Triple Threat: North Korea-Aligned TA406 Scams, Spies, and Steals | Proofpoint US

By November 18, 2021 Darien Huss and Selena Larson

Published: 2021-11-15 · Archived: 2026-04-05 17:12:48 UTC


Download full report (PDF)

Key Takeaways

- Throughout 2021, the North Korea-aligned threat actor TA406 conducted frequent credential theft campaigns targeting research, education, government, media and other organizations.
- Proofpoint considers TA406 to be one of several actors that make up the activity publicly tracked as Kimsuky, Thallium and Konni Group.
- TA406 doesn't usually employ malware in campaigns. However, two notable 2021 campaigns attributed to this group attempted to distribute malware that could be used for information gathering.
- TA406 engages in espionage, cyber crime and sextortion.

Overview

Throughout 2021, Proofpoint has tracked ongoing credential theft campaigns from TA406, an actor associated with the Democratic People's Republic of Korea (DPRK). Our analysts have tracked TA406 campaigns targeting customers since 2018, but the threat actor's campaigns remained low in volume until the beginning of January 2021. From January through June 2021, Proofpoint observed almost weekly campaigns targeting foreign policy experts, journalists and nongovernmental organizations (NGOs).

Introduction

In this report, we describe in detail many of the campaigns and behaviors associated with an actor operating on behalf of the North Korean government: TA406. (See Figure 1.) We begin by explaining how TA406 is associated with Kimsuky, a threat actor name broadly tracked by the threat intelligence community. We then elaborate on how Proofpoint tracks the activity of Kimsuky as three separate threat actors—TA406, TA408 and TA427. Also, we detail the differences between these actors, based on Proofpoint's visibility.

This report also examines campaign timing and targeting by TA406, and it provides a look into how TA406 conducts phishing campaigns, including the tools and services used.

TA406 employs both malware and credential harvesting in espionage and information-gathering campaigns. This report details several examples of each, including different types of credential collection and two implants used by TA406 that haven't been discussed before in open-source reporting. And finally, like all other North Korean state-

sponsored actors that Proofpoint tracks, we provide evidence that TA406 conducts financially motivated campaigns, including the targeting of cryptocurrency and sextortion.

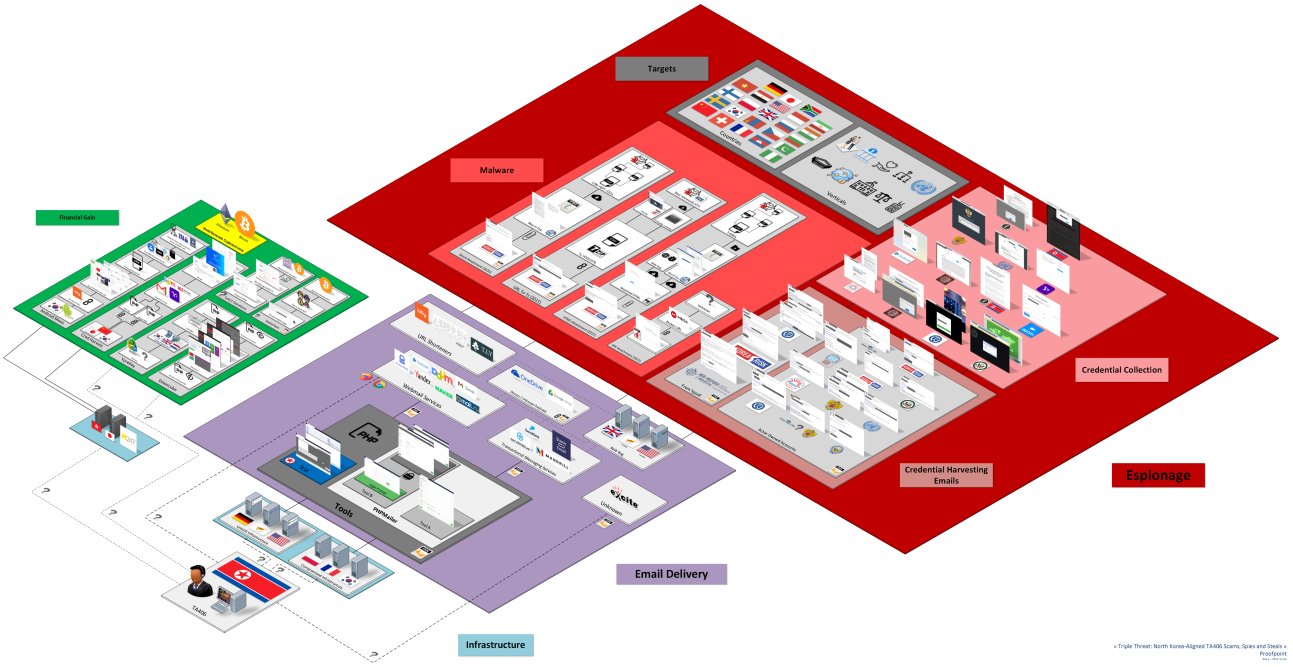

Figure 1. TA406 activity diagram.

To read more, [download the full report.]

To download indicators of compromise, head here.

Subscribe to the Proofpoint Blog

Source: https://www.proofpoint.com/us/blog/threat-insight/triple-threat-north-korea-aligned-ta406-scams-spies-and-steals