SANS Securing The Human - Whitelisting

Overview

The following document provides whitelisting information for our VLE Servers, Media Hosting, and Email Domains.

Virtual Learning Environment (VLE) – Whitelisting Information

Within the VLE, you have access to send six different emails to your Users. All emails are sent from noreply@securingthehuman.org. Please ensure this email is on your Safe Sender List. We also recommend that prior to sending any notifications from the VLE that your Users are aware that emails will be sent from this address.

NOTE: During your account setup you will choose who the "From" name and "Reply-To" to be associated with these email notifications based on Client Administrators added to your Sub-Accounts.

VLE Email IP Addresses

Email is sent from multiple mail servers in our Network Operations Center. The address will be in the range:

204.51.94.x *and* ***66.35.59.x***

Main VLE Site Access

- http, https (ports: 80, 443) securingthehuman.org (204.51.94.151)
- http, https (ports: 80, 443) securingthehuman.org (66.35.45.85)

Amazon CloudFront Access

SANS hosts our video files on our Amazon CloudFront. Content is automatically updated in the system for all Users that are in progress or have not started the new/updated training modules.

RTMP (uses ports 443, 1935 – in some cases corporate networks do not open port 1935):

- sxe9vg7lnyp4w.cloudfront.net
- d2phghrx3iz34s.cloudfront.net

As of January 30, 2014, the current CloudFront IP addresses are (listed in CIDR notation):

- 54.192.0.0/16
- 54.230.0.0/16
- 54.239.128.0/18
- 54.239.192.0/19
- 54.240.128.0/18
- 204.246.164.0/22
- 204.246.168.0/22
- 204.246.174.0/23
- 204.246.176.0/20
- 205.251.192.0/19
- 205.251.249.0/24
- 205.251.250.0/23
- 205.251.252.0/23
- 205.251.254.0/24
- 216.137.32.0/19

Other Amazon domains:

- Amazon AWS http, https (ports: 80, 443) s3.amazonaws.com (72.21.214.38)
- ssgy8u74zvabm.cloudfront.net
- s38jsjahtvsk9r.cloudfront.net
- s1lnmtvcosiomh.cloudfront.net
- s2p6mc768fegqw.cloudfront.net
- securehuman2.s3.amazonaws.com

Phishing Product – Whitelisting Information

Phishing Email Servers

At a minimum, the Phishing Email Servers need to be whitelisted in order to run Phishing Campaigns. Phishing emails are sent from one of the following mail servers:

- mailer1.threatsim.com (107.23.16.222)
- mailer2.threatsim.com (54.173.83.138)

Phishing Domains (From: & Landing Pages – used to enable images within campaign messages)

- 4ooi.com
- corp-hr.com
- entwurf-laden.de
- firstfedtrust.com
- office3889.com
- payablaccounts.com
- phishingtraining.com
- qqffi55.cc
- qqoffi55.com
- saleslinkforce.com
- salesteamlink.com
- voicemailaccess.net
- account-maintenance.com
- corp-internal.com
- corp-internal.net
- corp-internal.us
- corpbenefitplan.com
- internalitsupport.com
- netbenefits-access.com
- password-update.com
- password-update.net
- user-account-maintenance.com
- corp-internal.co.uk
- corpoutlook.com
- sec-10k.com
- annualenroll.com
- corp-proxy.com
- emailquarantine.com
- webfilteralert.com
- dcsanscation.com
- detailswire.com
- hpdocument.com
- tradeinternationai.com
- corp-hr.com
- exch01-corp.com
- localhostlocaldomain.com
- www01-local.com
- mail-delivery-system.com
- mailcenter-alert.com
- maildeliverysystem.net
- dynssi.com
- microsoftsql.net
- updamicrosoft.com
- voicemailaccess.net
- linkedincdn.com
- sphotos-fbcdn.com
- shipment-confirm.com
- byt.im
- prnewsnet.us
- eservce.com
- flightstatalert.com
- travelresinfo.com
- dropboxlink.com
- breaking-news-network.net
- breaking-news-now.com
- cyber-sale.net
- postcardfast.com
- shippingupdate.net
- trackingupdate.net
- itnues.net
- updatracking.com
- enegry.org
- freeenergypress.com
- pipelinenews.net
- info-week.net
- info-week.us

Phishing Image Domains

It may also be necessary to whitelist the following domains as they are used for images within certain Landing Pages:

- ajax.googleapis.com
- fonts.googleapis.com
- assets.threatsim.com
- tslp.s3.amazonaws.com
- d25q7gseii1o1q.cloudfront.net

Tracking "Opened" Phishing Emails

In order for your "Opened" Email statistics to be tracked in your results, recipients **must** have "Images Enabled" within their email client. In addition, there may need to be additional "Safe Sender" domains whitelisted **(see Phishing Domains above)**.

To display images within phishing emails the image used must be viewable to the User in the email message. This is done by hosting the image on a specific domain (defined above) and using that domain in the email message for the targeted User.

For example, if the phishing campaign created with a Landing Domain of secure.account-maintenance.com – the URL to the image embedded for your Target User Group would be:

http://secure.account-maintenance.com/pixel_abc123.gif

where pixel_abc123.gif is the image used by the selected Landing Domain. The purpose of the images is to allow you to track "Opened" email rates in your campaigns. For this reason, the campaign URL (shown below) must be added to your Safe Sender's List:

secure.account-maintenance.com