Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:27:02 UTC

APT group: Covellite

Names	Covellite *(Dragos)* CTG-2460 *(SecureWorks)* Nickel Academy *(SecureWorks)* Black Artemis *(PWC)*
Country	North Korea
Motivation	Information theft and espionage
First seen	2017
Description	(Dragos) Covellite compromises networks associated with civilian electric energy worldwide and gathers intelligence on intellectual property and internal industrial operations. Covellite lacks an industrial control system (ICS) specific capability at this time. Covellite operates globally with targets primarily in Europe, East Asia, and North America. US targets emerged in September 2017 with a small, targeted phishing campaign directed at select U.S. electric companies. The phishing emails contained a malicious Microsoft Word document and infected computers with malware. The malicious emails discovered in the fall masqueraded as resumes or invitations. They delivered a remote access tool (RAT) payload which was used to conduct reconnaissance and enable persistent, covert access to victims' machines. Covellite's infrastructure and malware are similar to the hacking organization known as Lazarus Group, Hidden Cobra, Labyrinth Chollima by Novetta and Hidden Cobra by the U.S. Department of Homeland Security. Lazarus Group is responsible for attacks ranging from the 2014 attack on Sony Pictures to a number of Bitcoin heists in 2017. Technical analysis of Covellite malware indicates an evolution from known Lazarus toolkits. However, aside from technical overlap, it is not known how the capabilities and operations between Covellite and Lazarus are related. Covellite remains active but appears to have abandoned North American targets, with indications of activity in Europe and East Asia. Given the group's specific interest in infrastructure operations, rapidly improving capabilities, and history of aggressive targeting, Dragos considers this group a primary threat to the ICS industry.

Observed	Sectors: Energy. Countries: USA and Europe and East Asia.
Tools used	
Information	<https://dragos.com/resource/covellite/>

Last change to this card: 07 January 2021

Download this actor card in PDF or JSON format
