INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

ATTACK OF THE TROJANS, BOTS & ZOMBIES

Once of the most common questions we are asked by users is: How do these spammers get my e-mail address? Previously we looked at Rumpelstiltskin attacks and this week we will focus on the second of the methods - by using Trojan Horses, Bots and Zombies. Now, thet may sound like something from a movie, but they do pose quite a serious threat to you as e-mail user.

Let us use a familiar example. You regularly exchange emails with your elderly mother who has a computer. Your mother uses Outlook or Thunderbird and has dozens of emails from you in her inbox. She even added you to her address book. She also has lots of emails from a distant family member – cousin Johan from Australia. You haven't stayed in touch with Johan that closely over the years, but you definitely know who he is.

Last year, just before the Christmas, Johan downloaded and installed this really pretty Christmas screensaver that showed tranquil tree and candle scenes when he wasn't using the computer. What he didn't know was that the screen saver had a sinister hidden payload. While the candles flickered peacefully on his screen, the software went to work combing through his emails and address book, his browser's cache of past webmail sessions and other files, storing every email address it would find in a separate list.

Then it sent the entire list to a server in Russia, where a criminal combined it with other such submissions to build the ultimate monster spam list that can be sold and resold over and over again.

But as if that wasn't enough, when the "screensaver" sent the address list to Russia, it received some content in return – messages to be sent to all of Johan's contacts. Then, unbeknownst to John, his computer started creating hundreds of emails randomly using the harvested email addresses in the To: and From: field along with the content from the Russian server and sent them out using Johan's Internet connection. One of them used your mother's email address as sender and yours as recipient.

Now you received some spam from your mother asking you to buy fake watches and you're ready to speak to her telling her to stop. Well, don't. Your mother has obviously nothing to do with the whole thing and you'll never find out that it was actually Johan's computer.

*You just had a look into the really nasty underworld of the Internet where **botmasters** (the guy in Russia) control **botnets** (infected computers that all report to the same server) of remote-controlled **zombies** (Johan's computer) that were compromised using **trojan horses** (the screensaver) or similar **malware**.*

And it doesn't even end there. The botmaster typically doesn't spam for his own account but hires out his botnet to whoever pays the most. The equally shady factory in China wanting to sell more fake Rolexes can now hire the botmaster to blast their offers all over the internet. The guy in Russia doesn't even care if you open or click on that email from your mother, he gets paid either way. And when he's done with the watches, he'll inform his entire mailing list that they all won the lottery and can pick up the prize if only they pay a small "transfer fee" up front. And after that, he'll mail a Paypal phish for yet another "client". And for good measure, he'll sell his entire email address database, incl. yours, to a friend who is in the same line of "business".

*In other words, once your email address got picked up by a **botnet**, Pandora's Box is wide open. The whole scheme is particularly wicked because now you have to depend on others to keep your address safe. Unfortunately, there is little you can do:*

- *First of all, do your own share: **NEVER open email attachments** that you didn't ask for, even if they appear to come from good friends like Johan. If you're still curious, ask Johan or your mother first if they really sent it.*

- ***NEVER download anything*** *where you can't in-de-pend-ent-ly verify it's safe. With"independently verify" I mean you can read about it in forums, blogs, news sites, your local "computer geek" etc. Facebook fan pages, even with 1000s of "fans", do NOT count, they are way too easy to manipulate and are usually full of misinformation!*
- ***NEVER get fooled by fake "security scans"*** *(they're quite the opposite!) or"video codec updates" to see that funny kitten clip. If you think you need a new Flash player, type in flash.com by hand and update from there. If afterwards the site still says you need an "update" get out of there as fast as you can.*
- *Then* ***educate your friends and family*** *about the same. Explain how trojans work. Send them a link to this blog page!*
- *You can try having* ***multiple private email addresses****. Keep a super-private one, only for family and very few of your closest friends. Use your university address for everyone you work with and don't use this for private mail – EVER! Get a semi-private one for your wider social circle. The latter two do get some spam, although it's still manageable. GMail has a very good "spam filter", and blacklisting spammers is very easy!*

[ARTICLE BY DAVID WILES & MATERIAL BY BustSpammers.com]

Posted in:E-mail,Security | Tagged:Bank Emails,Bots,Malware,Trojan,Zombies | With 1 comments