How North Korean APT groups exploit DMARC misconfigurations — and what you can do about it

By Barracuda Networks

Published: 2024-10-02 · Archived: 2026-04-06 00:06:31 UTC

In the world of email security, nothing is foolproof — especially when misconfigurations open the door to attacks. Recently, the North Korean cybercrime group Kimsuky has shown just how dangerous those vulnerabilities can be, using poorly configured Domain-based Message Authentication, Reporting & Conformance (DMARC) policies to run spear-phishing campaigns. This isn't just a geopolitical concern; it's a reminder that email security flaws, however small, can be exploited by anyone with malicious intent.

What happened?

Kimsuky is an advanced persistent threat (APT) group acting under North Korea's Reconnaissance General Bureau. This threat actor has been targeting experts in think tanks, media, and academia to collect intelligence. Their strategy? Spoofing legitimate domains by bypassing weak or misconfigured DMARC protocols. The FBI and NSA issued a joint advisory warning about these campaigns, which are designed to extract sensitive information, particularly about foreign policy and nuclear matters.

Why DMARC matters

DMARC is supposed to protect against these kinds of email-based attacks. It works by verifying the authenticity of emails using SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) checks. If an email fails these checks, DMARC tells the email server what to do next — either quarantine, reject, or pass through the email based on the set policy.

Unfortunately, DMARC can only do its job if it's configured correctly. Many organizations set weak or incomplete DMARC policies, allowing malicious emails to slip through. In the case of Kimsuky, the attackers used real-looking spoofed emails that passed initial checks, but DMARC was not set up to filter or block these attempts. The result? Malicious emails land right in the inbox.

The attack in action

Here's how it works: Kimsuky starts with an email from what looks like a credible source, such as a university or research institute. The first email might seem harmless, designed to build trust. Once that trust is established, a second email comes in with a malicious attachment or link. In some cases, attackers even manage to access legitimate email systems, making their phishing attempts even more convincing.

One example? A spear-phishing email inviting a target to speak at a North Korea policy conference. The email passed SPF and DKIM checks because the attackers had access to the legitimate system. But DMARC wasn't

configured properly, so despite some red flags, the email went through.

Misconfigurations are common — and dangerous

What makes this particularly troubling is that DMARC misconfigurations are more common than you'd think. Many organizations don't regularly update or monitor their DMARC settings. Some might not even have one in place, leaving them wide open to attack. Even when they do, a "monitor" policy (which logs threats without taking action) is far too common. This gives organizations a false sense of security and allows malicious emails to slip through unnoticed.

How to defend against this

You need a multilayered defense strategy. Here are three key steps to take:

1. **Get your DMARC right**: Set your DMARC policy to "quarantine" or "reject" emails that fail SPF and DKIM checks. A "monitor" policy might seem like a safe first step, but without action, you're still exposed.
2. **Invest in AI-driven solutions**: Email threats are becoming more sophisticated, and DMARC alone may not be enough. Barracuda's AI-driven email protection solutions, for instance, can detect unusual email patterns and suspicious behaviors, even when they seem to pass traditional checks.
3. **Train your team**: Humans are often the weakest link in the security chain. Regular phishing simulations and training can significantly reduce the risk of someone clicking on a malicious email. Barracuda Phishing and Impersonation Protection can help your employees recognize red flags before it's too late.

The bottom line

Cyber-espionage groups like Kimsuky are constantly looking for ways to exploit weak spots in email security. DMARC misconfigurations provide an easy in. But with the right tools, configurations, and training, you can close those gaps and keep your organization safe. Whether you're worried about nation-state actors or more common cybercriminals, getting email security right is non-negotiable. And for companies like yours, every layer of security matters.
