How North Korean APT Kimsuky Is Evolving Its Tactics

By Kelly Sheridan

Published: 2021-05-07 · Archived: 2026-04-05 19:46:20 UTC

Sara Peters contributed to this reporting.

North Korean APT group Kimsuky is adopting new tactics, techniques, and procedures in global attacks, report researchers whose findings indicate the group's operations have sufficient differences to warrant splitting it into two smaller subgroups: CloudDragon and KimDragon.

Kimsuky is not a new group but has adopted new methods to support its mission of collecting intelligence. A US government alert issued in October 2020 reported the group had been operating since 2012 and often employs social engineering, spear-phishing, and watering hole attacks to collect information from targets primarily located in South Korea, Japan, and the US.

A team of researchers observing North Korean APT groups have collected evidence suggesting there are several significant distinctions in the way different facets of Kimsuky operate. Today at the virtual Black Hat Asia event, Jhih-Lin Kuo and Zih-Cing Liao, both senior threat intelligence researchers at TeamT5, divided the group into two smaller groups based on their targets, malware, and infrastructure, and shared details on how the groups' operations have evolved.

The Kimsuky group that Kaspersky disclosed in 2013 has been dubbed KimDragon by the team; the more publicly known Kimsuky seen in news headlines and vendor reports is CloudDragon.

"There are still some things they share together, but there are differences as well," said Kuo in today's briefing. Both focus on South Korea as their primary target, in addition to the US. Both attack government agencies and educational targets such as universities and research centers.

"However, when we look back to [the] malware, they're using totally different tools," she continued. CloudDragon relies on malware including TroiBomb, RoastMe, JamBog (AppleSeed), BabyShark, and DongMulRAT (WildCommand). KimDragon uses malware variants: Lovexxx (GoldDragon variant), JinhoSpy (NavRAT variant), BoboStealer (FlowerPower), and MireScript.

Their targets also varied. CloudDragon had a broader geographical footprint, branching out to attack Japan and several European Union countries, while KimDragon had only expanded to India. CloudDragon also had a broader scope of industry targets, which included financial institutions, energy companies, high-tech businesses, and aerospace and defense industries.

"Although all the North Korean APTs are attacking South Korea, they still have differences in other countries they're also interested in, and also the target industry can be slightly different as well," Kuo said in an interview with Dark Reading.

Kuo and Liao primarily focused their talk on CloudDragon, which they have observed adopting supply chain attacks, cross-platform attacks, and new modifications to its phishing campaigns.

"A supply chain attack is not easy work and can always make a big impact," said Liao of how this underscores the group's evolution.

New Attack Techniques
Between August and October 2020, CloudDragon launched a supply chain attack against a firm in the Korean cryptocurrency industry. Attackers went after a hardware wallet surface, which typically specializes in security but needs software to assist with blockchain on the Internet. Attackers created a malicious version of its management software and deployed it to the official website.

This attack targeted Windows users, though Liao noted CloudDragon also targets mobile devices. The group deployed a malicious app to Google Play; if a victim launches the app and has auto-update enabled, the malware will be downloaded without notice and upload the user's data to a command-and-control server belonging to the attackers. Researchers believe the group will strengthen its infrastructure using virtual currency obtained in the attack.

"Smartphones have become a new target of APT groups, and CloudDragon is no exception," said Kuo, noting how the attackers are expanding more of their attacks from desktop to mobile. Some of the malware researchers saw on Android devices had the ability to upload files, execute shell commands, send SMS messages, and update itself, she noted. In the future, the researchers predict attackers will continue to add more powerful functions, such as the ability to take screenshots, conduct video and audio recording, and track a victim's GPS location.

To illustrate this, she pointed to a screenshot of code from a plugin observed in the JamBog malware that indicates attackers are pursuing the ability to record audio of target devices. This, combined with the transition to mobile malware, indicates their targets could be accompanied by the attackers 24/7.

The researchers also observed CloudDragon adopting an interesting, new phishing technique in which attackers automatically fill in phishing websites with content from the legitimate website they are trying to mimic. When a victim opens a malicious link, the phishing site simultaneously sends a request to the real website, fetches the content, modifies it so it's malicious, and shows the result on the phishing site.

"The user cannot distinguish whether they are using the wrong website," said Kuo. This "ProxyMirror" attack enables attackers to auto-update content on their malicious website, reducing the amount of effort they have to spend on developing it.

About the Author

Former Senior Editor, Dark Reading

Kelly Sheridan was formerly a Staff Editor at Dark Reading, where she focused on cybersecurity news and analysis. She is a business technology journalist who previously reported for InformationWeek, where she covered Microsoft, and Insurance & Technology, where she covered financial services. Sheridan earned her BA in English at Villanova University. You can follow her on Twitter @kellymsheridan.

Source: https://www.darkreading.com/operations/how-north-korean-apt-kimsuky-is-evolving-its-tactics/d/d-id/1340956