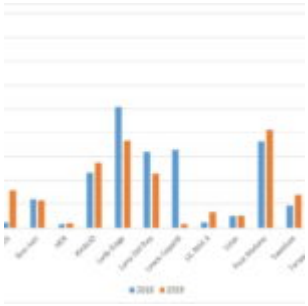
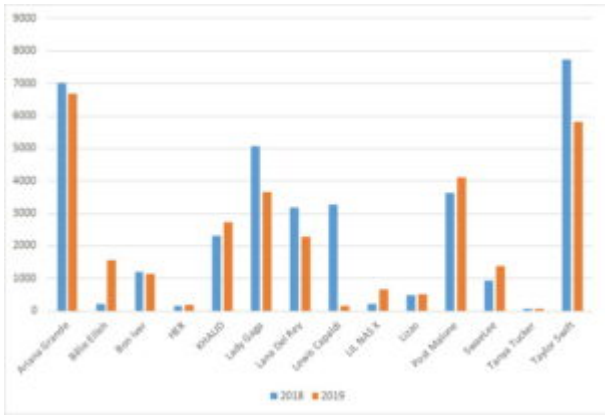
Kaspersky found malware hiding behind top music award nominees





Cybercriminals are actively abusing the names of artists and songs nominated for a Grammy 2020 award, in order to spread malware. Kaspersky protection technologies detected a 39% rise in attacks (attempts to download or run malicious files) under the guise of nominees' work in 2019, compared to 2018. Ariana Grande, Taylor Swift and Post Malone were attackers' favorites, with these nominees' names used most often in 2019 as a disguise for malware.

Music has universal appeal – it is not just entertainment, but a form of therapy and education, as well as providing an atmosphere and message platform. Its popularity and widespread availability is the reason why, even in the age of streaming services, music is not free from malicious activity: criminals use popular artists' names to spread malware hidden in music tracks or video clips.

In light of the biggest music awards of the year, to show the extent of the problem, Kaspersky researchers analyzed Grammy 2020 nominated artists' names and song titles for malware . As a result, Kaspersky found 30,982 malicious files that used the names of artists or their tracks in order to spread malware, with 41,096 Kaspersky product users having encountered them.

Analysis of the nominated artists showed that the names of Ariana Grande, Taylor Swift and Post Malone were used most to disguise malicious files, with over half (55%) of detected malicious files named after them.

The number of attempts to download or run the files containing names of these pop stars also grew significantly for almost all artists in the research.

The connection between the rise in popularity and malicious activity is very evident in the case of newer artists such as Billie Eilish. The teenage singer became hugely popular in 2019, and the number of users who downloaded malicious files with her name has risen almost tenfold compared to 2018 – from 254 to 2171, the number of unique distributed malicious files – from 221 to 1,556.

However, while nomination for a prestigious award and recognition connected to it affects users' interest in specific artists and, as a result, a growth in malicious activity, this is not necessarily the case for more established artists such as Lady Gaga, whose name use also experienced a rise in attacks in the past year.

Kaspersky also analyzed which records and songs, nominated for a Grammy in 2019, received most attention from cybercriminals. Post Malone's 'Sunflower', Khalid's 'Talk' and Lil Nas X's 'Old Town Road', led the way for songs with the most malware attacks.

"Cybercriminals understand what is popular and always strive to capitalize on that. Music, alongside TV shows, is one of the most popular types of entertainment and, as a result, an attractive means to spread malware, which criminals readily use. However, as we see more and more users subscribe to streaming platforms, which do not require file download in order to listen to music, we expect that malicious activity related to this type of content will decrease," – comments Anton Ivanov, Kaspersky security analyst.
To avoid falling victim to malicious programs pretending to be popular music files, Kaspersky recommends taking the following steps:

• If you want to listen or download famous artists' songs, use reputable services like Apple Music, Spotify Premium, and Amazon Music. Or try to find a recognized free music site that allows you to download songs legally.
• Try to avoid suspicious links, promising exclusive music content. Check musicians' official social media accounts or read reputable music blogs like Pitchfork, to make sure that such content exists.
• Look at the downloaded file extension. Even if you are going to download an audio or video file from a source you consider trusted and legitimate, the file should have an mp3, .avi, .mkv or .mp4 extension among other music and video formats, definitely not .exe or .lnk.
• Use a reliable security solution, such as Kaspersky Security Cloud, for comprehensive protection from a wide range of threats.