WINSTON & STRAWN LLP

BLOG

Government Issues North Korea Cyber Threat Advisory

APRIL 20, 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 relating to North Korea (DPRK). The DPRK relies on cybercrime and other illicit activities to generate revenue for weapons of mass destruction and ballistic missile programs.

The Government has expressed concern about North Korea's malicious cyber capabilities, given the code name "HIDDEN COBRA." 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 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.

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

Share technical information at the national and international level to detect and defend against DPRK cyber threats. The Cybersecurity Information Sharing Act of 2015 provides that 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.

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 the Compliance program. Companies should have an integrated compliance program, which implements anti-money laundering (AML), countering the financing of terrorism (CFT), counter-proliferation financing (CPF) compliance, Financial Action Task Force (FATF) standards on AML/CFT/CPF.

Read Winston & Strawn's Global Trade & Foreign Policy Insights blog post for more on this topic.

TIP: To ensure they can protect against sophisticated cyber-crimes, financial institutions should have an integrated compliance program addressing cyber-security, AML, sanctions, export controls, fraud, and anti-corruption/anti-bribery.

3 Min Read

Author

Cari Stinebower

Related Locations

Houston | Washington, DC

Related Topics

Asia Privacy | Data Breach

Related Capabilities

Privacy & Data Security | Compliance Programs | Financial Services

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.