1. All large software has bugs in it, and the most powerful nation-state actors will have a collection of zero-day attacks for all of the most popular systems.

So why is installing the latest software updates still good security advice for most people in spite of this?

Check when your Chromebook's updates will stop

Chromebooks, Chromebases and Chromeboxes automatically manage updates so that your device has the latest software and security features. To check your Auto Update Expiry (AUE) date:

1. At the bottom right, select the time.
2. Select Settings .
3. At the left panel, at the bottom, select **About Chrome OS**.
4. Select **Additional details**.
5. In the 'Update schedule' section, you'll find when your Chromebook will receive its last update.

2. Suppose you run a web service that has become targeted by political activists. What sorts of attacks might they be able to launch at your system, and how might you defend against them?

Abuse

- Terrorism recruitment and child sex abuse material
- Hate campaigns such as Gamergate
- Intimate relationship abuse
- School and workplace bullying
- Growing pressure from governments to censor
- Big service firms already do a lot of filtering at great expense (sex abuse, terror, hate speech, nudity)
- 'Like' and 'Retweet' led to performative shaming; social media became an outrage machine

3. Why would Google run a hacker team like Project Zero?

Project Zero

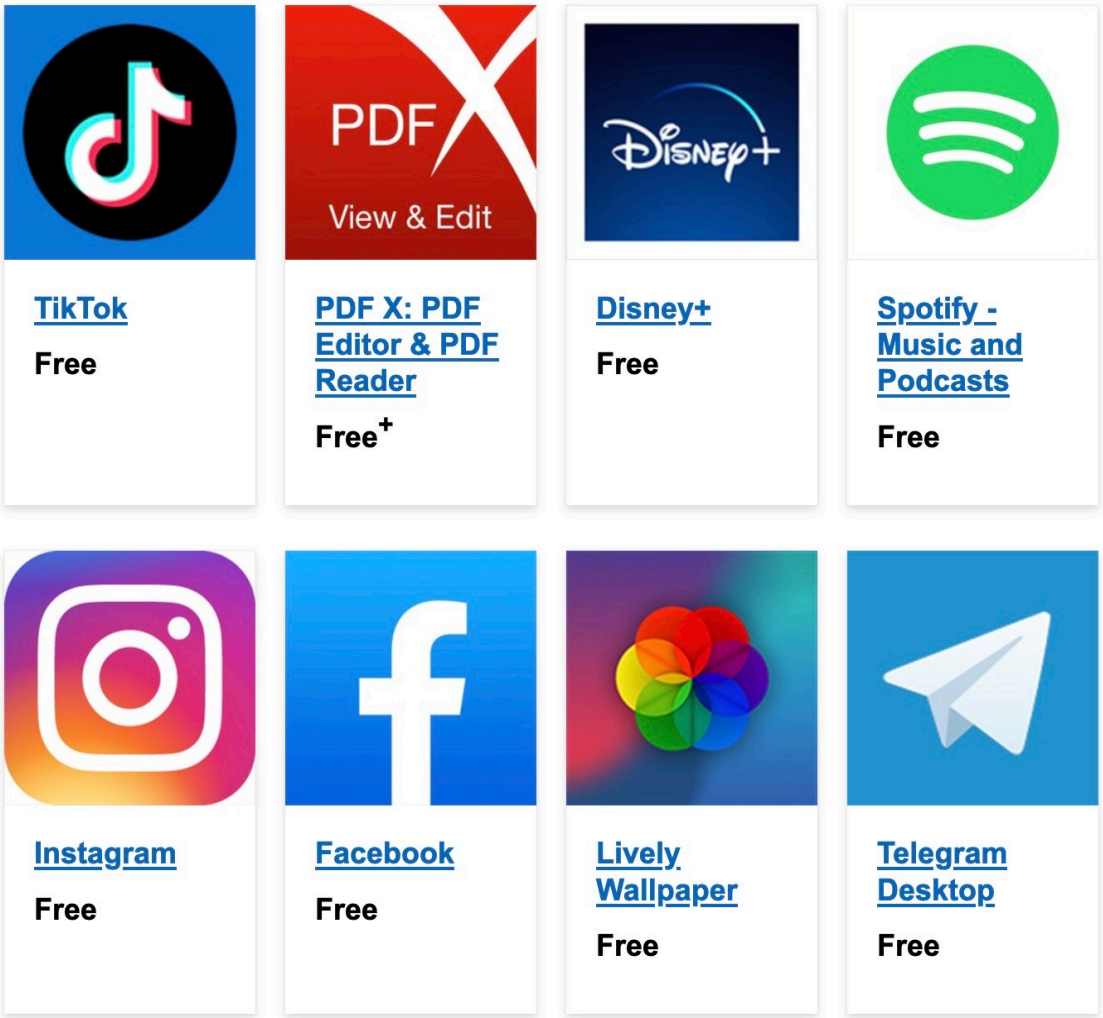
News and updates from the Project Zero team at Google

About Project Zero

Formed in 2014, Project Zero is a team of security researchers at Google who study zero-day vulnerabilities in the hardware and software systems that are depended upon by users around the world. Our mission is to make the discovery and exploitation of security vulnerabilities more difficult, and to significantly improve the safety and security of the Internet for everyone.

We perform vulnerability research on popular software like mobile operating systems, web browsers, and open source libraries. We use the results from this research to patch serious security vulnerabilities, to improve our understanding of how exploit-based attacks work, and to drive long-term structural improvements to security.

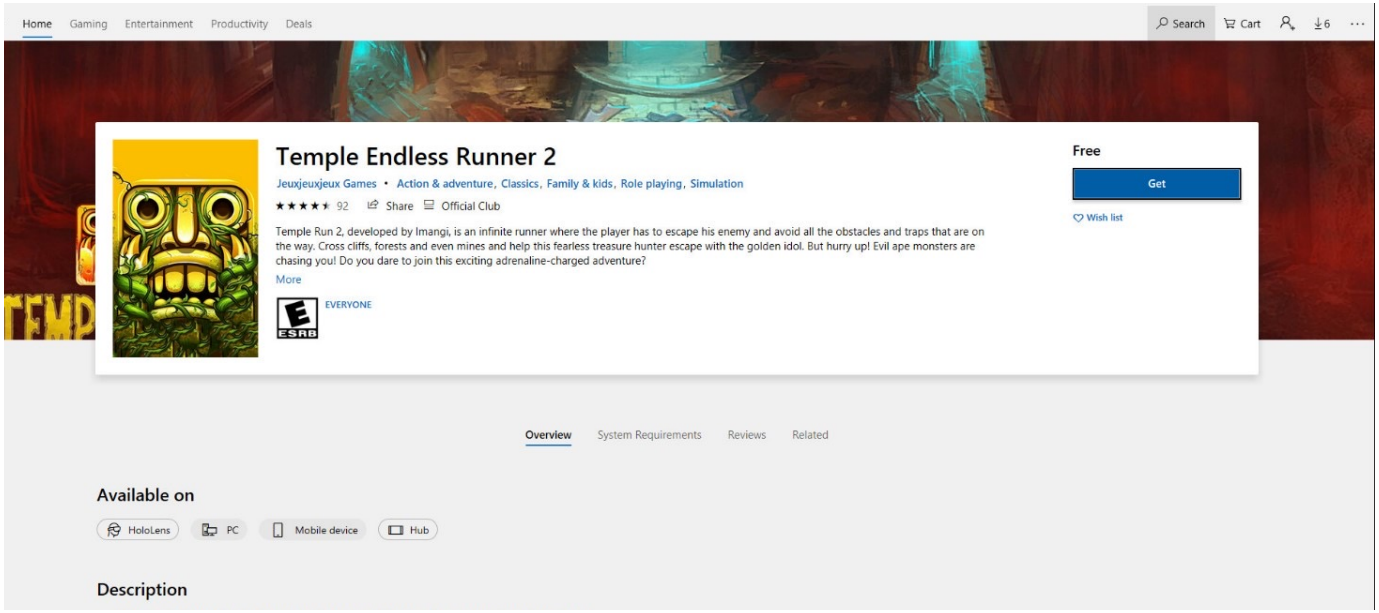
4. Microsoft describes the apps on its Windows Store as “trusted”. Is this good news or bad?

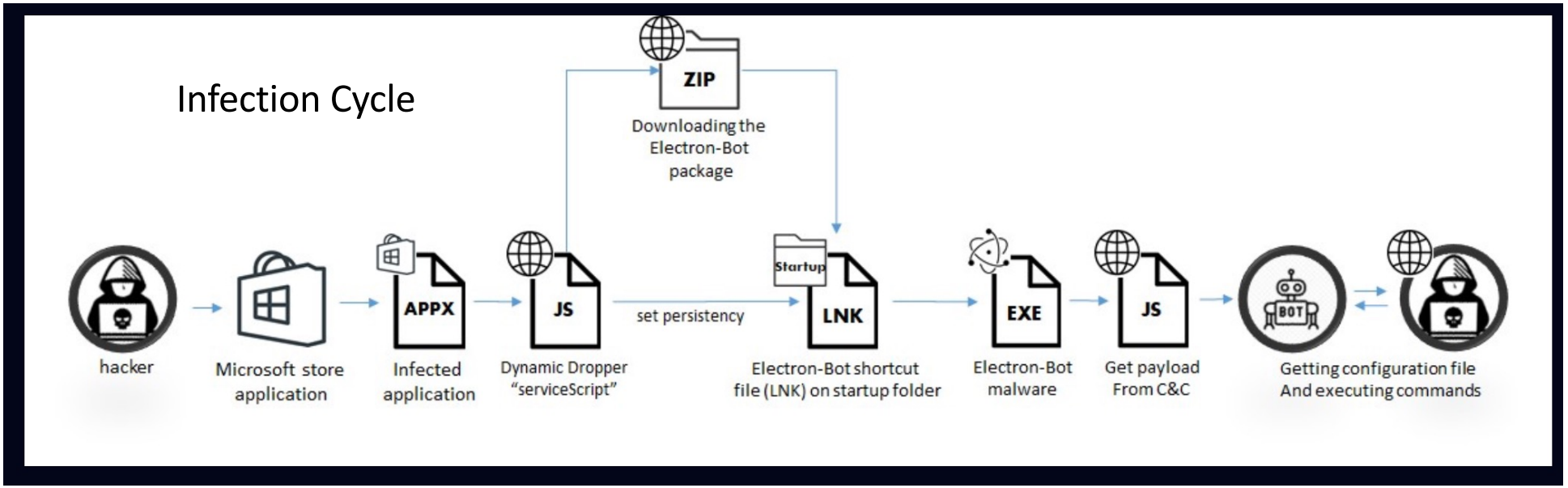


Electron Bot

Malware sneaks into Windows Store disguised as Popular Games – Temple Run, Subway Surfers, etc.

Attackers can use the installed malware as a backdoor to gain full control on the victim's machine





For more details, visit -- https://shorturl.at/yGX17

- 5. When might it be desirable or even possible to implement a system with both BIBA and Bell-LaPadula guarantees simultaneously?

Bell LaPadula

- *Simple Rule (No Read Up):* A subject at a given security level may not read an object at a higher security level.
- ** Property: (No Write Down):* A subject at a given security level may not write to any object at a lower security level.

BIBA

- *Simple Rule (No **Write** Up):* A subject at a given security level may not write to an object at a higher security level.
- ** Property: (No **Read** Down):* A subject at a given security level may not read from any object at a lower security level.

6. How might the concept of “Separation of Duty” as used in book-keeping systems also be applicable to writing secure code? In what ways might it be less applicable?

Actual Bookkeeping Systems

- How do you do separation of duties?
- Serial:
  - Lecturer gets money from EPSRC, charity, …
  - Lecturer gets finance office to register supplier
  - Gets stores to sign order form and send to supplier
  - Stores receives goods; department gets invoice
  - Department checks delivery and tell finance to pay
  - Lecturer gets statement of money left on grant
  - Audit by grant giver, university, …
- Parallel: two signatures (e.g. where transaction large, irreversible, as in bank guarantee)

7. Why might the poor “Policy” (“This policy is approved by management...”) pass as a valid security policy in many companies?

1. *This policy is approved by Management.*
2. *All staff shall obey this security policy.*
3. *Data shall be available only to those with a ‘need-to-know’.*
4. *All breaches of this policy shall be reported at once to Security.*

What’s wrong with this?