ALLANITE | Dragos

dragos.com/blog/20180510Allanite.html

May 30, 2020

Threat Activity Group

ALLANITE

Since 2017

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 operations continue and intelligence indicates activity since at least May 2017. ALLANITE activity closely resembles Palmetto Fusion described by the US Department of Homeland Security (DHS). In October 2017, a DHS advisory documented ALLANITE technical operations combined with activity with a group Symantec calls Dragonfly (which Dragos associates with DYMALLOY).

ALLANITE's targeting and techniques are similar to other activity groups, including Dragonfly, and activity Dragos labels DYMALLOY. However, ALLANITE's technical capabilities are significantly different from Dragonfly and DYMALLOY.

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.

Public disclosure by third-parties, including the DHS, associate ALLANITE operations with Russian strategic interests. However, Dragos does not corroborate the attribution of others.

US officials told the media in July 2017 these adversaries gained access to business and administrative systems, not operations networks. Since then, third-party reporting indicates ALLANITE has gathered information directly from ICS networks, which Dragos can independently confirm.

Dragos threat intelligence leverages the Dragos Platform, our threat operations center, and other sources to provide comprehensive insight into threats affecting industrial control security and safety worldwide. Dragos does not corroborate nor conduct political attribution to threat activity. Dragos instead focuses on threat behaviors and appropriate detection and response. Read more about Dragos' approach to categorizing threat activity and attribution.

Dragos does not publicly describe ICS activity group technical details except in extraordinary circumstances in order to limit tradecraft proliferation. However, full details on ALLANITE and other group tools, techniques, procedures, and infrastructure is available to network defenders via Dragos WorldView.