Indra Group Attack on Iran Highlights the Threats to Global Critical Infrastructure

By etal

Published: 2021-08-14 · Archived: 2026-04-05 17:19:04 UTC

Check Point Research (CPR) warns governments everywhere of the importance of protecting critical infrastructure, as it learns that the July 9 cyber attack on Iran's train system was carried out by Indra, a group that identifies itself as regime opposition and has the capability to wipe out data without direct means for recovery.

- CPR analyzed artifacts left by the July 9 cyber attack on Iran's train system, attributing the attacks to a group that self-identifies as Indra
- CPR confirms that Indra was also responsible for cyber attacks against multiple companies in Syria in 2019 and 2020
- CPR cites cyber attack on Iran's train system as an example for governments around the world of how a single group can create disruption on critical infrastructure

Check Point Research (CPR) has attributed the recent cyber attacks on Iran's train system to a group called Indra that self-identifies as opposition. Under the radar since 2019, Indra has been confirmed by CPR to be responsible for multiple cyber attacks carried out against companies in Syria. Two of the victims, Katerji Group and Arfada Petroleum, are on the US sanctions list.

On July 9, local news outlets began reporting on a cyberattack targeting the Iranian train system, with hackers defacing display screens in train stations by asking passengers to call '64411', the phone number of Iranian Supreme Leader Khamenei's office. Train services were disrupted and just a day later, hackers took down the website of Iran's transport ministry. According to news outlets, the ministry's portal and sub-portal sites went down after the attack targeted computers at the Ministry of Roads and Urban Development.

CPR analyzed artifacts left by the cyber attack on Iran's train system, learning that the attack tools were technically and tactically similar to those used in malicious activity against multiple companies in Syria.

Complicated Recovery Process

Indra's tools destroyed data without direct means to recover it. To carry out its cyber attacks, Indra ran what's known as a "wiper", malware designed to wipe the entire data system of critical infrastructure, making the recovery process complicated, locking users out of machines, changing passwords and replacing wallpapers to custom messages crafted by attackers.

Concern over Replication

CPR is concerned about the damage and disruption a single entity or group, such as Indra, can cause to critical infrastructure around the globe, as Indra's methods managed to infiltrate several sensitive and critical networks in

Iran and Syria, potentially harming human life.

We now live in an age where critical infrastructure in any corner of the world can easily be disrupted. If it can happen in Tehran, it can happen in Toronto, Tokyo, or San Francisco. What's most alarming to us is that a single group infiltrated and caused massive damage to critical infrastructure, potentially harming human life.

Governments around the world should take the recent cyber attack on Iran's train system as an example of how disruption can be created by hackers, not by penetrating entire strategic infrastructures, but by simply creating damage on screens or another visual focal point. This case in Iran is just one example, and can happen in any other country in the world. Check Point strongly recommends governments everywhere maintain the latest security patches and data backups, improve personal cyber-awareness training, and install anti-ransomware solutions.

Security and Protection Tips for Governments

1. **Enact a disaster recovery plan.** Make sure your organization or institution implements an effective disaster recovery plan, especially if it provides or supports any critical infrastructure. Such plan should usually include a full backup plan as well, as secondary networks should be activated in case of malfunction in the primary systems.
2. **Be up-to-date.** Make sure your systems are up to date and all recent security patches have been installed and deployed.
3. **Leverage 3rd party security software.** Use third party protection software to help protect against threat such as ransomware, wipers and many other attack vectors that might lead to disruption of your business.

For more technical details, please visit the CPR blog.
