



The role of JANET CSIRT

Bradley Freeman
JANET(UK) CSIRT Member
UKNOF 15 – 21st January 2010

bradley.freeman@ja.net



What to expect

Overview of how we detect and deal with incidents on JANET

Including;

- Our perspective
- What our role is
- Conficker
- Using Netflow to find nasties
- Copyright Infringements
- Other notable incidents

We're unique



Our Network \neq Your Network

Cheap 40Gbs+ security hardware only exists in my
dreams...



Academic perspective

- We believe in the good of the Internet, openness, freedom and privacy.
- That means an open network
- No blocked ports, very rarely blocked IPs
- Deep Packet Inspection (DPI) not practical, possibly not legal
- Legal issues, its not our data, scanning?



What CSIRTs Do

Names may vary;

- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CERT (Computer Emergency Response Team)

Co-ordinate with our community and other CERTs, ISPs

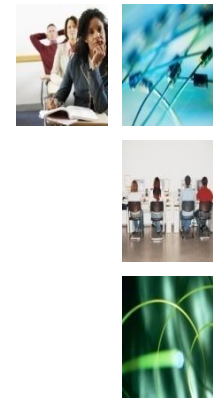
Provide advice, and assistance in relation to security with confidentiality

Scalable security tools

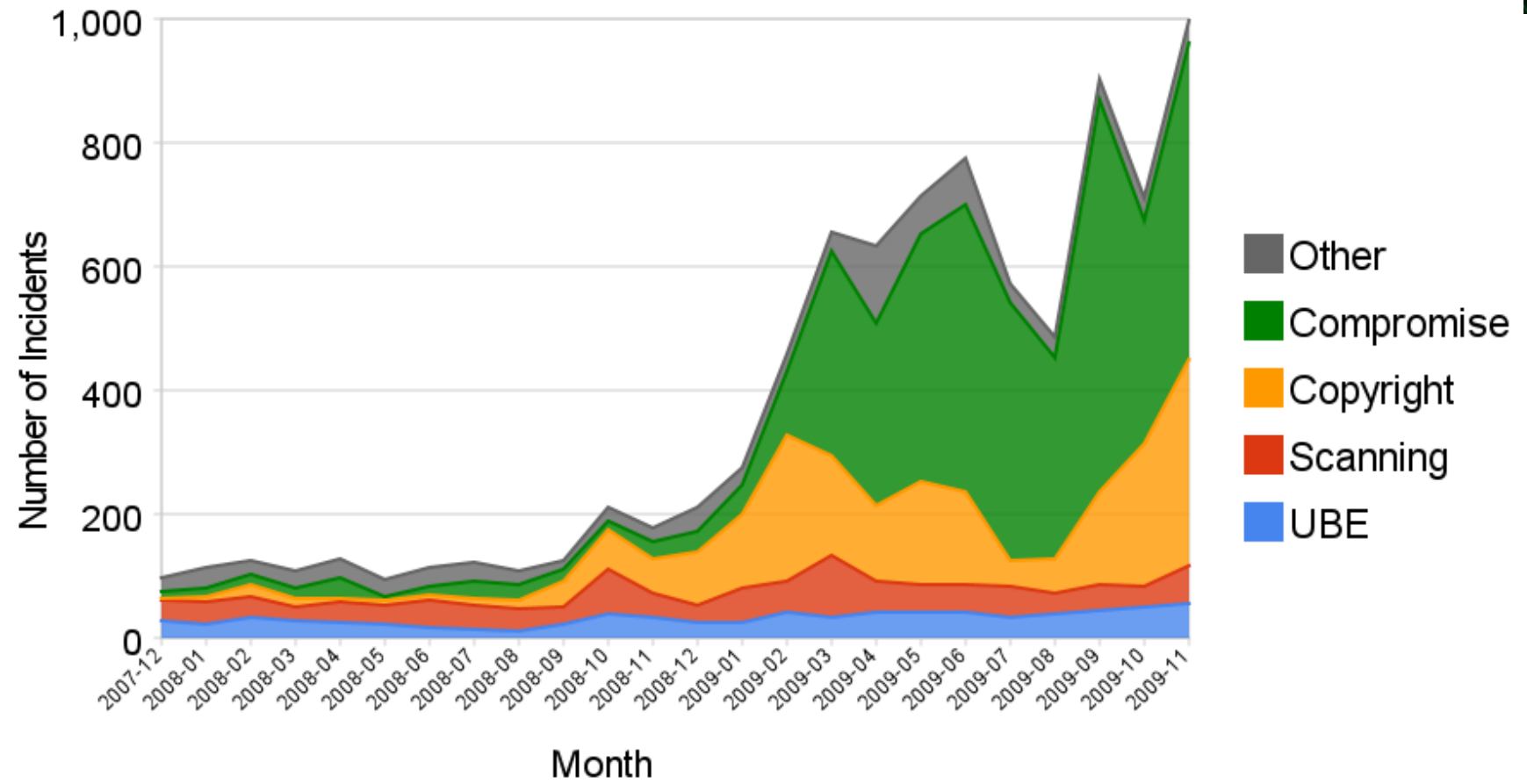
- JANET Acceptable Use Policy
- JANET Security Policy



Pretty Graph



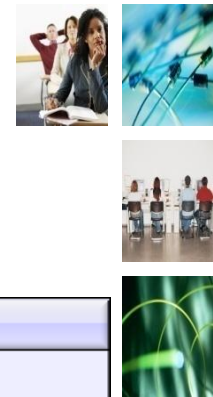
Incident Classification per Month



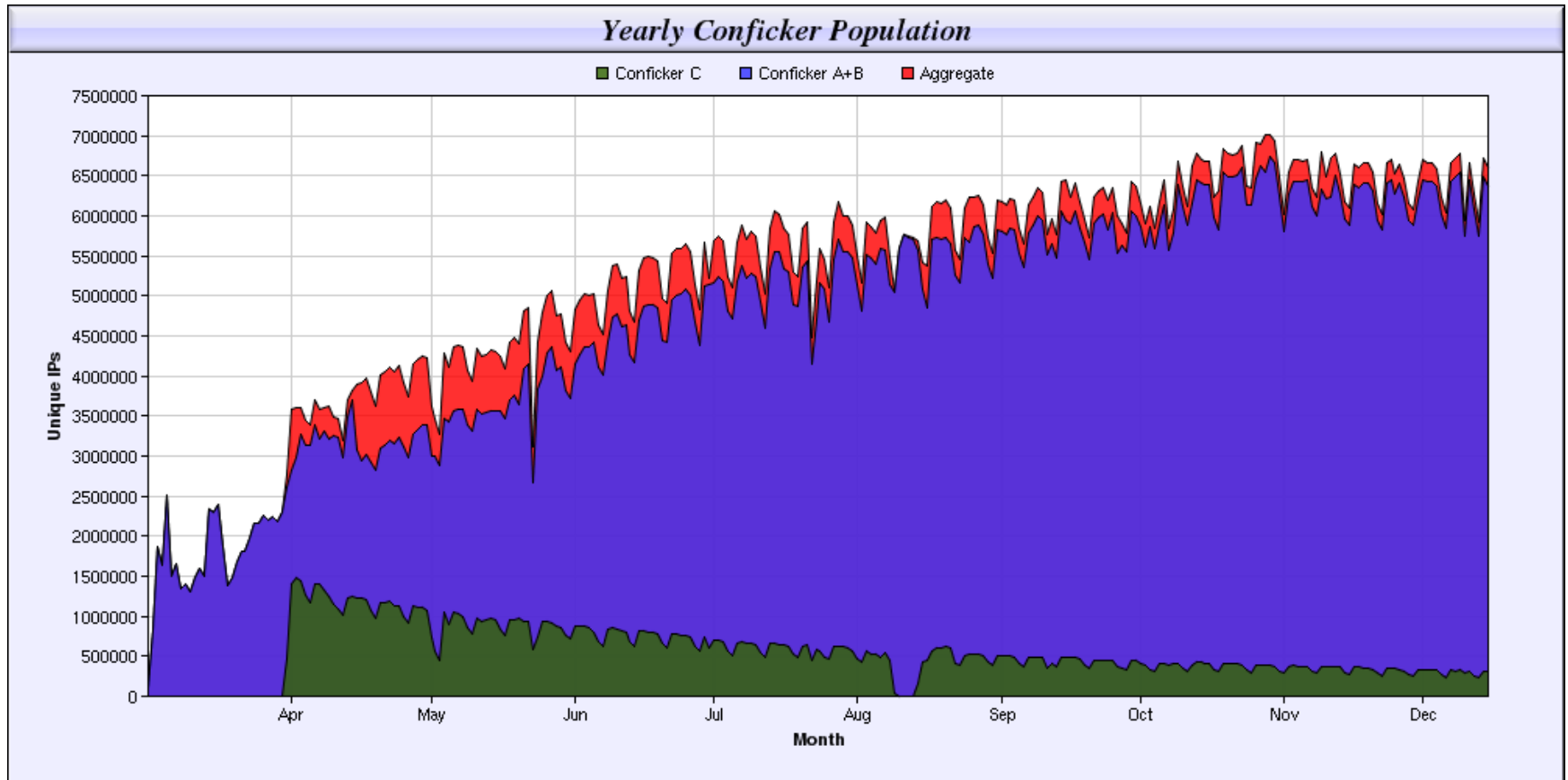


Conficker is still a threat

- Admirable method of updating using DNS
- Led ICANN to develop the Expedited Registry Security Process
- Currently infected 6.8million IPs from 12,000 ASNs
(December 2009 – source Shadowserver.org)



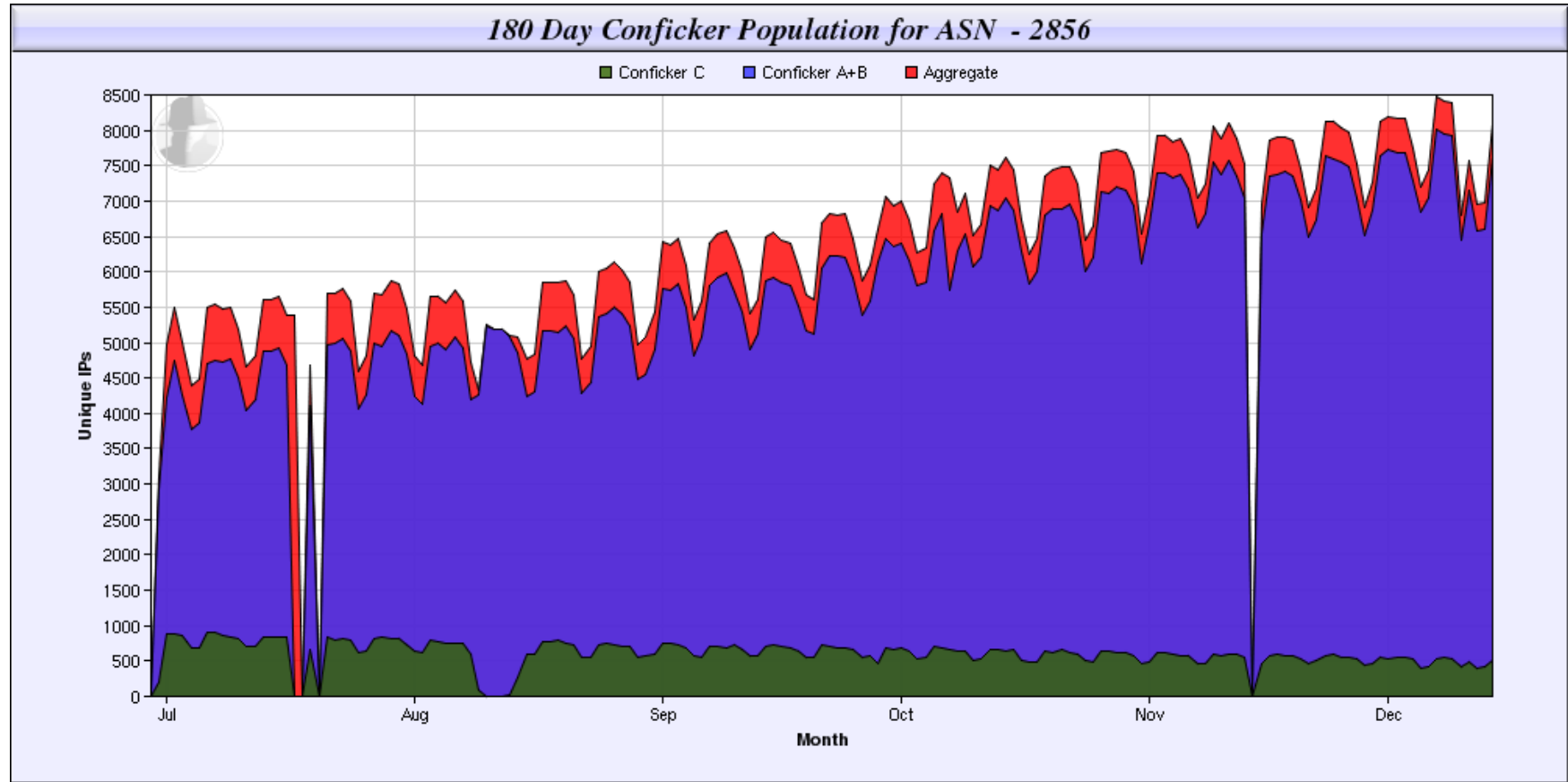
Worldwide Infections



December 2009 - <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>



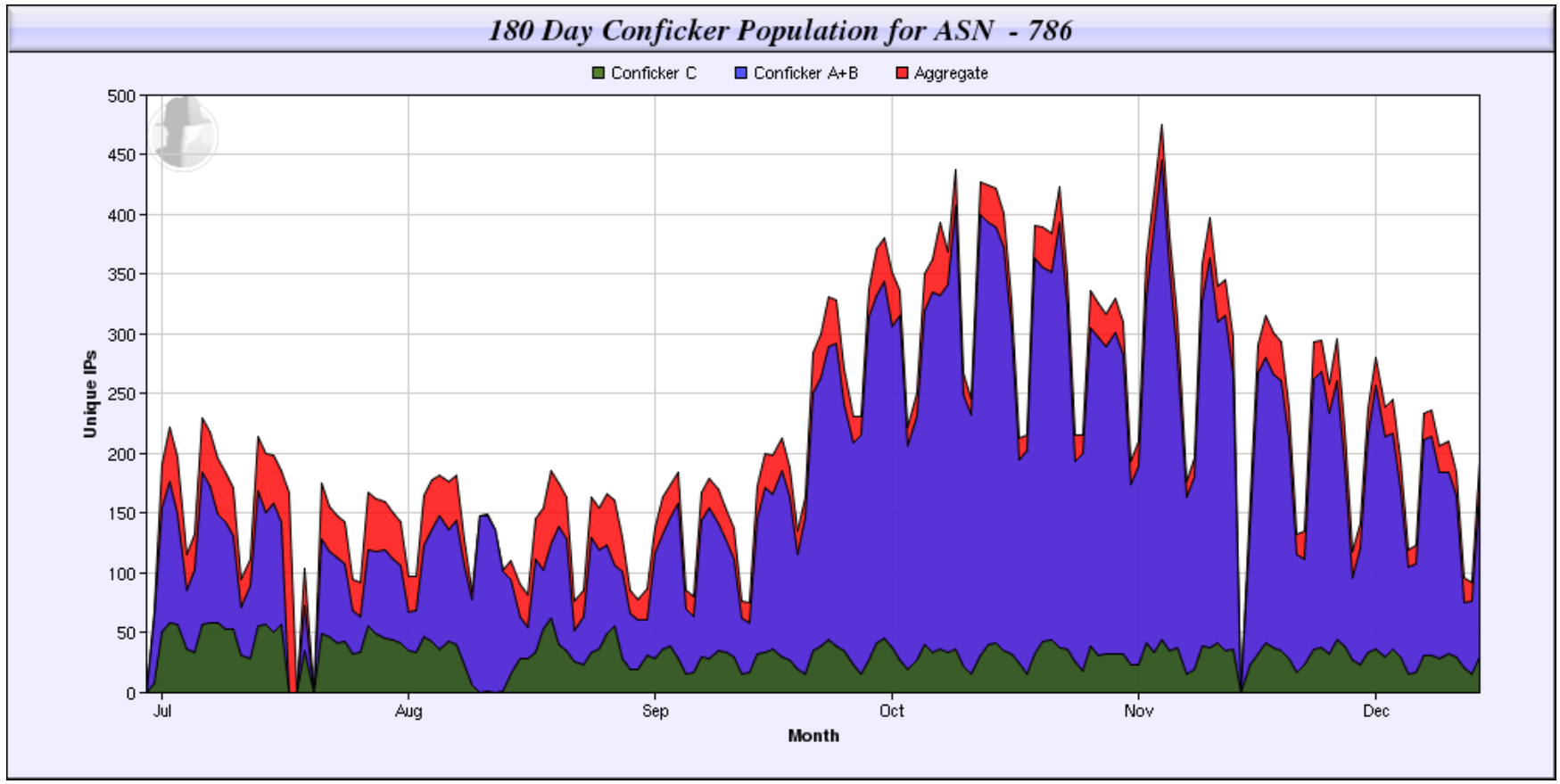
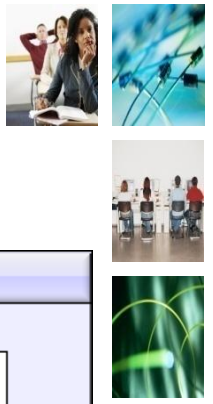
UK Commercial ISP



~ 10,500,000 Unique Routed IPs from 189 prefixes

December 2009 - <http://www.shadowserver.org/wiki/uploads/Stats/conficker-asn-abc-180day-2856.png>

JANET



~ 7,500,000 Unique Routed IPs from 190 prefixes

December 2009 - <http://www.shadowserver.org/wiki/uploads/Stats/conficker-asn-abc-180day-786.png>



Not a fair comparison

- Totally different scenarios
- NAT used heavily in UK Academic networks
- But we do attempt to resolve every infection!
- How does your network look?



Hide | Home

HomePage

Shadowserver

Mission

Standards and Guidelines

Organizations

Calendar

Future Goals

Job Opportunities

Press

Security Organizations

News Articles

Blogs and Forums

Misc

Presentations

Chronological

Operations Status

Knowledge Base

Botnets

Botnet Detection

Honeypots

eFraud

Malware

Whitepapers

Links

Get Involved

Get Reports on your Network

Mailing List

Submit a Botnet

Build a Honeypot

Hall of Fame

Get Reports On Your Network

Shadowserver - ASN & Netblock Alerting & Reporting Service

On this page... (hide)

- [Shadowserver - ASN & Netblock Alerting & Reporting Service](#)
- [How to request service](#)

The Shadowserver Foundation is pleased to announce the formal rollout of our ASN/netblock alerting and reporting service.

This reporting service is provided free-of-charge and is designed for ISPs, enterprises, hosting providers, and others that directly own or control network space. It allows them to receive customized reports detailing detected malicious activity that can assist in their detection and mitigation program. Shadowserver has been providing this service to many subscribers for several years, and currently generate over 4000 reports nightly. Since the response to this service has been extremely positive from a consumer base, we now wish to make it more widely and openly available.

The reporting service monitors and alerts the following activity:

- Detected Botnet Command and Control servers
- Infected systems (drones)
- DDoS attacks (source and victim)
- Scans
- Clickfraud
- Compromised hosts
- Proxies
- Spam relays
- Malicious software droppers and other related information.

The Shadowserver Foundation filters data received from its worldwide sensor and monitoring networks and employs...

<http://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork>



Netflow is our friend

- Netflow != replacement for IDS
- Try to sample 1 in 10
- Process 125k records a second



Finding needles in a haystack

- Every 30 mins we log flows to 4 million unique destination Ips (Netflow logs Dec 2009)
- Emerging threats block list 7,645 entries (Dec 2009)
- Botnet C&C Servers 1,651 entries (Dec 2009)
- What do you look for?!?



Finding needles in a haystack

- Score omni directional flow
- Weighting flows on IP, Protocol, Port etc
- Greater weighting for commonly exploited sockets eg 22/tcp, 445/tcp, 3389/tcp etc
- Also on demand reports...

Handling copyright

Dear JANET CSIRT:

We are writing this letter on behalf of the relevant subsidiaries of CBS Corporation.

We have received information that an individual has utilized the below-referenced IP address at the noted date and time to offer downloads of copyrighted television programs through a "peer-to-peer" service, including such title(s) as:

90210

The distribution of unauthorized copies of copyrighted television programs constitutes copyright infringement under the Copyright Act, Title 17 United States Code Section 106(3). This conduct may also violate the laws of other countries, international law, and/or treaty obligations.

Since you own this IP address (194.[snip].[snip].[snip]), we request that you immediately do the following:





Handling copyright

INFRINGEMENT DETAIL

Infringing Work: 90210

First Found: 10 Dec 2009 18:35:48 EST (GMT -0500)

Last Found: 10 Dec 2009 18:35:48 EST (GMT -0500)

IP Address: 194.[snip].[snip].[snip]

IP Port: 35832

Protocol: BitTorrent

Torrent InfoHash: B143BC878D68AA38AA5C7362A39E76E3FCA80EE2

Containing file(s):

90210.S02E10.HDTV.XviD-2HD.avi.torrent (367,141,156 bytes)

RIPA Notices



NOTICE UNDER SECTION 22(4) OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Where it appears to the designated person that a CSP is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice require the CSP -

- (a) if the CSP is not already in possession of the data, to obtain the data; and
 - (b) in any case, to disclose all of the data in his possession or subsequently obtained by him.
- S. 22(6) - It is the duty of the CSP to comply with any notice given to him under subsection (4).

Unique reference number of Notice	[REDACTED]
CSP	JANET - JANET or JANET(UK)
CSP address	JANET Service Desk, JANET(UK), Lumen House, Library Avenue, Harwell Science and Innovation Campus, Didcot, Oxfordshire, OX11 0SG,
CSP contact	
Legislation	This data is necessary for one or more of the following purposes as specified in The Regulation of Investigatory Powers Act 2000: - For the prevention and detection of crime or preventing disorder S22 (2)(b)
DCG grade	3
Designated person and date and time of issue	[REDACTED]
Telephone number/other communication to which this Notice relates	[REDACTED]
Details of service/data required including dates	[REDACTED]
SPOC Office Contact Details and Address	[REDACTED]
Telephone No	[REDACTED]
Fax No	[REDACTED]
SPOC e-mail	[REDACTED]
SPOC Postal Address	[REDACTED]
SPOC Officer	[REDACTED]
SPOC Officer Telephone No	[REDACTED]
Date served	[REDACTED]

CSPs must ensure the data is returned to a verified SPOC address, email or fax number. For information about how a CSP may verify the identity of a SPOC by use of the SPOC PIN list, contact commdata@homeoffice.gsi.gov.uk

DNS DDOS

\$ dig @<DNSSERVER> .

```

;<<<>> DiG 9.6.0 <<<>> @<DNSSERVER> .
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28909
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;      IN      A

;; AUTHORITY SECTION:
.      195650 IN    NS   H.ROOT-SERVERS.NET.
.      195650 IN    NS   I.ROOT-SERVERS.NET.
.      195650 IN    NS   J.ROOT-SERVERS.NET.
.      195650 IN    NS   K.ROOT-SERVERS.NET.
.      195650 IN    NS   L.ROOT-SERVERS.NET.
.      195650 IN    NS   M.ROOT-SERVERS.NET.
.      195650 IN    NS   A.ROOT-SERVERS.NET.
.      195650 IN    NS   B.ROOT-SERVERS.NET.
.      195650 IN    NS   C.ROOT-SERVERS.NET.
.      195650 IN    NS   D.ROOT-SERVERS.NET.
.      195650 IN    NS   E.ROOT-SERVERS.NET.
.      195650 IN    NS   F.ROOT-SERVERS.NET.
.      195650 IN    NS   G.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET. 282050 IN    A     198.41.0.4
A.ROOT-SERVERS.NET. 282050 IN    AAAA  2001:503:ba3e::2:30
B.ROOT-SERVERS.NET. 282050 IN    A     192.228.79.201
C.ROOT-SERVERS.NET. 282050 IN    A     192.33.4.12
D.ROOT-SERVERS.NET. 282050 IN    A     128.8.10.90
E.ROOT-SERVERS.NET. 282050 IN    A     192.203.230.10
F.ROOT-SERVERS.NET. 282050 IN    A     192.5.5.241
F.ROOT-SERVERS.NET. 282050 IN    AAAA  2001:500:2f::f
G.ROOT-SERVERS.NET. 282050 IN    A     192.112.36.4
H.ROOT-SERVERS.NET. 282050 IN    A     128.63.2.53
H.ROOT-SERVERS.NET. 282050 IN    AAAA  2001:500:1::803f:235
I.ROOT-SERVERS.NET. 282050 IN    A     192.36.148.17
J.ROOT-SERVERS.NET. 282050 IN    A     192.58.128.30
J.ROOT-SERVERS.NET. 282050 IN    AAAA  2001:503:c27::2:30

;; Query time: 45 msec
;; SERVER: <SERVERIP>
;; WHEN: Mon Jun 22 17:12:53 2009

```

;; MSG SIZE rcvd: 500


- Attacker sends high volume of small UDP query packets with spoofed source IP
- Significantly larger responses sent from DNS server to spoofed IP to amplify DOS attack by swamping target





phpMyAdmin Exploit

- Relates to vulnerability patched in April, POC code available June



INSECURE . ORG

Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Hackers
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

- Pass crackers
- Sniffers
- Vuln Scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News

Site Search:

Google Custom Search

Site Search

Full Disclosure: phpMyAdmin exploited in masses

phpMyAdmin exploited in masses

- *This message:* [[Message body](#)] [[More options](#)]
- *Related messages:* [[Next message](#)] [[Previous message](#)]

From: John Doe <johndo.jd_at_gmail.com>
Date: Fri, 3 Jul 2009 13:49:52 +0200

Hi,

Disclosing out of boredom and for the crawlers to archive.

Keywords: phpmyadmin, web, exploit, zavod, devitalia, mwstudio, szervernet, infotel, oodrive, iceman, romania, scriptkiddie.

An example of the phpmyadmin exploit used in masses without thinking.

IRC server: irc10.iceman.ro has address 85.214.36.2 (| h747052.serverkompetenz.net)
 IRC port: 9999

A few domains that are webhosted on the same IP: freebid.de, soccortreff.de, junge-werbung.com, pocket.marktcom.de.

Other possible IRC servers:

irc11.iceman.ro has address 87.106.2.154
 irc12.iceman.ro has address 85.214.84.18
 irc14.iceman.ro has address 82.165.30.30



Phishing Attacks

- Very common this year
- Phishers went through a phase of liking free hosting companies
- +1 by working with hosting providers (mostly positive with the right approach)



Its not just security incidents..

Anything that *may* be outside of the AUP;

- Feuding Couples
- Angry lawyers
- Fire engines on farms
- Cross posting on Usenet
- Attacks from RFC 1918 space



How to contact JANET CSIRT

For Security Incidents;
Email: irt@csirt.ja.net
Telephone: 0870 850 2340
Outside UK: +44 1235 822 340

More details at
<http://www.ja.net/services/csirt/>



Any Questions?

bradley.freeman@ja.net