Don’t Be That DEV

Developer Attack Surface InfoSec Presentation
John Van Lowe (JVL) @ ATX JavaScript May Meetup

But first… Thank you CloudFlare!

i2Coalition

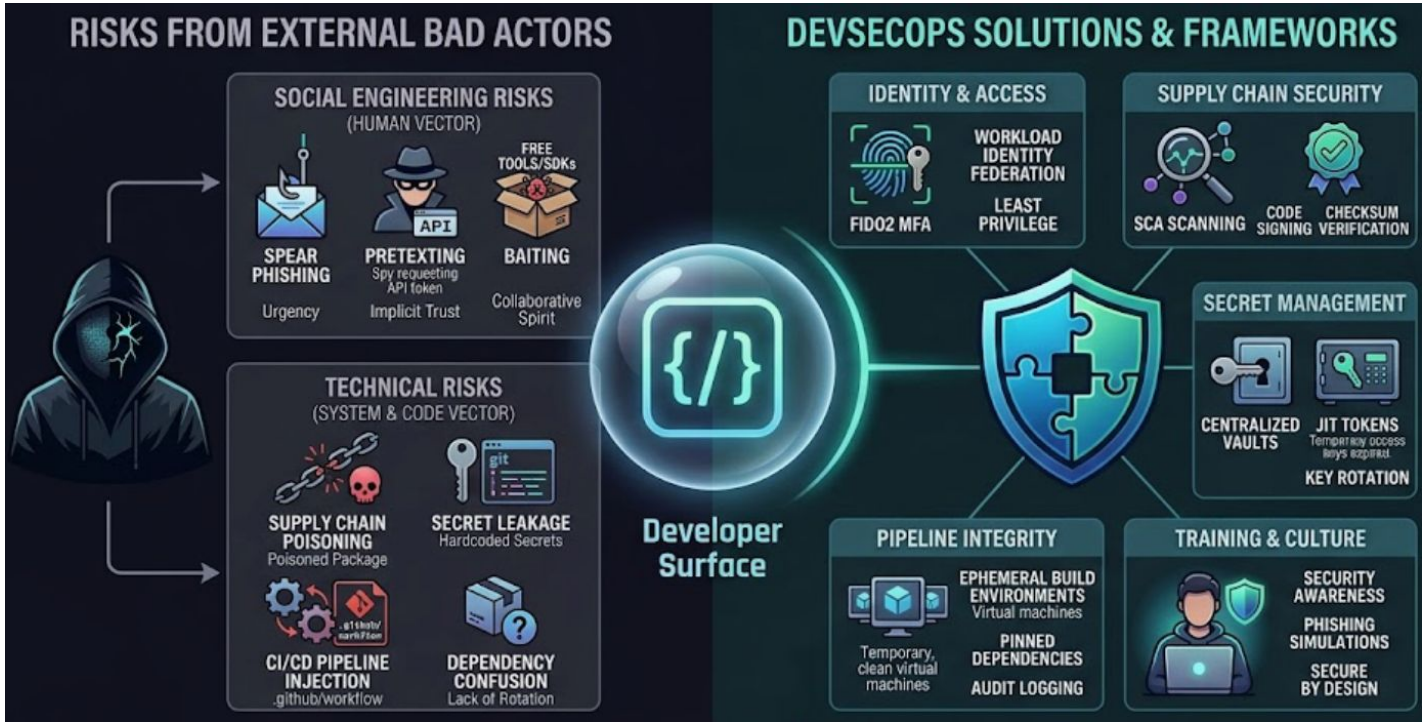
Secure Hosting Alliance

Italy DNS

Wall of Entropy

Boots?

Why are we here?



[ISC2 ATX May 20 Virtual]

[OWASP ATX May 26 Hybrid]

Brilliant People Who Do Silly Things

Things we'll discuss

Take-Home Malware Scams

Deepfake Technical Interview

Equipment Buy-Back Onboarding

GitHub Supply Chain Infiltration

Urgent Security Audit Phishing

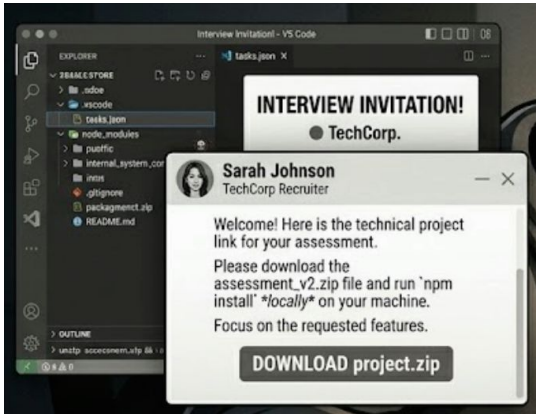
The Take-Home Malware Trap

A "recruiter" or "hiring manager" sends a GitHub repository or a zip file for a technical assessment.

You are asked to debug a project or add a feature as part of the interview.

The repo contains hidden malware (often in `.vscode/tasks.json`, `npm install` hooks, or obfuscated within a `node_modules` folder). As soon as you open the project or run the install command, it installs a **Remote Access Trojan (RAT)** or a **Credential Stealer** to harvest SSH keys, browser cookies, and environment variables.

The "company" is a startup you've never heard of, or the interviewer insists you run the code locally rather than using a cloud IDE.



Contagious Interview: NK campaign specifically targets developers with fake job offers
DEV#POPPER: attackers pose as interviewers and bait malicious npm run
BeaverTail & InvisibleFerret: steeler and backdoor
JADESNOW: js malware next.js

The Identity & Interview Scams

Scammers are now using real-time AI to impersonate reputable engineering leads from well-known companies.

You get a video call invite that looks legitimate. On camera, the interviewer looks and sounds like a real person (often spoofing a real employee's LinkedIn profile).

They use the "interview" to gather high-fidelity biometrics of your voice and face, or they ask you to "log in" to a fake portal to complete a coding challenge. This portal captures your **Single Sign-On (SSO)** credentials for Google, GitHub, or Microsoft.

The interviewer’s video has slight glitches (unnatural blinking or mouth movements), or they claim their "camera is broken" but want yours on.

Synthetic Identity: fake profile based on real person
Video Injection: term describing ability to inject a deepfake
Proxy Interviewing: shadow dev answering in background
Laptop Farms: physical locations with numerous devices enabling access for US or EU

"Equipment Buy-Back" Onboarding

A classic scam evolved for the remote-work era. After a suspiciously fast "interview" and "offer," you are officially hired.

The company sends you a check to buy your high-end workstation, monitors, and specialized dev gear from their "approved vendor."

The check is fraudulent. By the time your bank realizes it, you have already sent real money to the "vendor" (who is actually the scammer).

Receiving a job offer without ever speaking to a human on video, or an offer that arrives within hours of your first contact. Receiving a check for payment. Being asked to go physically purchase something they could have just shipped vs a check.

Mule Onboarding: hired for a front to move stolen funds through your bank account
Overpayment Gambit: scammer “accidentally” sends a check for more and asks to wire the excess payment back

GitHub Supply Chain Infiltration

This targets developers already working at a company.

You receive a message from a "fellow developer" or a "security researcher" on LinkedIn or X claiming they found a bug in one of your open-source repos or company projects.

They send a "Pull Request" or a link to a "fix." If you merge it or even just test it locally, you introduce a backdoor into your company's codebase. This is often used for **Corporate Espionage** or **Ransomware** deployment.

Unusual urgency or a "researcher" who refuses to use official bug bounty channels.

Thread-jacking: scammers jumping into real github issues or PR threads offering "fixes"
Typosquatting: historically a domain name attack, now common in package managers for all programming languages and social engineering with usernames and email addresses

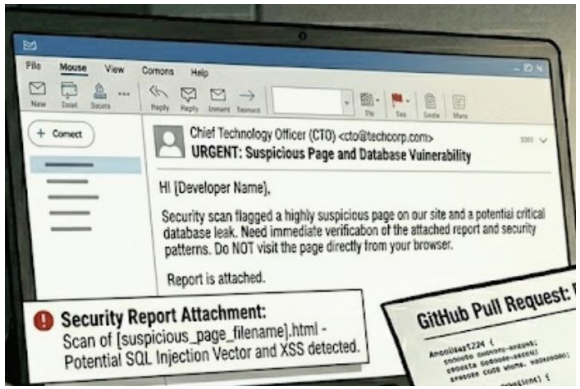
The Urgent Security Audit Phish

Targeting employed devs, this scam exploits the sense of responsibility.

You get an "urgent" Slack, Teams, or email notification from your CTO or Head of IT stating that your developer environment has been flagged for a security violation.

You are directed to a "verification" page that looks exactly like your company's internal SSO login. Once you enter your credentials and MFA code, the scammers gain full access to your company's AWS/Azure environment or internal repositories.

The URL of the login page is slightly off (e.g., `okta-company.com` instead of `company.okta.com`).



MFA Fatigue: hitting accept after denying numerous two factor attempts prior
Gift Card Scam: Same scam format, often forged from a CEO via text messages to non technical team members with direction to buy gift cards and discreetly send the details

Additional Resources - Before & After an Incident

BBB Scam Tracker: A searchable database where users report specific scams. You can search by company name or keywords like "software engineer interview."

Crunchbase: Use this to verify if a startup actually exists, who their investors are, and if they have a legitimate leadership team.

WHOIS (RDAP) Lookup: Check the registration date of the company's domain. **If a "Fortune 500" company is emailing you from a domain registered only three weeks ago, it is a scam.**

Glassdoor & Indeed: Look specifically for recent reviews mentioning "fake interviews" or "recruitment scams." Scammers often impersonate real companies, so check if the "official" career page matches the one you are using.

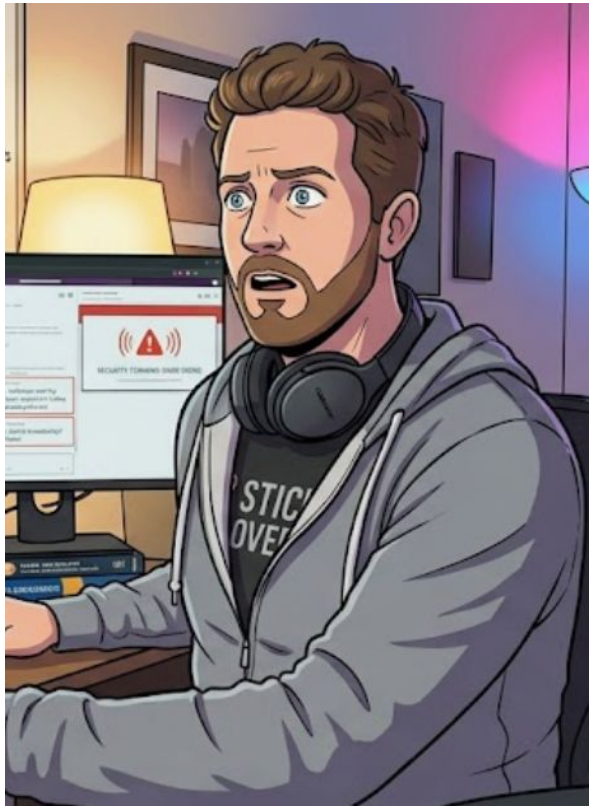
https://reportfraud.ftc.gov/ The primary portal for the Federal Trade Commission. Reporting here helps them build civil cases against scammers.

https://www.ic3.gov/ The internet crime complaint center exists to report "cyber-enabled" crimes, including identity theft, wire fraud, or phishing.

IdentityTheft.gov: If you provided your SSN or bank details, use this FTC site to create a recovery plan and freeze your credit.

Red Flags - AVOID!!!

- **Unsolicited** LinkedIn, Facebook, Reddit, or Telegram **message, especially for crypto, blockchain, Web3, or AI roles**
- **Salary noticeably above market, often without the company name being disclosed upfront**
- **Urgency in the first message, often paired with a Calendly link**
- **Website / GitHub / LinkedIn profile that look recent — few connections, no organic post history, no mutual contacts at real companies**



Red Flags - Declaration! 🚩

I will NOT:

- **Install a custom video conferencing app instead of Zoom, Meet, or Teams**
- **Download a "required" VPN, SDK, or security tool to participate**
- **Paste and run a terminal command to "fix" an error during an assessment**
- **Click "Trust this author" in VS Code when opening the recruiter's repo**
- **Disable antivirus, EDR, or other security controls to make the project run**
- **Open short links that redirect through file-hosting services**
- **Send personal info, banking details, ID documents, or any payment before an offer.**

CONNECT & RESOURCES

GITHUB:
Code & Contributions

github.com/johnvanlowe

LINKEDIN:
Professional Network

linkedin.com/in/johnvl