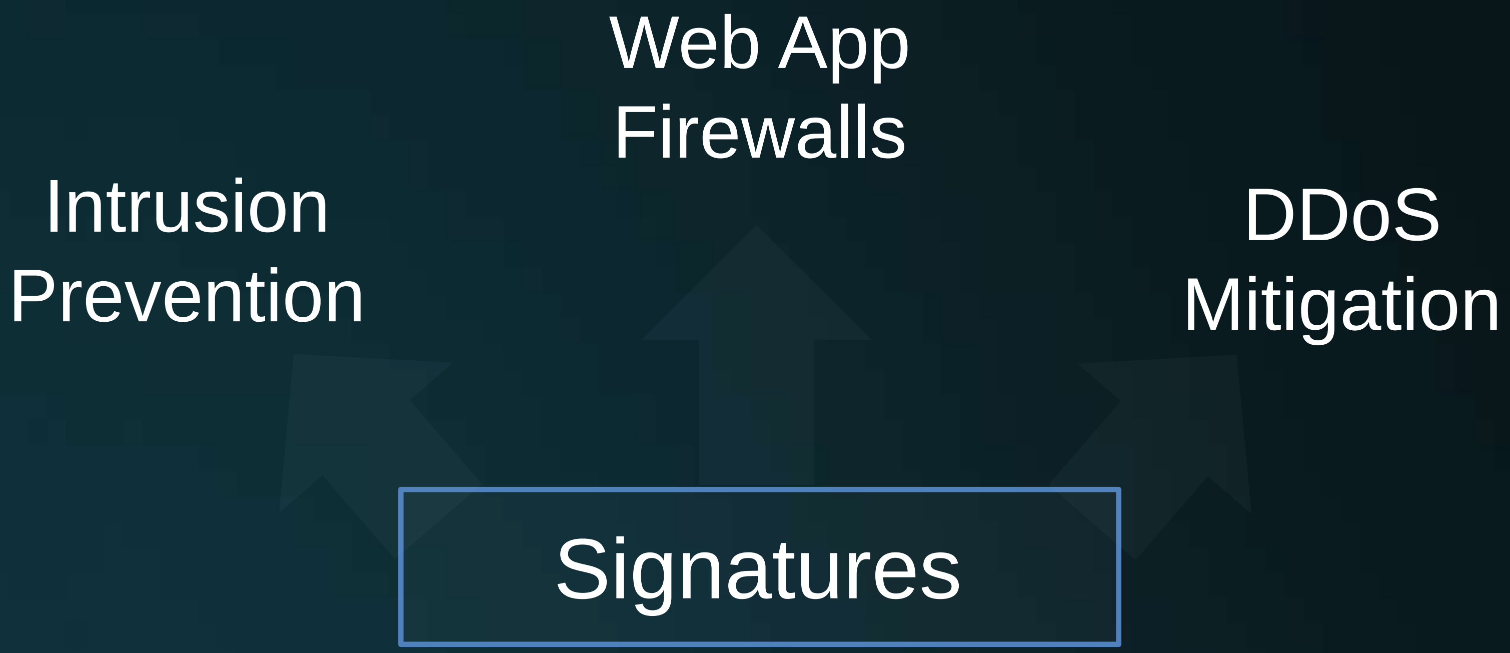
Anti-virus

80

New Viruses

5%

Catch Rate



Web App Firewalls

Intrusion Prevention

DDoS Mitigation

Signatures

40

Anti-virus

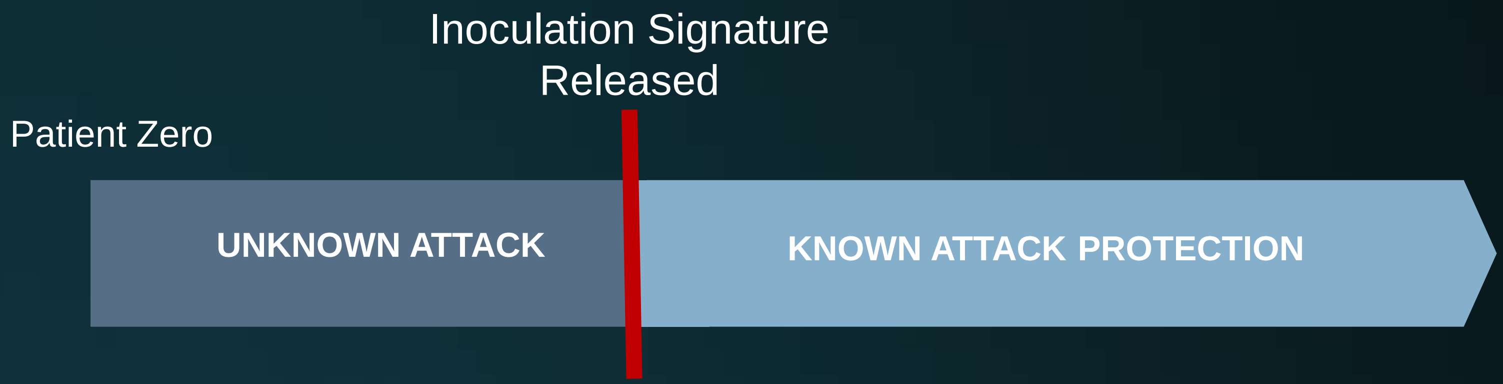
80

New Viruses

5%

Catch Rate

NO-ONE WANTS TO BE PATIENT ZERO


Inoculation Signature Released

Patient Zero

UNKNOWN ATTACK

KNOWN ATTACK PROTECTION

1

The Datacenter Problem

2

A different approach

3

Change the economics of hacking

The insecurity of the web

633,706,564

web sites on the internet

56%

say that securing web traffic is their biggest concern

Sources: Ponemon Institute Report on Efficacy of Emerging Network Security 2013

54%

of breaches of large organizations are via insecure web applications

Sources: Verizon Data Breach Investigations Report 2012.

17%

deploy a web application firewall in block mode

Sources: Ponemon Institute Report on Efficacy of Emerging Network Security 2013

60%

of WAFs not deployed in block mode because of high false positives

Sources: Ponemon Institute Report on Efficacy of Emerging Network Security 2013

62%

said web-based attacks are the most serious type of cyber attacks experienced by their company

Sources: Ponemon Institute Report on Efficacy of Emerging Network Security 2013

48%

said next generation security technologies are not adequately protecting against attacks

Sources: Ponemon Institute Report on Efficacy of Emerging Network Security 2013

Next generation security products are not getting it done

36%

believe next gen security effectively addresses **zero-day threats**

34%

believe next gen security effectively addresses **SQL injection**

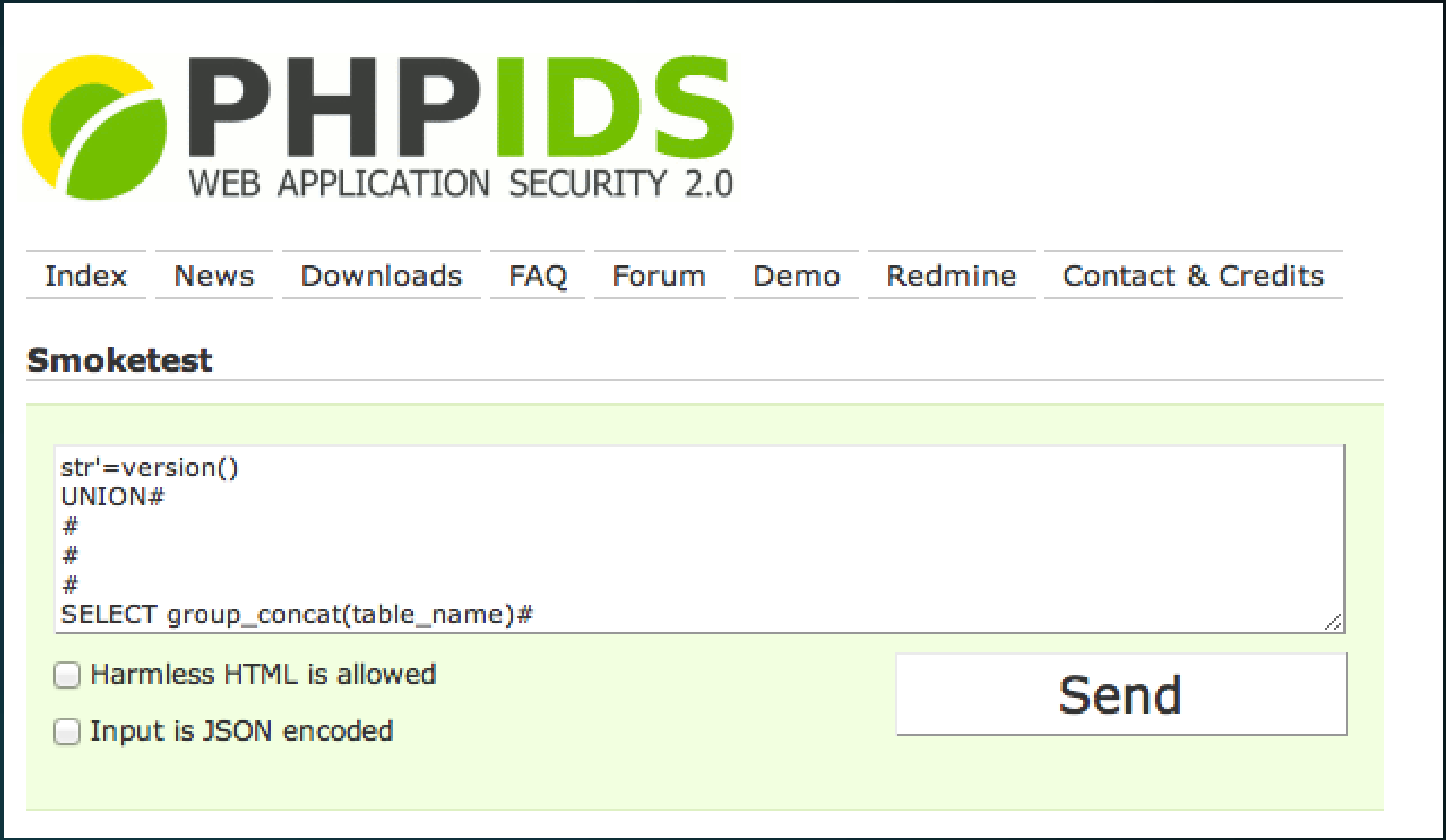
Sources: Ponemon Institute Report on Efficacy of Emerging Network Security 2013

Learn Security Online

Signature Based IDS (My Opinion)

T5D351 Advanced SQL Injection
Joseph McCray

Source: DEFCON 17: Advanced SQL Injection, YouTube

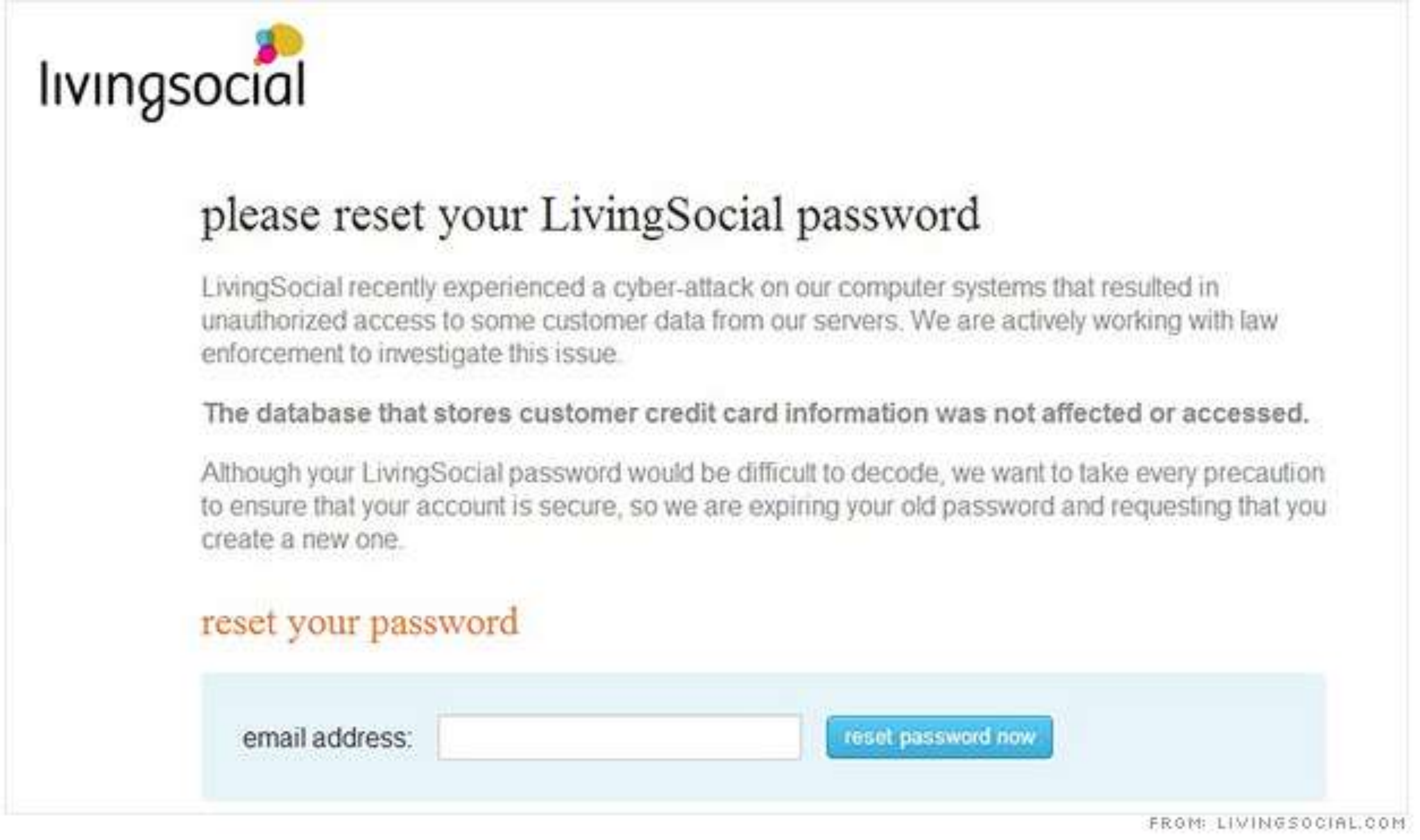


Smoketest

```
str'=version()
UNION#
#
#
#
SELECT group_concat(table_name)#
```

☐ Harmless HTML is allowed

☐ Input is JSON encoded



livingsocial

please reset your LivingSocial password

LivingSocial recently experienced a cyber-attack on our computer systems that resulted in unauthorized access to some customer data from our servers. We are actively working with law enforcement to investigate this issue.

The database that stores customer credit card information was not affected or accessed.

Although your LivingSocial password would be difficult to decode, we want to take every precaution to ensure that your account is secure, so we are expiring your old password and requesting that you create a new one.

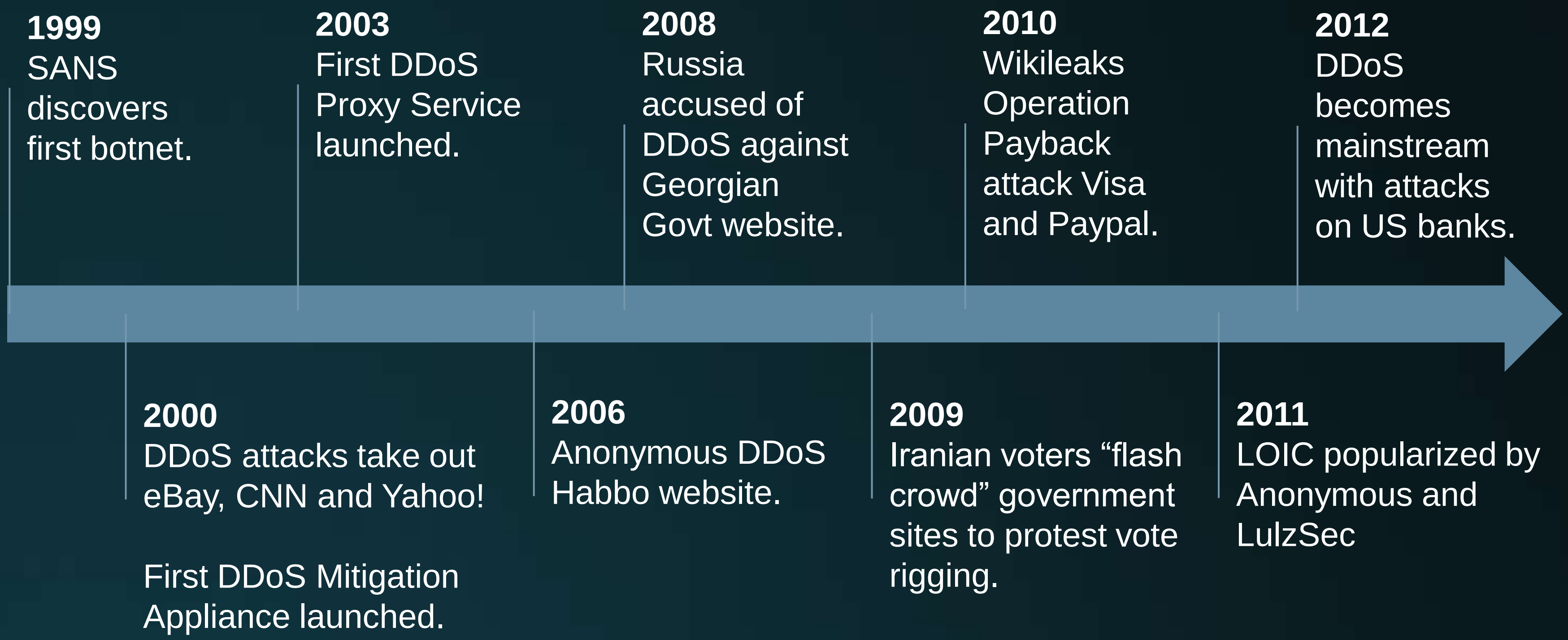
reset your password

FROM: LIVINGSOCIAL.COM

DDoS

Distributed Denial of Service

HISTORY OF DDOS



1999
SANS discovers first botnet.

2000
DDoS attacks take out eBay, CNN and Yahoo!

First DDoS Mitigation Appliance launched.

2003
First DDoS Proxy Service launched.

2006
Anonymous DDoS Habbo website.

2008
Russia accused of DDoS against Georgian Govt website.

2009
Iranian voters “flash crowd” government sites to protest vote rigging.

2010
Wikileaks Operation Payback attack Visa and Paypal.

2011
LOIC popularized by Anonymous and LulzSec

2012
DDoS becomes mainstream with attacks on US banks.

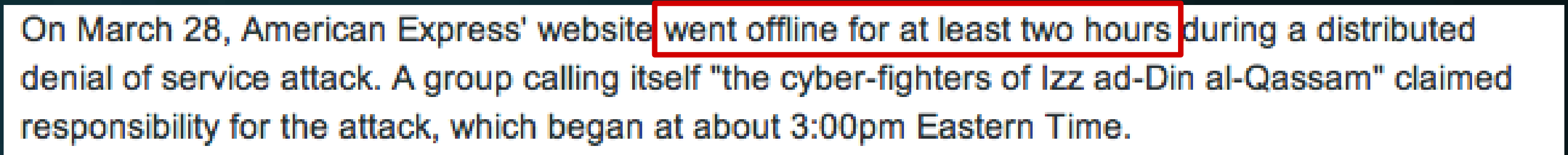
THE MOTIVATIONS BEHIND DDOS ATTACKS

Extortion “Pay us or your site stays down”	**Last Man Standing** Take out your competition so your sales go up during peak times.	**Protest Flash Mobs** Legitimate use of site, just infrastructure can’t handle the volume.	**Sport Teams Fans Hooliganism** Fans DDoS to prevent access to live feeds of games, prevent purchase of tickets /merchandise
Diversionary Smokescreen DDoS to hide the theft.	**Supply and Demand** DDoS to affect access to online ticket sales	**Cyber War** Russia accused of using DDoS during invasion of Georgia.	**Individual Gamer** Player DDoS’d by other players because he is good.
Direct Criminal Activity	Indirect Criminal Activity	Political/Protest	Revenge and “Because I can”

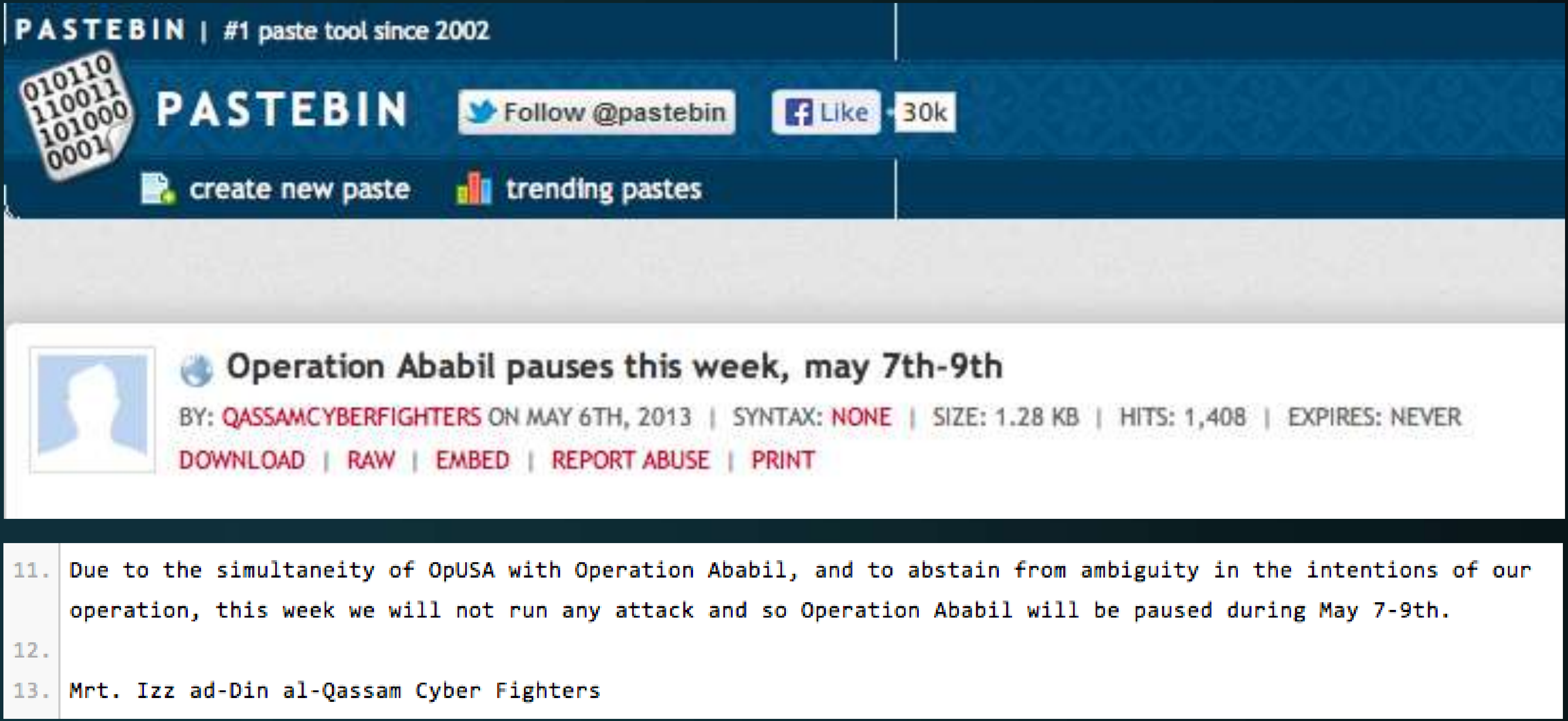
ITSOKNOPROBLEMBRO

```
alert TCP $EXTERNAL_NET any -> $HOME_NET 80
(msg:"stcp.php TCP PORT 80 Flood";\ content:
"|4141 4141 4141 4141 4141 4141 4141 4141|
"; offset: 0; \threshold: type threshold, track by_src, count
5, seconds 1; \ reference:itsoknoproblembro;

sid:100000002; rev:1;)
```



On March 28, American Express' website went offline for at least two hours during a distributed denial of service attack. A group calling itself "the cyber-fighters of Izz ad-Din al-Qassam" claimed responsibility for the attack, which began at about 3:00pm Eastern Time.

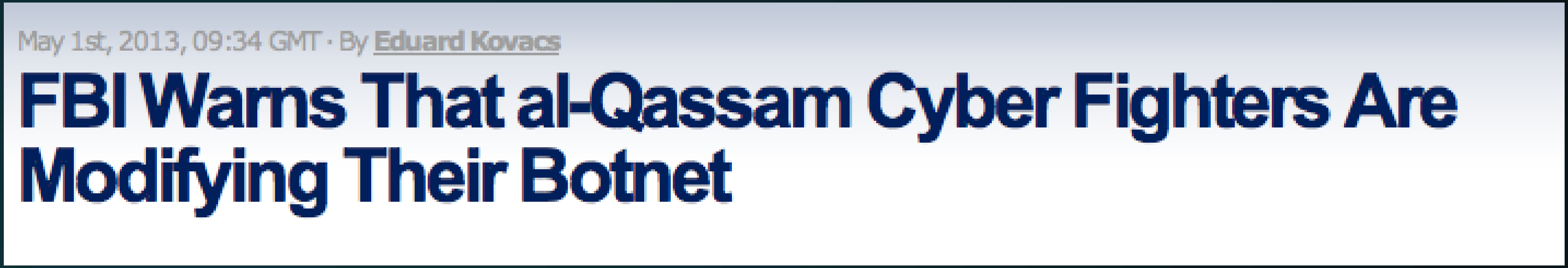

PASTEBIN | #1 paste tool since 2002
PASTEBIN
Follow @pastebin
Like
30k
create new paste
trending pastes
DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

Operation Ababil pauses this week, may 7th-9th

BY: QASSAMCYBERFIGHTERS ON MAY 6TH, 2013 | SYNTAX: NONE | SIZE: 1.28 KB | HITS: 1,408 | EXPIRES: NEVER

```
Due to the simultaneity of OpUSA with Operation Ababil, and to abstain from ambiguity in the intentions of our operation, this week we will not run any attack and so Operation Ababil will be paused during May 7-9th.

Mrt. Izz ad-Din al-Qassam Cyber Fighters
```

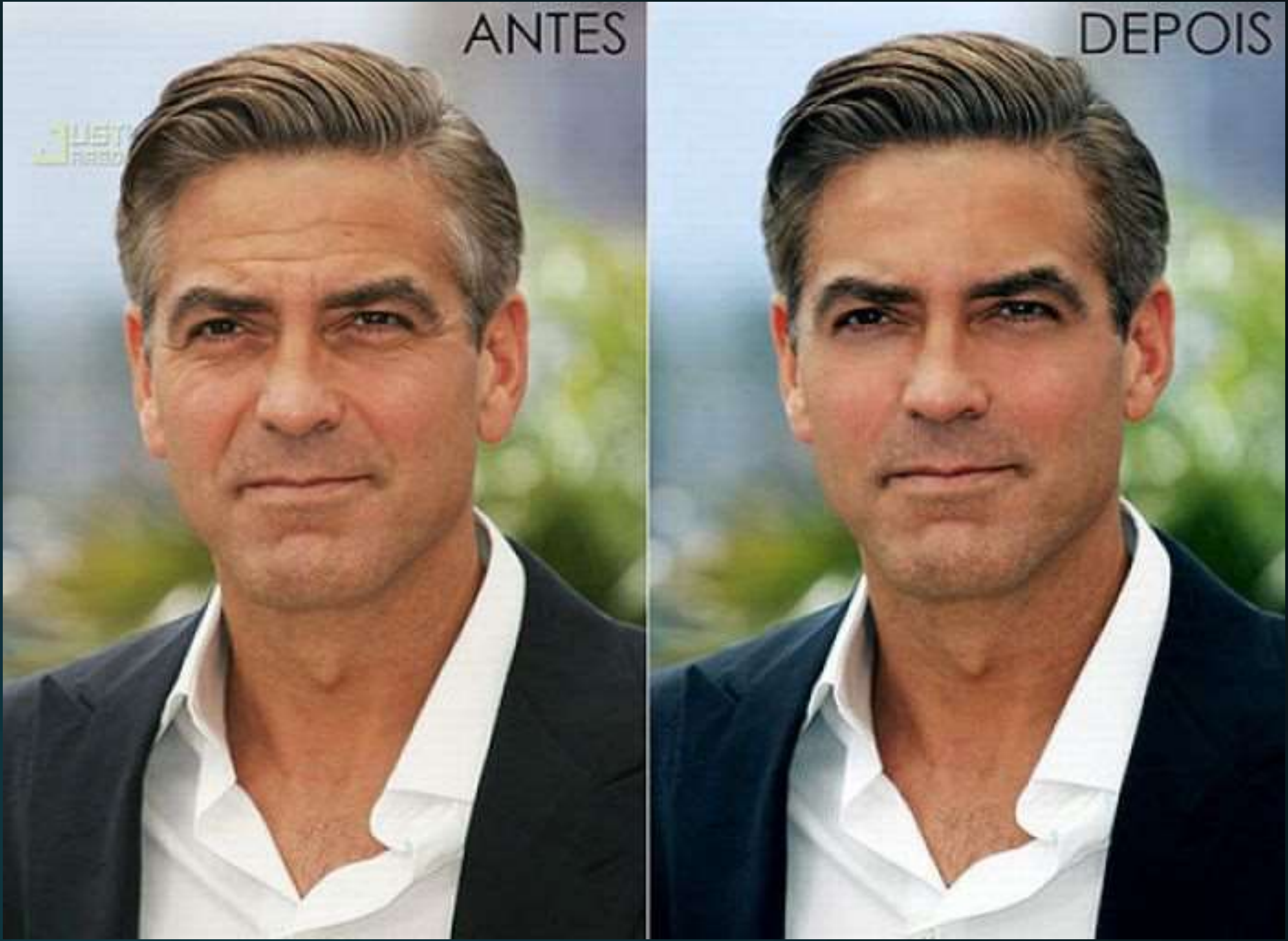


May 1st, 2013, 09:34 GMT · By Eduard Kovacs

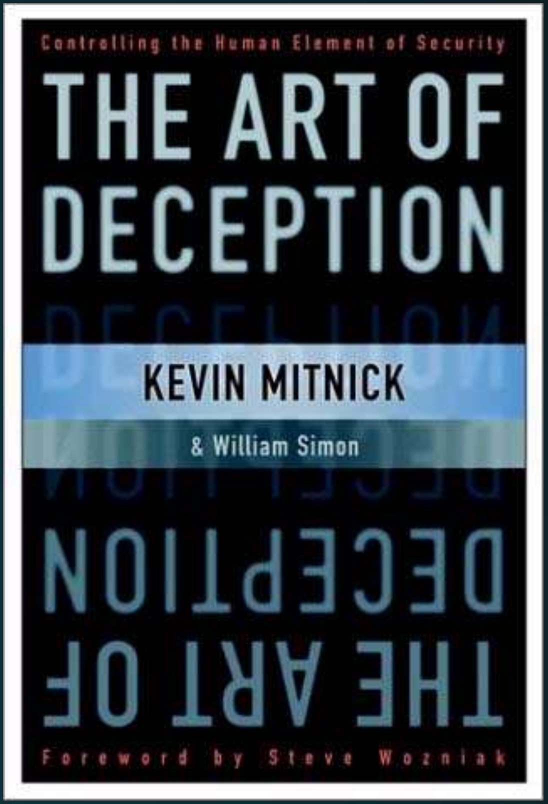
FBI Warns That al-Qassam Cyber Fighters Are Modifying Their Botnet

Stop
Chasing
Attacks

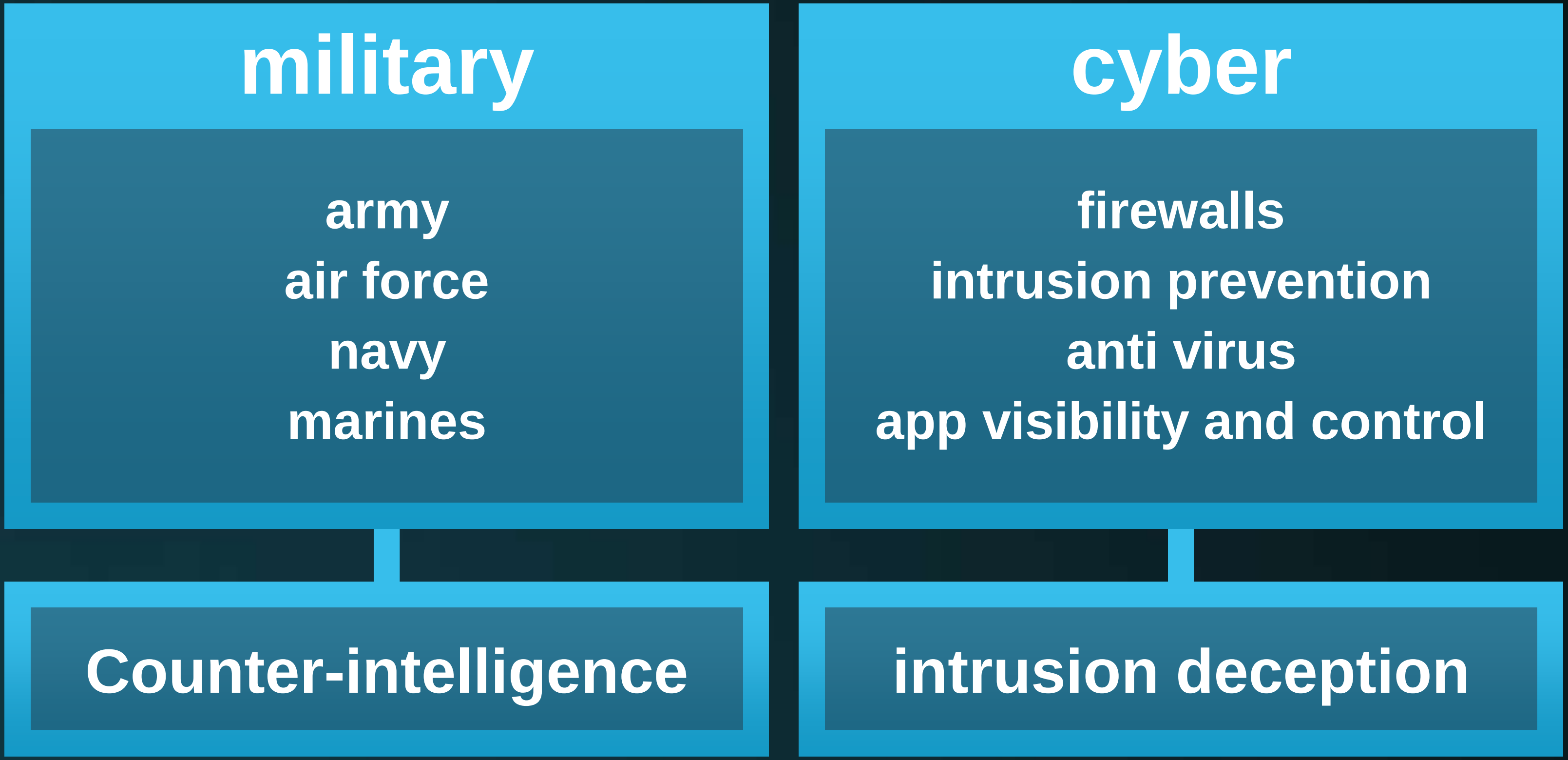
Deception


ANTES
DEPOIS

Used by Hackers as a standard tool


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN MITNICK
& William Simon
Foreword by Steve Wozniak

Security



military

army
air force
navy
marines

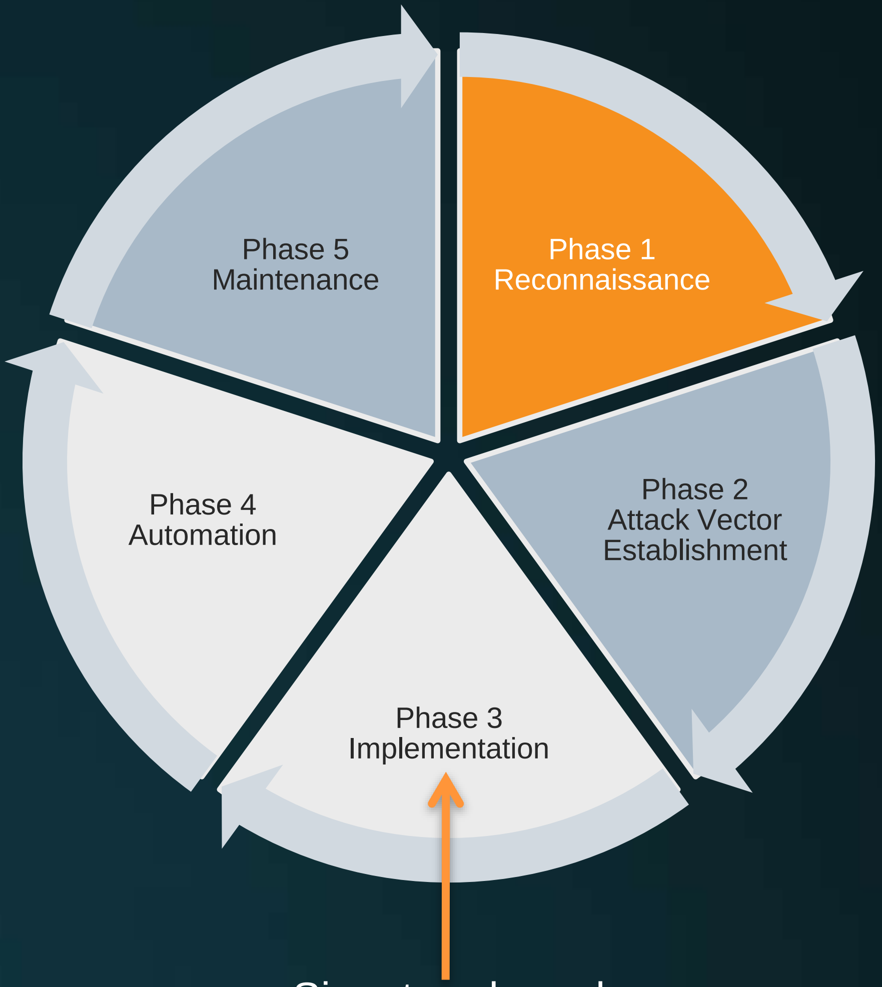
Counter-intelligence

cyber

firewalls
intrusion prevention
anti virus
app visibility and control

intrusion deception

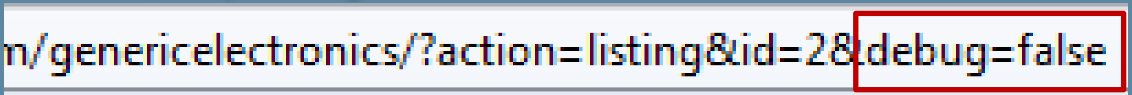
The Anatomy of an Attack



Signature-based
Security products

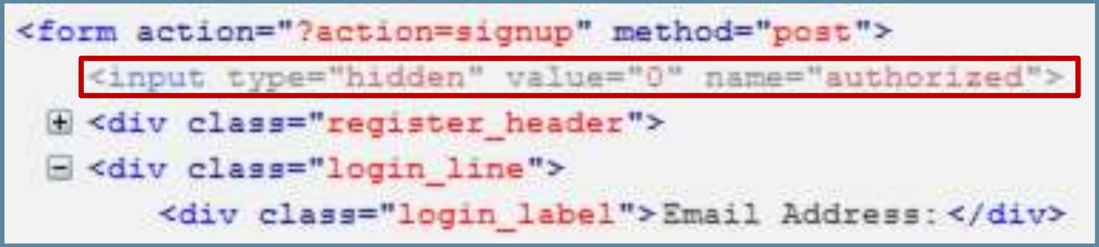
Intrusion Deception

Fake Query String Parameters



```
n/genericelectronics/?action=listing&id=2&debug=false
```

Fake Hidden Input Fields



```
<form action="?action=signup" method="post">
   <input type="hidden" value="0" name="authorized">
 ⊞ <div class="register_header">
 ⊟ <div class="login_line">
      <div class="login_label">Email Address:</div>
```

Changing the Economics

Deceptive Responses

Block the IP address

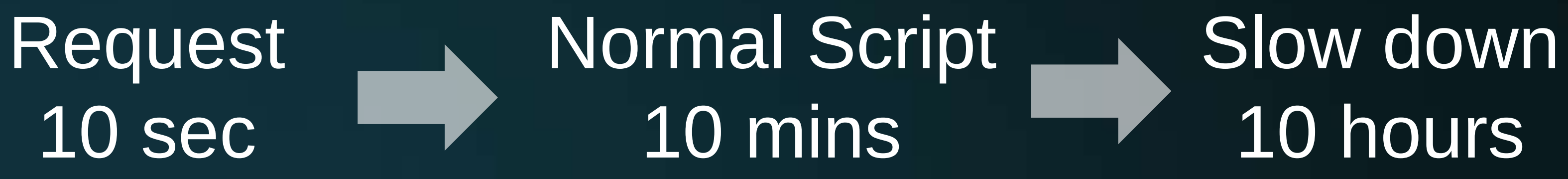
or

Let traffic through

Changing the Economics

Deceptive Responses

SLOW DOWN CONNECTION



Request
10 sec

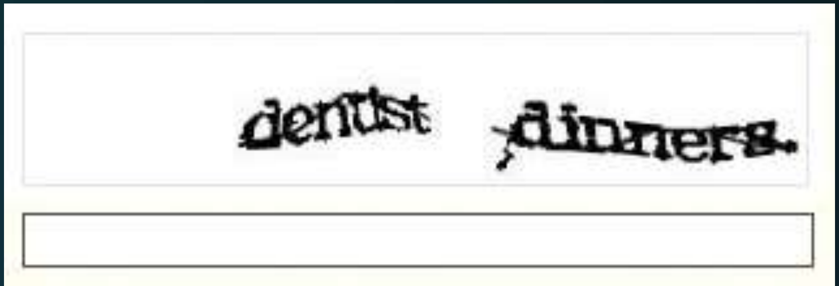
Normal Script
10 mins

Slow down
10 hours

Changing the Economics

Deceptive Responses

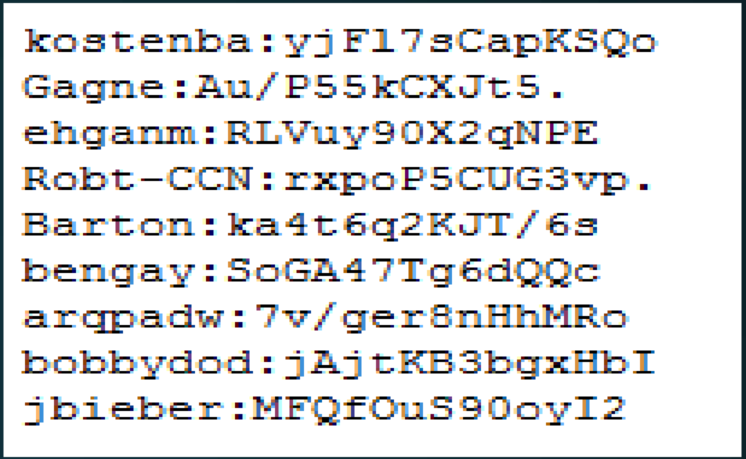
CAPTCHA TO BREAK AUTOMATION



Changing the Economics

Deceptive Responses

FAKE CREDENTIALS

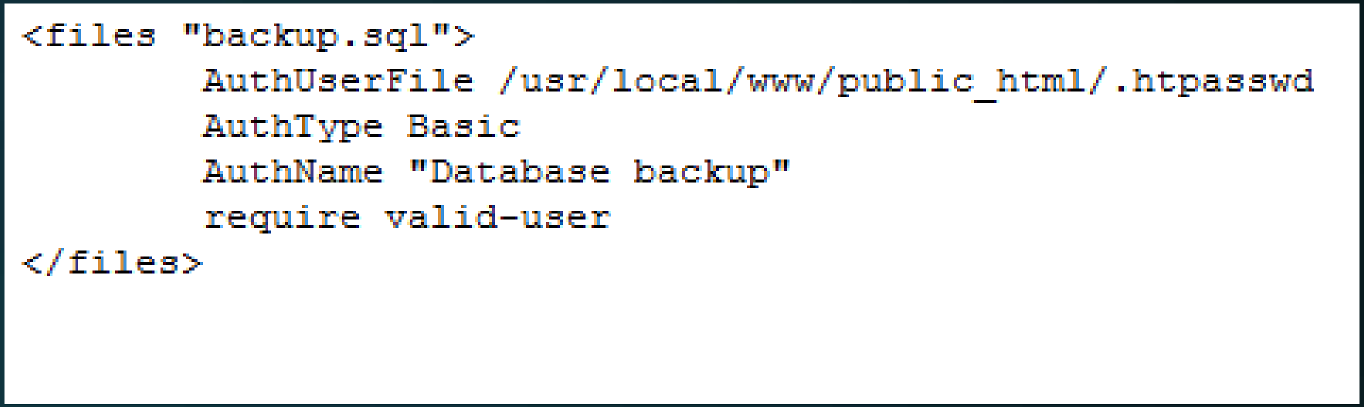


```
kostenba:yjF17sCapKSQo
Gagne:Au/P55kCXJt5.
ehganm:RLVuy90X2qNPE
Robt-CCN:rxpoP5CUG3vp.
Barton:ka4t6q2KJT/6s
bengay:SoGA47Tg6dQQc
arqpadw:7v/ger8nHhMRo
bobbydod:jAjtKB3bgxHbI
jbieber:MFQfOuS90oyI2
```

Changing the Economics

Deceptive Responses

FAKE FILES

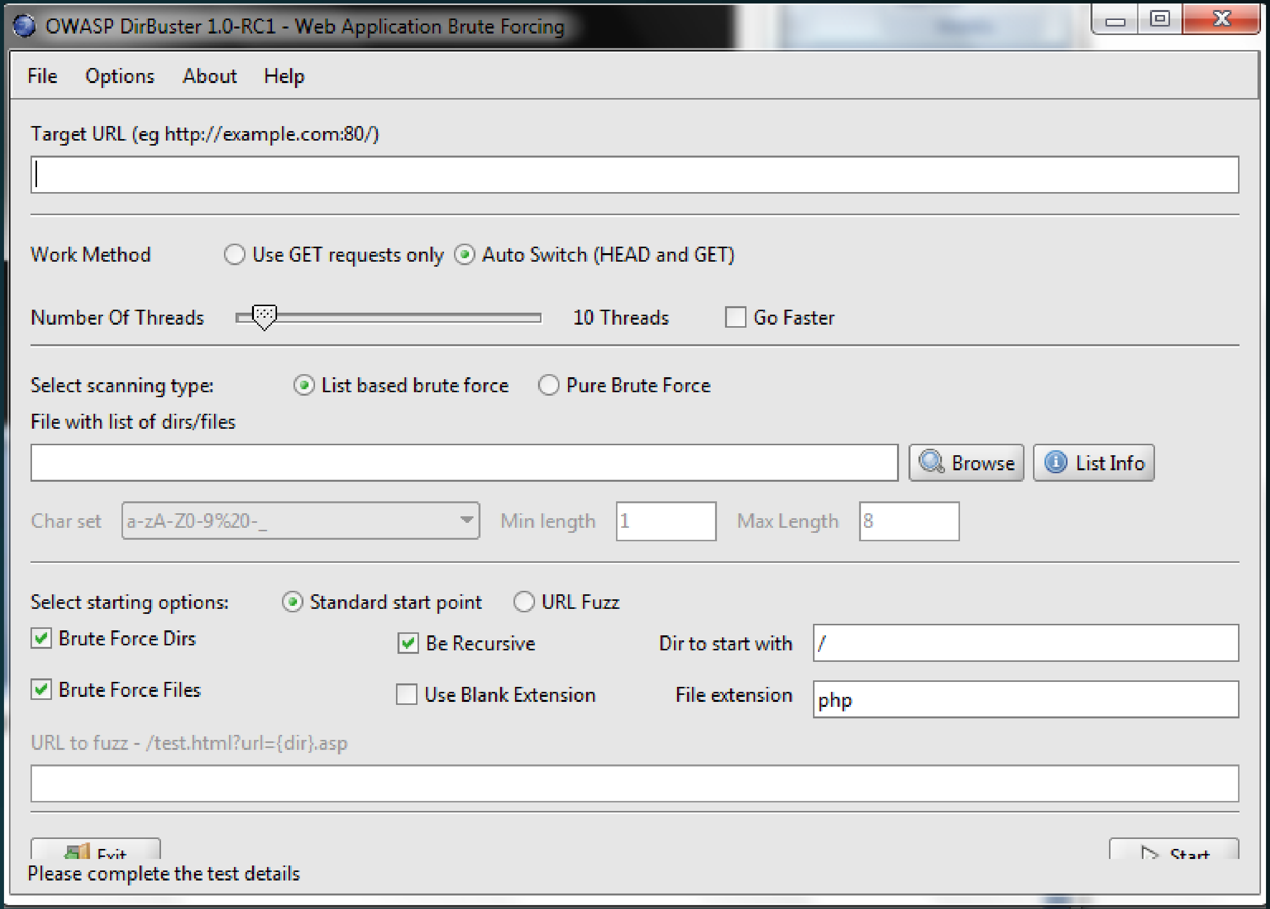


```
<files "backup.sql">
        AuthUserFile /usr/local/www/public_html/.htpasswd
        AuthType Basic
        AuthName "Database backup"
        require valid-user
</files>
```

Changing the Economics

Deceptive Responses

BREAK HACKING TOOLS



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

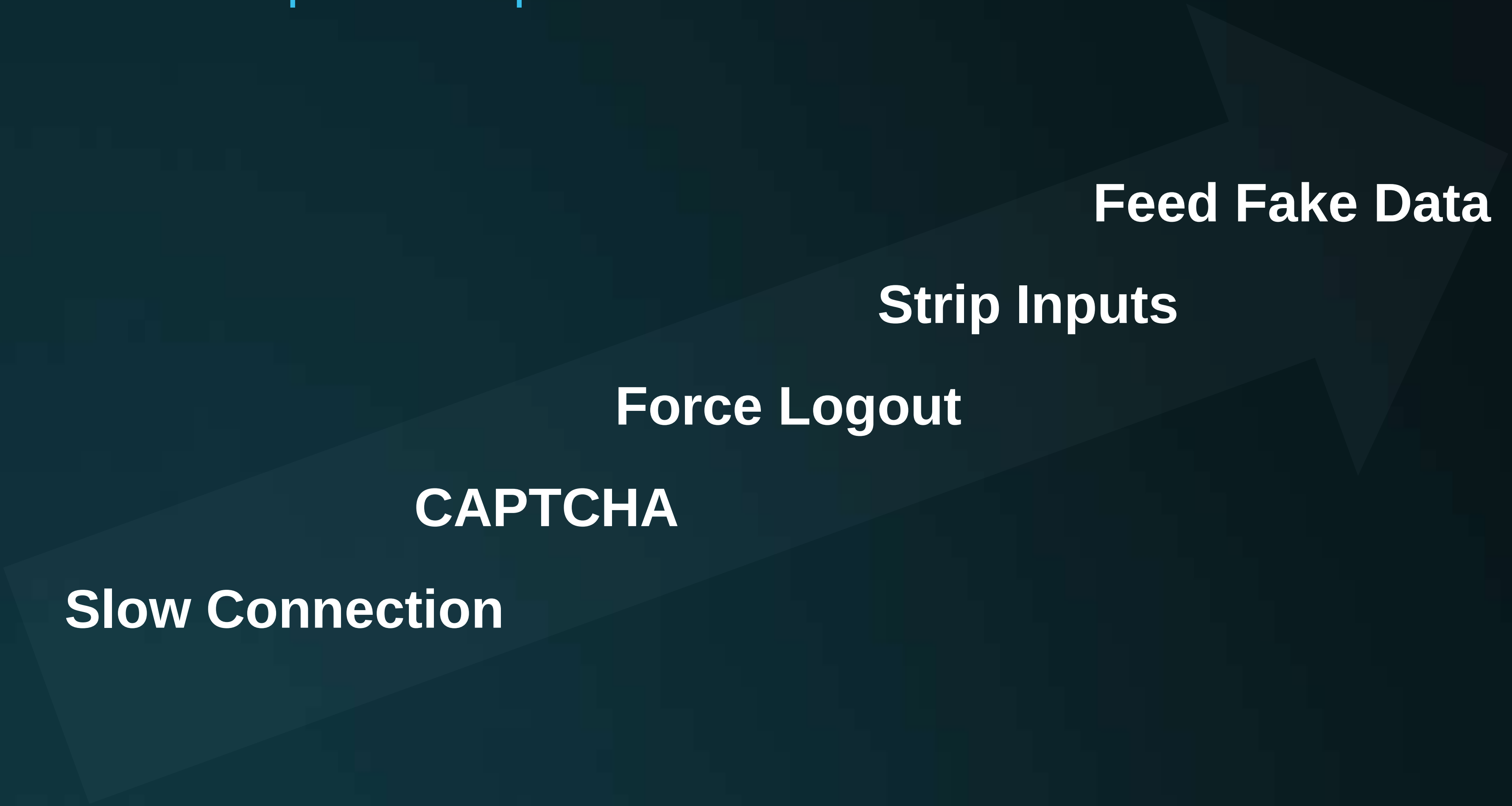
☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

Changing the Economics

Deceptive Responses



Feed Fake Data

Strip Inputs

Force Logout

CAPTCHA

Slow Connection

Stop

Chasing

Attacks

Tracking

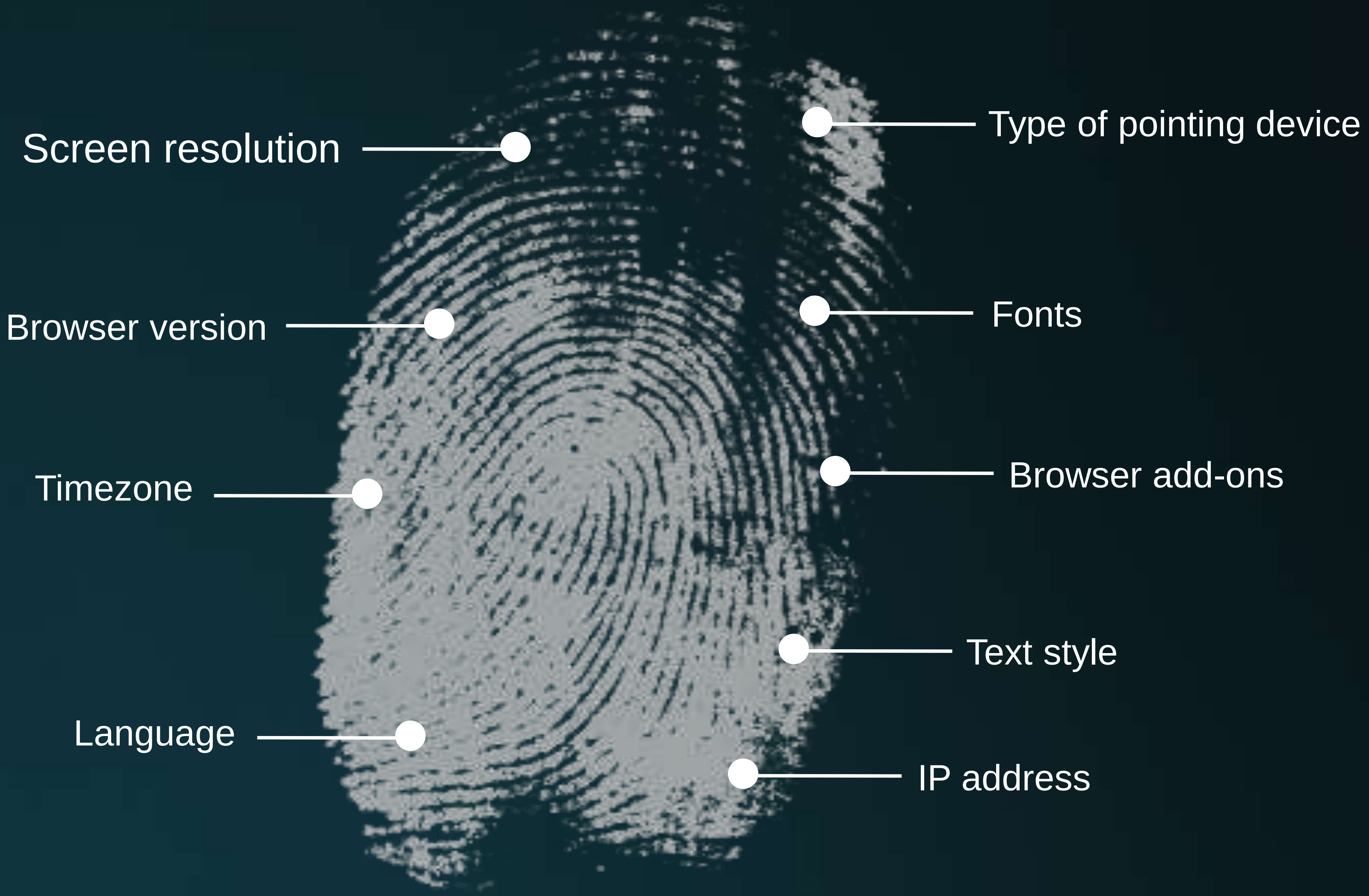
Tracking Beyond the IP

Persistent Token

Persists in all browsers even with privacy controls enabled. Site specific.

Fingerprint

Analyze environment and connection. Not site specific.



Screen resolution

Browser version

Timezone

Language

Type of pointing device

Fonts

Browser add-ons

Text style

IP address

Sharing

Stop Chasing Attacks