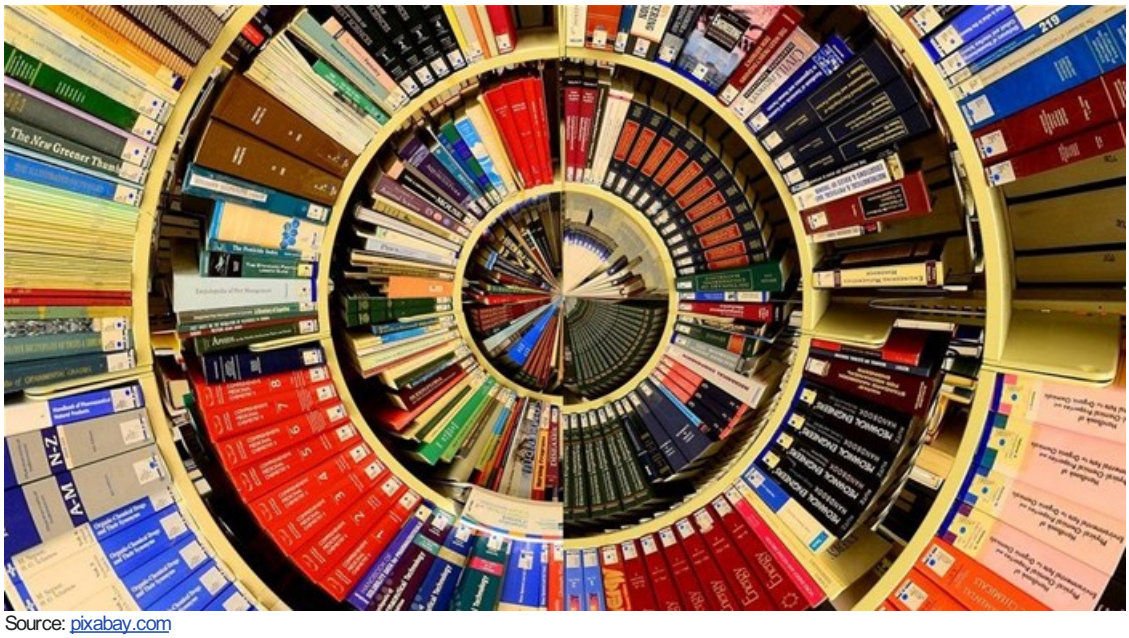
Beware of malware disguised in textbook and student essays

Kaspersky experts have uncovered 53,531 malicious or potentially unwanted files disguised as ready-to-use essays and textbooks for schools and universities. From August 2018 to July 2019 they were used in 356,662 attacks on 104,819 users - a 21% decrease, compared to the figures from the previous year. These are among the main findings of Kaspersky's 'Back to School report'.



Source: pixabay.com

While some might find the cost of student books to be quite expensive, they are an inevitable part of any educational programme. As a result, many textbooks can be found online, and students might avoid the high costs by downloading them from pirate websites or file hosting forums, along with student essays.

Threat actors, however, are willing to create mischief and use students' hunger for knowledge and academic success as an opportunity to distribute malware.

Overall, there were 17,755 threats disguised as student books, and most often, these were falsely circulated English (2,080), math (1,213) and literature (870) textbooks. The vast majority of threats hiding under these disguises were downloaders of various files: from annoying, yet not fatal adware or unrequested software, to highly dangerous money-stealing malware.

The remaining 35,776 threats were disguised as essays and student papers on various topics. As researchers were taking a closer look at them, they noticed something unusual.

In 35.5% of cases, the most popular malware was an eight-year-old worm – an outdated type of threat that is not often seen in use nowadays. It was actively distributed through a specific attack vector - USB-sticks. Upon closer examination, the experts came to the conclusion that the worm 'lives' on computers at student printing services, that are often used for years without regular security updates and run old versions of operations, getting there through what seems to be a student essay that needs to be printed.

"Students attempting to avoid paying for textbooks and other educational materials creates an opportunity for cybercriminals that they simply cannot resist. This turns into are a serious problem for educational entities, as once the infection gets on a school network computer, it can easily spread. Not all schools are prepared to carry out effective incident response, as educational organisations are considered to be an a-typical target for fraudsters, but threat actors use every opportunity they can get. This is why precautionary measures are vital for such organisations," said Maria Fedorova, security researcher at Kaspersky.

Safety tips

To not fall victim to malware, students are advised to:

- Not open email attachments that seem suspicious, or from someone you do not know
- Only search for books you need offline or in trusted online libraries
- Pay attention to the downloaded file's extension. If you are going to download academic books, the file should not end in the extension .exe
- Pay attention to the person who lends or gives you a USB drive with work to share. Do not take USB drives from anyone you don't know
- Start using a reliable security solution like Kaspersky Internet Security. Configure it to automatically scan every time an external drive or USB drive is connected to your PC

Kaspersky advises universities and schools to do the following:

- Use an up-to-date version of the machine's Operating System (OS)
- Do not neglect to use a dedicated cybersecurity product for organisations such as Kaspersky Endpoint Security for Business