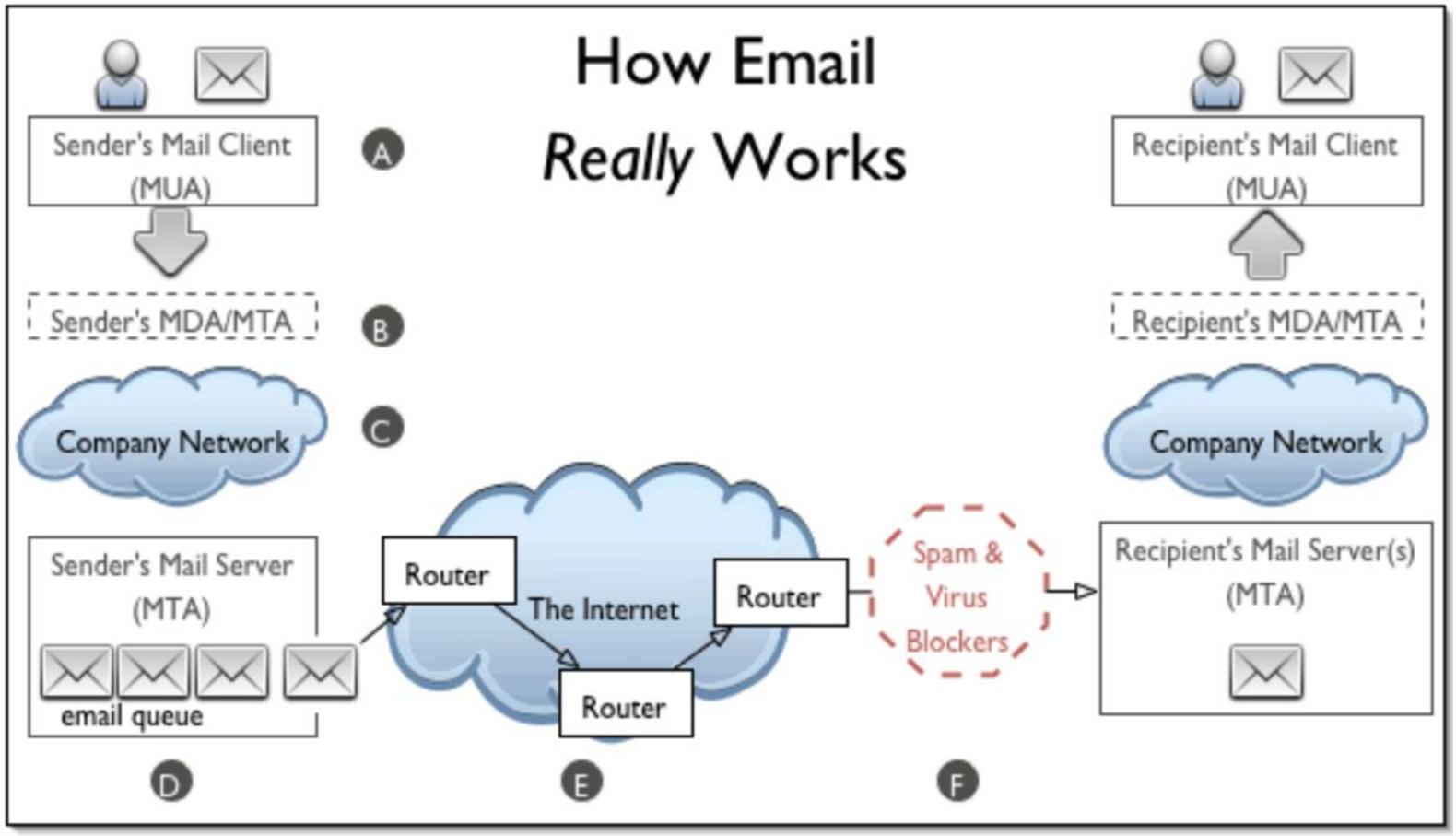
Spam

Unsolicited bulk email

Can be used to:

- Send advertising material
- Collect information
- Mount phishing attacks
- Mount pharming attacks
- Distribute malware
- Conduct social engineering attacks

Spam --- How Email works



Tracing Spam E-mails

- Spam e-mails comprise 70~90% of all e-mails.
- About 60% of all spam e-mails carry links to malware and pharming sites. About 30% are ads for drugs.
- Used extensively for scams, fraud, phishing attacks.
- Most spam is sent by **spam-bots** (automated spam generation and addressing).

Spam-Bot

- A type of malware which is used to send spam.
- Can create e-mail accounts.
- Search the web for e-mail addresses.
- Generate pseudo-random spam and send it.
- Some can
  - Crack passwords, solve CAPTCHA puzzles.
  - Install malware, host servers.

Tracing Spam E-mails

- Spam can be identified by the path it travels to get to you.
- Every email comes with **a header** listing the names and IP addresses of each mail server through which it has passed.
- The sender can be verified by performing a reverse DNS lookup on the sender's IP address.
- Known sources of spam can be looked up using a published black-list.

MIME --- Sending User Authentication

- MIME: Multipurpose Internet Mail Extension
- MIME message body:
  - Message itself including text and attachments
  - Signature

Fig 1. Email message structure

DKIM --- Sending MTA Authentication

- DKIM: DomainKeys Identifier Mail
- Some attributes of DKIM:
  - a: identifier of cryptographic algorithm
  - c: canonicalization algorithms for header and body
  - d: domain of the signing entity
  - s: selector of the signing key
  - bh: hash of the body of the message
  - b: signature

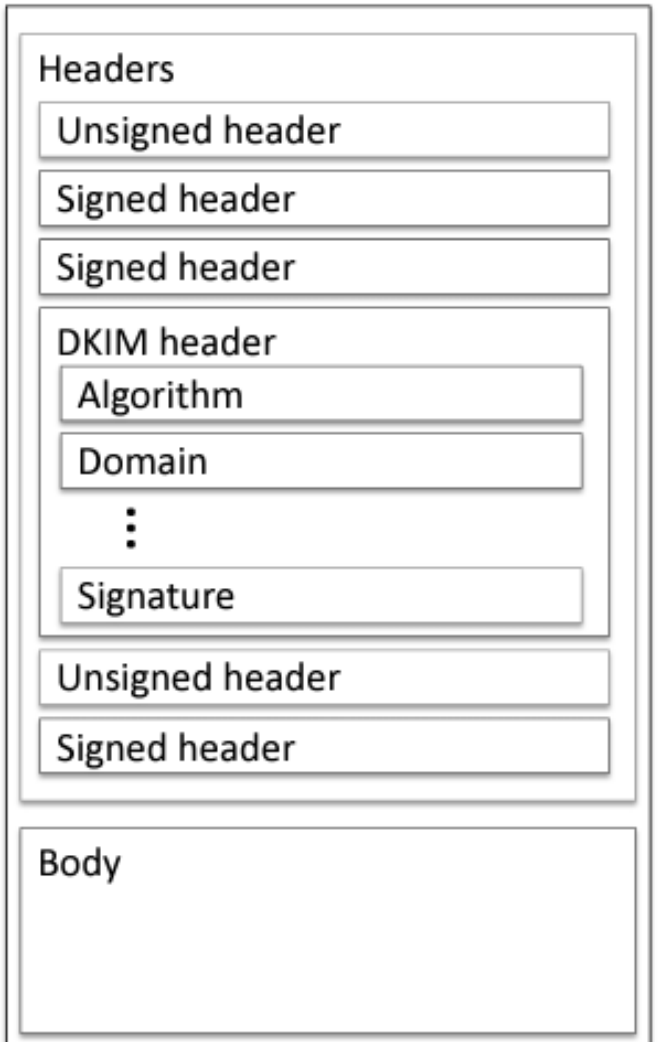


Fig 1. Email message structure

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=brown.edu; s=cs;
    h=domainkey-signature:mime-version:received:in-reply-to:references
     :date:message-id:subject:from:to:cc:content-type;
    bh=L+J52L7uTfKTel/+2ywqQMH1eiGvl6tsXjDNAySew+8=;
    b=vE2bvcj8GVHGHeECJA4WJ/t1BRbLBvlTQywbZl/HgFSMRfoIVUvH9lyVeMitOaNMeQ
     C29TNP5fJPphaFhHb9tf8EkJBIojRryWRAl5/r5RgT6z5DLWs8fgHe0wUbWEwBQ+sSTs
     A+vbfuLObS1Gwdxtu81HNOfiSLY0u2CM6R31s=
```

Fig 2. An example of DKIM-Signature

E-mail Headers

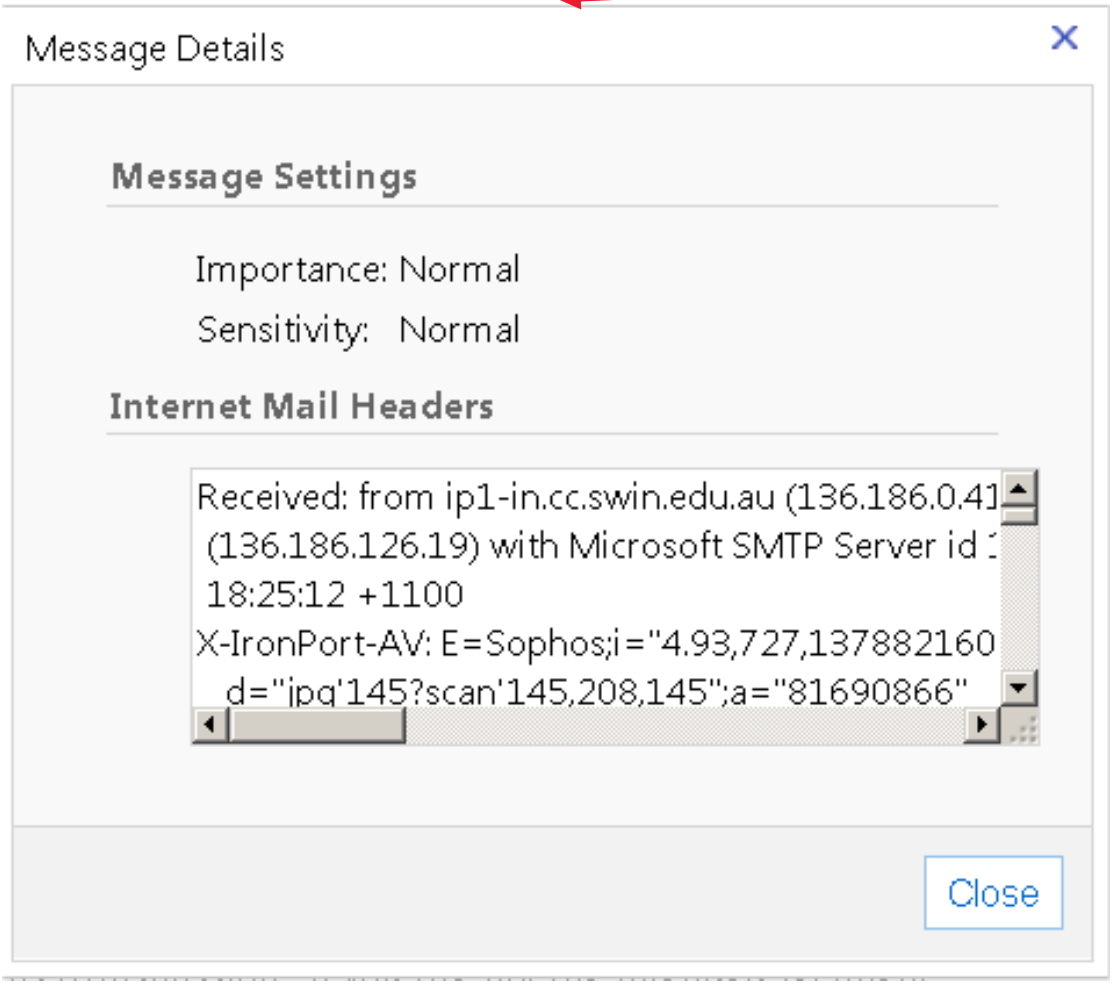


Fig 2. Intent Mail Headers

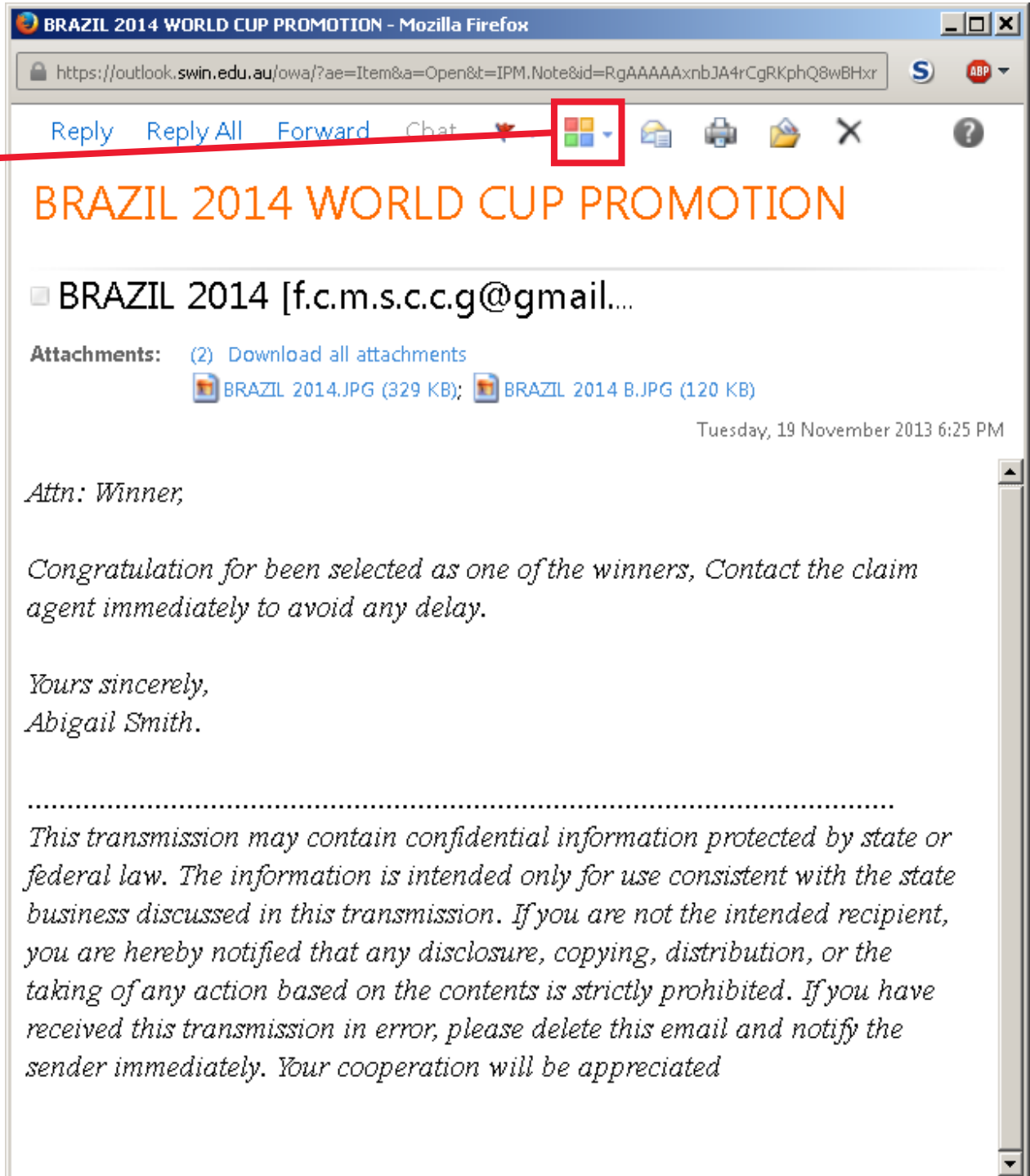


Fig 1. An example of an e-mail

E-mail Header

```
Received: from ip1-in.cc.swin.edu.au (136.186.0.41) by outlook.swin.edu.au
 (136.186.126.19) with Microsoft SMTP Server id 14.3.158.1; Tue, 19 Nov 2013
 18:25:12 +1100
X-IronPort-AV: E=Sophos;i="4.93,727,1378821600";
   d="jpg'145?scan'145,208,145";a="81690866"
Received: from gpo4.cc.swin.edu.au ([136.186.1.33])  by ip1-in.cc.swin.edu.au
 with ESMTP; 19 Nov 2013 18:25:12 +1100
Received: from mail-oa0-f52.google.com (mail-oa0-f52.google.com
 [209.85.219.52])   by gpo4.cc.swin.edu.au (8.14.3/8.14.3) with ESMTP id
 rAJ7P2gH031114     (version=TLSv1/SSLv3 cipher=RC4-SHA bits=128 verify=FAIL)   for
 <jhamlynharris@swin.edu.au>; Tue, 19 Nov 2013 18:25:06 +1100
Received: by mail-oa0-f52.google.com with SMTP id h16so2441195oag.11
        for <jhamlynharris@swin.edu.au>; Mon, 18 Nov 2013 23:25:02 -0800 (PST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:reply-to:date:message-id:subject:from:to:content-type;
        bh=PnUts3Gl3c94wk5Da3k/D3nWn0cpih/ZY7pTWmhAPYw=;
        b=ivxuMhRYnDPAeH1R58QXjhFfOkfcOW7m/IouIT+R+YzBhemFVc+IGnqK6Jez3tVSXq
         DBQqdZHcr6qoImqHq3IjhX4zk+TexM4azjConDXDgxa4pruTnrhv3hFwFWQGMyKFwFfX
         KtZqe9sXhPnSSWOf6mBzypzUnUTO7HMpB5FAdNFyIv9mHWhG6f9xB03lS0XCBt2Mptir
         LmVvAcz3XcBwg4YvY7QwM3kOC5iVlFVahTzmeMDajTJE4JLwU24OcpxDHOt7sOS+lprl
         A+U/fXrdq3Vwajqqdo/vIW0CU4UARe69KU8u8bPCPCwOfv/wPbDYXM2+XBrNbk4Bkpno
         5w8A==
MIME-Version: 1.0
X-Received: by 10.182.66.164 with SMTP id g4mr887457obt.47.1384845901691; Mon,
 18 Nov 2013 23:25:01 -0800 (PST)
Received: by 10.182.59.70 with HTTP; Mon, 18 Nov 2013 23:25:01 -0800 (PST)
```

What does this mean?
It's in Base64..

E-mail Spam Checker Report

```
Reply-To: <b2013.2014.bfwcoc@gmail.com>
Date: Tue, 19 Nov 2013 09:25:01 +0200
Message-ID: <CAG9WAb2v1ch7hburHTPft8hEfZgKHYhydm106mwFEQgkXaoT4A@mail.gmail.com>
Subject: BRAZIL 2014 WORLD CUP PROMOTION
From: BRAZIL 2014 <f.c.m.s.c.c.g@gmail.com>
To: undisclosed-recipients:;
Content-Ty pe: multipart/mixed; boundary="089e0160c35e0a59d704eb8290ec"
X-Spam-Status: score=5.3
          tests=RCVD_IN_DNSWL_LOW,FREEMAIL_FROM,SUBJ_ALL_CAPS,HTML_MESSAGE,DKIM_VALID_AU,DKIM_SIGNED,,LOTTO_AGENT
          ,FREEMAIL_REPLYTO
X-Spam-Level: *****
X-Spam-Report: * -0.7 RCVD_IN_DNSWL_LOW      RBL: Sender listed at http://www.dnswl.org/, low
          *                              trust
          *                              [209.85.219.52 listed in list.dnswl.org]
          *  0.0 FREEMAIL_FROM           Sender email is commonly abused enduser mail provider
          *                              (f.c.m.s.c.c.g[at]gmail.com)
          *  1.6 SUBJ_ALL_CAPS           Subject is all capitals
          *  0.0 HTML_MESSAGE            BODY: HTML included in message
          * -0.1 DKIM_VALID_AU           Message has a valid DKIM or DK signature from author's
          *                              domain
          *  0.1 DKIM_SIGNED             Message has a DKIM or DK signature, not necessarily valid
          * -0.1 DKIM_VALID              Message has at least one valid DKIM or DK signature
          *  3.5 LOTTO_AGENT             Claims Agent
          *  1.0 FREEMAIL_REPLYTO        Reply-To/From or Reply-To/body contain different
          *                              freemails
          *
```

Remaining Headers

```
Return-Path: f.c.m.s.c.c.g@gmail.com
X-MS-Exchange-Organization-AuthSource: gsp-ex03.ds.swin.edu.au
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-PRD: gmail.com
X-MS-Exchange-Organization-SenderIdResult: SoftFail
Received-SPF: SoftFail (gsp-ex03.ds.swin.edu.au: domain of transitioning
 f.c.m.s.c.c.g@gmail.com discourages use of 136.186.1.33 as permitted sender)
X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0
```

Another Example

Dear Woolworths client - Mozilla Firefox

https://outlook.swin.edu.au/owa/?ae=Item&a=Open&t=IPM.Note&id=RgAAAAAxnbJA4rCgRKphQ8wBHx

Reply Reply All Forward Chat

Dear Woolworths client

Woolworths [office49@wumt.co...

To: Recipients [office49@wumt.com]

Monday, 31 March 2014 8:45 AM

Dear ANZ / Westpac member and Woolworths client,

ANZ / Westpac and Woolworths agreed to reward all ANZ and Westpac members who are shopping at Woolworths.

If you are a ANZ / Westpac member and have made at least one purchase at Woolworths please click here and complete a quick survey and get your **150$ reward**.
Thank you.

This is an automated message. Please do not reply.
Message Id: 0019268154-wmrtsrv.

E-mail Header

Received: from ENP-EX02.ds.swin.edu.au (136.186.126.148) by
gsp-ex03.ds.swin.edu.au (136.186.126.19) with Microsoft SMTP Server (TLS) id
14.3.158.1; Mon, 31 Mar 2014 08:53:23 +1100
Received: from ip1-in.cc.swin.edu.au (136.186.0.41) by outlook.swin.edu.au
(136.186.126.148) with Microsoft SMTP Server id 14.3.158.1; Mon, 31 Mar 2014
08:53:23 +1100
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result:
AjBpAAGSOFOIugEgnGdsb2JhbABZgWwCAVN/SwEBqzECgSYBhUKIDYEmGYhEFg4BAQEBAQgUCTyCRIEAARw0TogL
AQ2fVoIrjRxRoQQXkTQPgXsEiRo2hguIc4EzhRqPJYFe
X-IronPort-AV: E=Sophos;i="4.97,761,1389704400";
d="scan'208,217";a="87288458"
Received: from gpo3.cc.swin.edu.au ([136.186.1.32]) by ip1-in.cc.swin.edu.au
with ESMTP; 31 Mar 2014 08:53:23 +1100
Received: from smtp42.singnet.com.sg (smtp42.singnet.com.sg [165.21.103.146])
by gpo3.cc.swin.edu.au (8.14.3/8.14.3) with ESMTP id s2ULr7Hm012561; Mon, 31
Mar 2014 08:53:21 +1100
Received: from [192.100.100.2] ([203.125.107.86]) by smtp42.singnet.com.sg //the source
(8.14.3/8.14.1) with ESMTP id s2ULpbv4021067; Mon, 31 Mar 2014 05:51:58 +0800
Message-ID: <201403302151.s2ULpbv4021067@smtp42.singnet.com.sg>
Content-Type: multipart/alternative; boundary="==========1720182961=="
MIME-Version: 1.0

E-mail Header

```
Subject: Dear Woolworths client
To: Recipients office49@wumt.com  //fake
From: Woolworths <office49@wumt.com>
Date: Mon, 31 Mar 2014 05:45:19 +0800
X-PMX-Version: 5.5.2.363555, Antispam-Engine: 2.6.1.350677, Antispam-Data: 2014.3.30.214218
X-PMX-AS: AS-Check
X-PMX-Score: Probability=10%
X-Spam-Status: score=2.5 tests=RCVD_IN_DNSWL_NONE,URIBL_BLACK,HTML_MESSAGE   //blacklist
X-Spam-Level: **
X-Spam-Report: * -0.0 RCVD_IN_DNSWL_NONE     RBL: Sender listed at http://www.dnswl.org/, no
                *                    trust
                *                    [165.21.103.146 listed in list.dnswl.org]
                *  2.5 URIBL_BLACK          Contains an URL listed in the URIBL blacklist
                *                    [URIs: sungazette.com]
                *  0.0 HTML_MESSAGE         BODY: HTML included in message
                *
Return-Path: office49@wumt.com
X-MS-Exchange-Organization-PRD: wumt.com
X-MS-Exchange-Organization-SenderIdResult: None
Received-SPF: None (ENP-EX02.ds.swin.edu.au: office49@wumt.com does not  designate permitted sender hosts)
X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0
X-MS-Exchange-Organization-AuthSource: ENP-EX02.ds.swin.edu.au
X-MS-Exchange-Organization-AuthAs: Anonymous
```

Tracing Spam E-mails

- The link inside take us to:
  - http://extras.sungazette.com/wool.html (Now broken)
- It's the Sun Gazette -- a local Williamstown newspaper
- It's US hosting

12.169.112.230 | Lookup IP Address

General IP Information

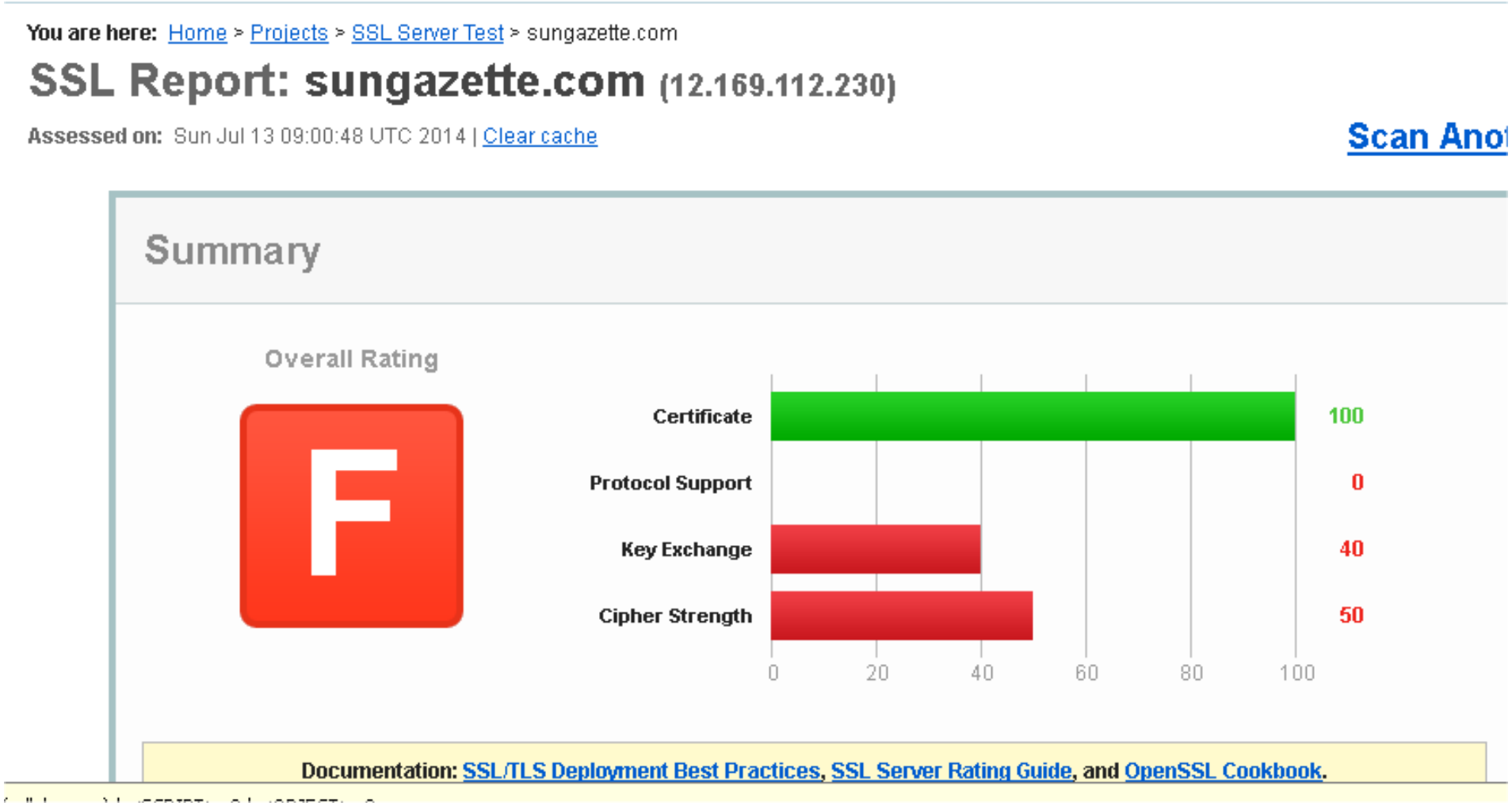
IP: 12.169.112.230
Decimal: 212431078
Hostname: sungazette.com
ISP: AT&T Services
Organization: Ogden Newspapers
Services: None detected
Type: Corporate
Assignment: Static IP
Blacklist: Blacklist Check

Geolocation Information

Country: United States
State/Region: West Virginia
City: Wheeling
Latitude: 40.0582 (40° 3' 29.52" N)

Tracing Spam E-mails

- Vulnerable to being hacked?



Tracing Spam E-mails

- Vulnerable to being hacked?

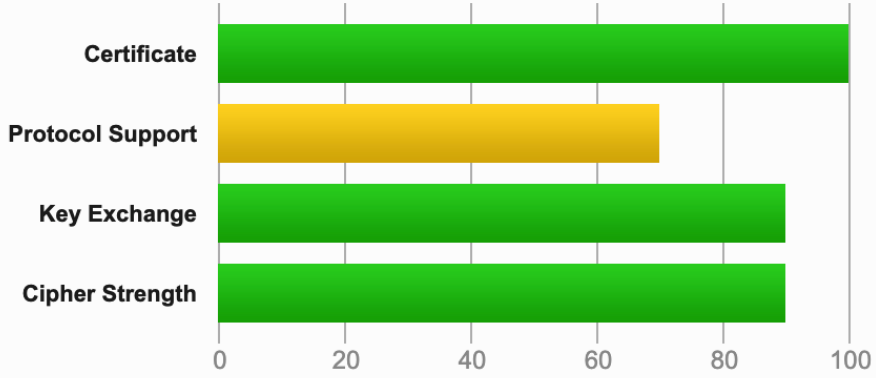
You are here: Home > Projects > SSL Server Test > sungazette.com > 35.170.139.128

SSL Report: sungazette.com (35.170.139.128)

Assessed on: Wed, 07 Oct 2020 05:39:51 UTC | Hide | Clear cache

Summary

Overall Rating



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Blacklists

- System Administrators have option of subscribing to various **blacklists**.

  - Lists of domain names and hosts identified as sources of spam e-mail.
    - http://www.rahul.net/falk/#blocklists
    - http://www.spamhaus.org/lookup.lasso
  - Some sites are blacklisted by mistake.
  - There are whitelist services available as well for default-deny e-mail servers.

Open Relays

- There are a few **open relays** – public and anonymous e-mail servers which allow anyone to send an e-mail.
  - They are a leftover from the days when the internet was used for good and not evil
  - Highly sought-after by spammers
  - A compromised or owned PC can act as an open relay.
    - http://multiproxy.org/all_proxy.htm

Free E-mail Services

- Rather than using **open relays**, spammers tend to set up an e-mail server on an owned PC. (never use their own e-mail account)
- Spammers also use public web-based e-mail sites to send spam. Bots can be used to create new e-mail accounts with random or dictionary-based names for the purposes of sending spam.
- Such services are increasingly trying to prevent this by adding puzzles that bots can't solve:
  - CAPTCHA puzzles
  - Phone call-backs
  - Audio CAPTCHAs

CAPTCHA Puzzles

- **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part
  - Require the person opening the account to interpret a scrambled image or sound. The theory is that a bot is not smart enough to solve the puzzle, but the algorithms for this already exist
  - http://www.cs.sfu.ca/~mori/research/gimpy/

- Can be avoided if the bot tricks a real user on another site to decode the puzzle on his behalf (Security Now 101):
  - Some CAPTCHA puzzles have been implemented on the client-side using Javascript (epic fail!)

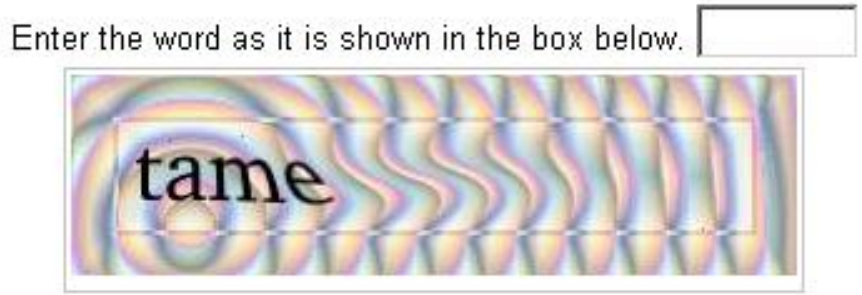


Fig 1. Picture of a CAPTCHA in use at Yahoo

E-mail Harvesting

- Collecting e-mail addresses is part of the enumeration process.
  - E-mail addresses reveal usernames and domain names.

- Names can be lifted by automatic tools (spiders) which sift through web sites on the web.
  - Companies doing this represent themselves as legitimate companies providing a service or a "web directory" product
  - Include directories of coffee shops, health care and education providers

- E-mails are sent to the harvested e-mail addresses inviting the recipients to visit the web site and confirm the details. Confirmed e-mail addresses are worth more on the hacker/spam market.

E-mail Harvesting

- Spam-bots also generate random e-mail addresses and send spam to them.
  - ➢ The messages include an **unsubscribe link** which if followed logs the e-mail address of the victim, confirming it as real and therefore saleable.

- The messages often say something like "**don't reply to this e-mail address**".
  - ➢ The "**from**" e-mail address does not exist – it was spoofed or has been shut down by the ISP managing the bot's domain