DOI: 10.53477/2668-6511-22-08

"LAZARUS" THE NORTH KOREAN HACKER GROUP

Attila GULYÁS,
Lieutenant Colonel (Retired), Ph.D. Student,
Safety and Security Sciences Doctoral School, Obuda University, Budapest, Hungary.
E-mail: gulyas.attila@Ph.D.uni-obuda.hu

Abstract: *The Democratic People's Republic of Korea (DPRK) is famous for the poverty, destitution and backwardness, however in spite of these negative features it is among the most advanced cyber warfare countries. In the daily news quite often can be read about cyber-attacks against different states, media institutions or banks where the experts assume that the DPRK supported hacker group the "LAZARUS" is behind the attacks. According to the latest news the group in connection with stealing a big amount of crypto currency and money laundering got into the limelight. The state officially denies the existence of the group however cyber analysts and security experts found direct and circumstantial evidences that prove the connection between the North Korean state and the hacker group.*

Keywords: *North Korea; Lazarus; APT; Bluenoroff; cybercrime; hacker.*

Introduction

The dissolution of the socialist world order posed a big challenge for the economy of North Korea. It lost its supporters and markets, today China is the primary trading partner of North Korea. In spite of its advantageous geographical location, and its mineral resources the economy of the country is in ruins due to the decades of mismanagement, under-investment, resource misallocation, poor maintenance and corruption. Big part of the population is continuously malnourished and live in deep poverty. The government spends up to 24 percent of the GDP on the military and military industry. The North Korean army is one of the biggest armies in number on the world with its more than million personnel, but their equipment is obsolete. The most part of the military budget spent on the nuclear and the ballistic missile programs which are condemned by the international community, except Iran. The government blackmails the international community with its nuclear program to get food and other supports from abroad. Depending on its interests it follows the international calls, and treaties or breaks the agreements. The United States declared North Korea as a rogue state in 2001, and then introduced monetary, export-import sanctions together with the United Nations to curb the North Korean nuclear and ballistic missile programs (United States Department of State, 2019).

The socialist leadership elaborated two way-outs to solve this seemingly hopeless situation. The first one is to improve the pressure on the International community with the nuclear black mailing while the second is a new cyber strategy that helps protect their cyber security and provides them with the cutting-edge technologies, and last but not least financially supports their nuclear and ballistic missile programs. They realized that the countries with high computer network and Internet penetration are vulnerable to cyber-attacks and cyber espionage. They also recognized that the cyber warfare is very cost effective because with relatively low investment the gain is high (Bartlett 2020a). The last element of their cyber strategy is similar to Queen Elizabeth's invention in the sixteenth century called „strategic crime". As is well known the Queen encouraged her piratical „Sea Dogs" to fill up her treasury (Arquilla 2021, 4).

1. The North Korean cyber organizational and the technological bases

The cyber activity of North Korea is coordinated by the Chief of Staff of Korean People's Democratic Army, Reconnaissance General Bureau (RGB), and the Korean Workers Party (Center for Strategic & International Studies 2014). According to the United States the Reconnaissance General Bureau is responsible for the cyber-attacks (Cha, & Lewis 2014, 26) that is why the paper focuses on it after presenting the technological, and educational bases of North Korea.

1.1. Industrial and technological bases

North Korea started improving its cyber capabilities in the late eighties, but the real breakthrough was in the late nineties when established the College Computer Science at Kim Il-sung University, and the Ministry of Electric Power Industry. The party leadership declared that the science technology as one of the three pillars to achieve the status as a "strong and prosperous nation." (ROK Ministry of Unification 2015). North Korea has systemically improved its IT industry focused on the software development. This technology is a very important part of the education both middle and higher level. The country has its own hardware and semiconductor development and production as well. According to South Korean police estimation approximately ten thousand IT professionals as guest workers are employed in Shenyang and Dangdong, China where they have access to the cutting edge hardware and software technologies (Seok & Sang-ki 2008, 7).

The Korea Computer Center and the Pyongyang Informatics Center are the main cores of the software and hardware developments.

In the country there are four independent intranet networks. One of them is for the military and the others are for governmental purposes. All of them are under strict control and cyber protection.

Korea Computer Center (KCC)

The Center was established in 1990. It is responsible for the research and development, and the hardware, software production. It is also supervising the IT education at university level. The center has right to trade abroad, allegedly it has subsidiaries in Germany, China, and Syria. The Center takes part in cyber-attacks and it uses its subsidiaries as cover firms (Jun et al. 2015, 54). The main profiles of their software development are Linux based operational systems. They developed the "Red Star" operational system that is North Korea's first operational system and their significant exported software solution. The KCC has more than one thousand personnel of which more than one hundred have PhD (Jun et al. 2015, 54). The organization multiple times was blamed for cyber related crimes especially in connection with South Korea. In the late nineties its employees developed illegal game exploits to popular pc games which were actually spy software solutions and these exploits were sold under false flag (pretending Chinese) in South Korea (Seok-woo 2011).

Pyongyang Informatics Center (PIC)

The PIC was established in 1986, and is located in Kyungheung-Dong, Botonggang District, Pyongyang. The Center primarily focuses on software development. It has more than 500 personnel including 180 researchers of which 30 have PhDs. The employees of the PIC developed the "Changduk" word processing software and the Dangun Korean language processing software, both are widely used in North Korea. The PIC has subsidiaries in Japan and Singapore.

The PIC was the center of the Inter-Korean IT cooperation in the early 2000s as a part of the South Korean "Sunshine Policy" which was a fruitful cooperation until the North Korean torpedo attack against the ROK Cheonan ship in March 2010. As a result of the attack the South Korean government banned all inter- Korean trade, and investment.

According to their original plans they would have produced competitive software solutions and establish a Silicon Valley like area and a software developing center in Dandong (Seongwook 2009). During the years of the cooperation the South Korean partner carried out site visitations and they concluded that the North Korean programmers were highly skilled and well ahead of the South Korean counterparts in IT security (Seunghyun 2004).

1.2. Educational basis

One of the North Korean government's priorities is the establishment of the educational basis of the cyber warfare. In order to accomplish this aim at the higher level IT educational institutes they introduced the hacker training. According to defectors reports in May 2020 the military recruited more than 100 hackers from the top science and technology universities to manage its intranet networks and tactical planning systems. One of these universities is the Kim Chaek University of Technology. Another good example is the Mirim College where more than 100 hackers graduate every year. North Korean defector reported that the students study the MS Windows operating systems, learn how to create destructive computer viruses, and code in various computer languages.

1.3 Organizational basis

Reconnaissance General Bureau

The first report on the RGB published in 2009. Analyst Joseph Bermudez describes this new organization as a new intelligence unit built of numerous special units and intelligence organizations (Bermundez 2010). These units were involved into commando, intelligence, sabotage, radio reconnaissance, and different kinds of covert actions. Until 2010 the general cyber capabilities were dispersed among different organizations and governmental agencies.

This service is responsible for all intelligence collection and covert operations, including cyber related crimes. It established companies and joint venture companies in Asia in order to cover the illicit financial operations. The Bureau in this way it tries to cloak its illicit activities including its launder money operations (Bartlett 2020a).

The next section gives an overall picture of the cyber warfare involved units of the RGB. Unfortunately, the strict censorship and the closed society make hard to get authentic information on these units, we can only refer to the open sources. It is not uncommon in the North Korean way of conspiracy that they give different names to units which has nothing to do with their original functions. Today the North Korean government command more than 6000 cyber agents through the RGB's subunits across the world - one of them is the "LAZARUS" of which activity will be discussed later in details in this study (Bartlett 2020a). The theoretical organizational chart of the RGB is can be seen on the Figure no. 1.

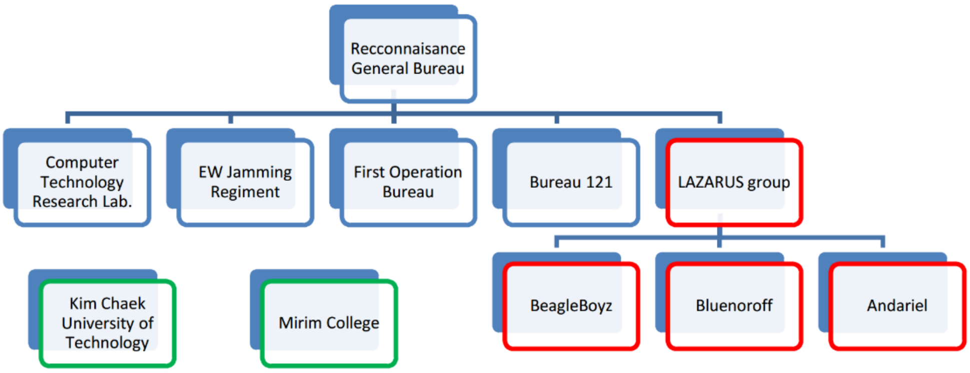

Figure no. 1: Identified North Korean Intelligence-led cyber organizations[1]

[1] Source: https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers, and complemented by the author

Bureau 121

The Bureau is the most important cyber unit of North Korea. Its mission includes offensive and defensive cyber operations, cyber espionage, network exploitation and cyber-crime. Different sources refer to it by different names such as Unit 121, Bureau 121 just to name a few. There is no available authentic open source information on its structure, or its personnel. According to North Korean defectors its new building complex was built in 2013 along with luxury apartments for the employees of the bureau in the northern part of Pyongyang (Jun et al. 2015, 41). The analysis of the satellite pictures didn't corroborate the information, but it didn't refute either, because it is not uncommon that the important objects are hidden under the surface.

Computer Technology Research Lab

It is a very interesting organization because this unit was identified that has hacking technics advanced enough to carry out attacks against South Korean financial institutes according to an open source report published in 2013 (Soonpyo Park 2013). The existence of this unit today is unknown, it may be disbanded, or merged into other units.

1st Operations Bureau or 414 Liaison Office or 128 Liaison Office

South Korean reports, and researches often refer to this organization as a major cyber unit under the RGB. In the Korean terminology the "liaison" word means support of the intelligence collection and commando actions against South Korea. This unit is responsible for the connection with the covert agents deployed abroad and it conducts surveillance on South Korean Law Enforcement Agencies (Lee 2014). Likely they develop cyber means for the cheaper and more effective information collection and for the connection with the agents. It is not unthinkable that the unit shares its cyber tools with other RGB units. Yet, it seems that major unit is an overstatement.

2. "LAZARUS" group

The LAZARUS group a cyber-criminal organization controlled by the North Korean intelligence Service (RGB). The group attacks governmental institutions, military, financial, manufacturing, publishing, media, telecommunication, entertainment and international shipping companies, educational institutions as well as critical infrastructures using means of cyber espionage, data theft, monetary heist, and destructive malware operations. The group was established for supporting the North Korean nuclear and ballistic-missile program by the means of cyber espionage and monetary heist. Unlike many other nation-states groups, the LAZARUS 'cyber -espionage in most cases have financial goal. The number of the group members is unknown. Cyber security experts categorize the group as Advanced Persistent Threat (APT) due to its characteristics. Different cyber security firms have given the group different names: Lazarus Group (Kaspersky), Labyrinth Chollima (CrowdStrike), Group 77 (Talos), Hastati Group (SecureWorks), Whois Hacking Team (McAfee), NewRomanic Cyber Army Team (McAfee), Zinc (Microsoft), Hidden Cobra (Trend Micro), Appleworm (?), APT-C-26 (Qihoo 360), ATK 3 (Thales), SectorA01 (ThreatRecon), ITG03 (IBM). Presumably, due to its three main missions the group has three subgroups. Each has special mission, but they exchange information, tactics and software tools.

2.1. The "LAZARUS" subgroups

Subgroup 1: Andariel aka. Silent Chollima

Andariel: The subgroup focuses on South Korean governmental organizations and businesses by using specially tailored malicious cyber operations. "Andariel" is also responsible for developing and creating unique malware to hack into online poker and gambling sites to steal money. This subgroup carries out malicious cyber activity against purposefully selected South Korean government personnel and military officers to gather intelligence.

Subgroup 2: BeagleBoyz

BeagleBoyz: This group is responsible for the sophisticated cyber-enabled ATM cash-out campaigns identified as "FASTCash" in October 2018. Since 2016, the group has perpetrated the FASTCash scheme targeting banks' retail payment system infrastructure. The BeagleBoyz's bank robberies posture severe risk for firms beyond reputational harm and financial loss from theft and high recovery costs. The BeagleBoyz have attempted to steal nearly $2 billion since at least 2015, according to public estimates (Us-cert.cisa.gov. 2020).

Subgroup 3: Bluenoroff aka. APT 38 or aka. Stardust Chollima

Bluenoroff: A subgroup focused on attacking foreign financial institutions. They are responsible for a wide array of financial theft incidents, including the notorious SWIFT attack in 2016 when attacked dozens of banks in 11countries. After this series of attacks they managed to get away with $81million.

2.2. The activities of the "LAZARUS" groups

The group popped up in 2007, when in the course of „Operation Flame" action attacked important South Korean governmental institutions paralyzing financial and political webservices. Since this action the group has been in the focus of cyber security firms because dozens of attacks can be attached to this group. Listing these attacks would exceed the frames of this study, but some of them worth to mention because of their characteristics. The most famous, and nefarious attacks are e.g the "Blockbuster" attack against the Sony Pictures in 2014, or the attack against the international financial wire system (SWIFT) in numerous countries in 2016, where the criminals stole $81 million. The most outrageous action was the spreading of the WannaCry ransom worm that infected more than 300 thousand computers in more than 150 countries (Hern & MacAskill 2017). One of the publicly identified victims was the United Kingdom's (UK) National Health Service (NHS). More than one third of the UK's secondary care hospitals, other emergency services, and eight percent of general medical practices in the UK were crippled by the ransomware attack. As a result of the attack more than 19,000 appointments were cancelled and the recovery costs exceeded $112 million. It was the biggest known ransomware outbreak in history.

Besides the banks the ATM machines are also in the target cross of the LAZARUS group. The attacks against the ATM machines can be attached to the BeagleBoyz subgroup that withdrawn money from ATMs in more than 30 countries. According to public estimations the group tried to steal more than $2 billion since 2015. In addition to the robberies they install destructive malwares on the victims' computer. As a result of a such a kind of attack an African bank wasn't able serve its customers for two months (Us-cert.cisa.gov. 2020), (The Economic Times 2019).

With the growing popularity of the cryptocurrencies in the last few years the group turned towards the crypto-exchanges exploiting the partial anonymity of the crypto currencies. Besides the cryptocurrency stealing they also used these currencies to launder the robbed and stolen money. According to a United Nation report as of mid- 2019 North Korea approximately gained more than $2 billion by attacks on banks and crypto currencies (Bitcoin, Ethereum, Ripple and so on…) (Arquilla 2021, 4).

Owing to the sanctions and bans on the trading and the new technologies, and the resourceless economy the country has no other choice than stealing the cutting-edge technologies from the developed countries. In order to acquire the advanced technologies, they launched numerous attacks against the defense sphere, universities, research labs around the world e.g in the "Ghostsecret" action just to name one. During the course of this action the group attacked educational, telecommunication, critical infrastructures systems of more than

17 countries (including the USA) in the early of 2018. The group continuously develops its cyber capabilities. The Kaspersky lab discovered a new malware framework of the "LAZARUS" that is able to attack the IoTs with the aim of exploiting them in their further attacks. The Kaspersky lab published that the group also developed a special malware framework with a set of plugins that is able to work in any popular operating systems including MS Windows, Linux, IOS just to name a few (Lemos 2020). The group doesn't shy away from buying information on high value networks from cyber-criminal groups either. The researchers of the Kaspersky Lab during their investigation found the "LAZARUS" group among the customers of the Trickbot cybercriminal group that sells information on high value networks.

In the beginning the group focused on South Korea, and the US than they expanded their interest actually to the whole world. Today there is no country that can feel safe from the North Korean cyber-criminal group. In order to shed some light on the volume of the campaign here is a short list about the concerned countries: Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam. This short list proves that the "LAZARUS" group's activity is global in nature.

2.3. Notable tactics

In the next section some of the notable tactics of "LAZARUS" will be presented. These technics form a complex system that helps the group achieve its aims and hide their traces, and in some cases destroy the target infrastructures in addition fostering the basis of the plausible deniability.

Disruption: The disruptive technics such DDOS attacks, hard disk wipers, MFT destroyers, or wipers are used in destroyer actions when the aim is to paralyze or destroy the enemy's systems.

Misdirection: The group often disguises its actions as hackctivist activities claiming the responsibilities for these virtually fabricated groups like „GOP", „WhoAmI, or New Romanic Army". They also tried to emulate the modus operandi of hacktivists by defacing web pages and leaking information. It is not uncommon that the "LAZARUS" plants false flags inside their tools to distract the suspicions from itself. In the "KLIPOD" backdoor,e.g. they used Romanized Russian words for backdoor commands.

Protectors: The "LAZARUS" uses commercially available protectors (e.g. exepackers) for its tools. Although, in some cases they use during their attacks both protected and unprotected versions of their tools on the same target.

Anti-Forensics technics: They separate their malwares into function based components. It is mainly the feature of the "Bluenoroff" sub group. The group also tries to curb the reverse engineering by obfuscating the codes.

Command line tools: They prefer to use the command line backdoors, and installers and the use of special arguments for execution. These arguments can be among others e.g. the IP address of the C2 server, or passwords. The installer of the "Nestegg" framework, or the "KLIPOD" backdoor are good examples for such tools.

Disk wipers: These tools can be used as destroyers, but in the recent years they are used to destroy the traces of the groups' activities. They use special tools to wipe the traces without destroy the system. The group prefers to use MFT table wipers, prefetch wipers, registry, and event log wipers just to name a few.

2.4. Technical and operational support from abroad

North Korea receives valuable support from China, and India. These countries provide it with academic training, cutting edge technology, and operational support in addition they ignore the North Korean violations of the international agreements, and also ignore the sanctions against North Korea.

China

The North Korean crime syndicates employ Chinese citizens who have access to cutting edge technologies to support their actions. In March 2020 the US Department of Justice charged two Chinese nationals who tried to launder over 100 million worth stolen cryptocurrency in favor of North Korea. The investigation found evidences that proved the link between the Chinese nationalities and the "LAZARUS" group.

North Korean students often study in China at top science and technology universities where they can access to the newest technologies. As it mentioned above thousands of guest workers are employed in the centers of the advanced technologies in China.

The Chinese government has official academic partnership (2020-2030) with the North Korean government which was renewed in 2019 (Bartlett 2020b).

India

India is well known for its high level IT expertisement and its lax stance on North Korea. India's Centre for Space Science and Technology Education in Asia and the Pacific (CSSTEAP) offers postgraduate diploma courses in science and technology for North Korean nationals. The CSSTEAP provides access to the most advanced technologies, computers and cutting-edge software solutions, and hardware for the North Korean students and scientists. This help is vital for the North Korean hacker campaigns created for fostering the funds for the its nuclear program. The reader can find North Korea among the 16 signatory countries on the homepage of the university (https://www.cssteap.org/international-linkages).

Conclusions

The „LAZARUS" group is a typical example of a state sponsored cyber-criminal group that poses threat for practically the whole world mainly for field of the financial system, cutting-edge technologies, education, and telecommunication. The end of its course of action can't be foreseen today. The North Korean government or policy can't be stopped by international bans or sanctions especially while it has strong supporter countries. It seems that the „LAZARUS" or its descendant groups will work while the North Korean ideology and policy are in power.

BIBLIOGRAPHY:

ARQUILLA, John. 2021. Bitskrieg. 1st ed. Cambridge: Medford: Polity Press.

BARTLETT, Jason. 2020. Exposing the Financial Footprints of North Korea's Hackers. [online] Cnas.org. Accessed on October 2 2021. URL: https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers

BARTLETT, Jason. 2020. „Why Is North Korea So Good at Cybercrime?". Thediplomat.com. Accessed on June 16 2021. URL: https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/

BERMUNDEZ, jr, Joseph. 2010. „A new emphasis on operations against South Korea? 38 norths special report:". 38north.org. Accessed September 16 202. https://doczz.net/doc/5259579/a-new-emphasis-on-operations-against-south-korea

Center for Strategic & International Studies. 2014. „The Organization of Cyber Operations in North Korea". Washington DC: Center for Strategic & International Studies. Accessed

September 17 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141218_Cyber_Operations_North_Korea.pdf

CHA, Victor, and JAMES Andrew Lewis. ”North Korea's Cyber Capabilities”. Center for Strategic and International Studies. December 18, 2014. p. 26.

HERN, Alex and EWEN MacAskill. 2017. „WannaCry ransomware attack 'linked to North Korea'”. The Guardian. Accessed on 12 August 2021. URL: https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group

JUN, Jenny, LAFOY, Scott, and SHONN, Ethan. 2015. North Korea's Cyber Operations. [online] London, New York: CSIS, p.41. Accessed August 5 2021. URL: https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations

JUN, Jenny, CHA, Victor, LEWIS, James A., LAFOY, Scott and SOHN Ethan. 2015. „North Korea’s cyber operations: strategy and responses”. Washington, DC: Center for Strategic & International Studies.

LEE, Michael. 북한의 對南공작 활동(上)-34(in English: “North Korea’s Intelligence Operations against South Korea,”). 2014. Chogabje.com, November 3, 2014, Accessed on August 5 2021. URL: http://www.chogabje.com/board/column/view.asp?C_IDX=58208&C_CC=bC.

LEMOS, Robert. 2020. “North Korea's Lazarus Group Developing Cross-Platform Malware Framework”. Dark Reading. Accessed on August 14 2021. URL: https://www.darkreading.com/threat-intelligence/north-korea-s-lazarus-group-developing-cross-platform-malware-framework

ROK Ministry of Unification. “North Korea Encyclopedia: 5-year Science Technology Development Plan,” North Korea Information Portal, November 17, 2015, Accessed 8 September 2021. http://nkinfo.unikorea.go.kr/nkp/term/viewNkKnwldgDicary.do?pageIndex=2&koreanChrctr=&dicaryId=8

SEOK, Lee and SANG-KI Kim. 중국(심양·단동)출장보고서 (in English: “Report on Travels from China (Shenyang and Dandong))”. 2008. Seoul: Korea Development Institute, Accessed September 7 2021. URL: https://www.kdi.re.kr/data/download/attach/12241_28.pdf, p.7.

SEOK-WOO, Lee. 2011. 北 39호실의 새 외화벌이 수법… 리니지 아이템 해킹프로그램 판매 (in English: „A new way to earn foreign currency in Room 39 in North Korea... Lineage item hacking program sales”). [online, translated from Korean] Chosun. Accessed September 17 2021. URL: https://www.chosun.com/site/data/html_dir/2011/08/05/2011080500076.html

SEONGWOOK, Kim. 2009. 노무현정부, 북한 IT 인력양성 해마다 지원 (in English: „The Roh Moo-hyun government supports North Korea's IT manpower training every year”). NewDaily.co.kr. Accessed on October 1 2021. URL: http://www.newdaily.co.kr/site/data/html/2009/12/18/2009121800038.html

SEUNGHYUN, Lee. “남북경협,말들 많았지만 남은건 하나비즈뿐”(in English: “Despite Many Talks, hanabiz the Only Outcome from Economic Cooperation between North and South Korea,”). 2004. Tongil News, March 24, Accessed September 5 2021. URL: http://www.tongilnews.com/news/articleView.html?idxno=42717

SOONPYO Park, 사이버 공격 5년 동안 7만건..."대부분 북한 소행 (in English: "North Korea Responsible for Most of 70,000 Cases of Cyberattacks during the Last Five years,"). 2013. yTN, March 21, Accessed on August 5 2021. URL: http://www.ytn.co.kr/_ln/0101_201303211024217337?ems=12714

The Economic Times. 2019. Beware! North Korean hackers are watching your ATM transactions. Accessed on July 17 2021. URL: https://economictimes.indiatimes.com/industry/banking/finance/banking/beware-north-korean-hackers-are-watching-your-atm-transactions/articleshow/71323817.cms?from=mdr

United States Department of State. 2019. Democratic People's Republic of Korea Sanctions - United States Department of State. Accessed September 7 2021. URL: https://www.state.gov/democratic-peoples-republic-of-korea-sanctions/

Us-cert.cisa.gov. 2020. FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks | CISA. Accessed July 17 2021. URL: <https://us-cert.cisa.gov/ncas/alerts/aa20-239a