BLACKSWAN CYBERSECURITY

THREAT ADVISORY

May 8, 2024

North Korea Leveraging Weak DMARC Policies

SUMMARY

The NSA and FBI warn of North Korean APT43 (a.k.a. Kimusky) exploiting weak DMARC policies for spear phishing. APT43's objectives are to gather geopolitical intelligence.

TECHNICAL DETAILS

APT43 uses spoofed emails from trusted sources to gain access to private documents and communications. Their goal is to collect intelligence on geopolitical events and adversary strategies. Since 2018, they have targeted organizations in the US, Europe, Japan, and South Korea, impersonating journalists and academics. They supply the North Korean government with stolen data and significant geopolitical information by infiltrating policy analysts and other professionals. These successful breaches allow Kimsuky to create more believable and impactful spear phishing emails, which they can use against more valuable and sensitive targets.

They exploit weak email Domain-based Message Authentication Reporting and Conformance (DMARC) policies to mask spear phishing attacks. Weak DMARC policies include "p=none" configurations, allowing their emails to bypass checks and reach targets. 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.

According to a recent report by Proofpoint, Kimsuky started using this method in December 2023 as part of a larger set of initiatives.

RED FLAG INDICATORS

Key sectors should take note of the following activities, which could indicate or suggest malicious behavior by 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 spear phishing 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.

RECOMMENDATIONS

- Update DMARC policies to "v=DMARC1; p="quarantine;"" or "v=DMARC1; p="reject;"" to block or quarantine unauthorized emails.
- Set other DMARC policy fields like 'rua' (Reporting URI Aggregate) to receive aggregate reports.
- Implement SPF and DKIM: Ensure that your domain has SPF and DKIM records properly set up. SPF verifies the authorized IP addresses for sending emails, while DKIM signs your outgoing emails to help receiving domains verify their authenticity.