Malware infiltrates Microsoft Store via clones of popular games

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

February 24, 2022 09:34 AM 1

A malware named Electron Bot has found its way into Microsoft's Official Store through clones of popular games such as Subway Surfer and Temple Run, leading to the infection of roughly 5,000 computers in Sweden, Israel, Spain, and Bermuda.

The malware, spotted and analyzed by cyber-intelligence firm Check Point, is a backdoor that gives the adversaries complete control over compromised machines, supporting remote command execution and real-time interactions.

The goal of the threat actors is social media promotion and click fraud, which they achieve by controlling social media accounts on Facebook, Google, YouTube, and Sound Cloud, as Electron Bot supports new account registration, commenting, and liking on these platforms.

Three years of evolution

The operation was first discovered at the end of 2018 when an early Electron Bot variant was submitted to the Microsoft Store as “Album by Google Photos,” published by a spoofed Google LLC entity.

Since then, the malware authors have added several new features to their tool and advanced detection evasion capabilities like dynamic script loading.

The malware is written in Electron, hence the name, and it can emulate natural browsing behavior and perform actions as if it’s a real website visitor.

For this, it opens a new hidden browser window using the Chromium engine in the Electron framework, sets the appropriate HTTP headers, renders the requested HTML page, and finally performs mouse movement, scrolling, clicks, and keyboard typing.

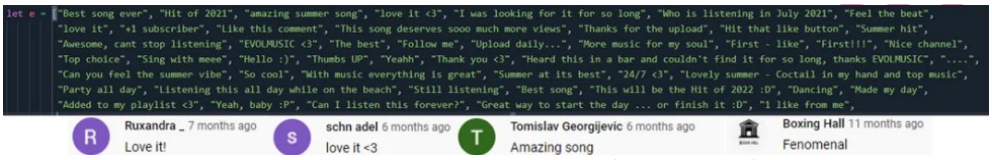
```
264  let humanMouseMove = async function(e, n = 40, o = 20, t = 50) {
265      e = e || {
266          x: randomGenerator(0, window.innerWidth),
267          y: randomGenerator(220, window.innerHeight)
```

Human mouse movement emulation *(Check Point)*

Electron Bot's primary goals in the ongoing campaign analyzed by the Check Point researchers are:

- SEO poisoning – Create malware-dropping sites that rank high on Google Search results.
- Ad clicking – Connect to remote sites in the background and click on non-viewable advertisements.

- Social media account promotion – Direct traffic to specific content on social media platforms.
- Online product promotion – Increase store rating by clicking on its advertisements.



Hardcoded YouTube comments *(Check Point)*

These functions are offered as services to those who want to increase their online profits illegitimately, so the gains for the malware operators are indirect.

As for attribution, Check Point reports (https://research.checkpoint.com/2022/new-malware-capable-of-controlling-social-media-accounts-infects-5000-machines-and-is-actively-being-distributed-via-gaming-applications-on-microsofts-official-store/) finding evidence pointing to the actors being based in Bulgaria, but besides that, nothing is known about the malicious actors' identity or location.

Infection chain

The infection chain begins with the victim installing one of the laced apps from within the Microsoft Store, an otherwise trustworthy source of software.

Electron Bot infection chain *(Check Point)*

Upon launching the application, a JavaScript dropper is loaded dynamically in the background to fetch the Electron Bot payload and install it.

The malware launches at the next system startup, connects to the C2 (*Electron Bot[.]s3[.]eu-central-1[.]amazonaws.com* or *11k[.]online*), retrieves its configuration, and executes any commands in the pipeline.

Because the main scripts are loaded dynamically at run time, the JS files dropped on the machine's memory are very small and seemingly innocuous.

Commands supported by Electron Bot *(Check Point)*

More than just a game

All laced games identified by Check Point featured the expected functionality while the malicious operations unfolded in the background.

This results in having positive user reviews on the Microsoft Store. For instance, Temple Endless Runner 2, which was published on September 6, 2021, has close to a perfect five-star rating from 92 reviews.

Of course, the crooks constantly refresh their lures and use different game titles and apps to deliver the malware payloads to unsuspecting victims.

Laced Temple Runner game on the Microsoft Store *(Check Point)*

For now, users may take note of the publishers who released confirmed malicious game apps using the following names:

- Lupy games
- Crazy 4 games
- Jeuxjeuxkeux games
- Akshi games
- Goo Games
- Bizzon Case

It is important to emphasize that while the existing version of Electron Bot isn't causing catastrophic damage to the infected machines, the threat actors may easily modify the code to fetch a second-stage payload like a RAT or even ransomware.

Check Point suggests that Windows users avoid downloading applications with a low review count, scrutinize the developer/publisher details, and ensure that the app name is correct and not typo-squatted.