Don’t be a DDoS Attacker

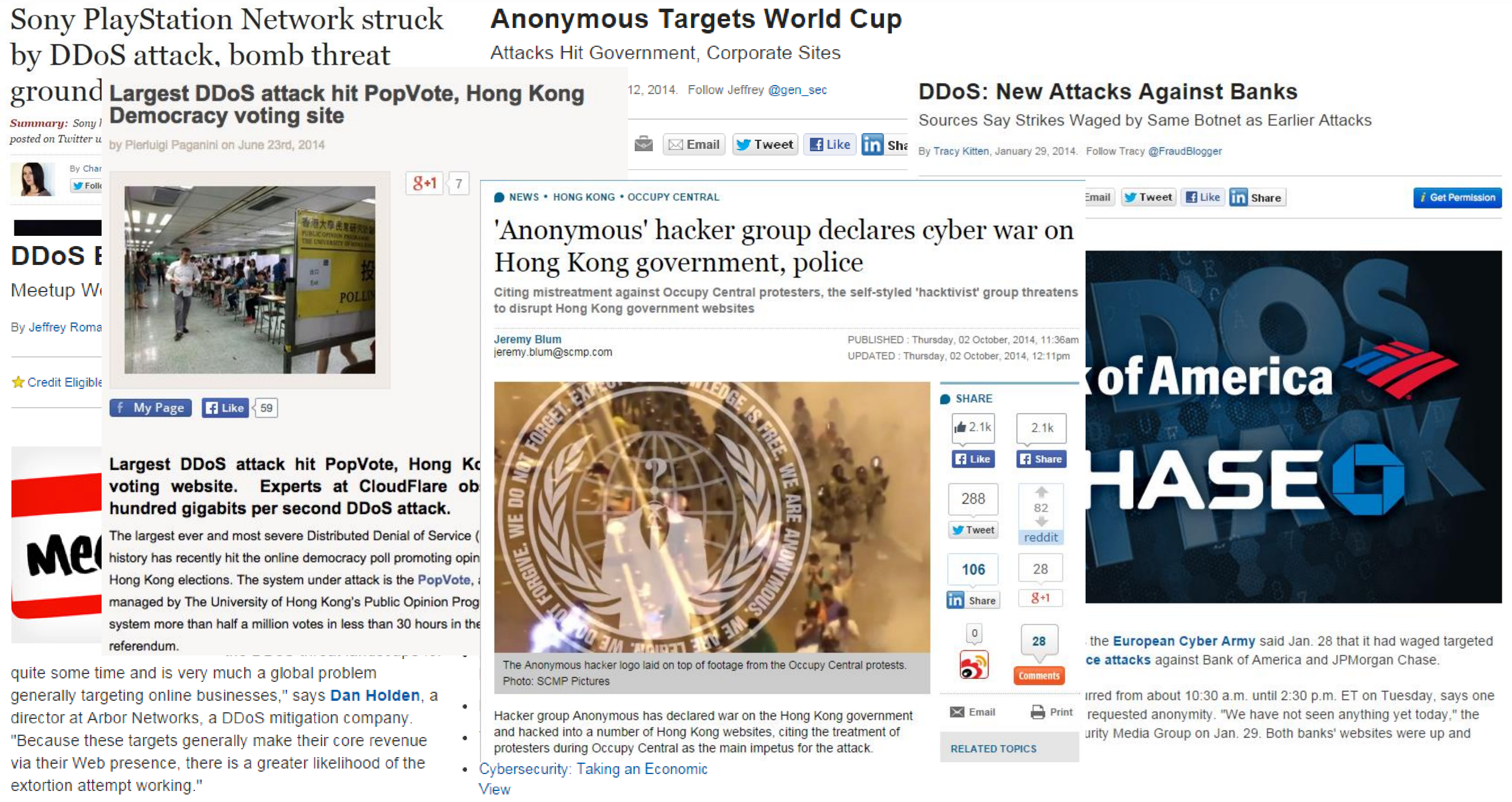
Tony Miu

About us

NEXUSGUARD
DDoS Mitigation Lab

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

Who is under DDoS attack?
Cyber Warfare News



Sony PlayStation Network struck by DDoS attack, bomb threat ground

Summary: Sony

posted on Twitter u

By Char

Foll

DDoS E

Meetup W

By Jeffrey Roma

Credit Eligible

Me

quite some time and is very much a global problem generally targeting online businesses," says **Dan Holden**, a director at Arbor Networks, a DDoS mitigation company. "Because these targets generally make their core revenue via their Web presence, there is a greater likelihood of the extortion attempt working."

Largest DDoS attack hit PopVote, Hong Kong Democracy voting site

by Pierluigi Paganini on June 23rd, 2014

Largest DDoS attack hit PopVote, Hong Ko voting website. Experts at CloudFlare ob hundred gigabits per second DDoS attack.

The largest ever and most severe Distributed Denial of Service (history has recently hit the online democracy poll promoting opin Hong Kong elections. The system under attack is the PopVote, managed by The University of Hong Kong's Public Opinion Prog system more than half a million votes in less than 30 hours in the referendum.

Anonymous Targets World Cup

Attacks Hit Government, Corporate Sites

12, 2014. Follow Jeffrey @gen_sec

- Cybersecurity: Taking an Economic View

NEWS • HONG KONG • OCCUPY CENTRAL

'Anonymous' hacker group declares cyber war on Hong Kong government, police

Citing mistreatment against Occupy Central protesters, the self-styled 'hacktivist' group threatens to disrupt Hong Kong government websites

Jeremy Blum
jeremy.blum@scmp.com

PUBLISHED : Thursday, 02 October, 2014, 11:36am
UPDATED : Thursday, 02 October, 2014, 12:11pm

The Anonymous hacker logo laid on top of footage from the Occupy Central protests. Photo: SCMP Pictures

Hacker group Anonymous has declared war on the Hong Kong government and hacked into a number of Hong Kong websites, citing the treatment of protesters during Occupy Central as the main impetus for the attack.

DDoS: New Attacks Against Banks

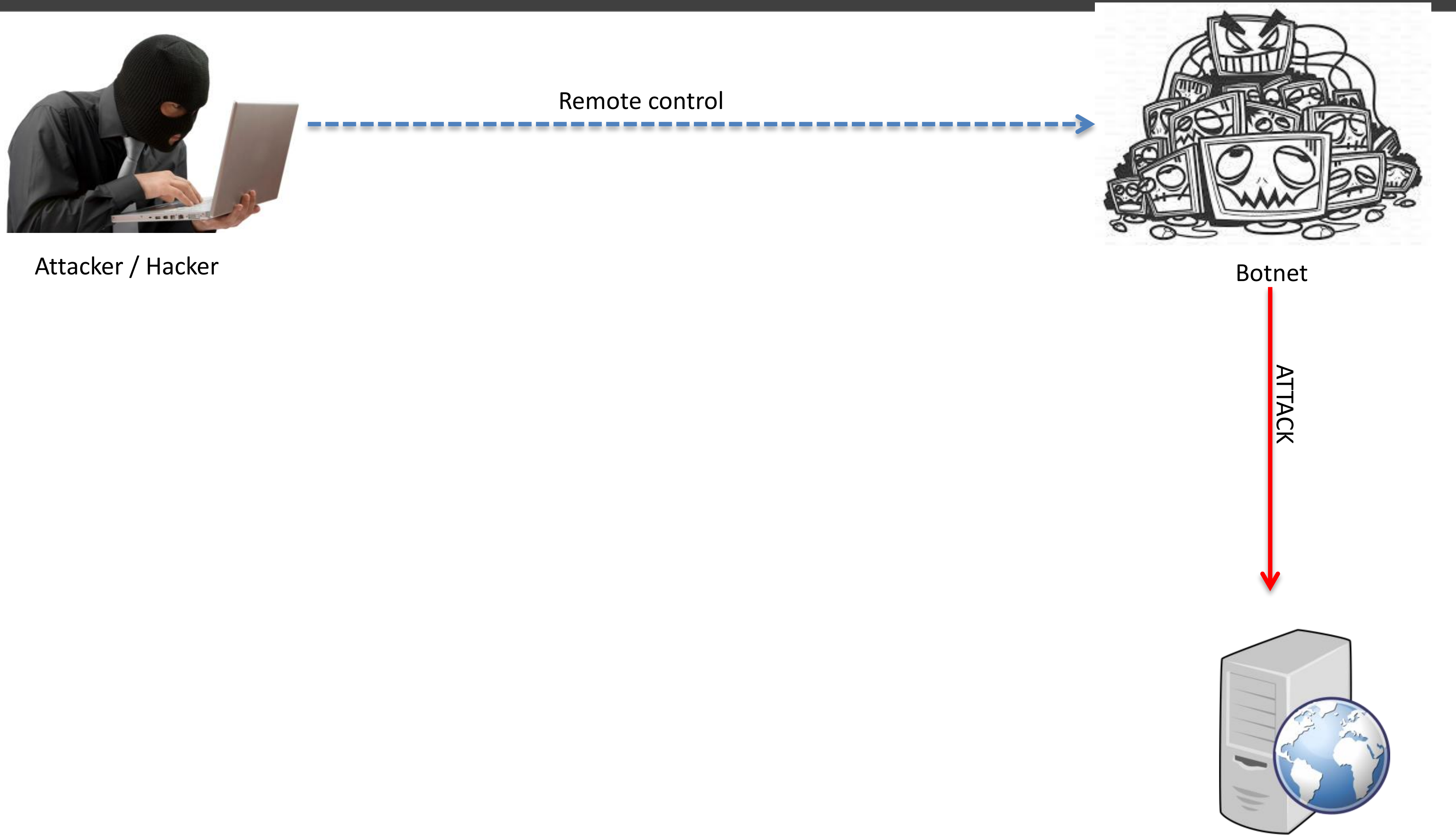
Sources Say Strikes Waged by Same Botnet as Earlier Attacks

By Tracy Kitten, January 29, 2014. Follow Tracy @FraudBlogger

the **European Cyber Army** said Jan. 28 that it had waged targeted **ce attacks** against Bank of America and JPMorgan Chase.

urred from about 10:30 a.m. until 2:30 p.m. ET on Tuesday, says one requested anonymity. "We have not seen anything yet today," the urity Media Group on Jan. 29. Both banks' websites were up and

Is it the full story of Attack?



Remote control

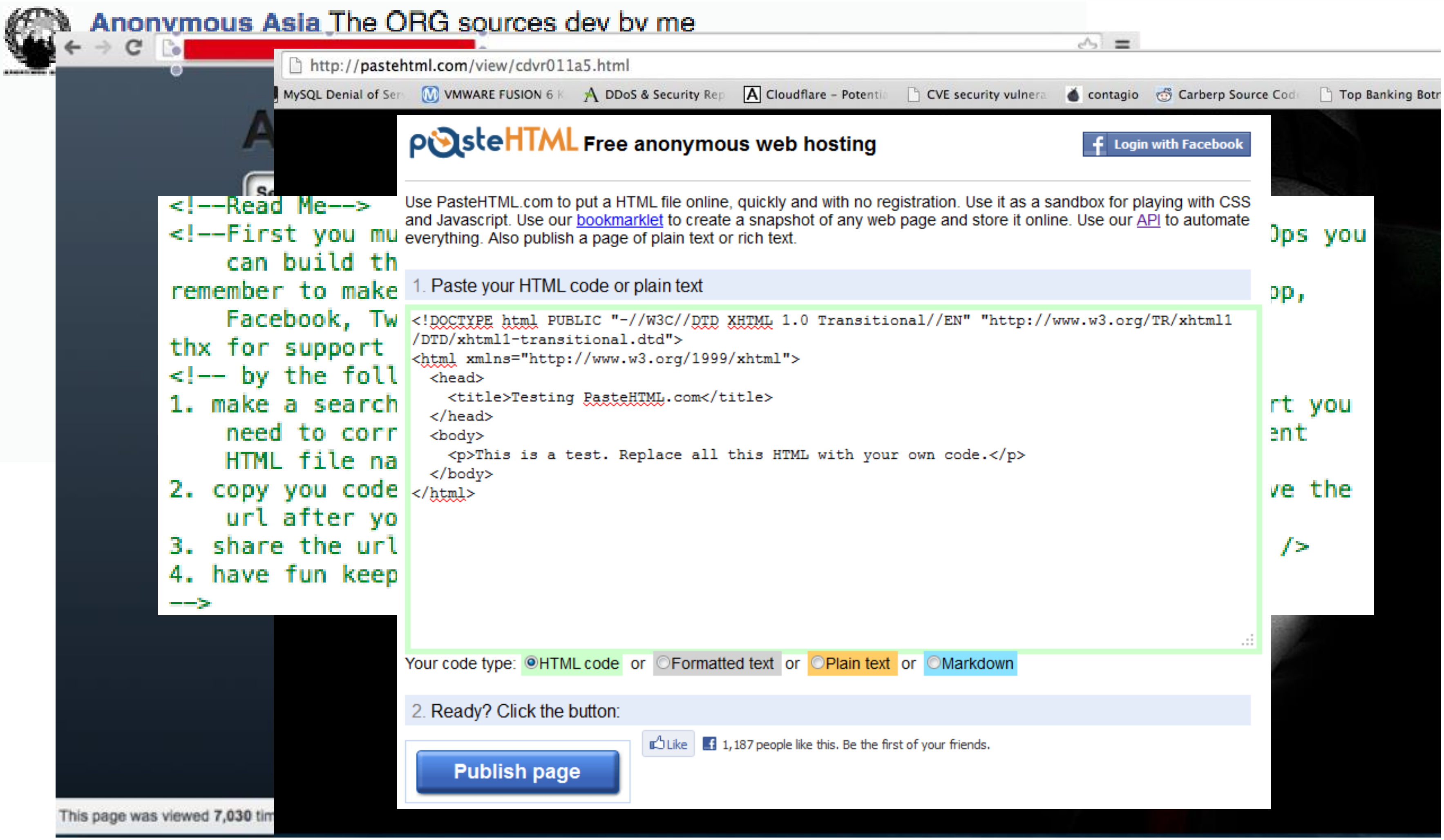
Attacker / Hacker

Botnet

ATTACK

Web server under Attack

Web base DDoS attack Tool - WebHIVE



Anonymous Asia The ORG sources dev by me

http://pastehtml.com/view/cdvr011a5.html

```
<!--Read Me-->
<!--First you mu
    can build th
remember to make
    Facebook, Tw
thx for support
<!-- by the foll
1. make a search
    need to corr
    HTML file na
2. copy you code
    url after yo
3. share the url
4. have fun keep
-->
```

```
Ops you

op,

rt you
ent

ve the

/>
```

pasteHTML Free anonymous web hosting

Use PasteHTML.com to put a HTML file online, quickly and with no registration. Use it as a sandbox for playing with CSS and Javascript. Use our bookmarklet to create a snapshot of any web page and store it online. Use our API to automate everything. Also publish a page of plain text or rich text.

1. Paste your HTML code or plain text

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1
/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Testing PasteHTML.com</title>
  </head>
  <body>
    <p>This is a test. Replace all this HTML with your own code.</p>
  </body>
</html>
```

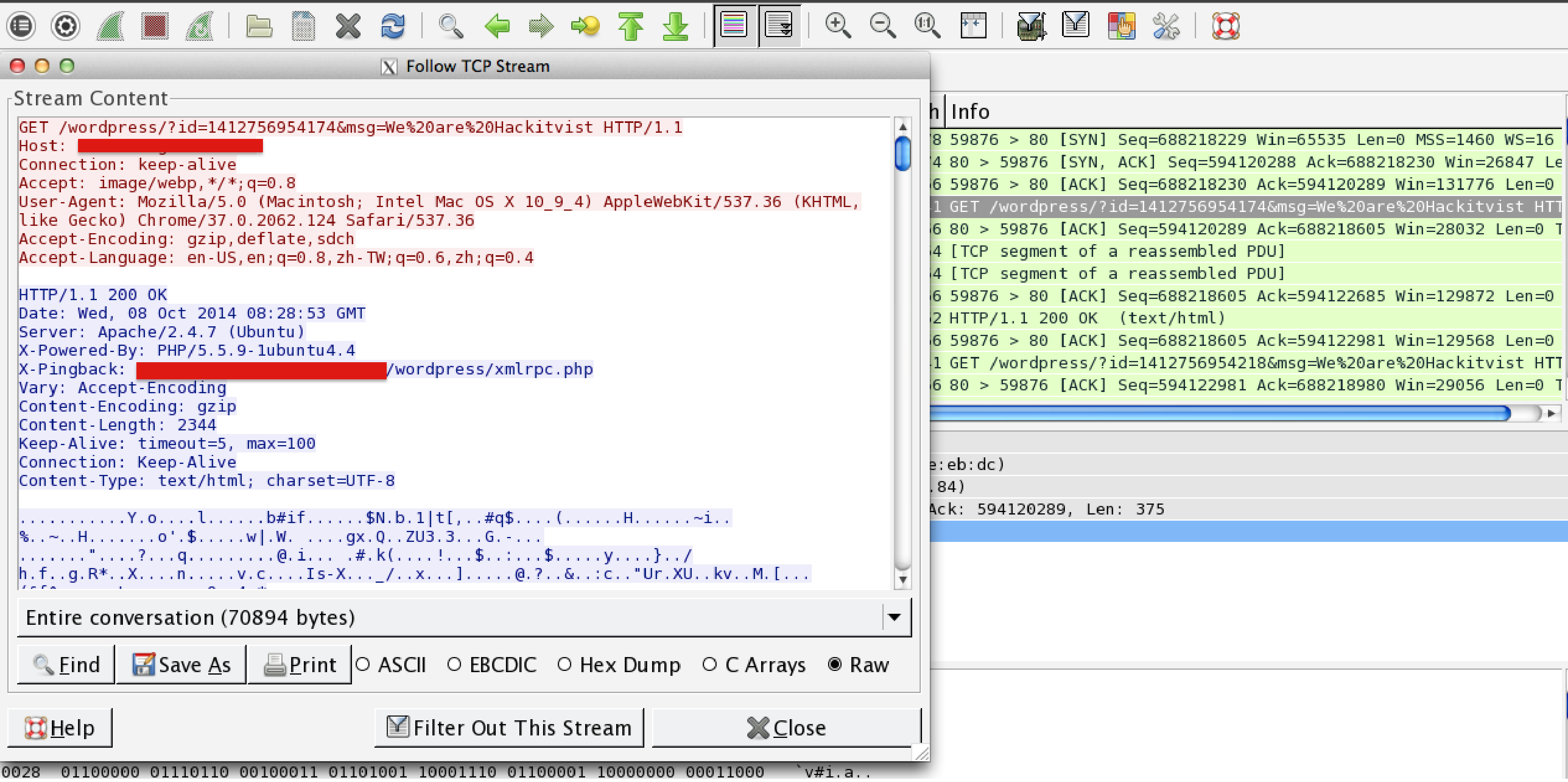
Your code type: ● HTML code or ○ Formatted text or ○ Plain text or ○ Markdown

2. Ready? Click the button:

1,187 people like this. Be the first of your friends.

This page was viewed 7,030 tim

Attack pattern of WebHIVE



```
GET /wordpress/?id=1412756954174&msg=We%20are%20Hackitvist HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept: image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_4) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/37.0.2062.124 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8,zh-TW;q=0.6,zh;q=0.4

HTTP/1.1 200 OK
Date: Wed, 08 Oct 2014 08:28:53 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.4
X-Pingback: [redacted]/wordpress/xmlrpc.php
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 2344
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

..........Y.o....l......b#if......$N.b.1|t[,..#q$....(......H......~i..
%..~..H.......o'.$.....w|.W.  ....gx.Q..ZU3.3...G.-...
......."....?...q.........@.i...  .#.k(....!...$..:...$.....y....}../
h.f..g.R*..X....n.....v.c....Is-X..._/..x...].....@.?..&..:c.."Ur.XU..kv..M.[...
```

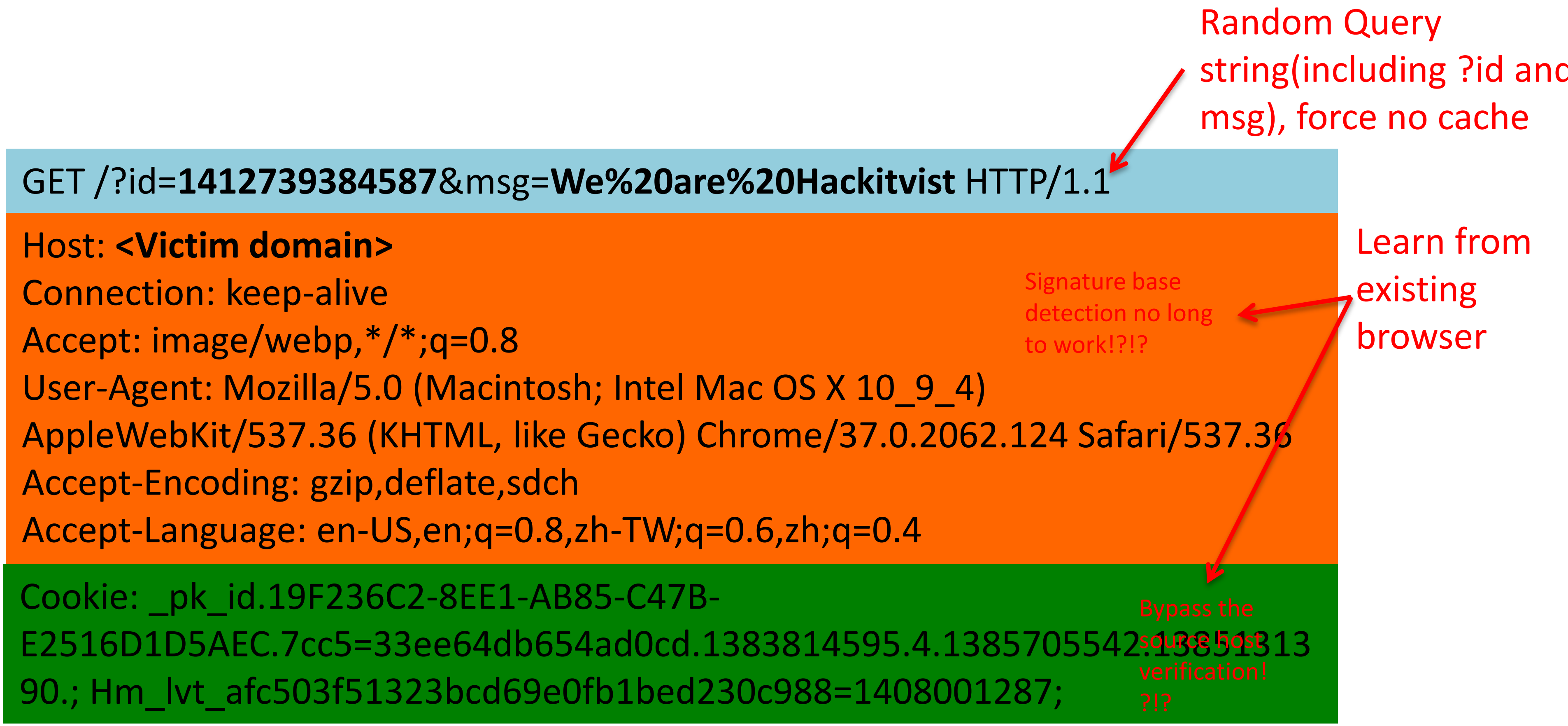
```
8 59876 > 80 [SYN] Seq=688218229 Win=65535 Len=0 MSS=1460 WS=16
4 80 > 59876 [SYN, ACK] Seq=594120288 Ack=688218230 Win=26847 Le
6 59876 > 80 [ACK] Seq=688218230 Ack=594120289 Win=131776 Len=0
1 GET /wordpress/?id=1412756954174&msg=We%20are%20Hackitvist HTT
6 80 > 59876 [ACK] Seq=594120289 Ack=688218605 Win=28032 Len=0 T
4 [TCP segment of a reassembled PDU]
4 [TCP segment of a reassembled PDU]
6 59876 > 80 [ACK] Seq=688218605 Ack=594122685 Win=129872 Len=0
2 HTTP/1.1 200 OK  (text/html)
6 59876 > 80 [ACK] Seq=688218605 Ack=594122981 Win=129568 Len=0
1 GET /wordpress/?id=1412756954218&msg=We%20are%20Hackitvist HTT
6 80 > 59876 [ACK] Seq=594122981 Ack=688218980 Win=29056 Len=0 T

e:eb:dc)
.84)
Ack: 594120289, Len: 375

0028  01100000 01110110 00100011 01101001 10001110 01100001 10000000 00011000   `v#i.a..
```

NEXUSGUARD

The challenge of mitigation



```
GET /?id=14127393845873&msg=We%20are%20Hackitvist HTTP/1.1
Host: <Victim domain>
Connection: keep-alive
Accept: image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_4)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.124 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8,zh-TW;q=0.6,zh;q=0.4
Cookie: _pk_id.19F236C2-8EE1-AB85-C47B-
E2516D1D5AEC.7cc5=33ee64db654ad0cd.1383814595.4.1385705542.13851313
90.; Hm_lvt_afc503f51323bcd69e0fb1bed230c988=1408001287;
```

Random Query string(including ?id and msg), force no cache

Learn from existing browser

Signature base detection no long to work!?!?

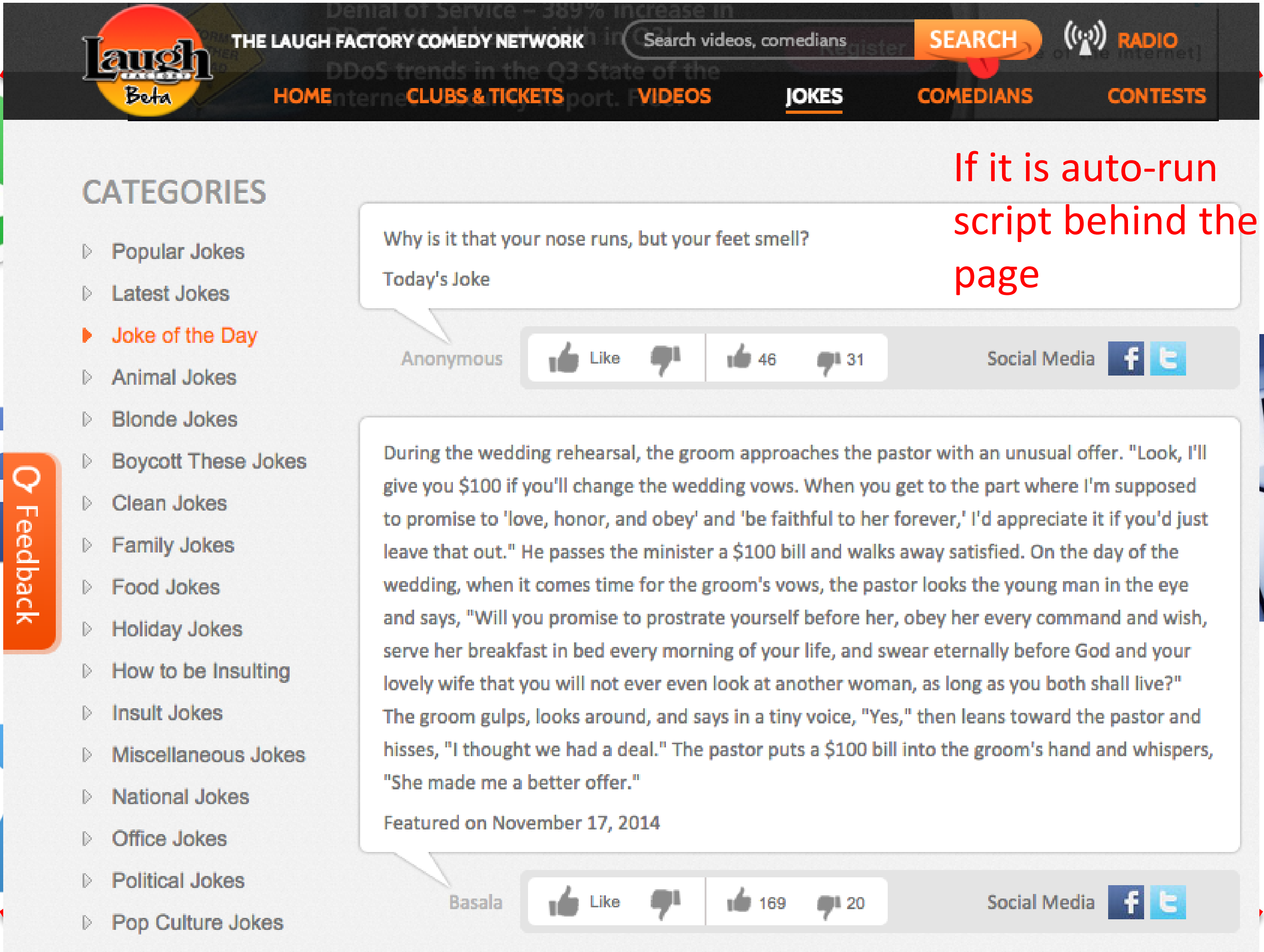
Bypass the source host verification! ?!?

Web base Attack Tools VS traditional attack tool

- No need to install extra things, e.g. python, java, .NET, library, etc
- Cross platform available e.g. including Smart Phone, Windows, IOS, Mac, etc
- Easy to share
- No significant/interesting signature
- Any one can build the code with free online tools

  (e.g. pastehtml.com, pastebin.com, etc)
- Customize, e.g. auto-run script, hidden inside webpage

Risk and Impact



CATEGORIES

- Popular Jokes
- Latest Jokes
- Joke of the Day
- Animal Jokes
- Blonde Jokes
- Boycott These Jokes
- Clean Jokes
- Family Jokes
- Food Jokes
- Holiday Jokes
- How to be Insulting
- Insult Jokes
- Miscellaneous Jokes
- National Jokes
- Office Jokes
- Political Jokes
- Pop Culture Jokes

Why is it that your nose runs, but your feet smell?

Today's Joke

Anonymous | Like | 46 | 31 | Social Media

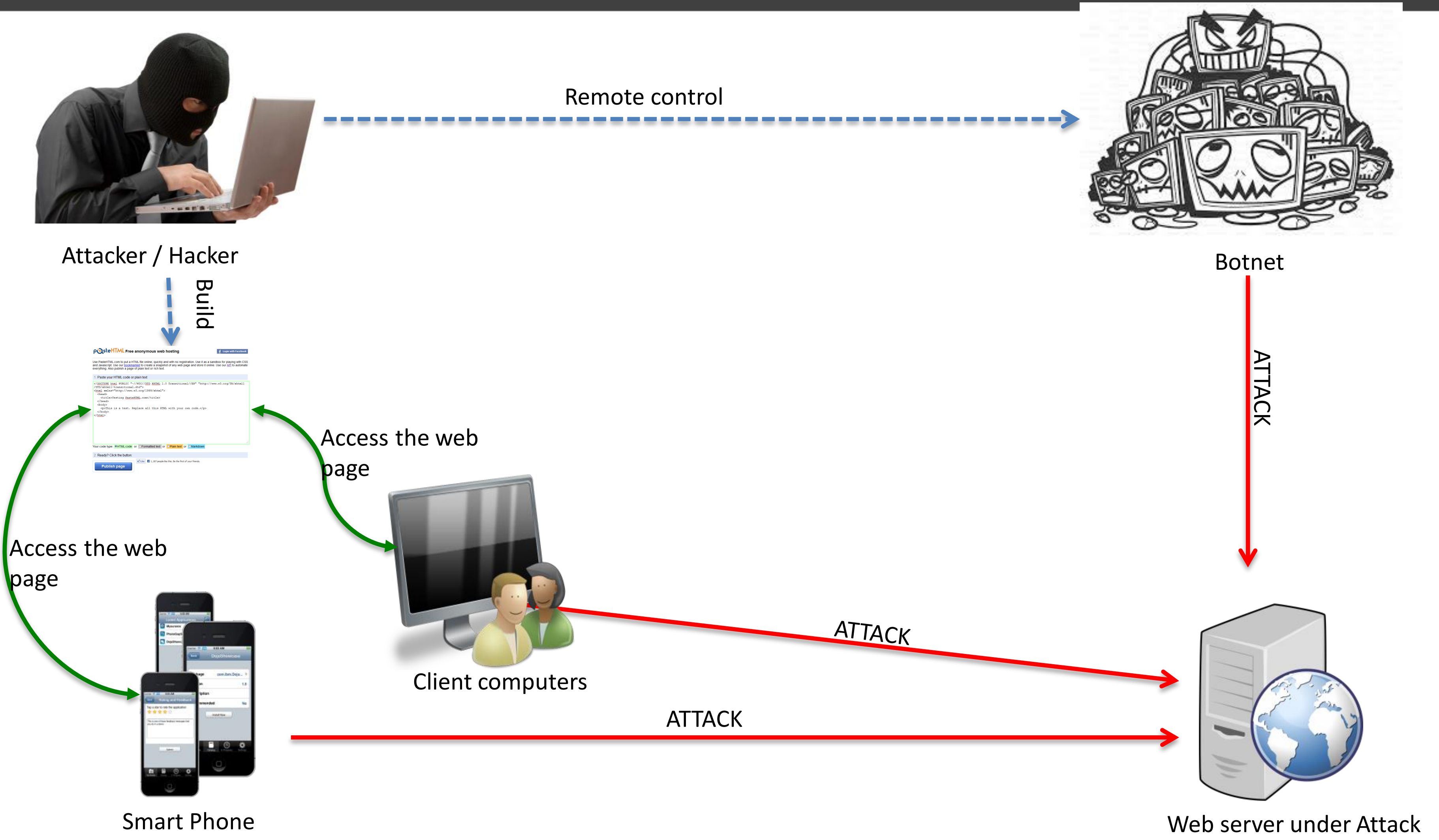
During the wedding rehearsal, the groom approaches the pastor with an unusual offer. "Look, I'll give you $100 if you'll change the wedding vows. When you get to the part where I'm supposed to promise to 'love, honor, and obey' and 'be faithful to her forever,' I'd appreciate it if you'd just leave that out." He passes the minister a $100 bill and walks away satisfied. On the day of the wedding, when it comes time for the groom's vows, the pastor looks the young man in the eye and says, "Will you promise to prostrate yourself before her, obey her every command and wish, serve her breakfast in bed every morning of your life, and swear eternally before God and your lovely wife that you will not ever even look at another woman, as long as you both shall live?" The groom gulps, looks around, and says in a tiny voice, "Yes," then leans toward the pastor and hisses, "I thought we had a deal." The pastor puts a $100 bill into the groom's hand and whispers, "She made me a better offer."

Featured on November 17, 2014

Basala | Like | 169 | 20 | Social Media

If it is auto-run script behind the page

Botnet + WebHive



Remote control

Attacker / Hacker

Build

Botnet

ATTACK

pasteHTML Free anonymous web hosting

Use PasteHTML.com to put a HTML file online, quickly and with no registration. Use it as a sandbox for playing with CSS and Javascript. Use our bookmarklet to create a snapshot of any web page and store it online. Use our API to automate everything. Also publish a page of plain text or rich text.

1. Paste your HTML code or plain text

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1
/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Testing PasteHTML.com</title>
  </head>
  <body>
    <p>This is a test. Replace all this HTML with your own code.</p>
  </body>
</html>
```

Your code type: ● HTML code or ○ Formatted text or ○ Plain text or ○ Markdown

2. Ready? Click the button:

1,187 people like this. Be the first of your friends.

Access the web page

Access the web page

Client computers

ATTACK

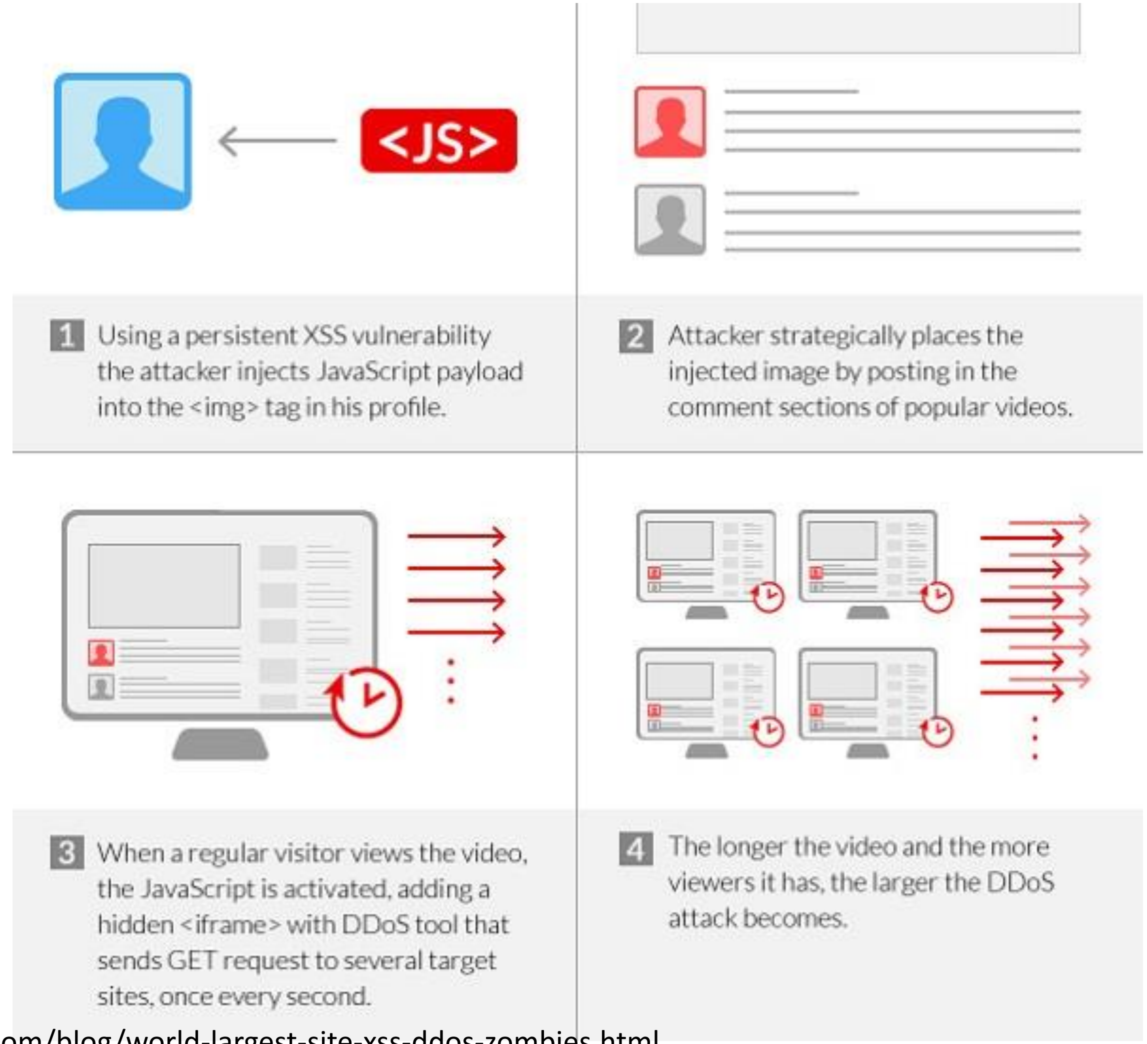
ATTACK

Smart Phone

Web server under Attack

NEXUSGUARD™

Persistent cross-site scripting(XSS) used and injected into <img> tag



1 Using a persistent XSS vulnerability the attacker injects JavaScript payload into the <img> tag in his profile.

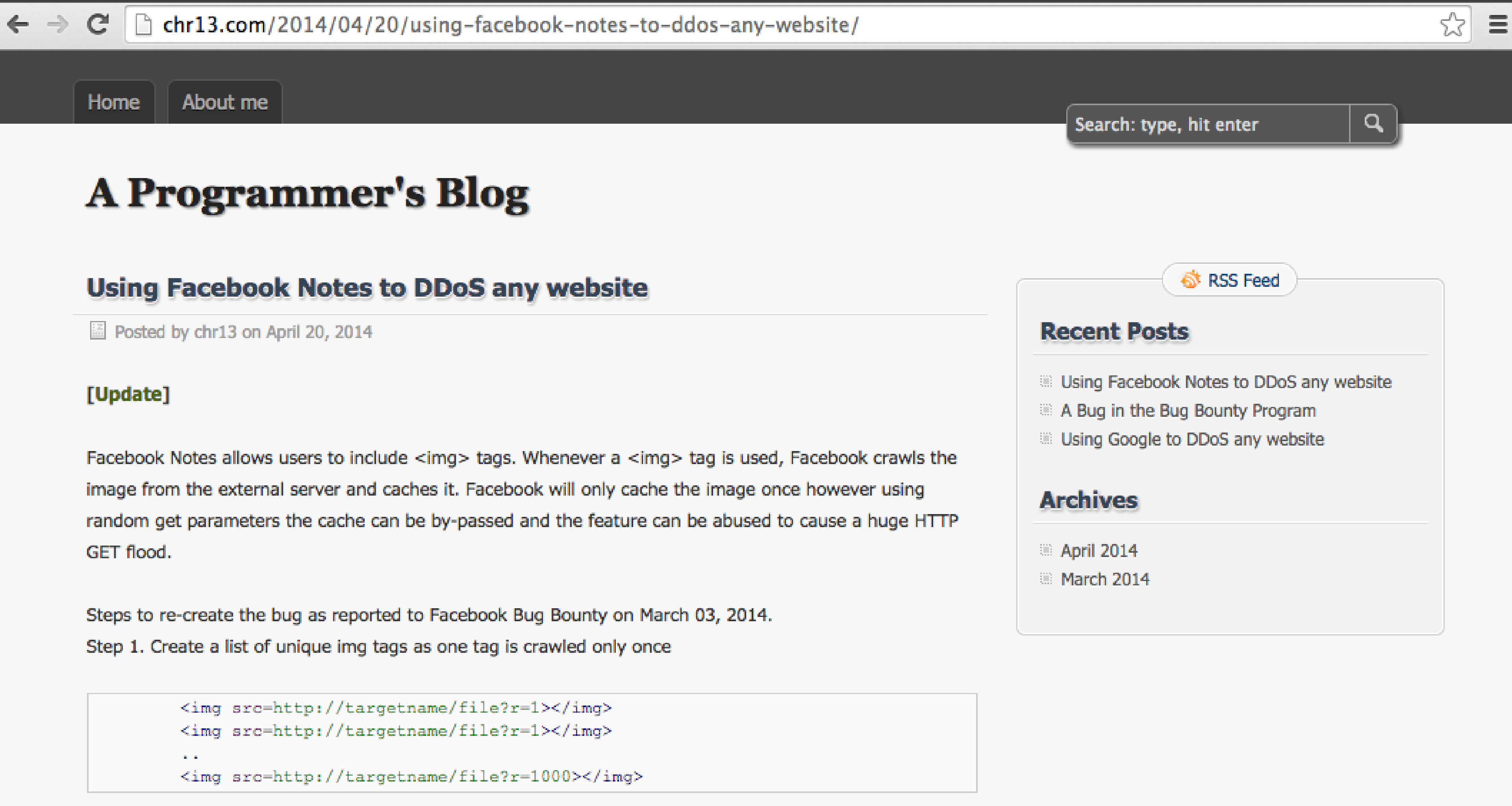
2 Attacker strategically places the injected image by posting in the comment sections of popular videos.

3 When a regular visitor views the video, the JavaScript is activated, adding a hidden <iframe> with DDoS tool that sends GET request to several target sites, once every second.

4 The longer the video and the more viewers it has, the larger the DDoS attack becomes.

Ref: http://www.incapsula.com/blog/world-largest-site-xss-ddos-zombies.html

Facebook Notes to DDoS any website



chr13.com/2014/04/20/using-facebook-notes-to-ddos-any-website/
Home
About me
Search: type, hit enter

A Programmer's Blog

Using Facebook Notes to DDoS any website

Posted by chr13 on April 20, 2014

[Update]

Facebook Notes allows users to include <img> tags. Whenever a <img> tag is used, Facebook crawls the image from the external server and caches it. Facebook will only cache the image once however using random get parameters the cache can be by-passed and the feature can be abused to cause a huge HTTP GET flood.

Steps to re-create the bug as reported to Facebook Bug Bounty on March 03, 2014.
Step 1. Create a list of unique img tags as one tag is crawled only once

```
        <img src=http://targetname/file?r=1></img>
        <img src=http://targetname/file?r=1></img>
        ..
        <img src=http://targetname/file?r=1000></img>
```

RSS Feed

Recent Posts

- Using Facebook Notes to DDoS any website
- A Bug in the Bug Bounty Program
- Using Google to DDoS any website

Archives

- April 2014
- March 2014

Incapsula's Blog

03
Apr
2014

One of World's Largest Websites Hacked: Turns Visitors into "DDoS Zombies"

By Ronen Atias

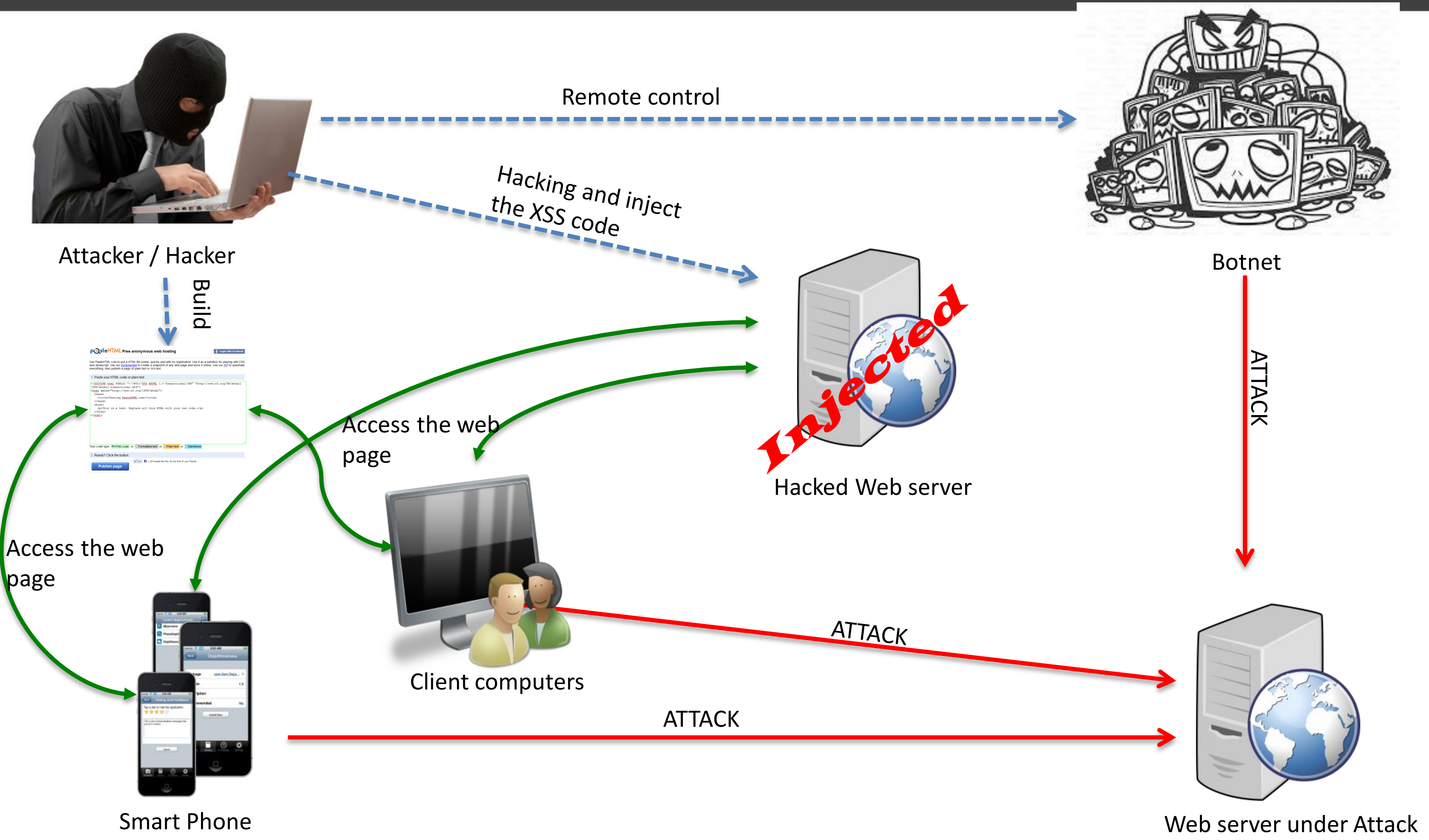
Yesterday we mitigated a unique application layer DDoS attack against one of our clients. The attack was carried out using traffic hijacking techniques, which flooded our client with over 20 ET requests originating from the browsers of over 22,000 Intern ll turned into unwilling accomplices by the offender.

What makes this case especially interesting is the fact that the attack was enabled by a vulnerability in one of the world's largest and most popular sites - one of the domains on Alexa's "Top 50" list.

We can't disclose the domain name in question at this time, as our team is now working to resolve the breach. However, we will provide further details, once the vulnerability is fixed.

Having said that, we can already describe the method used by the attackers, in the hopes that it will help prevent similar abuse of other websites.

Botnet + WebHive + Injected Web server



pasteHTML Free anonymous web hosting

Use PasteHTML.com to put a HTML file online, quickly and with no registration. Use it as a sandbox for playing with CSS and Javascript. Use our bookmarklet to create a snapshot of any web page and store it online. Use our API to automate everything. Also publish a page of plain text or rich text.

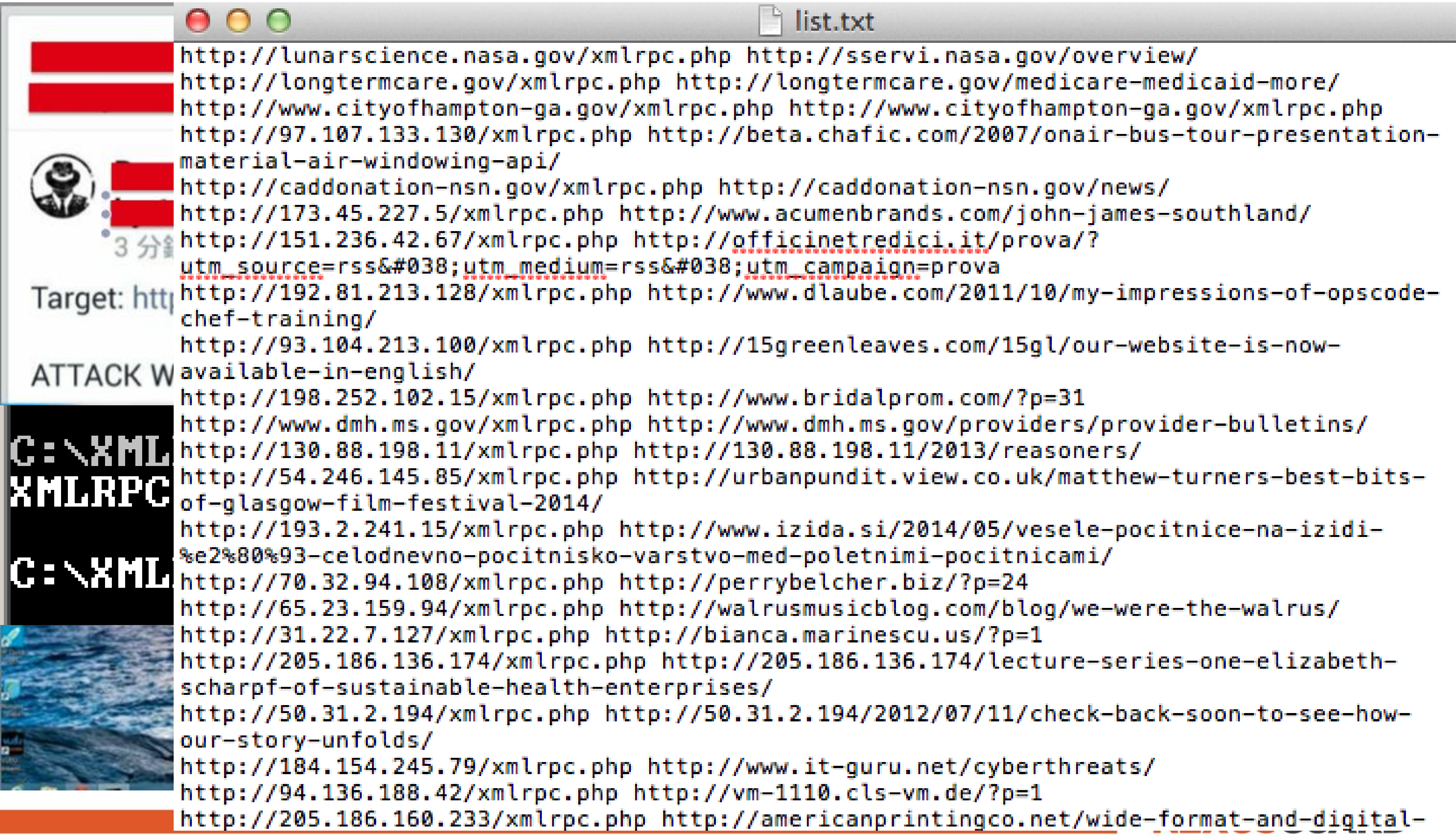
1. Paste your HTML code or plain text

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1
/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>Testing PasteHTML.com</title>
  </head>
  <body>
    <p>This is a test. Replace all this HTML with your own code.</p>
  </body>
</html>
```

Your code type: ● HTML code or ○ Formatted text or ○ Plain text or ○ Markdown

2. Ready? Click the button:

Layer 7 Amplified attack - XMLRPC



[redacted]

[redacted]

3 分鐘

Target: http

ATTACK W

C:\XML

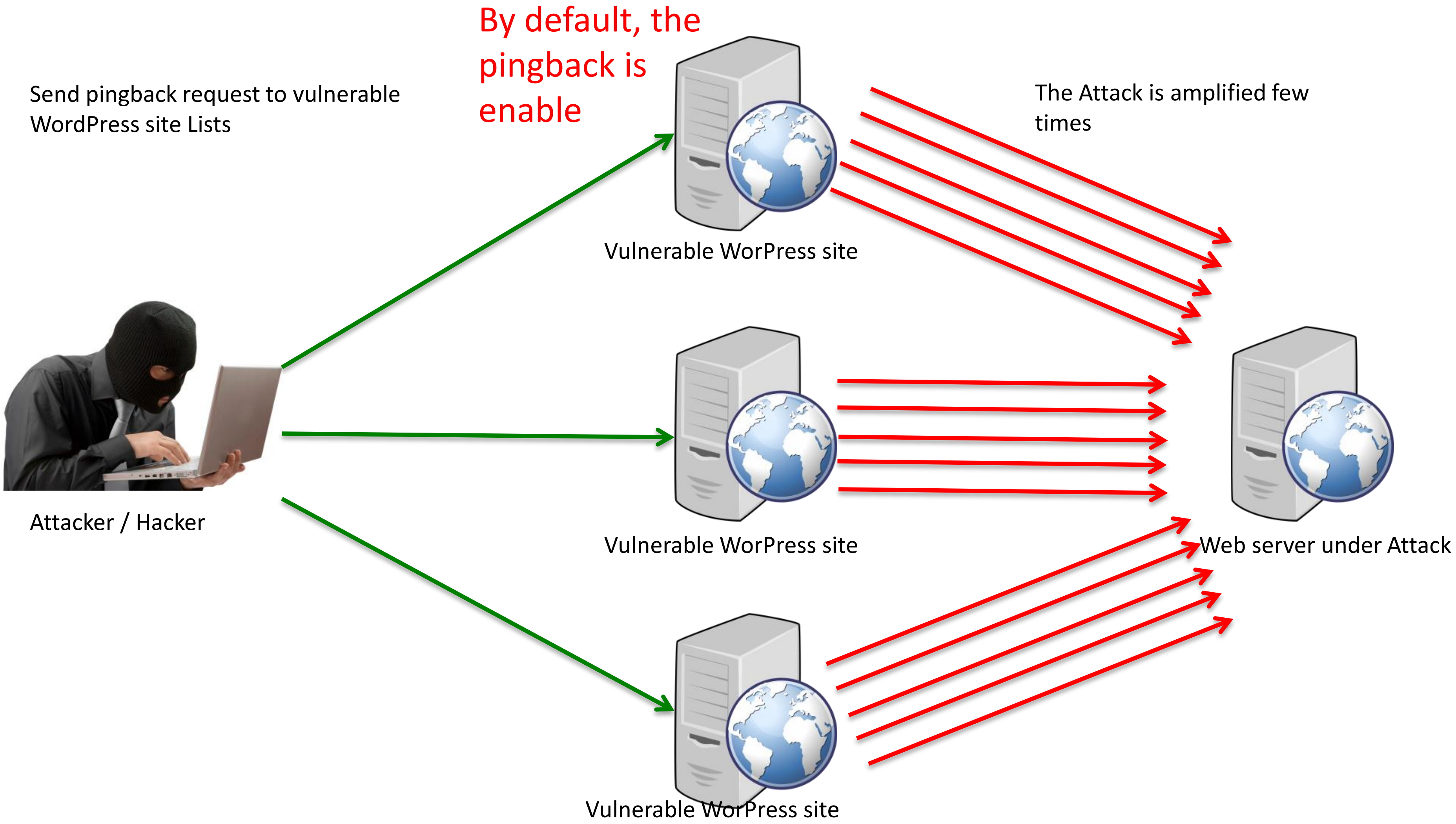
XMLRPC

C:\XML

list.txt

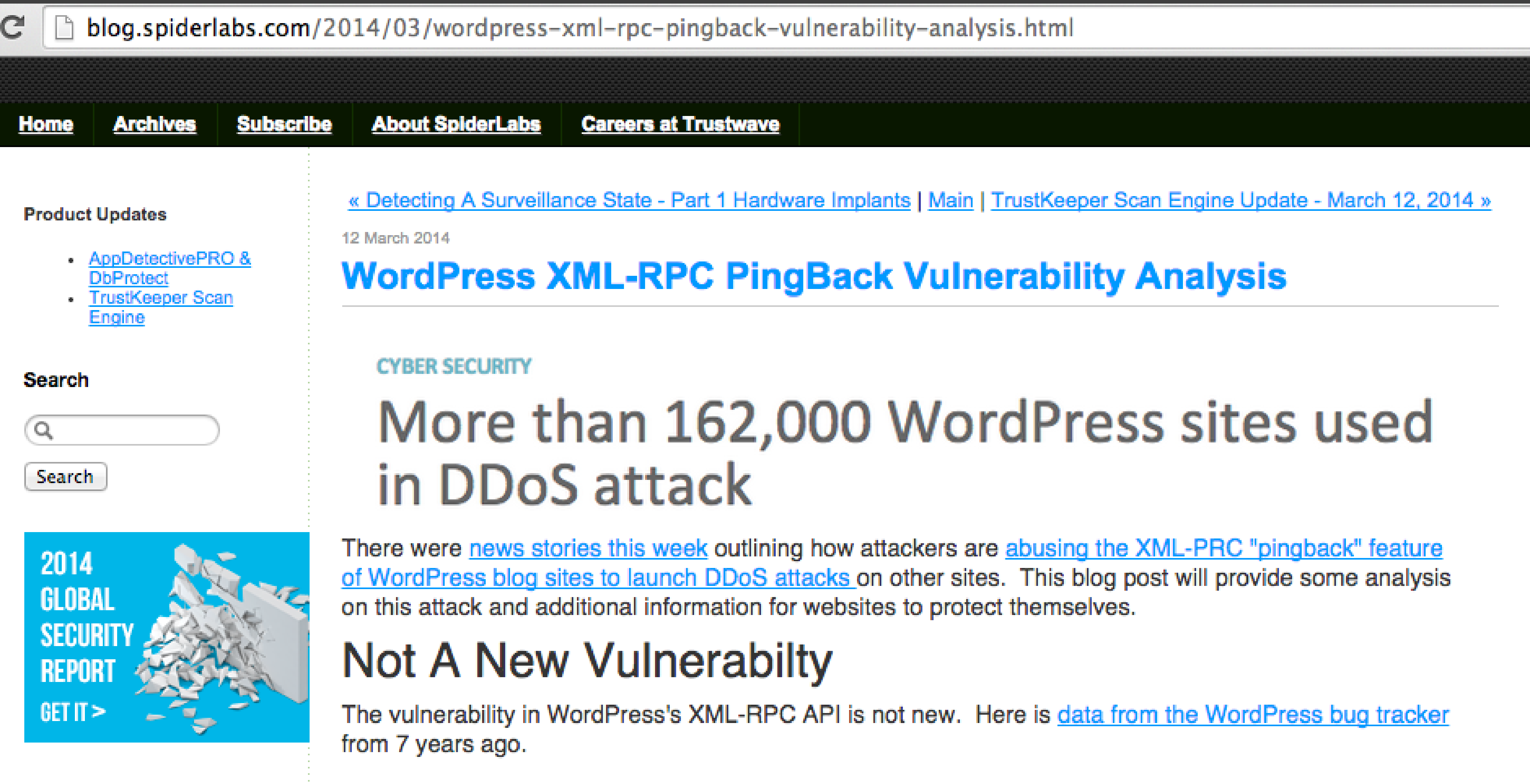
```
http://lunarscience.nasa.gov/xmlrpc.php http://sservi.nasa.gov/overview/
http://longtermcare.gov/xmlrpc.php http://longtermcare.gov/medicare-medicaid-more/
http://www.cityofhampton-ga.gov/xmlrpc.php http://www.cityofhampton-ga.gov/xmlrpc.php
http://97.107.133.130/xmlrpc.php http://beta.chafic.com/2007/onair-bus-tour-presentation-material-air-windowing-api/
http://caddonation-nsn.gov/xmlrpc.php http://caddonation-nsn.gov/news/
http://173.45.227.5/xmlrpc.php http://www.acumenbrands.com/john-james-southland/
http://151.236.42.67/xmlrpc.php http://officinetredici.it/prova/?utm_source=rss&#038;utm_medium=rss&#038;utm_campaign=prova
http://192.81.213.128/xmlrpc.php http://www.dlaube.com/2011/10/my-impressions-of-opscode-chef-training/
http://93.104.213.100/xmlrpc.php http://15greenleaves.com/15gl/our-website-is-now-available-in-english/
http://198.252.102.15/xmlrpc.php http://www.bridalprom.com/?p=31
http://www.dmh.ms.gov/xmlrpc.php http://www.dmh.ms.gov/providers/provider-bulletins/
http://130.88.198.11/xmlrpc.php http://130.88.198.11/2013/reasoners/
http://54.246.145.85/xmlrpc.php http://urbanpundit.view.co.uk/matthew-turners-best-bits-of-glasgow-film-festival-2014/
http://193.2.241.15/xmlrpc.php http://www.izida.si/2014/05/vesele-pocitnice-na-izidi-%e2%80%93-celodnevno-pocitnisko-varstvo-med-poletnimi-pocitnicami/
http://70.32.94.108/xmlrpc.php http://perrybelcher.biz/?p=24
http://65.23.159.94/xmlrpc.php http://walrusmusicblog.com/blog/we-were-the-walrus/
http://31.22.7.127/xmlrpc.php http://bianca.marinescu.us/?p=1
http://205.186.136.174/xmlrpc.php http://205.186.136.174/lecture-series-one-elizabeth-scharpf-of-sustainable-health-enterprises/
http://50.31.2.194/xmlrpc.php http://50.31.2.194/2012/07/11/check-back-soon-to-see-how-our-story-unfolds/
http://184.154.245.79/xmlrpc.php http://www.it-guru.net/cyberthreats/
http://94.136.188.42/xmlrpc.php http://vm-1110.cls-vm.de/?p=1
http://205.186.160.233/xmlrpc.php http://americanprintingco.net/wide-format-and-digital-
```

Attacker amplify the DDoS Attack from single computer



By default, the pingback is enable
Send pingback request to vulnerable WordPress site Lists
The Attack is amplified few times
Vulnerable WorPress site
Attacker / Hacker
Vulnerable WorPress site
Web server under Attack
Vulnerable WorPress site

Impact and Risk



blog.spiderlabs.com/2014/03/wordpress-xml-rpc-pingback-vulnerability-analysis.html

Product Updates

- AppDetectivePRO & DbProtect
- TrustKeeper Scan Engine

Search

« Detecting A Surveillance State - Part 1 Hardware Implants | Main | TrustKeeper Scan Engine Update - March 12, 2014 »

12 March 2014

WordPress XML-RPC PingBack Vulnerability Analysis

CYBER SECURITY

More than 162,000 WordPress sites used in DDoS attack

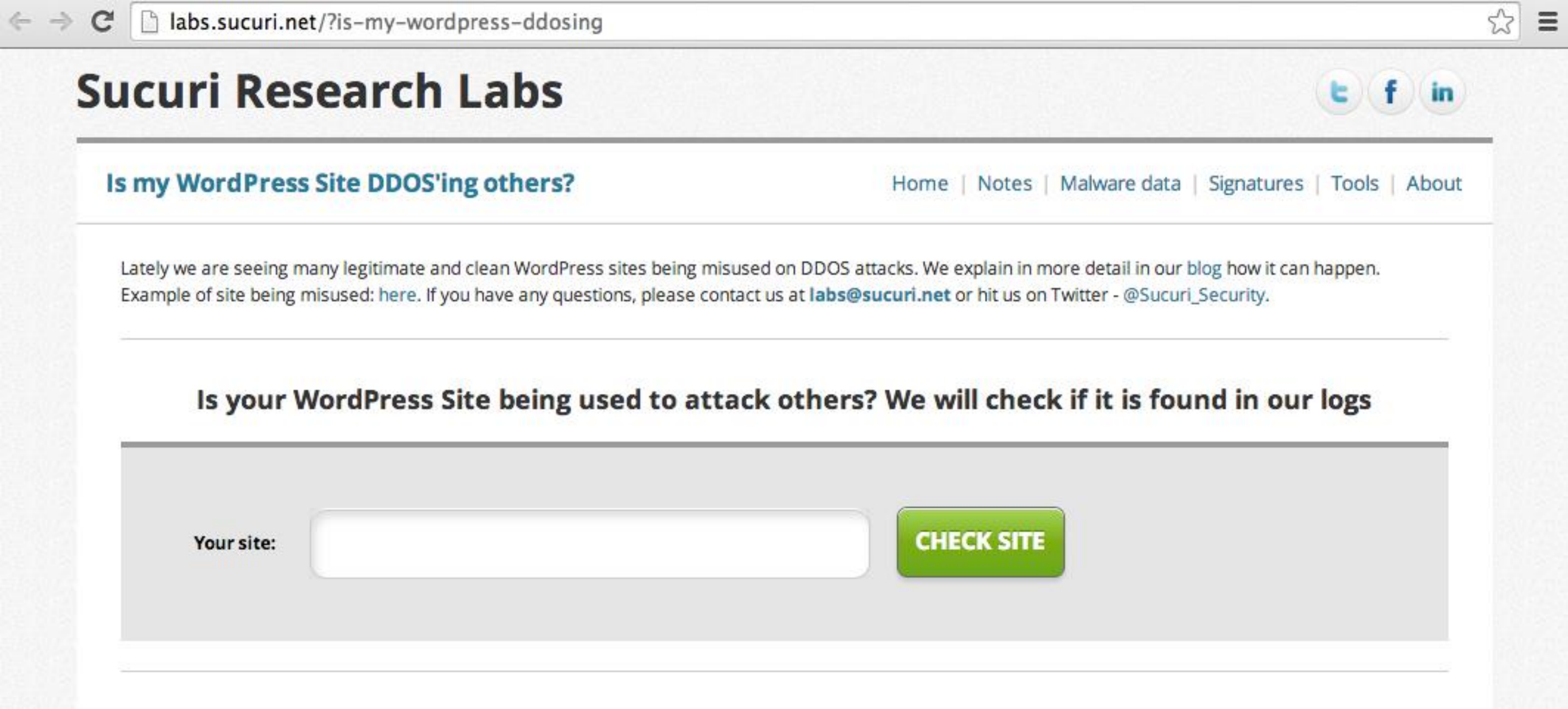
There were news stories this week outlining how attackers are abusing the XML-PRC "pingback" feature of WordPress blog sites to launch DDoS attacks on other sites. This blog post will provide some analysis on this attack and additional information for websites to protect themselves.

Not A New Vulnerabilty

The vulnerability in WordPress's XML-RPC API is not new. Here is data from the WordPress bug tracker from 7 years ago.

NEXUSGUARD

Online checking for WordPress site



labs.sucuri.net/?is-my-wordpress-ddosing

Sucuri Research Labs

Is my WordPress Site DDOS'ing others?

Lately we are seeing many legitimate and clean WordPress sites being misused on DDOS attacks. We explain in more detail in our blog how it can happen. Example of site being misused: here. If you have any questions, please contact us at **labs@sucuri.net** or hit us on Twitter - @Sucuri_Security.

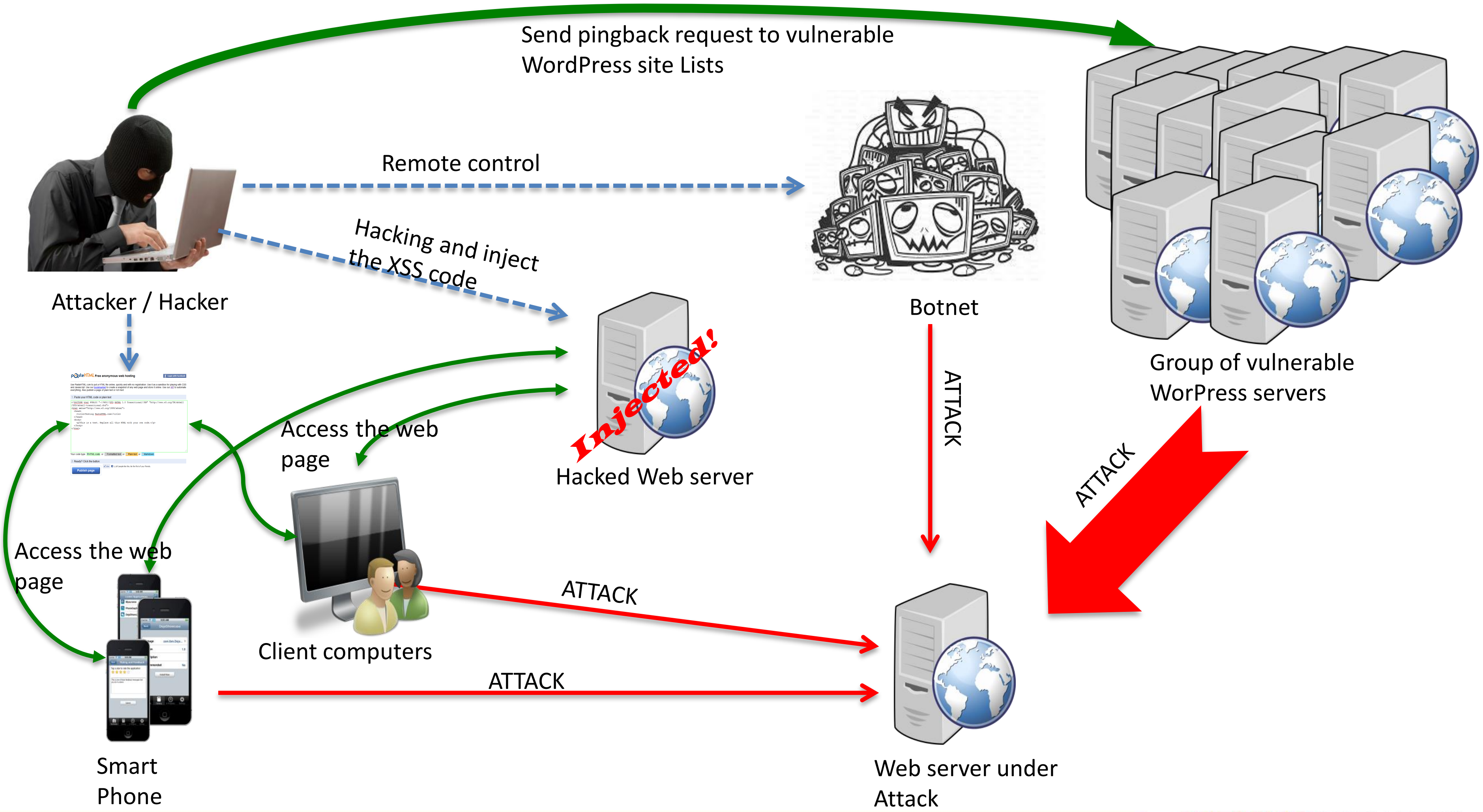
Is your WordPress Site being used to attack others? We will check if it is found in our logs

Your site:

WordPress XML-RPC PingBack Vulnerability

- Any WordPress site with Pingback enabled can be used in DDoS attack against other sites
- By default, the pingback is enabled
- From some hacker forums, they already provided the attack tool and vulnerable WordPress List
- Statistics from Spider Lab, it is more than 162,000 site used in DDoS attack (March 2014)
- The vulnerability in WordPress's XMP-RPC API is not new, it is over 7 years ago!!!!

Attack Representation



Send pingback request to vulnerable WordPress site Lists

Remote control

Hacking and inject the XSS code

Attacker / Hacker

Botnet

Group of vulnerable WorPress servers

Access the web page

Injected!

Hacked Web server

ATTACK

ATTACK

Access the web page

Client computers

ATTACK

ATTACK

Smart Phone

Web server under Attack

NEXUSGUARD

Conclusion

- Who are the victims today?
  - Web server under attack
  - People who open the injected/hacked web page
  - vulnerable web server amplify and forward the attack
- The Trend of cyber war is changed, WE need to build up our security sense to prevent the attack from us
- Information security start from everyone, today!!!

Thank You!

tony.miu@nexusguard.com

http://www.nexusguard.com

Technical detail please visit

http://miutony.blogspot.hk/