February 8, 2022

TLP White

This week, *Hacking Healthcare* begins by examining an article that claims an American civilian took it upon himself to launch a cyberattack against the government of the Democratic People's Republic of Korea (DPRK). We look at how this case relates to the broader conversation around hacktivism and the headaches this type of action could cause the U.S. government. Next, we explore the news that the Department of Homeland Security (DHS) has initiated the launch of a Cyber Safety Review Board (CSRB), including how it might be beneficial and how it might not. Welcome back to *Hacking Healthcare*.

1. **American Allegedly Hacks DPRK Internet Infrastructure**

   Last week, an article from Wired alleged that the unusual internet connectivity problems the DPRK appeared to be suffering from for the past few weeks was in fact not caused by internal problems or by an outside government retaliating for continued DPRK missile tests.[1] According to Wired, the cause was an independent American civilian who was disgruntled over being caught up in a DPRK cyber operation against cybersecurity researchers and the American government's apparent lack of public response to it.

   The individual, identified only as P4x, commented to Wired that his actions "felt like the right thing to do" in order to impose some costs on the government of the DPRK.[2] He further stated that "I want them to understand that if you come at us, it means some of your infrastructure is going down for a while."[3]

   Alleging to have found "numerous known but unpatched vulnerabilities," P4x carried out large-scale denial-of-service (DDoS) attacks. His attacks appear to have been fairly successful with evidence that nearly all of the DPRK's websites went down.[4] While, P4x stated that he acknowledged that his actions were akin to "tearing down government banners or defacing buildings," he stated that he counted annoying the N. Korean government as a success.[5]

   Perhaps concerningly, P4x does not appear content with his DDoS being the end of his operations. He revealed to Wired that he hopes to actually hack into the DPRK's systems to steal information and share it with experts.[6] He is also looking to expand his one-man

operation by recruiting other "hacktivists" for his "FU North Korea" project. The goal would be to "keep North Korea honest" and "perform proportional attacks and information-gathering in order to keep NK from hacking the western world completely unchecked."[7]

While clearly unhappy at being targeted by the DPRK's earlier cyber operation, a not-insignificant source of P4x's motivation appears to come from his disappointment in how the U.S. government responded. In addition to a lack of public reprisal against the DPRK, P4x believes that the FBI did not adequately respond to his own outreach for help, making him feel somewhat alone against a state actor.

Action & Analysis
Included with H-ISAC Membership

2. DHS Cyber Safety Review Board

One long-awaited element of the Biden administration's cybersecurity executive order appears to finally be on its way to completion. Section 5 of last May's *Executive Order on Improving the Nation's Cybersecurity* directed the Secretary of Homeland Security to establish a Cyber Safety Review Board (CSRB) to address significant cyber incidents. After many months of silence, a Federal Register notice announcing the creation of the board dropped on February 2.[8]

The cybersecurity executive order laid out that the CSRB "shall review and assess, with respect to significant cyber incidents…affecting Federal Civilian Executive Branch Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses."[9] As reiterated in the Federal Register notice, "Upon completion of its review of an applicable incident, the CSRB may develop advice, information, or recommendations for the Secretary for improving cybersecurity and incident response practices and policy," which may then be passed on to the president.[10] The goal of these activities, as the Department of Homeland Security (DHS) summed up, is "so that government, industry, and the broader security community can better protect our nation's networks and infrastructure."[11]

Among those ordered to be included in the CSRB's membership are The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CSIA), and "representatives from appropriate private-sector cybersecurity or software suppliers."[12] The addition of others from the private sector is to be on a case-by-case basis at the discretion of the Secretary of Homeland security. The Federal Register notice appears to expand the potential for private sector membership by rewording the executive order slightly to read "CSRB members will also include individuals from private sector entities to include appropriate cybersecurity or software suppliers."

The notice further clarifies that the CSRB shall be composed of no more than 20 members and that "members shall consist of subject matter experts from appropriate professions and diverse communities nationwide, be geographically balanced, and shall include representatives of a broad and inclusive range of industries."[13] It will be chaired by Rob Silvers, the Department of Homeland Security's undersecretary for strategy, policy, and plans. While the CSRB's output is to be made public whenever possible, the notice acknowledges that redactions will need to be made "consistent with applicable law and the need to protect sensitive information from disclosure."[14]

Action & Analysis
Included with H-ISAC Membership

Congress -

Tuesday, February 8th:
- Senate – Committee on Homeland Security & Governmental Affairs: Responding to and Learning from the Log4Shell Vulnerability

Wednesday, February 9th:
- No relevant hearings

Thursday, February 10th:
- No relevant hearings

International Hearings/Meetings –
- No relevant meetings

EU –
Wednesday, February 9th:
- HSE cyberattack: a wake-up call for healthcare right across Europe | How European-funded research can boost your cyber resilience in 2022

Conferences, Webinars, and Summits
https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author
Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, and as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

[1] https://www.wired.com/story/north-korea-hacker-internet-outage/

[2] https://www.wired.com/story/north-korea-hacker-internet-outage/

[3] https://www.wired.com/story/north-korea-hacker-internet-outage/

[4] https://www.wired.com/story/north-korea-hacker-internet-outage/

[5] https://www.wired.com/story/north-korea-hacker-internet-outage/

[6] https://www.wired.com/story/north-korea-hacker-internet-outage/

[7] https://www.wired.com/story/north-korea-hacker-internet-outage/

[8] https://www.federalregister.gov/documents/2022/02/03/2022-02171/notice-of-the-establishment-of-the-cyber-safety-review-board

[9] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[10] https://www.federalregister.gov/documents/2022/02/03/2022-02171/notice-of-the-establishment-of-the-cyber-safety-review-board

[11] https://www.dhs.gov/news/2022/02/03/dhs-launches-first-ever-cyber-safety-review-board

[12] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[13] https://www.federalregister.gov/documents/2022/02/03/2022-02171/notice-of-the-establishment-of-the-cyber-safety-review-board

[14] https://www.federalregister.gov/documents/2022/02/03/2022-02171/notice-of-the-establishment-of-the-cyber-safety-review-board