AllTheTalks.online

The threat is real: Software supply chain vulnerabilities

April 15, 2020

Presented by Maya Kaczorowski, Product Manager, GitHub

 @mayakacz  @MayaKaczorowski

@MayaKaczorowski

Maya Kaczorowski

Product Manager,
Software Supply Chain Security

GitHub

Agenda

What's a software supply chain

Supply chain compromises

- Kinds of attacks
- Real world examples 😨

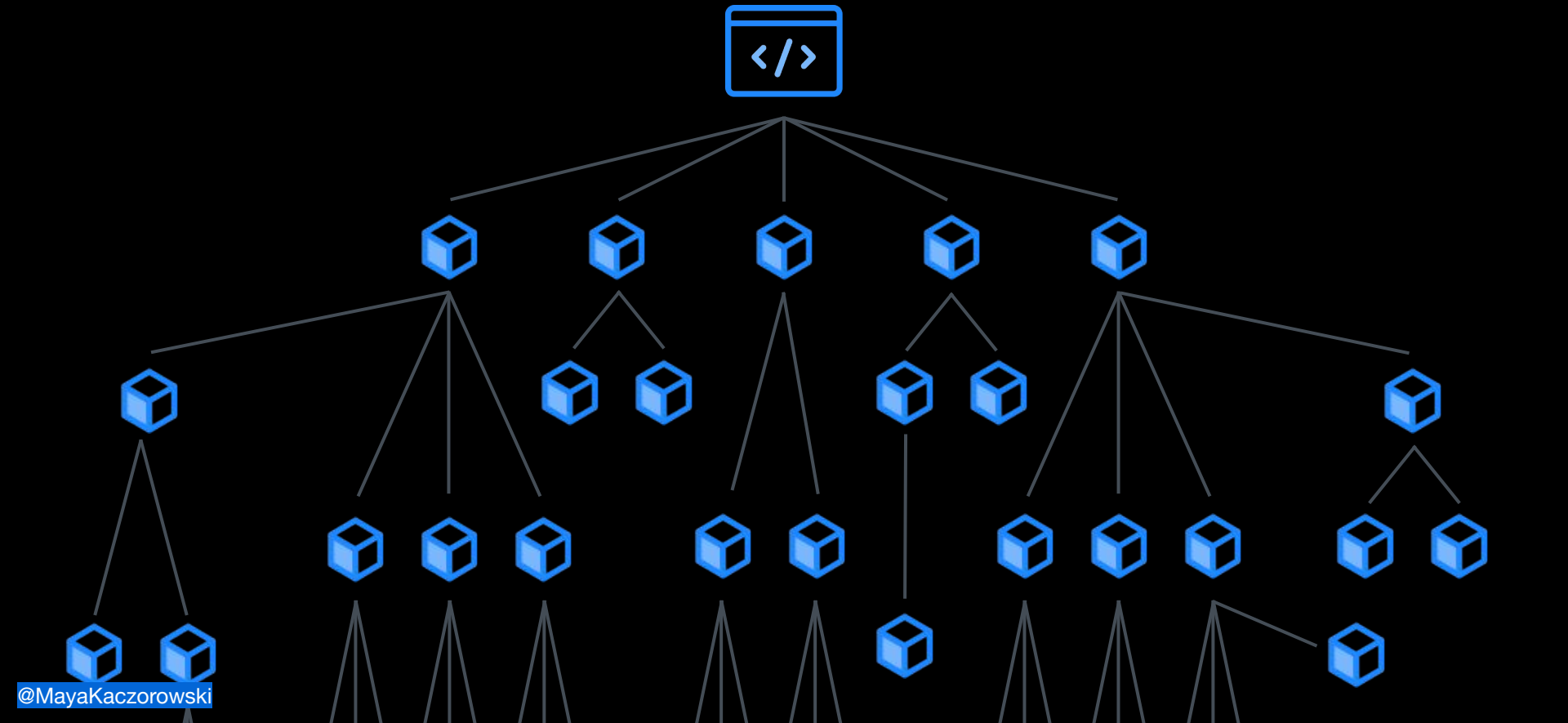
What can you do?

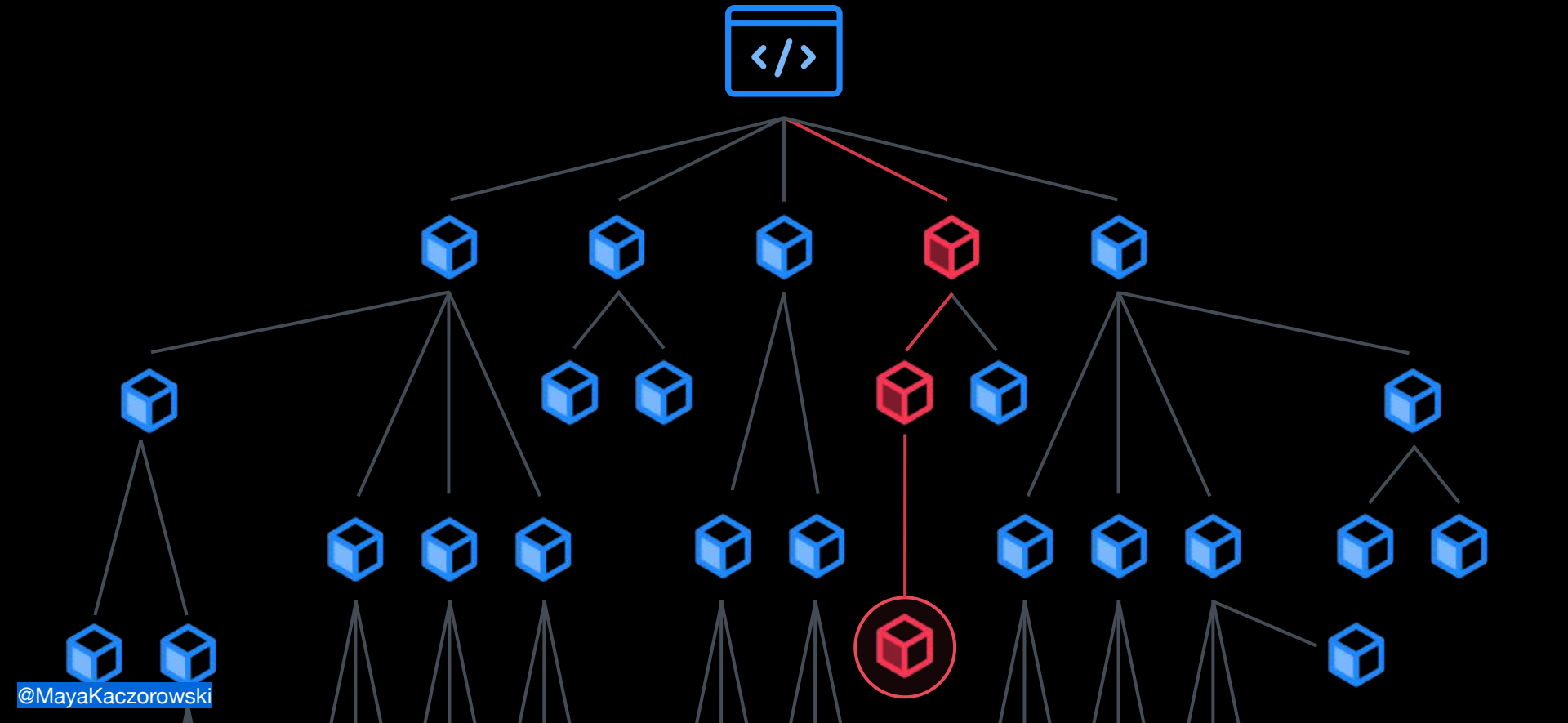
We're all dependent on open source code

A vast majority of code is open source

You don't actually know what you're running

- You don't know what dependencies you have
- You don't know what vulnerabilities you've introduced
- You don't know what licenses you're using


@MayaKaczorowski


@MayaKaczorowski

A software supply chain is anything that touches your code - from development, through your CI/CD pipeline, until it gets deployed into production.

Supply chain attacks

Method

- Malicious code, e.g., backdoor, malware, known vulnerability
- Compromised build tool
- Compromised signing keys
- Compromised package manager
- Compromised vulnerability reporting
- Account takeover
- Project takeover
- Accidental, e.g., typosquatting
- Deletion

Goal

- Backdoor, e.g., targeted, watering hole
- Malware, e.g., cryptocurrency mining
- Service disruption, e.g., deletion

event-stream

Widely used npm library
CVE-2018-1000851

Method: Project takeover
“he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years.”

Goal: Backdoor
Highly targeted to Copay developers, to distribute malware to capture credentials for Dash Copay bitcoin wallets

- `right9ctrl` volunteered to take over the package on GitHub, then added `flatmap-stream` as a dependency
- Another user `hugeglass` added malware to steal credentials to bitcoin wallets to `flatmap-stream`
- Profit

https://blog.npmjs.org/post/180565383195/details-about-the-event-stream-incident

eslint

npm package for Javascript static code analyzer

Method: Account takeover
Credential stuffing

Goal: Backdoor
To get `.npmrc` npm publishing creds!

- Attacker generated new auth tokens and published two malicious packages
- Second package discovered within an hour; altogether published for <4 hrs
- npm revoked ALL access tokens before the incident
- “A very small number” of packages and users affected

https://eslint.org/blog/2018/07/postmortem-for-malicious-package-publishes
https://gist.github.com/hzoo/51cb84afdc50b14bffa6c6dc49826b3e
https://status.npmjs.org/incidents/dn7c1fgrr7ng

EVlog “Kingslayer”

Initially undisclosed Windows log management software

Method: Compromised distribution tool
Website and update server used in software distribution

Goal: Backdoor
Credential theft?

- Compromised both the website for initial downloads, and the update website for updates
- Though company republished a patched version within two weeks, backdoored versions remained running in the wild for over a year later
- Poor disclosure process
- At least one defense contractor affected; potentially affected 24 banks, 5 defense contractors, 4 telcos, and many in Fortune 500

https://krebsonsecurity.com/2017/02/how-to-bury-a-major-breach-notification/

Webmin

Web app with 1M+ installs
CVE-2019-15107

Method: Compromised build tool
“malicious code inserted into Webmin and Usermin at some point on our build infrastructure”

Goal: Backdoor
Unauthenticated RCE

- Backdoor for unauthenticated RCE disclosed as a 0day at Defcon 27
- Unauthenticated requests, or where password expiry policy allowed users with expired passwords to reset them
- Backdoored packages on SourceForge only
- Distributed for more than a year

https://www.virtualmin.com/node/66890
https://www.pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthenticated-Remote-Command-Execution.html
https://www.zdnet.com/article/backdoor-found-in-webmin-a-popular-web-based-utility-for-managing-unix-servers/

docker123321

17 Docker Hub images

Method: Accidental
Easy to type registry name

Goal: Malware
Mining ~$90k of Monero

- 17 images in `docker123321` registry
- Contained malware since at least July 2017
- Suspected malware, positively identified as part of a cryptomining botnet
- Removed by Docker Hub in May 2018

https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers

left-pad

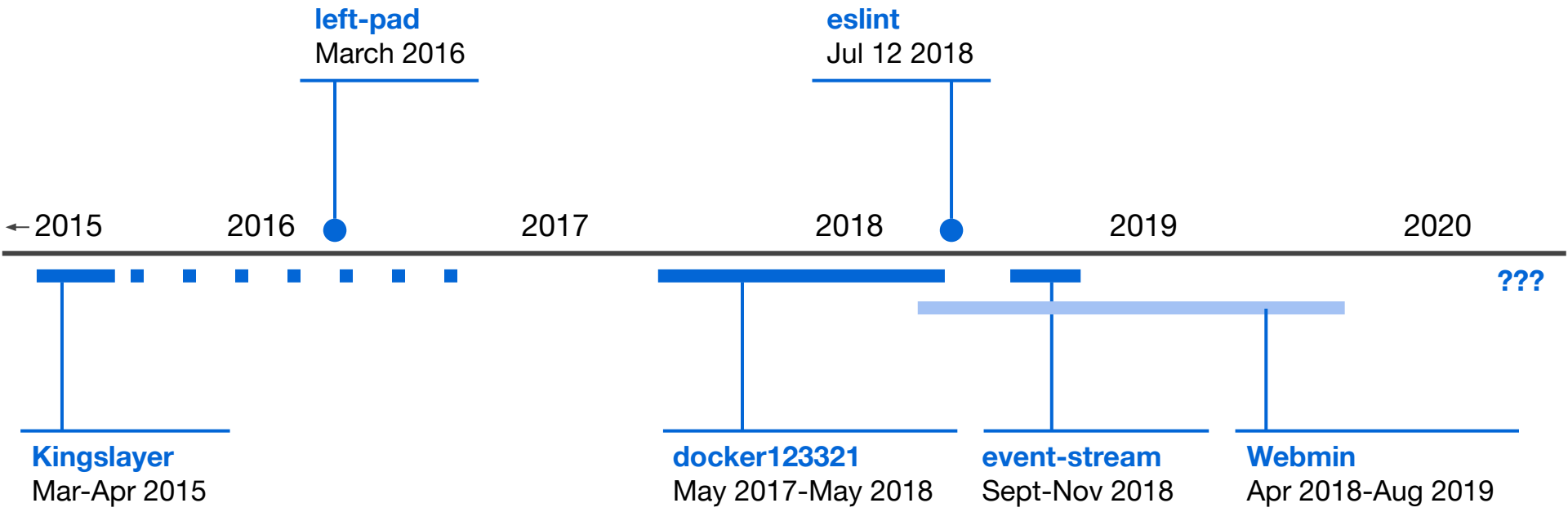
11-line npm library

Method: Deletion
“I think I have the right of deleting all my stuff”

Goal: Service disruption
Major packages like React

- `kik` library maintainer approached by Kik.com for copyright reasons
- Deletes 273 packages, including `left-pad`
- Reverted within 2 hours

https://qz.com/646467/how-one-programmer-broke-the-internet-by-deleting-a-tiny-piece-of-code/



Sample Software Supply Chain attacks

@MayaKaczorowski

Vulnerabilities are still more common than compromises

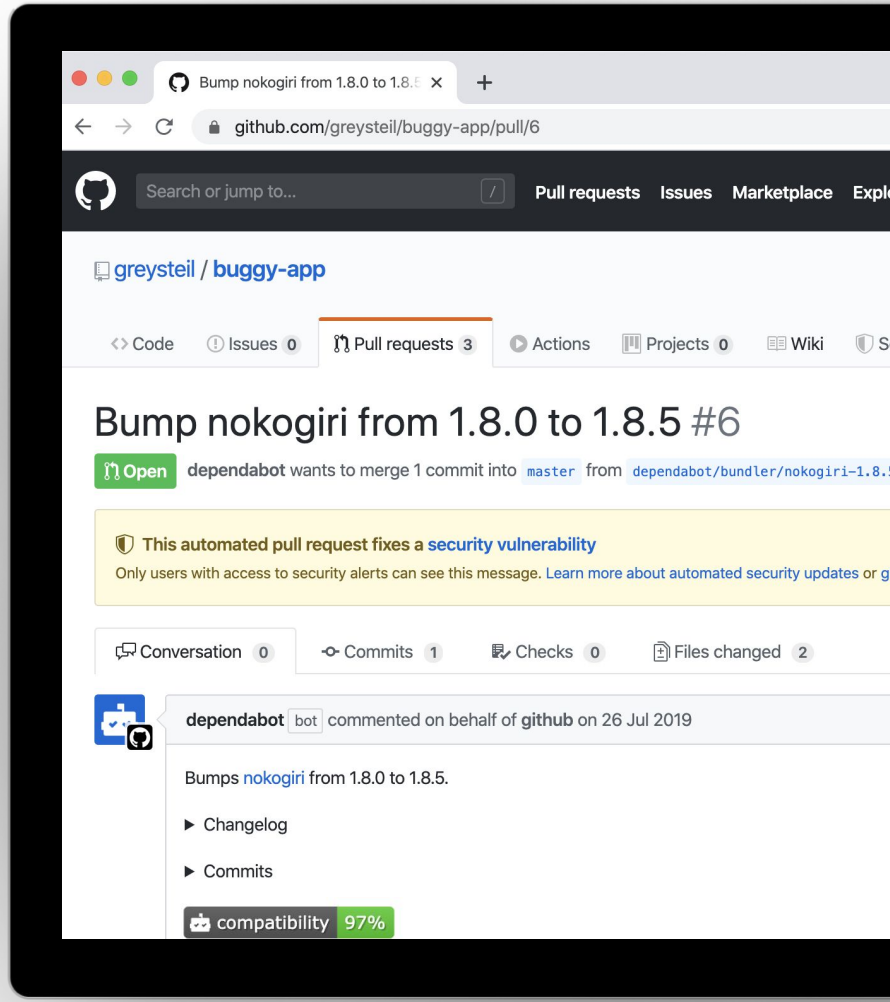
85% of open source vulnerabilities have a fix available at disclosure

What can you do, as a developer?

- Figure out your dependencies
  - Declare them explicitly
- Remove unnecessary dependencies
- Automate security updates
  - If your testing isn't that good, pay attention to security advisories
- Trust but verify
  - Security audits
  - Scan code, packages, e.g., `npm audit`
  - Check checksums

Turn on these GitHub features!

- Security alerts to notify you of vulnerabilities in code dependencies
- Automated Security updates generate a PR to move to a fixed version
- Generated automatically when a new vulnerable dependency is found
- Supports Composer, Maven, npm, NuGet, pip, and RubyGems



Learn more:
Software supply chain compromises

Supply chain compromises:
https://github.com/cncf/sig-security/tree/master/supply-chain-security/compromises

Turn on security alerts:
https://help.github.com/en/github/managing-security-vulnerabilities/about-security-alerts-for-vulnerable-dependencies

Turn on automated security updates:
https://help.github.com/en/github/managing-security-vulnerabilities/configuring-automated-security-updates

Questions? Concerns? Comments?