Spam

Spam Complaints

Before working on any spam complaints, go through the Abuse Open queue and merge all spam complaints involving the same IP address.

1. Verify that the complaint involves a WiredTree IP address
    a. Each spam complaint should include headers of the offending spam message. Within the headers, look for our IP addresses and ensure that the spam was sent. For example:

```
Received: from [208.79.236.104] by usgo.net
          (USFamily MTA
v5/:PGdhcnlAZmFpdGhtYWRlc2ltcGxlLmNvbT48c2pzYW52aWtAdXNmYW1pbHkubmV0Pg--)
          with SMTP id <20140827051128100683500013> for
<sjsanvik@usfamily.net>;
          Wed, 27 Aug 2014 05:11:28 -0500 (CDT)
          (envelope-from gary@faithmadesimple.com, notifiable emailnetwork
208.79.236.)
Received: from [217.118.79.29] (port=34976 helo=faithmadesimple.com)
 by shepherd.flockhosting.com with esmtpa (Exim 4.82)
 (envelope-from <gary@faithmadesimple.com>)
 id 1XMaCJ-0006ol-Kx
 for sjsanvik@usfamily.net; Wed, 27 Aug 2014 03:11:25 -0700
```

    In this case, look at the "Received:" lines. The first line says: "Received: from 208.79.236.104", so this is the IP address that sent the spam to this user. As this is one of our IP addresses, the spam originated from a server on our network.

2. Look up the spamming server's hostname
    a. Telnet to the IP address on port 25. The hostname will be in the first line of the server response: "220-mail.wiredtree.com ESMTP Exim 4.82 #2 Fri, 29 Aug 2014 18:52:03 -0500"
    b. Search for the IP address in IPPlan

3. Once you have obtained the server's hostname, look up the hostname in Ubersmith to obtain their contact email address and server access information.

4. Log in to the server and attempt to locate the spamming account
    a. **Searching mail currently in the queue**
    The following will show you the location of any PHP script that has sent email through the server using the PHP mail() function:

```
exim -bpru | awk '$3 != "" {print $3}' | while read a; do exim -Mvh ${a} |
grep -E "X-PHP-Script"; done;
```

    b. **Searching email logs**
    The following script will count how many emails were sent from each directory in /home/. If you see a directory where scripts have sent large number of emails, you will likely find the spamming PHP script within that directory:

```
zgrep "cwd=/home/" /var/log/exim_mainlog* |awk '{print $3}' | cut -d'=' -f2
|sort |uniq -c | sort -n
```

    The following script will count the number of times an email address has logged on to Exim to send an email. Often, a high number of logons will indicate that the email address has been compromised:

```
zgrep "A=dovecot_login:" /var/log/exim_mainlog* | awk -F 'A=dovecot_login:'
'{print $2}' | awk '{print $1}' | sort | uniq -c | sort -nr | head
```

c. **Other tools that may help in identifying which account is spamming on the server**
The following will count the number of emails sent by a user account

```
for i in `ls /var/cpanel/users`; do printf "$i\t";  grep "U=$i"
/var/log/exim_mainlog |wc -l; done | sort -nrk2 | head
```

d. **Use this if you need to clean up a mail queue on a customer's server**

Clear Mail Queue

```
exim -bp | exiqgrep -i | xargs exim -Mrm
```

5. Take action on the spamming script/email account
    a. If you have located the offending script that is sending out email, restrict access to it by using chmod to set the permissions to 000
    b. If you are unable to locate the offending script but have located the offending cPanel account, suspend the account if it is still aggressively spamming.
    c. If an email account has been compromised, you'll want to change the password for this account immediately in cPanel -> Mail -> Email Accounts. Note the new password that you have used.

6. Open a new Abuse ticket with the customer, setting it up as follows:
    a. **From**: abuse@wiredtree.com
    b. **Subject**: *HOSTNAME* -- Spam
    c. **User E-mail Address:** Obtain from Ubersmith
    d. **Status:** In Progress
    e. **Contents:** *Predefined Replies -> Abuse -> Spam -> Spam First Contact - Compromised Scripts* or *Spam First Contact - Compromised Email* depending on the information you discovered. Replace the placeholders with the relevant information you obtained in step 4.

7. After you send the ticket to the customer, make a ticket note including the link to the original spam complaint ticket. Send a response to the spam complaint indicating that we are aware of the issue and are working to correct it immediately.

8. You may start a courtesy clamscan of the server and provide them with the results:

```
bash <(curl http://files.wiredtree.com/misc/clamscan.sh)
```

9. Continue to follow-up with the customer on a consistent basis to ensure the issue is resolved.

10. If the customer does not respond and they are still spamming, you can begin suspending accounts if they have not responded after 2 days. If they unsuspend any of the spamming accounts without sending us a response, you may change their root password so that they are unable to unsuspend the accounts.