Headwaters confirms unauthorized access in suspicious email activity

Written By **Paula Brown**

Local Journalism Initiative Reporter

Headwaters Health Care Centre (HHCC) has confirmed the cause of suspicious email activity that led to the shutdown of their internal systems, and the closure of the COVID-19 assessment centre.

On Friday (Nov. 26) the local hospital released an updated notice on their website noting their system had been subjected to ?unauthorized access? resulting in a number of spam emails.

?We are working with cybersecurity experts who will help us safely restore our IT services and investigate what happened and whether any sensitive data was exposed,? said the hospital.

The hospital's information technology system noticed suspicious email activity the day previous (Nov. 25), with a number of spam emails sent from the CEO Kim Delahunt's email account to hundreds of contacts, primarily staff members of the hospital. As a result of the security breach, the hospital shut down their internal system as well as access to the internet and key external partners.

?As an organization we take cybersecurity very seriously and have numerous measures in place to protect our data,? wrote the hospital in a Nov. 25 notice. ?Thankfully, our team noticed unusual activity quickly and [acted] immediately.?

The suspicious email, repeatedly sent from Delahunt's email address on Nov. 25 was from Lorenz ransomware, stating all the hospitals files across its entire system has been encrypted, which includes private medical data.

The email continues, ?We will publish all the contents of your company on our site includes all your confidential medical history, employers information, documentation, catalogs, reports, configs, mail, database's, invoice's, signature's etc.?

The email says to prevent the publishing of this data, visit its website and follow its instructions which entails downloading a TOR browser and paying money to recover the files.

Lorenz is a new variant of Sz40 ransomware, which is designed to encrypt data and demand ransom for decryption. This means Lorenz renders affected files inaccessible and then asks for payment to regain access.

Meanwhile, the shutdown of Headwaters Health Care Centre's systems isn't impacting patient care, as the local hospital said they have ?robust processes' in place.

Scheduled surgeries or procedures have not been impacted at the time of print as well, and the emergency department remains open 24/7.

With the COVID-19 assessment centre temporarily closed, alternative testing locations in Peel Region and in Wellington-Dufferin-Guelph have been given to residents.

At the time of print, there is no timeline for when the hospital expects to have their systems back up and running.

?This process will take some time. We are committed to being transparent and will notify individuals if we learn that personal information has been exposed,? said Headwaters.