APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations | Mandiant

By Mandiant

Published: 2023-03-28 · Archived: 2026-04-05 17:23:48 UTC

Written by: Fred Plan, Van Ta, Michael Barnhart, Jeff Johnson, Dan Perez, Joe Dobson

---

Today we are releasing a report on APT43, a prolific threat actor operating on behalf of the North Korean regime that we have observed engaging in cybercrime as a way to fund their espionage operations.

Mandiant tracks tons of activity throughout the year, but we don't always have enough evidence to attribute it to a specific group. However, as we continue to observe more activity over time and our knowledge of related threat clusters matures, we may graduate it to a named threat actor.

Such is the case with APT43. This report represents the culmination of endless hours of research and connecting the dots across numerous Mandiant groups, and highlights collaboration with our new colleagues at Google Cloud as well. It also marks our first official graduation since Mandiant announced APT42 in September 2022.

Dive into the report now for in-depth analysis on APT43 targeting and TTPs, examples of their campaigns and operations, and an annex of malware and indicators. Here's a little taste of what you can expect to learn:

- **Attribution:** Mandiant has tracked this group since 2018, and APT43's collection priorities align with the mission of the Reconnaissance General Bureau (RGB), North Korea's main foreign intelligence service.
- **Activity:** APT43 steals and launders enough cryptocurrency to buy operational infrastructure in a manner aligned with North Korea's juche state ideology of self-reliance, therefore reducing fiscal strain on the central government.
- **Targeting:** Espionage targeting is regionally focused on South Korea, Japan, Europe, and the United States, especially in the following sectors: government, business services, and manufacturing, along with education, research, and think tanks focused on geopolitical and nuclear policy. The group shifted focus to health-related verticals throughout the majority of 2021, likely in support of pandemic response efforts.
- **Tactics:** The group creates numerous spoofed and fraudulent (but convincing) personas for use in social engineering, and also masquerades as key individuals within their target area (such as diplomacy and defense), and leveraged stolen personally identifiable information (PII) to create accounts and register domains. APT43 has also created cover identities for purchasing operational tooling and infrastructure.
- **Procedures:** APT43 buys hash rental and cloud mining services to provide hash power, which is used to mine cryptocurrency to a wallet selected by the buyer without any blockchain-based association to the buyer's original payments—in other words, they use stolen crypto to mine for clean crypto.

APT43 is able to support espionage efforts with cybercrime, is willing to engage in operations over longer periods of time, and has collaborated with other North Korean espionage operators on multiple operations, underscoring the major role APT43 plays in the regime's cyber apparatus.

Download the report now to learn about APT43. Not enough? Seeking even more? Listen to our latest podcast embedded in this post, and register today for our APT43 webinar.

Posted in

- Threat Intelligence
