The DPRK delicate sound of cyber

blog.sekoia.io/the-dprk-delicate-sound-of-cyber/

16 December 2022

Jamila B. and Threat & Detection Research Team - TDR December 16 2022
2058 0

Read it later Remove

14 minutes reading

This blogpost aims at contextualising and analysing trends pertaining to cyber malicious activities associated to the Democratic People's Republic of Korea-nexus Intrusion Sets reported in open sources in 2022.

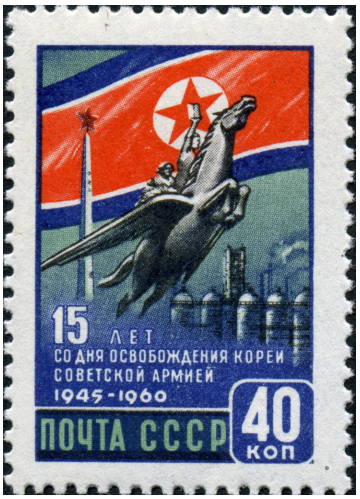
TLDR;

• All known Intrusion Sets associated to the Democratic People's Republic of Korea (DPRK) were reported being active over the year, Lazarus and Kimsuky activities being the most reported on.

• Kimsuky, Bluenoroff, and Lazarus mandates continue to overlap, and Lazarus, Bluenoroff and Andariel keep on conducting dual objectives operations pertaining to revenue generation (AppleJeus, SnatchCrypto) and cyberespionage (DreamJob), in line with Pyongyang strategic interests.

• DPRK associated Intrusion Sets continued demonstrating efforts to update their TTPs and expand their toolset (Lazarus'use of the BYOVD technique and Kimsuky's Sharpext malware) further contributing to these groups' stealthiness and goals achievement.

• SEKOIA.IO analysts assess cyber malicious campaigns orchestrated by Pyongyang will almost certainly continue in the short-term.



Associated with the development of a ballistic, nuclear, and bacteriological arsenal, the cybernetic component, called "secret war" by Pyongyang, is part of the North Korean offensive approach since at least 2004. DPRK offensive cyber activities include cyberespionage and lucrative campaigns and are resolutely asymmetrical and a force multiplier in subverting international sanctions and funding Pyongyang's economy. These facets contribute to the survival of the North Korean state, as well as maintaining its position within the international system as a "small great power."

DPRK malicious cyber activities involve multiple state organisations, including the Ministry of State Security (MSS aka Bowibu) and the Reconnaissance General Bureau. Associated Intrusion Sets include Lazarus, Bluenoroff, Andariel, Reaper, and Kimsuky.

A saucerful of Secrets

Let there be more spy

All North-Korea-associated Intrusion Sets continued carrying out **cyberespionage activities** throughout the year, with a particularly **high tempo of activity** demonstrated by Lazarus and Kimsuky. Targeted sectors notably included a strong **focus on cryptocurrency-related entities and the aerospace and defence industry** (operation DreamJob). Additional sectors of interest include technology, civil society (journalists, activists, defectors), academia, think tanks, media, and diplomacy, notably pertaining to nuclear policy, Korean Peninsula and Asia-Pacific subject matters. Reported malicious activities suggest a **renewed interest in targeting international organisations** [1] [2] for strategic intelligence collection.

SEKOIA.IO analysts noticed Kimsuky refocusing on their traditional assigned locations, namely the United States (U.S.), Japan, and the Republic of Korea (aka RoK and South Korea), and refocusing on military intelligence collection, as well as expanding their victimology to target the shipping industry [3] and a company involved in carbon credits [4].
Last reported in April 2022, DPRK-nexus Intrusion Set **Reaper** was seen carrying out **targeted surveillance operations** against human rights activists, journalists, and defectors from North Korea notably leveraging the Chinotto malware [5], Goldbackdoor, a variant of the BlueLight malware [6], and newly discovered CloudMensis, a spyware based on RokRAT and designed to target Windows and MacOS systems [7].

Additional DPRK-aligned cyberespionage activities include the targeting of the **energy and military sectors** [8], as well as energy providers in Canada, Japan, and the United States between February and July 2022 [9]. Of note, energy-related targeting is a consistent longstanding assignment for the Andariel Intrusion Set. Additionally, **Andariel** was reported deploying their signature **Maui ransomware** on at least one occasion in 2022 [10]. Based on available information, it is not clear whether the deployment of Maui was part of a lucrative objective and / or an anti-forensic effort from the Intrusion Set. It is also plausible ransomware operations carried out by Andariel are part of **moonlighting activities for personal gain or selffunding**.

You get a good (Dream)job

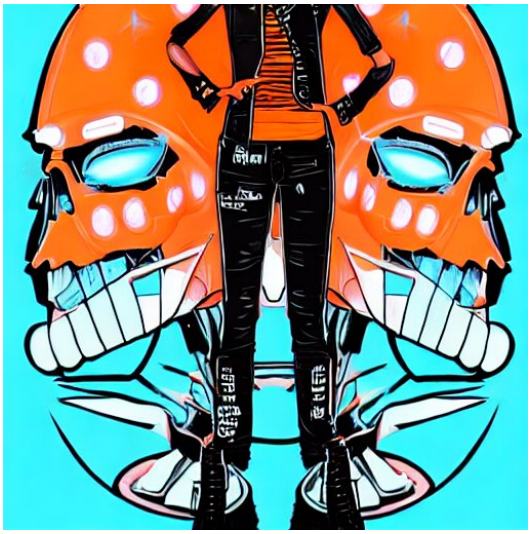
2022 saw the **continuation of DreamJob** (aka ShowState, DeathNote, Operation In(ter)ception), a two-fold campaign run by Lazarus since March 2019. DreamJob encompasses the targeting of aerospace and defence related organisations and individuals, security researchers, and cryptocurrency related entities for cyberespionage and lucrative objectives.

Lazarus continued relying on **social engineering**, including leveraging social networks and messaging applications (notably LinkedIn, WhatsApp and Slack) masquerading as recruiters from defence [11] and cryptocurrency high profile companies. Recent victimology notably includes defence contractors in France, Belgium, Italy, Spain, Germany, Czech Republic, the Netherlands, Poland, Ukraine, Turkey, South Africa, Qatar, and Brazil [12].

SEKOIA.IO analysts assess the targeting of security researchers observed in this campaign likely provides Lazarus with knowledge to improve their Tactics, Techniques and Procedures (TTPs), notably those pertaining to persistence, defence evasion and anti-forensics efforts. This activity also possibly aims at contributing to capacity building for Lazarus, providing them with new tools and malware for follow-up operations.

The DPRK side of the mo(o)ney

DPRK-nexus Intrusion Sets, including Lazarus and Bluenoroff continued carrying out **lucrative cyber campaigns**, notably targeting cryptocurrency and financial technology-related activities. As previously mentioned, this includes part of Operation DreamJob conducted by Lazarus, whose financially motivated aspect was notably illustrated by the targeting of a Brazilian cryptocurrency company with NukeSped [13]. Of note, SEKOIA.IO assess it is likely that Brazil “Bitcoin Law” debates occurring in October 2021 [14] renewed Lazarus’ interest in targeting this country in lucrative motivated campaigns.



Apples and Oranges

Lazarus also continued running the **AppleJeus campaign**, targeting cryptocurrency and fintech platforms and users with backdoored cryptocurrency trading applications, active since at least 2018 [15]. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) publicly attributed the malicious campaign against decentralized finance (DeFi) platform Ronin Network (Axie Infinity) that occurred in March to Lazarus [16].

Snatch that cash

Another long-running campaign called **SnatchCrypto** (aka CryptoCore, DangerousPassword) carried out by **Bluenoroff** since 2017 was still active through 2022 [17]. From SEKOIA.IO analysts' vantage point, this campaign notably includes **TraderTraitor activities**, a series of malicious applications masquerading as trading or price prediction tools, using the Electron framework and cross-platform JavaScript code to deliver the Manuscrypt RAT [18]. This campaign appears **opportunistic** in nature, victimology notably includes Europe, Asia, the U.S., and the UAE.

Financially motivated campaigns are a trademark of DPRK-nexus Intrusion Sets, almost certainly to evade economic sanctions and funding of follow-up cyber malicious campaigns. Open-source reports also indicate funding of nuclear weapons through the Reconnaissance General Bureau (RGB), specifically Bureau 121, which Lazarus, Andariel and Bluenoroff are allegedly subordinated to. However, recent reporting indicates that DPRK-nexus Intrusion Sets tend to hold stolen cryptocurrency for several years, possibly as part of their monetary policy. Another hypothesis is that unlaundered cryptocurrency funds could possibly result from an operator error.

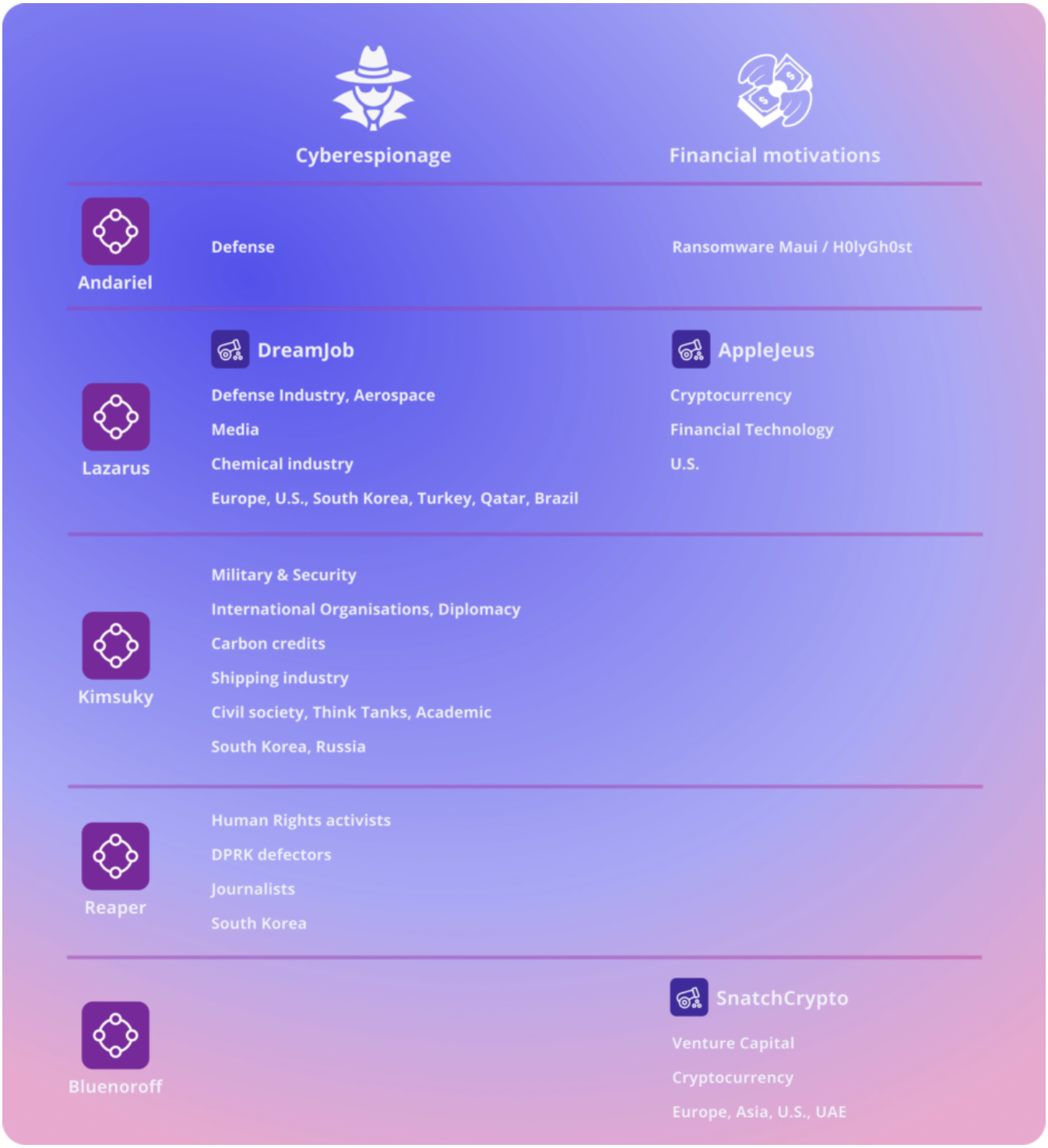
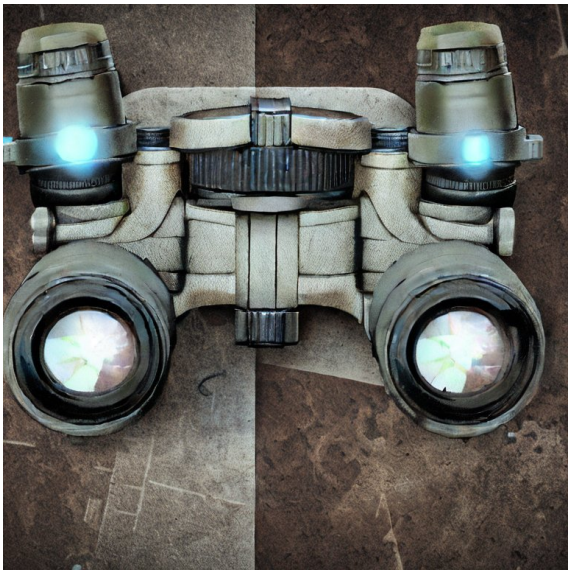


Figure 1. DPRK-nexus Intrusion Sets 2022 activities. Source : SEKOIA.IO

The Peek at the gates

Based on reported TTPs and malware analysis provided in open sources, SEKOIA.IO analysts observed North Korea-nexus Intrusion Sets strong and **continued efforts in selectively targeting their victims and improving their stealthiness**.

Besides advanced reconnaissance efforts, Intrusion Sets can further screen their targets before delivering their payload. For instance, Kimsuky was recently observed using an **IP validation method** as part of its GoldDragon infection mechanism [19]. The same Intrusion Set also newly implemented a **geofencing** mechanism in their signature malware Konni RAT [20], and similar behaviour was observed in the FastSpy infection chain [21]. In a recent campaign Kimsuky also used a file exfiltrator component to find and collect specific files of interest via filelists hosted on a remote server [22].



While North Korea-nexus Intrusion Sets traditionally reuse their infrastructure, they demonstrate increased efforts to achieve stealthiness, notably through obfuscation, defence evasion mechanisms as well as regularly updating their infection chain. Of note, spearphishing remains the principal observed vector of intrusion in these Intrusion Sets malicious cyber activities.

In a campaign against South Korean diplomacy and security-related entities, Kimsuky impersonated a South Korean institution to engage in an email exchange, sending a malicious URL only if the recipient responds positively to the initial email. Similarly, Lazarus was observed hosting a ZIP file containing a malicious document to bypass recent changes made by Microsoft for Office macros [23] . Also increasingly reported is the **hosting of malicious Command and Control (C2) on open-source hosting services** such as DropBox, GitHub or Blogspot.

Of particular interest and documented as a **first seen in the wild in 2022** (although leveraged at least since October 2021 as part of Operation DreamJob), Lazarus' **Bring Your Own Vulnerable Driver (BYOVD)** technique to deploy BLINDINGCAN [24]. Lazarus was also observed leveraging CVE-2022-0609, a 0-day remote code execution vulnerability in Google Chrome web browser to target cryptocurrency and fintech entities through spearphishing, fake websites, or compromised legitimate websites.

These TTPs are a sign of adaptability by North Korea-nexus Intrusion Sets, and SEKOIA.IO analysts assess this is almost certainly a way to preserve their offensive capabilities.

Household objects

Over the course of this year, North Korea-nexus Intrusion Sets continuously dedicated efforts to **update and / or renew their toolsets**. Notable changes to SEKOIA.IO analysts include:

- Lazarus recent development of **KiTTY**, a weaponized PuTTY fork, as part of its BLINDINGCAN infection chain [25].
- **MagicRAT**, a new C++ malware delivered after exploitation of publicly exposed VMware Horizon platforms [26].
- As touched upon before, Kimsuky was observed leveraging new Android malware known as **FastFire, FastViewer, and FastSpy**. Another interesting malicious web browser extension used by Kimsuky is **Sharpext**, used by Kimsuky a post-exploitation tool since 2021 [27].

Is there anybody out there?

Us and them

In 2022, open-source reports mentioned overlaps between DPRK Intrusion Sets and cybercriminal groups, including:

> **Suspected links between Lazarus and Wizard Spider**

Based on infrastructure links, security researchers initially assessed a potential connection between Russia-based cybercriminal group Wizard Spider and Lazarus [28]. Based on the report documenting the Exotic Lily Initial Access Broker (IAB), SEKOIA.IO assess **it is likely that Lazarus resorted to IAB services**, including Exotic Lily's, and entertain connections with the cybercriminal ecosystem.

Connections between Quantum Builder and Lazarus

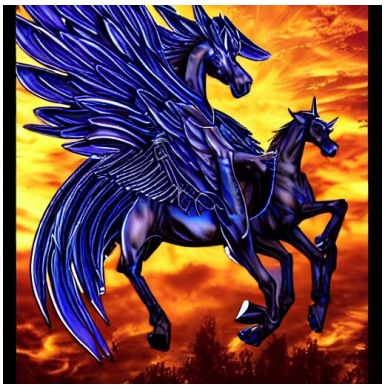
A report published in open sources in June 2022 mentioned a possible use of the .lnk builder Quantum Software / Quantum Builder by Lazarus [29]. Upon script comparison, it was observed the PowerShell script deobfuscation loop and initialization of variables were similar. As Lazarus increasingly resorted to .lnk since the second half of 2020, SEKOIA analysts assess **it is plausible they use Quantum Builder as part of their toolset**.

Connections between DEV-0530 and Andariel

Tracked under the DEV-0530 alias, the cybercriminal group which developed the H0lyGh0st ransomware is assessed to be originating from the DPRK [30]. Microsoft security researchers assess that DEV-0530 “has connections” with Andariel. This assessment is notably based on the observation of communication between DEV-0530 email accounts and Andariel accounts, infrastructure links, as well as DEV0530’s use of tools exclusively used by Andariel. SEKOIA.IO analysts concur with Microsoft hypothesis of moonlighting activities. **It is likely that DEV-0530 is an offshoot of Andariel**.

Wish you were here

In 2022, the **DPRK cyber offensive strategy continued relying on the physical layer**.



In April 2022, two South Korean individuals, the CEO of a virtual asset investment company and an active-duty officer, were charged with violating the South Korea National Security Act for leaking military information to a suspected North Korean agent [32]. The operation reportedly involved a camera watch and a PoisonTap USB device [33] to infiltrate a South Korean military base and gain access to a military laptop between January and March 2022.

In May 2022, the U.S. Department of State issued an advisory, alerting organisations against hiring North Korean IT workers [34].

This highlights that North Korean intelligence operatives continue leveraging individuals, including insider threats, that will notably assist in obtaining access to systems of interest. SEKOIA.IO assess that part of stolen cryptocurrency plausibly contributes to fund incentives for such operations. Furthermore, it is also possible that North Korean IT workers abroad could leverage the acquired skills to carry out malicious campaigns in line with Pyongyang interests.

The Sanction bell

In 2022, DPRK-associated cyber malicious activities garnered **increased attention, in a context of heightened tensions in the Korean Peninsula**.

In January, North Korea’s Internet was hit by two waves of Distributed Denial of Service (DDoS) attacks [35] which turned out to be a hackback carried out by a hacker in retaliation to Lazarus DreamJob campaign [36].

In addition, Nation-State political and economic measures were undertaken. SEKOIA.IO analysts notably observed a more coordinated, time-constrained approach to the attribution process and efforts to hinder malicious cyber activities. U.S. agencies officially attributed the TraderTraitor campaign to Bluenoroff, the Maui ransomware to Andariel [37], and the Ronin Network cryptocurrency theft to Lazarus.

In March 2022, the U.S. Department of Treasury sanctioned Blender.io, a virtual currency mixer, used by Lazarus to launder USD 20.5 million (out of the USD 620 million stolen) on the account of financially supporting DPRK [38]. In August 2022, the U.S. also blacklisted Tornado Cash, a virtual currency mixer used by Lazarus to launder at least USD 7 billion worth of virtual

currency since its creation in 2019 [39]. This was followed by the arrest of a Tornado Cash developer in the Netherlands by the Fiscal Information and Investigation Service (FIOD) [40].

Assessements

Based on DPRK-nexus Intrusion Sets reported activities, SEKOIA.IO analysts assess the following:

- It is almost certain **financially motivated cyber campaigns will remain a high priority for Pyongyang**. DPRK-nexus Intrusion Sets lucrative activities will continue in the short-to-medium term, with a consistent targeting of cryptocurrency and fintech related entities and individuals. It is likely Lazarus and Bluenoroff wil**l expand their victimology to include countries inclined to legalise cryptocurrency and / or where cryptocurrency is a legal tender** (i.e., Ecuador, Central Africa, Salvador).
- It is almost certain that military intelligence, strategic intelligence, and economic intelligence collection and surveillance will remain strong drivers for DPRK-originating cyberespionage campaigns. This notably includes continuation of the long-running campaign DreamJob.
- While ongoing sanction measures are likely to slow down DPRK Intrusion Sets activities in the short-term, SEKOIA.IO analysts assess this is **unlikely to disrupt cyber malicious campaigns orchestrated by Pyongyang**.

SEKOIA.IO will continue monitoring and tracking Intrusion Sets associated to DPRK and welcome any feedback and / or additional input to further contribute to understanding and countering this threat.

External References

[1] [Nikkei] North Korea targeted IAEA in cyberattacks: draft U.N. report.
[2] [Ahnlab] Attack on word documents targeting companies specializing in carbon emissions.
[3] [ESET] (Are you) afreight of the dark? Watch out for Vyveva, new Lazarus backdoor.
[4] [Cluster25] Le groupe nord-coréen « KONNI » cible le secteur diplomatique russe avec de nouvelles versions d'implants de logiciels malveillants.
[5] [Securelist] ScarCruft surveilling North Korean defectors and human rights activists.
[6] [Stairwell] The ink-stained trail of GOLDBACKDOOR.
[7] [ESET] I see what you did there: A look at the CloudMensis macOS spyware.
[8][Symantec] Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage
[9] [Talos] Lazarus and the tale of three RATs.
[10] [Securelist] Andariel deploys DTrack and Maui ransomware.
[11] [MalwareBytes] North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign.
[12] [ESET] Lazarus attacks aerospace and defence contractors worldwide while misusing LinkedIn and WhatsApp.
[13] [ESET] An instance of Operation In(ter)ception by Lazarus for Mac.
[14] [Decrypt] Brazilian Lawmaker Aims to Make Bitcoin a Legal 'Payment Currency'.
[15] [Google TAG] Countering threats from North Korea.
[16] [The Record] US agency attributes \$540 million Ronin hack to North Korean APT group.
[17] [Securelist] The BlueNoroff cryptocurrency hunt is still on.
[18] [U.S. CISA] TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies.
[19] [Securelist] Kimsuky's GoldDragon cluster and its C2 operations.
[20] [Ahnlab] Distribution of Kimsuky Group's xRAT (Quasar RAT) Confirmed.
[21] [S2W] Unveil the evolution of Kimsuky targeting Android devices with newly discovered mobile malware.
[22] [Talos] North Korean attackers use malicious blogs to deliver malware to high-profile South Korean targets.
[23] [MalwareBytes] Microsoft is now disabling Excel 4.0 macros by default.
[24] [Ahnlab] A Case of Malware Infection by the Lazarus Attack Group Disabling Anti-Malware Programs With the BYOVD Technique.
[25] [Microsoft]ZINC weaponizing open-source software.
[26]Talos]MagicRAT: Lazarus' latest gateway into victim networks. (last accessed 16/12/2022)
[27] [Volexity] SharpTongue Deploys Clever Mail-Stealing Browser Extension "SHARPEXT".
[28][Prevailion] What Wicked Webs We Un-weave : https://www.prevailion.com/what-wicked-webs-we-unweave/ (last accessed 16/12/2022)
[29] [Cyble] Quantum Software: LNK File-Based Builders Growing In Popularity.
[30] [Microsoft] North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware.

[31] [Reversing Labs] GwisinLocker ransomware targets South Korean industrial and pharma firms.
[32] [YNA] Leaked military secrets by enlisting active duty officers…Cryptocurrency exchange representative arrested and indicted.
[33] [Samy Kamkar] PoisonTap.
[34] [U.S. Department of State] Guidance on the Democratic People's Republic of Korea Information Technology Workers.
[35] [Reuters] N.Korean internet downed by suspected cyber attacks -43.
[36] [Wired] North Korea Hacked Him. So He Took Down Its Internet.
[37] [U.S. CISA] North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector.
[38] [U.S. Dpt of Treasury] U.S. Treasury Sanctions-Notorious Virtual Currency Mixer Tornado Cash.
[39] [FIOD] Arrest of suspected developer of Tornado Cash.
[40] [NK News] Japan sanctions 5 North Korean companies, following US and South Korea's lead.
Read other blogpost :