Phishing Assessment (GoPhish) Public

Friday, December 15, 2017 9:12 AM

****

GON' PHISHIN'

****

System Overview

The system runs on an Ubuntu 64-bit 14.04 virtual machine with 4 vCPU, 2 GB RAM, and 20 GB storage. The VM lives on an ESXi server. We are implementing the open source project Gophish (https://github.com/gophish/gophish) for campaign orchestration. It is currently on version 0.6.0. The webserver on port 80 is open to the world. There is documentation for the system at http://gophishsite:3333/gophish_user_guide.pdf and the API guide lives at http://gohpishsite:3333/api/

Maintenance of the Server

Regularly updating the host OS is important and won't affect GoPhish for the most part.

Third-Party Accounts

We used a third party email relay for authenticity

****

PART UNO

****

Running a Campaign

Running a successful campaign with no issues is an impossible task. It is possible to craft a campaign in such a way to not get the cops called on you, however.

There are 6 parts to a great self-phishing assessment:

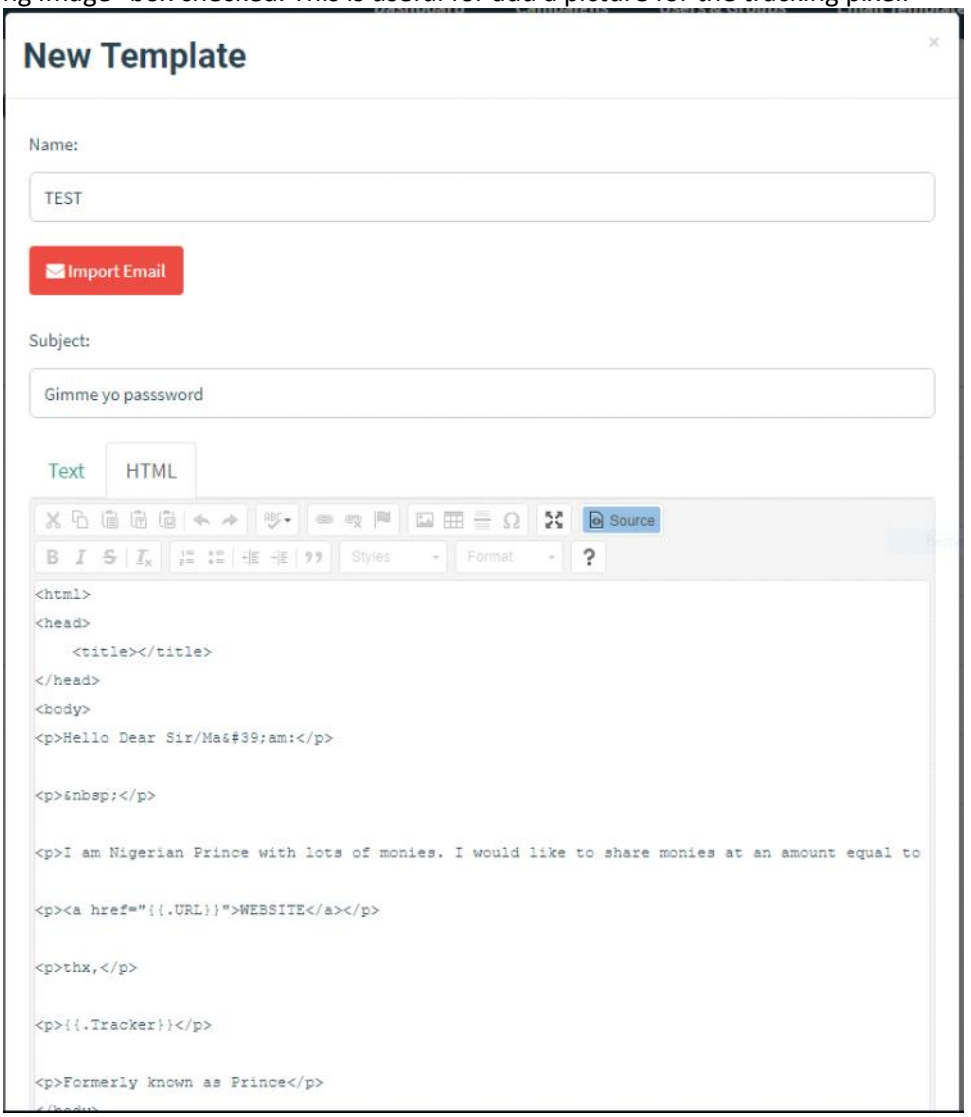
1. Email template from a real phishing email used in the wild
2. A landing page that emulates the "quality" of landing pages in the real world
3. An updated list of users and groups that will receive the emails
4. A "believable" sender address
5. Updating the website that users are redirected to after entering credentials
6. Putting it all together for scheduling

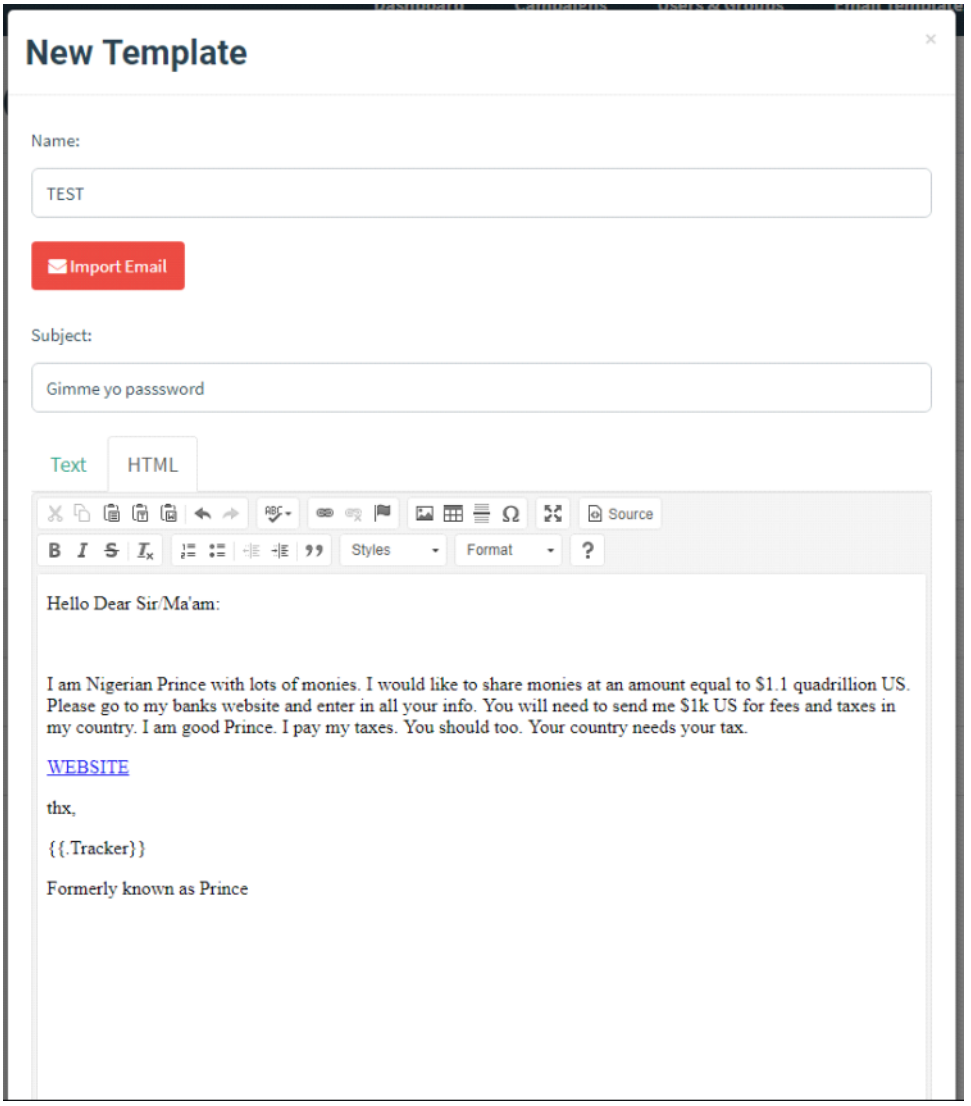
There are scripts that exist to help automate most of the tedious campaign setup. They are written in PowerShell because PowerShell is the future and it is available on all Windows machines and even on Linux and Unix machines (Microsoft did not pay me for the shameless PowerShell plug).

Setting up an email template

1. Log in at http://gophishsite:3333
2. Go to Email Templates
3. Click New Template
4. Give the template a unique name and a subject that will be sent with the email
5. For the body of the email, an example email can be pasted into the HTML tab of the body.

6. Be sure to check the source of the HTML for any strange trackers or embedded code
7. The email should have a hyperlink or a regular URL in it for users to click on
8. The URL to the landing page that will be defined when creating the campaign has a variable {{.URL}} to be used as a placeholder in the email.
9. A tracking pixel can be added to the email with {{.Tracker}} placed in the body and the "Add Tracking Image" box checked. This is useful for add a picture for the tracking pixel.





Creating a Landing Page

1. Go to the Landing Pages section in the Gophish UI.
2. Select "New Page"
3. There are two options for creating a page: Import a live website or create one using HTML
4. If a page is being imported, be sure to check for malicious or suspicious code. Trust no one
5. After the page looks "decent", check "Capture Submitted Data", make sure "Capture Passwords" in NOT checked, and make sure "Redirect to:" has the site you want to send users to entered in the box. This is where users will be sent after entering credentials.
6. We can add HTML code to the top of the webpage to automatically redirect users to the information page after a set amount of time. Statistics show that it takes an average of 33 seconds for a user to type in their credentials, so the site will redirect after 45 seconds by adding:

   <!DOCTYPE html>
   <html xmlns="http://www.w3.org/1999/xhtml">
   <head>
   <meta http-equiv="Content-Type" content="text/html; charset=windows-1252"/><meta http-equiv="refresh" content="45;url=https://yourlandingpage"/>
   </head>
   <body>

   Before the <body> tag

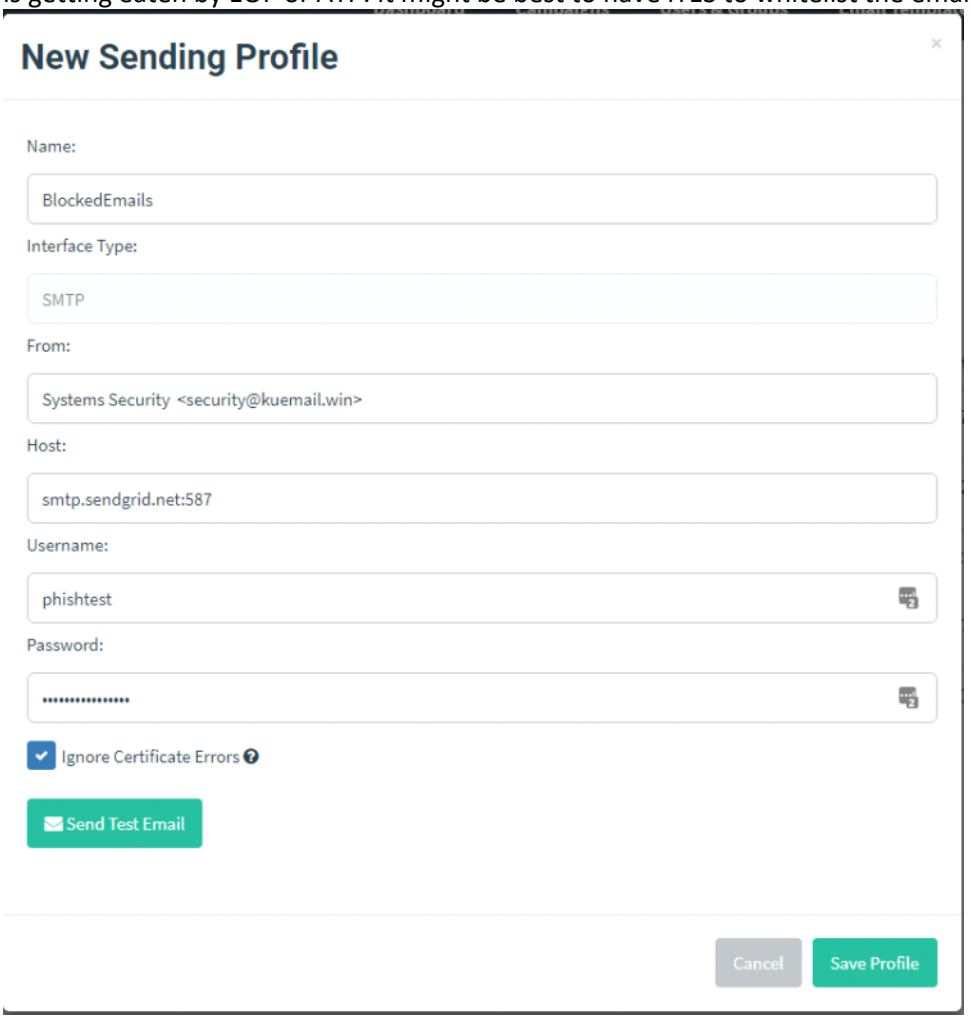
7. If there is a requirement for an image or other object to be served statically from the web server for the campaign, the static files will need to be copied to /<install directory>/static/endpoint on the server and they can be referred to in HTML with src="http://gophishserver/static/xxxx.png"
8. Save the page and that is done. Be sure to view the page before starting. It can be viewed in the editor by toggling between HTML mode and display mode.

Updating Users & Groups

1. This will not require any manual intervention in the UI unless something goes tango uniform
2. Use Create-GoPhishGroups.ps1
3. The script will pull from the AD groups listed at the top of the script and create groups in GoPhish based on those AD groups. It will also delete the previous groups that are already there automagically.
4. That is it

Updating the Sender Profiles

1. Go to Sending Profiles
2. Select "New Profile"
3. Give it a name. Whatever you will remember
4. Interface Type: SMTP
5. From: Name Name<email@email.com> i.e. "Threat Butticus <threatbutt@itisraining.men>"
6. I recommend sending a test email to yourself to make sure that the subject or email address is getting eaten by EOP or ATP. It might be best to have ITES to whitelist the email



Scheduling the Campaigns

The scheduling of the campaigns is mostly automated as well. There is a python script that doesn't exist at the time of this writing, but when it does it will require some input such as the start of the first group of emails to go out, the name of the email template, the name of the landing page, and the name of the sending profile. The script with then delete the old campaigns and schedule the news ones starting at the input time and each group will go 5 minutes after the previous group.

****

PART DEUX

****

Ending the campaigns & Obtaining the results

A python tool named GoReport is leveraged to complete the campaigns and pull the reports from them. The tool lives on the GoPhish server but can be installed on a local machine for ease of use. It is at https://github.com/chrismaddalena/GoReport. It will require the campaign IDs that are outputted during scheduling. They can also be obtained from the campaignstatus.py script. There are three ways to output campaign data: csv, word, and terminal. The CSV method is quicker, but not as easy to read. The word doc method takes a while since every user gets a table of data and much more GUI intensive and about 3 seconds per user so at 14k users it can take a long, long time.