SNL

Friday, August 11, 2017 6:19 PM ET Extra

'State-sponsored' hackers breach Irish power grid, fears linger over hidden code

By Andrew Coffman Smith

Ireland's all-island power grid was the target of a "state-sponsored" cyberattack that exposed all of Eirgrid's internal communications sent over a power cable after hackers gained access through an Internet router used by the grid operator in Wales and Northern Ireland.

As reported by the Irish *Independent* newspaper, state-owned EirGrid learned of the breach from its telecommunications company Vodafone and the United Kingdom's National Cyber Security Centre. The virtual wiretap installed by the hackers, known as generic routing encapsulation tunneling, was only discovered in July — more than two months after the initial April 20 attack on EirGrid's Direct Internet Access, or DIA, service at its Shotton, Wales site for the 500-MW undersea East-West Interconnector high-voltage, direct current power cable connecting British and Irish electricity markets.

The attack on the DIA router lasted almost seven hours and gave hackers direct access to all information that passed to and from the Shotton site, including information on commercial customers but not residential customers. A follow-up security check by EirGrid discovered that the offices of its UK subsidiary in Northern Ireland, the System Operator for Northern Ireland Ltd., or SONI, were also compromised and its data also being monitored by hackers. Northern Ireland is also connected to Britain's power grid via a 500-MW HVDC Moyle Interconnector between County Antrim and South Ayrshire in Scotland.

According to *The Independent*, sources said both Vodafone and the British cybersecurity agency believe the breach was a "state-sponsored attack" by hackers working via IP addresses listed in Bulgaria and Ghana. Irish and British police do not believe the hack originated in either country.

More devious attacks

The Independent's sources also said it is still not known if any malicious software have been installed on EirGrid's control systems nor how much data was compromised. However, Vodafone informed the Irish grid operator that the attackers copied all the firmware and files on the compromised routers. Another source said these files will allow the hackers to inspect the network configuration of Vodafone and launch further "devious" attacks in the future.

"We can confirm that though our computer systems have not been breached, there was a breach of an external service provided by a third party which sat outside of our infrastructure," said EirGrid Group spokesman David Martin in a statement. "The impacted equipment has been replaced and there has been no interruption to the group's systems or business."

Formed in 2015, the Republic of Ireland's cybersecurity agency, also called the National Cyber Security Centre, or NCSC, has expanded its duties from initially protecting only government infrastructure and data to also safeguarding critical national infrastructure. The cybersecurity agency is overseen by Ireland's Department of Communications, Climate Action and Environment. A spokesman with the Irish department said in a statement that the NCSC "continues to work on" the breach and is working closely with critical infrastructure providers and other entities across Europe on cybersecurity.

Furthermore, the Irish government spokesman said the communications and environmental department will "shortly" propose legislation to strengthen security measures for critical infrastructure and to implement the European Union's Network and Security Directive that threatens severe fines if owners of critical infrastructure, like energy and transport, fail to promptly report cybersecurity breaches. In anticipation of this, Ireland's cybersecurity agency has just finished significantly expanding its workforce, the spokesman said.

Vodafone and the U.K. NCSC did not immediately respond to requests for comment.