

Securiteam: [NEWS] UK's Internet Infrastructure Open to Prying Eyes (Zone Transfers)

[NEWS] UK's Internet Infrastructure Open to Prying Eyes (Zone Transfers)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0062.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/15/03

To: list@securiteam.com

Date: 15 Oct 2003 10:29:15 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

UK's Internet Infrastructure Open to Prying Eyes (Zone Transfers)

SUMMARY

Network Penetration conducted a survey at the start of 2003 to check the status of the UK's DNS infrastructure. The second scan of the year has just been completed with the results are much more positive. There are still some serious holes in major areas, but much improvement has been made in the last 8 months. The rest of the paper will discuss what was tested, the results, some sample zone transfers and finally some recommendations.

DETAILS

What was tested?

During each scan, only one test was performed against each domain:

A full zone transfer (axfr) against the first authoritative DNS server assigned to that domain.

A zone transfer consists of copying the contents of a zone file from a DNS server. This normally occurs when a secondary DNS server wishes to replicate the information for a zone from a primary DNS server for purposes of backup / redundancy. A zone file consists of all the

Securiteam: [NEWS] UK's Internet Infrastructure Open to Prying Eyes (Zone Transfers)

information about that zone such as the IP address of a web server or mail server or possibly the hostname and IP of a firewall. Much of the information is open to request such as what email server is used for that domain, but other records such as the IP address and domain name of the firewall should not.

First and second level zones generally do not contain IP addresses of firewalls and such like, but they do contain huge lists of every subdomain. Take for example the zone file for the co.uk domain, it would contain every domain with a co.uk extension.

Example Zone Transfers:

All the transfers were conducted using free online tools provided by demon.net

Example one – Secured Domain

A zone transfer from the .biz domain returns in a timeout and no information is returned

Example Two – Secured Domain

Where as when trying to zone transfer .mil a connection refused is returned.

Domain: mil.

Primary Nameserver: G.ROOT-SERVERS.NET

E-mail Contact: HOSTMASTER@NIC.mil

/www/cgi-bin/demon/external/bin/dig @G.ROOT-SERVERS.NET mil. axfr

```
; <<>> DiG 2.1 <<>> @G.ROOT-SERVERS.NET mil. axfr ; (1 server found)
```

```
:: Received 0 records.
```

```
:: FROM: nu7www.demon.net to SERVER: 192.112.36.4 ;; WHEN: Tue Aug 12 01:08:14 2003
```

Example Three – Insecure Domain

An unsecured domain however such as fake.com would return the following

Domain: fake.com.

Primary Nameserver: ns1.fakehosting.com E-mail Contact:

admin@fakehosting.com

/www/cgi-bin/demon/external/bin/dig @ns1.fakehosting.com fake.com. axfr

```
; <<>> DiG 2.1 <<>> @ns1.netincomehost.com fake.com. axfr ; (1 server found)
```

```
fake.com.3600SOAns1.fakehosting.com. admin.fakehosting.com. (
```

```
10; serial
```

```
3600; refresh (1 hour)
```

```
600; retry (10 mins)
```

```
1209600; expire (14 days)
```

Securiteam: [NEWS] UK's Internet Infrastructure Open to Prying Eyes (Zone Transfers)

```
3600 ); minimum (1 hour)
fake.com. 3600 A 1.2.3.4
fake.com. 3600 NS ns1.fakehosting.com
fake.com. 3600 NS ns2.fakehosting.com
fake.com. 3600 MX10 smtp.fake.com.
webmail.fake.com. 3600 CNAME webmail.freemail.com.
cisco.fake.com. 3600 A 1.2.3.1
fw1.fake.com. 3600 A 1.2.3.2
snort.fake.com. 3600 A 1.2.3.3
www.fake.com. 3600 A 1.2.3.4
ftp.fake.com. 3600 A 1.2.3.5
pdc.fake.com. 3600 A 1.2.3.6
fake.com. 3600 SOA ns1.fakehosting.com admin.fakehosting.com. (
    10; serial
    3600; refresh (1 hour)
    600; retry (10 mins)
    1209600; expire (14 days)
    3600 ); minimum (1 hour)
```

:: Received 10 records.

:: FROM: nu7www.demon.net to SERVER: 64.42.224.9 :: WHEN: Mon Aug 11
23:20:47 2003

The factious zone file for fake.com shows a whole range of possible targets that a hacker could use to quickly map a network without having to send hardly any packets to the network.

The information regarding the top and second level domains are not being published due to the possibility of them being exploited at some point in the future.

Results for UK DNS Infrastructure

At the start of the year nearly all the second level domains in the UK allowed a zone transfer, but now its only really sections of the government lagging behind.

Domain Transfer Possible Number of Records Notes

Jan 03 August 03 Jan 03 August 03

```
uk Yes yes 220 248
ac.uk no no --
bl.uk Yes no 1892 -
co.uk no no --
gov.uk yes no 5 -
govt.uk no no --
ltd.uk yes no 26723 - Over 1 Mb
me.uk yes no 57329 - Over 1 Mb
mod.uk yes yes 1484 1729
net.uk yes no 1298 -
nls.uk yes no 438 -
org.uk yes no 422265 - Over 20 Mb
plc.uk yes no 3646 -
```

Securiteam: [NEWS] UK's Internet Infrastructure Open to Prying Eyes (Zone Transfers)

police.uk yes yes 234 241
sch.uk yes no 71360 – Over 1 Mb

The only test performed against each server was a full zone transfer, some returned the full zone file while others such as gov.uk only returned a partial zone file.

In total 15 domains were tested, 3 passed test with transfers not possible at the start of the year compared to 12 in August. 20% at the start of the year, 80% in August can the UK score a 100% by the end of the year and lock down all there DNS servers? One would like to think so.

After sending an early copy of this report to various domain administrators, Network Penetration received a response from Jay Daley Director of IT at Nominet UK.

"It is our policy that .uk is not closed to zone transfers though all of the second level domains (SLDs) that we manage are. There are a large number of people who pull the .uk zone to allow their nameservers fast repudiation of non-existent SLDs (e.g. when someone types in xxx.com.uk by accident)."

The two remaining zones mod.uk and police.uk may be open for a specific reason unknown to Network Penetration at this time but upon initial inspection, they appear to be unsecured DNS servers. One possible reason is that zone transfers are extremely useful for debugging problems with domain name servers.

The information provided in this report does not necessarily mean that each domain was unsecured / secured but merely gives a rough guide to the state of the UK's DNS infrastructure.

Recommendations

Zone files contain lots of crucial information that a hacker or terrorist could use to attack a nations infrastructure due to zone files containing information on a networks design and also highlighting key nodes within a networks infrastructure. Zone transfers should be blocked and not allowed from un-trusted hosts e.g. the general public. Disallowing zone transfers from hosts other than your backup DNS servers, still allow hostnames to be resolved.

DNS Zone Transfer Protocol Clarifications

<<http://www.ietf.org/internet-drafts/draft-ietf-dnsext-axfr-clarify-05.txt>>
<http://www.ietf.org/internet-drafts/draft-ietf-dnsext-axfr-clarify-05.txt>

Why is securing DNS zone transfer necessary?

<<http://www.sans.org/rr/paper.php?id=868>>
<http://www.sans.org/rr/paper.php?id=868>

ADDITIONAL INFORMATION

Securiteam: [NEWS] UK's Internet Infrastructure Open to Prying Eyes (Zone Transfers)

The original copy of this paper can be found at:

<<http://www.networkpenetration.com/ukdns.html>>

<http://www.networkpenetration.com/ukdns.html>.

The information has been provided by Network Penetration.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.