Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:13:10 UTC

APT group: Allanite

Names	Allanite *(Dragos)* Palmetto Fusion *(DHS)* G1000 *(MITRE)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2017
Description	(Dragos) Allanite accesses business and industrial control (ICS) networks, conducts reconnaissance, and gathers intelligence in United States and United Kingdom electric utility sectors. Dragos assesses with moderate confidence that Allanite operators continue to maintain ICS network access to: (1) understand the operational environment necessary to develop disruptive capabilities, (2) have ready access from which to disrupt electric utilities. Allanite uses email phishing campaigns and compromised websites called watering holes to steal credentials and gain access to target networks, including collecting and distributing screenshots of industrial control systems. Allanite operations limit themselves to information gathering and have not demonstrated any disruptive or damaging capabilities. Allanite conducts malware-less operations primarily leveraging legitimate and available tools in the Windows operating system.
Observed	Sectors: Energy. Countries: UK, USA.
Tools used	Inveigh, PsExec, SecreetsDump, THC Hydra and Powershell scripts.
Information	<https://dragos.com/resource/allanite/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G1000/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format