JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:



TLP:CLEAR Product ID: JCSA-20240502-001

May 2, 2024

North Korean Actors Exploit Weak DMARC Security Policies to Mask Spearphishing Efforts

SUMMARY

Actions to take today to mitigate malicious activity:

- Update your or your organization's DMARC security policy to one of the two configurations found below.

The Federal Bureau of Investigation (FBI), the U.S. Department of State, and the National Security Agency (NSA) are jointly issuing this advisory to highlight attempts by Democratic People's Republic of Korea (DPRK, a.k.a. North Korea) Kimsuky cyber actors to exploit improperly configured DNS Domain-based Message Authentication, Reporting and Conformance (DMARC) record policies to conceal social engineering attempts. Without properly configured DMARC policies, malicious cyber actors are able to send spoofed emails as if they came from a legitimate domain's email exchange. The North Korean cyber actors have conducted spearphishing campaigns posing as legitimate journalists, academics, or other experts in East Asian affairs with credible links to North Korean policy circles. North Korea leverages these spearphishing campaigns to collect intelligence on geopolitical events, adversary foreign policy strategies, and any information affecting North Korean interests by gaining illicit access to targets' private documents, research, and communications. This Joint Cybersecurity Advisory (CSA) includes indicators of North Korean social engineering (page 4) for potential victims receiving spearphishing emails as well as mitigation measures (page 9) for organizations who could be victims of North Korean impersonation. For additional information on state-sponsored North Korean malicious cyber activity, see the June 2023 Kimsuky CSA, "North Korea using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media."

To report suspicious or criminal activity related to information found in the Joint Cybersecurity Advisory, contact your local FBI field office or submit a report to the FBI Internet Crime Complaint Center (IC3). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

BACKGROUND

North Korea's cyber program provides the regime with broad intelligence collection and espionage capabilities. The United States Government (USG) has observed sustained information-gathering efforts originating from North Korean cyber actors. North Korea's premier 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. The authoring agencies of this advisory assess the principal goals of North Korea's regime cyber program include maintaining consistent access to current intelligence about the United States, South Korea, and other countries of interest to impede any perceived political, military, or economic threat to the regime's security and stability.

The USG and private sector cybersecurity companies currently track the specific set of North Korean cyber actors conducting these large-scale social engineering campaigns as Kimsuky, Emerald Sleet, APT43, Velvet Chollima, and Black Banshee (herein referred to as Kimsuky). Kimsuky is administratively subordinate to the 63rd Research Center, 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 by compromising policy analysts and other experts. Successful compromises further enable Kimsuky actors to craft more credible and effective spearphishing emails, which can then be leveraged against more sensitive, higher-value targets.

The authoring agencies seek to bring awareness of these campaigns to degrade or minimize the effectiveness of Kimsuky spearphishing operations. This advisory provides detailed information on how Kimsuky actors exploit DMARC policies; red flags to consider when encountering common themes and campaigns; and general mitigation measures for entities worldwide to implement to better protect against Kimsuky's computer network exploitation (CNE) operations.

KIMSUKY'S OPERATIONS: DMARC POLICY NOT ENABLED

DMARC is an email security protocol that authenticates whether an email message seemingly sent from an organization's domain was legitimately sent from that organization's domain. A DMARC policy can be configured and applied to a domain to specify actions to be taken when email authentication fails. When an organization securely configures a DMARC policy, it helps ensure malicious actors, like Kimsuky, are unable to spoof the organization's legitimate email domain when sending spearphishing messages to a target. A DMARC policy tells a receiving email server what to do with the email after checking a domain's Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) records. Depending on if an email passes or fails SPF and DKIM, the email can be marked as spam, blocked, or delivered to an intended recipient's inbox.[1]

[1] SPF and DKIM are additional email authentication methods that separately provide layers of security on which DMARC protocols also rely. Together, DMARC, DKIM, and SPF function like a background check on email senders, to make sure they really are who they appear to be. Email servers can mark emails as spam if there is no DMARC record, but DMARC provides clearer instructions on when to do so.

North Korean cyber actors rely on social engineering techniques such as spearphishing—the use of fabricated emails tailored to deceive a target—as their primary vector for initiating a compromise and gaining access to a target's device and networks. Kimsuky spearphishing campaigns begin with broad research and preparation, including leveraging open source information to identify potential targets of value and then creating tailored online personas to appear more realistic and appealing to their targets. The cyber actors may also use content from emails of previously compromised email accounts to enhance the seeming authenticity of their spoofed emails.

In addition to convincing email messages, Kimsuky cyber actors have been observed creating fake usernames and using legitimate domain names to impersonate individuals from trusted organizations, including think tanks and higher education institutions, to gain trust and build rapport with email recipients. Spoofed emails do not come from the trusted organization's actual domain email exchange, but rather from the actor-controlled email address and domain. Even if a skeptical recipient wanted to verify whether the sender was legitimate, the recipient email response would be sent back to a spoofed email address at the trusted domain. The 'reply-to' section of the email header would reveal the North Korean actor-controlled email address and domain, but it would still appear to be legitimate.

The sample emails beginning on page 5 are real unedited examples of Kimsuky spearphishing attempts reported to the USG and contain spelling and other errors. The email headers of each sample are real excerpts that illustrate how technical analysis can be conducted. The names of individuals and impacted entities have been redacted.

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 and 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 North Korean cyber activities, to local FBI field offices.

RED FLAG INDICATORS

Sector targets should be aware of the following activity that may be indications or behaviors of malicious North Korean cyber actors:

- Innocuous initial communication with no malicious links/attachments, followed by communications containing malicious links/documents, potentially from a different, seemingly legitimate, email address
- Email content that may include real text of messages recovered from previous victim engagement with other legitimate contacts
- Emails in English that have awkward sentence structure and/or incorrect grammar
- Emails or communications targeting victims with either direct or indirect knowledge of policy information, including U.S. and ROK government employees/officials working on North Korea, Asia, China, and/or Southeast Asia matters; U.S. and ROK government employees with high clearance levels; and members of the military
- Email accounts that are spoofed with subtle incorrect misspellings of legitimate names and email addresses listed in a university directory or an official website
- Malicious documents that require the user to click “Enable Macros” to view the document
- Follow-up emails within 2-3 days of initial contact if the target does not respond to the initial spearphishing email
- Emails purporting to be from official sources but sent using unofficial email services, identifiable through the email header information being a slightly incorrect version of an organization’s domain

Sample Email 1:

Between late 2023 and early 2024, North Korean cyber actors sent the following email to USG officials and others at international organizations. Notably, a speaker fee is offered to further entice the recipient. The body of the text also contains basic errors.

Subject: [Invitation] US Policy Toward North Korea Conference

Dear **<name of target expert>**,

I hope you and your family are enjoying a lovely holiday and a restful season.

It is my privilege to invite you to provide a keynote address for an private workshop, hosted by the **<name of legitimate think tank>** to discuss the US policy toward North Korea. Given developments in North Korea since the collapse of US-DPRK and inter-Korean negotiations in 2019, as well as the changing strategic environment in East Asia, the traditional US approach to North Korea is unlikely to be effective going forward. It is time to question old assumptions and begin crafting a new strategy/approach that takes into consideration current strategic realities.

We understand your schedule is quite busy, but we were hoping you could join us at least for the that lunch (12:30- 1:30pm EST). If you are able to join in person, we would cover your travel and accommodations to attend, and can provide you with a modest $500 speaker fee. If you are not available to join in person, we can accommodate remote participation as well.

Please let me know if might be willing to join us and we can provide more details about the event and logistics right away. I look forward to hearing from you soon.

All the best,

<name of legitimate think tank staff>

Sample Email Header 1:

In the sample email header below, all referenced portions are highlighted. The email returns a "pass" for the corresponding SPF and DKIM checks, implying the North Korean actor was successful in gaining access to a university's legitimate email client to send the email. The DMARC protocol returns as "fail" because the sender's email domain—presented as the domain of the legitimate think tank—differs from the SPF and DKIM records identified as a **<legitimate university email host domain>** and **<legitimate university email account>**, respectively. The "p=NONE" indicates that a DMARC policy was set in which no email filtering action is taken on the message, despite the failed DMARC verification. This ultimately allows the spearphishing email to be delivered to the victim's inbox. Additionally, the North Korean actor edited the "Reply-To" email to route replies back to another seemingly legitimate, but fraudulent, account controlled by the actor.

While the sender of the email and the organization's email domain appear to be legitimate, the North Korean cyber actor exploited the organization's weak and overly permissive, rather than specifically defined, DMARC policy that allowed the North Korean actor to obfuscate the true sender domain.

ARC-Authentication-Results: i=l; mx.google.com

dkim=pass header.i=**<legitimate university email account>** header.s=default header.b=pUMk3rBI;

spf=pass (google.com: domain of **<legitimate university email host domain>** designates **<IP address associated with university email host domain>** as permitted sender) smtp.mailfrom=**<legitimate university email host domain>**;

dmarc=fail (p=none sp=none dis=none) header.from=**<spoofed domain of think tank>**

…

Received: from evanger8 by box2239.bluehost.com with local (Exim 4.96.2)

(envelope-from <evanger8@box2239.bluehost.com>) id lrKTlk-OOOEeX-36 for **<expert's receiving email>**; Mon, 01 Jan 2024 18:40:37 -0700

To: **<expert's receiving email>**

Subject: [Invitation]

X-PHP-Script: **<legitimate university email account>**/move/send/fooe.php for 59.6.130.254, 59.6.130.254 X-PHP-Originating-Script: 1171:mail.php

MIME-Version: 1.0

Content-Type: text/html; charset=utf-8 Content-Transfer-Encoding: quoted-printable

From: **<email address of legitimate think tank>**

Cc:

Reply-To: **<name of legitimate think tank staff> <spoofed account of legitimate think tank staff>**

Sample Email 2:

In November 2023, the authoring agencies received spearphishing reports of a North Korean cyber actor posing as a legitimate journalist and seeking comment from an expert on North Korea issues. Importantly, the North Korean actor openly notes they will not have access to the sending account and requests responses be sent to a fake personal account of the legitimate journalist. This novel tactic offers victims a plausible reason to respond to the alternative fake account.

Subject: [**<name of legitimate news media outlet>**] Questions about N. Korea

Dear **<name of target expert>**,

I hope this email finds you well. This is **<name of legitimate journalist>** from **<name of legitimate news media outlet>**. I'm writing to request that you consider granting us a brief interview.

North Korea is accelerating its sprint towards nuclear armament. After the breakdown of the 2019 Trump-Kim Hanoi Summit, Pyongyang has focused on intensifying North Korean nuclear and missile capabilities while rebuffing calls from the international community to resume denuclearization talks. North Korea has not only attempted to agitate the U.S. by drastically escalating its development of strategic nuclear weapons such as intercontinental ballistic missiles (ICBMs), but also wielded threats against the Republic of Korea and Northeast Asia in the form of tactical nuclear weapons development. Furthermore, in September 2022, North Korean leadership announced a new "law on state policy on nuclear weapons," thereby lowering its threshold for nuclear weapons employment. Among countries that possess or aim to possess nuclear weapons, North Korea is alone jn openly expressing that the use of such weapons lie in national defense and deterrence, but in belligerent employment against any specific country. On this basis, North Korea has continued to openly pressure the Republic of Korea and the international community, and pose a real and present threat to security in the Korean Peninsula and across Northeast Asia.

In connection with this, I would like to get your opinions about some questions. If interested, please respond to this email at your earliest convenience.

Then, I will send you the questions soon. Thanks for your consideration and time.

Best regards,

<name of legitimate journalist>

P.S. One thing: my **<name of legitimate news media outlet>** account will be blocked temporarily soon. So, I will receive the emails on my personal account (**<spoofed account of compromised journalist>**) for a while. Sorry for troubling you and hope you understand. Thanks in advance.

Sample Email Header 2:

In this case, the North Korean actor is able to exploit the absence of a DMARC policy that would have authenticated the sending email address against the SPF check. The North Korean actor spoofed both the name of a legitimate journalist and the real email domain of that journalist's news media outlet as given in the "From" and "Sender" portions of the email's header information. Similar to Sample Email 1, the actor changed the "Reply-to" email address so that victim responses would be routed to the account controlled by the North Korean actor.

Authentication-Results: mx.google.com;

spf=pass (google.com: domain of bounce-cgi-moo.bitalbania@yourhostingaccount.com designates 35.89.44.36 as permitted sender) smtp.mailfrom=bounce-cgi-moo.bitalbania@yourhostingaccount.com

Received: from eig-obgw-5006a.ext.cloudfilter.net ([10.0.29.179])

by cmsmtp with ESMTPS

id 0F89rlyjsKOkL0HcwrYFL4; Tue, 07 Nov 2023 08:40:02 +0000

Received: from moo.bitalbania by walcustweb0804.yourhostingaccount.com with local (Exim) id lrOHcP-000771-1N for **<targeted expert email>**; Tue, 07 Nov 2023 03:39:29 -0500

X-EN-Info: U=moo.bitalbania P=/ref/send.php

X-EN-CGIUser: moo.bitalbania X-EN-CGIPath: /ref/send.php

X-EN-OrigIP: 23.83.134.149

Message-Id: <1699346369-786-moo.bitalbania@walcustweb0804.yourhostingaccount.com>

To: **<targeted expert email>**

Subject: [**<name of legitimate news media outlet>**] Questions about N. Korea

X-PHP-Originating-Script: 4816993:mail.php

MIME-Version: 1.0

Content-Type: text/html; charset=utf-8

Content-Transfer-Encoding: quoted-printable

From: **<name of legitimate journalist> <spoofed journalist email>**

Cc:

Reply-To: **<spoofed journalist email>**

X-EN-Timestamp: Tue, 07 Nov 2023 03:39:29 -0500

Date: Tue, 07 Nov 2023 03:39:29 -0500

Sender: **<name of legitimate journalist> <spoofed journalist email>**

MITIGATION MEASURES

The FBI, U.S. Department of State, and NSA recommend organizations implement the mitigations below to improve their cybersecurity posture of DMARC security policies. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections. For email security specifically, CPG 2.M recommends enabling DMARC and setting it to "reject."

Missing DMARC policies or DMARC policies with "p=none" indicate that the receiving email server should take no security action on emails that fail DMARC checks and allow the emails to be sent through to the recipient's inbox. In order for organizations to make their policy stricter and signal to email servers to consider unauthenticated emails as spam, the authoring agencies recommend mitigating this threat by updating your organization's DMARC policy to one of these two configurations:

- "v=DMARC1; **p=quarantine;**"

"p=quarantine" indicates that email servers should quarantine emails that fail DMARC, considering them to be probable spam.

- "v=DMARC1; **p=reject;**"

"p=reject" instructs email servers to block emails that fail DMARC, considering them to be almost certainly spam.

In addition to setting the "p" field in DMARC policy, the authoring agencies recommend organizations set other DMARC policy fields, such as "rua" to receive aggregate reports about the DMARC results for email messages purportedly from the organization's domain.

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 authoring agencies.

VERSION HISTORY

May 2, 2024: Initial version.