cloud.google.com /blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine/

APT45: North Korea’s Digital Military Machine

Mandiant ⋮⋮ 7/25/2024

Written by: Taylor Long, Jeff Johnson, Alice Revelli, Fred Plan, Michael Barnhart

Executive Summary

- APT45 is a long-running, moderately sophisticated North Korean cyber operator that has carried out espionage campaigns as early as 2009.
- APT45 has gradually expanded into financially-motivated operations, and the group’s suspected development and deployment of ransomware sets it apart from other North Korean operators.
- APT45 and activity clusters suspected of being linked to the group are strongly associated with a distinct genealogy of malware families separate from peer North Korean operators like TEMP.Hermit and APT43.
- Among the groups assessed to operate from the Democratic People's Republic of Korea (DPRK), APT45 has been the most frequently observed targeting critical infrastructure.

Overview

Mandiant assesses with high confidence that APT45 is a moderately sophisticated cyber operator that supports the interests of the DPRK. Since at least 2009, APT45 has carried out a range of cyber operations aligned with the shifting geopolitical interests of the North Korean state. Although the group's earliest observed activities consisted of espionage campaigns against government agencies and defense industries, APT45 has expanded its remit to financially-motivated operations, including targeting of the financial vertical; we also assess with moderate confidence that APT45 has engaged in the development of ransomware. Additionally, while multiple DPRK-nexus groups focused on healthcare and pharmaceuticals during the initial stages of the COVID-19 pandemic, APT45 has continued to target this vertical longer than other groups, suggesting an ongoing mandate to collect related information. Separately, the group has conducted operations against nuclear-related entities, underscoring its role in supporting DPRK priorities.

Shifts in Targeting and Expanding Operations

Similar to other cyber threat activity attributed to North Korea-nexus groups, shifts in APT45 operations have reflected the DPRK's changing priorities. Malware samples indicate the group was active as early as 2009, although an observed focus on government agencies and the defense industry was observed beginning in 2017. Identified activity in 2019 aligned with Pyongyang's continued interest in nuclear issues and energy. Although it is not clear if financially-motivated operations are a focus of APT45's current mandate, the group is distinct from other North Korean operators in its suspected interest in ransomware. Given available information, it is possible that APT45 is carrying out financially-motivated cybercrime not only in support of its own operations but to generate funds for other North Korean state priorities.

Financial Sector

Like other North Korea-nexus actors, APT45 targeting includes the financial sector. In 2016, APT45 likely leveraged RIFLE to target a South Korean financial organization. Direct targeting continued through at least 2021 when the group was identified spear-phishing a South Asian bank.

Critical Infrastructure

In 2019, APT45 directly targeted nuclear research facilities and nuclear power plants such as the Kudankulam Nuclear Power Plant in India, marking one of the few publicly known instances of North Korean cyber operations targeting critical infrastructure.

Intellectual Property Theft to Address Domestic Deficiencies

In September 2020, APT45 targeted the crop science division of a multinational corporation, possibly due to the exacerbation of deteriorating agricultural production following the closure of border trade related to COVID-19 contagion fears.

Multiple North Korea-nexus operators, including APT45, focused on the healthcare and pharmaceutical verticals during a suspected COVID-19 outbreak in North Korea in 2021.

Activity observed from APT45 indicating continued interest in health-related research in 2023 suggests the continued assignment of resources to related targeting.

Potential Ransomware Use

Mandiant tracks several clusters of activity where we suspect, but cannot confirm APT45 attribution. Public reporting has claimed that these clusters have used ransomware, possibly to fund their operations or generate revenue for the regime. While Mandiant cannot confirm this ransomware use by APT45, it is plausible as they have employed diverse schemes to raise money.

- In 2022, the U.S. Cybersecurity and Infrastructure Security Agency reported on North Korean state-sponsored actors' use of MAUI ransomware to target the healthcare and public health sectors.
- In 2021, Kaspersky reported on the identification of ransomware tracked by Mandiant as SHATTEREDGLASS, which has been used by suspected APT45 clusters.

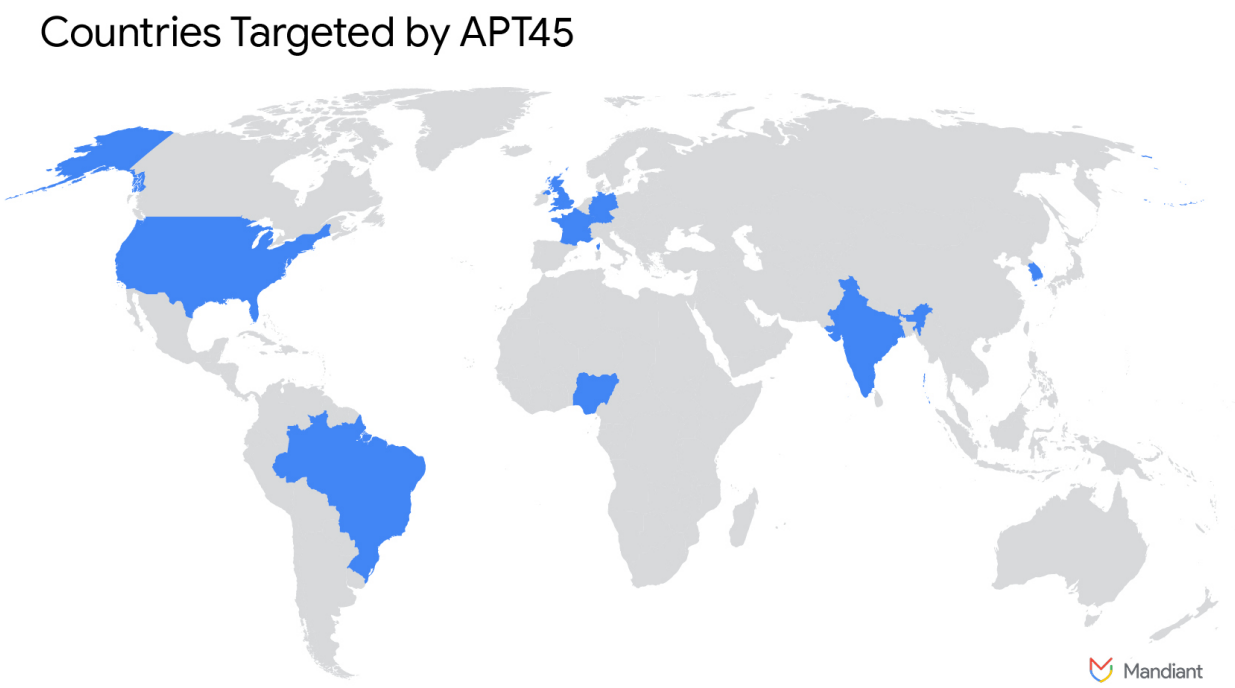

Figure 1: Countries targeted by APT45

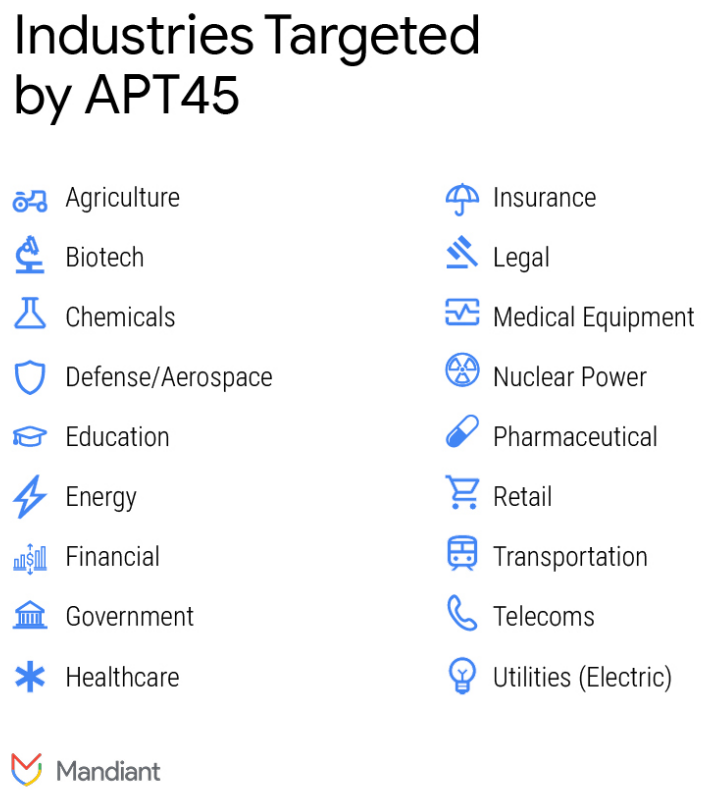

Figure 2: Industries targeted by APT45

Malware

APT45 relies on a mix of publicly available tools such as 3PROXY, malware modified from publicly available malware such as ROGUEEYE, and custom malware families. Like most groups of DPRK activity, APT45 malware exhibits distinct shared characteristics over time, including the re-use of code, unique custom encoding, and passwords. APT45 leverages a library of malware tools which are relatively distinct from other North Korean activity clusters.

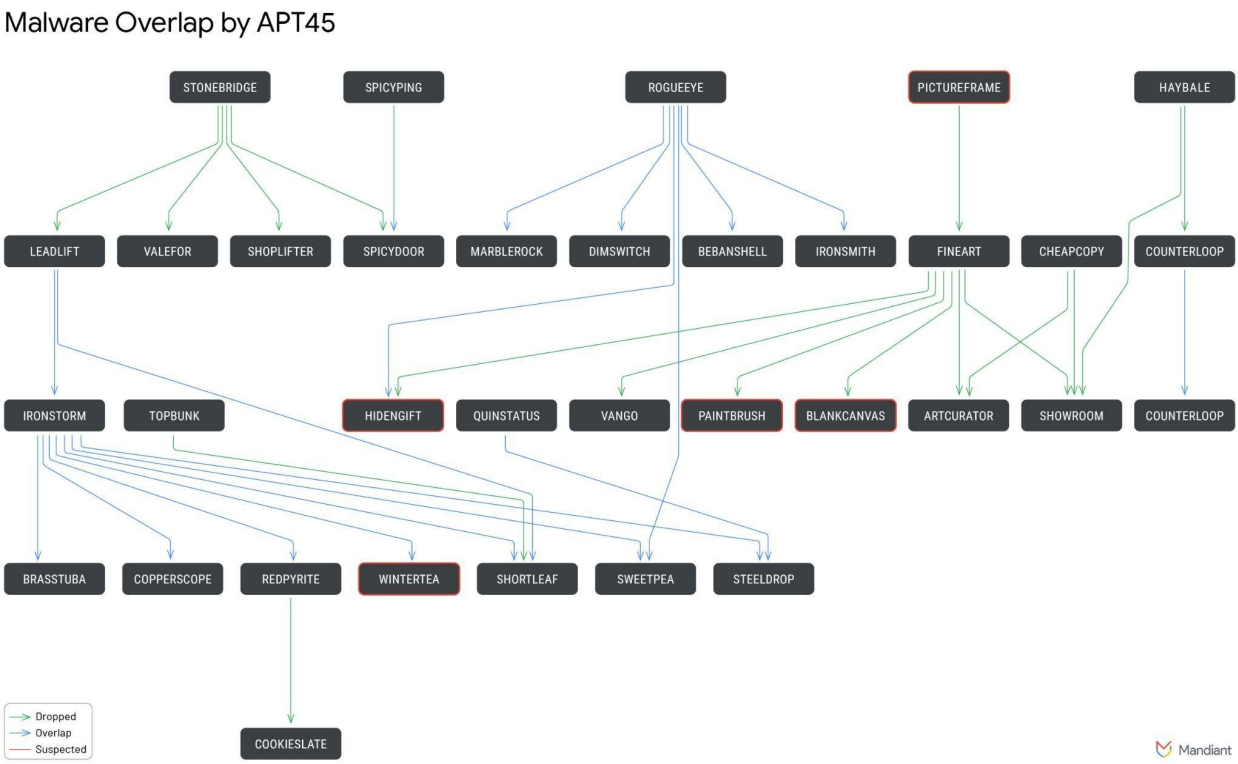

Figure 3: APT45 Malware Overlap

Attribution and Links to Other Tracked Operations

Mandiant assesses with high confidence that APT45 is a state-sponsored cyber operator conducting threat activity in support of the North Korean regime. We assess with moderate confidence that APT45 is attributable specifically to North Korea's Reconnaissance General Bureau (RGB).

Activity attributed to APT45 by Mandiant has been publicly reported as "Andariel", "Onyx Sleet", "Stonefly", and "Silent Chollima". The group's activity is also frequently reported as linked to "Lazarus Group".

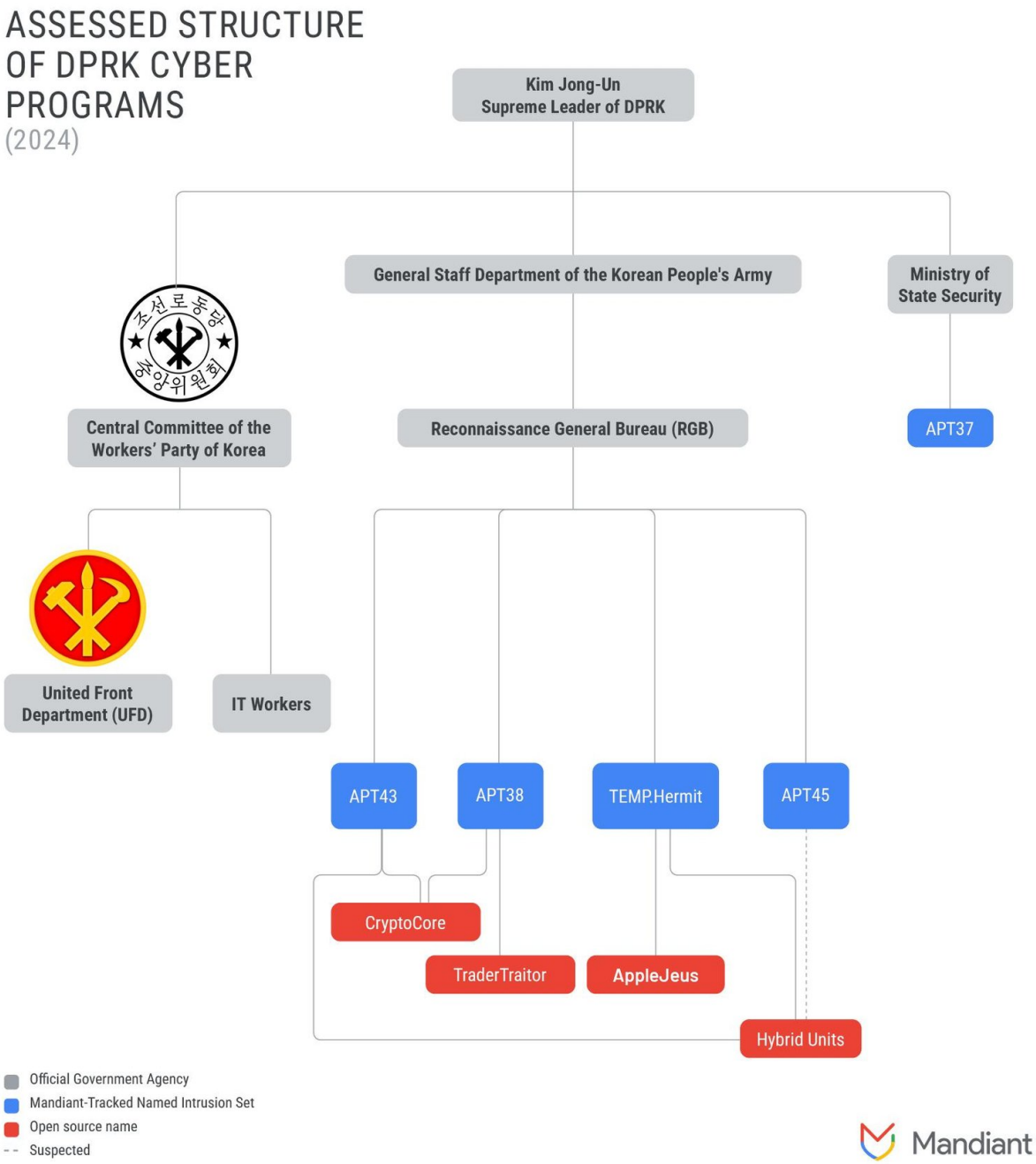

Figure 4: Assessed structure of DPRK cyber operations in 2024

Looking Ahead

APT45 is one of North Korea's longest running cyber operators, and the group's activity mirrors the regime's geopolitical priorities even as operations have shifted from classic cyber espionage against government and defense entities to include healthcare and crop science. Financially motivated activity occurring alongside intelligence collection has become a defining characteristic of North Korean cyber operations, and we expect APT45 to continue both missions. As the country has become reliant on its cyber operations as an instrument of national power, the operations carried out by APT45 and other North Korean cyber operators may reflect the changing priorities of the country's leadership.

Acknowledgements

Special thanks to Mandiant Advanced Practices, Mandiant FLARE, Mandiant Validation, and FBI Kansas City.

Technical Annex: Attack Lifecycle

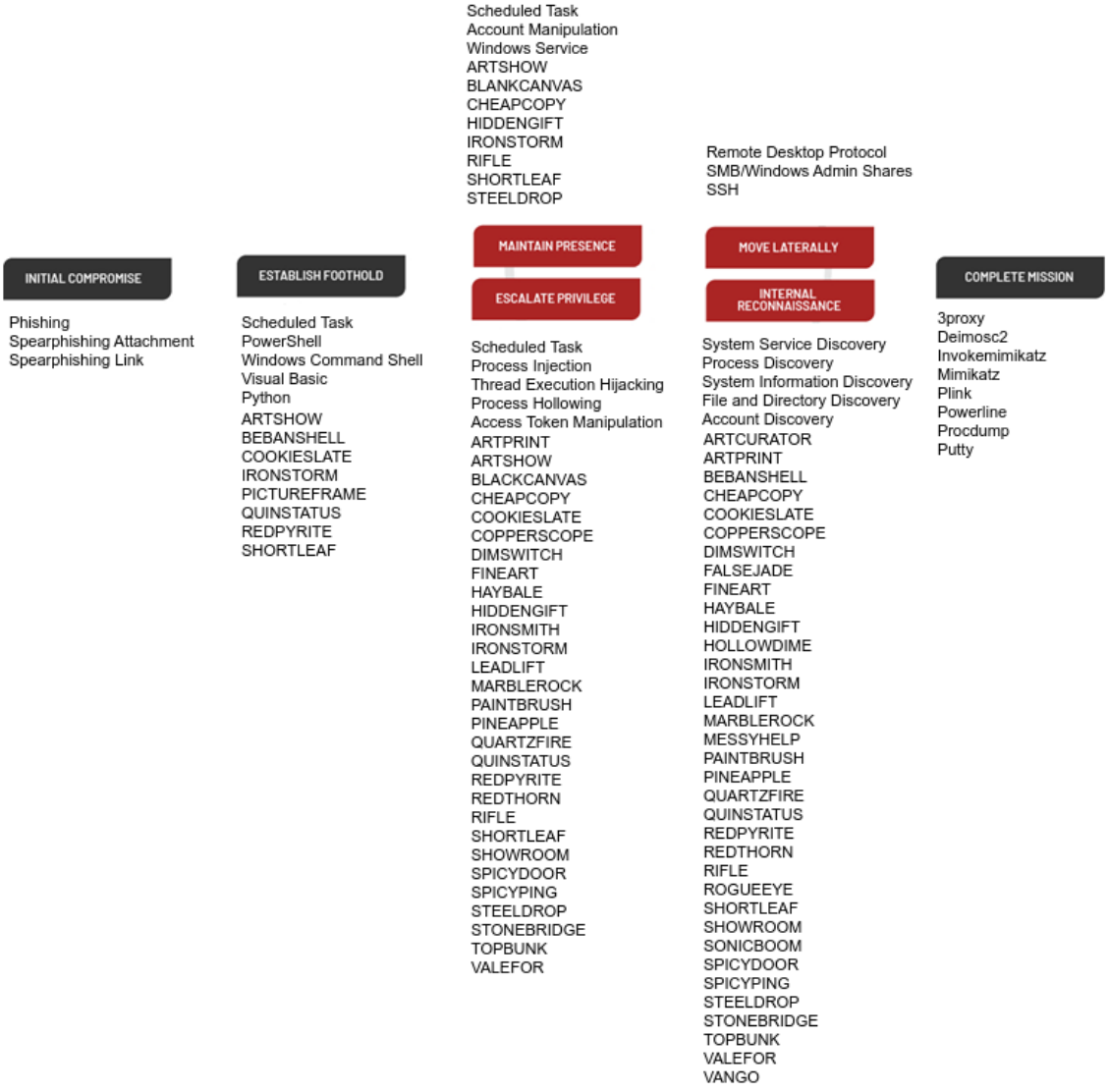

Figure 5: Attack Lifecycle

Technical Annex: APT45 Indicators of Compromise

A GTI Collection featuring APT45-related indicators of compromise is now available for registered users.