

kaspersky

A Far Cry from safety: Video-gaming threats Flash Report

Maria Fedorova, Lead Malware Analyst
Tatyana Sidorina, Senior Web Content Analyst

13.06.2019

Kaspersky Flash Report

Gamers a top target for summer scammers and malware

Kaspersky researchers reviewing cyber threats facing video gamers have found that starting from around May and continuing into the fall, there is a surge in phishing scams targeting gamers through the leading gaming platforms.

The researchers also found that as with other forms of digital entertainment, malware distributors are exploiting popular and not-yet-released versions of video games to spread malicious code.

Phishing on the rise

The phishing attacks targeting gamers tend to focus on the main publishing brands or hosting platforms that users need to sign into for authentication and more. A review of phishing attacks spoofing the brands of EA Origin, Blizzard Battle.net and Steam revealed that attacks soared in the first six months of 2019 compared to the previous six months. The data for 2018 also showed that the months of May to July were particularly popular for attacks.

In the case of EA (Electronic Arts), the company behind games such as Anthem, Apex Legends and FIFA, the peak number of daily attacks on users increased by around a third from one year to the next. The majority of attacks on users in 2018 came in at under 500 a day. This ended on November 16, after which daily numbers regularly came in at over 1,500 and 2,000.

Steam, estimated to be the largest digital game distribution platform, was not surprisingly the disguise of choice for many fraudsters, with attacks on users regularly exceeding 1,000 a day during the second half of 2018 and then rising to a steady 2,000 plus into 2019. The greatest daily number of users hit in 2019 to date is 6,383 – compared to a peak of 4,175 in 2018.

Malware on the menu

In a review of the most popular video games, our researchers discovered that between early June 2018 and early June 2019, 932,464 users were hit by attacks designed to distribute malware.

Leading the list of abused games was 'Minecraft'. Malware disguised as this game accounted 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.

For those gamers unable to resist the temptation to get their hands on a new edition of a game that has not yet been officially released, the penalty for doing could be quick and unexpected. Our researchers discovered malware lurking behind spoofs of at least 10 pre-release games, with 80% of detections focused on FIFA 20, Borderlands 3, and the Elder Scrolls 6.



Stay safe to play safe

Video gaming is a thriving industry enjoyed by many millions of people the world over. To avoid being scammed or infected, there are a few things you can do to keep yourself and your virtual worlds safe:

- 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 starting downloads.
- Don't click on suspicious links, such as those promising a chance to play a pre-release game.
- Use a reliable security solution for comprehensive protection from a wide range of threats, such as [Kaspersky Security Cloud](#).



www.kaspersky.com/
www.securelist.com

© 2019 AO Kaspersky Lab.
All rights reserved. Registered trademarks and service marks are the property of their respective owners.