Mandiant is now part of Google Cloud. **Learn More.**

✕

EN ⌄

BLOG

# APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations

FRED PLAN, VAN TA, MICHAEL BARNHART, JEFF JOHNSON, DAN PEREZ, JOE DOBSON

**MAR 28, 2023 |** **3 MIN READ** | LAST UPDATED: AUG 16, 2023

**#NORTH KOREA**     **#THREAT INTELLIGENCE**     **#ADVANCED PERSISTENT THREATS (APTS)**

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**.

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**.

The Defender's Advantage Podcast
**Threat Trends: Ho**

00:00 | 39:17

Mandiant is now part of Google Cloud. **Learn More.**　　　　　　　✕

**Link to RSS feed**

# Prepare for 2024's cybersecurity landscape.

Get the Google Cloud Cybersecurity Forecast 2024 report to explore the latest trends on the horizon.

Download now

Google Cloud

Have questions? Let's talk.

Mandiant experts are ready to answer your questions.

Mandiant is now part of Google Cloud. **Learn More.**

Follow us

**Mandiant Advantage Platform**

Platform Overview

Breach Analytics for Chronicle

Security Validation

Attack Surface Management

Threat Intelligence

Digital Threat Monitoring

Managed Defense

**Solutions**

Proactive Exposure Management

Ransomware

Industrial Controls & OT

Cyber Risk Management

Digital Risk Protection

Insider Threats

Cyber Security Skills Gap

Election Security

Government Cyber Security

Manufacturing

Cyber Threat Visibility

Attack Surface Visibility

Cyber Preparedness

Detection and Response

Financial Services Cyber Security

**Services**

Services Overview

**Mandiant Academy**

Overview

Mandiant is now part of Google Cloud. **Learn More.**                                    ✕

View all Services (18)                        ThreatSpace Cyber Range

Expertise on Demand                            Free Course Sneak Peaks

**Resources**                                  **Company**

Resource Center                                About Us

Blog                                           Careers

Podcasts                                       Events

Customer Stories                               Media Center

Reports

Webinars

Insights

eBooks

Infographics

White Papers

Datasheets

**Partners**                                   **Connect with Mandiant**

Partners Overview                              Contact Us

Technology Partners                            Report an Incident

Cyber Risk Partners                            Customer Support

Service Partners                               Email Preferences

Channel Partners                               Customer Success

Partner Portal                                 Media Inquiries