FrostyGoop Incident, Campaign C0041 | MITRE ATT&CK®

Archived: 2026-04-05 17:50:16 UTC

Domain	ID		Name	Use
Enterprise	T1071		Application Layer Protocol	During FrostyGoop Incident, the adversary initiated Layer Two Tunnelling Protocol (L2TP) connections to Moscow-based IP addresses.[1]
Enterprise	T1190		Exploit Public-Facing Application	FrostyGoop Incident was likely enabled by the adversary exploiting an unknown vulnerability in an external-facing router.[1]
Enterprise	T1562	.010	Impair Defenses: Downgrade Attack	During FrostyGoop Incident, the adversary downgraded firmware on victim devices in order to impair visibility into the process environment.[1]
Enterprise	T1003	.002	OS Credential Dumping: Security Account Manager	During FrostyGoop Incident, the adversary retrieved the contents of the Security Account Manager (SAM) hive in the victim environment for credential capture.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	FrostyGoop Incident deployed a ReGeorg variant web shell to impacted systems following initial access for persistence.[1]
ICS	T0826		Loss of Availability	During FrostyGoop Incident, the adversary modified victim control system parameters resulting in the loss of heating services to impacted district heating customers.[1]
ICS	T0829		Loss of View	During FrostyGoop Incident, the adversary initiated a firmware downgrade on victim devices to a

Domain	ID	Name	Use
			version lacking monitoring.[1]
ICS	T0836	Modify Parameter	In FrostyGoop Incident, the adversary caused the victim controllers to report incorrect measurements by modifying parameters.[1]
ICS	T0857	System Firmware	During FrostyGoop Incident, the adversary initiated a firmware downgrade on impacted devices.[1]

Source: https://attack.mitre.org/campaigns/C0041