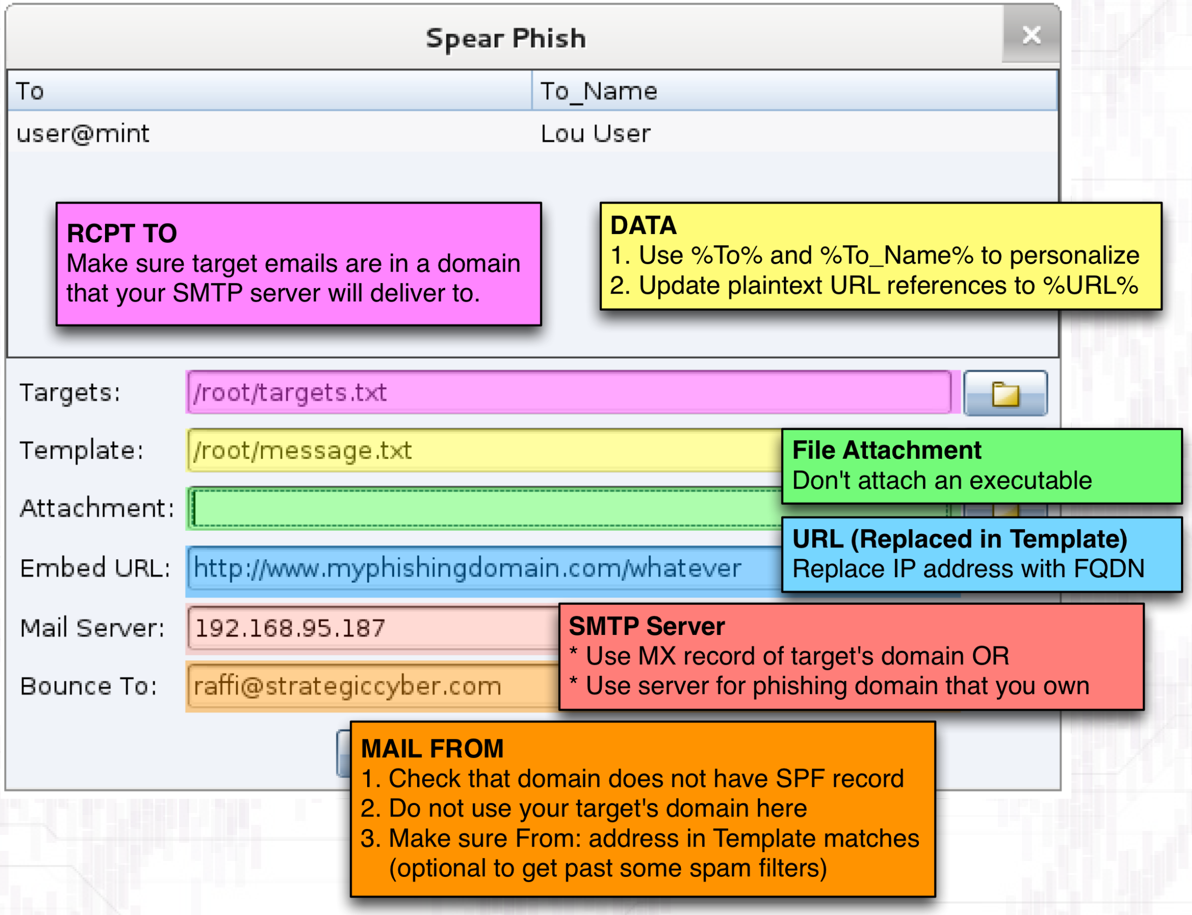
Spear Phishing

Cobalt Strike's spear phishing tool allows you to send pixel perfect spear phishing messages using an arbitrary message as a template. Go to **Attacks** -> **Spear Phish** to open the spear phishing tool.



To	To_Name
user@mint	Lou User

RCPT TO
Make sure target emails are in a domain that your SMTP server will deliver to.

DATA
1. Use %To% and %To_Name% to personalize
2. Update plaintext URL references to %URL%

Targets: /root/targets.txt

Template: /root/message.txt

Attachment:

Embed URL: http://www.myphishingdomain.com/whatever

Mail Server: 192.168.95.187

Bounce To: raffi@strategiccyber.com

File Attachment
Don't attach an executable

URL (Replaced in Template)
Replace IP address with FQDN

SMTP Server
* Use MX record of target's domain OR
* Use server for phishing domain that you own

MAIL FROM
1. Check that domain does not have SPF record
2. Do not use your target's domain here
3. Make sure From: address in Template matches (optional to get past some spam filters)

Set **Targets** to import a list of targets. You may import a flat text-file containing one email address per line. Import a file containing one email address and name separated by a tab or comma for stronger message customization.

Set **Template** to an email message template. A Cobalt Strike message template is simply a saved email message. Cobalt Strike will strip unnecessary headers, remove attachments, rewrite URLs, re-encode the message, and rewrite it for you.

Cobalt Strike does not give you a means to compose a message. Use an email client, write a message, and send it to yourself. Most webmail clients include a means to see the original message source. In GMail, click the down arrow next to Reply and select Show original.

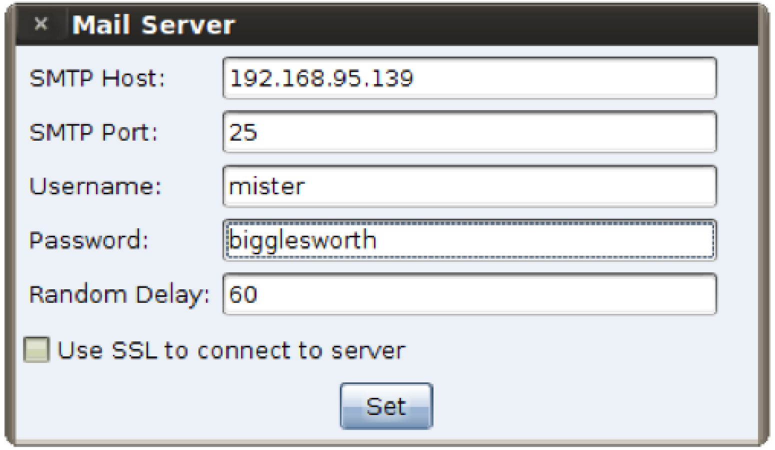
You may customize a saved message with Cobalt Strike tokens. Cobalt Strike replaces these tokens when sending an email. The tokens include:

Token	Description
%To%	The email address of the person the message is sent to
%To_Name%	The name of the person the message is sent to. This token is only available when importing a tab-separated file containing a name.
%URL%	The contents of the URL field in the spear phishing dialog.

Set **Embed URL** to have Cobalt Strike rewrite each URL in the message template to point to the embedded URL. URLs added in this way will contain a token that allows Cobalt Strike to trace any visitor back to this particular spear phishing attack. Cobalt Strike's reporting and web log features take advantage of this token. Press **...** to choose one of the Cobalt Strike hosted sites you've started.

Set **Mail Server** to an open relay or the mail exchange record for your target. If necessary, you may also authenticate to a mail server to send your phishing messages.

Press **...** next to the Mail Server field to configure additional server options. You may specify a username and password to authenticate with. The Random Delay option tells Cobalt Strike to randomly delay each message by a random time, up to the number of seconds you specify. If this option is not set, Cobalt Strike will not delay its messages.



SMTP Host: 192.168.95.139

SMTP Port: 25

Username: mister

Password: bigglesworth

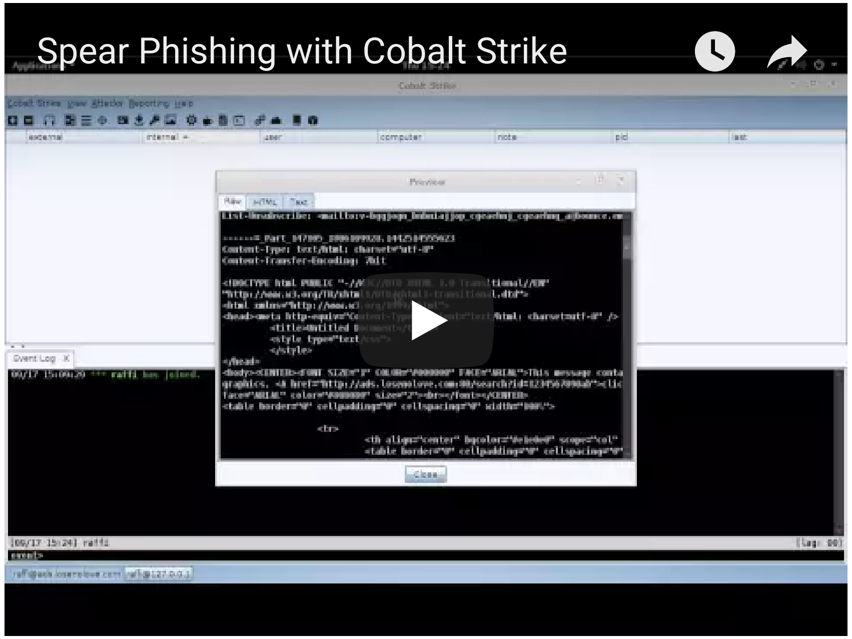
Random Delay: 60

□ Use SSL to connect to server

Mail Server Options

Set **Bounce To** to an email address where bounced messages should go. This value will not affect the message your targets see. Press **Preview** to see an assembled message to one of your recipients. If the preview looks good, press **Send** to start your attack.

Cobalt Strike's spear phishing tool sends messages through the team server you're connected to.



```
List-Unsubscribe: <mailto:v-bgqjoqn_bnbmiajjop_cqeaehmj_cqeaehmj_ajbounce.m
------=_Part_147005_1006109928.1442504555623
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: 7bit

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title>Untitled Document</title>
        <style type="text/css">
        </style>
</head>
<body><CENTER><FONT SIZE="1" COLOR="#000000" FACE="ARIAL">This message conta
graphics. <A href="http://ads.losenolove.com:80/search?id=1234567890ab"><lic
face="ARIAL" color="#000000" size="2"><br></font></CENTER>
<table border="0" cellpadding="0" cellspacing="0" width="100%">

            <tr>
                    <th align="center" bgcolor="#ebebeb" scope="col"
                    <table border="0" cellpadding="0" cellspacing="0"
```

```
09/17 15:09:29 *** raffi has joined.
[09/17 15:24] raffi                                   [lag: 00]
event>
```

raffi@ads.losenolove.com | raffi@127.0.0.1

Press Information Contact

© 2012-2018 Strategic Cyber, LLC | Blog