Hackers say they encrypted Belarusian Railway servers in protest

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** January 24, 2022 12:34 PM 0

A group of hackers (known as Belarusian Cyber-Partisans) claim they breached and encrypted servers belonging to the Belarusian Railway, Belarus's national state-owned railway company.

They say their attack was prompted by Russia using Belarusian Railway's rail transport network to move military units and equipment into the country.

"At the command of the terrorist Lukashenka, Belarusian Railway allows the occupying troops to enter our land," the group said (https://twitter.com/cpartisans/status/1485615555017117700) today on Twitter.

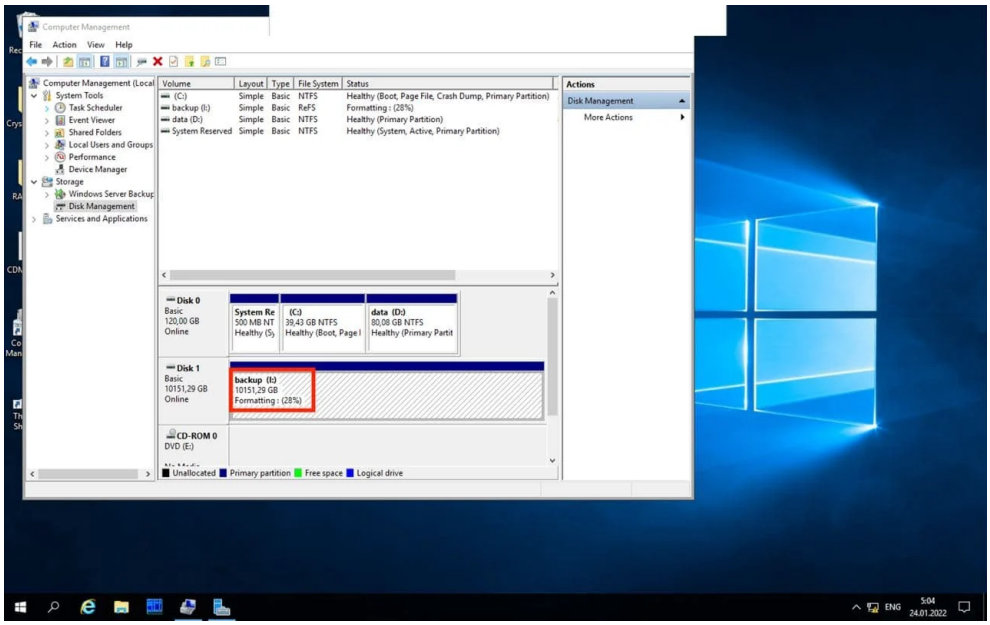
"We encrypted some of BR's servers, databases and workstations to disrupt its operations. Automation and security systems were NOT affected to avoid emergency situations."

The Belarusian Cyber-Partisans hacktivists say they have the encryption keys for the compromised Belarusian Railway servers. They added that they're also ready to return the systems to normal mode under some conditions.

They ask (https://twitter.com/cpartisans/status/1485618881557315588) for the release of 50 political prisoners in need of medical assistance and want the Russian troops out of Belarus.

On their Telegram channel, the group also shared screenshots from systems compromised in the incident, showing they had access to internal Belarusian Railway systems, Veeam backup servers, the Windows domain controller, and the backup server that contains tens of terabytes allegedly awaiting destruction.

One of the snapshots also shows the Belarusian Railway's online ticket service throwing an error when running an SQL query.



An alleged screenshot of the Belarusian Railway backup server

While Belarusian Railway has not issued an official statement, the company published an 'Attention passengers!' alert on its website today warning of ongoing problems with issuing electronic travel documents.

"For technical reasons, reference web-resources of the Belarusian Railways and services for issuing electronic travel documents are temporarily unavailable. To arrange travel and return electronic travel documents, please contact the ticket office." the company says (https://www.rw.by/corporate/press_center/news_of_passengers/2022/01/vnimaniyu-passazhirov_24012022/).

"Currently, work is underway to restore the performance of the systems. Belarusian Railways apologizes for the inconvenience caused."

The hackers say today's attack is part of a more extensive campaign they dubbed "Inferno (https://twitter.com/cpartisans/status/1461096501690736646)," "the largest sabotage cyberattacks in the history of Belarus."

Today's attack follows another incident from November (https://t.me/cpartisans/481) when they allegedly compromised and encrypted the entire network "of the Academy of Management under the President."

Related Articles:

Cyber espionage campaign targets renewable energy companies (https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/)

New White Rabbit ransomware linked to FIN8 hacking group (https://www.bleepingcomputer.com/news/security/new-white-rabbit-ransomware-linked-to-fin8-hacking-group/)

BlueNoroff hackers steal crypto using fake MetaMask extension (https://www.bleepingcomputer.com/news/security/bluenoroff-hackers-steal-crypto-using-fake-metamask-extension/)

'Elephant Beetle' spends months in victim networks to divert transactions (https://www.bleepingcomputer.com/news/security/elephant-beetle-spends-months-in-victim-networks-to-divert-transactions/)

Telecom operators targeted in recent espionage hacking campaign (https://www.bleepingcomputer.com/news/security/telecom-operators-targeted-in-recent-espionage-hacking-campaign/)