**Think like a Attacker, Protect Your JS Apps Against Malicious Packages – Charlie Gerard, Stripe @devdevcharlie**

“Zero-day attacks”?

1. Protestware: software created to raise awareness
2. Ransomware: form of malware designed to encrypt files on a device and demand payment
   1. Asymmetric encryption
      1. Generating a private key
      2. Generating a public key
   2. Make a Script.sh
      1. \*a bunch of steps\*
   3. Package json…
      1. “postinstall”: “bash script.sh”
      2. Install.js
3. Reverse shells: gaining remote access to a machines to opening a tunnel btwn computers. execute files on your machine
   1. Netcat command
4. Hiding Malware
   1. Use install scripts in package.json
   2. Code obfuscation
   3. Corrupt “resolved” urls in package-lock.json
   4. Bin script confusion
   5. VScode extensions
5. How to protect youself?
   1. You can’t really 😳
   2. BUT…. 👇🏽
      1. use a security tool (snyk, socket- check an npm package if its safe or not)
      2. integrate manual security checks in your workflow
      3. don’t install packages you don’t need
      4. regularly update your dependencies
      5. be careful of typosquatting
      6. prepare a cybersecurity disaster recovery plan