Home • Security • North Korean threat actor APT43 pivots back to strategic cyberespionage

by Lucian Constantin
CSO Senior Writer

North Korean threat actor APT43 pivots back to strategic cyberespionage

News Analysis
Mar 29, 2023 • 6 mins

Advanced Persistent Threats | Social Engineering

The APT43 group is highly adept at using social engineering to target individuals and extract sensitive information.

Credit: Gerd Altmann

When it comes to threat actors working for the North Korean government, most people have heard of the Lazarus group (APT38). It was responsible for the 2014 attack against Sony Pictures, the 2016 cyber heist of funds belonging to the central bank of Bangladesh, and the 2017 WannaCry ransomware worm. However, another team that security researchers call APT43, Kimsuky, or Thallium has been carrying out cyberespionage and cybercrime operations at the behest of the North Korean government since at least 2018.

APT43 specializes in credential harvesting and social engineering with a focus on foreign policy and nuclear security issues, topics that

track two diplomatic channels including religious groups, universities, non-governmental organizations, journalists, academics, bloggers, and human rights activists.

"APT43 collection priorities align with the mission of the Reconnaissance General Bureau (RGB), North Korea's main foreign intelligence service," researchers from Google-owned cybersecurity firm Mandiant said in **a new report**. "Although the overall targeting reach is broad, the ultimate aim of campaigns is most likely centered around enabling North Korea's weapons program including collecting information about international negotiations, sanctions policy, and other country's foreign relations and domestic politics as these may affect North Korea's nuclear ambitions."

Credential harvesting in support of highly targeted phishing campaigns

There's no evidence that APT43 ever used zero-day exploits in its operations like other state-sponsored APTs do, but the group is very apt at social engineering. Its email-based phishing campaigns are highly tailored to its victims' interests and often involve impersonation or building very credible personas.

APT43 has impersonated key people in the security and defense industries, as well as reporters and think-tank analysts to build a rapport with their targets. Sometimes they don't even need to deploy malware because they can extract the information they're interested in by having email conversations with the victim. In one case highlighted by Mandiant, the APT43 operators impersonated a journalist working on a story following some of North Korea's missile tests and managed to extract strategic analysis from an academic.

The group also registers a lot of domains and builds a lot of websites, often with stolen personally identifiable information (PII) of real individuals from certain industries to make the websites more credible. They also engage in cybercriminal activities, particularly cryptocurrency theft and laundering to fund their infrastructure needs.

Some of the APT43 websites impersonate institutions or services that are specific to their target audience, such as university portals, search engines, web platforms, and they're used to host phishing pages with the goal of harvesting credentials. It's believed those credentials are then used to further the group's operations. For example, contact lists stolen from compromised email addresses are used to discover further targets for social engineering.

"The group is primarily interested in information developed and stored within the US military and government, defense industrial base (DIB), and research and security policies developed by US-based academia and think tanks focused on nuclear security policy and nonproliferation," the Mandiant researchers said. "APT43 has displayed interest in similar industries within South Korea, specifically non-profit organizations and universities that focus on global and regional policies, as well as businesses, such as manufacturing, that can provide information around goods whose export to North Korea has been restricted. This includes fuel, machinery, metals, transportation vehicles, and weapons."

Aside from South Korea and the US which sit at the top of the North Korean government's intelligence collection activities, APT43 has also targeted organizations and individuals from Japan and Europe.

APT43's malware toolkit

APT43 also uses an expansive toolkit of public and custom-made malware programs. For example, the group has been using off-the-shelf remote access trojans such as Ghost RAT, QUASARRAT, XRAT, and Amadey. However, its most known for a custom backdoor that's built out of Visual Basic scripts and is known as LATEOP or BabyShark.

The group makes constant improvements to its arsenal, building upon old versions and adding new features. This involves creating versions of its malware for other platforms. One example is with a Windows malware downloader that Mandiant tracks at PENCILDOWN and for which APT43 created an Android variant.

There is evidence that APT43 collaborates with and shares some of the tools with other North Korean state-sponsored groups including Lazarus and other clusters of activity that are being tracked separately from these two known groups but might be associated.

For example, during the campaigns targeting organizations involved in COVID-19 response globally, "A subset of APT43 almost certainly worked closely with other RGB-linked units, including sharing existing malware tools, developing new tools initially used in the expanded tasking, and carrying out sustained campaigns against healthcare research and related organizations," Mandiant said.

This saw APT43 use a version of HANGMAN, a backdoor usually linked with Lazarus, as well as ENDOWN, VENOMBITE, and EGGHATCH, downloaders derived from existing APT43 tooling like PENCILDOWN. In another operation that targeted cryptocurrency, APT43 deployed LONEJOGGER, a tool associated with a cluster of activity that Mandian tracks as UNC1069 and which displays some links to Lazarus.

North Korean threat actors have had a long history of engaging in monetary theft and cybercrime, which aligns with the government's financially dire situation and its need for funds. APT43 has been highly active in cryptocurrency, stealing assets from users and using hash rental and cloud mining services to launder the stolen cryptocurrency. Mandiant believes the primary goal of these operations is for the group to be self-sufficient and fund its own operational needs without burdening the government.

"Barring a drastic change in North Korea's national priorities, we expect that APT43 will remain highly prolific in carrying out espionage campaigns and financially motivated activities supporting these interests," the Mandian researchers said. "We believe North Korea has become increasingly dependent on its cyber capabilities and, APT43's persistent and continuously developing operations reflect the country's sustained investment and reliance on groups like APT43."

The Mandiant report contains a complete list of APT43-related malware tools, indicators of compromise and file hashes as well as MITRE ATT&CK framework TTPs.

by **Lucian Constantin**
CSO Senior Writer

Lucian Constantin writes about information security, privacy, and data protection for CSO.

More from this author

Most popular authors

Shweta Sharma
Senior Writer

Joe Sullivan
Contributor

Linda Rosencrance
Contributing Writer

Show me more

Popular *Articles* *Podcasts* *Videos*

01

News

CISA adds patched MS SharePoint server vulnerability to KEV catalog

By Shweta Sharma
Jan 12, 2024 • 2 mins

Vulnerabilities

02

Podcast

CSO Executive Sessions Australi

Nov 20, 2023 • 15 mins

CSO and CISO

About

About Us

Advertise

Contact Us

Foundry Careers

Reprints

Newsletters

Brandposts

Policies

Privacy Policy

Cookie Policy

Copyright Notice

Member Preferences

About AdChoices

E-commerce Links

Your California Privacy Rights

Privacy Settings

Our Network

CIO

Computerworld

Infoworld

Network World