EuRepoC

ADVANCED PERSISTENT THREAT profile

Lazarus Group

The APT with countless lives

Associated APT designations

- **Lazarus Group** (Novetta/Kaspersky/generic designation)
- **Labyrinth Chollima** (CrowdStrike)
- **Diamond Sleet, fka ZINC** (Microsoft)
- **G0032** (MITRE ATT&CK)
- **HIDDEN COBRA** (CISA/US Department of Homeland Security)
- **NICKEL ACADEMY** (Secureworks)
- **Guardians of Peace** (self-given)
- **New Romantic Cyber Army Team** (McAfee)
- **Whois Hacking Team** (McAfee)
- **Group 77** (Talos)
- **Appleworm** (origin unknown)

Sources: [1], [2], [33]

Country of origin

Time period of activity

2009 - present

Sources: [5], [33]

Political affiliations

It is important to emphasise that there is little consolidated, broadly-recognised knowledge about the Lazarus Group and its specific political affiliations within the North Korean state apparatus compared to the knowledge of other nation-state APTs. The name usually acts as an umbrella term for a wider subset of North-Korean cyber activities and responsible sub-groups, which makes the attribution of specific operations often difficult (see section "Attribution Ambiguities" below). The threat intelligence community, academics, and state authorities have no common understanding of a clearly-defined hierarchy or the organisation of North Korean cyber units and their respective APT designations so far. The present profile therefore seeks to differentiate the more general aspects that can be perceived as a given common denominator from more specific details that are still contested by varying actors analysing the regime's cyber posture.

In general, the Lazarus Group refers to a large subset of state-sponsored cyber activities of the Democratic People's Republic of Korea (DPRK), operating as an integral wing of North Korea's central foreign intelligence agency, the Reconnaissance General Bureau (RGB) that comprises six different bureaus. It is a widely-accepted understanding that North Korean cyber activity of any kind is most likely directed or controlled by the RGB. Within the RGB, most sources, including academic analyses and threat intelligence reports, such as

By Kerstin Zettl-Schabath, Alisa Jazxhi and Camille Borrett

one from Mandiant in 2023, associate the Lazarus group with the RGB Lab 110. Mandiant represents Lab 110 as an expanded/reorganised version of the better-known Bureau 121, often referred to as North Korea's primary hacking unit. Older sources, such as an academic chapter by South Korean researchers from 2019, consider Lab 110 to be subordinate to Bureau 121.

The activities of the Lazarus Group are directly linked to North Korea's efforts to circumvent international sanctions, particularly those imposed by the UN Security Council in 2009 (Resolution 1874) and intensified in March 2013 (Resolution 2094). These sanctions, aimed at limiting North Korea's nuclear and missile programmes, have significantly impacted the nation's economic landscape, prompting the regime to seek alternative revenue streams through cyber operations. As such, its financial cyber operations are not only a means of state-sponsored espionage against its victim targets, but also serve as a vital source of funding for the regime. Lazarus' association with the RGB and its sophisticated financial cyber operations reinforce its status as a prominent and formidable player in the international cybersecurity space, and it highlights the complicated nature of state-sponsored cyber threat actors.

Sources: [4], [6], [7], [11], [15], [30]

Agency type

State-ordered/integrated hacker group(s) (partially comprising a cyber military unit): The Lazarus Group operates as a state-integrated hacker collective as part of the constantly-evolving offensive cyber programme of the DPRK. The RGB, which follows next in this chain, is said to have six bureaus operating under its control. Lazarus, among other groups, operates under the Third Bureau (responsible for foreign intelligence) as a specialised cyber operations unit that has become a major force and threat in global cyber warfare since its establishment in 2009. According to a press release by the US Department of the Treasury from September 2019, Lazarus is "subordinate to the 110th Research Center, 3rd Bureau of the RGB."

However, whether Lazarus should be presented as one homogenous "unit" is a topic of debate. Instead, it potentially acts as an umbrella group for other, more specialised North Korean hacking teams responsible for various tasks, such as Andariel, BlueNoroff or BeagleBoyz. This is a similar to the Chinese APT Winnti, which also comprises different other APTs, further complicating attribution due to extensive tool-sharing among them. At the same time, this stands in stark contrast to the Russian APT ecosystem which is dominated by different, competing intelligence agencies, guiding APT groups that are more distinct and thus make attribution efforts more straightforward.

What differentiates North Korean hacker units from Chinese groups is their usual deployment abroad. Given the country's weak digitalisation and its compartmentalisation against external influences, North Korean hackers often operate from countries such as China, India, Cambodia, or Vietnam, often disguised as students or software engineers. This characterisation speaks against the label of a "state-executed" hacking group, rather emphasising the informal aspect of state control over its nationals abroad, who act as third-party attackers outside the national intelligence apparatus but with a purportedly high degree of control. Thus, it is still unclear how many cyber incidents actually originate from North Korean soil that would qualify them as state-executed attacks.

Sources: [13], [30]

Most frequent targets

 South Korea
 USA
 Japan
 India
 Germany
 UK
 UAE
 EU/Europe
 Taiwan
 Bangladesh

Source: [22]

Group composition/organisational structure

As per the RGB corpus, the Lazarus Group is made up of elite cyber operatives, each of whom is trained and focussed on different aspects of cyber warfare. The group is purportedly divided into specialised units, such as Andariel and BlueNoroff, with each unit focussing on different areas of operation. It is unknown how large the personnel corpus of Lazarus is, but there are at least some reports, such as that of Bugcrowd, which discuss rough estimates of the personnel size of the two subgroups. Andariel is said to have 1,600 employees and BlueNoroff is estimated to have around 1,700. Another proxy indicator could be the size of Bureau 121, assuming that Lazarus comprises most of its employees. A Powerpoint presentation by the US Health Sector Cybersecurity Coordination Center (HC3) from 2021 estimated that the Bureau includes at least 6,000 employees (not all of whom are intelligence agents).

According to Mandiant, the activities of the DPRK's cyber units and interconnected sub-groups, as well as their organisational structure, can adapt according to the regime's goals over time, as it was the case during the COVID-19 pandemic: Mandiant reports that the new Bureau 325 was publicly announced in January 2021 and soon after focussed its espionage operations on vaccine research; it is allegedly also staffed by members of other APTs, such as Kimsuky.

The actual degree of control the regime effectively exercises over its hackers stationed abroad cannot be judged with certainty. However, it seems plausible that, once they are subject to international search warrants, indictments, or sanctions, the regime tries to return them home to North Korea as soon as possible in order to eliminate the potential loss of intelligence.

Sources: [8], [9], [21], [35]

Impact type(s)

Direct

- **Intelligence impact** (e.g., espionage against the South Korean chemical sector in 2022)
- **Political intelligence impact: continuous campaigns against South Korea** (e.g., Operation Dream Job or operation against Windows IIS Web Servers)
- **Economic/financial impact: attacks against the public** (Bangladeshi bank heist) **and private sector** (theft of $37.3 million from CoinsPaid, as well as roughly $100 million from Atomic Wallet; hack against Sony Pictures in 2014)

Indirect

- **Reputational Impact** (hack against Sony Pictures in 2014)

Sources: [11a], [11c]

Incident type(s)

- **Data Theft** (intelligence gathering/cyber espionage)
- **Hijacking with misuse** (financial theft against banks or cryptocurrencies)
- **Disruption** (wiper attacks/DDoS operations)

Threat Level Index

12/24 moderate threat level

Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the sectorial and geographical scope of the APT's attacks, the intensity of the attacks, the frequency of attacks and the use of zero-days. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here and here.

Threat level sub-indicator	Score	Explanation
Intensity of attacks	1 /5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information.
Sectorial scope of attacks	3 /8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. Incidents attributed to the Lazarus Group in the EuRepoC database, targeted, on average, 1.5 sectors per attack and 66% were against state institutions/political systems or critical infrastructure.
Geographical scope of attacks	3 /4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of the Lazarus Group, on average three countries were targeted per incident attributed to the group in the EuRepoC database.
Frequency of attacks	4 /4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. The Lazarus Group was responsible for more than 3 incidents per year of activity.
Exploitation of Zero days	1 /3	This indicator calculates the percentage of attacks attributed to the APT that use one or multiple zero days. The score obtained is then converted to a three-level scale. 2 incidents (4%) in the EuRepoC database attributed to the Lazarus Group used zero-days.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

The Lazarus Group has consistently demonstrated its advanced technical capabilities and sophistication in its cyber operations since its creation. Its sophisticated attack patterns include a mixture of targeted spear-phishing attacks and exploitation of software vulnerabilities, as well as exploitation of zero-days and the use of customised malware that can be identified as such and attributed to Lazarus, targeting both public and private international targets.

Basic attack pattern

The Lazarus Group's attack pattern and its repertoire are diverse, sophisticated, and highly refined. Lazarus tailors its MO (*modus operandi*) and the associated methods and tools to its desired target. The group often initiates spear-phishing campaigns using bogus emails to spread malware. Once it has illegally infiltrated a victim's network, the group exploits vulnerabilities to create backdoors and communicate with command-and-control servers. The group's operations include collecting credentials to move within networks - sometimes months before initial detection – thus enabling its operatives to access sensitive areas and escalate privileges. In addition, the group exfiltrates and destroys data - often sensitive political, military, or financial information - to gain an intelligence advantage over political opponents and adversaries.

Sources: [2], [36]

Zero-day exploits

The group is also known to strategically use zero-day exploits.

A recent example is the active exploitation of a zero-day vulnerability in the MagicLine4NX software to potentially carry out supply-chain attacks, which was the subject of a joint statement published by the UK and South Korea in November 2023. MagicLine4NX is a security authentication software developed by the South Korean software company Dream Security. Previously, similar attacks took place in March 2023 against financial entities in South Korea.

Sources: [16], [23]

List of malware and tools used (non-exhaustive)

The Lazarus Group and its customised malware and other tools are constantly evolving, recycled, or completely reassembled from time to time. Some of the main tools and malware it has used are:

- **Backdoors:** these are used to gain persistent access to compromised networks. Examples include Appleseed, HardRain, BadCall, Hidden Cobra, Destroyer, Duuzer, OpenCarrot, KLIPO, and DESTOVER.
- **Remote access Trojans (RATs):** For remote control of infected systems, Lazarus has RATs such as Fallchill, Joanap, and Brambul.
- **Ransomware:** WannaCry.

Sources: [1], [2], [17], [36]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access
Phishing: Spearphishing Attachment **Phishing: Spearphishing Link**

MITRE Persistence
Account Manipulation **Scheduled Task/Job** **Hijack Execution Flow: DLL Side-Loading**

MITRE Defense Evasion
Access Token Manipulation: Create Process with Token **Debugger Evasion** **Hide Artifacts: Hidden Files and Directories**

MITRE Impact
Data Encrypted for Impact Defacement Disk Wipe: Disk Content Wipe Service Stop

Sources [22]

ATTRIBUTION

Major attribution milestones

1) Sony Hack Attributions:

- Attribution towards the North Korean government by the FBI and US President Barack Obama (December 2014)
- Threat Intelligence coalition led by Novetta attributes Sony Hack towards a group dubbed "Lazarus" in "Operation Blockbuster" report (2016)
- Criminal complaint by the US against Park Jin Hyok (박진혁; aka Jin Hyok Park and Pak Jin Hek), identifying him as a former Lazarus member and employee of North Korean government front company Chosun Expo Joint Venture (September 2018)

2) Bangladesh Cyber Heist Attributions:

- BAE Systems links the Bangladesh Cyber Heist with the Sony Hack for the first time (May 2016)
- FBI attributes the heist as "state-sponsored" by North Korea (March 2017)
- Report by Kaspersky links Lazarus and North Korea via an IP address (April 2017)

3) WannaCry Attributions:

- Identification of code-sharing between WannaCry and previous Lazarus operations by Google security researcher Neel Mehta (May 2017)
- Symantec attributes WannaCry to the Lazarus Group due to the same command-and-control infrastructure as was used in the Sony Hack (May 2017)
- US and UK governments attribute the North Korean government as responsible for WannaCry (December 2017)
- US criminal complaint against Park Jin Hyok (September 2018)
- Restrictive measures against Chosun Expo within the EU's Cyber Diplomacy Toolbox Framework (July 2020)

4) Expansion of US charges against Park Jin Hyok from 2018:

- Indictment against Chang Hyok (전창혁), Kim Il (김일), and Park Jin Hyok (박진혁) due to their work for the RGB within the Lazarus Group, referencing multiple cyber operations (Sony Hack, bank heists, FASTCash campaign, WannaCry, and operations against cryptocurrency companies) (February 2021)

Sources: [3], [10], [20], [27], [31], [37], [38], [39], [40], [41], [42], [43], [44]

Attribution ambiguities

APT designations are, to a certain extent, social constructions by threat intelligence companies which reflect their assessments of group compositions, collaborations, and divisions of labour. This is particularly evident for the Lazarus Group, as this label is often used in a generic way for nearly all kinds of DPRK-related cyber activities. Hence, the US authorities decided to label all cyber operations attributed to North Korea under the moniker "HIDDEN COBRA," also reflecting the less-consolidated knowledge base surrounding the regime in Pyongyang compared to knowledge surrounding Russian or Chinese intelligence agencies. This "conventional intelligence knowledge" about internal structures, profiles, and responsibilities often complements an attribution assessment for certain hacking groups in case of missing, incomplete, or inconclusive technical evidence. In many cases, a final attribution of a responsible state unit for certain cyber activities is only possible because of this information.

Nonetheless, private threat intelligence companies and state authorities alike came up with a number of additional subgroup-labels, all attached to the Lazarus Group. However, no unanimous picture of the internal DPRK cyber hierarchy has emerged so far.

The following aspects summarise resulting ambiguities regarding attributions towards Lazarus or its subgroups:

Lazarus as an umbrella label: To date, there are diverging assessments of the command chain between Lazarus and other designated North Korean APTs, such as Andariel, BlueNoroff, and BeagleBoyz. Most observers (e.g., TrendMicro) conclude that Andariel is the Lazarus-subgroup in charge of operations against South Korea, while BlueNoroff is responsible for activities against financial institutions. To date, however, what is not proven beyond doubt is the exact nature of the relationship between North Korean APTs or Lazarus. For example, Lazarus might actually act as a "core group," superior to the other subgroups, or it could rather act as a collective of equal groups with different tasks, which often share malware and infrastructure for their operations.

Another ambiguity relates to Lazarus' **associated intelligence unit(s).** According to South Korean researchers, Bureau 121 acts in parallel to the other RGB bureaus. Mandiant, however, assesses that the Bureau 121 is subordinate to the RGB's Third Bureau, which ties in with the evaluation of the US Department of the Treasury from September 2019.

The **label APT38** is often discussed as an equivalent of Lazarus (e.g., by the FBI). In contrast, the US HC3 states that it is on an equal level as BlueNoroff, which would be closer to the MITRE assessment of APT38 as another Lazarus-subgroup.

The attribution of the **Sony Pictures Hack** towards the regime in North Korea was contested for some time by different IT-experts (e.g., Bruce Schneier in December 2014). In the meantime, the 2018 indictment consolidated the US' position on North Korean responsibility, further presenting technical and intelligence evidence.

Another attribution controversy emerged for the so-called **"Olympic Destroyer"** operation against the 2018 Winter Olympics in South Korea, in which the Russian military hacking group Sandworm tried to pose as Lazarus as part of a false-flag operation, using malware normally associated with the North Korean hackers.

The lesser-known **"Operation Sharpshooter,"** which targeted global nuclear, defence, energy, and financial companies, presented numerous obvious technical links to the Lazarus Group. This is why McAfee also discussed the possibility of a potential false-flag operation, indicating Lazarus as the perpetrator. For this operation, however, no alternative threat actor has been identified so far. As a potential third explanation, McAfee also theorised about code-sharing between Lazarus and the (true) responsible group, without further specifying the latter´s origin or national affiliation.

Sources: [22], [36], [45], [46], [47], [50], [51]

Attribution and detection sensitivity

Different industry reports describe Lazarus´ extensive use of so-called "anti-forensics techniques," defined as the "tampering of evidence in an attempt to mitigate the effectiveness of a forensics investigation at a crime scene" (ASEC 2023). TrendMicro previously observed the group's separation of components, as well as its employment of command line tools, disk wiping and prefetch, event logs, and MFT record wipers in 2018. A more recent report by South Korean AhnLab Security Intelligence Center (ASEC) observed the following techniques: data hiding (e.g., encryption), artifact wiping (e.g., file wiping), and trail obfuscation (e.g., timestamp changes). The latter was also observed in campaigns by other APTs, such as Russian APTs (APT28 and APT29), according to ASEC.

Sources: [36], [48]

POLITICAL/LEGAL/LAW ENFORCEMENT ACTIONS

1) September 2018/February 2021
In the wake of the WannaCry attack, the US Department of Justice (DOJ) indicted three North Koreans who were not only proven to be employees of the RGB, but were also allegedly instrumental in its cyber operations. The individuals in question are as follows:

- Park Jin Hyok (박진혁) (first indictment in September 2018)
- Jon Chang Hyok (전창혁)
- Kim Il (김일)

2) 13 September 2019
The US Treasury Department sanctioned the Lazarus Group and its two sub-groups BlueNoroff and Andariel for their continuous malicious cyber activities, including the WannaCry ransomware attack and several financial thefts.

The sanctions blocked all property of these groups in the US and prohibited transactions with the RGB.

3) 2 March 2020
The US Office of Foreign Assets Control (OFAC) within the US Department of the Treasury sanctioned two Chinese nationals, 田寅寅 Tian Yinyin (Tian) and 李家东 Li Jiadong (Li), for laundering stolen cryptocurrencies in connection with a 2018 cyberattack by North Korea's state-sponsored Lazarus Group, in which $250 million in virtual currencies were stolen from a cryptocurrency exchange. They are said to have provided the group with material, financial, and technological support.

4) 20 July 2020

The European Council decided to sanction Chosun Expo, which played an important role in cyberattacks such as the WannaCry attack, as part of a fourth sanctions package. The activities of Chosun Expo are closely linked to the Lazarus Group, with Park Jin Hyok identified as a former employee and Lazarus member.

5) 6 May 2022

The US OFAC imposed sanctions on Blender.io, a virtual currency mixer used by Lazarus Group to launder money. Blender.io was involved in laundering over $20.5 million from Lazarus' $620 million theft from the blockchain game Axie Infinity. The sanctions blocked all US business with Blender.io and identified other virtual currency addresses that were used by Lazarus.

6) 24 April 2023

The US OFAC imposed sanctions on three individuals for North Korea's illicit financial activities, including hacking and virtual currency theft. Wu HuiHui, Cheng Hung Man, and Sim Hyon Sop were alleged to have cooperated with North Korea; the first two were even directly linked with the Lazarus Group and allegedly provided the group with material support. The sanctions, which were coordinated with South Korea, blocked the US assets of these individuals and prohibited transactions with them.

On the same day, two federal indictments were unsealed in the District of Columbia against the same three individuals.

Sources: [1], [10], [12], [13], [14], [19], [25], [26]

Landmark operations

Sony Pictures Hack in 2014:
In this sophisticated cyberattack, the Lazarus Group infiltrated Sony Pictures Entertainment's IT network over an extended period of time and exploited vulnerabilities in Microsoft Windows-based systems to stage a large-scale data breach. Their main objective was to disrupt the release of "The Interview," a satirical film depicting the assassination of North Korean leader Kim Jong Un. The attack resulted in significant data loss and financial damage to Sony. The attack, which was discovered on 24 November 2014, revealed deep vulnerabilities in Sony's cybersecurity that had been exploited for several months prior to discovery. The Lazarus Group attack, one of the first attributed to the DPRK, carefully exploited the administrative and network-wide file-sharing capabilities of Microsoft Windows Server. This allowed the attackers to access, extract, and finally delete a wide range of confidential information, including sensitive employee data and unpublished films. The incident attracted international attention and ultimately led to the politicisation by former US President Barack Obama. In response to this direct attack on the right to freedom of expression and the security of American assets, President Obama promised "decisive action" against North Korea on 19 December 2014.

Bangladesh Central Bank heist in 2016:
This operation attempted to steal nearly $1 billion from the Bangladesh Central Bank's account at the US Federal Reserve Bank. Although Lazarus did not quite achieve their goal, it still managed to transfer $81 million to Philippine accounts by using the "SWIFT Client" malware to access the bank's SWIFT system and then send fraudulent transfer requests to the Federal Reserve Bank of New York. The heist began on 4 February 2016, when hackers breached the Bangladesh Central Bank's systems and gained access to SWIFT credentials. Using these credentials, the group submitted a series of wire transfer requests, cleverly disguising them with the names of fake charities and nonprofit organisations. Fortunately, a simple typo in one of the requests aroused the suspicion of the Federal Reserve Bank and prevented further unauthorised transactions.

WannaCry ransomware attack in 2017:
In its most destructive cyber campaign ever, the Lazarus Group strategically released the WannaCry ransomware, which ended up affecting between 230,000 and 300,000 computers in 150 countries. This attack exploited a vulnerability in Windows, specifically targeting systems that had not installed a crucial Microsoft security patch. WannaCry encrypted data on infected computers and demanded a ransom in Bitcoin for its release. The attack had a significant impact on various sectors, i.a., on the health and financial sectors, which resulted in a loss of over one billion US dollars. The rapid spread of WannaCry was traced back to the utilisation of the EternalBlue exploit, which was presumably discovered and used by the US National Security Agency. The exploit was published by the hacker group Shadow Brokers and thus became publicly available. Prominent victims of the attack included large organisations such as the UK's National Health Service, FedEx, Honda, and Nissan, highlighting the disruptive potential of the ransomware. The spread of WannaCry was inadvertently halted when security researcher Marcus Hutchins registered a domain found in the malware's code, triggering a built-in kill switch. Nevertheless, WannaCry remains a strong threat, as unpatched systems are still vulnerable to the ransomware. In 2018, the United States charged a North Korean agent/member of Lazarus for his involvement in both WannaCry and the hack of Sony Pictures in 2014.

Lazarus COVID-19-Campaign - Health Ministry in 2020:
On 27 October 2020, the Lazarus Group carried out a sophisticated cyberattack on an unspecified Ministry of Health to secretly obtain COVID-19 information. Using "wAgent," a versatile malware, the group managed to infiltrate two Windows servers, bypassing existing security measures. "wAgent" worked mainly within the system's memory and was able to retrieve additional malicious payloads from remote servers, demonstrating its advanced remote-control capabilities. The attack was highly customised, indicating a targeted approach rather than an indiscriminate large-scale attack. The complexity of the operation was also evident in the persistent access strategy, which utilised malware that mimicked legitimate software components. This tactic ensured that the attackers gained persistent access to the ministry's systems, which could enable continuous monitoring or data extraction. The sophistication and execution pattern of this operation - from stealth tactics to persistence - was subsequently linked to the Lazarus Group's known operational methods, confirming their involvement in this high-risk cyber espionage operation.

Crypto heist against Atomic Wallet in 2023:
In June 2023, the Lazarus Group reportedly stole $100 million in cryptocurrencies from the Estonian cryptocurrency wallet 'Atomic Wallet" and further affecting around 1% of users by compromising their accounts. This sophisticated cyberattack was linked to Lazarus by blockchain analytics firm Elliptic, as similar money-laundering techniques had been observed in previous attacks. While it is not yet entirely certain how Lazarus threat actors gained access, it is suspected that a bug in the wallet provider's application, which exposed users' private keys, helped them; this is believed to have been the root cause. The group's methods also went beyond the actual hack: it used the sanctioned Russian crypto exchange Garantex to launder a significant portion of the stolen funds.

Sources: [11], [18], [28], [29], [32], [34], [49]

SOURCES

[1] Electronic Transactions Development Agency (2023). *Lazarus Group, Hidden Cobra, Labyrinth Chollima*. ETDA. Available at https://web.archive.org/web/20230127112614/https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Lazarus%20Group%2C%20Hidden%20Cobra%2C%20Labyrinth%20Chollima&n=1 [Archived on: 27.01.2023].

[2] MITRE (2023). *Group: Lazarus Group (G0032)*. MITRE ATT&CK. Available at https://web.archive.org/web/20240114095351/https://attack.mitre.org/groups/G0032/ [Archived on: 14.02.2024].

[3] A.L. Johnson (2016). *SWIFT Attackers' Malware Linked to More Financial Attacks*. Symantec Enterprise; Broadcom Communications. Available at https://web.archive.org/web/20240214151208/https://community.broadcom.com/symantecenterprise/viewdocument/swift-attackers-malware-linked-to?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments [Archived on: 14.02.2024].

[4] NATO Cooperative Cyber Defence Centre of Excellence (2014). *Sony Pictures Entertainment attack (2014)*. CCDCOE Cyber Law Portal. Available at https://web.archive.org/web/20240102195715/https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014) [Archived on: 02.01.2024].

[5] Rapid7 (n.d.). *Lazarus Group*. InsightIDR Documentation. Available at https://web.archive.org/web/20240105020559/https://docs.rapid7.com/insightidr/lazarus-group/ [Archived on: 05.01.2024].

[6] United Nations (2009). *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*. United Nations Digital Library. Available at https://web.archive.org/web/20240214151725/https://digitallibrary.un.org/nanna/record/861367/files/S_2017_150-EN.pdf?withWatermark=0&withMetadata=0&version=1&registerDownload=1 [Archived on: 14.02.2024].

[7] United Nations (2013). *Report of the Panel of Experts Established Pursuant to Resolution 1718 (2006)*. United Nations Digital Library. Available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/253/06/PDF/N1325306.pdf?OpenElement.

[8] Michael Raska (2020). *Nordkoreas Cyber-Krieg Strategie: Kontinuität und Wandel*. In *Sirius* 2020, Issue 3; De Gruyter. Available at https://web.archive.org/web/20230202065858/https://www.degruyter.com/document/doi/10.1515/sirius-2020-2003/html [Archived on: 02.02.2023].

[9] Michael Raska (2020). *North Korea's Evolving Cyber Strategies: Continuity and Change*. In *Sirius* 2020, Issue 30; De Gruyter. Available at https://web.archive.org/web/20231002113554/https://www.degruyter.com/document/doi/10.1515/sirius-2020-3030/html [Archived on: 02.10.2023].

[10] Official Journal of the European Union (2020). *Council Decision (CFSP) 2020/1127 of 30 July 2020*. EUR-Lex. Available at https://web.archive.org/web/20240214150301/https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&rid=7 [Archived on: 14.02.2024].

[11] European Repository of Cyber Incidents. Cyber Incidents Table Views. Various incidents. Available at:
- [11a] Incident 644
- [11b] Incident 842
- [11c] Incident 1847
- [11d] Incident 2336
- [11e] Incident 2450
- [11f] Incident 2459
- [11g] Incident 2493
- [11h] Incident 2596

[12] U.S. Department of the Treasury (2022). *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*. Press Release JY0768. Available at https://web.archive.org/web/20240131054328/https://home.treasury.gov/news/press-releases/jy0768 [Archived on: 31.01.2024].

[13] U.S. Department of the Treasury (2019). *Treasury Sanctions Individuals and Entities for Abuse of Human Rights and Support of the Russian Government*. Press Release SM774. Available at https://web.archive.org/web/20240114071406/https://home.treasury.gov/news/press-releases/sm774 [Archived on: 14.01.2024].

[14] U.S. Department of the Treasury (2020). *Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware*. Press Release SM924. Available at https://web.archive.org/web/20240114032733/https://home.treasury.gov/news/press-releases/sm924 [Archived on: 14.01.2024].

[15] MoonX (2018). *Lazarus: The Cyberwarfare Group of North Korea*. Medium. Available at https://web.archive.org/web/20240214155730/https://medium.com/@moonxfamily/lazarus-the-cyberwarfare-group-of-north-korea-f24238570d3f [Archived on: 14.02.2024].

[16] Pierluigi Paganini (2023). *Lazarus Group has been spotted using a new supply chain attack*. Security Affairs. Available at https://web.archive.org/web/20240105081947/https://securityaffairs.com/154765/apt/lazarus-magicline4nx-supply-chain-attack.html [Archived on: 05.01.2024].

[17] Socradar (2021). *APT Profile: Who is Lazarus Group?* Available at https://web.archive.org/web/20230924174453/https://socradar.io/apt-profile-who-is-lazarus-group/ [Archived on: 24.09.2023].

[18] Daryna Antoniuk (2023). *North Korean hacking group Lazarus linked to $35 million cryptocurrency heist.* The Record. Available at https://web.archive.org/web/20240206013413/https://therecord.media/lazarus-group-attributed-to-atomic-wallet-heist-elliptic [Archived on: 06.02.2024].

[19] BankInfoSecurity (2020). *EU Issues First-Ever Sanctions Over Past Cyberattacks*. Available at https://web.archive.org/web/20240214145929/https://www.bankinfosecurity.com/eu-issues-first-ever-sanctions-over-past-cyberattacks-a-14749 [Archived on: 14.02.2024].

[20] BBC News (2014). *US accuses North Korea of cyber-attacks since 2009*. Available at https://web.archive.org/web/20230611003622/https://www.bbc.com/news/world-us-canada-30555997 [Archived on: 11.06.2023].

[21] Bugcrowd (n.d.). *Lazarus Group*. Bugcrowd Glossary. Available at https://web.archive.org/web/20230926063440/https://www.bugcrowd.com/glossary/lazarus-group/ [Archived on: 26.09.2023].

[22] Cyfirma (2022). *Lazarus Group: Recent Trends.* Available at https://web.archive.org/web/20240214162808/https://www.cyfirma.com/outofband/lazarus-group-recent-trends/ [Archived on: 14.02.2024].

[23] Korean National Intelligence Service and UK National Cyber Security Centre (2023). *ROK-UK Joint Cyber Security Advisory*. DocumentCloud. Available at https://web.archive.org/web/20240118055515/https://www.documentcloud.org/documents/24174869-rok-uk-joint-cyber-security-advisoryeng [Archived on: 18.01.2024].

[24] Group-IB (2017). *Lazarus Arisen: Architecture/Tools/Attribution*. Group-IB Research Hub. Available at https://web.archive.org/web/20240215123510/https://go.group-ib.com/report-lazarus-en?_gl=1%2Acl6al5%2A_ga%2AMTI5MzQ3MjgxMC4xNzA4MDAwNDcz%2A_ga_QMES53K3Y2%2AMTcwODAwMDQ3My4xLjAuMTcwODAwMDQ3My42MC4wLjA. [Archived on: 15.02.2024].

[25] U.S. Department of Justice (2018). *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. Available at https://web.archive.org/web/20240212144631/https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and [Archived on: 12.02.2024].

[26] U.S. Department of Justice (2021). *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*. Available at https://web.archive.org/web/20240127042147/https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and [Archived on: 27.01.2024].

[27] United States Attorney's Office - Central District of California (2018). *United States v. Park Jin Hyok et al.* U.S. Department of Justice. Available at https://web.archive.org/web/20240214180840/https://www.justice.gov/usao-cdca/press-release/file/1091951/download [Archived on: 14.02.2024].

[28] digiALERT (2023). *Case Study: Bangladesh Banking Heist*. Digialert on LinkedIn. Available at https://web.archive.org/web/20240214182254/https://www.linkedin.com/pulse/case-study-bangladesh-banking-heist-digialert [Archived on: 14.02.2024].

[29] Malwarebytes (n.d.). *WannaCry ransomware*. Available at https://web.archive.org/web/20240211023756/https://www.malwarebytes.com/wannacry [Archived on: 11.02.2024].

[30] Michael Barnhardt, et al. (2022). *Not so Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations*. Mandiant. Available at https://web.archive.org/web/20240214183557/https://www.mandiant.com/resources/blog/mapping-dprk-groups-to-government [Archived on: 14.02.2024].

[31] John S. Davis, et al. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace.* RAND. Available at https://web.archive.org/web/20240214183948/https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2081/RAND_RR2081.pdf [Archived on: 14.02.2024].

[32] SecureOps (n.d.). *The Hack on Sony Pictures Entertainment: The Anatomy of One of the Most Devastating Attacks in History*. Available at https://web.archive.org/web/20240215123717/https://www.secureops.com/wp-content/uploads/2021/06/Sony-Breach-Analysis-v4.pdf [Archived on: 15.02.2024].

[33] SecureWorks (n.d). *Threat Profile: Nickel Academy*. Available at https://www.secureworks.com/research/threat-profiles/nickel-academy.

[34] Trend Micro (2014). *The Hack of Sony Pictures: What We Know and What You Need to Know*. Available at https://web.archive.org/web/20240215125555/https://www.trendmicro.com/vinfo/es/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know [Archived on: 15.02.2024].

[35] HHS Cybersecurity Information Program, Office of Information Security (2021). *North Korean Cyber Activity*. Health Sector Cybersecurity Coordination Center. Available at https://web.archive.org/web/20230522041127/https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf [Archived on: 15.02.2024].

[36] TrendMicro (2018). *A Look into the Lazarus Group's Operations*. Available at https://web.archive.org/web/20240108032333/https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations [Archived on: 08.01.2024].

[37] US Federal Bureau of Investigation (2014). *Update on Sony Investigation.* Available at https://web.archive.org/web/20240126213516/https://www.fbi.gov/news/press-releases/update-on-sony-investigation [Archived on: 26.01.2024].

[38] Novetta (n.d.). *Operation Blockbuster: Unraveling the Long Thread of the Sony Attack*. United States Naval Academy. Available at https://web.archive.org/web/20240215130535/https://www.usna.edu/CyberCenter/_files/documents/Operation-Blockbuster-Report.pdf [Archived on: 15.02.2024].

[39] Jim Finkle and Sanjeev Miglani (2016). *Bangladesh Bank heist similar to Sony hack; second bank hit by malware*. Reuters. Available at https://www.reuters.com/article/idUSKCN0Y40SF/

[40] Karen Lema and Raju Gopalakrishnan (2017). *Bangladesh Bank heist was 'state-sponsored': U.S. official.* Reuters. Available at https://www.reuters.com/article/idUSKBN1700RG/

[41] GReAT (2017). *Lazarus Under the Hood*. SecureList. Available at https://web.archive.org/web/20240122093608/https://securelist.com/lazarus-under-the-hood/77908/ [Archived on: 24.01.2024].

[42] Nicole Perlroth (2017). *More Evidence Points to North Korea in Ransomware Attack*. New York Times. Available at https://web.archive.org/web/20230527201804/https://www.nytimes.com/2017/05/22/technology/north-korea-ransomware-attack.html [Archived on: 27.05.2023].

[43] Olivia Solon (2017). *WannaCry ransomware has links to North Korea, cybersecurity experts say*. The Guardian. Available at https://web.archive.org/web/20231128162545/https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group [Archived on: 28.11.2023].

[44] BBC (2017). *Cyber-attack: US and UK blame North Korea for WannaCry*. Available at https://web.archive.org/web/20231003082959/https://www.bbc.com/news/world-us-canada-42407488 [Archived on: 03.10.2023].

[45] US Federal Bureau of Investigation (2023). *FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft*. Available at https://web.archive.org/web/20240102065440/https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft [Archived on: 02.01.2024].

[46] Ryan Shershtobitoff (2018). *'Operation Sharpshooter' Targets Global Defense, Critical Infrastructure*. McAfee. Available at https://web.archive.org/web/20230927040937/https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/ [Archived on: 27.09.2023].

[47] Scott Ferguson (2018). *'Operation Sharpshooter': Lazarus Revived or False Flag Operation?* DarkReading. Available at https://web.archive.org/web/20240214144516/https://www.darkreading.com/cybersecurity-operations/-operation-sharpshooter-lazarus-revived-or-false-flag-operation- [Archived on: 14.02.2024].

[48] AFIRST.SH (2023). *Anti-Forensic Techniques Used by Lazarus Group.* AhnLab Security Intelligence Center. Available at https://web.archive.org/web/20231128092124/https://asec.ahnlab.com/en/48223/ [Archived on: 28.11.2023].

[49] Mat di Salvo (2023). *North Korean Hackers pocketed more than $100M in Atomic Wallet Hack.* Decrypt. Available at https://web.archive.org/web/20231204040055/https://decrypt.co/144444/north-korean-hackers-pocket-over-100-m-in-atomic-wallet-heist [Archived on: 04.12.2023].

[50] Bruce Schneier (2014). *Did North Korea Really Attack Sony?* The Atlantic. Available at https://web.archive.org/web/20231215161605/https://www.schneier.com/essays/archives/2014/12/did_north_korea_real.html [Archived on: 15.12.2023].

[51] Andy Greenberg (2019). *The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History.* Wired. Available at https://web.archive.org/web/20231207100657/https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/ [Archived on: 07.12.2023].

About the authors

- **Kerstin Zettl-Schabath** is a researcher at the Institute of Political Science (IPW) at Heidelberg University.
- **Alisa Jazxhi** is a political science student at the Institute for Political Science (IPW) at Heidelberg University and a Student Assistant for the European Repository of Cyber Incidents.
- **Camille Borrett** is a Data Analyst at the German Institute for International and Security Affairs (SWP).

Last updated 18.02.2024