Commonwealth Fusion Center (CFC)
Massachusetts
508.820.2233 | fusion@mass.gov

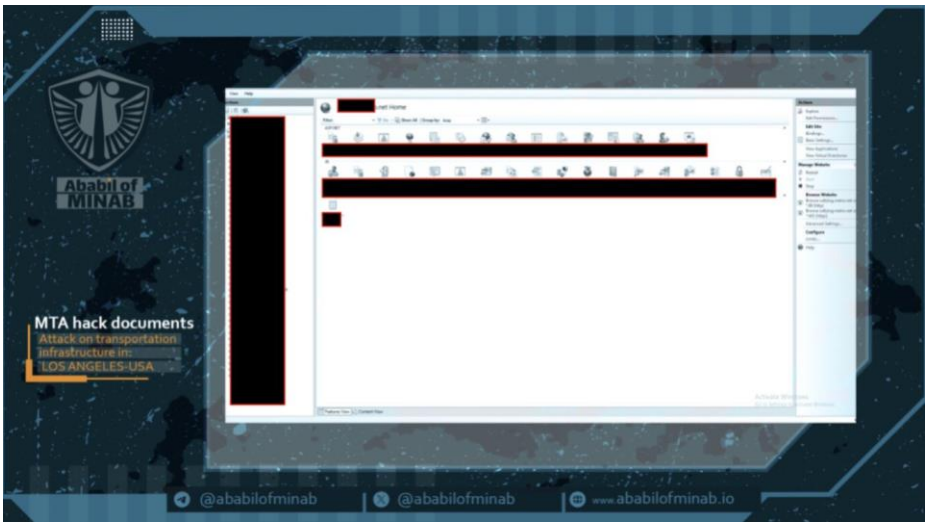
CYBER INTELLIGENCE BRIEF

(U) Iranian Cyber Threat Actor Claims Cyberattack on two US Entities

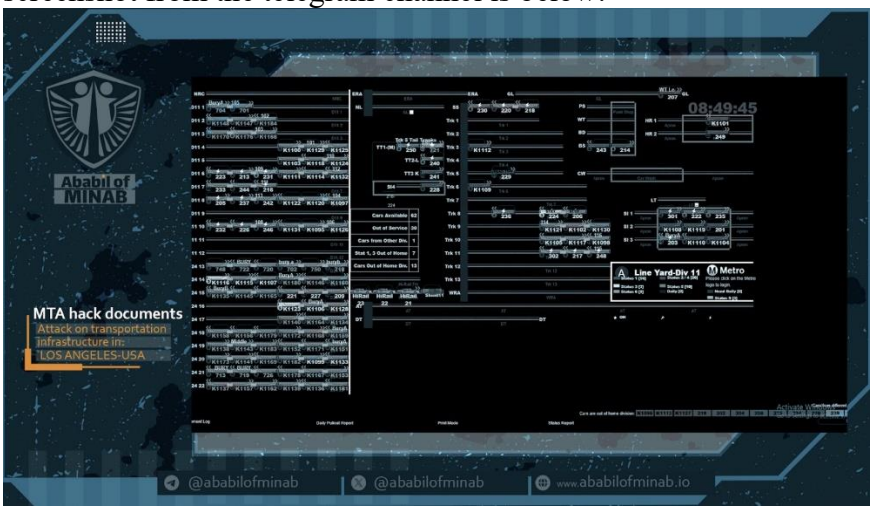
(U//FOUO) As part of the ongoing conflict with Iran, open-sources are reporting that Iranian state-sponsored cyberoperations are still active and is targeting US critical infrastructure. According to open-source reporting and active threat intelligence, Pro-Iranian threat actor **Ababil of Minab** has claimed responsibility for cyberattacks against Los Angeles County Metro Transit Authority (LACMTA) and GPS Services provider VYNCS.

(U//FOUO) The Iranian Advanced Persistent Threat (ATP) group has been identified through posts on their Telegram Channel and a Clearnet Website. The name is a combination of two locations in Iran. Minab is a city in Iran that was highlighted during missile strikes on February 28, 2026. A girls' elementary school in Minab was struck by a missile and resulted in the death of 180 children. Ababil is a drone (HESA Ababil-3) that is stationed on an airstrip in Minab. Ababil is mentioned in the Quran as a miraculous bird that dropped stones on their enemies. The City of Minab is located on the Strait of Hormuz.

(U//FOUO) According to Dataminr, Ababil of Minab claimed to have attacked LA County Metro IT systems including administrative access to VMware vCenter Server environment. Open-source reporting stated this cyber-attack required LA Metro Transit to take down internal systems which caused delays to patrons adding funds to their metro cards. Message boards showing departure and arrival times for trains and buses were not operational.



According to Dataminr, one of the most significant posts related to this attack is a screen shot showing real time car positions and track occupancy. This has been identified as an operational technology (OT) system. A screenshot from the telegram channel is below:



(U//FOUO) Ababil of Minab has also claimed to have breached a US company identified as VYNCS. This is a GPS Tracking Company that is based in Maryland. VYNCS serves both consumers and fleets, providing features like trip history, geofencing, fuel economy tracking, and maintenance alerts via a mobile app.

(U//FOUO) The Clearnet site for Ababil of Minab is hosted on Cloudflare with an associated IP of 188.114.97.3.

Recommendations:

(U//FOUO) Although intrusion methods are not known, The Commonwealth Fusion Center recommends that organizations remain vigilant and not ignore alerts or anomalies on their systems. Please report any suspicious activity to the Commonwealth Fusion Center and the FBI though IC3.gov.

Other References:

https://www.dataminr.com/resources/intel-brief/pro-iran-actor-ababil-of-minab-claims-cyberattack-on-la-metro/

https://www.securitymagazine.com/articles/102230-pro-iranian-actor-claims-la-metro-cyberattack