

Disappointed with the lack of US response to the Hermit Kingdom's attacks against US security researchers, one hacker took matters into his own hands.

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.

Just over a year ago, an independent hacker who goes by the handle P4x was himself hacked by North Korean spies. P4x was just one victim of a hacking campaign that targeted Western security researchers with the apparent aim of stealing their hacking tools and details about software vulnerabilities. He says he managed to prevent those hackers from swiping anything of value from him. But he nonetheless felt deeply unnerved by state-sponsored hackers targeting him personally—and by the lack of any visible response from the US government.

So after a year of letting his resentment simmer, P4x has taken matters into his own hands. “It felt like the right thing to do here. If they don’t see we have teeth, it’s just going to keep coming,” says the hacker. (P4x spoke to WIRED and shared screen recordings to verify his responsibility for the attacks but declined to use his real name

for fear of prosecution or retaliation.) “I want them to understand that if you come at us, it means some of your infrastructure is going down for a while.”

5 P4x says he's found numerous known but unpatched vulnerabilities in North Korean systems that have allowed him to singlehandedly launch “denial-of-service” attacks on the servers and routers the country's few internet-connected networks depend on. For the most part, he declined to publicly reveal those vulnerabilities, which he argues would help the North Korean government defend against his attacks. But he named, as an example, a known bug in the web server software NginX that mishandles certain HTTP headers, allowing the servers that run the software to be
10 overwhelmed and knocked offline. He also alluded to finding “ancient” versions of the web server software Apache, and says he's started to examine North Korea's own national homebrew operating system, known as Red Star OS, which he described as an old and likely vulnerable version of Linux.

15 P4x says he has largely automated his attacks on the North Korean systems, periodically running scripts that enumerate which systems remain online and then launching exploits to take them down. “For me, this is like the size of a small-to-medium pentest,” P4x says, using the abbreviation for a “penetration test,” the sort of whitehat hacking he's carried out in the past to reveal vulnerabilities in a client's network. “It's pretty interesting how easy it was to actually have some effect in
20 there.”

“If they don't see we have teeth, it's just going to keep coming.”

P4X, HACKER

Those relatively simple hacking methods have had immediate effects. Records from the uptime-measuring service Pingdom show that at several points during P4x's
25 hacking, almost every North Korean website was down. (Some of those that stayed up, like the news site Uriminzokkiri.com, are based outside the country.) Junade Ali, a cybersecurity researcher who monitors the North Korean internet, says he began to observe what appeared to be mysterious, mass-scale attacks on the country's internet starting two weeks ago and has since closely tracked the attacks without having any
30 idea who was carrying them out.

Ali says he saw key routers for the country go down at times, taking with them not only access to the country's websites but also to its email and any other internet-based services. “As their routers fail, it would literally then be impossible for data to be routed into North Korea,” Ali says, describing the result as “effectively a total
35 internet outage affecting the country.” (P4x notes that while his attacks at times disrupted all websites hosted in the country and access from abroad to any other

internet services hosted there, they didn't cut off North Koreans' outbound access to the rest of the internet.)

As rare as it may be for a single pseudonymous hacker to cause an internet blackout on that scale, it's far from clear what real effects the attacks have had on the North Korean government. Only a tiny fraction of North Koreans have access to internet-connected systems to begin with, says Martyn Williams, a researcher for the Stimson Center think tank's North Korea-focused 38 North Project. The vast majority of residents are confined to the country's disconnected intranet. Williams says the dozens of sites P4x has repeatedly taken down are largely used for propaganda and other functions aimed at an international audience.

While knocking out those sites no doubt presents a nuisance to some regime officials, Williams points out that the hackers who targeted P4x last year—like almost all the country's hackers—are almost certainly based in other countries, such as China. “I would say, if he's going after those people, he's probably directing his attentions to the wrong place,” says Williams. “But if he just wants to annoy North Korea, then he is probably being annoying.”

For his part, P4x says he would count annoying the regime as a success, and that the vast majority of the country's population that lacks internet access was never his target. “I definitely wanted to affect the people as little as possible and the government as much as possible,” P4x says.

He acknowledges that his attacks amount to no more than “tearing down government banners or defacing buildings,” as he puts it. But he also says that his hacking has so far focused on testing and probing to find vulnerabilities. He now intends to try actually hacking into North Korean systems, he says, to steal information and share it with experts. At the same time, he's hoping to recruit more hacktivists to his cause with a dark website he launched Monday called the FUNK Project—i.e. “FU North Korea”—in the hopes of generating more collective firepower.

“This is a project to keep North Korea honest,” the FUNK Project site reads. “You can make a difference as one person. The goal is to perform proportional attacks and information-gathering in order to keep NK from hacking the western world completely unchecked.”

P4x says his hacktivist efforts are meant to send a message not only to the North Korean government, but also his own. His cyberattacks on North Korean networks are, he says, in part an attempt to draw attention to what he sees as a lack of government response to North Korean targeting of US individuals. “If no one's going to help me, I'm going to help myself,” he says.

P4x knows the exact moment last year when he was hit by North Korea's spies. In late January of 2021, he opened a file sent to him by a fellow hacker, who had described it as an exploitation tool. Just 24 hours later, he spotted a blog post from Google Threat Analysis Group warning that North Korean hackers were targeting security researchers. Sure enough, when P4x scrutinized the hacking tool he'd received from a stranger, he saw that it contained a backdoor designed to provide a remote foothold on his computer. P4x had opened the file in a virtual machine, digitally quarantining it from the rest of his system. But he was nonetheless shocked and appalled by the realization that he'd been personally targeted by North Korea.

P4x says he was later contacted by the FBI but was never offered any real help to assess the damage from North Korea's hacking or to protect himself in the future. Nor did he ever hear of any consequences for the hackers who targeted him, an open investigation into them, or even a formal recognition from a US agency that North Korea was responsible. It began to feel, as he put it, like "there's really nobody on our side."

When WIRED asked the FBI about its response to the North Korean targeting of US security researchers, it responded in a statement: "As the lead agency responsible for threat response we rely on the public and private sector to report suspicious activity and intrusions, and work together to ensure we understand what's happening, prevent it from happening to others, and hold those responsible accountable," the FBI statement reads. "The FBI is committed to pursuing the malicious actors and countries behind cyberattacks, and will not tolerate intellectual property theft or intimidation."

After his experience as a target of state-sponsored cyberespionage, P4x spent much of the next year on other projects. But after a year had passed, still without public or private statements from the federal government about the targeting of security researchers and no offer of support from any US agency, P4x says he decided it was time to make his own statement to both the North Korean and American governments.

Other hackers targeted by North Korea don't all agree that P4x's hacking spree is the right way to make that statement. Dave Aitel, a former NSA hacker and the founder of security firm Immunity, was similarly targeted in the same espionage campaign. But he questions whether P4x has taken a productive approach to getting even, given that he may actually be getting in the way of stealthier intelligence efforts targeting the same North Korean computers.

"I would not want to disrupt real Western intelligence efforts that are already in place on those machines, assuming there is anything of value there," Aitel says.

- Aitel agrees, though, that the government response to North Korea's campaign has been lacking. He says he never received any contact from a government agency and lays the blame for that silence specifically at the feet of the Cybersecurity and Infrastructure Security Agency. “This is one of the biggest balls CISA, in particular, has dropped,” Aitel says. “The United States is good at protecting the government, OK at protecting corporations, but does not protect individuals.” He points out that many of the targeted security researchers likely had significant access to software vulnerabilities, enterprise networks, and the code of widely used tools. That could result, he says, in “the next SolarWinds.”
- 10 When WIRED reached out to CISA, a spokesperson responded in a statement that the agency “is committed to supporting the cybersecurity community in detecting and protecting against malicious cyber actors,” adding that “as part of this work, we encourage any researcher that is being targeted by cyber threats to contact the US government so we can provide all possible assistance.”
- 15 US government criticisms aside, P4x is clear that his hacking aims primarily to send a message to the Kim regime, which he describes as carrying out “insane human rights abuses and complete control over their population.” While he acknowledges that his attacks likely violate US computer fraud and hacking laws, he argues he hasn't done anything ethically wrong. “My conscience is clear,” he says.
- 20 And what's the final goal of his cyberattacks on that totalitarian government's internet infrastructure? When will he end them?
- “Regime change. No, I'm just kidding,” P4x says with a laugh. “I just want to prove a point. I want that point to be very squarely proven before I stop.”