kindred

Security Newsletter

24 May 2021

Subscribe to this newsletter

The Full Story of the Stunning RSA Hack Can Finally Be Told

In 2011, Chinese spies stole the crown jewels of cybersecurity—stripping protections from firms and government agencies worldwide.

In the decade that followed, many key RSA executives involved in the company's breach have held their silence, bound by 10-year nondisclosure agreements.

After 10 years of rampant state-sponsored hacking and supply chain hijacks, the RSA breach can now be seen as the herald of our current era of digital insecurity—and a lesson about how a determined adversary can undermine the things we trust most.

Read More on Wired

More #News

- Bizarro banking malware targets 70 banks in Europe and South America
- Irish High Court issues injunction to prevent HSE data leak
- Microsoft releases SimuLand, a test lab for simulated cyberattacks
- US introduces bills to secure critical infrastructure from cyber attacks
- Colonial Pipeline CEO Confirms $4.4 Million Ransom Payment
- Florida water treatment plant was involved in second security incident before poisoning attempt
- US insurance giant CNA Financial paid $40 million ransom to regain control of systems
- Try This One Weird Trick Russian Hackers Hate
- How Apple Gave Chinese Government Access to iCloud Data and Censored Apps
- Regulator fines COVID-19 tracker for turning contact data into sales leads
- Inside 'TALON' the Nationwide Network of AI-Enabled Surveillance Cameras

- Inside TALON, the Nationwide Network of AI-Enabled Surveillance Cameras

#Breach Log

- Air India data breach impacts 4.5 million customers
- FBI: Conti ransomware attacked 16 US healthcare, first responder orgs
- E-commerce giant Mercari suffers major data breach in Codecov incident
- Conti ransomware gives HSE Ireland free decryptor, still selling data
- Misconfiguration of third party cloud services exposed data of over 100 million users
- Student health insurance carrier Guard.me suffers a data breach

#Patch Time!

- Wormable Windows HTTP vulnerability also affects WinRM servers
- QNAP confirms Qlocker ransomware used HBS backdoor account
- May Android security updates patch 4 zero-days exploited in the wild

#Tech and #Tools

- Comcast now blocks BGP hijacking attacks and route leaks with RPKI
- That single GraphQL issue that you keep missing
- AWS CloudFormation Guard v2.0.1 a general-purpose policy-as-code evaluation tool
- Counter-Strike Global Offsets: reliable remote code execution
- Browser fuzzing at Mozilla
- Active Directory persistence through userAccountControl manipulation
- Getting a persistent shell on a 747 IFE

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 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 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