P4x Retaliatory Hack of North Korea's Internet

Published 28 February 2022

Earlier this month, it was reported that a hacker based in the United States claimed to have disrupted North Korea's internet, after deliberately taking down most of the country's websites, including the site that functions as the state's official online platform. This was after reports of supposed outages in the country's internet connectivity surfaced. Unsurprisingly, there are only a few dozen websites in the country and at certain moments all sites appeared to be down.

It is understood the disruption started shortly after a sequence of missile tests had been carried out, which led to certain commentators asking if the disruption was at the hands of foreign countries who may have been demonstrating their disapproval to these tests.

However, there are now reports that the mysterious American hacker, who goes by the handle P4x, has taken credit for the attack which appears to have been an act of retaliation after being targeted by a North Korean hacking campaign that was supposedly directed at Western security researchers, of which he is one.

It appears that as part of this campaign, the North Koreans undertook a degree of reconnaissance in an effort to steal information relating to recent vulnerabilities and hacking tools. Although still unverified, P4x maintains they were unable to take anything from his system. In response, the hacker suggests that given the lack of assistance and interest from law enforcement, he took matters into his own hand and felt it was the right thing for him do in order to send a message to the state.

In order to carry out the act of retaliation, P4x was able to locate and exploit a number of unpatched bugs in the North Korean network which allowed him to launch a DDoS attack (Distributed Denial of Service), flooding the servers with excessive internet traffic. This in turn affected the few internet networks relied upon by the country. One example he gave was a known vulnerability that enabled him to take the servers offline. He has chosen not to publicise the other vulnerabilities so as not to give the North Korean government an opportunity to defend against similar incidents.

The consequences of P4x's response remain uncertain at this time and the effect to the North Korean government is yet to be seen. P4x points out that his objective is to simply prove a point and to show that there will be consequences to those who choose to initiate this attacks against civilians. It also seems that part of his objective was to send a message to his own government to draw attention to the lack of government response to external cyber threats to US civilians.

In light of the recent publicity it remains to be seen what the response from the far side of the world will be to the state wide disruption caused by a foreign national. P4x has suggested that his campaign is far from over and will start to look for ways to retrieve valuable information from the North Korean government - he is even looking to recruit like-minded hackers to join the fight.

Authors

Brett Randles

+44 (0) 20 7894 6377
brandles@dacbeachcroft.com