DYMALLOY

By September 4, 2025 11:25 AM

Archived: 2026-04-05 14:40:10 UTC

DYMALLOY activity stretches back to 2015 and includes associations with activity into 2011. The activity focuses on intelligence gathering from industrial control system networks with an unknown intent.

DYMALLOY uses common malicious behaviors like spear phishing campaigns to directly target individuals' digital communications and watering hole attacks that place malware on industrial-related websites in an effort to steal corporate credentials.

DYMALLOY leveraged malware backdoors including Goodor, DorShel, and Karagany. These are commodity malware families—not unique to any particular group—that are used together as a toolkit and make this group's behavior unique. Overall, DYMALLOY avoids using custom toolkits or malware in its operations, making detection and specific attribution more difficult without recognizing the entirety of adversary actions.

Between late 2015 through early 2017, DYMALLOY successfully compromised multiple industrial control system (ICS) targets in Turkey, Europe and North America. The group penetrated ICS networks and stole confidential information from several organizations.

Dragos also found the group leveraged Mimikatz, an open-source software security tool that can let attackers extract passwords from memory on Windows systems.

In fall 2018, Dragos identified multiple new malware infections matching DYMALLOY's behavior. These observations may indicate a potential resurgence of DYMALLOY activity, or a different entity leveraging similar toolsets. This discovery is concerning; the malware Dragos recently identified as part of new activity is only associated with known intrusions into ICS networks.

DYMALLOY has some links to activity Symantec labels Dragonfly, which initially targeted industrial organizations from 2011 to 2014. Dragos began tracking DYMALLOY following the "Dragonfly 2.0" report published in September of last year, which described activity that began in late 2015. While there are some similarities, we consider them to be two separate activities due to significant technical differences in observed activity.

US-CERT reported TA18-074A in March 2018 notably attributing the malicious activity to actors associated with the Russian government. However, Dragos makes no assessment of this claim.

Source: https://www.dragos.com/threat/dymalloy/