JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: CSA-20230601-1

June 1, 2023

North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media

SUMMARY

The Federal Bureau of Investigation (FBI), the U.S. Department of State, and the National Security Agency (NSA), together with the Republic of Korea's National Intelligence Service (NIS), National Police Agency (NPA), and Ministry of Foreign Affairs (MOFA), are jointly issuing this advisory to highlight the use of social engineering by Democratic People's Republic of Korea (DPRK a.k.a. North Korea) state-sponsored cyber actors to enable computer network exploitation (CNE) globally against individuals employed by research centers and think tanks, academic institutions, and news media organizations. These North Korean cyber actors are known to conduct spearphishing campaigns posing as real journalists, academics, or other individuals with credible links to North Korean policy circles. The DPRK employs social engineering to collect intelligence on geopolitical events, foreign policy strategies, and diplomatic efforts affecting its interests by gaining illicit access to the private documents, research, and communications of their targets.

BACKGROUND

North Korea's cyber program provides the regime with broad intelligence collection and espionage capabilities. The Governments of the United States and the Republic of Korea (ROK a.k.a. South Korea) have observed sustained information-gathering efforts originating from these North Korean cyber actors. North Korea's primary military intelligence organization, the Reconnaissance General Bureau (RGB), which has been sanctioned by the United Nations Security Council, is primarily responsible for this network of actors and activities.

We assess the primary goals of the DPRK regime's cyber program include maintaining consistent access to current intelligence about the United States, South Korea, and other countries of interest to impede any political, military, or economic threat to the regime's security and stability.

Currently, the U.S. and ROK Governments, and private sector cyber security companies, track a specific set of DPRK cyber actors conducting these large-scale social engineering campaigns as

Kimsuky, Thallium, APT43, Velvet Chollima, and Black Banshee. Kimsuky is administratively subordinate to an element within North Korea's RGB and has conducted broad cyber campaigns in support of RGB objectives since at least 2012. Kimsuky actors' primary mission is to provide stolen data and valuable geopolitical insight to the North Korean regime.

Some targeted entities may discount the threat posed by these social engineering campaigns, either because they do not perceive their research and communications as sensitive in nature, or because they are not aware of how these efforts fuel the regime's broader cyber espionage efforts. However, as outlined in this advisory, North Korea relies heavily on intelligence gained by compromising policy analysts. Further, successful compromises enable Kimsuky actors to craft more credible and effective spearphishing emails that can be leveraged against more sensitive, higher-value targets. The authoring agencies believe that raising awareness of some of these campaigns and employing basic cyber security practices may frustrate the effectiveness of Kimsuky spearphishing operations. This advisory provides detailed information on how Kimsuky actors operate; red flags to consider as you encounter common themes and campaigns; and general mitigation measures for entities worldwide to implement to better protect against Kimsuky's CNE operations.

If you believe you have been targeted in one of these spearphishing campaigns, whether or not it resulted in a compromise (particularly if you are a member of one of the targeted sectors), please file a report with www.ic3.gov and reference #KimsukyCSA in the incident description.

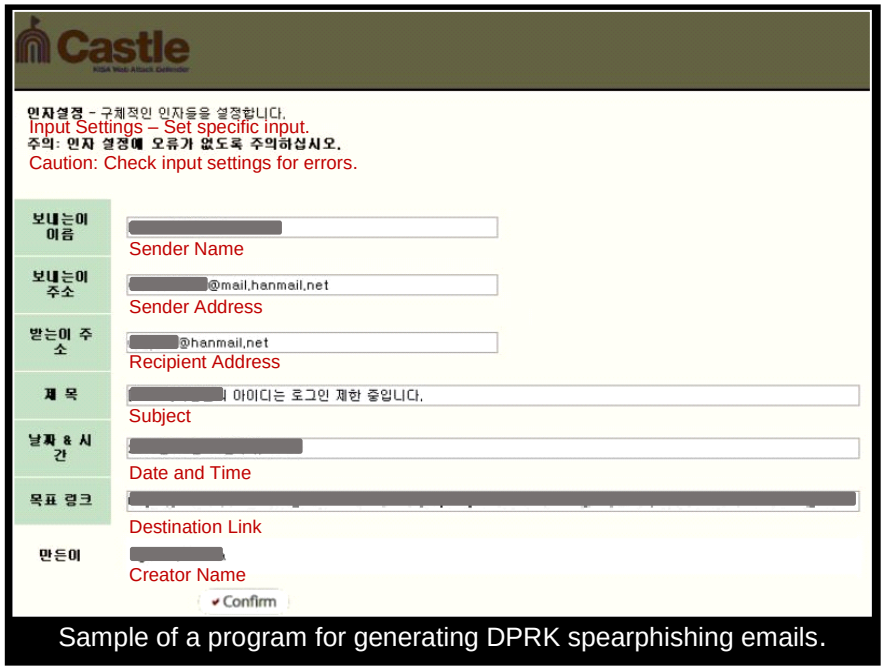
Please include as much detail as you can about the incident including the sender email address and the text of the email message, specifying any links/URLs/domains. Please specify whether you responded to the email, clicked on any links, or opened any attachments. Please retain the original email and attachments in case you are contacted by an investigator for further information.

- Please visit **www.ic3.gov** and use **#KimsukyCSA** in your submission.
- The U.S. Government also encourages victims to report suspicious activities, including any suspected DPRK cyber activities, to local FBI field offices.
- For the ROK government, you can report suspicious activities to the National Intelligence Service (www.nis.go.kr, 111), the National Police Agency (ecrm.police.go.kr, 182), or the Korea Internet & Security Agency (boho.or.kr, 118)

KIMSUKY OPERATIONS: SOCIAL ENGINEERING

In a cybersecurity context, social engineering is a broad term referring to the use of deception to exploit human error and manipulate a target into unwittingly exposing confidential or sensitive information for fraudulent purposes. DPRK cyber actors employ social engineering techniques to enable much of Pyongyang's malicious CNE. Among social engineering techniques, Kimsuky actors use spearphishing—or the use of fabricated emails and digital communications tailored to deceive a target—as one of their primary vectors for initiating a compromise and gaining access into a target's devices and networks. For over a decade, Kimsuky actors have continued to refine their social engineering techniques and made their spearphishing efforts increasingly difficult to discern.

A Kimsuky spearphishing campaign begins with broad research and preparation. DPRK cyber actors often use open-source information to identify potential targets of value and then tailor their online personas to appear more realistic and appealing to their victims.



Sample of a program for generating DPRK spearphishing emails.

The Kimsuky actors will create email addresses that resemble email addresses of real individuals they seek to impersonate and generate domains that host the malicious content of a spearphishing message. DPRK actors often use domains that resemble common internet services and media sites to deceive a target.

- For example, Kimsuky actors are known to impersonate well-known news outlets and journalists using a domain such as "@XYZkoreas.news" spoofing a real news station while actual emails from the news service appear as "@XYZnews.com."

- DPRK cyber actors commonly take on the identities of real people to gain trust and establish rapport in their digital communications. Kimsuky actors may have previously compromised the email accounts of the person whom they are impersonating. This allows the actors to search for targets while scanning through compromised emails, with a particular focus on work-related files and personal information pertaining to retirees, social clubs, and contact lists. They craft convincing spearphishing emails by repurposing the person's email signature, contact list, and past email exchanges. DPRK cyber actors are also known to compromise

email accounts belonging to foreign policy experts and subsequently create a secondary email account, using the email account and identity of the expert to communicate with other significant targets.

- In other cases, a Kimsuky actor will use multiple personas to engage a target; one persona to conduct initial outreach and a second persona to follow-up on the first engagement to distract a potential victim from discerning the identity of the original persona. Another tactic is to "resend" or "forward" an email from a source trusted by a target.

- The initial phishing email occasionally contains a malicious link or document, often purporting to be a report or news article. These attached malicious documents are frequently password-protected, which helps them evade detection by antivirus software and other security measures. However, more often, the initial spearphishing email does not contain any malicious links or attachments and is instead intended to gain the trust of the victim.

- Once DPRK cyber actors establish engagement with a target, the actors attempt to compromise the account, device, or network belonging to the target by pushing malicious content in the form of a malicious macro embedded within a text document. This document is either attached directly to the email, or stored in a file hosting service, such as Google Drive or Microsoft OneDrive. These malicious macros, when enabled, quietly establish connections with Kimsuky command and control infrastructure, and result in the provision of access to the target's device.

- In some cases, Kimsuky actors have developed "spoofed" or fake but realistic versions of actual websites, portals, or mobile applications, and directed targets to input credentials and other information that are harvested by the DPRK. Compromise of a target account can lead to persistent access to a victim's communications, often through a malware used by Kimsuky actors called BabyShark. Kimsuky actors have also been known to configure a victim's email account to quietly auto-forward all emails to another actor-controlled email.

Notably, victim responses to spearphishing lures also provide Pyongyang with the added benefit of insight into foreign policy circles. This covert collection against the community of DPRK watchers is probably of high value to the Kim regime and provides another channel of information on top of what it gains through computer network operations.

Although all DPRK advanced persistent threat groups employ social engineering techniques, the campaigns and themes described in this advisory are specific to Kimsuky.

RED FLAG INDICATORS

Sector targets should be aware of the following activity that may be indications or behaviors of malicious DPRK cyber actors.

- Initial communications are often seemingly innocuous with no malicious links/attachments; follow-on communications usually contain malicious links/documents to facilitate exploitation of a computer or network.
- Email content may include real text of messages recovered from previous victim engagement with other legitimate contacts.
- Emails in English may sometimes have awkward sentence structure and/or incorrect grammar.
- Email content may contain a distinct Korean dialect exclusively used in North Korea.
- Victims/targets with both direct and indirect knowledge of policy information i.e., U.S. and ROK government employees/officials working on North Korea, Asia, China, Southeast Asia matters; U.S. and ROK government employees with high clearance levels; and members of the military, are approached with common themes and questions as referenced in this advisory.
- Email domains look like a legitimate news media site, but do not match the domain of the company's official website. The domains also may be identified as such in open-source malware repositories like Virus Total.
- Spoofed email accounts have subtle incorrect misspellings of the names and email addresses of the legitimate ones listed in a university directory or an official website.
- Malicious documents require the user to click "Enable Macros" to view the document.
- Actors are persistent if the target does not respond to the initial spearphishing email. They will likely send a follow-up email within 2-3 days of initial contact.
- Emails purporting to be from official sources but sent using unofficial email services.

CAMPAIGNS AND THEMES

Kimsuky cyber actors craft their spearphishing campaigns around themes characterizing the target, message content, and the malicious mechanism, or lure, through which a compromise is initiated. The main themes to beware of are impersonations and targeting of **journalists**, **academic scholars**, and **think tank researchers** to:

- solicit responses to foreign policy-related inquiries,
- conduct a survey,
- request an interview,
- review a document,
- request a resume, or
- offer payment for authoring a research paper.

Kimsuky actors tailor their themes to their target's interests and will update their content to reflect current events discussed among the community of North Korea watchers.

The following are examples of real Kimsuky spearphishing attempts that illustrate variations of the common themes. In some instances, the cyber actor poses as a journalist and targets a think tank researcher, while at other times, the DPRK actor may take on the persona of an academic scholar to target other scholars—virtually every combination of these themes and lures has been previously observed.

1. Impersonation of journalists

Kimsuky actors often spoof real journalists and broadcast writers to craft a credible front and make inquiries to prominent individuals working North Korea matters. Usually, the questions will revolve around current events and whether U.S. experts believe North Korea will re-join talks with the U.S., whether they believe North Korea will resume testing its missiles, and how they see China responding. In many instances, Kimsuky actors do not attach malware to their initial email. Instead, they first send an introductory email to inquire about interview opportunities.

Sample email communication 1:

Title: <**name of legitimate Korean journal program**>

Greetings,

My name is <**name of writer**>, and I am a writer for <**name of legitimate Korean journal program**>.

I am writing to you today because I am currently preparing for a program related to North Korean issues. Professor <**name of professor**> of <**actual Korean university**>, whom I contacted earlier, recommended you as an expert on this issue. I would be grateful if you could spare some time to answer a few questions.

Thank you for considering my request. I look forward to hearing from you soon.

Best regards,

Follow-on email: If the targets agree to the interview, the actors will then follow up with a second email containing malicious content.

Title: RE: RE: <**name of legitimate Korean journal program>**

Dear <**name of expert**>,

As promised, I am sending you a questionnaire. It would be greatly appreciated if you could answer each question in 4-5 sentences. Thank you for your cooperation.

Best regards,

@ attached file: [<**name of legitimate Korean journal program**>] questionnaire.docx

Additionally, we have seen Kimsuky actors spoof legitimate journalists to specifically target think tank employees. Kimsuky actors commonly pose questions in their spearphishing emails about current events, such as issues regarding Russia's invasion of Ukraine; U.S.-DPRK relations; DPRK nuclear and security topics; policymaker stances on the Asian region; and thoughts on current China-North Korea and Russia-North Korea relations.

Sample email communication 2:

Greetings,

I hope you've been well! This is <**name of real journalist**> with <**legitimate U.S. news organization**>.

North Korea Fires Powerful Missile on 4 Oct using Old Playbook in a New Worlds. The last time Pyongyang launched a weapon over Japan was in 2017, when Donald J. Trump was president and Kim Jong-un seemed intent on escalating conflict with Washington.

I have some questions regarding this:

1) Would Pyongyang conduct its next nuclear test soon after China's Communist Party Congress in mid-October?

2) May a quieter approach to North Korean aggression be warranted?

3) Would Japan increase the defense budget and a more proactive defense policy?

I would be very grateful if you could send me your answers within 5 days.

Have a good weekend.

Sincerely,

<**name of legitimate journalist**>

2. Impersonation of academic scholars

Kimsuky actors impersonate South Korean academic scholars to send spearphishing emails to researchers at think tanks. In these emails, the targets are asked to participate in a survey, such as on North Korean nuclear issues and denuclearization on the Korean Peninsula or requesting an email interview.

Sample email communication 3:

Title: <**name of legitimate Korean think tank institute**> Request for survey

Hello,

I am <**name of an academic scholar**> from <**name of legitimate Korean think tank**>.

I am reaching out to ask if you would be willing to participate in a survey on North Korea's nuclear development titled, "A survey on the perception on experts on the advancement of North Korean nuclear weapons and the denuclearization of the Korean Peninsula". Our goal is to find ways to resolve North Korean nuclear issues and achieve denuclearization on the Korean Peninsula. Rest assured that all answers will be kept confidential and used solely for research purpose. As a token of appreciation, we would like to offer 300,000 won to those who participate in the survey. If you're interested in participating, please reply to this message, and we will send you the survey questionnaire. Looking forward to hearing from you soon.

Best regards,

Follow-on email: Once targets respond to inquiries, Kimsuky actors send them a survey questionnaire and a document form for payment, which contains malicious content.

Title: RE: RE: <**name of legitimate Korean think tank institute**> Request for survey

Thank you for your response.

We will send you a document form for payment, which includes a personal information usage agreement. If possible, please fill out your affiliation, name, ID number, bank account, and signature, and attach copies of your bankbook and ID card.

Best regards,

P.S. The attached document is password-protected, and I will send you the password in a 'password.txt file'

@ attached file: PersonalInformationUsageAgreement

Sample email communication 4:

Below is an example of Kimsuky actors pursuing responses to questions on sector targets by posing as a university professor and research student. Once an initial response is received, actors will request an email interview with a list of questions and request that targets access documents via a malicious link to a cloud-hosted service.

To: <**name of foreign affairs expert**>

Subject: Re: Request for an interview

Dear <**name of foreign affairs expert**>, Sorry for my late response because of the Profs busy time and thanks so much for replying me your kind answers. I did confer with <legitimate U.S. University Professor >about it and modified a bit. Please find the link below and let me know if you have the different opinions.

https: <**malicious drive link**>

PWD: <**redacted**>

Best, <**fictitious university student**>

To: <**foreign affairs expert**>

Cc: <**scholar**>

Dear <**foreign affairs expert**>, Thanks so much for your fast feedback. I did confer with <**legitimate U.S. university professor**> again and complete it as your request. Please find the updated below. https: <**malicious drive link**>

PWD: <**redacted**>

We're planning to upload it on our website within a week after final review. Please feel free to contact with me if you have any questions.

Best, <**fictitious university student**>

3. Impersonation of think tank researchers

Kimsuky actors impersonate researchers from legitimate South Korean think tanks to send spearphishing emails to political and North Korean experts. They initiate communication by sending genuine emails to establish rapport and seek opinions on various topics, such as “North Korea’s foreign policy and our response.”

Sample email communication 5:

Title: [Request for opinion] I'm <**name of legitimate Korean think tank**> <**name of deputy director**>

Greetings,

I am <**name of legitimate Korean think tank**>, deputy director of the <**name of deputy director**>.

I am reaching out to you to discuss an article I am currently working on.

The topic, "North Korea's foreign policy and South Korea's response" is somewhat distant from my expertise, so I would greatly appreciate hearing the opinions of experts like you.

I would kindly request your comments on my writing, as I believe you are the most appropriate person to provide valuable insights on the subject. Your earlier article caught my attention, and I found myself nodding in agreement with each sentence. That is why I feel confident in asking for your opinion.

I am eagerly awaiting your reply and appreciate your willingness to assist me. Thank you for your time and consideration.

Follow-on email: After receiving replies from their targets, the Kimsuky actors exchange multiple emails, which may include attachments containing malicious links or files and instructions on how to open the attached files. Even after stealing the account information of their victims and infecting their devices with malware, they sometimes continue to send "thank you" emails to their targets.

Title: RE: RE: [Request for opinion] I'm <**name of legitimate Korean think tank**> <**name of deputy director**> <**attached large size file**>

Thank you for agreeing to provide your opinion. Please find the attached files.

We greatly appreciate your input. To ensure security in the face of increasing hacking activity, we have set a password (<**password string**>) for the attached file.

We look forward to hearing your valuable feedback.

Sample email communication 6:

Below is an example of Kimsuky actors spoofing a think tank employee and utilizing a spoofed think tank domain in order to target another think tank employee. Once the target responds with input, the Kimsuky actor sends a follow-on email with a malicious attachment.

Dear <**think tank employee**>,

Hope you are doing well. On behalf of <**another think tank**>, it is my pleasure to invite you to write a 1,200-word piece on the recent NK's provocation.

North Korea's latest missile launches, including the launch of an intermediate-range ballistic missile (IRBM) over Japan on October 4 and two short-range ballistic missiles (SRBMs) on October 6, provide a stark reminder of the numerous missile programs it is pursuing.

Subject is as follows:

1) Would Pyongyang conduct its next nuclear test soon after China's Communist Party Congress in mid-October?

2) May a quieter approach to North Korean aggression be warranted?

3) Would Japan increase the defense budget and a more proactive defense policy?

You can send me this email by Oct 21. You can make your own title for your article. We can provide you with a small honorarium of around USD 480.00.

I would really appreciate it if you can contribute.

Best,

<**Redacted**>

Senior Fellow, <**think tank**>

Director, <**think tank**>

Follow-on email: The Kimsuky actor then sent a second communication with malicious content.

Dear <**think tank employee**>,

Sorry for my late response.

As promised, I'm writing to send our result of the review. Please find the attached and let me know if any problems.

PW: <redacted>

Best,

<**Redacted**>

Senior Fellow, <**think tank**>
Director, <**think tank**>

4. Impersonation of government officials, law enforcement, web administrators

Below is an example of how Kimsuky actors approach their targets by impersonating individuals responsible for North Korean policies in government agencies, such as the South Korean National Assembly or the presidential office. These impersonated individuals may have already had their accounts compromised through a previous attack. Kimsuky actors may mention specific information about the target's position or schedule, which they obtained from the target's email exchanges or address book.

Sample email communication 7:

Title: Office of <**member of the National Assembly**>/Seminar "Proposal for the Unification Policies of the Yoon Government"

Hello, this is <**name of secretary**> from the office of <**member of the National Assembly**>.

Let me express our gratitude for your attendance and participation at the seminar we hosted yesterday. Your presence and insights contributed greatly to the success of the event.

If it's not too much trouble, could you kindly provide us with a brief summary of the remarks you made during the seminar? We would like to keep it as an internal reference material.

Additionally, we would greatly appreciate it if you could fill out the attached form and send it back to us. This will serve as an evidence document for the speaking fee payment procedure.

Password: <**redacted**>

Thank you again for your participation and we hope to see you at future events. Have a great weekend.

Kimsuky actors may also impersonate investigative agencies or law enforcement officials to deceive a target into believing that their email account has been involved in an illegal incident. They use the authority of investigative agencies to approach the target, implying that their account may have been stolen and that they could be involved in a criminal or national security-related incident.

Sample email communication 8:

Title: <**legitimate Investigator**> of <**legitimate investigation agency**>.

I am <**legitimate Investigator**> of <**legitimate investigation agency**>.

I'm writing to inform you that someone has published content on YouTube using your email account that violates the National Security Law.

Link: https:// HYPERLINK "https://%3cyoutube/"< HYPERLINK "https://%3cyoutube/"YouTube video link>. The video was posted on <**Date: 0000. 0. 00.>** by <**target**>

We also suspect that the same user has posted content that slanders North Korean defectors. We need your cooperation to identify the real publisher of these posts.

1. Provide us with your computer media access control address (MAC address) and Ethernet hardware address, as they are needed to track any illegal access to your email account.

2. If you cannot locate these addresses in your computer system, please run the program below and send us the resulting document: <check tool.zip>

3) Please respond to this email within 24 hours and delete it immediately after sending your reply.

Thanks you for your cooperation

Additionally, Kimsuky actors impersonate operators or administrators of popular web portals and claim that a victim's account has been locked following suspicious activity or fraudulent use. Victims are advised to protect their personal information and unlock their account by clicking a link attached to the email and changing their password. The link leads to a phishing site that mimics a legitimate web portal login page where victims are directed to input personal information, including their usernames and passwords, for harvesting by DPRK cyber actors.

Sample email communication 9:

Title: Your Password for <**legitimate portal site**> Account Has Been Compromised

We regret to inform you that we have detected an attempt to log into your account (<**email address**>) from an unauthorized application. The incident occurred on <**date**> at <**time**> (Korea Standard Time), and the IP address used was <**IP address**> located in Washington, the U.S.

In order to prevent any further unauthorized access to your account, we recommend that you change your password immediately. You can do this by clicking on the following link: <**link to change password - legitimate**>

Please note that if you fail to change your password, we may have to permanently delete or close your account in accordance with our security policy.

POTENTIAL MITIGATION MEASURES

For email recipients:

- Implement basic cyber hygiene to include robust passwords, multifactor authentication, and installation of antivirus tools. See NSA's Best Practices for Securing Your Home Network or NIS's guidance for email security for more details.
- Do not enable macros on documents received via email, unless the source is verified.
- Do not open documents from cloud hosting services when shared via email, unless the source is verified.
- Closely scrutinize identities and associated social media or credentials for fraud. Be especially cautious of:
    - Official messages coming from unofficial or personal email accounts using commercial providers.
    - Domain/subdomain variations, as DPRK cyber actors have been known to register spoofed domains (e.g., johndoe@abccompany.live vs. johndoe@abccompany.com).
- If you were previously in communication with the individual, use the known legitimate contact information instead of the new, potentially malicious email or account.
- When in doubt, consult the organization's official website for correct contact information.
- If you are still not sure, verify identities via phone or video call before engaging further. DPRK cyber actors are not known to engage outside of the virtual environment and will avoid voice/video communications.

- If you cannot verify the source of an email inquiry, consider the risks before responding.
- Consider navigating to websites using a search engine's non-sponsored results instead of clicking on URLs provided in the email(s).
- Be cautious of a request to move communications to a separate messaging platform.
- If sending documents, only send to verified email addresses.

For potential recipients' systems administrators:

- Implement a user training program and phishing exercises to raise awareness among users about the risks of visiting websites, clicking on links, and opening attachments. Reinforce the appropriate user response to phishing and spearphishing emails.
- Require phishing-resistant multi-factor authentication (MFA) for as many services as possible—particularly for webmail, virtual private networks (VPNs), accounts that access critical systems, and privileged accounts that manage backups.
- Regularly use port checking capabilities to determine if your network is being accessed remotely via desktop sharing software or a VPN or VPS, particularly if usage of remote desktop sharing software or VPN services to access accounts is not standard practice.
- If you allow the use of Remote Desktop Protocol (RDP), or other potentially risky remote services, secure and monitor them closely.
    - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require phishing-resistant MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.
    - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols not in use for a business purpose (e.g., RDP Transmission Control Protocol port 3389).
    - Restrict the Server Message Block (SMB) protocol within the network to only access necessary servers and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.

  - Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
  - Implement application control policies that only allow systems to execute known and permitted programs.

- Open document readers in protected viewing modes to help prevent active content from running.
- Install updates for operating systems, software, and firmware as soon as they are released. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Regularly check for software updates and end-of-life notifications and prioritize patching known exploited vulnerabilities. Consider leveraging a centralized patch management system to automate and expedite the process.
- Install and regularly update antivirus and antimalware software on all hosts.
- Consider requiring administrator credentials to install software.
- Add an email banner to messages coming from outside your organizations indicating that they are higher risk messages.
- Consider adding rules to block emails that match the sample emails provided in this advisory. Ensuring that you know how to scan for malicious undelivered email messages on email servers is a critical step for preparing to understand the scope of this type of targeting once malicious email identifiers are discovered.
- Enabling DMARC and DKIM on email domains generally makes certain forms of email spoofing more difficult, though it may not directly mitigate the tactics described above.

DPRK Rewards for Justice

The U.S. and ROK Governments encourage victims to report suspicious activities, including those related to suspected DPRK cyber activities, to relevant authorities. If you provide information about illicit DPRK activities in cyberspace, including past or ongoing operations, you may be eligible for a reward. If you have information about illicit DPRK activities in cyberspace, including past or ongoing operations, providing such information through the Department of State's Rewards for Justice program could make you eligible to receive an award of up to $5 million. For further details, please visit https://rewardsforjustice.net/.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or service by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the co-authors.

APPENDIX: ADDITIONAL SPEARPHISHING SAMPLES

Sample email communication 10:

"This is <**name of legitimate journalist**> from <**legitimate non-U.S. news organization**>

I'm writing to know your thoughts on North Korea's future direction after the Beijing Winter Olympics are over. Many believe a recent absence of North Korean provocations is due to Pyongyang's decision not to hurt Olympic vibes held in its lone major ally, but with the Games in the books, speculation is growing that North Korea is likely to pick up where it left off in January, or a series of missile tests.

-Do you believe North Korea will resume testing its missile launches? If so, when is the best time for it and what kind of missiles it will opt?

-China is scheduled to hold the National People's Congress, and the Chinese People's Political Consultative Conference from March 4 to 13 and do you think the schedule will further defer North Korea's possible missile testing?

-North Korea has indicated that it will lift its moratorium on missile and nuclear tests, but do you think there is the possibility that Pyongyang will offer to talk with the U.S., putting the moratorium on the line? If so, what would be the U.S. response? I'd be very grateful if you could send me your answers within this week

Sample email communication 11:

Title: Documents for the Policy Advisory Committee.

Hello, <**member of the committee**>,

I am <**name of government employee**> from <**government department**>.

I am writing to inform you that I have attached the filed related to the recent visit of Special Representative Biegun to this email.

As this email contains sensitive information, please treat it as confidential.

<**file name.pdf**>

Sample email communication 12:

Dear <**university professor**>:

I hope you are safe and well.

This is <**legitimate journalist**> from <**legitimate non-U.S. news organization**>. I am sending e-mail to you because I would like to hear your opinions about how Russia's invasion of Ukraine will affect the situation surrounding North Korea. Would you like to give me your opinions about the questions below?

1) Some analysts argue that Russia's invasion of Ukraine may make North Korea much more reluctant to give up nuclear weapons, given that Ukraine has been eventually invaded by Russia after it abandoned its nuclear arsenal in exchange for security guarantees under the Budapest Memorandum. This certainly looks similar to an agreement made between Trump and Kim Jong Un in Singapore in 2018. What do you think about this kind of argument?

2) While the Biden administration is concentrated on the evolving circumstances surrounding Ukraine, possibly lowering its guard in the Asia-Pacific region, North Korea Launches New ICBM and may try to carry out nuclear tests. What do you think about North Korea's future developments?

3) Do you think North Korea believes that Biden is already a "lame duck" and sees this as a good chance to concentrate on developing new weapons?

4) Do you expect China will tolerate North Korea's spate of ballistic missile launches and possible nuclear tests? Do you think North Korea can or will maintain stable and amicable relations with China? Does Russia not afford to care about North Korea?

I would be very grateful if you could send me your answers within 5 days. Thanks for your consideration and time in advance.

best regards.

<**legitimate journalist**>

Sample email communication 13:

Title: Your email account has been suspended

We are writing to inform you that your email account has been suspended because emails you sent appear to have violated relevant laws and in some cases you may be held legally liable. If you did not send any spam mails from your <portal site> mail account, it is possible that your account may have been compromised and used by someone else for spamming. We recommend checking your email settings to ensure that your POP/IMAP options have not 'Enabled' others to use your account.

If you are still unable to identify any problems with your email settings, it is possible that your account has been hacked and your personal information was stolen. To regain access to your email account, please follow the steps provided by our investigation department by clicking the button below.

<Button linking to phishing website disguised as a normal portal login page>

Sample email communication 14:

Title: Notification regarding your fraudulent account registration

This is the <legitimate portal site> operation team, and we regret to inform you that your ID <redacted> has been registered as a fraudulent account. To prevent any further harm, we recommend that you take immediate action.

We kindly request you to verify your identity as soon as possible to ensure the safety and security of your account. You can do this by visiting the member information page and checking the registered name. We also advise you to change your password to keep your account protected. Please be aware that the fraudulent account registration occurred on 00:00, 00/00/0000.

To unlock your account, please follow the link provided below:

<unlock your account: malicious link>

Thank you for choosing <legitimate portal site> as your trusted platform. We are committed to providing you with the best possible service and support.