kindred

Security Newsletter

4 Apr 2022

Subscribe to this newsletter

Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA

Multifactor authentication (MFA) is a core defense that is among the most effective at preventing account takeovers. In addition to requiring that users provide a username and password, MFA ensures they must also use an additional factor—be it a fingerprint, physical security key, or one-time password—before they can access an account. Nothing in this article should be construed as saying MFA isn't anything other than essential.

That said, some forms of MFA are stronger than others, and recent events show that these weaker forms aren't much of a hurdle for some hackers to clear. In the past few months, suspected script kiddies like the Lapsus$ data extortion gang and elite Russian-state threat actors (like Cozy Bear, the group behind the SolarWinds hack) have both successfully defeated the protection.

Read More on ArsTechnica

More #News

- Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"
- State-sponsored Attack Groups Capitalise on Russia-Ukraine War for Cyber Espionage
- Conti-nuation: methods and techniques observed in operations post the leaks
- EU draft law adds security checks to all crypto transactions
- Phishing uses Azure Static Web Pages to impersonate Microsoft
- US national emergency extended due to elevated malicious cyber activity

- Europol dismantles massive call center investment scam operation
- Ukraine dismantles 5 disinformation bot farms, seizes 10,000 SIM cards
- This Father-Son Team Helps People Brute-Force Their Lost Bitcoin Wallet Passwords
- Researchers Used a Decommissioned Satellite to Broadcast Hacker TV
- A Sinister Way to Beat Multifactor Authentication Is on the Rise
- PCI DSS 4.0; It's time to get serious on Magecart

#Breach Log

- Viasat confirms satellite modems were wiped with AcidRain malware
- Shutterfly discloses data breach after Conti ransomware attack

#Patch Time!

- Trend Micro fixes actively exploited remote code execution bug
- Critical GitLab vulnerability lets attackers take over accounts
- Zyxel patches critical bug affecting firewall and VPN devices
- Apple emergency update fixes zero-days used to hack iPhones, Macs
- Spring patches leaked Spring4Shell zero-day RCE vulnerability
- New Spring Java framework zero-day allows remote code execution
- Google Chrome Bug Actively Exploited as Zero-Day

#Tech and #Tools

- AcidRain | A Modem Wiper Rains Down on Europe
- Pwning Microsoft Azure Defender for IoT
- 15-Year-Old Bug in PEAR PHP Repository Could've Enabled Supply Chain Attacks
- New Python-based Ransomware Targeting JupyterLab Web Notebooks
- The end of the road for Cloudflare CAPTCHAs
- FORCEDENTRY: Sandbox Escape
- PacketStreamer: distributed packet capture for cloud-native platforms
- Digital Forensics Basics: A Practical Guide for Kubernetes DFIR
- TruffleHog v3 - Find leaked credentials
- SpringShell (Spring4Shell) Zero-Day Vulnerability CVE-2022-22965 : All You Need To Know

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