# Do NOT Open Herbalife Email

A new ransomware attack has been detected and it's spreading quickly around the world with a rate of 2 million attacks per hour. It's likely higher.

According to an analysis from Barracuda Networks, the massive attack is launching around 8,000 different versions of the virus script. This makes it very difficult to put a stop to the attack.

The attacks seem to have originated in Vietnam, but some are coming from a multitude of other countries including India, Colombia, Turkey, and Greece. As the attacks spread, computers in more countries will be part of the hack.

"What's remarkable about this one is just the sheer volume of it," said Barracuda's Eugene Weiss.

Right now, the attack is still spreading rapidly, and as evidenced by the WannaCry ransomware attacks of this year, its effects can be devastating. That's why we wanted to alert you of this attack as soon as we became aware it.

## What to look out for

Initial reports indicate that the conduit for this ransomware attack appears to be an email. Be on the look out for any email with a subject of "Herbalife" or a "copier" file.

There could also be variants of the email subjects as the attacks spread so be on alert. One wrong click of a link in the email and all your files are overtaken by ransomware.

However, since this attack is still evolving as we speak, please look out for phishing and suspicious emails in general.

## Here are the other latest facts about this new attack:

- The attackers seem to be using a kit that automates the ransomware's variations, resulting in 8,000 variants so far.
- The attackers are using proven social engineering and psychological tactics to get the victims to click on the malicious link.
- The targets appear to be email addresses belonging to business and institutional companies in the U.S. or Canada.
- The attack doesn't appear to be state-sponsored since it has a financial motive. When your files are locked, you'll need to pay but there's a gotcha here...
- **Important:** Victims who pay the ransom have not received the decryption tool so far.

Since this is still a developing attack, the full impact of this new ransomware campaign is not known yet. Details and its vector may evolve so please remain vigilant.

## Your backup is critical

Are you protected from this and the next massive ransomware attack? Cybercriminals are always developing more complicated variants that make it harder for anti-malware software to detect.

That's why you need to backup all of your critical data.