CYBERSECURITY ADVISORY

Guidance on the North Korean Cyber Threat

Last Revised: June 23, 2020 **Alert Code:** AA20-106A

Summary

The U.S. Departments of State, the Treasury, and Homeland Security, and the Federal Bureau of Investigation are issuing this advisory as a comprehensive resource on the North Korean cyber threat for the international community, network defenders, and the public. The advisory highlights the cyber threat posed by North Korea – formally known as the Democratic People's Republic of Korea (DPRK) – and provides recommended steps to mitigate the threat. In particular, Annex 1 lists U.S. government resources related to DPRK cyber threats and Annex 2 includes a link to the UN 1718 Sanctions Committee (DPRK) Panel of Experts reports.

The DPRK's malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial system. Under the pressure of robust U.S. and UN sanctions, the DPRK has increasingly relied on illicit activities – including cybercrime – to generate revenue for its weapons of mass destruction and ballistic missile programs. In particular, the United States is deeply concerned about North Korea's malicious cyber activities, which the U.S. government refers to as HIDDEN COBRA. The DPRK has the capability to conduct disruptive or destructive cyber activities affecting U.S. critical infrastructure. The DPRK also uses cyber capabilities to steal from financial institutions, and has demonstrated a pattern of disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace.

The United States works closely with like-minded countries to focus attention on and condemn the DPRK's disruptive, destructive, or otherwise destabilizing behavior in cyberspace. For example, in December 2017, Australia, Canada, New Zealand, the United States, and the United Kingdom publicly attributed the WannaCry 2.0 ransomware attack to the DPRK and denounced the DPRK's harmful and irresponsible cyber activity. Denmark and Japan issued supporting statements for the joint denunciation of the destructive WannaCry 2.0 ransomware attack, which affected hundreds of thousands of computers around the world in May 2017.

It is vital for the international community, network defenders, and the public to stay vigilant and to work together to mitigate the cyber threat posed by North Korea.

Click here <https://www.us-cert.gov/sites/default/files/2020-04/dprk_cyber_threat_advisory_04152020_s508c.pdf> for an English PDF version of this report.

Click the following links for PDF versions of this report in Arabic <https://www.us-cert.gov/sites/default/files/publications/dprk_cyber_advisory_ara_s508c.pdf>, French <https://www.us-cert.gov/sites/default/files/publications/dprk_cyber_advisory_fre_s508c.pdf>, Japanese <//www.us-cert.gov/sites/default/files/publications/dprk_cyber_advisory_jpn_s508c.pdf>, Korean <https://www.us-

cert.gov/sites/default/files/publications/dprk_cyber_advisory_kor_s508c.pdf>, Portuguese <https://www.us-cert.gov/sites/default/files/publications/dprk_cyber_advisory_por_s508c.pdf>, Spanish <https://www.us-cert.gov/sites/default/files/publications/dprk_cyber_advisory_spa_s508c.pdf>, and traditional Chinese <https://www.us-cert.gov/sites/default/files/publications/dprk_cyber_advisory_tradchn_s508c.pdf>, and Vietnamese </sites/default/files/publications/dprk_cyber_advisory_vie_s508c.pdf>.

Technical Details

DPRK's Malicious Cyber Activities Targeting the Financial Sector

Many DPRK cyber actors are subordinate to UN- and U.S.-designated entities, such as the Reconnaissance General Bureau. DPRK state-sponsored cyber actors primarily consist of hackers, cryptologists, and software developers who conduct espionage, cyber-enabled theft targeting financial institutions and digital currency exchanges, and politically-motivated operations against foreign media companies. They develop and deploy a wide range of malware tools around the world to enable these activities and have grown increasingly sophisticated. Common tactics to raise revenue illicitly by DPRK state-sponsored cyber actors include, but are not limited to:

Cyber-Enabled Financial Theft and Money Laundering. The UN Security Council 1718 Committee Panel of Experts' 2019 mid-term report (2019 POE mid-term report) states that the DPRK is increasingly able to generate revenue notwithstanding UN Security Council sanctions by using malicious cyber activities to steal from financial institutions through increasingly sophisticated tools and tactics. The 2019 POE mid-term report notes that, in some cases, these malicious cyber activities have also extended to laundering funds through multiple jurisdictions. The 2019 POE mid-term report mentions that it was investigating dozens of suspected DPRK cyber-enabled heists and that, as of late 2019, the DPRK has attempted to steal as much as $2 billion through these illicit cyber activities. Allegations in a March 2020 Department of Justice forfeiture complaint are consistent with portions of the POE's findings. Specifically, the forfeiture complaint alleged

how North Korean cyber actors used North Korean infrastructure in furtherance of their conspiracy to hack digital currency exchanges, steal hundreds of millions of dollars in digital currency, and launder the funds.

Extortion Campaigns. DPRK cyber actors have also conducted extortion campaigns against third-country entities by compromising an entity's network and threatening to shut it down unless the entity pays a ransom. In some instances, DPRK cyber actors have demanded payment from victims under the guise of long-term paid consulting arrangements in order to ensure that no such future malicious cyber activity takes place. DPRK cyber actors have also been paid to hack websites and extort targets for third-party clients.

Cryptojacking. The 2019 POE mid-term report states that the POE is also investigating the DPRK's use of "cryptojacking," a scheme to compromise a victim machine and steal its computing resources to mine digital currency. The POE has identified several incidents in which computers infected with cryptojacking malware sent the mined assets – much of it anonymity-enhanced digital currency (sometimes also referred to as "privacy coins") – to servers located in the DPRK, including at Kim Il Sung University in Pyongyang.

These activities highlight the DPRK's use of cyber-enabled means to generate revenue while mitigating the impact of sanctions and show that any country can be exposed to and exploited by the DPRK. According to the 2019 POE mid-term report, the POE is also investigating such activities as attempted violations of UN Security Council sanctions on t DPRK.

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

The DPRK has repeatedly targeted U.S. and other government and military networks, as well as networks related to private entities and critical infrastructure, to steal data and conduct disruptive and destructive cyber activities. To date, the U.S. government has publicly attributed the following cyber incidents to DPRK state-sponsored cyber actors and co-conspirators:

- **Sony Pictures.** In November 2014, DPRK state-sponsored cyber actors allegedly launched a cyber attack on Sony Pictures Entertainment (SPE) in retaliation for the 2014 film "The Interview." DPRK cyber actors hacked into SPE's network to steal confidential data, threatened SPE executives and employees, and damaged thousands of computers.
  - FBI's Update on Sony Investigation (Dec. 19, 2014) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>
  - DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>
- **Bangladesh Bank Heist.** In February 2016, DPRK state-sponsored cyber actors allegedly attempted to steal at least $1 billion from financial institutions across the world and allegedly stole $81 million from the Bangladesh Bank through unauthorized transactions on the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network. According to the complaint, DPRK cyber actors accessed the Bangladesh Bank's computer terminals that interfaced with the SWIFT network after compromising the bank's computer network via spear phishing emails targeting bank employees. DPRK cyber actors then sent fraudulently authenticated SWIFT messages directing the Federal Reserve Bank of New York to transfer funds out of the Banglades Bank's Federal Reserve account to accounts controlled by the conspirators.
  - DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>

- **WannaCry 2.0.** DPRK state-sponsored cyber actors developed the ransomware known as WannaCry 2.0, as well as two prior versions of the ransomware. In May 2017, WannaCry 2.0 ransomware infected hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries. WannaCry 2.0 ransomware encrypts an infected computer's data and allows the cyber actors to demand ransom payments in the Bitcoin digital currency. The Department of the Treasury designated one North Korean computer programmer for his part in the WannaCry 2.0 conspiracy, as well as his role in the Sony Pictures cyber attack and Bangladesh Bank heist, and additionally designated the organization he worked for.

  - CISA's Technical Alert: Indicators Associated with WannaCry Ransomware (May 12, 2017) https://www.us-cert.gov/ncas/alerts/TA17-132A <https://www.us-cert.gov/ncas/alerts/ta17-132a>
  - White House Press Briefing on the Attribution of WannaCry Ransomware (Dec. 19, 2017) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
  - DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>
  - Treasury Targets North Korea for Multiple Cyber-Attacks (Sept. 6, 2018) https://home.treasury.gov/news/press-releases/sm473 <https://home.treasury.gov/news/press-releases/sm473>

- **FASTCash Campaign.** Since late 2016, DPRK state-sponsored cyber actors have employed a fraudulent ATM cash withdrawal scheme known as "FASTCash" to steal tens of millions of dollars from ATMs in Asia and Africa. FASTCash schemes remotely compromise payment switch application servers within banks to facilitate fraudulent transactions. In one incident in 2017, DPRK cyber actors enabled the withdrawal of cash simultaneously from ATMs located in more than 30 different countries. In another incident in 2018, DPRK cyber actors enabled cash to be simultaneously withdrawn from ATMs in 23 different countries.

  - CISA's Alert on FASTCash Campaign (Oct. 2, 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A <https://www.us-cert.gov/ncas/alerts/ta18-275a>
  - CISA's Malware Analysis Report: FASTCash-Related Malware (Oct. 2, 2018) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A <https://www.us-cert.gov/ncas/analysis-reports/ar18-275a>

- **Digital Currency Exchange Hack.** As detailed in allegations set forth in a Department of Justice complaint for forfeiture in rem, in April 2018, DPRK state-sponsored cyber actors hacked into a digital currency exchange and stole nearly $250 million worth of digital currency. The complaint further described how the stolen assets were laundered through hundreds of automated digital currency transactions, to obfuscate the origins of the funds, in an attempt to prevent law enforcement from tracing the assets. Two Chinese nationals are alleged in the complaint to have subsequently laundered the assets on behalf of the North Korean group, receiving approximately $91 million from DPRK-controlled accounts, as well as an additional $9.5 million from a hack of another exchange. In March 2020, the Department of the Treasury designated the two individuals under cyber and DPRK sanctions authorities, concurrent with a Department of Justice announcement that the individuals had been previously indicted on money laundering and unlicensed money transmitting charges and that 113 digital currency accounts were subject to forfeiture.

  - Treasury's Sanctions against Individuals Laundering Cryptocurrency for Lazarus Group (March 2, 2020) https://home.treasury.gov/news/press-releases/sm924 <https://home.treasury.gov/news/press-releases/sm924>
  - DOJ's Indictment of Two Chinese Nationals Charged with Laundering Cryptocurrency from Exchange Hack and Civil Forfeiture Complaint (March 2, 2020) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>

Mitigations

Measures to Counter the DPRK Cyber Threat

North Korea targets cyber-enabled infrastructure globally to generate revenue for its regime priorities, including its weapons of mass destruction programs. We strongly urge governments, industry, civil society, and individuals to take all relevant actions below to protect themselves from and counter the DPRK cyber threat:

- **Raise Awareness of the DPRK Cyber Threat.** Highlighting the gravity, scope, and variety of malicious cyber activities carried out by the DPRK will raise general awareness across the public and private sectors of the threat and promote adoption and implementation of appropriate preventive and risk mitigation measures.
- **Share Technical Information of the DPRK Cyber Threat.** Information sharing at both the national and international levels to detect and defend against the DPRK cyber threat will enable enhanced cybersecurity of networks and systems. Best practices should be shared with governments and the private sector. Under the provisions of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. §§ 1501–1510), 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.** Adopting measures – both technical and behavioral – to enhance cybersecurity will make U.S. and global cyber infrastructure more secure and resilient. Financial institutions, including money services businesses, should take independent steps to protect against malicious DPRK cyber activities. Such steps may include, but are not limited to, sharing threat information through government and/or industry channels, segmenting networks to minimize risks, maintaining regular backup copies of data, undertaking awareness training on common social engineering tactics, implementing policies governing information sharing and network access, and developing cyber incident response plans. The Department of Energy's Cybersecurity Capability Maturity Model and the National Institute of Standards and Technology's Cybersecurity Framework provide guidance on developing and implementing robust cybersecurity practices. As shown i Annex I, the Cybersecurity and Infrastructure Security Agency (CISA) provides extensive resources, including technical alerts and malware analysis reports, to enable network defenders to identify and reduce exposure to malicious cyber activities.

- **Notify Law Enforcement.** If an organization suspects that it has been the victim of malicious cyber activity, emanating from the DPRK or otherwise, it is critical to notify law enforcement in a timely fashion. This not only can expedite the investigation, but also, in the event of a financial crime, can increase the chances of recovering any stolen assets.

  U.S. law enforcement has seized millions of dollars' worth of digital currency stolen by North Korean cyber actors. 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**. Countries should swiftly and effectively implement the Financial Action Task Force (FATF) standards on AML/CFT/CPF. This includes ensuring financial institutions and other covered entities employ risk mitigation measures in line with the FATF standards and FATF public statements and guidance. Specifically, the FATF has called for all countries to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the DPRK.[1] <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html> This includes advising all financial institutions and other covered entities to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf. In line with UN Security Council Resolution 2270 Operative Paragraph 33, Member States should close existing branches, subsidiaries, and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks.

Further, in June 2019, FATF amended its standards to require all countries regulate and supervise digital asset service providers, including digital currency exchanges, and mitigate against risks when engaging in digital currency transactions. Digital asset service providers should remain alert to changes in customers' activities, as their business may be used to facilitate money laundering, terrorist financing, and proliferation financing. The United States is particularly concerned about platforms that provide anonymous payment and account service functionality without transaction monitoring, suspicious activity reporting, and customer due diligence, among other obligations.

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 should ensure that they comply with their regulatory obligations under the Bank Secrecy Act (as implemented through the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) regulations in 31 CFR Chapter X). For financial

institutions, these obligations include developing and maintaining effective anti-money laundering programs that are reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities, as well as 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.

International Cooperation

To counter the DPRK's malicious cyber activities, the United States regularly engages with countries around the world to raise awareness of the DPRK cyber threat by sharing information and evidence via diplomatic, military, law enforcement and judicial, network defense, and other channels. To hamper the DPRK's efforts to steal funds through cyber means and to defend against the DPRK's malicious cyber activities, the United States strongly urges countries to strengthen network defense, shutter DPRK joint ventures in third countries, and expel foreign-located North Korean information technology (IT) workers in a manner consistent with applicable international law. A 2017 UN Security Council resolution required all Member States to repatriate DPRK nationals earning income abroad, including IT workers, by December 22, 2019. The United States also seeks to enhance the capacity of foreign governments and the private sector to understand, identify, defend against, investigate, prosecute, and respond to DPRK cyber threats and participate in international efforts to help ensure the stability of cyberspace.

Consequences of Engaging in Prohibited or Sanctionable Conduct

Individuals and entities engaged in or supporting DPRK cyber-related activity, including processing related financial transactions, should be aware of the potential consequences of engaging in prohibited or sanctionable conduct.

The 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 cybersecurity 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, among other potential restrictions, lose the ability to maintain a correspondent or payable-through account in the United States.

OFAC investigates apparent violations of its sanctions regulations and exercises enforcement authority, as outlined in the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, appendix A. Persons who violate the North Korea Sanctions Regulations, 31 C.F.R. part 510, may face civil monetary penalties of up to the greater of the applicable statutory maximum penalty or twice the value of the underlying transaction.

The 2019 POE mid-term report notes the DPRK's use, and attempted use, of cyber-enabled means to steal funds from banks and digital currency exchanges could violate multiple UN Security Council resolutions (UNSCRs) (i.e., UNSCR 1718 operative paragraph (OP) 8(d); UNSCR 2094, OPs 8 and 11; and UNSCR 2270, OP 32). The DPRK-related 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 (i.e., an asset freeze and, for individuals, a travel ban) on any individual or entity who engages in a business transaction with UN-designated entities or sanctions evasion.

The Department of Justice criminally prosecutes willful violations of applicable sanctions laws, such as the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 et seq. Persons who willfully violate such 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. The Department of Justice also criminally prosecutes willful violations of the Bank Secrecy Act (BSA), 31 U.S.C. §§ 5318 and 5322, which requires financial institutions to, among other things, maintain effective anti-money laundering programs and file certain reports with FinCEN. Persons violating 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. Where appropriate, the Department of Justice will also criminally prosecute corporations and other entities that violate these statutes. The Department of Justice also works with foreign partners to share evidence in support of each other's criminal investigations and prosecutions.

Pursuant to 31 U.S. Code § 5318(k), 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. Where the Secretary of the Treasury or Attorney General provides written notice to a U.S. financial institution that a foreign financial institutions has failed to comply with such a subpoena, the U.S. financial institution must terminate the correspondent banking relationship within ten business days. Failure to do so may subject the U.S. financial institutions to daily civil penalties.

DPRK Rewards for Justice

If you have information about illicit DPRK activities in cyberspace, including past or ongoing operations, providing such information through the Department of State's Rewards for Justice program could make you eligible to receive an award of up to $5 million. For further details, please visit www.rewardsforjustice.net <http://www.rewardsforjustice.net>.

ANNEX I: USG Public Information on and Resources to Counter the DPRK Cyber Threat

Office of the Director of National Intelligence Annual Worldwide Threat Assessments of the U.S. Intelligence Community. In 2019, the U.S. Intelligence Community assessed that the DPRK poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks. The DPRK continues to use cyber capabilities to steal from financial institutions to generate revenue. Pyongyang's cybercrime operations include attempts to steal more than $1.1 billion from financial institutions across the world – including a successful cyber heist of an estimated $81 million from Bangladesh Bank. The report can be found at https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Cybersecurity and Infrastructure Security Agency (CISA) Technical Reports. The U.S. government refers to the malicious cyber activities by the DPRK as HIDDEN COBRA. HIDDEN COBRA reports provide technical details on the tools and infrastructure used by DPRK cyber actors. These reports enable network defenders to identify and reduce exposure to the DPRK's malicious cyber activities. CISA's website contains the latest updates on these persistent threats: https://www.us-cert.gov/northkorea <https://www.us-cert.gov/northkorea>.

Additionally, CISA provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management and puts it into practice to protect the nation's critical functions. Below are the links to CISA's resources:

- Protecting Critical Infrastructure: https://www.cisa.gov/protecting-critical-infrastructure <https://www.cisa.gov/protecting-critical-infrastructure>
- Cyber Safety: https://www.cisa.gov/cyber-safety <https://www.cisa.gov/cyber-safety>
- Detection and Prevention: https://www.cisa.gov/detection-and-prevention <https://www.cisa.gov/detection-and-prevention>
- Information Sharing: https://www.cisa.gov/information-sharing-and-awareness <https://www.cisa.gov/information-sharing-and-awareness>

- CISA Insights: https://www.cisa.gov/insights <https://www.cisa.gov/insights>
- Combating Cyber Crime: https://www.cisa.gov/combating-cyber-crime <https://www.cisa.gov/combating-cyber-crime>
- Cyber Essentials: https://www.cisa.gov/cyber-essentials <https://www.cisa.gov/cyber-essentials>
- Tips: https://www.us-cert.gov/ncas/tips <https://www.us-cert.gov/ncas/tips>
- National Cyber Awareness System: https://www.us-cert.gov/ncas <https://www.us-cert.gov/ncas>
- Industrial Control Systems Advisories: https://www.us-cert.gov/ics <https://www.us-cert.gov/ics>
- Report Incidents, Phishing, Malware, and Vulnerabilities: https://www.us-cert.gov/report <https://www.us-cert.gov/report>

FBI PIN and FLASH Reports. FBI Private Industry Notifications (PIN) provide current information that will enhance the private sector's awareness of a potential cyber threat. FBI Liaison Alert System (FLASH) reports contain critical information collected by the FBI for use by specific private sector partners. They are intended to provide recipients with actionable intelligence that help cybersecurity professionals and system administrators to guard against the persistent malicious actions of cyber criminals. If you identify any suspicious activity within your enterprise or have related information, please contact FBI CYWATCH immediately. For DPRK-related cyber threat PIN or FLASH reports, contact cywatch@fbi.gov.

- FBI Cyber Division: https://www.fbi.gov/investigate/cyber <https://www.fbi.gov/investigate/cyber>

FBI Legal Attaché Program: The FBI Legal Attaché's core mission is to establish and maintain liaison with principal law enforcement and security services in designated foreign countries.

- https://www.fbi.gov/contact-us/legal-attache-offices <https://www.fbi.gov/contact-us/legal-attache-offices>

U.S. Cyber Command Malware Information Release. The Department of Defense's cyber forces actively seek out DPRK malicious cyber activities, including DPRK malware that exploits financial institutions, conducts espionage, and enables malicious cyber activities against the U.S. and its partners. U.S. Cyber Command periodically releases malware information, identifying vulnerabilities for industry and government to defend their infrastructure and networks against DPRK illicit activities. Malware information to bolster cybersecurity can be found at the following Twitter accounts: @US_CYBERCOM and @CNMF_VirusAlert.

U.S. Department of the Treasury Sanctions Information and Illicit Finance Advisories. ***The Office of Foreign Assets Control's (OFAC's)*** online Resource Center provides a wealth of information regarding DPRK sanctions and sanctions with respect to malicious cyber-enabled activities, including sanctions advisories, relevant statutes, Executive Orders, rules, and regulations relating to DPRK and cyber-related sanctions. OFAC has also published several frequently asked questions (FAQs) relating to DPRK sanctions, cyber-related sanctions, and digital currency. For questions or concerns related to OFAC sanctions regulations and requirements, please contact OFAC's Compliance Hotline at 1-800-540-6322 or OFAC_Feedback@treasury.gov.

- DPRK Sanctions
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx <https://www.treasury.gov/resource-center/sanctions/programs/pages/nkorea.aspx>
  - FAQs - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk <https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_other.aspx#nk>

- Malicious Cyber Activities Sanctions
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx <https://www.treasury.gov/resource-center/sanctions/programs/pages/cyber.aspx>
  - FAQs - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber <https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_other.aspx#cyber>
  - FAQs on Virtual Currency - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs <https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_compliance.aspx#vc_faqs>

Financial Crimes Enforcement Network (FinCEN) has issued an advisory on North Korea's use of the international financial system (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008 <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008>). FinCEN also issued specific advisories to financial institutions with suspicious activity reporting obligations that provide guidance on when and how to report cybercrime and/or digital currency-related criminal activity:

- Cybercrime
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005 <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005>
- Illicit digital currency activity
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003 <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003>
- Businesses e-mail compromise
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005 <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005>
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003 <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003>

Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool to help financial institutions identify their risks and determine their cybersecurity preparedness. The assessment tool can be found at https://www.ffiec.gov/cyberassessmenttool.htm <https://www.ffiec.gov/cyberassessmenttool.htm>.

ANNEX II: UN Panel of Experts Reports on the DPRK Cyber Threat

UN 1718 Sanctions Committee (DPRK) Panel of Experts Reports. The UN Security Council 1718 Sanctions Committee on the DPRK is supported by a Panel of Experts, who "gather, examine, and analyze information" from UN Member States, relevant UN bodies, and other parties on the implementation of the measures outlined in the UN Security Council Resolutions against North Korea. The Panel also makes recommendations on how to improve sanctions implementation by providing both a Midterm and a Final Report to the 1718 Committee. These reports can be found at https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>.

References

[1] FATF Call to Action on North Korea <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html>

Revisions

April 15, 2020: Initial Version|April 30, 2020: Added PDF versions of this report in Arabic, French, Japanese, Korean, Portuguese, Spanish, and traditional Chinese.|June 16, 2020: Added PDF version of this report in Vietnamese.

Tags

Nation-State Actor: North Korea

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

Give Feedback

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov