From Social Engineering to DMARC Abuse: TA427's Art of Information Gathering | Proofpoint US

By Greg Lesnewich, Crista Giering, and the Proofpoint Threat Research Team

Published: 2024-04-11 · Archived: 2026-04-05 15:18:29 UTC

Key takeaways

- TA427 regularly engages in benign conversation starter campaigns to establish contact with targets for long-term exchanges of information on topics of strategic importance to the North Korean regime.
- In addition to using specially crafted lure content, TA427 heavily leverages think tank and non-governmental organization-related personas to legitimize its emails and increase the chances that targets will engage with the threat actor.
- To craftily pose as its chosen personas, TA427 uses a few tactics including DMARC abuse in concert with free email addresses, typosquatting, and private email account spoofing.
- TA427 has also incorporated web beacons for initial reconnaissance of its targets, establishing basic information like that the email account is active.

Overview

Proofpoint researchers track numerous state-sponsored and state-aligned threat actors. TA427 (also known as Emerald Sleet, APT43, THALLIUM or Kimsuky), a Democratic People's Republic of Korea (DPRK or North Korea) aligned group working in support of the Reconnaissance General Bureau, is particularly prolific in email phishing campaigns targeting experts for insight into US and the Republic of Korea (ROK or South Korea) foreign policy.

Since 2023, TA427 has directly solicited foreign policy experts for their opinions on nuclear disarmament, US-ROK policies, and sanction topics via benign conversation starting emails. In recent months, Proofpoint researchers have observed (Figure 1) a steady, and at times increasing, stream of this activity. While our researchers have consistently observed TA427 rely on social engineering tactics and regularly rotating its email infrastructure, in December 2023 the threat actor began to abuse lax Domain-based Message Authentication, Reporting and Conformance (DMARC) policies to spoof various personas and, in February 2024, began incorporating web beacons for target profiling.

It is this initial engagement, and the tactics successfully leveraged by TA427, which this blog is focused on.

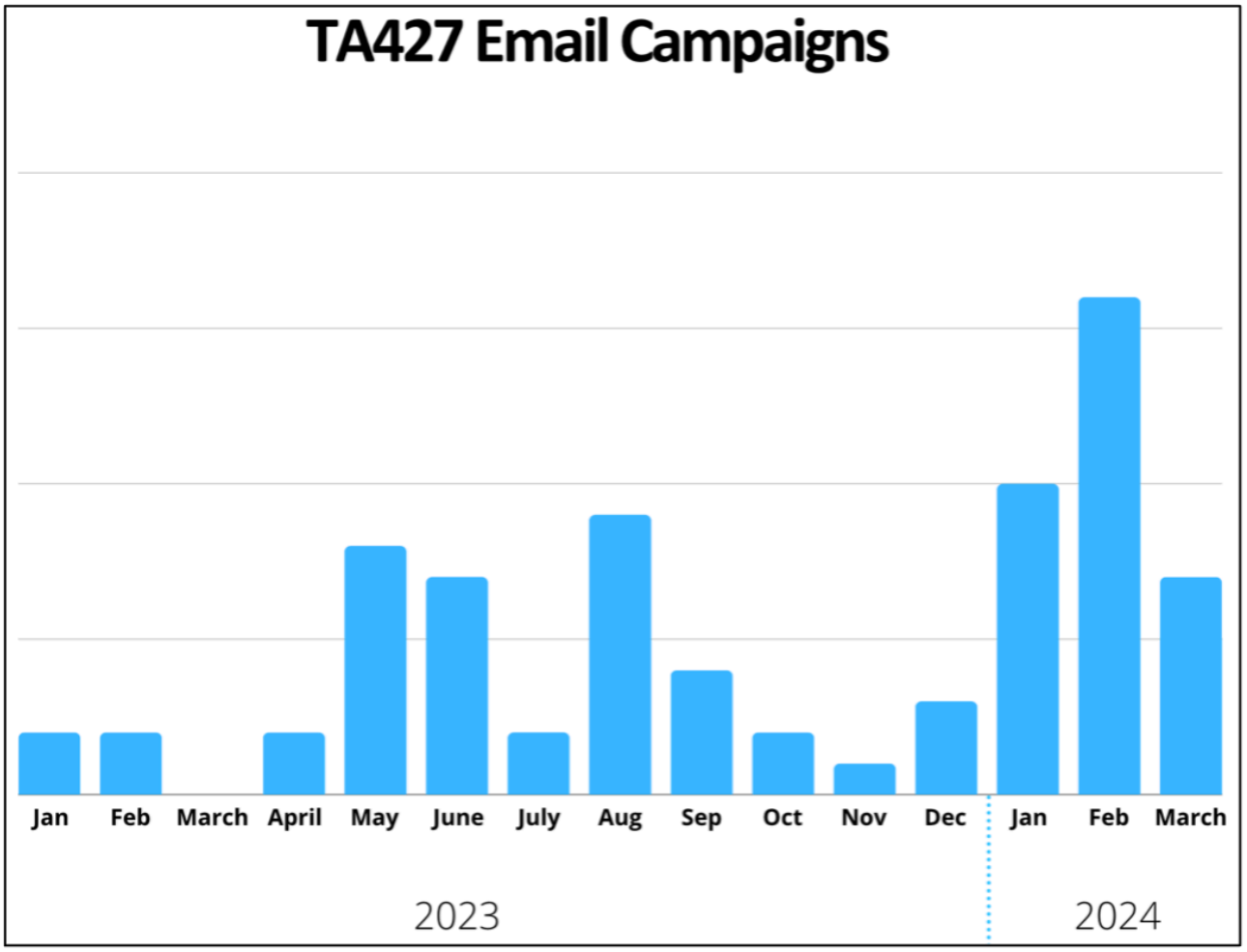


Figure 1. Volume of TA427 phishing campaigns observed between January 2023 and March 2024.

Social engineering

TA427 is a savvy social engineering expert whose campaigns are likely in support of North Korea's strategic intelligence collection efforts on US and ROK foreign policy initiatives. Based on the targets identified and the information sought, it is believed that TA427's goal is to augment North Korean intelligence and inform its foreign policy negotiation tactics (example Figure 2). TA427 is known to engage its targets for extended periods of time through a series of benign conversations to build a rapport with targets that can occur over weeks to months. They do so by constantly rotating which aliases are used to engage with the targets on similar subject matter.

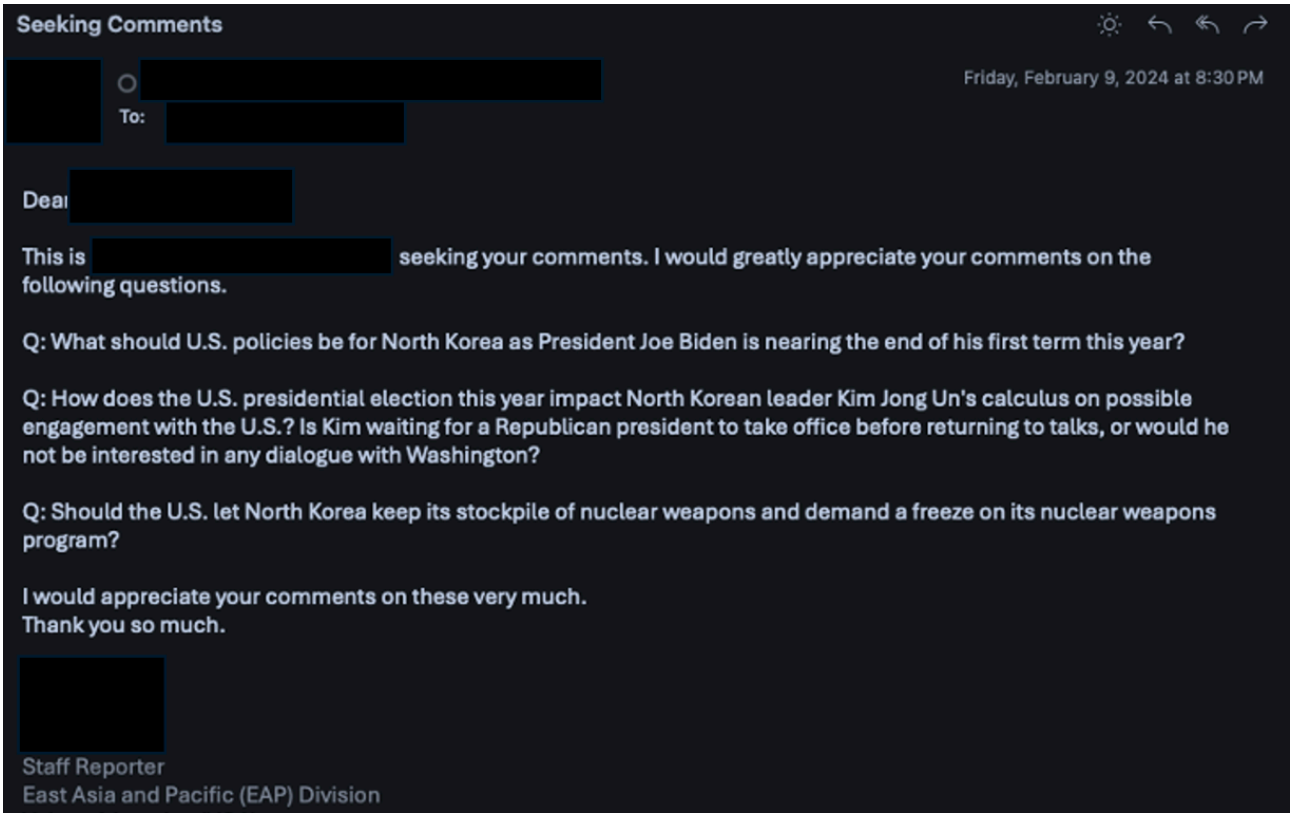


Figure 2. Example of TA427 campaign focused on US policy during an election year.

Using timely, relevant lure content (as seen in Figure 3) customized for each victim, and often spoofing individuals in the DPRK research space with whom the victim is familiar to encourage engagement, targets are often requested to share their thoughts on these topics via email or a formal research paper or article. Malware or credential harvesting are never directly sent to the targets without an exchange of multiple messages, and based on Proofpoint visibility, rarely utilized by the threat actor. It is possible that TA427 can fulfill its intelligence requirements by directly asking targets for their opinions or analysis rather than from an infection. Additionally, insight gained from the correspondence is likely used to improve targeting of the victim organization and establish rapport for later questions and engagement.

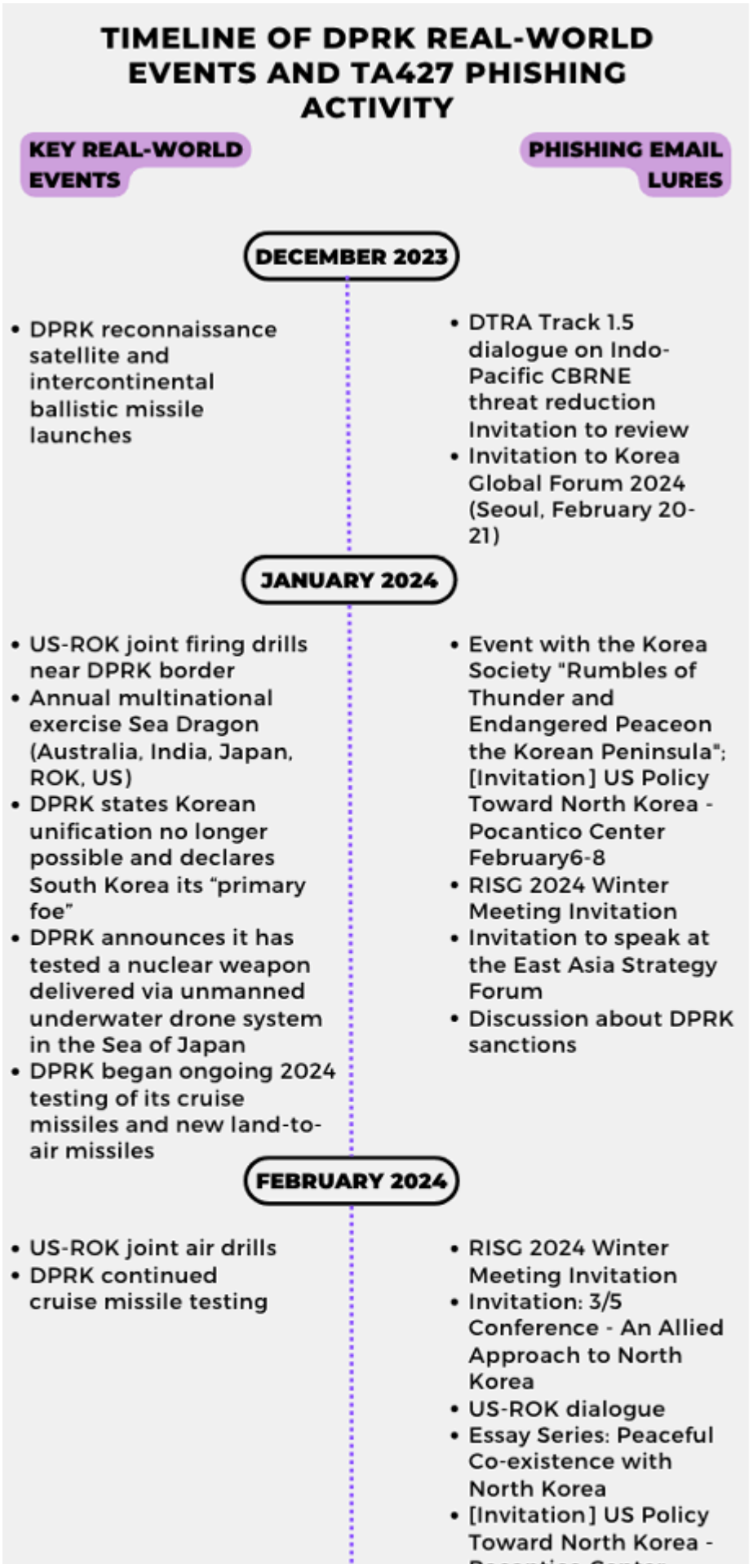
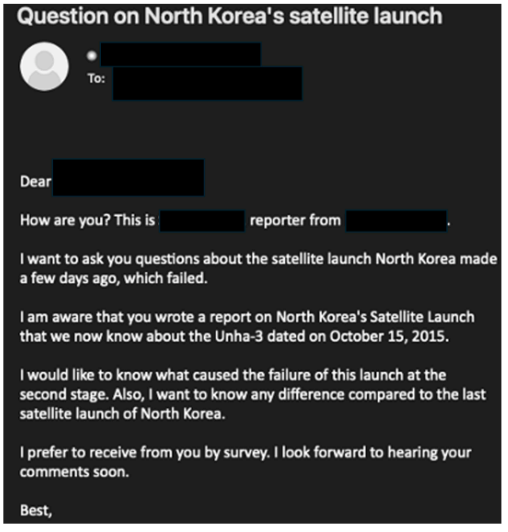

TIMELINE OF DPRK REAL-WORLD EVENTS AND TA427 PHISHING ACTIVITY
KEY REAL-WORLD EVENTS
PHISHING EMAIL LURES
DECEMBER 2023
• DPRK reconnaissance satellite and intercontinental ballistic missile launches
• DTRA Track 1.5 dialogue on Indo-Pacific CBRNE threat reduction Invitation to review
• Invitation to Korea Global Forum 2024 (Seoul, February 20-21)
JANUARY 2024
• US-ROK joint firing drills near DPRK border
• Annual multinational exercise Sea Dragon (Australia, India, Japan, ROK, US)
• DPRK states Korean unification no longer possible and declares South Korea its "primary foe"
• DPRK announces it has tested a nuclear weapon delivered via unmanned underwater drone system in the Sea of Japan
• DPRK began ongoing 2024 testing of its cruise missiles and new land-to-air missiles
• Event with the Korea Society "Rumbles of Thunder and Endangered Peaceon the Korean Peninsula"; [Invitation] US Policy Toward North Korea - Pocantico Center February6-8
• RISG 2024 Winter Meeting Invitation
• Invitation to speak at the East Asia Strategy Forum
• Discussion about DPRK sanctions
FEBRUARY 2024
• US-ROK joint air drills
• DPRK continued cruise missile testing
• RISG 2024 Winter Meeting Invitation
• Invitation: 3/5 Conference - An Allied Approach to North Korea
• US-ROK dialogue
• Essay Series: Peaceful Co-existence with North Korea
• [Invitation] US Policy Toward North Korea -

Figure 3. Timeline of real-world events based on international press reporting, side-by-side with Proofpoint observed subject lures.

Lure content often includes invitations to attend events about North Korean policies regarding international affairs, questions regarding topics such as how deterrence of other states has shaped North Korean policies, the prospect of a nuclear weapons program being developed in the ROK, if nuclear weapons would be used in a potential Chinese conflict with Taiwan, and requests to submit papers on similar subjects. Such questions and cold outreaches (Figure 4 and 5) are considered normal in the think tank and academic space, allowing TA427 to blend in.



Figures 4 and 5. Examples of TA427 cold outreaches to experts.

TA427 also weaves conversations in multiple email threads between a target's personal and corporate email addresses, likely to avoid security controls on corporate email gateways. This establishes some amount of trust but allows for the rare instances of malware, such as ReconShark, to be deployed to a corporate device if the victim is using their corporate computer to check personal email.

TA427's most impersonated

TA427's benign campaign activity tends to impersonate individuals that work in the following verticals: thinks tanks and non-governmental organizations (NGOs), media, academia, and government. TA427 usually masquerades as members of think tanks and NGOs to engage targets (Figure 6). This is likely due to better odds of successfully convincing targets of the legitimacy of the threat actor's requests for information or engagement by using such personalities. Over the years, Proofpoint researchers have observed TA427 pose as many well-known thinks tanks and NGOs, including the Stimson Center, the Atlantic Council, the Wilson Center, the Ronald Reagan Presidential Foundation and Institute, and the Maureen and Mike Mansfield Foundation, among others.

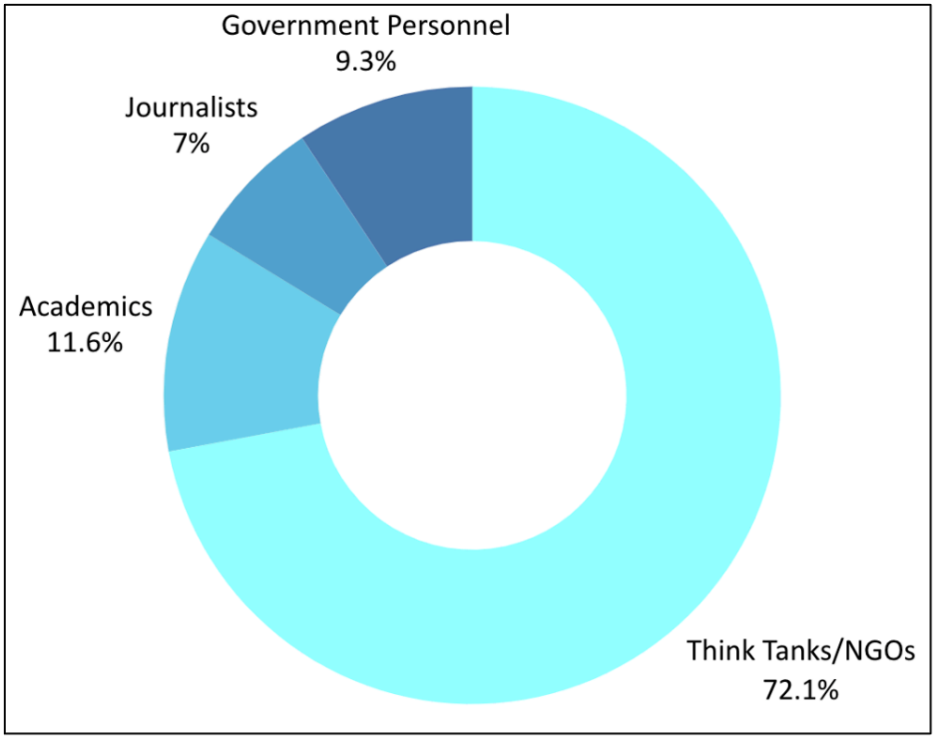


Figure 6. Percent of campaigns leveraging personas from four main verticals between January 2023 and March 2024.

Further, TA427 tends to rely on one of three methods of impersonation for this activity (Figure 7), specifically DMARC abuse, which will be delved into further in the next section, typosquatting (Figure 8), and private email account spoofing using free email services.

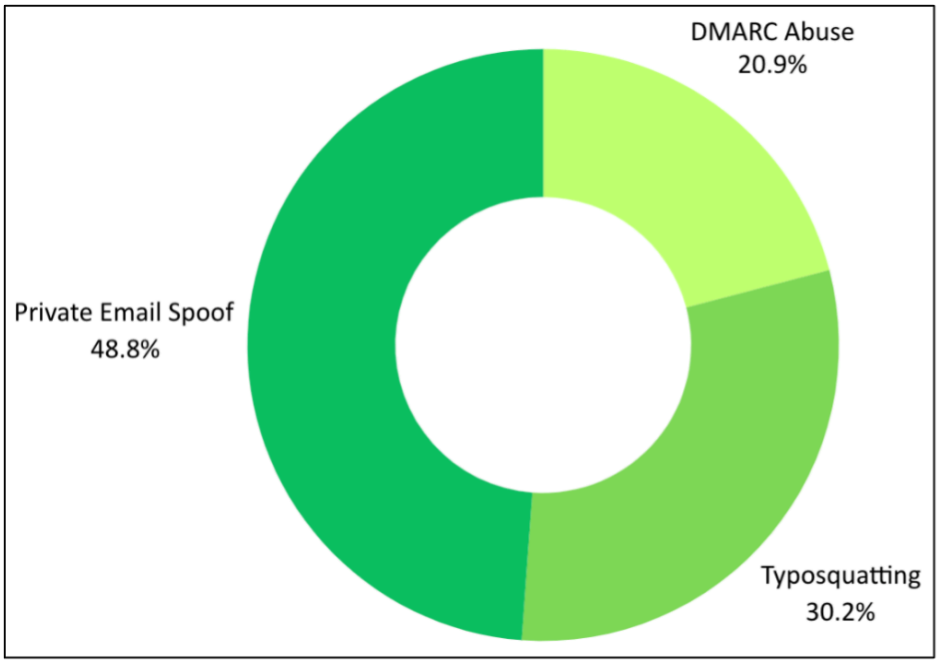


Figure 7. Percent of campaigns using DMARC abuse, private email account spoofing, and typosquatting to masquerade as various personas from January 2023 through March 2024.

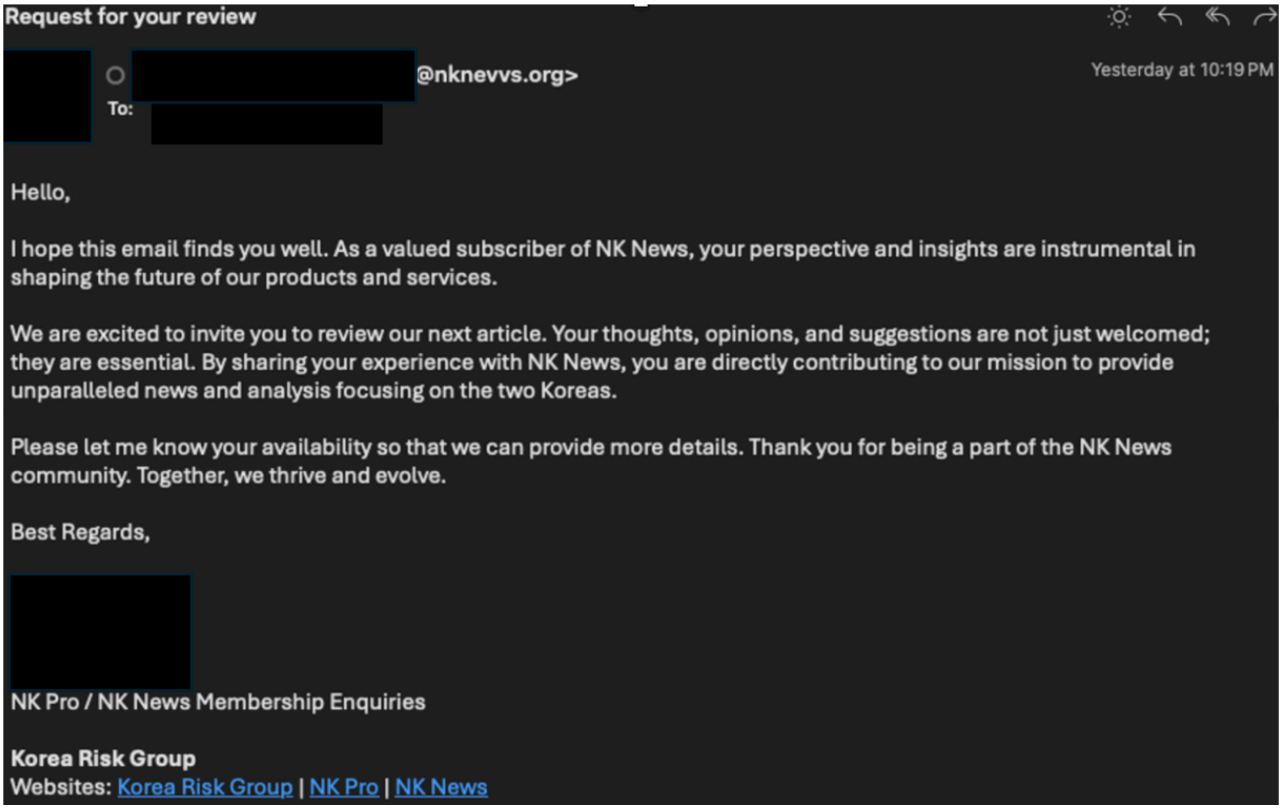


Figure 8. Example of TA427 campaign using typosquatting with an actor-controlled email sender of "nknevvs" instead of "nknews" to masquerade as the popular NK News publication.

DMARC spoofing

DMARC is an open email authentication protocol that provides domain-level protection of the email channel. DMARC authentication uses previously established standards, SPF and DKIM, using DNS TXT records and key exchanges to validate the senders.

Since December 2023, many of the entities that TA427 has spoofed either did not enable or enforce DMARC policies. A permissive DMARC policy such as "v=DMARC1; p=none; fo=1;" allows for spoofed emails to bypass security checks. This also ensures delivery to the targeted user even if security checks fail, and TA427 will modify the header to display the sender being from the spoofed organization. TA427 then uses free email addresses spoofing the same persona in the reply-to field to convince the target that they are engaging with legitimate personnel.

Proofpoint provides a free DMARC record checking tool that can be used to check the domain record of an organization and validate that it does not have a permissive policy.

Web beacon usage

The use of web beacons is a new tactic for TA427, which Proofpoint researchers first observed in February 2024. Web beacons, which are commonly referred to as tracking pixels, tracking beacons, and web bugs and are known to be leveraged by other advanced persistent threat actors, embed a hyperlinked non-visible object within the body of an email that, when enabled, attempt to retrieve a benign image file from an actor-controlled server. The web beacons are likely intended as initial reconnaissance to validate targeted emails are active and to gain fundamental information about the recipients' network environments, including externally visible IP addresses, User-Agent of the host, and time the user opened the email.

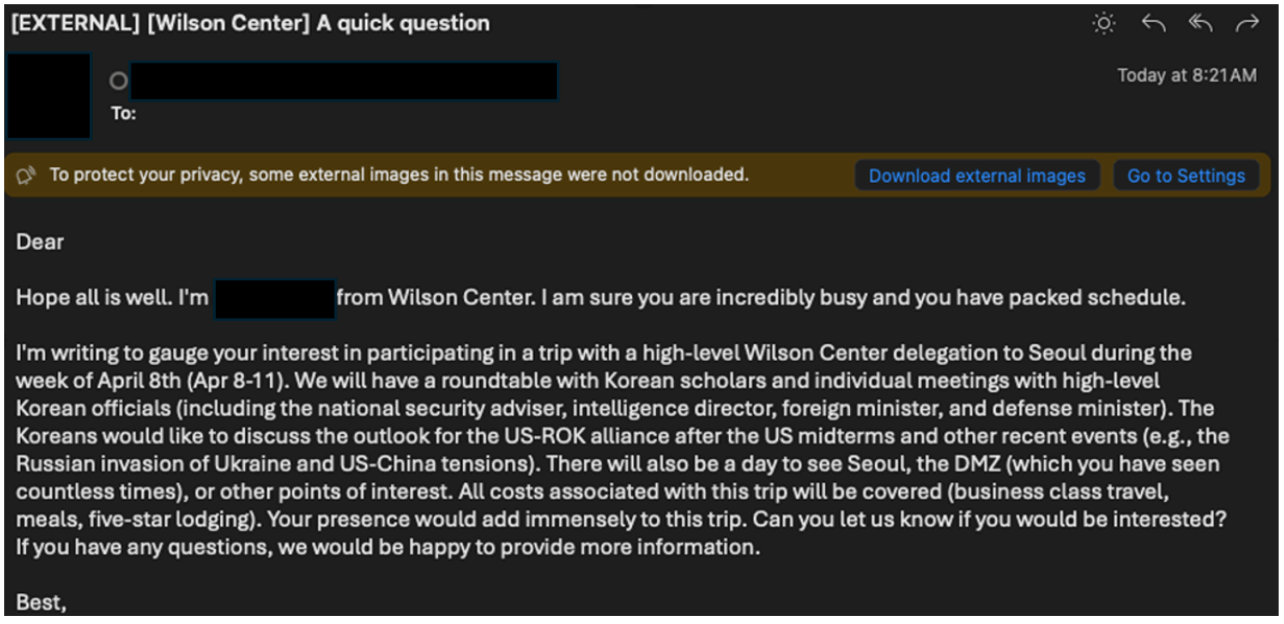


Figure 9. Example of TA427 campaign using a web beacon.

Conclusion

TA427 is one of the most active state-aligned threat actors currently tracked by Proofpoint. While the campaigns noted in this blog are not fleecing targets out of millions of dollars, this activity goes after something that is

infinitely more difficult to quantify: information and influence. For years, this threat actor has been impersonating key DPRK subject matter experts in academia, journalism, and independent research to target other experts and gain footholds at their respective organizations for long-term strategic intelligence gathering. With a clear degree of success, TA427 shows no indication of slowing down or losing its agility in adjusting its tactics and standing up new infrastructure and personas with expediency.

Indicators of compromise (IOCs)

Indicator	Type
Track 1.5 dialogue on CBRNE threat reduction in the Indo-Pacific Invitation: August DPRK meeting Draft Taiwan Issue emergence of Indigenous Nuclear Weapons Debate Request for Meeting(Korean Embassy) Invitation: 20/9 Conference - An Allied Approach to North Korea Invitation: 30/9 Conference - An Allied Approach to North Korea Request for Comments Invitation: 25/10 Conference - An Allied Approach to North Korea Invitation to CTR Workshop November 9 DTRA Track 1.5 dialogue on Indo-Pacific CBRNE threat reduction Invitation to review Invitation to Korea Global Forum 2024 (Seoul, February 20-21) Event with the Korea Society "Rumbles of Thunder and Endangered Peaceon the Korean Peninsula" [Invitation] US Policy Toward North Korea - Pocantico Center February6-8 RISG 2024 Winter Meeting Invitation Invitation to speak at the East Asia Strategy Forum Discussion about DPRK sanctions Invitation: 3/5 Conference - An Allied Approach to North Korea	2023 & 2024 Email Subjects

US-ROK dialogue Seeking Comments Essay Series: Peaceful Co-existence with North Korea [Invitation] US Policy Toward North Korea - Pocantico Center March 12-14 Invitation as a Discussant for a US-ROK Research Project Seminar Lunch Invitation to meet with Senior Deputy Minister for Foreign Affiars	
stimson[.]shop stimsonn[.]org nknevvs[.]org wilsoncenters[.]org wilsoncentre[.]org	2023 & 2024 Spoofed Domains

---

Source: https://www.proofpoint.com/us/blog/threat-insight/social-engineering-dmarc-abuse-ta427s-art-information-gathering