# Article information:

한국 정부 해킹 선포! 중국 해커조직의 실체는 ‘Teng Snake’... KISA도 공격 타깃 지목
<https://www.boannews.com/media/view.asp?idx=113697>

# Article summary:

1. The Chinese hacker organization 'Xiao Qi-ying' declared a large-scale network hacking operation targeting Korean government departments and public institutions on the 21st.

2. It was revealed to be the successor of 'Teng Snake', which has been notorious in Korea for carrying out numerous hacking attacks against Korea and the world.

3. The next target of the attack is the Korea Internet & Security Agency (KISA), which specializes in information protection in Korea, and the wave is getting bigger.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

This article provides an overview of a Chinese hacker organization that declared a large-scale network hacking operation targeting Korean government departments and public institutions on the 21st. The article states that it was revealed to be the successor of 'Teng Snake', which has been notorious in Korea for carrying out numerous hacking attacks against Korea and the world, and that KISA is now being targeted as well.

The article appears to be reliable as it provides detailed information about Teng Snake's past activities, such as their claims to have stolen classified documents from the Ministry of National Defense in May 2021, their recruitment of new members following their announcement of an attack on Korean government networks, and their previous hacks into Samsung, medical fields, construction policy studies websites, etc. However, there are some potential biases present in this article that should be noted. For example, while it does provide some background information about Teng Snake's past activities, it does not explore any counterarguments or other perspectives on these activities or provide any evidence for its claims about them. Additionally, while it does mention possible risks associated with this attack on KISA, it does not provide any details about what those risks may be or how they can be mitigated. Furthermore, while it mentions that Teng Snake has been active since 2021 and has been hacking for countries around the world, it does not provide any details about who these countries are or what kind of data they have stolen from them. Finally, while this article does mention some potential risks associated with this attack on KISA, it does not provide any details about what those risks may be or how they can be mitigated.

In conclusion, while this article appears to be reliable overall due to its detailed information regarding Teng Snake's past activities and its mention of potential risks associated with this attack on KISA, there are some potential biases present that should be noted when considering its trustworthiness and reliability.

# Topics for further research:

* Teng Snake hacking attacks
* Counterarguments to Teng Snake activities
* Mitigation strategies for KISA attack
* Countries targeted by Teng Snake
* Types of data stolen by Teng Snake
* Potential risks of KISA attack

# Report location:

<https://www.fullpicture.app/item/b072aecc16165fab196791a1580e7ca1>