SOC INCIDENT REPORT

Authentication abuse to PowerShell execution.

This report summarises a Windows telemetry investigation involving repeated failed logons, a successful privileged logon from the same source, encoded PowerShell, outbound traffic, file creation, and persistence staging.

SEVERITY	HOST	PRIVILEGED ACCOUNT	DROPPED FILE
High	WS-FIN-07	it-admin	C:\ProgramData\Adobe\

Assessment

The highest-value signal is the progression from repeated failures into privileged access and then into hidden PowerShell and persistence. That transition is why the activity should be escalated as likely credential compromise with post-authentication execution.

1. Repeated Event ID 4625 failures from a single external IP.
2. Event ID 4624 success for a privileged account from the same source.
3. Sysmon process creation showing hidden, encoded PowerShell.
4. Network, file-create, and scheduled-task activity showing host follow-on behaviour.

Findings

Repeated authentication failures from a single external IP

5 failed logons were recorded from 203.0.113.24 before a successful logon against a privileged account.

Suspicious success after failures

A successful 4624 network logon for it-admin followed the failure sequence from the same source IP.

Encoded PowerShell execution

Sysmon process creation telemetry captured hidden, encoded PowerShell launched through cmd.exe.

Follow-on activity consistent with persistence staging

The host made outbound connections, wrote a PowerShell script under ProgramData, and created a scheduled task.

Recommended analyst actions

- Reset the compromised account and rotate any reused credentials.
- Block and review the source IP and outbound destination IP.
- Review scheduled tasks, PowerShell logs, and other hosts for the same indicators.
- Tune detections around failed-logon bursts followed by success, encoded PowerShell, and suspicious scheduled task creation.

Timeline

TIME	SOURCE	ACCOUNT	EVENT SUMMARY
09 Mar 2026, 08:11 UTC	SecurityEvent 4625	svc-backup	Failed network logon against service account.
09 Mar 2026, 08:11 UTC	SecurityEvent 4625	svc-backup	Repeated failed network logon against service account.
09 Mar 2026, 08:11 UTC	SecurityEvent 4625	svc-backup	Repeated failed network logon against service account.
09 Mar 2026, 08:12 UTC	SecurityEvent 4625	svc-backup	Repeated failed network logon against service account.
09 Mar 2026, 08:12 UTC	SecurityEvent 4625	svc-backup	Repeated failed network logon against service account.
09 Mar 2026, 08:13 UTC	SecurityEvent 4625	it-admin	Failed network logon against privileged account.
09 Mar 2026, 08:13 UTC	SecurityEvent 4625	it-admin	Failed network logon against privileged account.
09 Mar 2026, 08:14 UTC	SecurityEvent 4624	it-admin	Successful network logon against privileged account after repeated failures.
09 Mar 2026, 08:14 UTC	Sysmon 1	it-admin	Encoded PowerShell launched through cmd.exe.
09 Mar 2026, 08:15 UTC	Sysmon 3	it-admin	PowerShell process initiated outbound network connection.
09 Mar 2026, 08:15 UTC	Sysmon 11	it-admin	PowerShell wrote script file into ProgramData.

TIME	SOURCE	ACCOUNT	EVENT SUMMARY
09 Mar 2026, 08:16 UTC	Sysmon 1	it-admin	Scheduled task created from PowerShell context.