THREAT INTELLIGENCE

North Korea's Kimsuky Evolves into Full-Fledged, Prolific APT43

In cyberattacks against the US, South Korea, and Japan, the group (aka APT43 or Thallium) is using advanced social engineering and cryptomining tactics that set it apart from other threat actors.

Elizabeth Montalbano, Contributing Writer
March 29, 2023

5 Min Read

SOURCE: GARY TYSON VIA ALAMY STOCK PHOTO

Cybercriminal group Kimsuky has evolved into a full-fledged, persistent threat, carrying out "unusually aggressive" social-engineering attacks aimed at gathering intelligence, and stealing and laundering cryptocurrency to support the North Korean government.

Researchers from Mandiant have tracked a number of changes to the activity of the group, which they call APT43, in a series of rapid-fire attacks against targets in the US, South Korea, and Japan, they revealed in a report published today.

Kimsuky, also tracked as Thallium, has been on various researchers' radar screens since 2018, and its previous activity has been widely reported. In earlier attacks, the group mainly focused on conducting cyber espionage against research institutions, geo-political think tanks, and — particularly during the height of the pandemic — pharmaceutical companies.

The group typically used spear-phishing campaigns to lure in users and then installed various public and non-public malware, including spyware, onto targeted devices, which were often Android-based smartphones. In fact, Kimsuky was identified as recently as earlier this month leveraging malicious Chrome browser extensions and Android app-store services to target individuals conducting research on the inter-Korean conflict.

Now, however, Mandiant researchers have found that APT43 is evolving in several ways.

New Financial & Social Tactics

For one, the group is now following in the shoes of other North Korean APTs and branching out beyond mere cyber espionage to steal cryptocurrency, the researchers have found. In addition to using the ill-gotten currency to fund the regime of Kim Jong-un, as other groups do, APT43 also uses it to bolster its own activities, they said.

The group is even going the extra step of laundering the crypto through legitimate cloud-mining services so it comes out as clean currency and is difficult to track — an activity that might be used by other groups, but has flown under the radar until now, the researchers said.

"The washing of funds and the 'how' has been the missing piece of the equation," notes Michael Barnhart, Mandiant principal analyst at Google Cloud. "We have indications that APT43 utilizes specific hash rental services to launder these funds by mining for different cryptocurrencies."

For a small fee, these services provide hash power, which APT43 uses to mine cryptocurrency to a wallet selected by the buyer without any blockchain-based association to the buyer's original payments. This allows the APT to use stolen funds to mine for a different cryptocurrency, the researchers said. By spending very little, threat actors walk away with untracked, clean currency to do as they wish, Barnhart explains.

Moreover, APT43 — while technologically unsophisticated — relies on advanced and persistent social-engineering tactics in which threat actors create convincing fake personas and exhibit patience in building relationships with targets over several weeks without using malware, the researchers said.

"I've never seen an APT quite as successful with such novel techniques," Barnhart notes. "They pretend to be subject-matter experts or reporters and ask targeted questions — often with the promise of quoting the victim in a report or news article — and successfully gain feedback."

Indeed, in some instances, attackers successfully convinced targeted victims to send over proprietary, geopolitical analysis and research without deploying malware at all, the researchers said.

This deviates from standard procedure for most threat groups, allowing APT43 to expend little effort or resources in building malware and gaining the information they are seeking in a low-fi way — by merely asking victims for it, Barnhart notes.

High Volume Cyberattacks, Shifting Targets

APT43 has shifted its targets, and the malware it uses, in campaigns over the years in response to the demands of the North Korean government and the cyberespionage activities it requires of the group, according to Mandiant.

"APT43 ultimately modifies its targeting and tactics, techniques, and procedures (TTPs) to suit its sponsors, including carrying out financially-motivated cybercrime as needed to support the regime," the researchers said in the report.

For example, prior to October 2020, the group primarily targeted US and South Korean government offices, diplomatic organizations, and think tank-related entities with a stake in foreign policy and security issues affecting the Korean peninsula. Over the next year, however, the group shifted its focus to COVID-19 response efforts in North Korea by targeting health-related verticals and pharmaceutical companies in South Korea, the US, Europe, and Japan.

One notable difference that has emerged between the group and other North Korean threat actors is a recent shift to expand, targeting "everyday users" based on "the sheer velocity and volume of attacks," says Joe Dobson, Mandiant principal analyst.

"By spreading their attack out across hundreds, if not thousands, of victims, their activity becomes less noticeable and harder to track than hitting one large target," he says. "Their pace of execution, combined with their success rate, is alarming."

APT43 is aiming its high-volume activity at entities and organizations in government, business services, and manufacturing as well as think tanks and organizations in education and research related to geopolitical and nuclear policy in the US, South Korea, and Japan, the researchers said.

Given its advanced social-engineering tactics and tendency to go after both specific individuals and wider-net targets, researchers advised organizations that may be at risk to share with their employees "a greater understanding of cyber hygiene and heightened awareness," Barnhart says. "It's important to make personnel aware of this threat actor's TTPs," Barnhart says.

He adds that the APT's spoofed emails are highly convincing, which makes them difficult to spot, even for savvy users; thus, organizations at risk should be on high alert.

About the Author(s)

Elizabeth Montalbano, Contributing Writer

Elizabeth Montalbano is a freelance writer, journalist, and therapeutic writing mentor with more than 25 years of professional experience. Her areas of expertise include technology, business, and culture. Elizabeth previously lived and worked as a full-time journalist in Phoenix, San Francisco, and New York City; she currently resides in a village on the southwest coast of Portugal. In her free time, she enjoys surfing, hiking with her dogs, traveling,...

You May Also Like

Threat Intelligence Flax Typhoon APT to Live Off the Land, Microsoft Warns

Threat Intelligence t Time Shrinks Again, Underscoring Need for Automation

Threat Intelligence tims Surge as Threat Actors Pivot to Zero-Day Exploits

Threat Intelligence det Blizzard' Behind Ukraine Wiper Attacks

More Insights

Cyber Resiliency 2023: How to Keep IT Operations Running, No Matter What

More Events

Editor's Choice

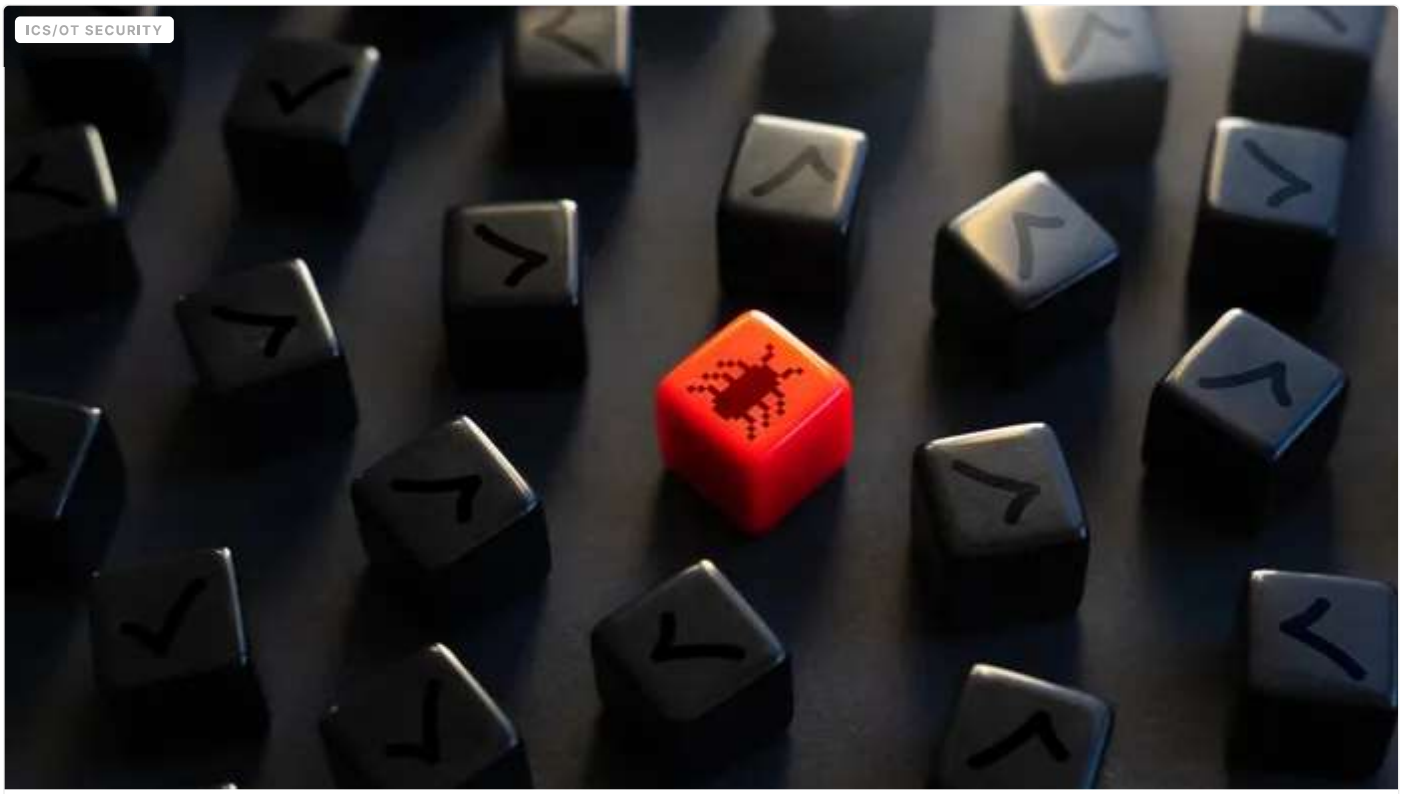
IOT

CES 2024: Will the Coolest New AI Gadgets Protect Your Privacy?

by **Nate Nelson, Contributing Writer**

JAN 10, 2024 6 MIN READ

ICS/OT SECURITY



Patch Now: Critical Windows Kerberos Bug Bypasses Microsoft Security

by **Jai Vijayan, Contributing Writer**

JAN 9, 2024 5 MIN READ

23andMe: 'Negligent' Users at Fault for Breach of 6.9M Records

by **Nate Nelson, Contributing Writer**

JAN 5, 2024 4 MIN READ

CISO Planning for 2024 May Struggle When It Comes to AI

by **Joan Goodchild, Contributing Writer**

JAN 2, 2024 4 MIN READ

Reports

Passwords Are Passe: Next Gen Authentication Addresses Today's Threats

The State of Supply Chain Threats

How to Deploy Zero Trust for Remote Workforce Security

What Ransomware Groups Look for in Enterprise Victims

How to Use Threat Intelligence to Mitigate Third-Party Risk

More Reports

White Papers

IT Zero Trust vs. OT Zero Trust: It's all about Availability

Buyer's Guide: Choosing a True DevSecOps Solution for Your Apps on AWS

2023 Software Supply Chain Attack Report

The Need for a Software Bill of Materials

The Developers Guide to API Security

More Whitepapers

Events

Black Hat Asia - April 16-19 - Learn More
APR 16, 2024

Black Hat Spring Trainings - March 12-15 - Learn More
MAR 12, 2024

Cyber Resiliency 2023: How to Keep IT Operations Running, No Matter What
AUG 24, 2023

More Events

DARKREADING

Discover More With Informa Tech

Black Hat

Omdia

Working With Us

About Us

Advertise

Reprints

Join Us

NEWSLETTER SIGN-UP

Follow Us

Cookies Preference Center
When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.
More information
Allow All
Manage Consent Preferences

Strictly Necessary Cookies
Always Active
These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

Performance Cookies
Always Active
These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

Functional Cookies
Always Active
These cookies enable the website to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies then some or all of these services may not function properly.

Targeting Cookies
Always Active
These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Back