ISB Phishing System

BC Provincial Government

TECHNICAL GUIDE (v0.01)

# Components

All components of the script are expected to run in the same folder on a linux distribution. The user logged on must have permissions to run sendmail.

* **The Phishing Script**: This script sends out the emails. It is a linux bash script that randomizes the available email templates and sends them at a rate that does not overwhelm the mail server.

sendemail\_multi.bash

The naming of this script is primarily historical and is based on the fact that we are sending emails using multiple email templates.

* **The Email List:** This is a text file containing all the emails that the phishing script needs to email. Each separate line should contain an email address. If you are given an outlook distribution list, you can ask messaging and communication to provide a CSV file of email addresses. Rename that file to match the existing file and it should work just fine.

emailaddr.txt

* **The Email Templates:** These are HTML files that try to trick users into clicking the links embedded in the message. The script will scan the folder for email addresses that match the following name format.

email\_content0.html

email\_content1.html

email\_content2.html

etc…

* **The Web Server:** The email templates will need to contain a link to a website. This site hosts the landing page for your phishing campaign. In order to collect data for your campaign, you’ll need to have access to the access\_log files for that web server.

# Usage

## Prepare the Email List

The email list is basically a plaintext list of email addresses on separate lines. Make sure that not information other than the address is on each line.

For multiple groups, you’ll need to prepare different files with the addresses for each group.

## Prepare the Email LINK

The email link will point to your phishing landing page. Usually you want to hide the link somehow so that users can recognise the address. To do this, you can use a link shortening service like <https://bitly.com/>.

If you are working with multiple groups that you want to measure in data collection, you’ll want to set up a different link for each group. Even if you have the same landing page, you can add a URL variable to make each link different.

For example:

www.mydomain.com/unsubscribe.html?id=group1

www.mydomain.com/unsubscribe.html?id=group2

etc…

## Create Email Templates

The email template is written in HTML and contains some basic header information such as the subject line and the sender address. If you want to create your own email templates, you can copy an existing template and edit it.

The phishing program itself can support multiple templates for a single campaign. The script expects email templates to be in the format email\_contentX.html, where X is a number starting from 0. This allows it to scan to see how to randomize the sending within an email list.

The numbers for the email templates must be sequential starting from zero (ie: 0,1,2,3… but not 1, 5,7…).

## Running the Script

Make sure to run a smaller scale test with a select group before engaging a larger campaign.

Once all the components are in place, you can run the script with the following command:

sh sendemail\_multi.bash

As the script runs, it will list out what format goes to what email address.

# Data Collection

Data is typically collected via the HTTP web server access logs. Make sure that all of your logs are in a single file for the campaign.

For small groups you can check to see who is accessing your phishing landing page.

If you are working with different groups as mentioned in the usage section, you can see the identifying variable in the URL they access.

For larger groups, you can run a command to measure how many unique IPs visited the site. Here is an example of using the awk command to count the number of hits from ‘group2’.

cat /var/log/httpd/access\_log-20180506 |awk '(($7 == "/unsubscribe.html?id=group2") && $13!="(TweetmemeBot/4.0;") {print $1}' | sort | uniq | wc –l

This command also makes sure to exclude results from web crawler services.

# Best Practices

## Notifications

Before running a phishing campaign there are a few notifications that need to go out in order to cover your bases.

* **Executive:** Make sure that you have some buy in on the executive level, and key members have been notified that you are conducting phishing campaigns in their area. Their support is essential for dealing with potential backlash or fallout from a phishing campaign.
* **Technical Support Teams:** Since technical support teams are on the front lines of dealing with viruses and malware, key members and communications need to be sent out in order to prevent any impact to business. If a technical support team is not notified, then user computers may be wiped in response to a perceived security breach. Make sure to provide the specific subject lines of the phishing emails to make sure that support teams can recognise real threats.
* **Email Communications Team:**  If your organisation has a team that handles email and network communications, they may need to be notified. Phishing campaigns can put strain on network resources and can set off alerts. Make sure to liaise with network communication staff to make sure that you are over straining the staff.
* **Security Teams:**  Security teams must be notified of Phishing campaigns so that they don’t treat it like an active incident. Make sure to provide the specific subject lines of the phishing emails to make sure that security teams can recognise real threats.

## Documentation

Before starting a phishing campaign, make sure to document communications and approvals at each step.

In particular, make sure to document these details are the corresponding approvals:

* The scope of the campaign
* The emails templates being used
* The time frame of the campaign, the start date and the end date
* The exact information that is being collected
* Any privacy measures being used to protect the results.

# Advanced Version: Images in Templates

The embedded image version of the script is optionally able to add a single image to a template if it is formatted in a correct way. The handling of email headers is a little bit more complicated, but it isn’t difficult to build based on pre-existing image templates.

Keep in mind that even if you are using a template without an image, this version of the script requires a corresponding image to exist, even if it is unused.

Typically images corresponding to templates that don’t use images are small and blank.