Incident review: connected AD activity

Independent analysis of recorded emulation | Prepared 2026-10-26 | Capture 2020-10-22

Historical evidence review; compromise unconfirmed

Assessment and scope

Seven distinct-account failures, five successful RC4 service-ticket requests and IPC$/srvsvc checks precede GUID-linked remote PowerShell on three targets. The connected activity warrants authorization and command review. Authorized emulation or administration remains a competing explanation; business impact is not established.

THESHIRE\pgustavo on WORKSTATION5; target records on WORKSTATION6, WORKSTATION7 and MORDORDC. Coverage: 25,993 host events and 1,121 packets; 226 host records selected. These are observed hosts, not confirmed compromised systems.

Key evidence / UTC

08:29:53 UTC. Seven failures share caller host, PID and session. Failure records have no client IP.

H00788, H00790, H00792, H00794, H00796, H00798, H00803, H00019

08:29:53-54 UTC. Five successful RC4 service tickets; IPC$/srvsvc checks span three hosts. Neither proves cracking or file theft.

H01125, H01136, H01140, H01144, H01148, H01198, H01284, H01324

08:29:57.967-58.095 UTC. Three wsmprovhost.exe / powershell.exe parent-child pairs have same-host GUID and account/session joins.

H03601, H04447, H03833, H04352, H23781, H24051

Analyst decisions

Correlate, with a causality limit. Matching TCP/5985 tuples corroborate client flows (for example H03882 / P00872). No end-to-end request ID proves a packet caused a particular PowerShell child.

Use execution time. The DC child executed at 08:29:58.095 UTC; collection at 08:30:37.907 UTC was 39.812 seconds later. This is collection delay, not a second execution wave.

Recommended handoff / proposed, not performed

1. SOC analyst / establish authorization. Check operator identity, change approval and full command/script-block content before assigning operational severity. Retain host, session and source references.

2. Incident lead + system owner / conditional response. If live evidence shows unauthorized ongoing activity, assess approved account/session restrictions and host isolation with the owner; preserve evidence and weigh service impact. No containment was performed in this historical review.

3. Detection engineer / validate before deployment. Baseline RC4 and WinRM use, test benign administration and late arrivals, then validate backend fields. Python analysis executed; the AD SPL/Sigma candidates remain unexecuted.

Evidence limits

OTRF recorded this PurpleSharp emulation in 2020; this is not a production incident or an owner-operated attack. Shared-password use, credential cracking, persistence, data theft and business impact remain unproven. Security timestamps use a calibrated capture-local UTC-04:00 assumption.

Source links: Full analysis and source references | Evidence JSON | Pinned source manifest