SentinelLabs has observed an ongoing campaign by Kimsuky, a North Korean APT group, targeting North Korea-related organizations and measures to vitalize them. This activity is spearheaded by the Kimsuky threat actor and involves the distribution of malicious CHM files, which are employed to deliver a VBScript-based malware known as RandomQuery.

**Overview**

This campaign is a continuation of Kimsuky's ongoing efforts to gain unauthorized access to targeted organizations and systems. The use of CHM files is a hallmark of Kimsuky's tactics, as they leverage this file type to deliver malware and subsequently perform system reconnaissance.

**Indicators of Compromise**

The indicators of compromise include:

- **SentinelOne detections**: The malware's ability to extract valuable information such as hardware, operating system, and file details, indicating its pivotal role in Kimsuky's reconnaissance operations for enabling tailored attacks.
- **RandomQuery behavior**: The malware's constant presence in Kimsuky's arsenal, with specific variants designed for different objectives such as information exfiltration.
- **Victim identification**: The campaign's targets are North Korea-related organizations, highlighting the need for enhanced cybersecurity measures to protect against such initiatives.

**RandomQuery**

RandomQuery is a standard staple in Kimsuky's arsenal and comes in various flavors. This campaign specifically uses a VBScript-only implementation. The malware's ability to extract information, such as hardware and system details, lays the groundwork for subsequent precision attacks.

**Conclusion**

Kimsuky strategically employs new TLDs and domain names for malicious infrastructure, mimicking standard .com TLDs, aiming to appear legitimate. This campaign demonstrates the group's consistent approach of delivering malware through CHM files, such as lures containing Document Object Model (DOM) scripting that performs clicks on hyperlinks. The lures are written in Korean, targeting human rights activists and defectors in relation to North Korea. The campaign focuses on reconnaissance and measures to vitalize targeted organizations.