

Forum:[Hack Forums](#)

Thread: [Spam email spreads "HeartBleed Bug Remover Tool", a keylogger](#)

Aura - May 28, 2014, 3:28 pm

Hey guys, Aura here with yet another malware warning for you.

Everyone knows the OpenSSL Heartbleed vulnerability that affected most websites on the web (if not, you can read all about this vulnerability [here](#)). Well, some spreaders are now "exploiting" that vulnerability in order to infect people with a keylogger. Symantec researchers discovered a spam campaign that sends email containing a message asking the user to download the "HeartBleed Bug Remover Tool" in order to see if his system was infected with HeartBleed and to remove it. Only problem is that, HeartBleed was a web-based vulnerability, how could it affect a whole system at a file level ? It didn't, it's a trap. The email impersonate an apparently popular password management company and ask the user to download their tool to remove the HeartBleed Bug from the user's system, even if it's not present and NEVER will. The attachment is seen as a doc/docx file but once is in-fact an encrypted .zip file that will extract an .exe and that if executed, will infect the system with a keylogger malware. When it's execute, a simple window will appear with a progress bar saying that the "tool" is looking for the HeartBleed Bug and then will end up in saying that it wasn't found and that the system is safe. Luckily for us, the scam is pretty obvious. The email is written in a pretty poor English (poor grammar) and so is the writing on the "HeartBleed Bug Remover Tool".

So if you ever come across this email (or any email that looks like it), quickly block the sender's email address, delete that email and move.

Read the full article here : [Beware Of Fake "HeartBleed Bug Remover Tool", Hijacks System with Malware](#)

I hope that you guys start enjoying these little threads. I'm doing my best to vulgarize the article as much as possible so everyone can easily understand it.

Once again, stay safe and secure my friends.