Security Newsletter
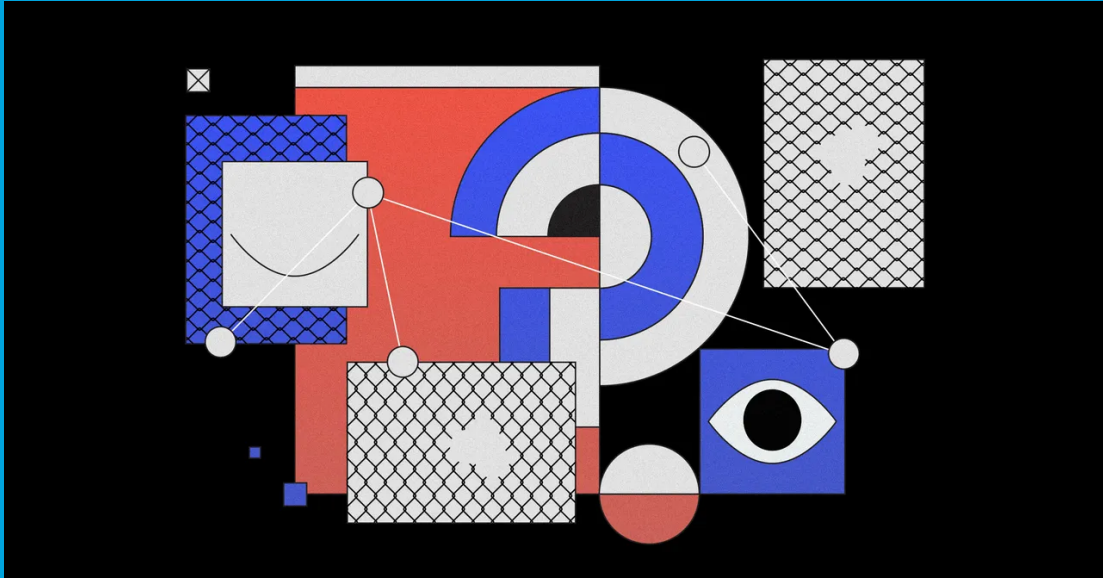
25 Apr 2022

Hackers Are Getting Caught Exploiting New Bugs More Than Ever

Previously unknown "zero-day" software vulnerabilities are mysterious and intriguing as a concept. But they're even more noteworthy when hackers are spotted actively exploiting the novel software flaws in the wild before anyone else knows about them. As researchers have expanded their focus to detect and study more of this exploitation, they're seeing it more often.

Two reports this week from the threat intelligence firm Mandiant and Google's bug hunting team, Project Zero, aim to give insight into the question of exactly how much zero-day exploitation has grown in recent years.

"We started seeing a spike early in 2021, and a lot of the questions I was getting all through the year were, 'What the heck is going on?!'" says Maddie Stone, a security researcher at Project Zero.

[Read More on Wired]

More #News

- [Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code](#)
- [Android banking malware intercepts calls to customer support](#)
- [Instagram beyond pics: Sexual harassers, crypto crooks, ID thieves](#)
- [Microsoft increases awards for high-impact Microsoft 365 bugs](#)
- [Hackers earn $400K for zero-day ICS exploits demoed at Pwn2Own](#)
- [T-Mobile confirms Lapsus$ hackers breached internal systems](#)
- [SMS Phishing Attacks are on the Rise](#)
- [Industrial Control System Malware Discovered](#)
- [The More You Know, The More You Know You Don't Know](#)

#Breach Log

- French hospital group disconnects Internet after hackers steal data
- Luxury fashion house Zegna confirms August ransomware attack
- Wind turbine firm Nordex hit by Conti ransomware attack
- GitHub: Attacker breached dozens of orgs using stolen OAuth tokens

#Patch Time!

- Microsoft Patch Tuesday, April 2022 Edition
- Critical Apache Struts RCE vulnerability wasn't fully fixed, patch now
- Critical flaw in Elementor WordPress plugin may affect 500k sites
- Hackers exploit critical VMware CVE-2022-22954 bug, patch now
- Google Chrome emergency update fixes zero-day used in attacks
- Newly found zero-click iPhone exploit used in NSO spyware attacks
- QNAP asks users to mitigate critical Apache HTTP Server bugs
- Atlassian fixes critical Jira authentication bypass vulnerability

#Tech and #Tools

- New XSS vectors
- Diving Deeper into WatchGuard Pre-Auth RCE - CVE-2022-26318
- Coercing NTLM Authentication from SCCM
- Abusing Azure Container Registry Tasks
- Inside the Black Box | How We Fuzzed Microsoft Defender for IoT and Found Multiple Vulnerabilities
- Mitigating the top 10 security threats to GCP using the CIS Google Cloud Platform Foundation Benchmark
- A brief look at Windows telemetry: CIT aka Customer Interaction Tracker
- Top 9 Fuzzers for pentest
- Researcher Releases PoC for Recent Java Cryptographic Vulnerability

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- Are you a developer with a strong security passion? Be part of our Cyber Security team

Kindred is one of the largest online gambling companies in the world with over 30 million customers. You can find all our open vacancies on our career page.

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