Security Newsletter
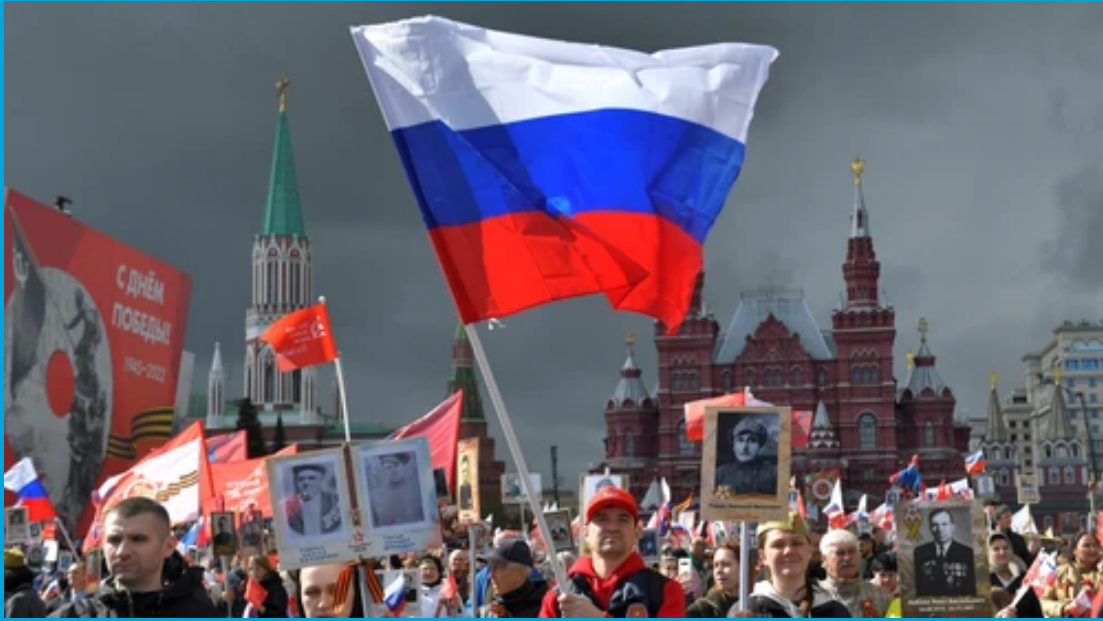
16 May 2022

Subscribe to this newsletter

Western Governments Accuse Russia of Hacking US Satellite Internet Provider

The European Union and the UK government accused Russia of conducting several hacks linked to its invasion in Ukraine, including one against a satellite provider of high-speed internet in Europe.

"The European Union and its Member States, together with its international partners, strongly condemn the malicious cyber activity conducted by the Russian Federation against Ukraine, which targeted the satellite KA-SAT network, operated by Viasat," read the press release from the EU.

"The UK's National Cyber Security Centre (NCSC) assesses that the Russian Military Intelligence was almost certainly involved in the 13 January defacements of Ukrainian government websites and the deployment of Whispergate destructive malware. The NCSC also assesses that it is almost certain Russia was responsible for the subsequent cyber-attack impacting Viasat on 24 February," the UK government's press release read.

Read More on Vice

Even More in EC's press release

More #News

- DEA Investigating Breach of Law Enforcement Data Portal
- Italian CERT: Hacktivists hit govt sites in 'Slow HTTP' DDoS attacks
- Iranian hackers exposed in a highly targeted espionage campaign
- Our Medical Devices' Open Source Problem – What Are the Risks?
- FBI, CISA, and NSA warn of hackers increasingly targeting MSPs
- US, EU blame Russia for cyberattack on satellite modems in Ukraine
- Researchers Find Potential Way to Run Malware on iPhone Even When it's OFF
- Google Created 'Open Source Maintenance Crew' to Help Secure Critical Projects
- E.U. Proposes New Rules for Tech Companies to Combat Online Child Sexual Abuse
- Europe Agrees to Adopt New NIS2 Directive Aimed at Hardening Cybersecurity
- How a pentester's attempt to be 'as realistic as possible' alarmed cybersecurity firms
- The NSA Says that There are No Known Flaws in NIST's Quantum-Resistant Algorithms
- ICE Is a Domestic Surveillance Agency
- Taking on the Next Generation of Phishing Scams

#Breach Log

- Engineering firm Parker discloses data breach after ransomware attack
- BRIEF Canadian fighter jet training company investigating ransomware attack
- Costa Rica's new president declares state of emergency after Conti ransomware attack

#Patch Time!

- Microsoft Patch Tuesday, May 2022 Edition
- Hackers are exploiting critical bug in Zyxel firewalls and VPNs
- HP fixes bug letting attackers overwrite firmware in over 200 models

#Tech and #Tools

- Hunting evasive vulnerabilities
- Putting Things in Context | Timelining Threat Campaigns
- BPFdoor: Stealthy Linux malware bypasses firewalls for remote access
- Release of Technical Report into the AMD Security Processor
- Where to begin? Prioritizing ATT&CK Techniques

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