Cyber Intel Brief: Pro-Iran Actor Claims Cyberattack on LA Metro

By Author Tim Miller, Field CTO for Public Sector April 13, 2026

Archived: 2026-04-17 02:01:19 UTC

Cybersecurity, Public sector, Artificial Intelligence

Key Takeaways

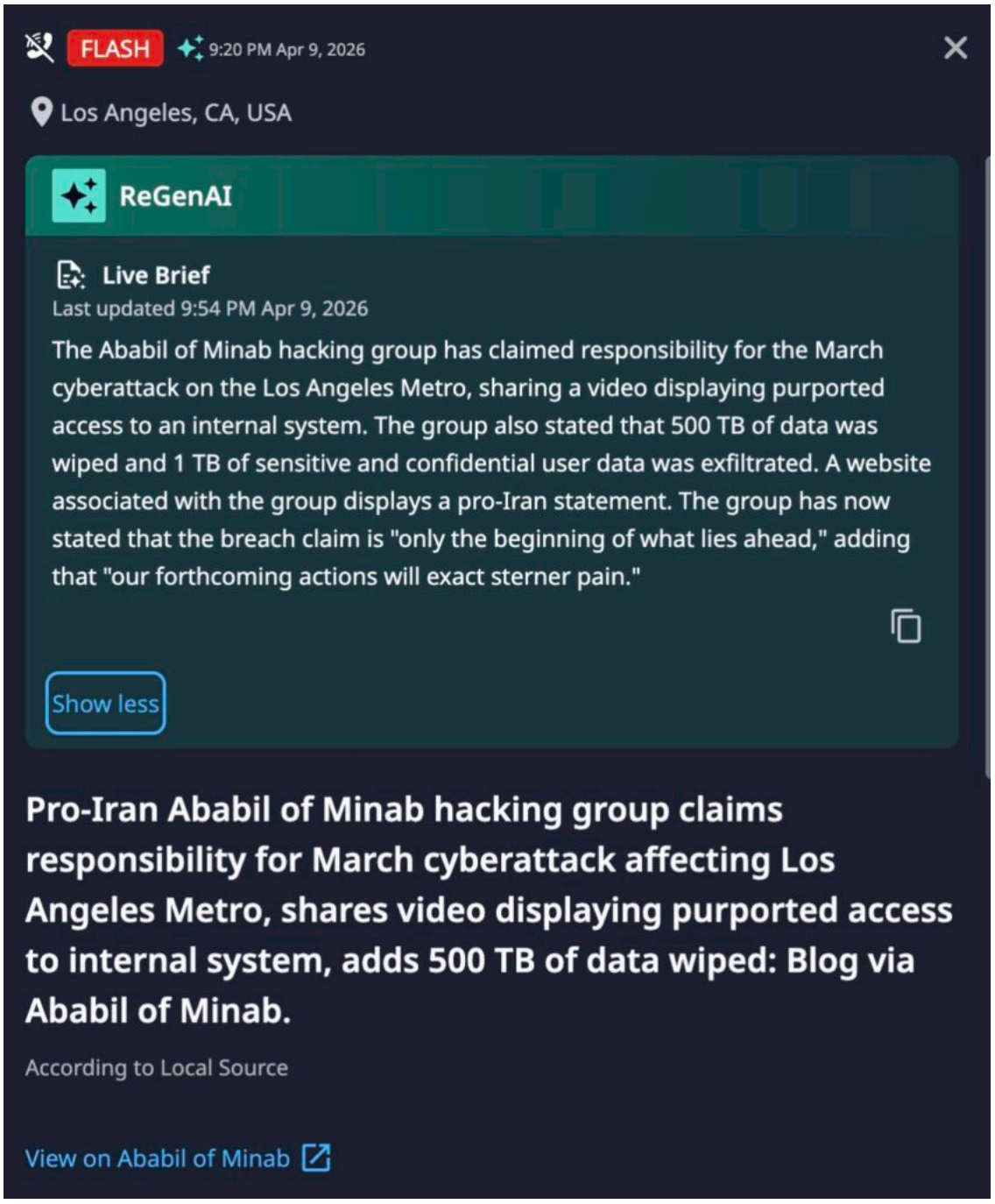
- **OT System Access Claimed:** Screenshots published by the group appear to show access to a real-time rail yard management and train control display system (Division 11), representing a potentially serious operational technology (OT) intrusion with safety implications beyond a standard IT breach.
- **Broad IT Compromise Alleged:** The group claims administrative access to LACMTA's VMware vCenter environment — managing approximately 1,421 VMs across 28 physical hosts — as well as IIS web servers hosting dozens of internal and public-facing LACMTA properties.
- **Significant Data Impact Claimed:** The group alleges 500 TB of data was wiped and 1 TB of sensitive user data was exfiltrated, though these claims have not been independently verified.
- **Escalatory Rhetoric:** Ababil of Minab has stated this incident is "only the beginning," explicitly threatening further, more severe actions against LACMTA or related targets.

Incident Overview

On April 9, 2026, the pro-Iranian hacking group **Ababil of Minab** claimed responsibility for a cyberattack targeting the Los Angeles County Metropolitan Transportation Authority (LACMTA). The group published claims via their Telegram channel (t[.]me/ababilofminab/7) and their threat actor website (ababilofminab[.]io/metro-net-is-hacked/), including a video and multiple screenshots purporting to demonstrate access to live LACMTA internal systems. The group's website displays explicitly pro-Iranian messaging. LACMTA has not publicly confirmed or denied the breach at time of writing.

A note on screenshot credibility: All published screenshots contain an "Activate Windows" watermark in the bottom-right corner of the display. This watermark appears on Windows installations that have not been activated with a valid license. In a properly managed enterprise environment — such as a large public agency like LACMTA — endpoints are typically activated automatically and silently through volume licensing via a Key Management Service (KMS) server, meaning legitimate LACMTA workstations would not display this watermark under normal circumstances. Its presence across all screenshots suggests they were likely captured from an attacker-controlled virtual machine, a pivot host, or a jump server rather than from a native LACMTA endpoint. While this does not invalidate the access claims — attackers routinely use unactivated VMs as operational infrastructure to remotely view and interact with compromised systems — it is a meaningful forensic indicator that should inform any verification effort by LACMTA's internal security team.

Dataminr Alert



Dataminr alert regarding the attack enhanced with a Live Brief summary

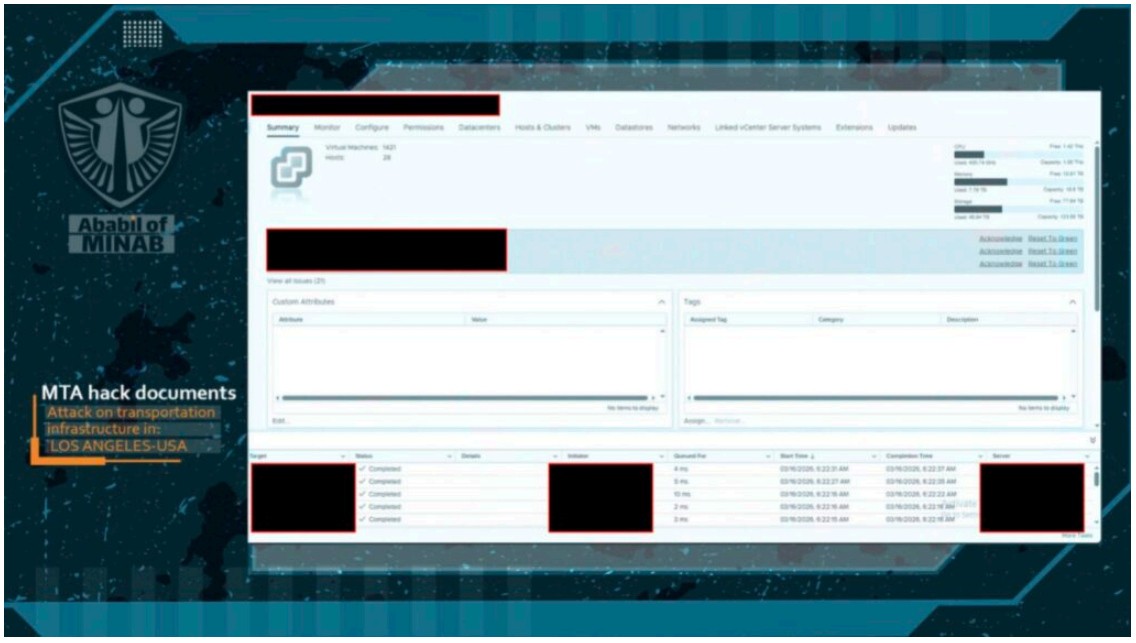
Technical Details

Three distinct system categories appear represented in the group's published evidence:

1. VMware vCenter Server Administrative access to LACMTA's core virtualization management platform, encompassing approximately 1,421 virtual machines, 28 physical hosts, ~430 GHz CPU, 7.79 TB RAM, and 45 TB active storage. Active system alarms were visible, indicating the environment was live at the time of capture.

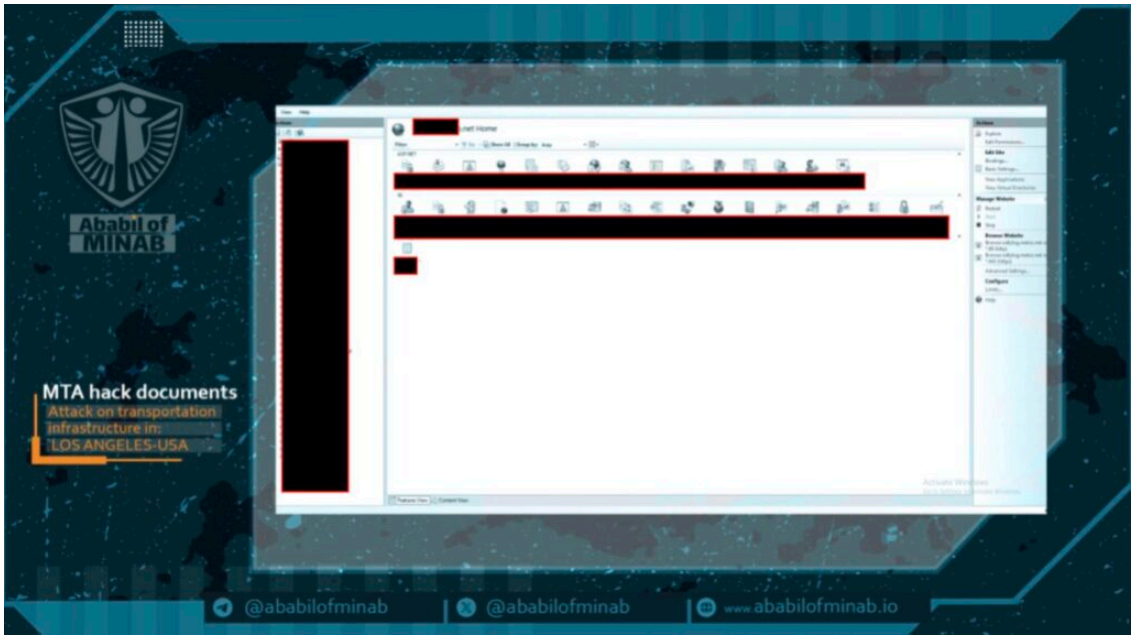
Compromise at this level could enable mass VM disruption, ransomware deployment, or persistent backdoor installation across LACMTA's server estate.

Sample of a screenshot from Ababil of Minab after targeting LA Metro. Source: Dataminr



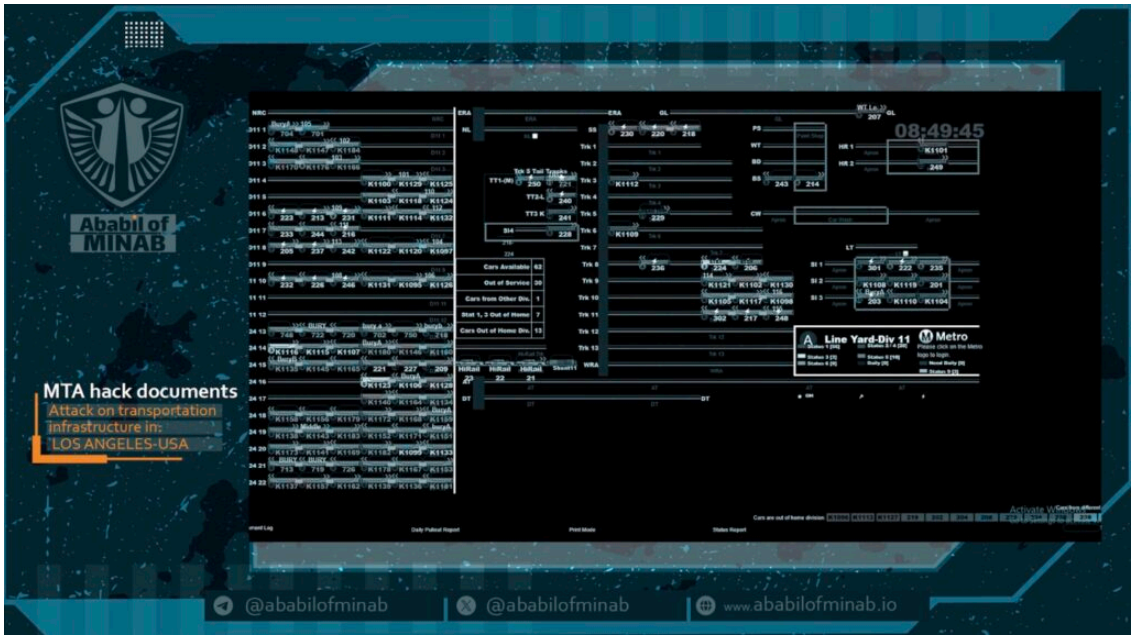
Sample of a screenshot shared from Ababil of Minab after targeting LA Metro. Source: Dataminr

2. Microsoft IIS Web Server Administrator-level access to an IIS instance hosting numerous internal and public-facing web properties including boardclerk.metro.net, sso.metro.net, registration.metro.net, and jobs.metro.net. This access level could enable web defacement, credential interception via the SSO portal, and lateral movement into backend application infrastructure.



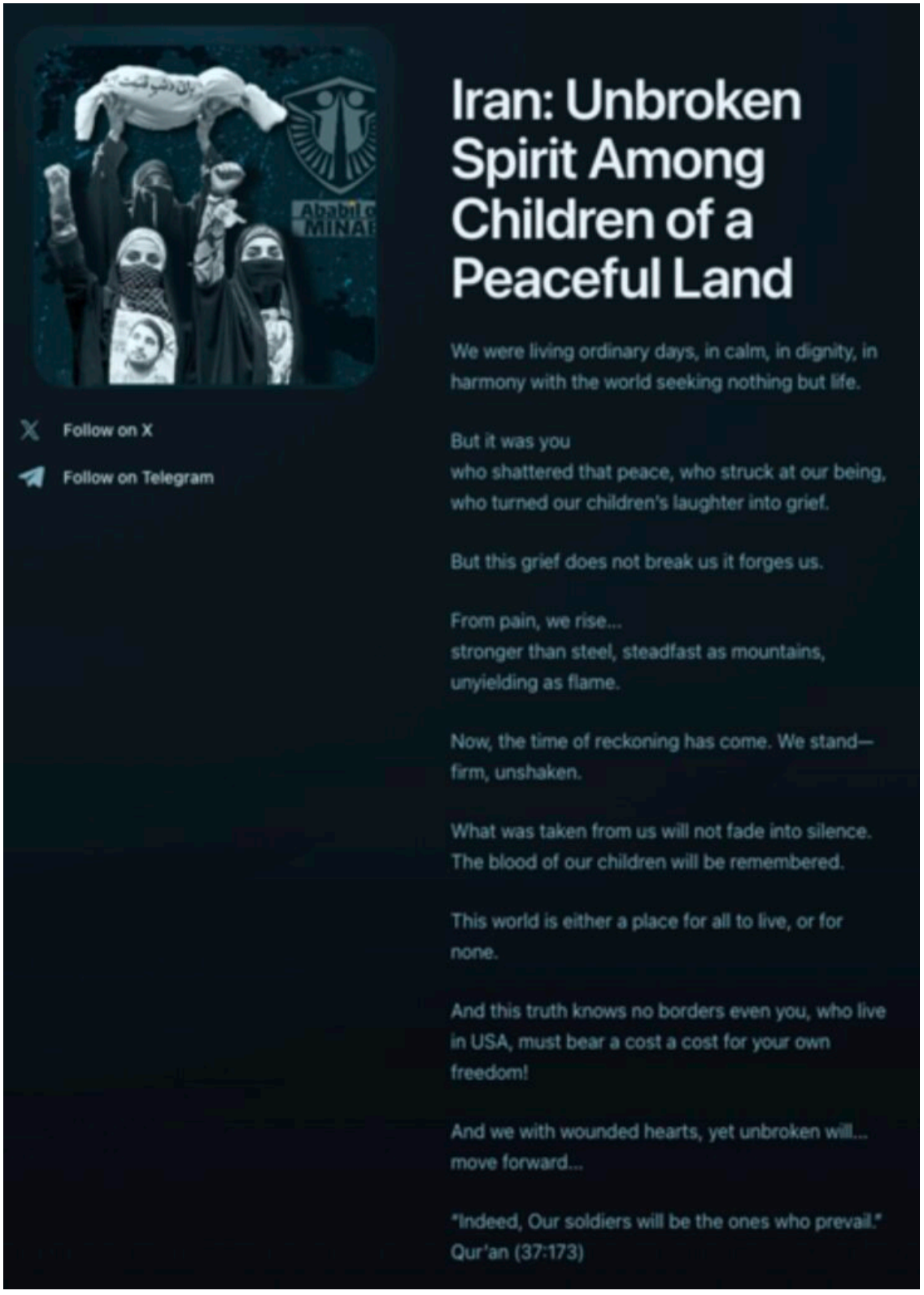
Sample of a screenshot shared from Ababil of Minab after targeting LA Metro. Source: Dataminr

3. Rail Yard Management / Train Control Display System The most operationally sensitive system visible in published evidence. The system appears to display real-time rail car positions, track occupancy, car availability, and out-of-service counts for one of LACMTA's division yards. This is an Operational Technology (OT) system. Unauthorized access to OT systems of this nature carries potential safety implications and may be subject to TSA and CISA critical infrastructure reporting requirements.



Sample of a screenshot shared from Ababil of Minab after targeting LA Metro. Source: Dataminr

Threat Actor & Motivation



Ababil of Minab's *own description of their mission and motivation. Source: Dataminr*

Ababil of Minab is an emerging pro-Iranian hacktivist group with a limited public profile and little verifiable prior activity in threat intelligence reporting — making any definitive capability or intent assessment premature at this stage. Despite this low prior visibility, Dataminr's real-time monitoring surfaced the group's claims at the point of initial publication, providing early warning ahead of traditional intelligence channels.

What can be cautiously observed from available evidence is that their explicit pro-Iran messaging and targeting of a major US public transit authority is broadly consistent with Iranian-aligned actors' known pattern of targeting US critical infrastructure. The group's escalatory language ("our forthcoming actions will exact sterner pain") may indicate further activity, though this should be treated as unverified rhetoric until corroborated by additional intelligence.

Immediate Actions & Recommendations

- **Isolate and Audit vCenter Environment:** Immediately audit VMware vCenter for unauthorized admin accounts, recent configuration changes, snapshot creation, or VM deletions. Review vCenter audit logs for sessions originating from unexpected IP ranges.
- **OT Network Segmentation — Urgent:** Verify that the Division 11 rail yard management and train control display systems are fully isolated from internet-facing IT networks. If any IT-to-OT pathway exists, implement emergency segmentation controls and notify relevant operations and safety teams immediately.
- **IIS Web Server Audit:** Review IIS server logs for unauthorized file modifications, web shell uploads, or configuration changes. Pay particular attention to the SSO portal for evidence of credential harvesting.
- **Credential Reset:** Force password resets for all privileged accounts across vCenter, IIS administration, and any systems visible in the published screenshots. Prioritize service accounts with broad environment access.
- **Regulatory Notification:** Assess reporting obligations to CISA, TSA Surface Division, and relevant California state authorities given the potential OT and critical infrastructure dimension of this incident.
- **Monitor Threat Actor Channels:** Continue monitoring Ababil of Minab's Telegram channel and website for additional published evidence, new target announcements, or escalating claims.
- **Block Known IOCs:** Block network traffic to and from ababilofminab[.]io and monitor for DNS lookups to this domain from within the LACMTA environment.
