MEDIA REPORT 5

Summary

In the CNBC News article, “How a North Korean cyber group impersonated a Washington D.C. analyst” written by Rohan Goswami, it is reporting on how a North Korean hacker group called APT43 hacked into Jenny Town’s computer to run scripts to collect personal information such as Town’s colleagues, her field of study, and her contact list to create a digital doppelganger of Town. Jenny Town is a leading expert on North Korea at the Stimson Institute and the director of Stimson’s 38 North Program. Town’s work builds on open-source intelligence where she uses publicly available data points to paint a picture of North Korean dynamics. At the time, Town didn’t have clearance to have access to any classified information. Note that APT43 was able to hack into Town’s computer in the middle of the night while Town left her computer to brush her teeth. APT43 then used the personal information to create a digital doppelganger of Town to use social engineering to attempt to get more information or to establish a relationship with Town’s colleagues. Town’s colleagues were suspicious of the digital doppelganger and questioned the doppelganger. Town’s colleagues were able to not get hacked and protected personal information from APT43.

Every country has an embassy for intelligence purposes and people attached to the embassy will take the pulse of the city to gauge what policy might be in the pipeline or how policymakers felt about a particular country or event. However, North Korea never had diplomatic relations with the US, so its intelligence officers can’t stalk public events or network with think tanks. To make up for that void, a country could obtain intelligence through hacking into government systems. Once they get access to someone's important information, hackers can use social engineering which involves sending fake emails while pretending to be someone important. This tactic has been less effective due to widening awareness but the most susceptible victims are older, less-tech-savvy academics who don't scrutinize domains or emails for typos.

Personal Opinion

Overall, I strongly agree with the actions that Town's colleagues took to prevent getting hacked and prevent APT43 from getting access to their personal information because they used APT43 to create more doppelgangers and prevent other colleagues from getting hacked. I believe that Jenny Town and other people should've practiced cybersecurity awareness because cybersecurity awareness training equips individuals with the knowledge and skills to identify/respond appropriately to such threats thus reducing the likelihood of successful attacks. Also with the rise of cyber crime in the recent decade, it would be crucial to get proper training to protect your data. Since 2023 there are 3,809,448 records stolen from breaches every day, 2,645 per minute, and 44 every second of every day.

While I believe people should get cybersecurity awareness training, I think another big issue is addressing the increasing number of cyber crimes that are happening right now. Cyber crimes affect everyone online and businesses/organizations. So it would make sense that there should be more protective software and cyber defense measures taken in place to prevent people's/organizations' data online.

Citation

Rogoswami, Rohan. "How a North Korean cyber group impersonated a Washington D.C. analyst". CNBC, September 18, 2023. https://www.cnbc.com/2023/09/18/how-a-north-korean-cyber-group-impersonated-a-washington-dc-analyst.html