St. Paul’s Mayor Confirms Interlock Data Leak - Against Invaders - Notícias

Data: 2025-08-14 18:38:33

Autor: Inteligência Against Invaders

Officials from the City of St. Paul, Minnesota, have confirmed that the Interlock ransomware group has published employee data online after refusing the attackers’ payment demands.

Mayor Melvin Carter said that the gang appeared to have published approximately 43GB of data stolen from St. Paul City Council systems.

“The files they posted appear to come from a single shared network drive used by our Parks and Recreation department, a place where individual employees have stored their own personal files over time,” Carter commented during a press conference on August 11.

“These are not core city systems like payroll, permitting or licensing. The contents are varied and unsystematic. They could include everything from work documents, copies of IDs submitted for HR for travel, or even personal items like recipes,” he continued.

The City is offering 12 months of credit monitoring and identity theft to all its employees.

The press conference took place shortly after cybersecurity threat analysts observed the Interlock group update its data leak site with information it purportedly stole from City of St. Paul systems, including personal details of employees and residents.

“A large part of the infrastructure was damaged, brought a lot of losses and damage,” the group wrote in its post containing the stolen data.

Mayor Provides Insights into Ransomware Negotiations

Carter revealed that the City had engaged in communications with Interlock. He said the group ended negotiations after officials requested evidence for their claims about the data exfiltrated.

“We asked them to demonstrate what they had and instead of demonstrating what they had they decided to end the conversation, which was an indication to us that they may not have thought they had much by way of value,” Carter said.

“That assessment is consistent with the fact that instead of trying to sell the data, they had they released it for free,” he added.

Carter noted that all of St. Paul’s data was backed up, allowing the authority to maintain full control of its systems and access to all its data.

These factors, in addition to advice from the FBI and Minnesota National Guard, led to the decision not to pay Interlock's ransomware demand.

Carter noted that the City of St. Paul hosts approximately 153TB of data on its servers, meaning the 43GB released by the attackers is a tiny fraction of the overall volume.

City Services Continue to be Disrupted

After the incident was detected on July 25, the City initiated a full network shutdown to contain the threat.

This was just three days after US government agencies issued an advisory about the activities of the Interlock gang, including its novel initial access techniques.

The network shutdown has significantly disrupted local services for St. Paul's approximately 307,000 residents, including online payments for services such as garbage collection, regional water services and other public works.

St. Paul residents have also been told to contact the authority via email for all non-emergencies while it continues to restore communication platforms.

Mission critical operations, including emergency response and public safety services, remain fully operational, and Carter emphasized that keeping these services functioning remains the priority amid the ongoing incident response.

On July 29, Carter declared a state of emergency in response to the incident, allowing the City's departments of Emergency Management and Office of Technology and Communications (OTC) to mobilize support from local, state and federal partners.

Carter also provided an update on new security measures implemented as it looks to securely its digital infrastructure:

- The completion of in-person password resets, credential verification and security scans for more than 2000 City Council employees
- Advanced security software installed on 90% of all unique city devices
- Collaborated with the Minnesota National Guard, the FBI and private cybersecurity experts to ensure the integrity of every server, system and application hosted by the City

No details have so far been provided on how the attackers gained initial access to St. Paul's systems.

Image credit:EWY Media / Shutterstock.com