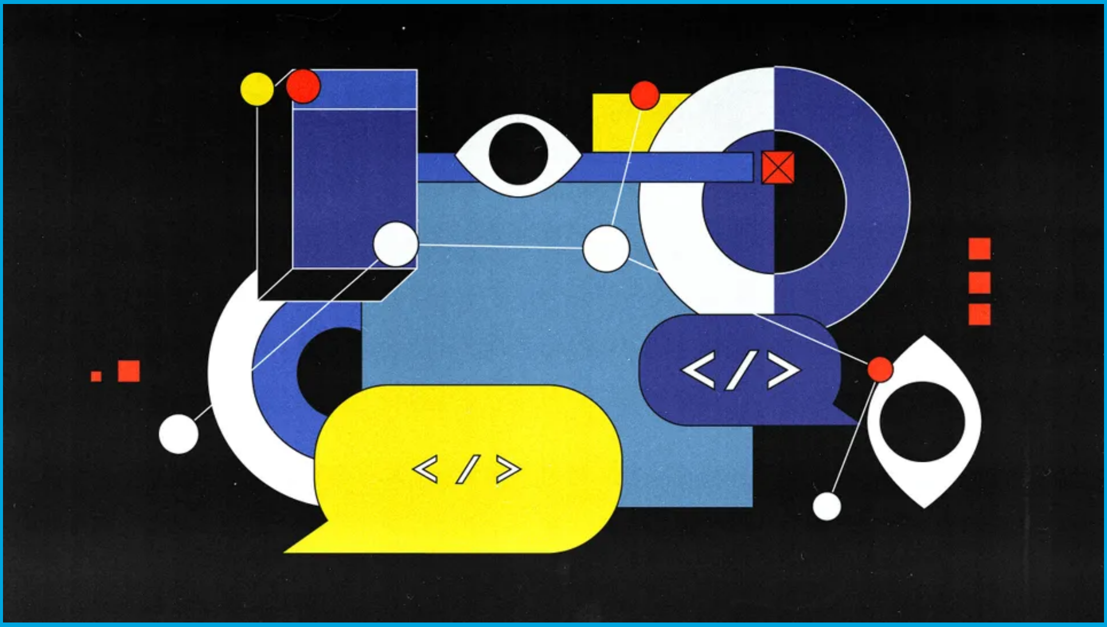
kindred

Security Newsletter

11 Apr 2022

Subscribe to this newsletter

The Tricky Aftermath of Source Code Leaks



The LAPSUS$ digital extortion group is the latest to mount a high-profile data-stealing rampage against major tech companies. And among other things, the group is known for grabbing and leaking source code at every opportunity, including from Samsung, Qualcomm, and Nvidia. At the end of March, alongside revelations that they had breached an Okta subprocessor, the hackers also dropped a trove of data containing portions of the source code for Microsoft's Bing, Bing Maps, and its Cortana virtual assistant. Sounds bad, right?

Businesses, governments, and other institutions have been plagued by ransomware attacks, business email compromise, and an array other breaches in recent years. Researchers say, though, that while source code leaks may seem catastrophic, and certainly aren't good, they typically aren't the worst-case scenario of a criminal data breach.

Typically, security researchers and attackers alike must use “reverse engineering” to find exploitable vulnerabilities in software, working backward from the final product to understand its components and how it works. And researchers say that process can actually be more helpful than looking at source code for finding bugs, because it involves more creative and open-ended analysis than just looking at a recipe. Still, there's no doubt that source code leaks can be problematic, especially for organizations that haven't done enough auditing and vetting to be sure that they've caught most basic bugs.

Read More on Wired

More #News

- Microsoft: Windows Autopatch steals the 'fun' from Patch Tuesdays
- Raspberry Pi removes default user to hinder brute-force attacks
- Google boosts Android security with new set of dev policy changes

- Google boosts Android security with new set of dev policy changes
- Malicious web redirect service infects 16,500 sites to push malware
- The Original APT: Advanced Persistent Teenagers
- GitHub can now auto-block commits containing API keys, auth tokens
- Android banking malware takes over calls to customer support
- First Malware Targeting AWS Lambda Serverless Platform Discovered
- Automaker Cybersecurity Lagging Behind Tech Adoption, Experts Warn
- Singapore begins licensing cybersecurity vendors
- OpenSSH now defaults to protecting against quantum computer attacks
- FBI removes malware from privately owned firewalls

#Breach Log

- Snap-on discloses data breach claimed by Conti ransomware gang
- UK retail chain The Works shuts down stores after cyberattack
- Cash App notifies 8.2 million US customers about data breach
- Hackers breach MailChimp's internal tools to target crypto customers

#Patch Time!

- Palo Alto Networks firewalls, VPNs vulnerable to OpenSSL bug
- VMware Releases Critical Patches for New Vulnerabilities Affecting Multiple Products

#Tech and #Tools

- CVE-2021-30737, @xerub's 2021 iOS ASN.1 Vulnerability
- Public Report – Google Enterprise API Security Assessment
- Learning Machine Learning Part 1: Introduction and Revoke-Obfuscation
- Nuclei: Packing a Punch with Vulnerability Scanning
- Double-Your-Crypto Scams Share Crypto Scam Host
- CI/CD Goat - A deliberately vulnerable CI/CD environment
- socialhunter: find broken social media links that can be hijacked
- PCI DSS v4.0 Resource Hub
- Server-side Request Forgery on FinTech Platform Enabled Administrative Account Takeover

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us