K2 Intelligence
Investigations · Compliance Solutions · Cyber Defense

FINANCIAL INTEGRITY NETWORK

POLICY ALERT /// APRIL 21, 2020

DPRK Continues Expansive Sanctions Evasion and Cyber Activity

The United Nations and the United States Government have released significant reports that detail North Korea's continued efforts to engage in wide-ranging sanctions evasion activity in support of its weapons of mass destruction and ballistic missile programs.

On April 13, 2020, the United Nations Panel of Experts on North Korea (POE) released a report on North Korean sanctions evasion activity.[1] Two days later, on April 15, the U.S. Departments of State, Treasury, and Homeland Security, and the Federal Bureau of Investigation issued a DPRK Cyber Threat Advisory.[2]

The UN warns that North Korea continues to build on long-standing sanctions evasion methods and presents ongoing illicit finance challenges to the private sector and governments.

- Ship-to-ship transfers continue to support natural resources trade between the DPRK and entities in countries like Russia and China. The POE report identifies several vessels engaged in this activity and recommends their designation.

- North Korean entities exploit jurisdictions where company formation rules allow a low degree of financial transparency. North Korean front and shell companies engage in business operations in numerous countries, including: Bulgaria, Nepal, Hong Kong, and mainland China.

- North Korean commercial and banking agents, including sanctioned persons, travel freely in many jurisdictions, including mainland China, Libya, Syria, Vietnam, Iran, and Lebanon.

- North Korea supplements its activities by relying on its diplomatic representatives to gain access to financial services.

The POE report advises that the private sector and governments should guard against this illicit activity by taking a number of important steps.

- Both the private sector and governments should continue to exercise vigilance around the creation of joint ventures and cooperative entities between North

Korean-linked individuals and companies and individuals and companies located in their respective jurisdictions.

- Financial institutions should screen their customers and transactions against those vessels or entities identified in the POE report and determine the best corrective action to take. Such steps include:
    - Exiting them as a customer;
    - Putting into place extensive controls; and
    - Revising know-your-customer or customer due diligence policies.
- Financial institutions should ensure that North Korean diplomats and their families are not using their official status to gain access to bank accounts.
- Jurisdictions should augment the ability of their private sectors to effectively respond to the illicit finance threat from North Korea.
    - Countries should expand financial transparency measures to require the collection of beneficial ownership information for corporate entities and establish regulations that allow for the prompt imposition of targeted financial sanctions against entities the United Nations Security Council designates.[3]

Both the POE report and the DPRK Cyber Threat Advisory highlight how, as international sanctions have put pressure on its revenue streams, North Korea has expanded its cyber activities, including offensive operations to steal financial resources and the use of front entities that offer information technology services for hire to companies and individuals around the world. North Korea continues to grow increasingly sophisticated in the cyber domain:

- North Korea's hacking capabilities allow it to steal financial resources from central banks, financial institutions, and virtual currency exchanges and users. Previous UN reports state that Pyongyang's cybercrime capabilities have generated up to $2 billion in total revenue through August 2019.[4]
- North Korea's hackers have pursued extortion schemes, through which they hold personal or corporate data hostage in exchange for money, often paid out in virtual currency to obscure the money trail.

- Although the nature of the cyber activities often means attribution of specific attacks is difficult, the U.S. government estimates North Korea's hack of the SWIFT system allowed it to steal $81 million from the Central Bank of Bangladesh.

- In March 2020, according to a Department of Justice complaint, two Chinese hackers stole upwards of $250 million from the exploitation of a cryptocurrency exchange. (Appendix 1, below, lists recent episodes of DPRK Cyber Activity.)

- DPRK-linked hacking groups have frequently hired out their expertise to third parties who utilize their criminal skills in hacking for pay schemes.

- DPRK-affiliated information technology workers living abroad have offered their freelance skills to legitimate clients through pay-per-project websites and applications in other countries, including the United States and Canada.[5]

The POE report and the DPRK Cyber Threat Advisory recommend the private sector and governments take additional action to harden their systems from DPRK attack.

- Businesses should increase the strength of their cybersecurity measures in light of the advanced capabilities of North Korean-linked actors. Such strategies include network and data segmentation and backup, awareness training of common email compromise and related social engineering techniques, and developing incident response plans.

- Jurisdictions should bolster their anti-money laundering, countering the financing of terrorism, and counter-proliferation financing laws and regulations, particularly pertaining to supervision of virtual currency providers.

    - Special attention should be paid to the Financial Action Task Force's Guidance on Virtual Assets.[6] Where those laws and regulations are lacking, jurisdictions should move swiftly to adopt and implement relevant laws and legislation. Such improvements will provide a strong framework for private sector actors to pursue innovations in financial services while protecting themselves from exploitation.

- Jurisdictions should establish information-sharing mechanisms such that private sector actors can safely share threat intelligence and leads on DPRK-linked cyberactivity.
    - The U.S. Cybersecurity Information Sharing Act of 2015 allows private sector actors to share sensitive information with the federal government about threat indicators and defensive measures without fears that such information will lead to legal liability or be disclosed to the public (such as through a Freedom of Information Act request, for example).

K2 Intelligence
Investigations · Compliance Solutions · Cyber Defense

FINANCIAL INTEGRITY NETWORK

Appendix 1: Recent Episodes of DPRK Cyber Activity

Target	Hacking Methods Used	What was Stolen	Additional Sources
Virtual Currency Exchange Hack **(April 2018)**	• Initial entry methodology not disclosed • The initial proceeds were laundered through hundreds of virtual currency transactions to prevent asset tracking and recovery	• $250 million	DOJ Indictment
WannaCry 2.0 **(May 2017)**	• Email and network delivery of ransomware (spearphishing) • Self-propagating worm, spread through local area network and regular internet connects	• Full scale of ransom payments will not likely ever be known • Individual ransom payments were made in Bitcoin, and then converted into Monero. • WannaCry 2.0 disrupted critical business operations, including for critical infrastructure, such as the UK National Health Service	DOJ Criminal Complaint DHS CISA Advisory
FASTCash Campaign **(2016 – present)**	• Remote compromise of payment servers • Hackers were able to approve fraudulent ATM withdrawal requests	• U.S. Government estimates amount stolen in the hundreds of millions of dollars	DHS CISA Advisory
Central Bank of Bangladesh **(February 2016)**	• Email delivery of malware (spearphishing; business email compromise) • Hackers leveraged network access to send fraudulent SWIFT messages to Federal Reserve Bank of New York	• $81 million	DOJ Criminal Complaint
Sony Pictures **(November 2014)**	• Email delivery of malware (spearphishing; business email compromise)	• Personal and commercial data, including employee emails • Damage to computers and network infrastructure	FBI Advisory

[1] United Nations Security Council, Report of the Panel of Experts established pursuant to resolution 1874 (2009), (April 13, 2020), available at https://s.wsj.net/public/resources/documents/unpanelofexperts.pdf?mod=article_inline

[2] United States Department of State, United States Department of the Treasury, United States Department of Homeland Security, and the Federal Bureau of Investigation, DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat, (April 15, 2020), available at https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_cyber_threat_advisory_20200415.pdf

[3] See especially FATF Recommendations 7 (targeted financial sanctions related to proliferation), 24 (transparency and beneficial ownership of legal persons) and 25 (transparency and beneficial ownership of legal arrangements). Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations, (February 16, 2012, as amended June 2019), available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[4] United Nations Security Council, Report of the Panel of Experts established pursuant to resolution 1874 (2009), (August 30, 2019), available at https://undocs.org/S/2019/691.

[5] The United Nations Panel of Experts relays a U.N. Member State's estimate that North Korea has dispatched at least 1,000 information technology workers abroad to generate revenue for the regime, which the Report estimates comes to about $20 million per year. Further information about North Korea's cyber capabilities can be found at Mathew Ha and David Maxwell, Kim Jong Un's 'All-Purpose Sword': North Korean Cyber-Enabled Economic Warfare, Foundation for Defense of Democracies (October 2018), available at https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf.

[6] Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Assets Service Providers, (June 21, 2019), available at https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.