Whistler resort municipality hit by new ransomware operation

bleepingcomputer.com/news/security/whistler-resort-municipality-hit-by-new-ransomware-operation/

Lawrence Abrams

By
Lawrence Abrams

- April 29, 2021
- 12:01 PM
- 1

The Whistler municipality in British Columbia, Canada, has suffered a cyberattack at the hands of a new ransomware operation.

The Resort Municipality of Whistler (RMOW) is a resort community with approximately 12,000 residents and over three million visitors annually.

The ski resort area is also known for its ski resort area, Whistler Blackcomb, which hosted the alpine skiing events in the 2010 Winter Olympics.

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

Whistler hit by new ransomware gang

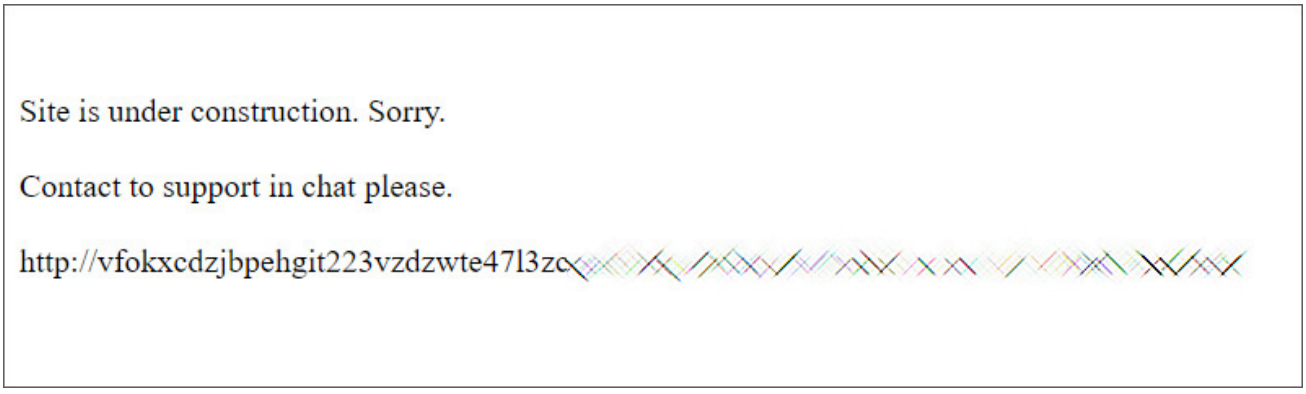
Yesterday, the Resort Municipality of Whistler (RMOW) suffered a ransomware attack that forced them to shut down their network, website, email, and phone systems.

Due to this disruption, all online activities and certain in-person municipality activities have been suspended.

"April 28, 2021: Whistler, B.C. – The Resort Municipality of Whistler (RMOW) has temporarily suspended all online and some in-person services as a precautionary measure due to a cyber security incident."

"This means RMOW email, phones, network services and website are currently unavailable. In-person service at municipal hall has also been temporarily suspended. We apologize for this inconvenience and will provide an update when we are able to return those services," the Whistler.ca website previously announced," said a statement on the Whistler.ca website.

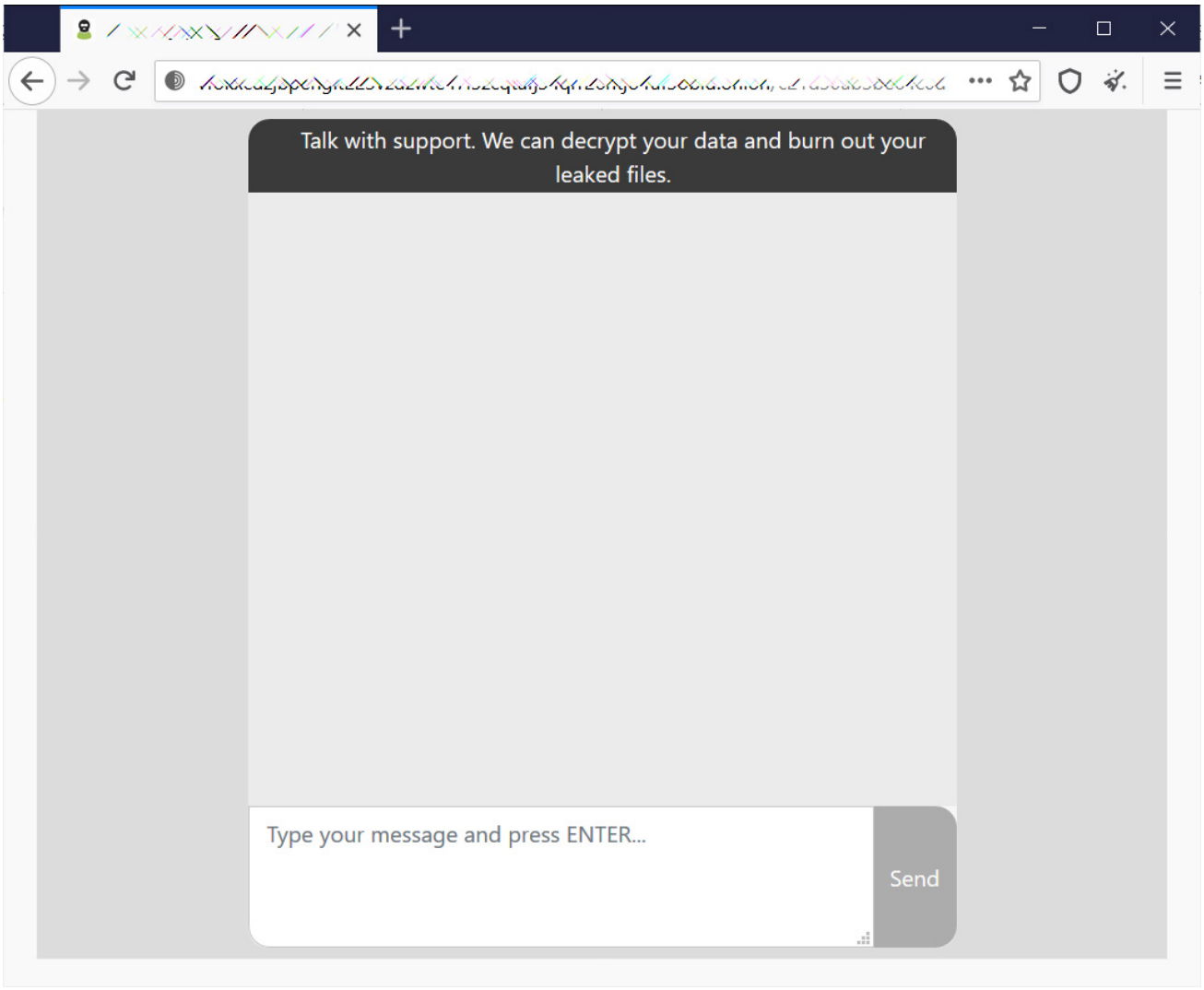
While the attack was ongoing, the Whistler.ca website was hacked to display a message stating that the site was under construction and that visitors should contact support at an included Tor dark web URL.



Message left by attackers on Whistler.ca site
Source: BleepingComputer

This URL leads to a dark web chat site used by the attackers to negotiate a ransom payment with Whistler and to prevent the leaking of stolen files.

When visiting the site, a chat screen is displayed with a message, "Talk with support. We can decrypt your data and burn out your leaked files," as shown below.



Dark web ransomware negotiation site

Source: BleepingComputer

This message indicates that RMOW's network has been encrypted and that unencrypted files were stolen during the attack, which has become common in ransomware attacks.

The website is one that neither BleepingComputer nor ransomware researchers we spoke to have seen before, indicating it is likely a new ransomware operation.

RMOW states they are currently working with cybersecurity experts and the Royal Canadian Mounted Police (RCMP) in response to the attack.

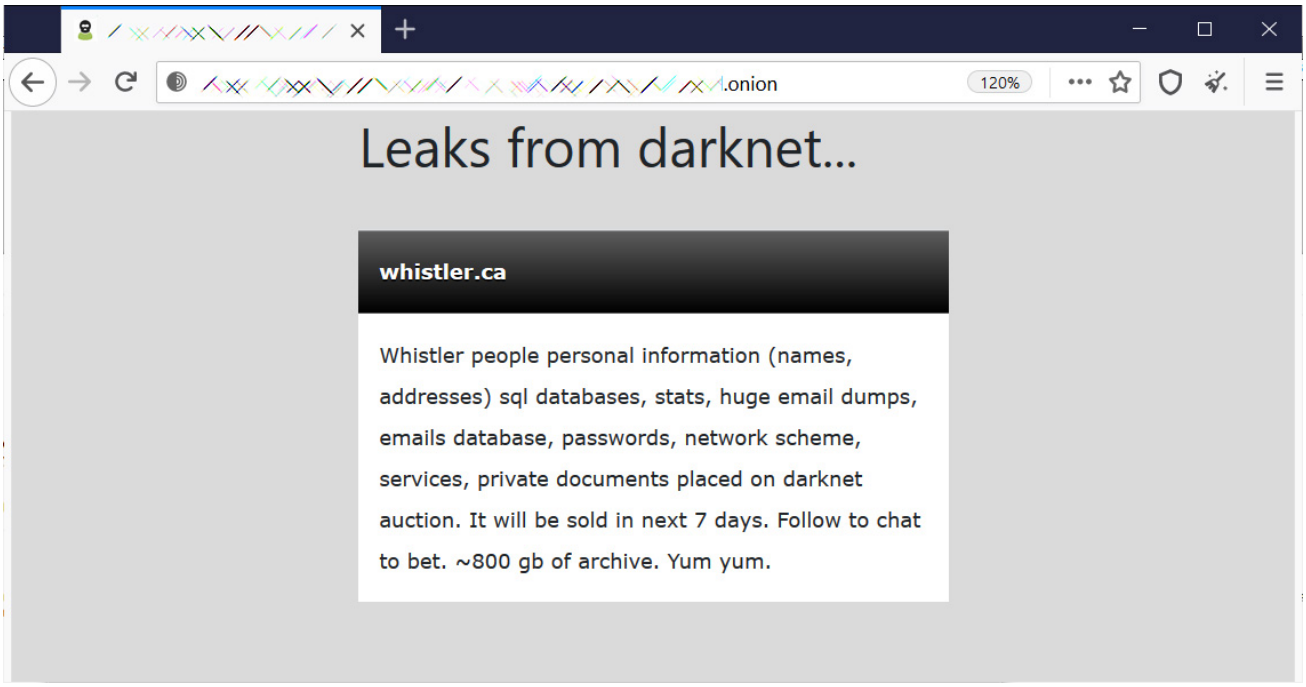
The municipality also warned the public to be suspicious of any phone calls or emails stating they are from RMOW.

> "In the meantime, the public should be vigilant about phone calls or emails that appear to be originating from the RMOW. The RMOW does not ask for private personal information by phone or email." - Resort Municipality of Whistler (RMOW).

BleepingComputer attempted to contact Whistler with further questions but was unable to reach anyone.

Update 4/30/21: The ransomware gang claims to have stolen 800 GB of data during their attack on Whistler, which they say will be auctioned if a ransom is not paid.

> "Whistler people personal information (names, addresses) sql databases, stats, huge email dumps, emails database, passwords, network scheme, services, private documents placed on darknet auction. It will be sold in next 7 days. Follow to chat to bet. ~800 gb of archive. Yum yum."



Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

- British Columbia
- Canada
- Cyberattack
- Hacked
- Ransomware
- Skiing
- Whistler

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

anthonymaw - 1 year ago

-
-

Ransomeware seems to be of the few actual uses of Bitcoin these days !!!

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: