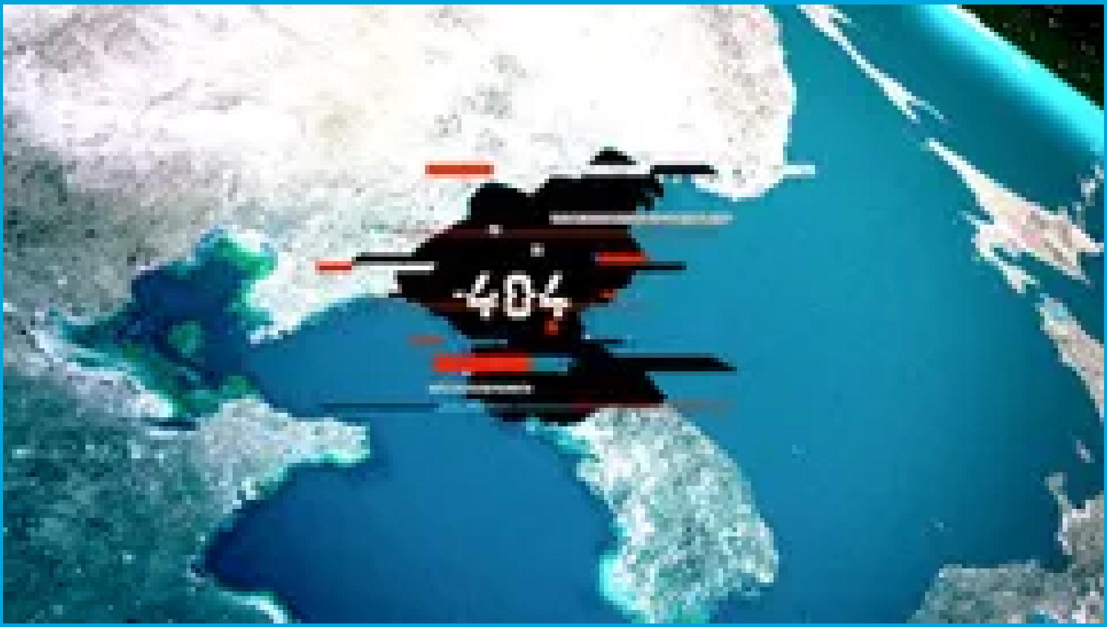
Security Newsletter

7 Feb 2022

Subscribe to this newsletter

North Korea Hacked Him. So He Took Down Its Internet



For the past two weeks, observers of North Korea's strange and tightly restricted corner of the internet began to notice that the country seemed to be dealing with some serious connectivity problems. On several different days, practically all of its websites—the notoriously isolated nation only has a few dozen—intermittently dropped offline en masse, from the booking site for its Air Koryo airline to Naenara, a page that serves as the official portal for dictator Kim Jong-un's government. At least one of the central routers that allow access to the country's networks appeared at one point to be paralyzed, crippling the Hermit Kingdom's digital connections to the outside world.

Some North Korea watchers pointed out that the country had just carried out a series of missile tests, implying that a foreign government's hackers might have launched a cyberattack against the rogue state to tell it to stop saber-rattling.

But responsibility for North Korea's ongoing internet outages doesn't lie with US Cyber Command or any other state-sponsored hacking agency. In fact, it was the work of one American man in a T-shirt, pajama pants, and slippers, sitting in his living room night after night, watching Alien movies and eating spicy corn snacks—and periodically walking over to his home office to check on the progress of the programs he was running to disrupt the internet of an entire country.

Read More on Wired

Welcome to the Burner Phone Olympics

As professional big air snowboarder Julia Marino completed her final preparations for the Winter Olympics, US officials sent Marino and her teammates a word of caution about China's surveillance apparatus. The athletes were warned not to take their personal phones to the games. "We are using burner phones while we're going to be there," Marino, a seven-time X Games medalist, said in an interview on Instagram. Athletes were also cautioned not to speak out against human rights abuses. "There has been discussion of what could happen if we do speak out," Marino said in the interview.

As the Beijing Winter Olympics kick off, Marino isn't alone. Thousands of foreign athletes, coaches, (some) diplomats, and members of the media are descending on the Chinese capital and taking extra measures to protect themselves from snooping by authoritarian law enforcement officials. That means burner laptops and phones to ensure sensitive data can't be hoovered up, and self-censoring potential criticism of human rights abuses against the Muslim Uyghur population in the northwestern Xinjiang region.

A lot has changed since China last hosted the Olympics in the summer of 2008. The nation has evolved into a technological superpower, with advanced capabilities in everything from artificial intelligence to quantum computing. Its homegrown tech giants make products that have hundreds of millions of users and underpin the essential tasks in people's daily lives. At the same time, technological surveillance and censorship of the country's citizens is rife, China maintains a sophisticated group of state-backed hackers, and the UN has warned about the detention and treatment of Uyghurs.

Read More on Wired

More #News

- Health Sites Let Ads Track Visitors Without Telling Them
- FBI shares Lockbit ransomware technical details, defense tips
- Microsoft blocked billions of brute-force and phishing attacks last year
- Telco fined €9 million for hiding cyberattack impact from customers
- Hackers Backdoored Systems at China's National Games Just Before Competition
- Another Israeli Firm, QuaDream, Caught Weaponizing iPhone Bug for Spyware
- U.S. Authorities Charge 6 Indian Call Centers Scamming Thousands of Americans
- Ransomware Wants You to Like and Subscribe, Or Else
- The EARN IT Act Is Back

#Breach Log

- HHS: Conti ransomware encrypted 80% of Ireland's HSE IT systems
- Swissport ransomware attack delays flights, disrupts operations
- KP Snacks giant hit by Conti ransomware, deliveries disrupted
- German petrol supply firm Oiltanking paralyzed by cyber attack
- Washington state agency discloses data breach impacting hundreds of thousands of licensed professionals
- Fortune 500 service provider says ransomware attack led to leak of more than 500k SSNs

#Patch Time!

- Argo CD vulnerability leaks sensitive info from Kubernetes apps
- Cisco fixes critical bugs in SMB routers, exploits available
- Zimbra zero-day vulnerability actively exploited to steal emails

#Tech and #Tools

- Apollo 2.0—New Year, New Features
- Invisible Sandbox Evasion
- Firefox JIT Use-After-Frees | Exploiting CVE-2020-26950
- Testing Infrastructure-as-Code Using Dynamic Tooling
- UEFI firmware vulnerabilities affect at least 25 computer vendors

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