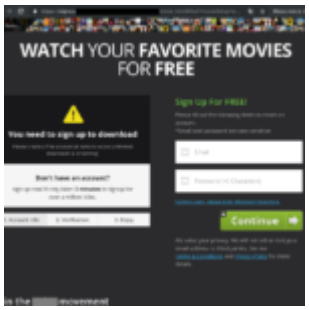
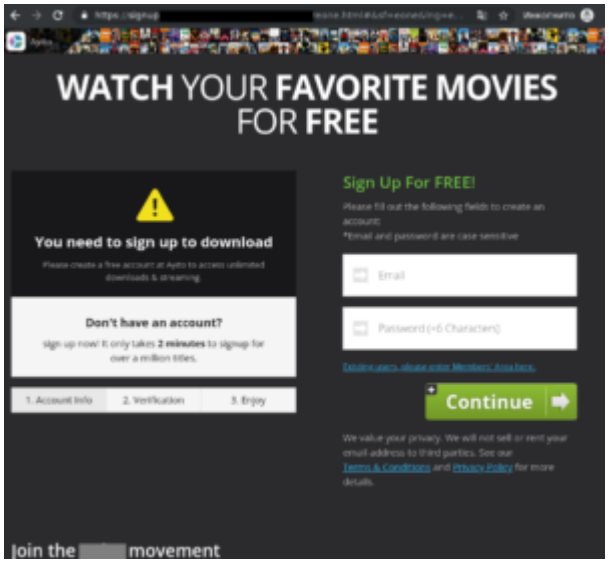
Kaspersky found over 20 phishing websites offering Oscars movies





Popular films gain the attention of cybercriminals, no less than movie fans, with the Oscars in the calendar only upping the stakes. To better understand how cybercriminals try to capitalize on our interest in high-profile movies, Kaspersky researchers looked into the prevalence of such scams. With over 20 phishing websites and 925 malicious files detected under the guise of this year's nominated films, the findings show that those who are looking for a nice evening in front of the screen watching the latest blockbuster, need to stay on the lookout for much more action, in the form of phishing and malware.

Kaspersky found over 20 phishing websites and Twitter accounts offering users the chance to watch nominated films for free. These phishing websites gather users' data and prompt them to carry out a variety of tasks in order to gain access to the desired film. These can vary from taking a survey and sharing personal details, to installing adware or even giving up credit card details. Needless to say, that at the end of the process, the user does not get the content.

The Best Picture nominees
1 1917
2 Ford v Ferarri
3 Jojo Rabbit
4 Joker
5 Little Women
6 Marriage story
7 Once upon a time in Hollywood
8 Parasite

9 The Irishman

To further support the promotion of fraudulent websites, cybercriminals also set up Twitter accounts, where they distribute links to the content. Coupled with malicious files spread via different channels, this brings them successful results.

Malicious files spread on the internet under the guise of copies of nominated films also provide an indication of the levels of interest towards the nominees. Kaspersky researchers compared malicious activity under the name of nominated films during the first four weeks after the public premiere of the film. As a result, 'Joker' took first place among films used – being the most popular film among cybercriminals with 304 malicious files named after the Gotham villain. '1917' was second in this rating with 215 malicious files, The Irishman, third with 179 files. Korean film 'Parasite' did not have any malicious activity associated with it.

The number of malicious files detected by Kaspersky products under the guise of nominated films Kaspersky also looked into whether there was a significant rise in malicious files just after the public release of the film. This showed that most malicious files appeared during the third or fourth week after the public cinema release of the film, although some were distributed even before the premiere.

Kaspersky experts also analyzed whether the availability of a film on a streaming platform influences the likelihood of users searching for an illegal copy of it on the web, by comparing malicious activity after the initial limited cinema release and actual release on Netflix streaming platform.

In the case of 'Marriage Story' no malware was found upon and after the initial release of the film in cinemas. However, cybercriminals started using the movie title after its release on Netflix, reflecting the interest that grew towards the film. In the case of Sorrento's long-awaited 'The Irishmen', even though less users were engaged in finding a copy of the movie on the internet, they were more determined to do so – the number of detections following the initial limited release of the film on screen was higher than after its release on Netflix.

"Cybercriminals aren't exactly tied to the dates of film premieres, as they are not really distributing any content except for malicious data. However, as they always prey on something when it becomes a hot trend, they depend on users' demand and actual file availability. To avoid being tricked by criminals, stick to legal streaming platforms and subscriptions to ensure you can enjoy a nice evening in front of the TV without having to worry about any threats," comments Anton Ivanov, Kaspersky malware analyst.

To avoid falling victim to malicious programs pretending to be popular films or TV shows, Kaspersky recommends taking the following steps:

• Pay attention to the official movie release dates in theaters, on streaming services, TV, DVD, or other sources
• Don't click on suspicious links, such as those promising an early view of a new film; check movie release dates in the cinema and keep track of them
• Look at the downloaded file extension. Even if you are going to download a video file from a source you consider trusted and legitimate, the file should have an .avi, .mkv or .mp4 extension among other video formats, definitely not .exe
• Check the website's authenticity. Do not visit websites allowing you to watch a movie 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, reading reviews about it and checking the domain's registration data before starting downloads

• Use a reliable security solution, such as Kaspersky Security Cloud, for comprehensive protection from a wide range of threats