WINSTON & STRAWN LLP

BLOG

DPRK Cyber Threat Advisory Summary

APRIL 17, 2020

On April 15, 2020, the U.S. Departments of State, the Treasury, Homeland Security, and the Federal Bureau of Investigation (FBI) issued the DPRK Cyber Threat Advisory to serve as a resource on managing the cyber threat posed by North Korea (DPRK). The advisory warns that the DPRK's cyber activities pose a significant threat to both the United States and the international community in terms of financial stability. The DPRK relies on cybercrime and other illicit activities to generate revenue for weapons of mass destruction and ballistic missile programs. The Advisory also provides specific examples of illicit activity and recommends mitigating procedures for governments and financial institutions, alike.

This advisory highlights how important the U.S. government considers financial institutions, money services business, and other institutions are in protecting national security. It also shows the clear expectation by the U.S. government that these institutions maintain strong and robust cyber-security systems that can protect data and day-to-day operations and programs that are sophisticated enough to be able to detect sanctions evasion tactics, financial fraud-related activities, and complex illicit activity schemes that may involve North Korean actors.

One of the United States' main concerns is North Korea's malicious cyber capabilities, given the code name "HIDDEN COBRA." The DPRK is capable of conducting disruptive, destructive, and destabilizing cyber activities aimed at financial institutions, critical U.S. infrastructure, and the international community. This advisory urges the international community to stay vigilant and work together to mitigate North Korea's cyber threat.

DPRK's Malicious Cyber Activities Targeting the Financial Sector

DPRK cyber actors primarily target financial institutions, digital currency exchanges, money services business, and foreign media companies through the development and deployment of a wide range of malware tools around the world. Common tactics include:

- cyber-enabled financial theft and money laundering across various jurisdictions and currency exchanges;
- extortion campaigns – threatening to shut down entities unless paid a ransom and sometimes under the guise of long-term paid consulting arrangements; and

- “cryptojacking” – schemes that compromises a victim machine and steals its computing resources to mine digital currency through North Korean servers.

The DPRK uses these activities to both evade sanctions and generate revenue.

Cyber Operations Publicly Attributed to DPRK by U.S. Government

DPRK has repeatedly targeted the U.S. along with other government, military, and private networks to steal data and disrupt or destroy cyber activities. Amongst the most recent cyber incidents attributed to DPRK state-sponsored hackers include:

- an attack on *Sony Pictures* in 2014 in retaliation to the release of the movie “The Interview”;
- a 2016 attempt to steal at least $1 billion from institutions around the world and an alleged theft of $81 million from Bangladesh Bank through unauthorized transactions on the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network;
- the infection of hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries through the use of the *WannaCry 2.0* malware for Bitcoin ransom payments;
- a fraudulent ATM cash withdrawal scheme – The FASTCash Campaign – which remotely compromise payment switch application servers within banks to facilitate fraudulent transactions resulting in the theft of tens of millions of dollars from ATMs in Asia and Africa; and
- a digital currency exchange hack on April 2018 in which DPRK state-sponsored cyber actors hacked into a digital currency exchange and stole nearly $250 million worth of digital currency and laundered the stolen assets through hundreds of automated digital currency transactions, to obfuscate the origins of the funds.

Measures to Counter the DPRK Cyber Threat

The advisory urges governments, industry, civil society, and individuals to take the following countermeasures.

- Raise awareness of the DPRK cyber threat to promote adoption and implementation of appropriate preventive and risk mitigation measures.
- Share technical information at the national and international level to detect and defend against DPRK cyber threats. Persons should look at the provisions of the Cybersecurity Information Sharing Act of 2015; non-federal entities may share cyber threat indicators and defensive measures related to HIDDEN COBRA with federal and non-federal entities.
- Implement and promote cybersecurity best practices. Financial institutions – including money services businesses – should, for example, share threat information through government and industry channels, regularly backup data, undertake awareness training on common social engineering tactics, implement policies on information sharing and network access, and develop response plans for cyber incidents.
    i. The Department of Energy’s Cybersecurity Capability Maturity Model (C2M2) and the National Institute of Standards and Technology’s Cybersecurity Framework provide guidance on developing and implementing robust cybersecurity practices. Both the C2M2 and the Cybersecurity Framework help organizations evaluate, prioritize, and improve their own cybersecurity capabilities based on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate. They also take “a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks.”

- Notify law enforcement in a timely fashion. The advisory highlights that "all types of financial institutions, including money services businesses, are encouraged to cooperate on the front end by complying with U.S. law enforcement requests for information regarding these cyber threats, and on the back end by identifying forfeitable assets upon receipt of a request from U.S. law enforcement or U.S. court orders and by cooperating with U.S. law enforcement to support the seizure of such assets".
- Strengthen anti-money laundering (AML) / countering the financing of terrorism (CFT) / counter-proliferation financing (CPF) compliance by:
  i. implementing the Financial Action Task Force (FATF) standards on AML/CFT/CPF;
  ii. ensuring financial institutions and other covered entities employ risk- mitigation measures in line with the FATF standards and FATF public statements and guidance;
  iii. giving special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf;
  iv. closing existing branches, subsidiaries, and representative offices of DPRK banks within their territories and terminating correspondent relationships with DPRK banks;
  v. regulating and supervising digital asset service providers, including digital currency exchanges;
  vi. mitigating against risks when engaging in digital currency transactions;
  vii. monitoring changes in customers' activities, particularly digital asset service providers, for potential indicators of money laundering, terrorist financing, and proliferation financing facilitation;
  viii. ensuring U.S. financial institutions, including foreign-located digital asset service providers doing business in whole or substantial part in the United States, and other covered businesses and persons comply with their regulatory obligations under the Bank Secrecy Act (BSA);
  ix. identifying and reporting suspicious transactions, including those conducted, affected, or facilitated by cyber events or illicit finance involving digital assets, in suspicious activity reporting to FinCEN.
- Engage in International Cooperation.

Consequences of Engaging in Prohibited or Sanctionable Conduct

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has the authority to impose sanctions on any person determined to have, among other things:

- engaged in significant activities undermining cyber security on behalf of the Government of North Korea or the Workers' Party of Korea;
- operated in the information technology (IT) industry in North Korea;
- engaged in certain other malicious cyber-enabled activities; or
- engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology.

Additionally, if the Secretary of the Treasury, in consultation with the Secretary of State, determines that a foreign financial institution has knowingly conducted or facilitated significant trade with North Korea or knowingly conducted or facilitated a significant transaction on behalf of a person designated under a North Korea-related Executive Order, or under Executive Order 13382 – Weapons of Mass Destruction Proliferators and Their Supporters – for North Korea-related activity, that institution may lose the ability to maintain a correspondent or payable-through account in the United States.

The DPRK-related UN Security Council resolutions (UNSCRs) also provide various mechanisms for encouraging compliance with DPRK-related sanctions imposed by the UN. For example, the UN Security Council 1718 Committee

may impose targeted sanctions on any individual or entity who engages in a business transaction with UN-designated entities or sanctions evasion.

Persons who willfully violate applicable sanctions laws may face up to 20 years of imprisonment, fines of up to $1 million or totaling twice the gross gain, whichever is greater, and forfeiture of all funds involved in such transactions. Persons who willfully violate the BSA may face up to 5 years' imprisonment, a fine of up to $250,000, and potential forfeiture of property involved in the violations. Further, the Secretary of the Treasury or the Attorney General may subpoena a foreign financial institution that maintains a correspondent bank account in the United States for records stored overseas. If the foreign financial institution fails to comply with the subpoena, the U.S. financial institution must terminate the correspondent banking relationship within 10 business days. Failure to do so may subject the U.S. financial institutions to daily civil penalties.

Conclusion

This advisory highlights the increasing importance for financial institutions, money services business, and other institutions to not only maintain strong and robust cyber-security systems that can protect data and day-to-day operations but to ensure that their compliance programs are sophisticated enough to be able to detect sanctions-evasion tactics, financial fraud-related activities, and complex illicit-activity schemes that may involve North Korean actors. In order to be able to protect against sophisticated cyber-crimes, a financial institution should have an integrated compliance program addressing cyber-security, AML, sanctions, export controls, fraud, and anti-corruption/anti-bribery. Independent audits and testing may help institutions identify weak areas in their programs and implement the necessary measures to enhance its program. It is also important for institutions to conduct enhanced due diligence on any party the institution identifies as operating in an abnormal manner.

"If you have additional questions or need further assistance, please reach out to Cari Stinebower (Cstinebower@winston.com) or your Winston relationship attorney."
7 Min Read

Author

Cari Stinebower

Related Locations

Washington, DC

Related Capabilities

Privacy & Data Security | International Trade | Maritime & Admiralty | Technology, Media & Telecommunications | Financial Services

Related Regions

Middle East & Africa

Related Professionals

Cari Stinebower

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.