FORT ST. JOHN

The Energetic City

February 2025 Cyber Incident

Summary

- The City of Fort St. John was the victim of a double extortion ransomware attack
- This will walk you through:
  - The Canadian cybersecurity landscape
  - What double extortion ransomware is
  - How the criminals got in
  - How they moved throughout the system
  - What they did once they were in
  - How the City recovered

FORT ST. JOHN
The Energetic City

Canadian Cybersecurity Landscape

“Ransomware is the top cybercrime threat facing Canada’s critical infrastructure. Ransomware directly disrupts critical infrastructure entities’ ability to deliver critical services, which can put the physical and emotional wellbeing of victims in jeopardy.” – *National Cyber Threat Assessment 2025-2026*

FORT ST. JOHN
The Energetic City

Canadian Cybersecurity Landscape

"**The Cybercrime-as-a-Service (CaaS) business model is almost certainly contributing to the continued resilience of cybercrime in Canada and around the world.** The CaaS ecosystem is underpinned by flourishing online marketplaces where specialized cyber threat actors sell stolen and leaked data and ready-to-use malicious tools to other cybercriminals." – *National Cyber Threat Assessment 2025-2026*

FORT ST. JOHN
The Energetic City

Cybercrime is on the rise

Most common causes of cyber losses in 2024

Cause	Loss
Bank Transfer Fraud	$44,000
Ransomware	**$1,000,000**
Business Email Compromise	$150,000
Hacker	$113,000
Malware/Virus	$533,000
Employee Error	$29,000

- Headlines:
  - There is no good news about ransomware statistics
  - $1,000,000 average cyber loss of a ransomware incident in 2024
  - The average cost of a cyber incident was $6.5 million in 2024
  - The cost of cybercrime was projected to be $10.5 trillion annually by 2025
  - Cybercrime will become the world's third-largest economy this year, worth $20 trillion

FORT ST. JOHN
The Energetic City

Canadian Cybersecurity Landscape

"CCCS [*Canadian Centre for Cyber Security*] assesses that the direct threat to Canada's critical infrastructure from PRC state sponsored actors is likely lower than that to U.S. infrastructure, **but should U.S. infrastructure be disrupted, Canada would likely be affected as well, due to cross-border integration**." *– PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*

FORT ST. JOHN
The Energetic City

Canadian Cybersecurity Landscape

“From October 2023 through September 2024, Shared Services Canada’s secure Enterprise Internet Service blocked about 6.6 trillion suspicious cyber security events.” - *2025 Report of the Auditor General of Canada to the Parliament of Canada*

Reference Paragraph 15

FORT ST. JOHN
The Energetic City

Major Themes

- Configuration Drift
- Project Tempo
- Defense-in-Depth

FORT ST. JOHN
The Energetic City

What is double extortion ransomware?

- The criminals attack you in two ways:
  - They encrypt your data
  - They exfiltrate your data
- Triple extortion ransomware is on the rise, **but not what the City was subjected to**.

FORT ST. JOHN
The Energetic City

Cybercrime-as-a-Service

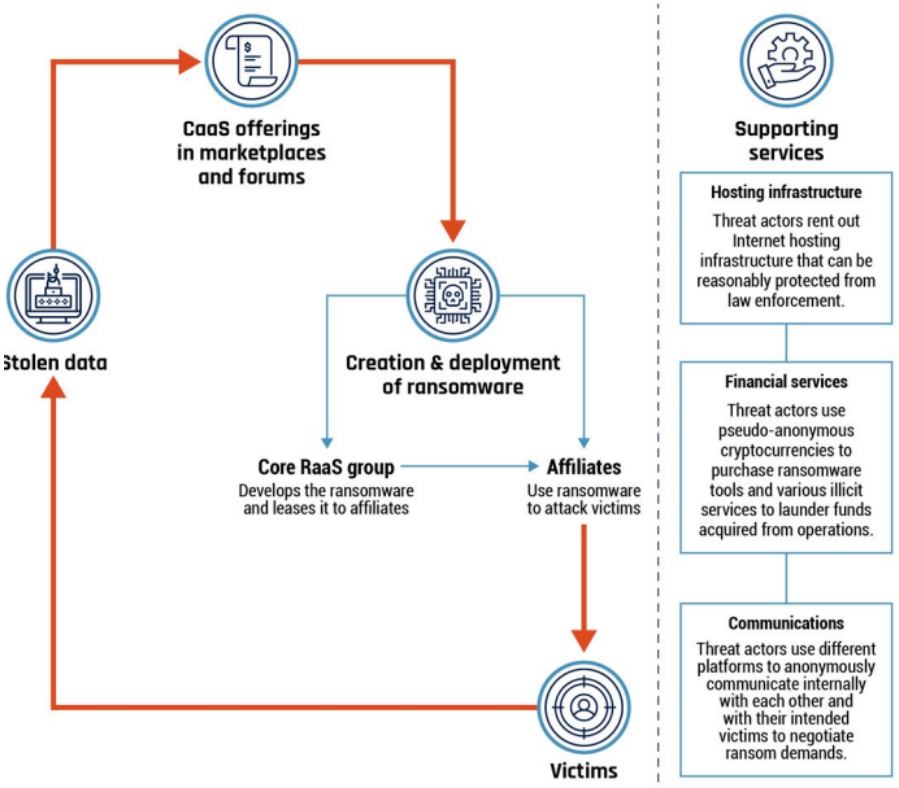
We were attacked by a “Cybercrime-as-a-Service” criminal group.

These groups buy compromised credentials from dark web markets and uses them in combination with exploits developed by other criminals.

Compromised credentials are not that expensive. Costs range between $30 USD to $65 USD per account.

Picture from the National Cyber Threat Assessment 2025-2026

Figure 10: RaaS ecosystem



FORT ST. JOHN
The Energetic City

How did we know something was wrong?

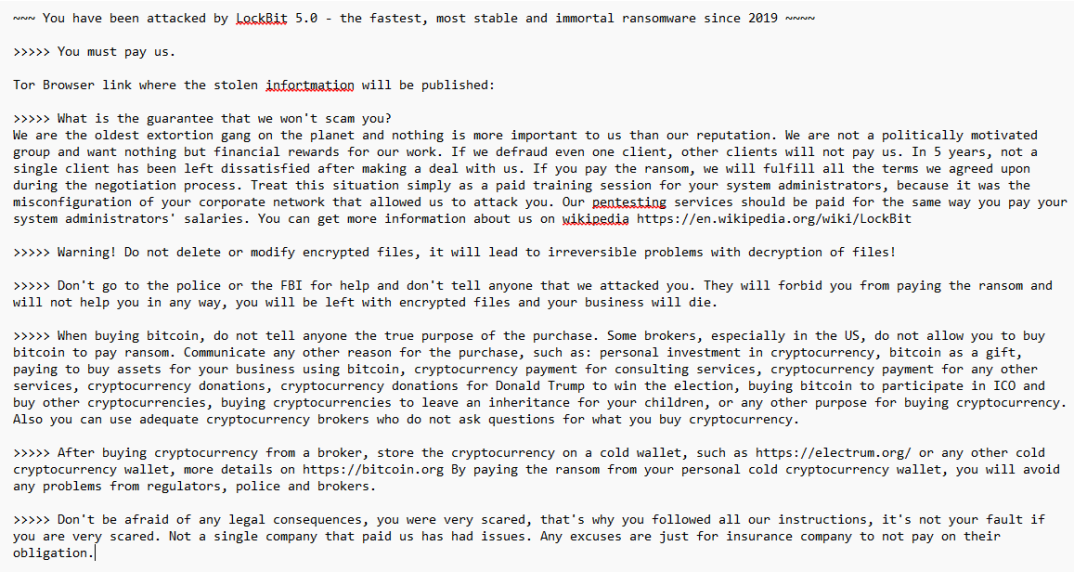
- Services were reported down by users around 6:30 AM.
- Servers were unresponsive upon investigation.
- When the server wouldn’t reboot, investigating them revealed that they were encrypted.
- Upon further inspection, a large amount of data was leaving the network.
- Attackers called to confirmed they had breached us around 7:00 AM that morning.

FORT ST. JOHN
The Energetic City

Ransom Notes

Most ransom notes follow a standard pattern:

- Here's how you get ahold of the criminal
- Don't contact the police
- Don't tell anyone you've been hacked
- Pay us in Bitcoins
- Get on the dark web



~~~ You have been attacked by LockBit 5.0 - the fastest, most stable and immortal ransomware since 2019 ~~~~

>>>>> You must pay us.

Tor Browser link where the stolen infortmation will be published:

>>>>> What is the guarantee that we won't scam you?
We are the oldest extortion gang on the planet and nothing is more important to us than our reputation. We are not a politically motivated group and want nothing but financial rewards for our work. If we defraud even one client, other clients will not pay us. In 5 years, not a single client has been left dissatisfied after making a deal with us. If you pay the ransom, we will fulfill all the terms we agreed upon during the negotiation process. Treat this situation simply as a paid training session for your system administrators, because it was the misconfiguration of your corporate network that allowed us to attack you. Our pentesting services should be paid for the same way you pay your system administrators' salaries. You can get more information about us on wikipedia https://en.wikipedia.org/wiki/LockBit

>>>>> Warning! Do not delete or modify encrypted files, it will lead to irreversible problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you. They will forbid you from paying the ransom and will not help you in any way, you will be left with encrypted files and your business will die.

>>>>> When buying bitcoin, do not tell anyone the true purpose of the purchase. Some brokers, especially in the US, do not allow you to buy bitcoin to pay ransom. Communicate any other reason for the purchase, such as: personal investment in cryptocurrency, bitcoin as a gift, paying to buy assets for your business using bitcoin, cryptocurrency payment for consulting services, cryptocurrency payment for any other services, cryptocurrency donations, cryptocurrency donations for Donald Trump to win the election, buying bitcoin to participate in ICO and buy other cryptocurrencies, buying cryptocurrencies to leave an inheritance for your children, or any other purpose for buying cryptocurrency. Also you can use adequate cryptocurrency brokers who do not ask questions for what you buy cryptocurrency.

>>>>> After buying cryptocurrency from a broker, store the cryptocurrency on a cold wallet, such as https://electrum.org/ or any other cold cryptocurrency wallet, more details on https://bitcoin.org By paying the ransom from your personal cold cryptocurrency wallet, you will avoid any problems from regulators, police and brokers.

>>>>> Don't be afraid of any legal consequences, you were very scared, that's why you followed all our instructions, it's not your fault if you are very scared. Not a single company that paid us has had issues. Any excuses are just for insurance company to not pay on their obligation.

Example ransom note from LockBit ransomware

FORT ST. JOHN
The Energetic City
~~~

How did they get in?

Zero Day VPN Exploit

- Files were found on our firewall that indicated a specific exploit.

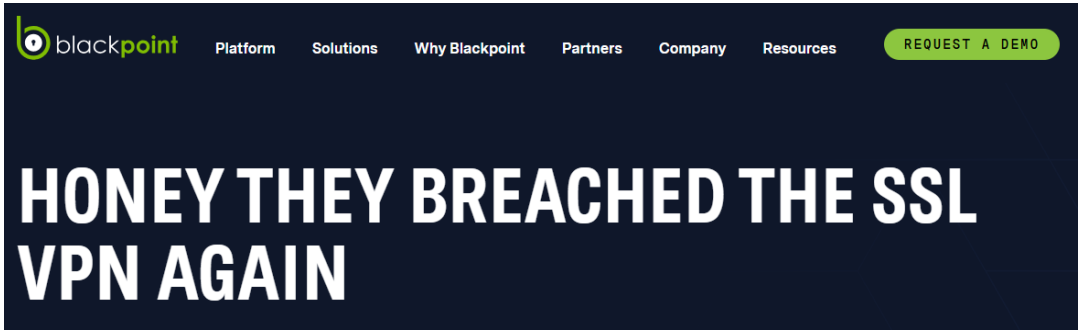
Stolen credentials from Dark Web

- Log activity indicated compromised accounts were used from untrusted locations.
- The first login occurred about a week prior to our patching date, suggesting the cybercriminals had been in the system for a week.

FORT ST. JOHN
The Energetic City

VPNs are high risk

- Corporate VPNs have seen an uptick in use since COVID
- Every major corporate VPN provider has had a zero-day exploit in the last 5 years
- An exploit is a bug or flaw in a software that can be used to hack a device
- A zero day means that the flaw is exploited before the company has a chance to fix it



FORT ST. JOHN
The Energetic City

How did they move around?

- Network reconnaissance
- Dictionary password attack against our servers
- Ambiguity on what happened next
- Admin accounts were then compromised

FORT ST. JOHN
The Energetic City

Once they were in, what did they do?

- Compromised accounts used to copy files
- Files were copied onto a staging server
- Tools were then run at low speed to compress the data

FORT ST. JOHN
The Energetic City

How did it end?

- Data was then exfiltrated starting at 4:30am
- Attackers started to encrypt our data at the same time

FORT ST. JOHN
The Energetic City

Post-Attack and Recovery

FORT ST. JOHN
The Energetic City

Incident Response

- Call your cyber insurance company today.
- Store your copy of your cyber insurance policy offline.
- Ransomware actors will use that policy against you if they find it.

- All networking equipment and servers were taken offline
- The City engaged its cyber insurance provider
- The City's cyber insurance engaged their incident response team
- Incident response team provided remediation and investigation tools
- Servers were restored and cleared over the following week
- Incident response team engaged in communications with the cybercriminals over the next few weeks

FORT ST. JOHN
The Energetic City

Incident Response

- Call your cyber insurance company today.
- Store your copy of your cyber insurance policy offline.
- Ransomware actors will use that policy against you if they find it.

- All networking equipment and servers were taken offline
- The City engaged its cyber insurance provider
- The City's cyber insurance engaged their incident response team
- Incident response team provided remediation and investigation tools
- Servers were restored and cleared over the following week
- Incident response team engaged in communications with the cybercriminals over the next few weeks

FORT ST. JOHN
The Energetic City

Attacker Communications

- Your incident response team will handle these types of communications.
- One of Incident Response's key tactics is stalling for time, because cybercriminals can and routine do forget about their victims.

- The criminals reached out at 7:00 AM to the CAO and started calling random workers at the City
- The criminals wanted a single payment of bitcoins, but was willing to split the cost into two separate costs
- The criminals wanted the City to get into a private chat
- The criminals then provided the City with a list of files they had
- The City then had the criminals prove they could decrypt the files by sending encrypted junk files to them

FORT ST. JOHN
The Energetic City

Posting

- Cybercriminals typically give you a few weeks to make a payment decision before previewing your information.
- Previewing involves posting a small sample of files publicly.
- If you don’t follow up after that, they then post everything they have *if they remember*.

FORT ST. JOHN
The Energetic City

What Can You Do About It?

FORT ST. JOHN
The Energetic City

Building a More Cyber-Ready Local Government

- Cyber readiness requires both everyday protective practices and support when incidents occur.
- MIABC helps our members understand risks and establish practical routines that reduce exposure.
- The Victor Cyber Program provides coordinated support, tools, and expert response during cyber events.
- Together, they strengthen your ability to prepare, prevent, detect, respond, and recover.

FORT ST. JOHN
The Energetic City

Cyber Awareness: Your First Line of Defence

- Most Incidents start with phishing
- Alert and aware staff stop threats early
- Awareness prevents escalation
- Supported by MIABC/Victor Programs and Training

FORT ST. JOHN
The Energetic City

Reducing Risk Through Credential Awareness

- Attackers often gain access using stolen or reused passwords
- Early detection enables fast response and account protection
- Victor Cyber Program helps detect credential risk sooner
- Credential monitoring reduces one of the most common entry points

FORT ST. JOHN
The Energetic City

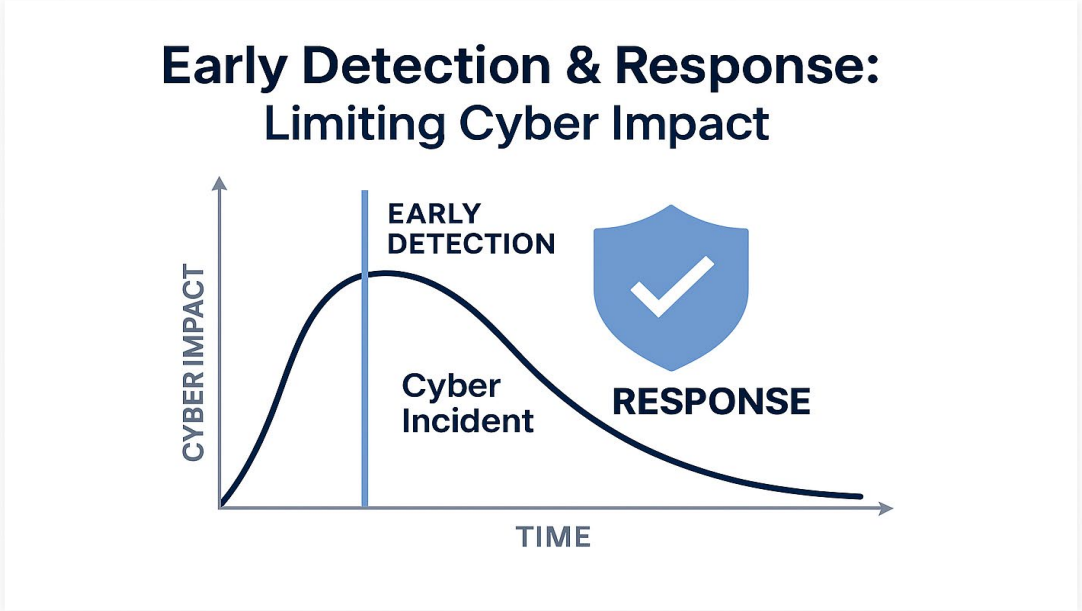
Stronger Logins, Stronger Security

- What is Multi Factor Authentication?
- MFA blocks most unauthorized access attempts
- MIABC and Victor via our program promote MFA and reduced admin access
- Victor Cyber reinforces proven controls
- Stronger login protections reduce impact and frequency of incidents

FORT ST. JOHN
The Energetic City

Early Detection & Response: Limiting Cyber Impact

- EDR tools detect unusual activity early
- Program features through MIABC/Victor encourages proactive monitoring
- Victor Cyber program provides thorough incident response expertise
- Early detection plus expert support limits spread and impact



FORT ST. JOHN
The Energetic City

Reducing Impact Through Updates and Reliable Recovery

PREVENTION: Regular Updates

- Out-of-date systems create exploitable vulnerabilities
- Regular patching removes known attack paths
- Victor Cyber Program recognizes updates as a key risk-reduction control

RECOVERY: Strong Backups

- Backups enable fast recovery after incidents
- Critical for legacy systems with limited protections
- 3-2-1 backup rule ensures resilient recover
  - 3 copies of data
  - 2 storage types
  - 1 off-site copy
- MIABC promotes simple, effective backup practices
- Victor Cyber Program supports coordinated restoration

FORT ST. JOHN
The Energetic City

Cyber Insurance: Understanding Your Policy and Coverage

POLICY AWARENESS

- Review your cyber insurance policy regularly
- Understand coverage limits and deductibles
- Know what services are included with your policy
- Be clear on reporting requirements and timelines

INCIDENT SUPPORT & RESPONSE

- Know who to contact during a cyber incident
- Understand how to report an incident quickly
- Victor Cyber Program provides immediate and ongoing support through multiple avenues
- Clear coverage knowledge from a staff and management level, enables faster decisions

FORT ST. JOHN
The Energetic City

Open Discussion

FORT ST. JOHN
The Energetic City