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.

Hackers had 'deep' access to Whistler systems, docs show

RANSOMWARE ATTACK MAY REQUIRE A COMPLETE REBUILD OF RMOW NETWORK

BY **BRADEN DUPUIS**

SOME SERVICES at the Resort Municipality of Whistler (RMOW) are beginning to come back online following a ransomware attack made public on April 27, but full recovery could take months, as documents posted to the dark web indicate the criminals had deep access to municipal systems.

Over the course of a week, the criminals posted various password-protected links ending in the names of different RMOW employees (which they claim to have sold on the dark web), followed by an excel spreadsheet that included sensitive system administration info, and ultimately a data dump of "important" passwords.

"Primarily they seem to be looking to demonstrate to the municipality that they did indeed have deep access to their systems," said Brett Callow, threat analyst with Emsisoft, a cyber security company with a particular expertise in ransomware.

"Gathering up the various credentials needed to access various parts of the network would obviously require them to access those parts of the network."

UNDER CONSTRUCTION **A message posted to the dark web by cyber criminals on April 30 claiming to have access to about 800 gigabytes of Resort Municipality of Whistler data. Documents leaked in the following days appear to back up the claim.**

IMAGE BY PIQUE STAFF

Having gained such pervasive access to the RMOW's systems, the problem will be "very hard to remediate," Callow added, and the RMOW may be looking at a complete rebuild of its network.

"That is absolutely the best solution—you rebuild your network," he said. "If you don't do that there is always a risk that you'll miss a backdoor they've created."

That process can cost millions of dollars and take months to complete, Callow said, noting that, according to statistics, the average ransomware incident costs $8.1 million and takes 287 days to recover from.

With an investigation ongoing, it's still unclear how the criminals accessed the RMOW's systems, but it's possible they exploited a "zero-day" vulnerability (an exploit previously unknown to the developer) found in SonicWall VPN, a service used by the RMOW.

Cyber security experts from a firm called FireEye documented the vulnerability in a blog post on April 29, noting that a patch was released to fix the problem in February.

Asked about the documents posted to the dark web, and if the RMOW installed the SonicWall patch released in February, a spokesperson said the municipality cannot comment on specific details of the investigation while it is still underway.

"We obviously can't say that that was the entry point, but it's certainly possible," Callow said.

"We can certainly say that ransomware groups do exploit vulnerabilities in VPN, including a zero-day that existed in SonicWall's VPN, and that the municipality seem to have used SonicWall."

"Primarily they seem to be looking to demonstrate to the municipality that they did indeed have deep access to their systems."

- BRETT CALLOW

The RMOW said in a May 11 update that its investigation "has not found evidence" that public or customer info has been compromised, and that it will reach out to affected individuals if that changes.

The leaked documents *Pique* viewed contained no definitive proof to the contrary.

Asked for his opinion, Callow cast doubt on the RMOW's reassurances.

"The question is: if they were able to gain access to the network and obtain credentials that would have enabled them to access other areas of the network, why didn't they and why didn't they take data?" he said.

As for what type of market there would be for the RMOW's data, "it would depend what the data is," Callow said.

"Information about individuals could be used for identity theft. Information about other organizations can be used to spear-phish them (phishing attempts targeted at individuals)," he said.

"So there is a market, but how much of a market I really can't say."

NO ESTIMATE FOR FULL RETURN OF SERVICES

After learning of the attack on April 27, the RMOW took all of its services offline as a precautionary measure.

The municipality is also working with the RCMP and Office of the Information and Privacy Commissioner for B.C. on the matter.

In a release issued May 11, the RMOW noted there is still no estimate for when all services will return to normal, but "a limited number of critical systems" are expected to start to return within two weeks.

"We apologize for this inconvenience to our community members and greatly appreciate everyone's patience as we work diligently to bring these services back

online," said chief administrative officer Virginia Cullen in the release. "The safety and security of the RMOW's systems is our highest priority to protect the information that we maintain for our employees and community members. It is a painstaking and lengthy process to make sure that our systems are fully secured before we bring them back online. We are working with cyber security experts to further strengthen our security safeguards in the ever-evolving cyber security landscape."

Once systems are back online, the RMOW will work through applications and requests in the order they were received, the release said, adding that alternate service delivery methods have been put in place where possible.

In-person service at municipal hall is still suspended, but all departments can be reached (find specific contact info, as well as RMOW updates and a FAQ at whistler.ca).

A call centre is available for the general public at 604-932-5535 from 8 a.m. to 4:30 p.m., Monday to Friday.

Though council meetings scheduled for May 4 were cancelled following the attack, a special council meeting was held May 11 to adopt an amendment to the five-year financial plan and the RMOW's 2021 tax bylaws (both were given first three readings on April 20).

A closed meeting was also held on May 11, to "discuss the security of the property of the municipality, the receipt of advice that is subject to solicitor-client privilege, and discussions regarding the provision of a municipal service, and discussions with municipal officers and employees respecting municipal objectives, measures and progress reports for the purposes of preparing an annual report."

The next public meeting is scheduled for May 18.

The property tax deadline for 2021 is currently Friday, July 2, and like last year, penalties will not be charged on late payments until Friday, October 1 due to COVID-19. Staff are recommending that this year's deadline be changed to July 31. Council will consider the recommendation on May 18th.

Individual property tax statements outline all the ways to pay property taxes (in-person, mail-in cheque, online banking, credit card), and those payment methods will be available any time after tax notices are mailed (mail-in and online banking are currently available.)

The RMOW is also reminding the public that it does not contact individuals by phone or email to request personal information.

"Additionally, the RMOW advises community members to continue to exercise a high level of awareness about protecting their sensitive personal information and to practice good password hygiene such as regularly changing passwords to all online accounts and not re-using the same password for multiple accounts," the release said.

A GROWING PROBLEM

Ransomware attacks have been increasing in frequency as of late, with cyber criminals carrying out operations on higher-profile targets.

Last weekend, a ransomware attack on the Colonial Pipeline—a critical U.S. pipeline that supplies about 45 per cent of the fuel used along the East Coast—prompted President Joe Biden to issue emergency legislation, while the City of Tulsa, Okla., also shut down services after a ransomware attack on May 7.

"The targeted organizations have gotten bigger and bigger," Callow said. "Ransomware used to be the bane of mainly small businesses, but that's no longer the case, and demands have risen considerably as well."

The average demand has gone from about $5,000 in 2018 to about $200,000 today, Callow said. And while there are no hard stats showing how many companies choose to pay the ransom, "about 30 per cent would seem to be a reasonable midpoint," he added.

DarkSide, for instance—the group claiming responsibility for the Colonial Pipeline hack—has released data stolen from 83 organizations, "and they have carried out at least 113 attacks that we know about," he said.

Cyber insurance—which the RMOW has—could potentially cover everything from the amount of the ransom demand that is paid to the cost of rebuilding the network (minus the deductible).

But it can also be a double-edged sword, Callow said.

"Some people believe that insured organizations may be more inclined to pay ransoms, because the money isn't coming from their own pocket, which of course pushes more money into the whole cyber crime ecosystem, which incentivizes more cyber crime," he said.

"The more profitable it is, the more attacks there will be." ■

"The safety and security of the RMOW's systems is our highest priority to protect the information that we maintain for our employees and community members."

- VIRGINA CULLEN