Reader code names famous games to infiltrate Microsoft Store

A malicious code called Electron Bot has infiltrated Microsoft's official app store, Microsoft Store.

A malicious code called Electron Bot has infiltrated Microsoft's official app store, Microsoft Store. It does this by faking popular titles like Subway Surfer and Temple Run. Currently, it has infiltrated more than 5,000 computers in countries such as Sweden, Israel, Spain and Bermuda.

Electron Bot was discovered by network intelligence analysis firm Check Point. It will provide a backdoor that gives its owner complete control over compromised machines, support for remote code execution, and real-time interaction.

The hacker's goal is to take over social media accounts such as Facebook, Google, YouTube and Sound Cloud to serve dirty SEO campaigns or click on ads and likes to generate illicit revenue.

Three years of evolution

Electron Bot is not a recent arrival. The first operation of this malicious code took place in late 2018. At that time the first version of Electron Bot was posted to the Microsoft Store as an "Album by Google Photos" application by the fake Google LLC entity.

Since then, the people behind this malicious code have updated a number of new features and tools. In addition, advanced detection avoidance such as dynamic script loading is also added.

Electron Bot is written in Electron language and it can simulate natural web browsing behavior as well as perform actions like a normal person browsing the web.

To do this, it will open a new hidden browser window using Chromium engine in Electron framework, set appropriate HTTP headers, display requested HTML page and finally perform mouse movement, scrolling , click and enter the keyboard.

According to an analysis by researchers at Check Point, the main goals of Electron Bot in the ongoing campaign are:

1. SEO poisoning - Creates a malware distribution site that ranks high in Google's search results list.
2. Click ads - Connect to websites in the background and click on non-viewable ads.
3. Social Media Account Promotion - Drive traffic to specific content on social networks.
4. Advertise products online - Increase your store's rating by clicking on its ads.

These functions are provided as a service to those who want to illegally increase their online revenue.

Games containing malicious code still work normally so that the victim does not have any suspicion. Meanwhile, all harmful activities will take place in the background. This leads to users still having positive reviews for those games on the Microsoft Store.

Of course, hackers will constantly refresh their scams and use different games and apps to spread malware.

For now, users should pay attention to the publishers that have been identified as distributing malicious applications below:

1. Lupy games
2. Crazy 4 games
3. Jeuxjeuxkeux games
4. Akshi games
5. Goo Games
6. Bizzon Case

Although Electron Bot does not cause serious damage to infected machines for now, there is no guarantee of this in the future. Hackers can easily modify the code so that Electron Bot downloads and installs RAT or even ransomware onto the victim's machine.