EFFECTIVE PHISHING
with
GOPHISH

CactusCon 2019 | Mesa, AZ

Jayme Hancock | BSI CSIR US

ABOUT

Senior Network Penetration Tester for BSI AppSec

GXPN, OSCP, OSWP, CISSP, etc.

Co-Instructor: Full Scope Social Engineering @ BlackHat
Practical Remote Social Engineering @ WWHF

On Twitter at @highmeh

PHISHING OVERVIEW

Why is this important?

thaddeus e. grugq
@thegrugq

Give a man an 0day and he'll have access for a day, teach a man to phish and he'll have access for life.

2:35 AM · Feb 7, 2015 · Tweetbot for iOS

5.2K Retweets **7.6K** Likes

ABOUT THIS TALK

For **beginners**

(although 1337 SE's may learn something, too)

Quickly set up a phishing server and build campaigns

Track user behavior **–or-** pwn users more effectively

The best way to teach good habits? Constant reinforcement

And finally…

5

...ITS FUN TO DO BAD THINGS.

PHISHING BY THE NUMBERS

For the C-Levels

33%

of breaches in 2018 involved social engineering

32%

of breaches in 2018 involved phishing

29%

of breaches in 2018 used stolen credentials

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

78%

...of all espionage incidents involved phishing

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

OVERVIEW

Blue Team

- Set up a GoPhish Server
- Build believable campaigns
- Scale up sophistication
- Track user interaction, reporting, and trends

Red Team

- Set up a GoPhish Server
- Build malicious portals to capture credentials
- Deliver payloads and reuse credentials

GOPHISH FRAMEWORK

https://getgophish.com/

- Mature and Robust
- Actively Maintained
- GUI and API
- FREE

GOPHISH SETUP IN 5 MINUTES

- Spin up an EC2 Instance
- Log in via SSH
- Install Golang
- Download and unzip GoPhish
- Run GoPhish

GOPHISH SETUP IN 5 MINUTES

- Download and Configure (Details)

On your host:

```
$ ssh user@ip_or_hostname
```

On your server:

```
$ sudo apt-get update && sudo apt-get –y install golang unzip
$ wget https://github.com/gophish/gophish/releases/download/v0.8.0/gophish-v0.8.0-linux-64bit.zip
$ sudo unzip gophish-v0.8.0-linux-64bit.zip –d /opt/gophish
$ cd /opt/gophish
$ tmux new –s gophish *
$ sudo ./gophish
```

* Optional, kinda

GOPHISH SETUP IN 5 MINUTES

- Log In

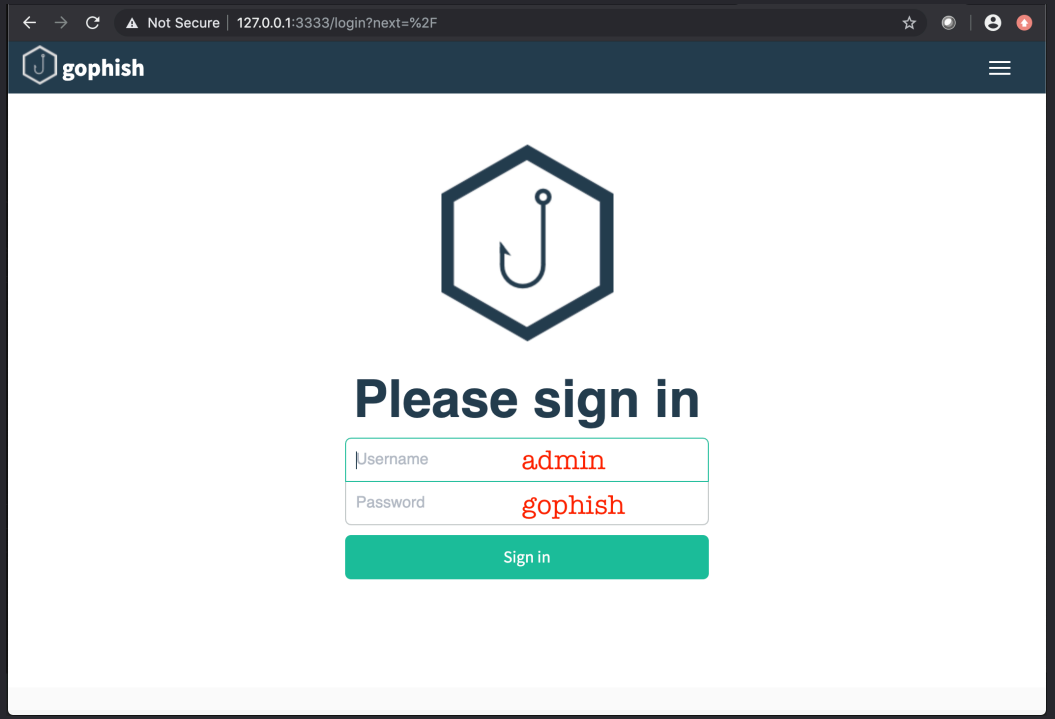
On your host:

```
$ ssh -Nf -L3333:localhost:3333
  user@ip_or_hostname
```

In your browser:

https://127.0.0.1:3333

```
Username: admin
Password: gophish
```



….but it doesn’t do anything yet.

GoPhish is a framework used to create and manage phishing campaigns, but it doesn’t create anything by default

Fortunately, it’s painless to set up a campaign from scratch.

BUILDING A CAMPAIGN: THE PIECES

Users & Groups

A list of users you want to phish, including emails, names, and titles

Email Templates

The actual e-mail you want to send, in HTML, text, or both

Landing pages

The page that users are sent to and interact with, if they click the link

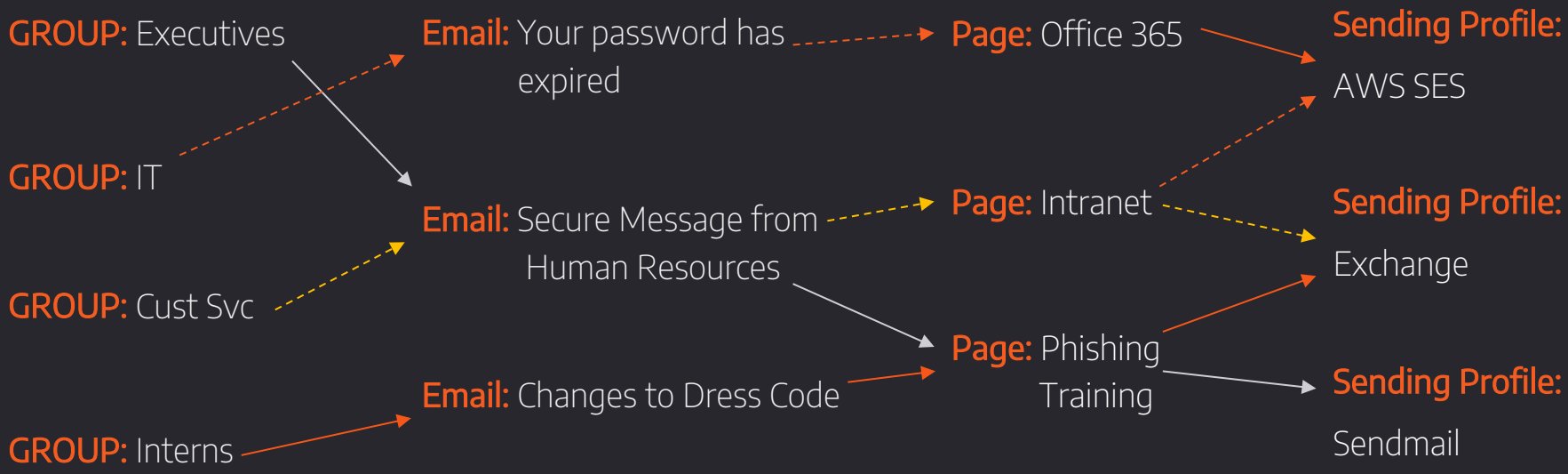
Sending Profile

The email server itself, and the settings that allow your phish to be sent

A Campaign consists of all of the above items together

Email Template sent via *Sending Profile* to *User Group* directing to a *Landing Page*

BUILDING A CAMPAIGN: MIX AND MATCH!



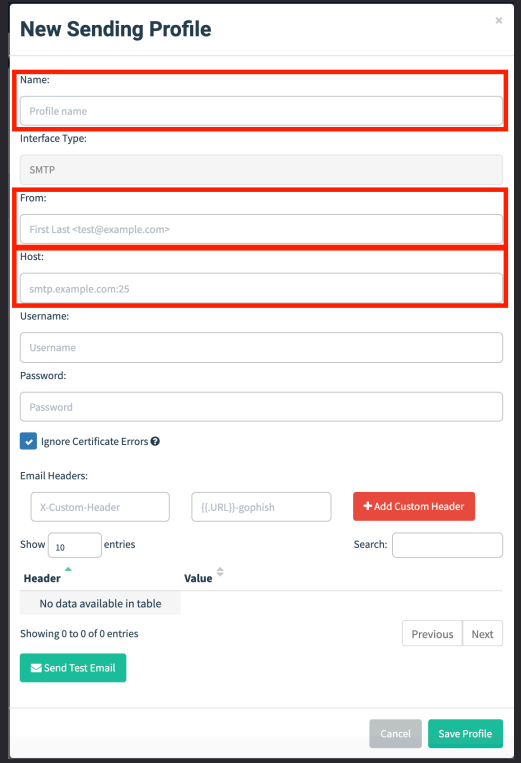
LETS BUILD A CAMPAIGN!

In the next few slides, we'll build out a phishing campaign in GoPhish, step by step.

LETS BUILD A CAMPAIGN! Sending Profile

The sending profile tells GoPhish how to send the email itself.

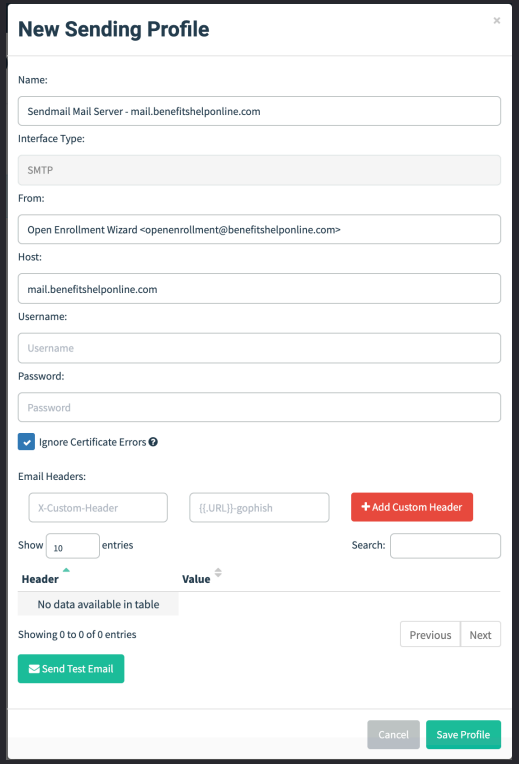
The only *required* fields are Name, From, and Host – but your server may require a username and password, too.



LETS BUILD A CAMPAIGN! Sending Profile

The sending profile tells GoPhish how to send the email itself.

The only *required* fields are Name, From, and Host – but your server may require a username and password, too.

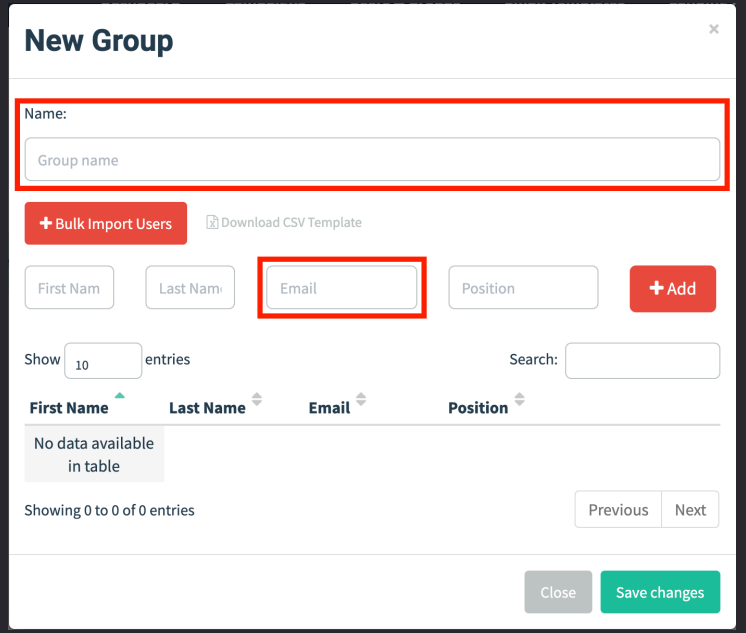


LETS BUILD A CAMPAIGN! Users and Groups

Users and groups allows you to enter logical groups of targets to phish.

The only *required* field is **Email**, but entering all fields allows you to pull from those fields into emails for a tailored phish

Tip: You can batch-upload via CSV file

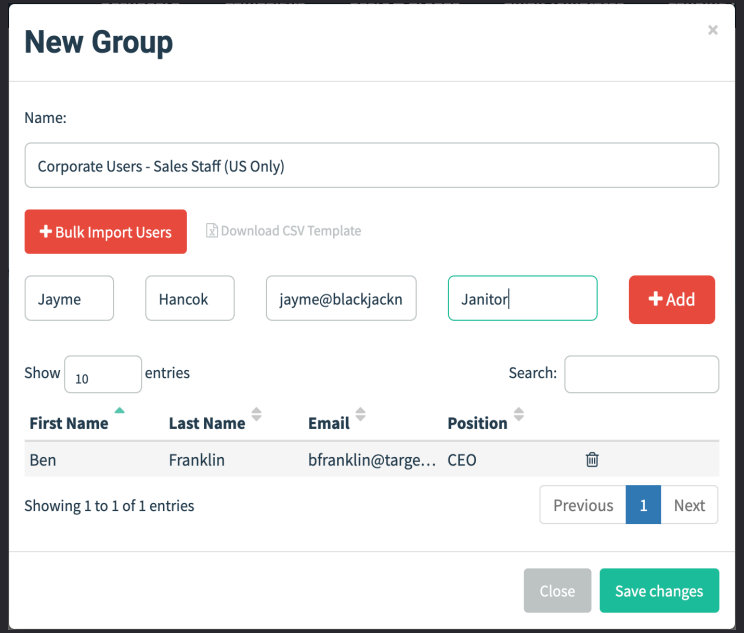


LETS BUILD A CAMPAIGN! Users and Groups

Users and groups allows you to enter logical groups of targets to phish.

The only *required* field is **Email**, but entering all fields allows you to pull from those fields into emails for a tailored phish

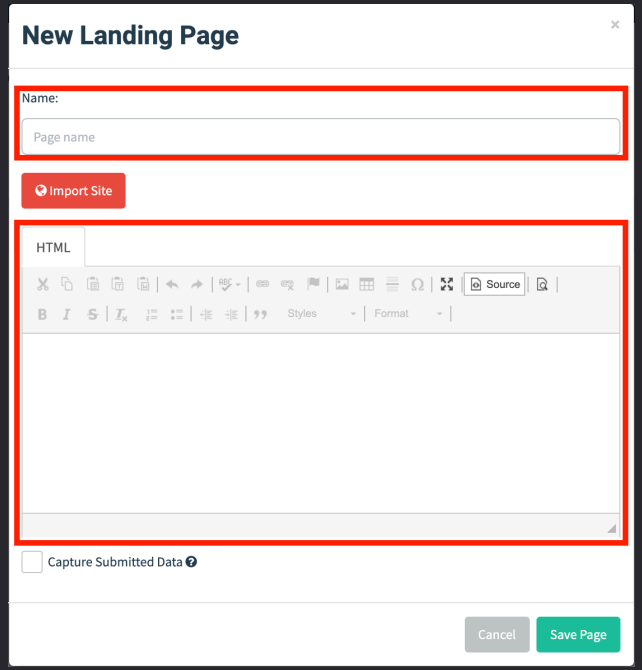
Tip: You can batch-upload via CSV file



LETS BUILD A CAMPAIGN! Landing Page

The landing page dialog gives you a WYSIWYG editor to build the page the user will see when they click the phishing link

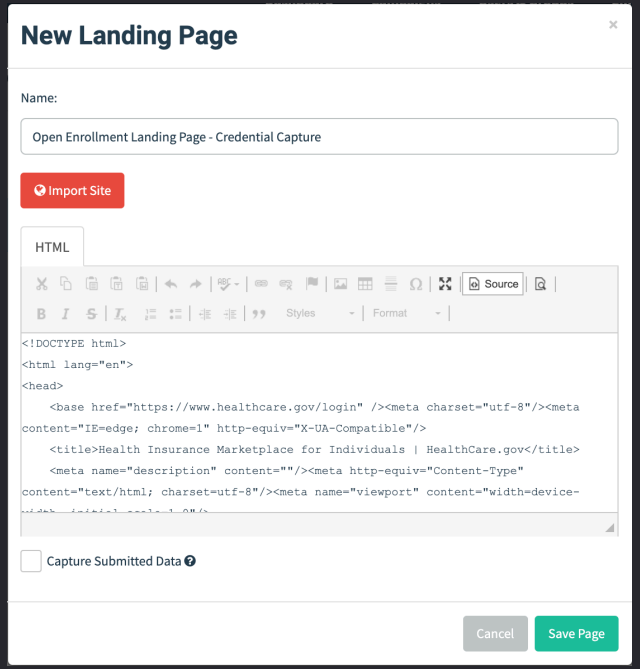
If “Capture Submitted Data” is checked, any posted forms will capture all user input (except passwords)



LETS BUILD A CAMPAIGN! Landing Page

The landing page dialog gives you a WYSIWYG editor to build the page the user will see when they click the phishing link

If “Capture Submitted Data” is checked, any posted forms will capture all user input (except passwords)

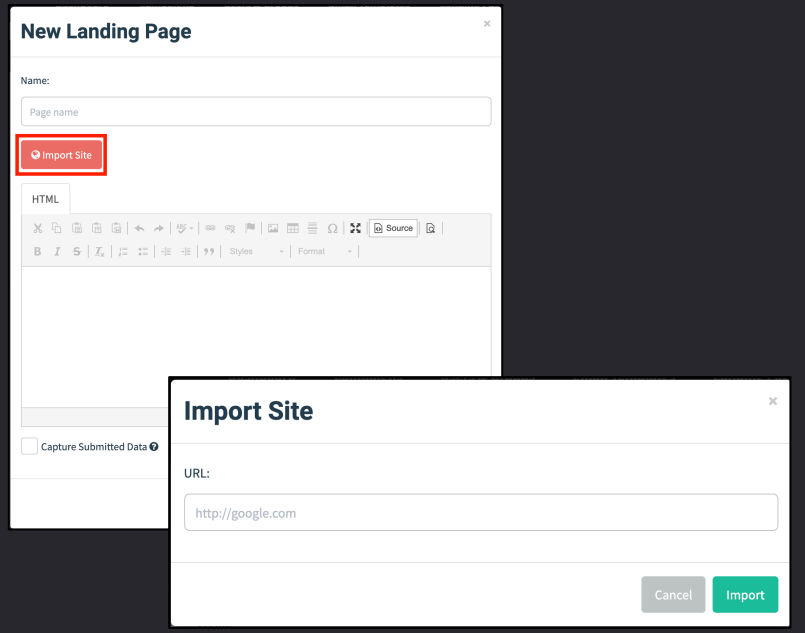


LETS BUILD A CAMPAIGN! Landing Page

You can also import a valid site by using the “Import Site” function.

This hotlinks images and keeps links intact, so be careful!

Note: Some scripts may not work – test before going live with a phishing campaign

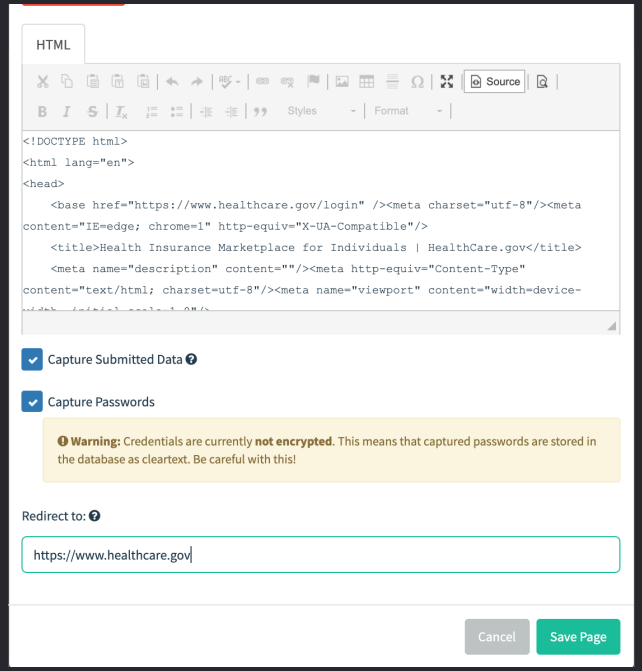


LETS BUILD A CAMPAIGN! Landing Page

For **red team** or offensive campaigns, the landing page dialog box has an option to capture passwords, and to redirect users to another page after the form is posted.

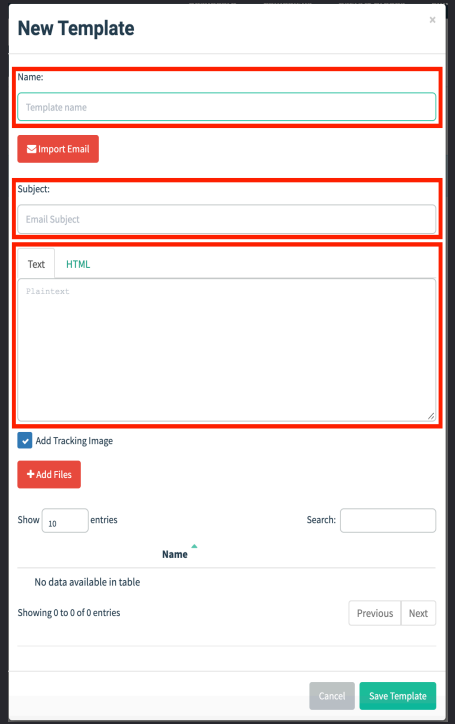
Red Tip: Send the users to a malicious payload (like an .hta) instead of a webpage

Blue Tip: Capture data but not passwords, redirect to a phishing education page



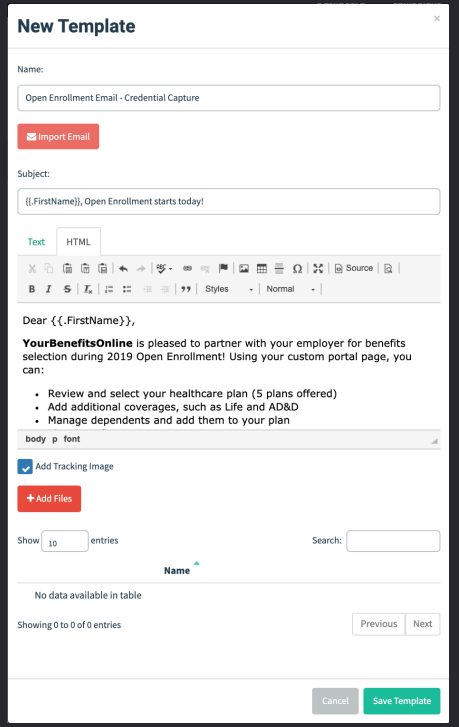
LETS BUILD A CAMPAIGN! Email Template

The Email Template dialog contains the text and HTML emails that will be sent to your targets. Note you can import an email if you have one you want to clone.



LETS BUILD A CAMPAIGN! Email Template

The Email Template dialog contains the text and HTML emails that will be sent to your targets. Note you can import an email if you have one you want to clone.



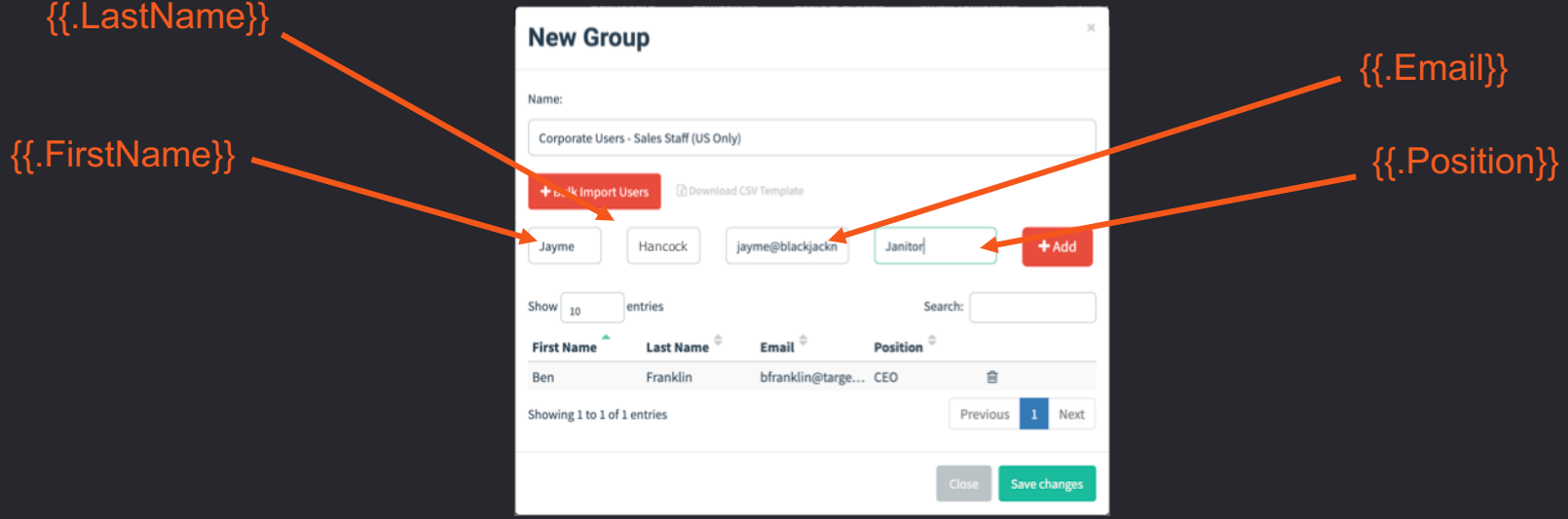
LETS BUILD A CAMPAIGN! Variables

You may have noticed code such as {{.FirstName}} in previous slides. These are variables that draw from other parts of GoPhish to customize a campaign.

Variables	Source
{{.FirstName}}, {{.LastName}}, {{.Email}}, {{.Position}}	Users & Groups
{{.RId}}, {{.TrackingURL}}, {{.Tracker}}, {{.URL}}, {{.BaseURL}}	Campaigns
{{.From}}	Sending Profile

LETS BUILD A CAMPAIGN! Variables

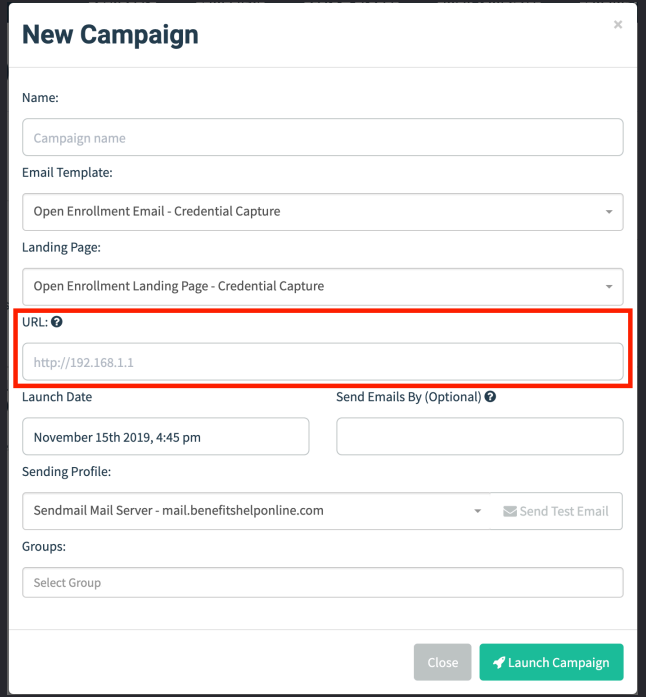
You may have noticed code such as {{.FirstName}} in previous slides. These are variables that draw from other parts of GoPhish to customize a campaign.



LETS BUILD A CAMPAIGN! Creating The Campaign

The Campaign dialog box ties everything together. This allows you to mix and match by selecting one of each:

- Sending Profile
- User Group
- Email Template
- Landing Page

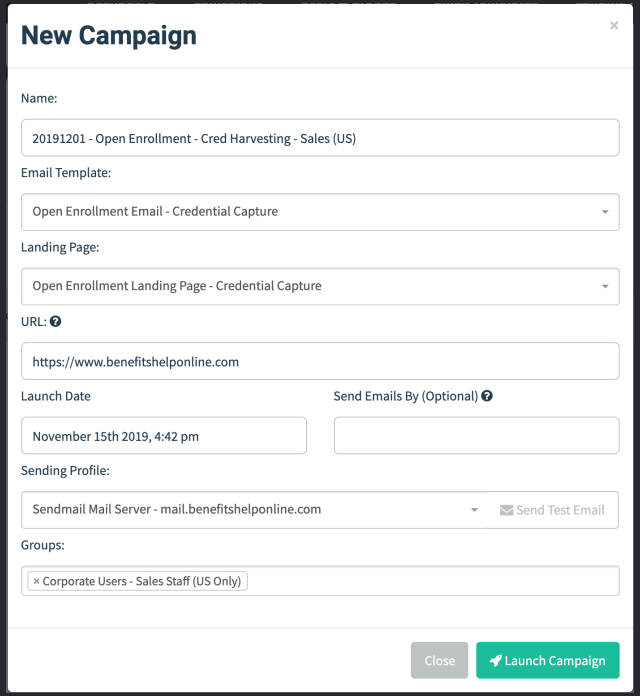


LETS BUILD A CAMPAIGN! Creating The Campaign

The Campaign dialog box ties everything together. This allows you to mix and match by selecting one of each:

- Sending Profile
- User Group
- Email Template
- Landing Page

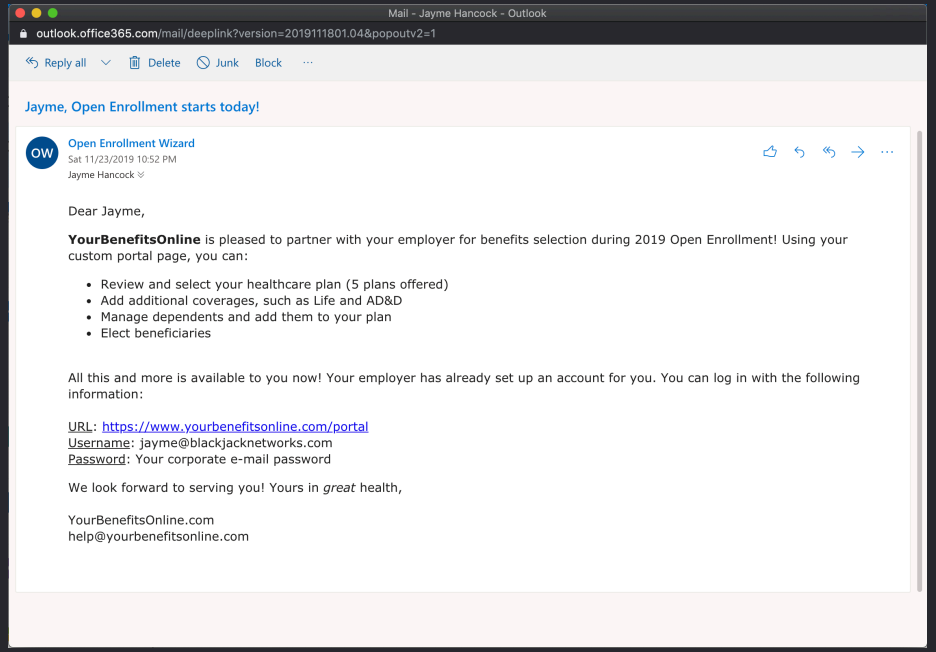
Note: As of this version, GoPhish doesn't have a dropdown for the URL. Be sure this is typed correctly and uses the correct protocol!



LETS BUILD A CAMPAIGN! Sending The Campaign

Once the campaign is sent and confirmed, the user receives an email. Note that the variables (*{{.FirstName}}*, etc.) are replaced with actual values.

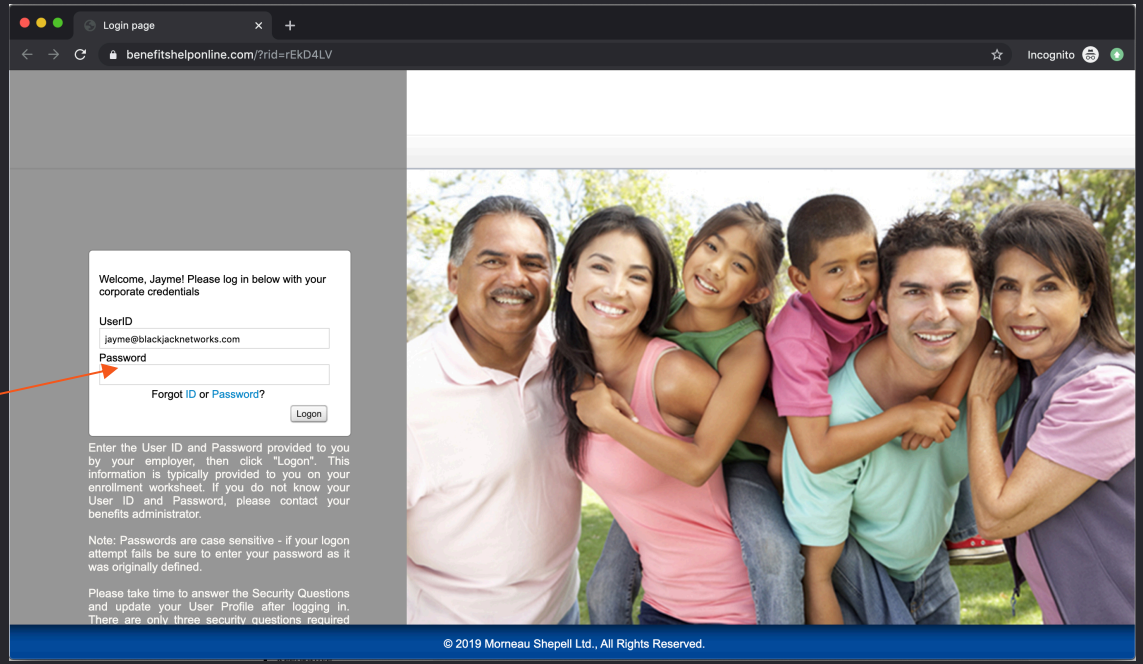
If the phish is convincing, the user clicks your link...



LETS BUILD A CAMPAIGN! Sending The Campaign

…and hits the landing page.

If the landing page is convincing, the user enters their creds…

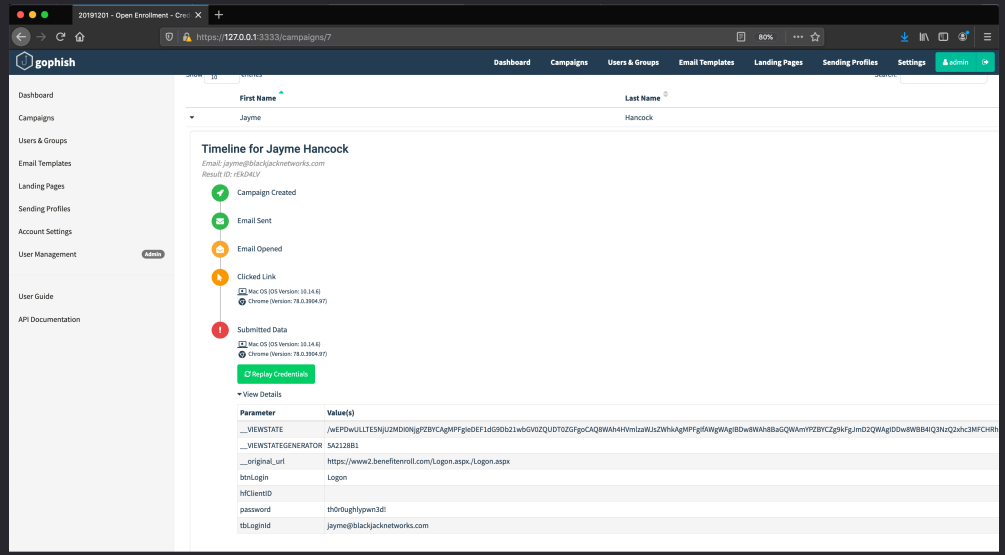


LETS BUILD A CAMPAIGN! Sending The Campaign

In the GoPhish Admin Console, under Campaigns, we can see a timeline of user interactions. Note that the one user in scope has opened the email, clicked the link, and entered data.

LETS BUILD A CAMPAIGN! Sending The Campaign

Selecting a user and scrolling down gives a detailed timeline, and all submitted data. We've now got credentials to continue our attack.



Now that we can phish, lets talk Phishing Strategy

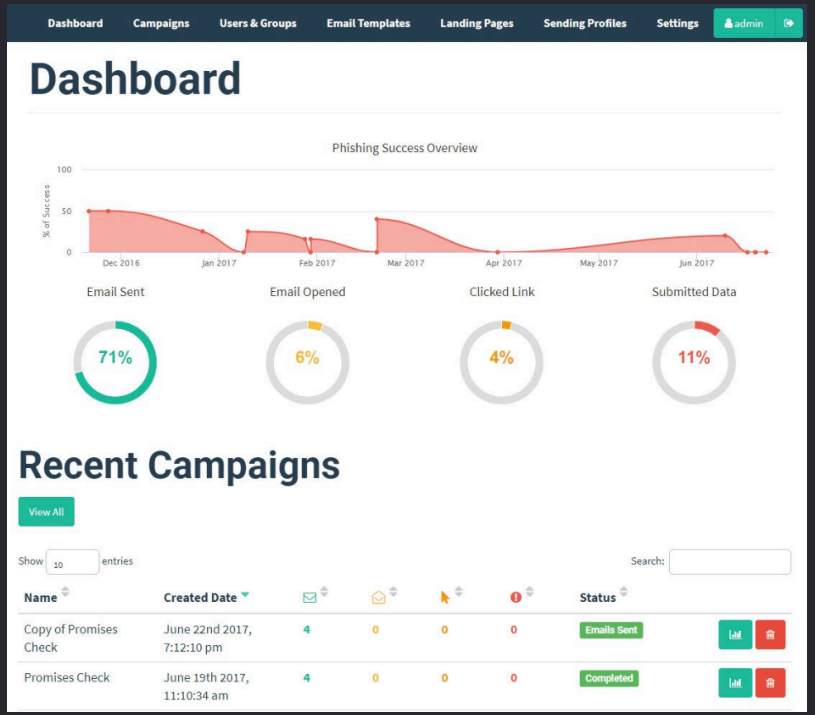
BLUE TEAM

GOALS: Blue Team

- Metrics, Metrics, Metrics
- Measuring security posture
- User Awareness Training
- Justification of services / controls

GOALS: Blue Team

- Metrics, Metrics, Metrics
  - Built in dashboard gives (limited) info at a glance



https://twitter.com/jw_sec

GOALS: Blue Team

- Metrics, Metrics, Metrics
  - Campaign Export:
    - **Results**
    - Raw Events

id	status	ip	latitude	longit	send_date	reported	modified_da	email	first_name	last_name
rEkD4LV	Submitted Data	100.15.	38	-97	2019-11-24T	FALSE	2019-11-24T	jayme@l	Jayme	Hancock
f2LgMg2	Submitted Data	99.241.	38	-97	2019-11-24T	FALSE	2019-11-24T	testuser(	Tom	Jones
a93MgnT	Clicked Link	13.4.11	38	-97	2019-11-24T	FALSE	2019-11-24T	internet(	Bob	Barker
t8f821v	Email Opened	91.91.3	38	-97	2019-11-24T	FALSE	2019-11-24T	fakeuser	Fake	User

“Export CSV > Results”

GOALS: Blue Team

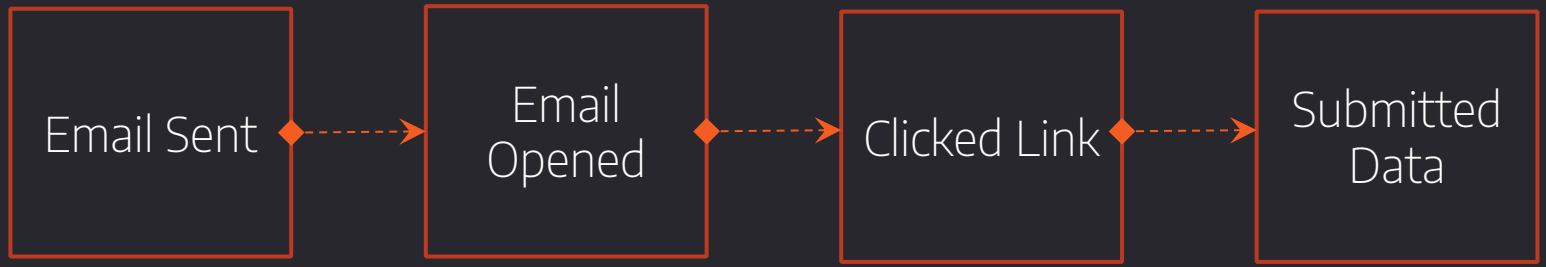
- Metrics, Metrics, Metrics
  - Campaign Export:
    - Results
    - **Raw Events**

email	time	message	details
	2019-11-24T03:54:19.096	Campaign Created	
jayme@l	2019-11-24T03:54:19.544	Email Sent	
jayme@l	2019-11-24T03:54:37.708	Email Opened	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T03:54:44.140	Clicked Link	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T03:56:25.197	Submitted Data	{"payload":{"__VIEWSTATE":["/wEPDwULLTE5NjU2MDI0NjgP
jayme@l	2019-11-24T16:44:38.721	Email Opened	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T16:45:45.869	Clicked Link	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T16:45:47.150	Clicked Link	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T16:46:04.585	Clicked Link	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T16:46:04.756	Clicked Link	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T16:47:17.600	Clicked Link	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.
jayme@l	2019-11-24T16:47:17.807	Clicked Link	{"payload":{"rid":["rEkD4LV"]},"browser":{"address":"100.15.

“Export CSV > Raw Data”

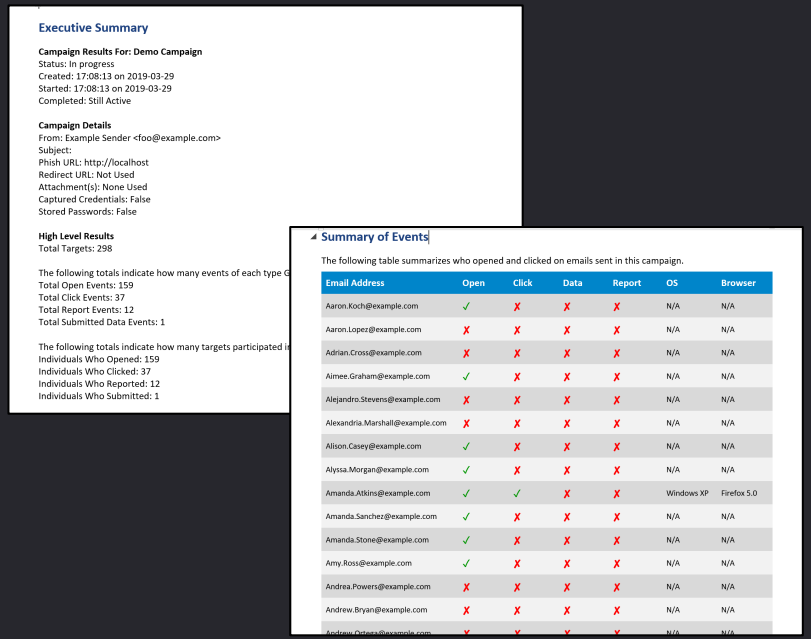
GOALS: Blue Team

Phishing Lifecycle:
Only the latest step is reported in the “Results” output



GOALS: Blue Team

- Metrics, Metrics, Metrics
  - Reporting: GoReport
    - Clean reporting style
    - Customizable .docx
    - Perfect for internal deliverables



Executive Summary

Campaign Results For: Demo Campaign
Status: In progress
Created: 17:08:13 on 2019-03-29
Started: 17:08:13 on 2019-03-29
Completed: Still Active

Campaign Details
From: Example Sender <foo@example.com>
Subject:
Phish URL: http://localhost
Redirect URL: Not Used
Attachment(s): None Used
Captured Credentials: False
Stored Passwords: False

High Level Results
Total Targets: 298

The following totals indicate how many events of each type G
Total Open Events: 159
Total Click Events: 37
Total Report Events: 12
Total Submitted Data Events: 1

The following totals indicate how many targets participated i
Individuals Who Opened: 159
Individuals Who Clicked: 37
Individuals Who Reported: 12
Individuals Who Submitted: 1

Summary of Events

The following table summarizes who opened and clicked on emails sent in this campaign.

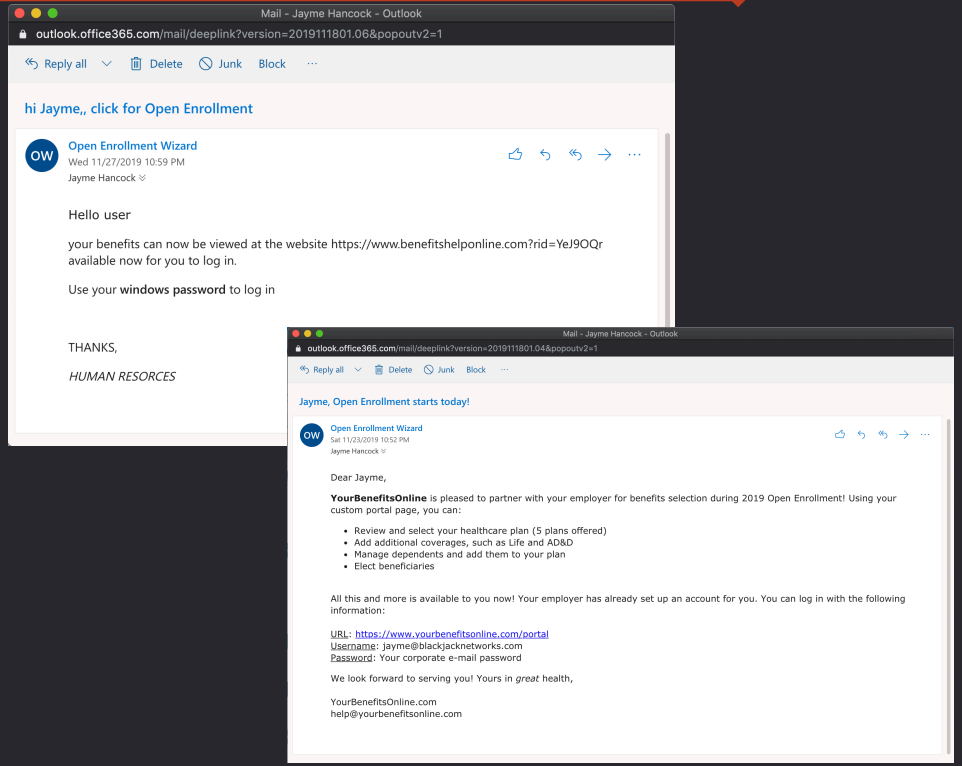
Email Address	Open	Click	Data	Report	OS	Browser
Aaron.Koch@example.com	✓	✗	✗	✗	N/A	N/A
Aaron.Lopez@example.com	✗	✗	✗	✗	N/A	N/A
Adrian.Cross@example.com	✗	✗	✗	✗	N/A	N/A
Aimee.Graham@example.com	✓	✗	✗	✗	N/A	N/A
Alejandro.Stevens@example.com	✗	✗	✗	✗	N/A	N/A
Alexandria.Marshall@example.com	✗	✗	✗	✗	N/A	N/A
Alison.Casey@example.com	✓	✗	✗	✗	N/A	N/A
Alyssa.Morgan@example.com	✓	✗	✗	✗	N/A	N/A
Amanda.Atkins@example.com	✓	✓	✗	✗	Windows XP	Firefox 5.0
Amanda.Sanchez@example.com	✓	✗	✗	✗	N/A	N/A
Amanda.Stone@example.com	✓	✗	✗	✗	N/A	N/A
Amy.Ross@example.com	✓	✗	✗	✗	N/A	N/A
Andrea.Powers@example.com	✗	✗	✗	✗	N/A	N/A
Andrew.Bryan@example.com	✗	✗	✗	✗	N/A	N/A

https://github.com/chrismaddalena/GoReport

GOALS: Blue Team

- Measuring Security Posture
  - Email Sophistication

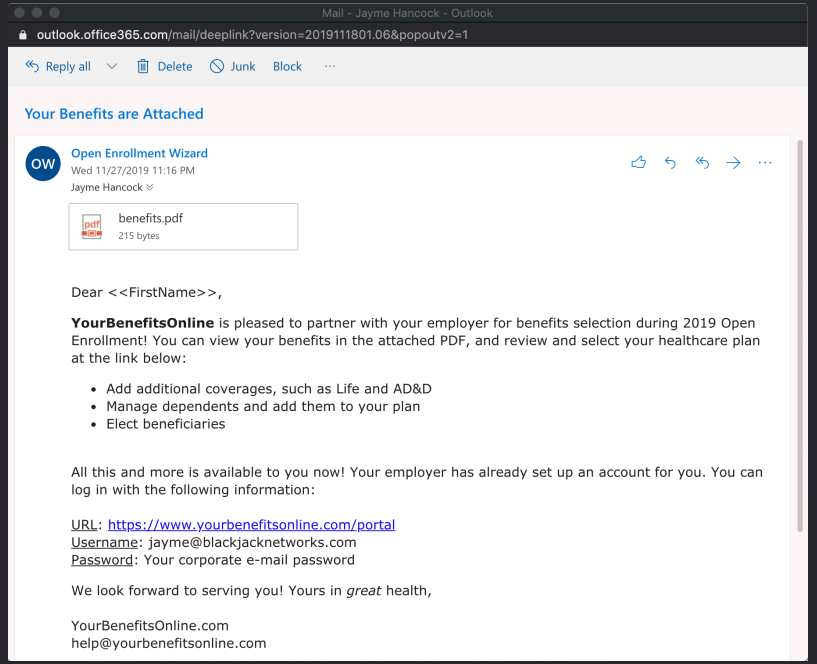
What level of sophistication gets spotted/reported? Which slips through?



GOALS: Blue Team

- Measuring Security Posture
  - Email Sophistication

Do users open emails with attachments more often?



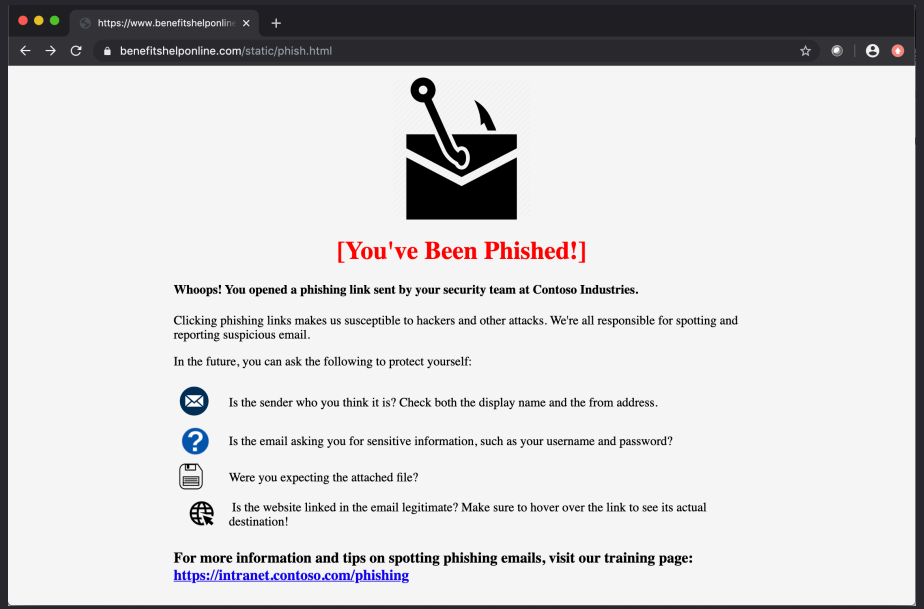
GOALS: Blue Team

- User Awareness Training
  - Redirect URL

Save static assets in:

gophish/static/endpoint

They'll upload to:
https://phishingurl.com/static/file.html



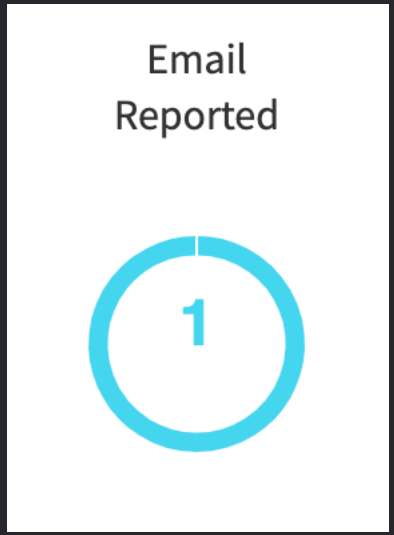
GOALS: Blue Team

- User Awareness Training
  - Built-In Reporting

GoPhish has a “Report” functionality built-in. Navigating to:

https://phishingurl.com/report?rid={{.Rid}}

Sets the report flag to “Yes”



GOALS: Blue Team

- User Awareness Training
  - Built-In Reporting

Downside: Server-side code exists to handle reporting. Client-side does not.

- You can build an Outlook/Gmail plug-in
- You can give your admins a tool like PhishReporter.py:

https://github.com/highmeh/phishing/blob/master/phishreporter.py

```
$ ./phishreporter.py
[+] Connecting...
[?] Enter RID to report: rEkD4LV
[+] Locating the campaign for rEkD4LV...
[+] Found RID in Campaign #7...
[+] jayme@blackjacknetworks.com reported rEkD4LV as a phishing email!
```

GOALS: Blue Team

- Justification of services / controls

  Pretty self explanatory: If your users continue to click phishing emails despite testing and training, you may be able to justify implementing additional technical controls. Data talks.

RED TEAM

GOALS: Red Team

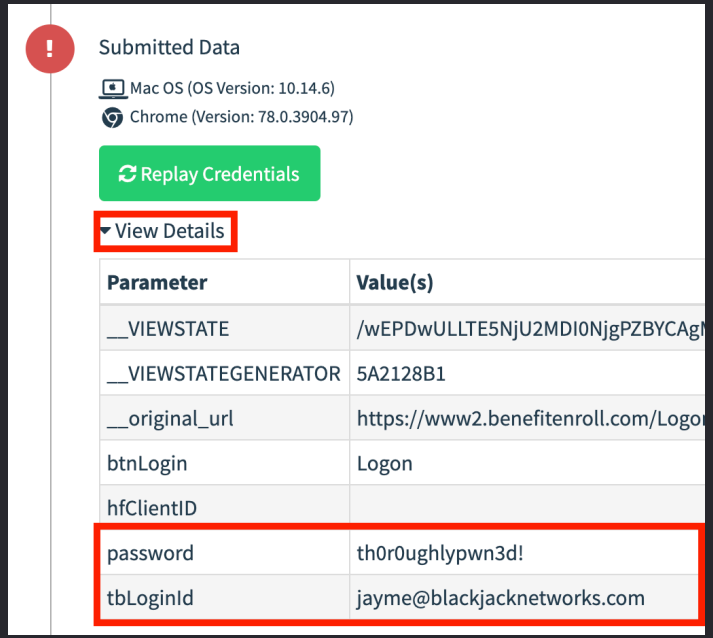
- Capture Credentials
- Deliver Payloads

GOALS: Red Team

- Capture Credentials
  - Raw Capture
  - Log in to service

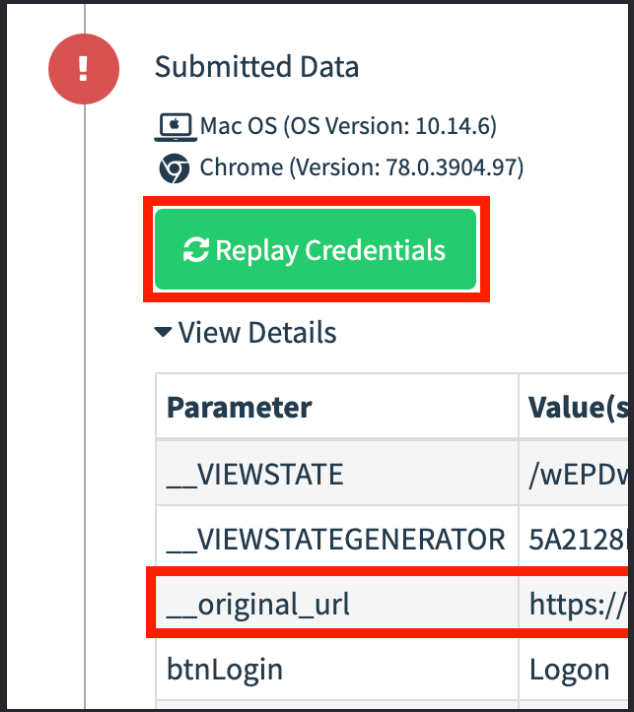
GOALS: Red Team

- Capture Credentials
  - **Raw Capture**
  - Log in to service



GOALS: Red Team

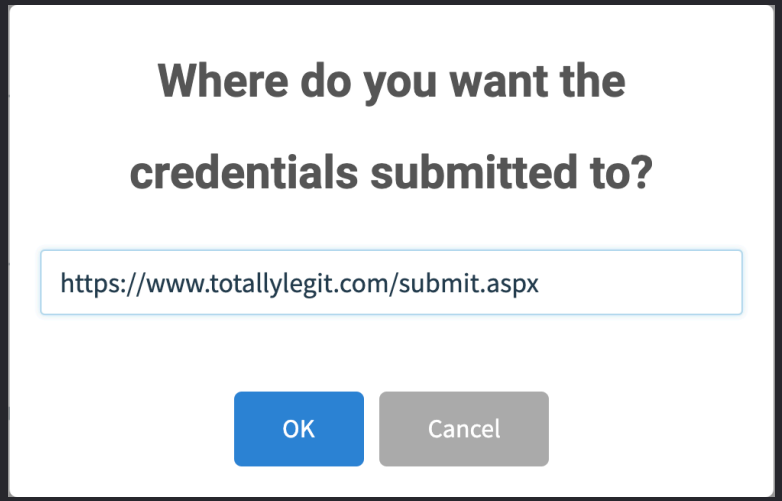
- Capture Credentials
  - Raw Capture
  - **Log in to service**



GOALS: Red Team

- Capture Credentials
  - Raw Capture
  - **Log in to service**

Sends a post request with the captured data in a separate browser window

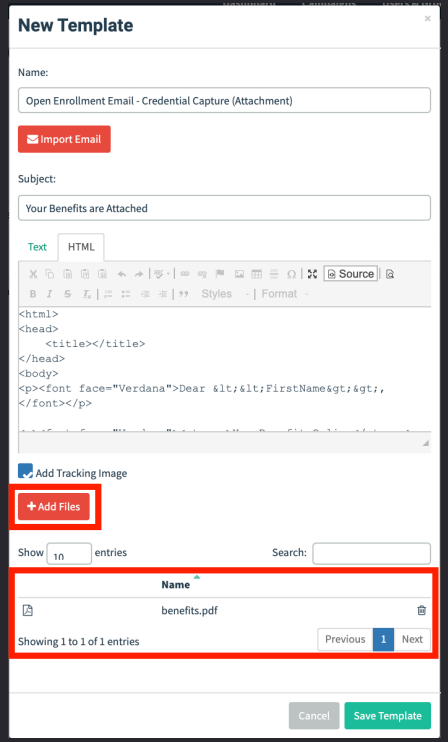


GOALS: Red Team

- Deliver Payloads
  - Email Attachment
  - Host and redirect

GOALS: Red Team

- Deliver Payloads
  - **Email Attachment**
  - Host and redirect



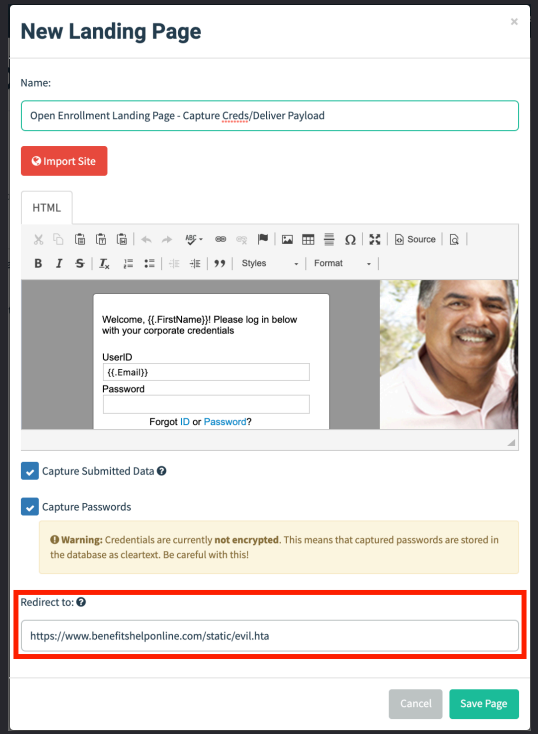
GOALS: Red Team

- Deliver Payloads
  - Email Attachment
  - **Host and redirect**

Save payloads (ex: evil.hta) in:

gophish/static/endpoint

They'll upload to: https://phishingurl.com/static/evil.hta



TARGET COLLECTION

The important part

TARGET COLLECTION

Targeting the right users is crucial to both red and blue team engagements

For Red: Staying in scope, finding likely targets
For Blue: Targeting training and continuous phishing

TARGET COLLECTION

Blue:

Determine users in scope, generate a list. Modify the list as data is gathered

Use Open-Source Intelligence Gathering to determine footprint available to an attacker

TARGET COLLECTION

Red:

Ask for a list of approved contacts, or a list of users to exclude

Use Open-Source Intelligence Gathering to find your targets

Automation

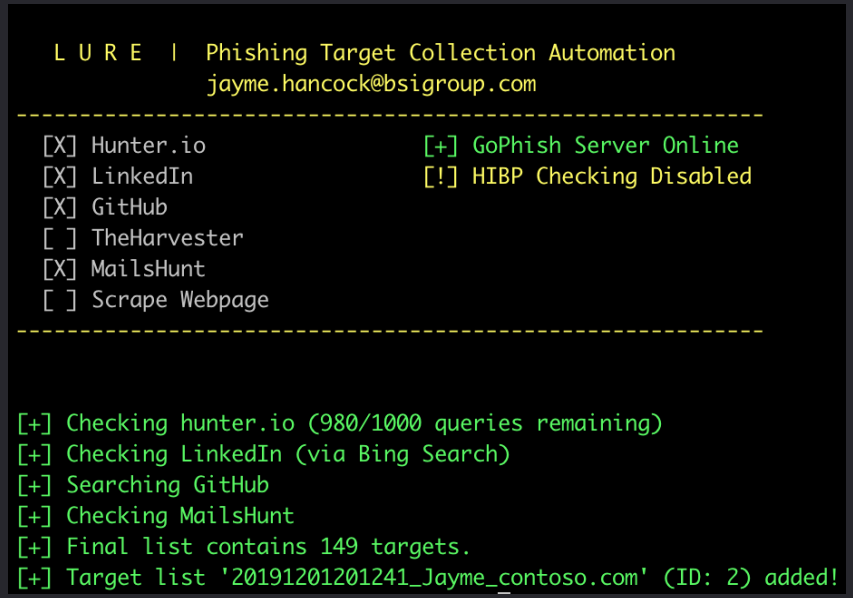
Multiple open-source tools exist to help collect target data from public internet sources.

TARGET COLLECTION

Automation: Lure

Lure scrapes webpages, pilfers email search pages, and checks databases to find targets. It's **designed** to work with GoPhish.

https://github.com/highmeh/lure



BEST PRACTICES

Increasing Effectiveness

GENERAL TIPS: HTTPS

Configure HTTPS!

By default, GoPhish uses a self-signed certificate. This isn't good if you want a successful campaign.

- Use LetsEncrypt!
- After issuing a certificate, add the path to config.json and enable TLS:

```
"use_tls": true,
"cert_path": ”/etc/letsencrypt/live/domain/fullchain.pem",
"key_path": ”/etc/letsencrypt/live/domain/privkey.pem"
```

GENERAL TIPS: HTTPS

HTTPS: Multiple Phishing Domains

If you host multiple phishing domains, consider configuring a TLS certificate with Subject Alternative Names:

```
$certbot certonly -d phishingdomain.com -d anotherphishingdomain.com –d
 athirdphishingdomain.com –d evenmorephishingdomains.net
```

GENERAL TIPS: TRANSPARENCY

GoPhish adds two headers to each email by default:

```
“X-Mailer: GoPhish”
“X-Gophish-Contact: admin@domain.com”
```

These add transparency to your campaigns:

- Identifies you as non-malicious to incident responders
- Provides an abuse contact

More info: https://github.com/gophish/gophish/issues/1057

GENERAL TIPS: TRANSPARENCY

Red teaming and afraid this will burn you?

Compile it yourself; comment out references to “X-Mailer” and “config.ServerName":

```
gophish/models/maillog_test.go
gophish/models/maillog.go
gophish/models/smtp_test.go
gophish/models/email_request.go
gophish/models/email_request_test.go
```

GENERAL TIPS: MAIL SERVERS

High Reputation Mail Servers

Sure, you can install up Sendmail and get your DNS records configured...

- Is the server configured properly?
- Are SPF, DKIM, and DMARC configured correctly?
- Has your mail server's IP been blacklisted in the past?

Consider using a high reputation mail server; many are available for free under a certain threshold (usually around ~10,000 emails per month.) Ex: Amazon SES, Sendgrid

TAKEAWAYS

In summary…

KEY TAKEAWAYS

Phishing doesn't have to be difficult.

Creating convincing campaigns shouldn't be subject to your budget.

Attackers aren't just hitting your external hosts and giving up – educate and prepare your users.

Numbers talk – baselining your users' social engineering readiness will get initiatives pushed through faster.

THANKS!

ANY QUESTIONS?

@highmeh