BEWARE OF “CRITICAL UPDATE” EMAIL FROM “MICROSOFT”

A new (November 22) malware campaign is under way and emails sent from a fake Microsoft address are pushing people to download a malicious Windows 10 “critical update”.

The subject of the mail says “Install Latest Microsoft Update now!” or “Critical Microsoft Windows Update!”

The mail contains one single line that says “Please install the latest critical update from Microsoft attached to this mail” and an attached file.

If you receive such an email, **delete the email right away. Period**.

Here’s how this malware works

The mail contains a graphics (jpg) file that is actually not a picture but an executable .NET file that will infect your PC.

This executable will download a program called “bitcoingenerator.exe” which comes from misterbtc2020 — a GitHub account. But this bitcoin generator doesn’t generate any virtual riches: it’s a ransomware called Cyborg.

Cyborg will encrypt all your files, locking their contents and changing their extensions to 777. You will also find a text file on your desktop named “Cyborg_DECRYPT.txt”, containing instructions about how to recover your life — for a price.

According to security company Trustwave, there are four variants of this malicious software.

Trustwave says this is a real danger to businesses and individuals alike, with the capacity to be attached to other emails and evade any gateway controls.

With that in mind, it’s good to remember to always distrust any mails you get, even if you think they come from a trustworthy source, and never blindingly click on something you didn’t ask for — even if you have the best antivirus software installed.