SECURITY UPDATE

Updated 10:07am PST Sept 22nd 2020

On September 16th at approximately 10am PST, one of Softree staff's computer became infected with an aggressive malware, specifically a trojan named *Wacatac.G! ml*.

Through this legitimate emails sent from cspeirs@softree.com and support@softree.com are being modified and re-sent to the original recipients. These emails can appear to come from any of the recipients included the original email chain.

The bogus emails are fairly easy to spot - **return email does not match the sender's name.** This can be particularly hard to identify when accessing email over a cell phone. If you receive one of these scam emails, please just delete them (and, obviously, don't open the attachments or follow the links).

We **have** eliminated the threat and taken aggressive actions internally to handle and prevent any future threats; however, the email chains that were compromised will likely be used by the hackers for a period of time.

Unfortunately, this scheme is extremely well thought out and sophisticated. They are using thousands of legitimate email servers from around the world, making documenting and blacklisting individual servers too challenging, and the higher quality servers allow many of these phishing emails to bypass traditional spam filters.

EMAIL FILTER RECOMMENDATIONS:

Softree has officially **retired** the following emails addresses and recommends using them as filters in the body of inbound emails:

amoon@softree.com
cspeirs@softree.com
dmills@softree.com
emmanuel@softree.com
ewasney@softree.com
fnayyer@softree.com
hbotero@softree.com
jrimac@softree.com
latinamerica@softree.com
matt@softree.com
Mchin@softree.com
ssachdeva@softree.com
sserrano@softree.com
support@softree.com

UPDATING SPAM FILTER RECOMMENDATIONS:

We (internally) have also found success with adjusting a few spam filtering values, including **MIME_BOUND_DD_DIGITS**, **BAYES_40**, **BAYES_50, BAYES_60**. These might be applicable to your team, depending on your email configuration.

Finally, the following NEW email addresses have been created to replace compromised accounts. Please contact us to update your address books!

**FYI - we will be monitoring the old accounts; this just helps with an easy filtering option.*

Please let us know if you (*or your IT dept*) have any questions or concerns. If the phishing emails continue to persist, please check back to our support.softree.com homepage for updates to this message and the suggested filtering rules.

Contact from Softree:

Erin Wasney
1-604-519-6222 ext 104