Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:28:11 UTC

APT group: Wassonite

Names	Wassonite *(Dragos)*
Country	North Korea
Motivation	Information theft and espionage
First seen	2018
Description	(Dragos) Dragos identified the WASSONITE activity group following a malware intrusion at the Kudankulam Nuclear Power Plant (KKNPP) nuclear facility in India. After further investigation, Dragos observed WASSONITE tools and behaviors targeting multiple industrial control system (ICS) entities including electric generation, nuclear energy, manufacturing, and organizations involved in space-centric research. WASSONITE has been active since at least 2018. WASSONITE targeting focuses on Asian entities, largely in India, as well as possibly Japan and South Korea. At this time, WASSONITE does not appear to have an ICS-specific disruptive or destructive capability. All the activity represents Stage 1 ICS kill-chain: access operations within IT networks. WASSONITE operations rely on deploying DTrack malware for remote access to victim machines, capturing credentials via Mimikatz and publicly available tools, and utilizing system tools to transfer files and move laterally within the enterprise system. Researchers first disclosed DTrack in late September 2019, and identified the tool targeting Indian financial institutions and research centers. DTrack is loosely connected to an earlier observed malware family, ATMDTrack, used for robbing ATM machines. Third-party security firms associate DTrack and its related malware to the Lazarus Group, Hidden Cobra, Labyrinth Chollima. Dragos also associates the activity group Covellite to Lazarus Group. However, while COVELLITE is also linked to broader Lazarus activity, this group leveraged substantially different capabilities and infrastructure to pursue a target set that does not overlap with observed WASSONITE activity.
Observed	Sectors: Energy, Oil and gas, Manufacturing, Research. Countries: India, Japan, South Korea.

Tools used	Dtrack, Mimikatz.	
Operations performed	Oct 2019	Breach of the Kudankulam Nuclear Power Plant <https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/>
Information	<https://dragos.com/resource/wassonite/>	

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
