The convergence of North Korean cyber threat actors represents a profoundly consequential menace warranting the need for a comprehensive, multi-faceted approach. With a high level of confidence, we attribute this intrusion to threat actors independently associated with North Korea. The target network was compromised, leading to the installation of a backdoor, previously linked to the ScarCruft APT, which we believe was used to facilitate further intrusions.

In light of these findings, it becomes crucial to address and mitigate this threat with utmost vigilance and strategic response. We observed the use of a single IP address for communication with the attackers' malicious infrastructure. This IP, 160.202.79.226, has been associated with various past activities and can be linked to the internal team's discovery.

Further, the domain dallynk.com was accessed, which is commonly attributed to the ScarCruft threat actor. This domain contains malware loading tools and techniques. We also observed similar server functionalities through ScarCruft activity using the RokRAT backdoor. These observations suggest a potential Rift in relations between Russia and North Korea, considering their growing relationship.

We advise particular care into how this infrastructure is further attributed when reviewed historically. For instance, the group associated with the domain dallynk.com could have been manipulated by the threat actors, given the proximity to the May 2022 suspected intrusion date. It's possible that the leaked data comprises a substantial volume of emails unrelated to our current research scope. This emphasizes the need for a robust security strategy to protect against such threats.

The discovery of a jumpcloud intrusion, followed by ScarCruft activity using the RokRAT backdoor, highlights the need for shared resources, infrastructure, implants, or access to victim networks. Moreover, we acknowledge the possibility of a network-wide activity that was not detected.

In mid-May 2022, roughly a week prior to the jumpcloud intrusion discovery, multiple hosts were detected accessing potentially malicious websites. This suggests the presence of a broader threat landscape and the potential for network-wide activity.

While conducting this research, we observed that the backdoor commands are indexed by consecutive integers, a common characteristic among Lazarus group malware. The backdoor's functionality enables full compromise of infected machines, as well as the coordination of multiple drives, such as USBs. If such an event occurs, the malware exits its sleep state before the configured sleep time.

The OpenCarrot variant we analyzed are not protected against timestomping. The malware implements executable code in a section named dll.mui. As part of its initialization process, OpenCarrot ingests configuration data from a file whose name is composed of the extension. The configuration data contains obfuscation. The configuration data also links to lower-confidence BlueNoroff relationships.

With a high level of confidence, we attribute this intrusion to threat actors independently associated with North Korea. Lastly, we advise particular care into how this infrastructure is further attributed when reviewed historically. For instance, the group associated with the domain dallynk.com could have been manipulated by the threat actors, given the proximity to the May 2022 suspected intrusion date.