KEY HIGHLIGHTS

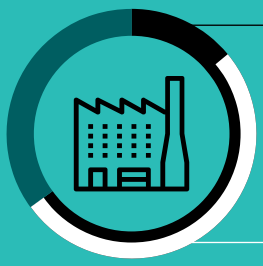
ACTIVITY GROUPS

KOSTOVITE PETROVITE ERYTHRITE

Dragos discovered **three new activity groups** with the assessed motivation of targeting ICS/OT.

Two of the groups have achieved Stage 2 of the ICS Cyber Kill Chain showing their ability to get access directly to ICS/OT networks.**

RANSOMWARE FINDINGS



65%

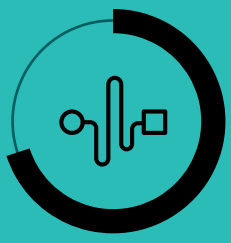
Manufacturing accounted for 65% of all ransomware attacks.

51%

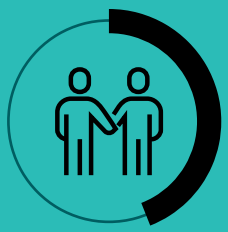
Two ransomware groups caused 51 percent of attacks (Lockbit 2.0 and Conti).

SERVICE ENGAGEMENT FINDINGS

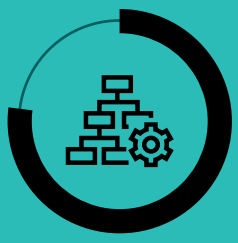
86% of service engagements have a lack of visibility across OT networks — making detections, triage, and response incredibly difficult at scale.



70% of service engagements included a finding of external connections from OEMs, IT networks, or the internet to the OT network.



44% of service engagements included a finding about shared credentials in OT systems, the most common method of lateral movement and privilege escalation.



77% of service engagements included a finding about improper network segmentation.

** The ICS Cyber Kill Chain breaks intrusions into Stage 1 and Stage 2 operations. Stage 1 are IT network compromises where the adversary appears to have a goal of getting into the ICS/OT networks of the company but has not achieved this yet. Stage 2 operations are those where the adversary has gained access to ICS/OT networks. At the completion of the ICS Cyber Kill Chain an adversary conducts disruptive or destructive operations. The paper can be found here.