New activity from and against North Korean hackers; Russian hackers target French IT monitoring company; Cambodia adopts China-style internet firewall; Facebook blocks Australian news outlets; and Most of London’s boroughs using Chinese surveillance tech linked to Xinjiang.

**Blog Post by Adam Segal**

*February 19, 2021, 7:00 am (EST)*

---

**New Activity From and Against North Korean Hackers**

Reports on Tuesday alleged that North Korea attempted to steal COVID-19 vaccine data from U.S. pharmaceutical company Pfizer. South Korea’s National Intelligence Service informed lawmakers of the attempted breach during a scheduled closed-door security meeting. In a statement following the meeting, Ha Tae-keung, a member of the Korean National Assembly’s intelligence committee, also revealed that South Korea has observed a 32 percent increase in the number of North
Korean cyber operations. This news comes three months after Microsoft accused Russian and North Korean state-backed hackers of targeting vaccine research in Canada, France, India, South Korea, and the United States. It remains unclear if any data was stolen during the operation announced on Tuesday.

On Wednesday, the U.S. Department of Justice publicly indicted three North Koreans alleged to be members of threat actor Lazarus Group for an array of cybercriminal activity dating back several years. The charges included conspiring to steal more than $1.3 billion from banks and cryptocurrency exchanges in order to circumvent sanctions, as well as the hack of Sony Pictures in 2014. It was not mentioned whether the three North Koreans included in the indictment played a role in the recent Pfizer operation.

Russian Hackers Target French IT Monitoring Company

More on:

Cybersecurity
Pharmaceuticals and Vaccines
Cambodia
Digital Policy
Privacy

On Monday, the French cybersecurity agency, known by its acronym ANSSI, announced that the IT monitoring software of French cybersecurity firm Centreon was targeted by hackers exhibiting similar characteristics to the Russian threat actor Sandworm. The agency reported that the campaign, which took place between 2017 and 2020, “most affected information technology providers, especially web hosting providers,” yet the initial attack vector is still unknown. In a statement released on Tuesday, Centreon claimed that only those that downloaded the open-source version of their software, which it says
had not been updated in the past five years, were impacted. The suspected number of compromised entities totals **fifteen**, and though none of the company’s major customers, which include Airbus, the French Ministry of Justice, and Euronews, were impacted, the breach is yet another reminder of the threats faced by third party IT companies in the wake of the SolarWinds intrusion.

**Cambodia Adopts China-Style Internet Firewall**

Cambodia has **adopted** new internet regulations that will enable the government to surveil, censor, and restrict the online activity of its citizens. The **eleven-page sub-ordinance** on the Establishment of the National Internet Gateway (NIG) was signed by Prime Minister Hun Sen on Wednesday and requires all internet connections in the country to be rerouted and filtered through a central regulatory gateway. This regulatory gateway, which has been compared to China’s “Great Firewall,” would be **tasked** with “prevent[ing] and disconnect[ing] all network connect[ions] that affect national incomes, security, social order, morality, culture, traditions and customs.” Internet providers have a one-year window to reroute their services. The decree has drawn **sharp criticism** from human rights advocates, with several fearing that it will facilitate the government’s continued repression of civil liberties and political freedoms within the country. “The establishment of the NIG is of grave concern for the future of fundamental human rights in Cambodia,” Chak Sopheap, the Director of the Cambodian Center for Human Rights **said** in a statement. “It will become another instrument for the Royal Government of Cambodia to control and monitor the flow of information in Cambodia.”

**Facebook Blocks Australian News Outlets**
Facebook has blocked Australian users from sharing or viewing Australian news content on its platform, a dramatic move that has further escalated tensions between the social media site and the Australian government. The controversial decision comes in response to a proposed media bargaining law that would require big tech companies like Google and Facebook to compensate news publishers for running ads alongside links to their news sites. Facebook’s Vice President of Global News Partnerships Campbell Brown argues that the law misunderstands its relationship with news outlets, stating in a blog post that “contrary to what some have suggested, Facebook does not steal news content. Publishers choose to share their stories on Facebook.” Unlike Facebook, Google has taken a more diplomatic approach to the proposed law—which could be replicated in other countries—by announcing media partnerships with several news outlets, including Australian publishers Sky News and the Australian.

Most of London’s Boroughs Using Chinese Surveillance Tech Linked to Xinjiang

A new report released by the Thomson Reuters Foundation on Thursday found that at least half of London’s councils—local authorities that oversee city boroughs—have purchased and deployed Chinese surveillance technology linked to the persecution of Uighur Muslims in Xinjiang. According to freedom of information requests filed late last year with London’s thirty-two councils and the next twenty largest UK councils, roughly two-thirds of these organizations purchased surveillance systems made by Hikvision and Dahua Technology, both of whom have ties to state surveillance in Xinjiang. Although none of the local authorities said they used facial recognition products from the companies, Samuel Woodhams, the report’s author, argued that hardware that the councils had purchased could be easily configured to
perform facial recognition, demographic, and behavioral analysis. Liberal Democrat Alistair Carmichael, who co-wrote a 2019 letter raising concerns about Hikvision, stated that the United Kingdom, “should not be working with companies that facilitate repression,” arguing that the government should ban Hikvision and Dahua, both of whom face strict trade restrictions in the United States.

Details: https://www.cfr.org/blog/cyber-week-review-february-19-2021