



CANADA

Inside the Chinese military attack on Nortel



By Sam Cooper · Global News

Posted August 25, 2020 4:00 am · Updated September 8, 2020 5:46 pm

MORE FROM GLOBAL NEWS



French court set to deliver verdict in trial over 2015 Paris attacks



Controversy rages over upcoming Newfoundland sugar tax

ADVERTISEMENT

This ad will end in 31

WATCH: Learn more about the Chinese military cyberattack on Canada's Nortel – Aug 25, 2020

Facebook Twitter Email Plus

-A A+

It was a mind-blowing clue.

In 2004 Nortel cyber-security advisor Brian Shields investigated a serious breach in the telecom giant's network. At the time Nortel's fibre optics equipment was the world's envy, with 70 per cent of all internet traffic running on Canadian technology.

And someone wanted Nortel's secrets.

Shields found that a computer in Shanghai had hacked into the email account of an Ottawa-based Nortel executive. Using passwords stolen from the executive the intruder downloaded more than 450 documents from "Live Link" — a Nortel server used to warehouse sensitive intellectual property.

Shields soon found the hacker controlled the accounts of at least seven Nortel executives. This was no random cybercriminal. But who was it?

Shields examined the numerical internet addresses of computers extracting Nortel data and found that they were clustered into a tiny pinprick of cyberspace. He was stunned because it looked like a room filled with web servers. Whoever was behind these hackers, Shields believed, seemed to control China's internet.

STORY CONTINUES BELOW ADVERTISEMENT

TRENDING



What causes long COVID? Canadian researchers think they've found a key clue

62712 READ

“It hit me like a ton of bricks,” Shields said.

“I knew this couldn’t be happening by chance.”

TWEET THIS

1:43
China ‘totally took us down’: former Nortel cyber-secur...

China ‘totally took us down’: former Nortel cyber-security investigator – Aug 25, 2020

Shields says the Internet addresses were all registered to Shanghai Faxian Corp., a company with no connection to Nortel that Shields determined was a front with no real business in China.

Shields spotted another major clue in Nortel’s logs of network traffic from Saturday, April 24, 2004. According to Shields, in just seven hours a Shanghai Faxian address downloaded 779 documents that day using the account of Nortel CEO Frank Dunn. The hack occurred four days before Dunn was fired, amid an investigation of accounting irregularities. To Shields, this suggested the Shanghai hackers knew exactly what Nortel’s board of directors planned, and the perfect time to extract a massive cache of records.

STORY CONTINUES BELOW ADVERTISEMENT

-64%

Total...
\$39.99

Undef...
\$9.99

Pilgrims
\$4.99

Warha
\$79.99


Buy Now

“To date, we have 1,488 documents which were downloaded,” Shields wrote to Nortel’s management in his “data theft” investigation report. “China is the source of all extractions we are aware of.”


READ MORE: [United Front groups in Canada helped Beijing stockpile coronavirus safety supplies](#)

For months Shields tracked the hackers. But Nortel’s brass was mostly disinterested in the investigation and did little more than change executive account passwords, Shields says. He says they were more focused on year-to-year profits and innovation budgets than protecting Nortel’s precious research. Mike Zafirovski, Nortel’s CEO from 2005 to 2009, did not respond to questions for this story sent to his LinkedIn account. Zafirovski said Shields was known to “cry wolf” and management didn’t believe hacking was a real issue, the Wall Street Journal reported in 2012.


So the systematic hacking continued, Shields says. And as a result, Shields says, in 2009 — after getting massively underbid on a series of contracts by China’s state-champion company Huawei — Nortel went bankrupt.




6 officers injured in shooting at Saanich, B.C. bank, 2 suspects killed
22396 READ



Tuesday’s \$70 million Lotto Max jackpot claimed by single ticket sold in Ontario
7229 READ




‘ER’ actor Mary Mara, 61, dies in apparent drowning in St. Lawrence River
5753 READ

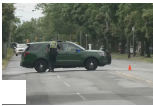


‘We are suffocating’: Details emerge as 21 teens found dead in South Africa nightclub
5649 READ


TOP VIDEOS




Ontario researchers focus on possible clue of long COVID
28930 VIEWED




Multiple people injured in shooting at Saanich, B.C. bank
16160 VIEWED



North Vancouver cat chases away bear
3609 VIEWED




Families seek answers after 21 teens likely killed by unknown substance at South Africa nightclub
3166 VIEWED



NASA’s CAPSTONE orbiter aims to create new path back to the moon
2872 VIEWED

MORE VIDEOS >



NATIONAL

Stay in the loop

Get a roundup of the most important and intriguing national stories delivered to your inbox every weekday.

ADVERTISEMENT



JCPenney
Ends 7/10
4th of July Home Sale
up to extra 50% + 30% off
with coupon | select styles
Shopping is back!
Shop Now
*Coupon required. Exclusions apply.
Fast + FREE Same-Day Pickup. Choose outside or in-store pickup.

In the end, Shields determined China's government gained complete control of Nortel's internal systems. After ten years of cyberattacks they could see everything Nortel was doing, he says. The infiltration was so insidious, Shields says, that technicians in China could send encrypted packages of stolen Nortel data to Shanghai and Beijing, by sending Internet commands to a "backdoor" buried in a Nortel computer.

STORY CONTINUES BELOW ADVERTISEMENT

To visualize that in the real world — it would be similar to a foreign army constructing a hidden tunnel into Canada's treasury vault, and marching out unimpeded with gold bars.

And it was more than coincidence, Shields believes, that upstart Huawei suddenly replaced Nortel as the world's dominant internet technology provider.

"You could have put Steve Jobs in to run Nortel. But if you are up against a nation-state, Nortel would have failed, without Canadian government intervention," Shields said.

"Canadians just don't realize the extent of the Chinese government's involvement in this thing."

TWEET THIS

1:18

Alliance Canada Hong Kong leader says a Huawei 5G ...

Alliance Canada Hong Kong leader says a Huawei 5G network in Canada would track citizens – Aug 25, 2020

Now, more than 20 years after Nortel was first warned of Chinese Communist Party espionage, Hong Kong Canadians such as Cherie Wong say that Ottawa's failure to protect Nortel and to promptly bar Huawei from modern 5G networks is putting lives at risk.

STORY CONTINUES BELOW ADVERTISEMENT

Wong, executive-director of Alliance Canada Hong Kong, an umbrella group for democracy advocates, says Chinese dissident groups are already tracked and targeted by the Chinese Communist Party in Canada, through Chinese social media apps like WeChat and TikTok. And the threat of Huawei 5G Internet in Canada is much worse, she says.

4:57

Inside the Chinese military's attack on Nortel

Inside the Chinese military's attack on Nortel – Aug 25, 2020

"It's a growing concern whether or not Canada is equipped to combat this level of interference from the Chinese Communist Party," Wong said.

"We are being threatened and harassed. So giving Huawei control of the internet means everything we do will be monitored and tracked and given to the Chinese state."

TWEET THIS

However, Huawei strongly denies benefiting from the hacking of Nortel, and says it has never been accused of wrongdoing in Canada. The company says it complies with Canadian law and will not spy on Canadians.

STORY CONTINUES BELOW ADVERTISEMENT

People's Republic of China officials in Canada did not respond to detailed questions for this story.

"Actionable intelligence"

A collection of Canadian military records sought by Global News that could shed light on reports of massive espionage inside Nortel's former Ottawa research headquarters are currently in a delayed vetting disclosure process, a Canadian military spokesman informed Global News. But Brian Shields says he is certain Ottawa has records that will show Canadians "the truth about what happened to Nortel."

One public record that suggests Ottawa may acknowledge a connection between China's attack on Nortel and Huawei's subsequent rise is a coy statement in the summary report of an academic conference held by Canadian Security Intelligence Service.

"Ex-Nortel employee Brian Shields, who had led the forensic investigation of the compromise, came forward to disclose his experiences," the summary report says. "Nortel went bankrupt in 2009. [Could there be a link between the Nortel breaches](#) and the rising fortunes of Nortel's main China-based competitors, Huawei and ZTE?"

The report doesn't answer that question.

But a Canadian intelligence expert with knowledge of investigations at Nortel says Ottawa knows exactly what happened in the case.

"The evidence that China compromised Nortel is indisputable," the expert said. "It was being systematically compromised, and everything was being taken. The only question is to what extent that caused Nortel to fall."

STORY CONTINUES BELOW ADVERTISEMENT

Global News has agreed not to name the expert because of his concerns that China's government is targeting him due to his probes of continuing cyberattacks.

The expert said China's attack on Nortel had many facets, from systematic hacking and planting of electronic bugs and spies inside Nortel facilities, to usage of Chinese PhD students hired by Nortel to steal research, and attempts to compromise Nortel managers by using spies from the Chinese Communist Party and People's Liberation Army.

READ MORE: [Canadian minister promises review after security contracts awarded to Chinese-state tech company](#)

Many of these allegations are consistent with a February 2020 U.S. Department of Justice indictment that [alleges Huawei](#) was involved in a decades-long conspiracy to steal technology from numerous victim companies in efforts to grow its market share, the expert said.

"There were visits by Nortel executives going to China to be wined and dined," the expert said. "It was China's classic [United Front statecraft](#). And those executives were told in no uncertain terms by their security, 'You are being recruited, and they will compromise your computers and cellphones.'"

But to Shields and former CSIS agents, it seemed Nortel management saw the warnings as exaggerated spy novel plots.

"There was detailed actionable intelligence naming people and methods and targets," the expert said. "There were people that were caught, and devices found, and backdoors found and traced back to the Chinese. And this was escalated up to Nortel leaders. And they didn't really want to see it."

STORY CONTINUES BELOW ADVERTISEMENT

The expert said Canadian intelligence eventually made the stunning discovery that the Chinese Communist Party was using Chinese organized crime gangsters, in attacks on Nortel.

"We have seen organized crime, industry and government all spy and collect on Nortel," the expert said.

“The best way to describe it is between a nation-state, industry and organized crime, there is cooperation to the point of collaboration and collusion. Spying on Nortel became a requirement that satisfied everyone in that community.”

TWEET THIS

READ MORE: [Fentanyl kings in Canada allegedly linked to powerful Chinese gang, the Big Circle Boys](#)

In July — in a case that mirrors such allegations — [the FBI accused Chinese intelligence services and organized crime groups](#) of colluding in cyberattacks targeting COVID-19 vaccine research and intellectual property in many nations, and Chinese dissidents in Canada.

Michel Juneau-Katsuya — former CSIS Asia-Pacific desk chief — confirmed his former CSIS colleague’s observations regarding China’s attack on Nortel.

Juneau-Katsuya said he first completed a threat assessment on Nortel in the 1990s, and determined it was China’s top corporate espionage target. Soon CSIS recognized “quite an interesting traffic between Nortel and China,” Juneau-Katsuya says.

But his alerts to Nortel fell on deaf ears, he said.

STORY CONTINUES BELOW ADVERTISEMENT

“What is missing in the Nortel story is exploring the relationship that has been flagged about all those [Nortel] leaders going to China for decades,” Juneau-Katsuya said. “I am confident you can see relationships where the [United Front Work Department](#) will appear in the Nortel case.”

Beijing’s United Front — according to a [2020 report](#) from Australian analyst Alex Joske — is the Chinese Communist Party’s vast political influence and espionage network, which uses actors from business, politics and organized crime, to target Western political and business leaders and obtain intellectual property for China.

Juneau-Katsuya suspects the Chinese Communist Party used the United Front to take Nortel down and boosted Huawei into its place by providing the company with subsidies and stolen technology.

READ MORE: [Canadian mayors may have unwittingly been targets of Chinese influence campaign](#)

“Nortel is one of those situations, where Canada had the lead internationally, and we let it go. Why? For one, there were forces within the Canadian government. And Huawei received billions from their government. So if I invest billions into you, I will expect to control that operation. And Huawei’s founder is from the People’s Liberation Army. So he knows how to follow orders. So I will make you very rich, and I will give you intelligence support, and I will assist in stealing information.”

STORY CONTINUES BELOW ADVERTISEMENT

“In retrospect, it’s clearly written on the wall how this happened. There is enough circumstantial evidence.”

TWEET THIS

Juneau-Katsuya’s former CSIS colleague said prior to Nortel’s collapse Ottawa lacked the strategic foresight and capacity to fight China’s infiltration.

The RCMP has jurisdictional and technical challenges investigating state-sponsored cybercrime, the expert said, while CSIS and the CSE, Canada’s cyberintelligence agency, are reluctant to involve themselves in threats against industry.

“It was like a game of volleyball when everyone calls the ball but no one goes for it,” the expert said. “The Nortel example was like we have a nation-state against our industrial complex, and we don’t even have an agency mandated to tackle it.”

8:41

Canada should listen to intelligence community when ...

Canada should listen to intelligence community when deciding on Huawei – Nov 24, 2019

The expert said Canada is starting to recognize the gravity of state-sponsored attacks on private industry but the government still isn’t prosecuting cases.

STORY CONTINUES BELOW ADVERTISEMENT

Meanwhile, in the United States, the FBI is opening a new case against Chinese espionage every ten hours, according to director Christopher Wray.

It isn’t only China involved in corporate espionage. Western high-tech companies have also faced accusations of IP theft, most often in civil court battles. But according to the FBI the majority of IP theft cases involve a range of actors sponsored by the Chinese Communist Party.

“It’s the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history,” Wray said in July.

READ MORE: [Trump administration imposes more Huawei restrictions, claims tech is used for spying](#)

It remains to be seen what details the FBI will allege in its IP theft indictment against Huawei. And Huawei rejects allegations that it stole technology from companies in the United States in order to grow its market share.

But some former Nortel employees recognize the types of allegations made so far.

Shields and former Nortel corporate security employee Mike Kennedy told Global News about a case that occurred in the United States from about 2000 to 2003, the same time that Huawei allegedly reverse-engineered Cisco Internet routers according to the FBI indictment.

STORY CONTINUES BELOW ADVERTISEMENT

Some Nortel investigators alleged a company linked to Huawei had returned expensive networking equipment to a Nortel office and asked for a refund. Investigators judged the equipment had been completely disassembled and copied for IP theft. Kennedy and Shields said a third-party company was involved in this alleged reverse-engineering case, which resembles the FBI's allegations against Huawei in the Cisco case.

But Huawei says it has never stolen IP from Nortel.

Wrestling with Unit 61398

For Brian Shields, when the U.S. cybersecurity firm Mandiant pointed to Unit 61398, it made perfect sense.

Unit 61398 is an elite People's Liberation Army cyberwar unit that operates from a Shanghai compound, where it's estimated hundreds of PLA hackers work day and night, sucking data from Western high-tech industries and political targets. According to Mandiant, the unit is tasked by the Chinese Communist Party's most elite leaders to steal technology for industries chosen for growth in the party's periodic five-year plans.

According to Mandiant, 61398 seeks broad swathes of intellectual property, business plans, pricing documents, and emails from targeted organizations' leadership.

And in 2013, [Mandiant reported](#) Nortel was one of 141 North American entities 61398 attacked. For Shields, 61398's reported tactics fit everything that he observed about the cluster of internet addresses in Shanghai.

STORY CONTINUES BELOW ADVERTISEMENT

Another fact that seems more than coincidental, Shields says, is that Huawei was founded in 1987 by former PLA engineer Ren Zhengfei. And the Chinese Communist Party's five-year plan for 1986 to 1990 was to "speed up the

construction of the energy, communications, telecommunications and raw materials industries.”

Equally damning, Shields says, is the intellectual property stolen from Nortel in 2004. The list of records, reviewed by Global News, includes strategy documents titled “Road-map values and challenges to Nortel,” and “Value Chain Dynamics & Industry Structure.”

And stolen R&D included documents with titles such as “Photonic Crystals and Large Scale Integration” and “Switching and Tuning Highly Integrated Optical Circuits” and “Speed Data Over Universal Mobile Telecommunications Service.”

These Nortel documents relate to its world-leading fibre optics equipment in 2004, and future innovations in 3G, 4G and 5G technology that enable incredibly detailed media to be sent worldwide via the internet.

“These were the crown jewels of Nortel R&D,” Shields said. “It was the future. And the only entity that could benefit from those kinds of documents being stolen, is a competitor.”

READ MORE: [Huawei still hopes to sell 5G equipment to Canada despite pressure from Five Eyes](#)

That’s why Shields says he cannot understand why Ottawa would even consider Huawei as a 5G network contender.

STORY CONTINUES BELOW ADVERTISEMENT

“I never said Huawei stole our technology, I said the Chinese government stole Nortel’s technology,” he said.

“I know what I found, and I know the discussions I had with certain people. Don’t Canadians deserve to know, too?”

TWEET THIS

But Huawei has repeatedly denied any wrongdoing in the Nortel case. Responding to questions from Global News, a spokesman pointed to a 2014 University of Ottawa study, which found that poor management decisions led to Nortel’s downfall, not hacking.

“There have been suggestions in the media that Chinese or other foreign espionage agents penetrated internal Nortel networks and computers in order to acquire technology and strategic information and that such action contributed to the downfall of the company,” the University of Ottawa study says. “We found no evidence of this and consider it unlikely.”

In an interview, Peter MacKinnon, one of the study authors, said any hacking of Nortel was inconsequential in comparison to Nortel management errors.

“There is no way the company could blame its failure on hacking by any party,” MacKinnon said. “It’s a timing thing, by saying Huawei has risen while Nortel went down. But that is not a direct relationship. There is no causation there.”

For his part, Ren Zhengfei — who did not respond to an interview request for this story — says Huawei did not steal Nortel’s IP, and it was the 2000 market crash that ultimately did in Nortel.

STORY CONTINUES BELOW ADVERTISEMENT

READ MORE: [Bell, Telus reveal 5G deals with European firms in major blow to Huawei](#)

“Unfortunately, Nortel collapsed because the IT bubble burst,” a [transcript](#) of Ren’s 2019 interview with the Globe and Mail posted on Huawei’s website says.

And there is ample evidence of bad management at Nortel and lingering wounds from the 2000 crash, most notably in the accounting scandals that ultimately led to RCMP charges against Frank Dunn and two other Nortel managers. Dunn and the other two were eventually acquitted. Dunn could not be reached for comment on this story.

Astronomically low bids

Commodore Patrick Tyrrell, a retired military intelligence officer and the U.K.’s first cyberwarfare chief, says the Chinese Communist Party has mastered the art of waging war in cyberspace. Cyberwar strategy, Tyrrell says, fits the methods taught by ancient Chinese military general Sun Tzu, who said that territory can be seized without bloodshed, if the attacker patiently exploits an opponent’s vulnerabilities.

Huawei’s incredible growth in 20 years under the Chinese Communist Party and guided by PLA engineer Ren Zhengfei has the look of a Sun Tzu strategy, Tyrrell said.

“The first thing is, nobody does anything in China without the approval of the Chinese Communist Party. And if you look at Ren Zhengfei and the development of Huawei, it is quite clear this is a person with a military vision,” Tyrrell said. “If you have good intelligence, any military man will want to know the vulnerabilities in a particular company.”

STORY CONTINUES BELOW ADVERTISEMENT

“And over the years Huawei was undoubtedly successful in being able to take over Nortel.”

[TWEET THIS](#)

In Nortel’s case, Tyrrell says Huawei realized the Canadian giant’s Achilles Heel was its huge and costly inventory of technology assets. Generally, Chinese state-champions can stay afloat as long as Beijing decides to fund them. So they can afford to burn money and undercut competitors in strategic areas, Tyrrell says. But Western companies die when costs rise above sales. By 2008 Nortel was in trouble and it desperately needed to land the 3G Universal Mobile Telecommunications wireless contract offered in Canada by Telus Corp. and BCE Inc.

1:48

United Kingdom's first cyberwarfare chief says Canadi...

United Kingdom's first cyberwarfare chief says Canadian sovereignty riding on Huawei 5G decision – Aug 25, 2020

But Huawei won the deal by underbidding Nortel an estimated 40 per cent. Telus and BCE did not respond to questions from Global News for this story.

"You go in and make sure Nortel can't get the money to keep this behemoth afloat," Tyrrell said. "Suddenly it collapses, and low and behold you can go pick the bits you want."

STORY CONTINUES BELOW ADVERTISEMENT

A similar case occurred in 2005, Tyrrell says, when Huawei beat out Nortel and U.K. telecom Marconi to construct part of a \$17-billion fibre optic network for British Telecom (BT).

Huawei underbid the next lowest bidder Marconi by \$US 1 billion — about a 40 per cent discount — Tyrrell said. And one year later, Marconi collapsed.

"Suddenly this company comes in with this astronomically low bid. And they would also have known if a company needs to get this bid to literally survive," Tyrrell said. "That is a powerful piece of information."

READ MORE: [A look at Huawei's involvement in telecoms networks around the world](#)

BT did not respond to questions for this story. But its network deal with Huawei was criticized in a 2013 U.K. parliament intelligence and security committee report.

The report summarized allegations made widely against Huawei by companies such as Cisco and Motorola.

"It is alleged that Huawei was able to win many contracts by stealing technology from its rivals and then undercutting them on price," the report says. "But Huawei strenuously denies that it has direct links with the Chinese Government or military, claiming that it receives no financial support from the Chinese Government."

STORY CONTINUES BELOW ADVERTISEMENT

In response to questions about Huawei's funding, a spokesman sent Global News a YouTube [video produced by Huawei](#) which says the company receives a minimal amount of R&D funding from the Chinese government.

"Huawei is repeatedly accused of being owned or funded by the Chinese government," the linked video claims. "Truth is, Huawei is a private company and is 100 per cent employee-owned."

On the BT deal, by 2006, security concerns were discovered on equipment installed by Huawei, the report says. And in 2008 British intelligence warned "theoretically, the Chinese State may be able to exploit any vulnerabilities in Huawei's equipment in order to gain some access to the BT network."

Finally, in 2011, the U.K. government briefed Huawei in China "on issues discovered with its equipment" the report says, and Huawei promised to address equipment problems.

Huawei did not respond to a question from Global News, regarding the alleged equipment problems.

Brian Shields and Patrick Tyrrell believe these sorts of network vulnerabilities cannot be mitigated because the Chinese Communist Party ultimately controls Chinese tech companies.

And Tyrrell says nothing less than Canada's sovereignty is riding on Ottawa's pending 5G decision.

READ MORE: [Most Canadians are wary of Huawei's role in 5G. Here's why some firms still favour it](#)

STORY CONTINUES BELOW ADVERTISEMENT

"Whatever happens on your information grid is known in Beijing before it is known in Ottawa in a Huawei 5G network," Tyrrell said.

"What that means is the Canadian government doesn't have control of its destiny."

TWEET THIS

The U.S. government has come to a similar conclusion.

This year former U.S. national security adviser H.R. McMaster asserted that in 2019, "a series of investigations revealed incontrovertible evidence of the grave national-security danger associated with a wide array of Huawei's telecommunications equipment."

"Many Huawei workers are simultaneously employed by China's Ministry of State Security and the intelligence arm of the People's Liberation Army," McMaster wrote in The Atlantic. "Huawei technicians have used intercepted cell data to help autocratic leaders in Africa spy on, locate, and silence political opponents."

© 2020 Global News, a division of Corus Entertainment Inc.

 JOURNALISTIC STANDARDS

 REPORT AN ERROR

Huawei 5G

Huawei Canada 5G

Will Canada ban Huawei

Canada United Front

+5


COMMENTS

SPONSORED STORIES

You could start your day with savings
Switch today!
Progressive | Sponsored

Warhammer® 40,000: Dawn Of War® – Winter Assault
We offer thousands of games on the Humble Store with sales happening every day.
Humblebundle US | Sponsored

White Diamond Accent 14K Rose Gold Over Sterling Silver Ring
Jewelry Television | Sponsored



Samsung 3.8V 2200mAh Replacement Battery
This Samsung 3.8V 2200mAh replacement battery is a great fit for your Samsung cell phone. - Walmart,...
Batteries Plus | Sponsored

Perfect Shave Without irritation or cuts! The Trimmer Every Man Needs!
Xisitors | Sponsored

Experience the Ultimate Comfort
Over 45,000 ⭐⭐⭐⭐⭐ Reviews
Warmies | Sponsored



Severance for making a mistake? A gas station employee's 69-cent-per-gallon lesson | Globalnews.ca



Dangerous driving is on the rise in Ontario, CAA survey suggests | Globalnews.ca



'Absolutely disgusting': Controversial float in Sundre, Alta. rodeo parade causes...

Sponsored 4/5

'Duck Dynasty' stars go treasure hunting on new show

New York Post

Read More >



West watches closely as Putin issues chilling message about 'purge' of society | Watch News...



Russia-Ukraine conflict: Trudeau says Canada doesn't have oil and gas infrastructure to replace...



[Gallery] This Is Real, And It Happens Every Day In Singapore
DailyChoices | Sponsored

Gallery 16" Watch
Citizen Watch | Sponsored

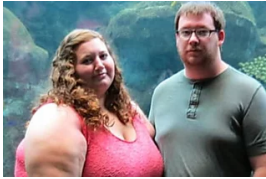
Rayovac 6V 6 Volt Lantern Heavy Duty Spring Top Battery
Batteries Plus | Sponsored



RCMP seize suitcase full of cash at Winnipeg airport - Winnipeg | Globalnews.ca



'A punch in the gut': Vancouver cyclist charged thousands to repair vehicle that hit him l...



[Gallery] A Couple Changes Lifestyle Completely - This is...
HistoryA2Z | Sponsored



New: OSHA Top 10 Violations for 2021
Grainger | Sponsored



Before you renew Amazon Prime, read this
Capital One Shopping | Sponsored

FLYERS [MORE WEEKLY FLYERS >](#)



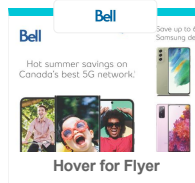
Hover for Flyer



Hover for Flyer



Hover for Flyer



Hover for Flyer



[About](#) [Principles & Practices](#) [Branded Content](#) [Contact us](#) [RSS](#) [Newsletters](#) [Notifications](#) [Smart home](#) [Advertisers Election Registry](#)

©2022 Global News, a division of Corus Entertainment Inc. Corus News. All rights reserved. Powered by [WordPress VIP](#)

[Privacy Policy](#) / [Copyright](#) / [Terms of Use](#) / [Advertise](#) / [Advertising Standards Terms](#) / [Corus Entertainment](#)