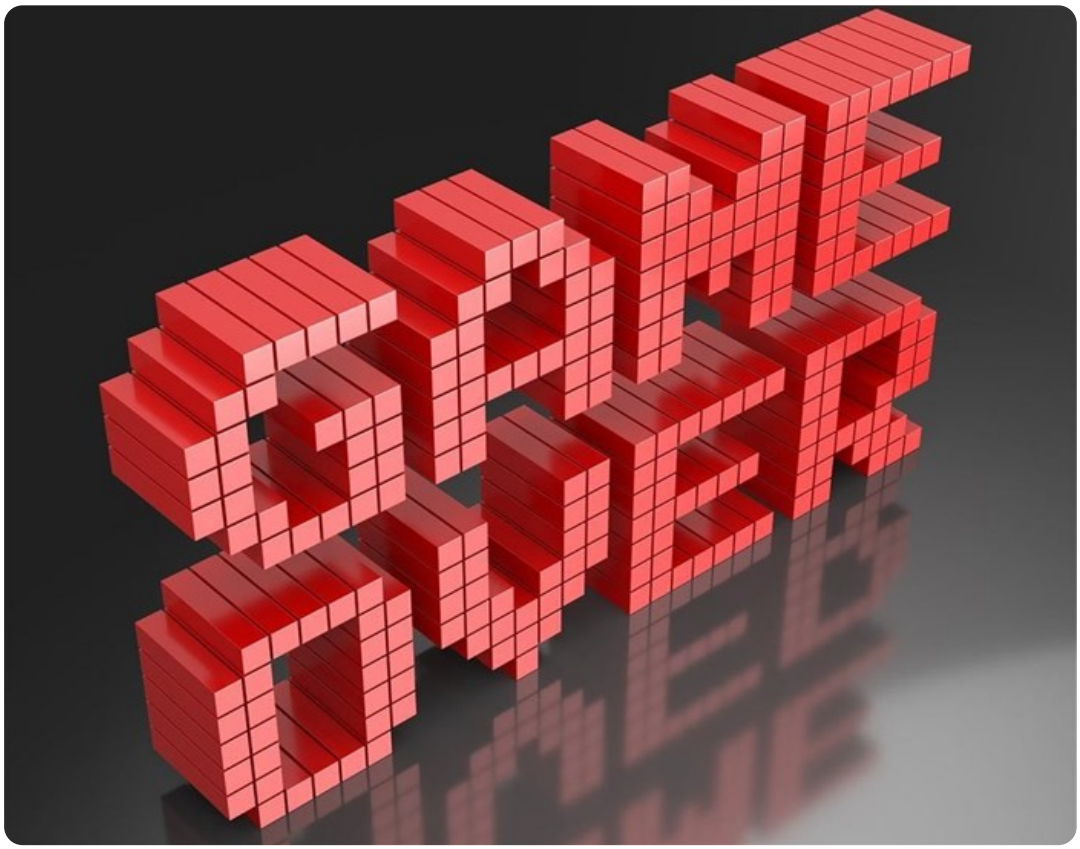
bizcommunity

# Over 900,000 users affected by fake video games spreading malware

Cyber criminals are taking advantage of the growing demand for video games by distributing malware through fake copies of the most popular ones, research by Kaspersky has found.



Source: pixabay.com

More than 930,000 users were hit by such attacks in the 12 months from early June 2018 to early June 2019. Over a third of the attacks centered on just three games.

Video gaming has been around for a while, but the power of the internet has accelerated its growth and evolution. Today around one in ten of the world's population plays online games. Like other types of digital entertainment, video games are vulnerable to abuse such as copyright infringement and illegal torrent-trackers, but they face another growing threat: the fraudulent use of their brand to disguise the distribution malware. Many of the top video games are hosted on digital distribution platforms. These cannot always detect whether the software files uploaded are legitimate gaming files or disguised malware samples.

Kaspersky researchers decided to take a closer look at the infected files detected during 2018 and the fir part of 2019. Leading the list of abused games was 'Minecraft'. Malware disguised as this game accounte for around 30% of attacks, with over 310,000 users hit. In second place was 'GTA 5', targeting more than 112,000 users. 'Sims 4' took fourth place with almost 105,000 users hit.

According to the researchers, criminals were also found trying to lure users into downloading malicious file pretending to be unreleased games. Spoofs of at least 10 pre-release games were seen, with 80% of detections focused on FIFA 20, Borderlands 3, and the Elder Scrolls 6.

“For months now we see that criminals are exploiting entertainment to catch users by surprise – be it serie of popular TV shows, premieres of top movies or popular video games. This is easy to explain – people c be less vigilant when they just want to relax and have fun. If they’re not expecting to find malware in something fun, they’ve used for years, it won’t take an advanced threat like infection vector to succeed. W urge everyone to stay alert, avoid untrusted digital platforms and suspicious looking offers, install security software and perform a regular security scan of all devices used for gaming,” said Maria Fedorova, securi researcher at Kaspersky.

To avoid falling victim to malicious programs pretending to be video games, Kaspersky Lab recommends taking the following steps:

- Use only legitimate services with a proven reputation.
- Pay extra attention to the websites’ authenticity. Do not visit websites allowing downloading video games until you are sure that they are legitimate and start with ‘https’. Confirm that the website is genuine by double-checking the format of the URL or the spelling of the company name, before starti downloads.
- Don’t click on suspicious links, such as those promising a chance to play a pre-release game.
- Use reliable security solution for comprehensive protection from a wide range of threats.