In New York, the Carthage Area Hospital and the Clayton-Hepburn Medical Center were both compromised by the LockBit ransomware organization.

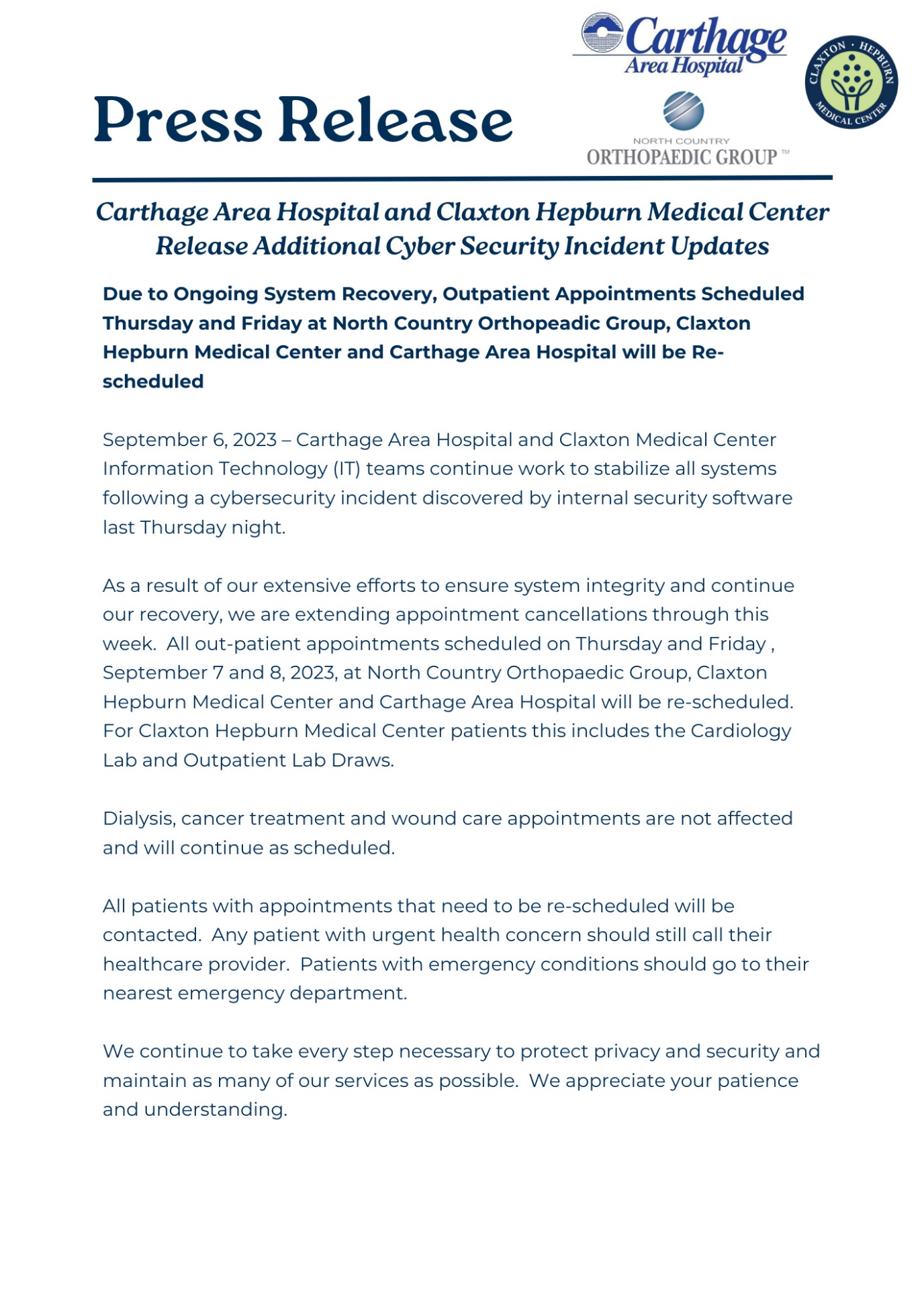


<https://www.google.com/url?sa=i&url=https%3A%2F%2Fblog.criminalip.io%2F2022%2F09%2F23%2Flockbit-3-0-ransomware%2F&psig=AOvVaw0_WaxFGWlM-BMKaKQgiUj-&ust=1694843902469000&source=images&cd=vfe&opi=89978449&ved=0CBIQjhxqGAoTCKDZiNj3q4EDFQAAAAAdAAAAABCfAQ>

The Carthage Area Hospital and Claxton-Hepburn Medical Center are two significant hospitals that the Lockbit ransomware gang claims to have been compromised. In upstate New York, the two hospitals provide care for hundreds of thousands of patients.

The two hospitals have been suffering greatly as a result of the hack that happened at the end of August in recent weeks. On September 2, the phone systems were brought back online, but various other services were still affected by the intrusions. The Carthage and Claxton emergency rooms have been diverted, the patients have been moved to other local hospitals, and the majority of the appointments have been rescheduled as a precaution.

“All patients with appointments that need to be rescheduled will be contacted. Any patient with urgent health concerns should still call their healthcare provider. Patients with emergency conditions should go to their nearest emergency department,” states the administration oat the hospital.



<https://www.facebook.com/photo.php?fbid=757814679687795&set=a.385955390207061&type=3&ref=embed_post>

The two hospitals are currently battling cyberattack recovery.

Along with the New York State Department of Health and the Division of Homeland Security and Emergency Services, the FBI opened an investigation into the event.

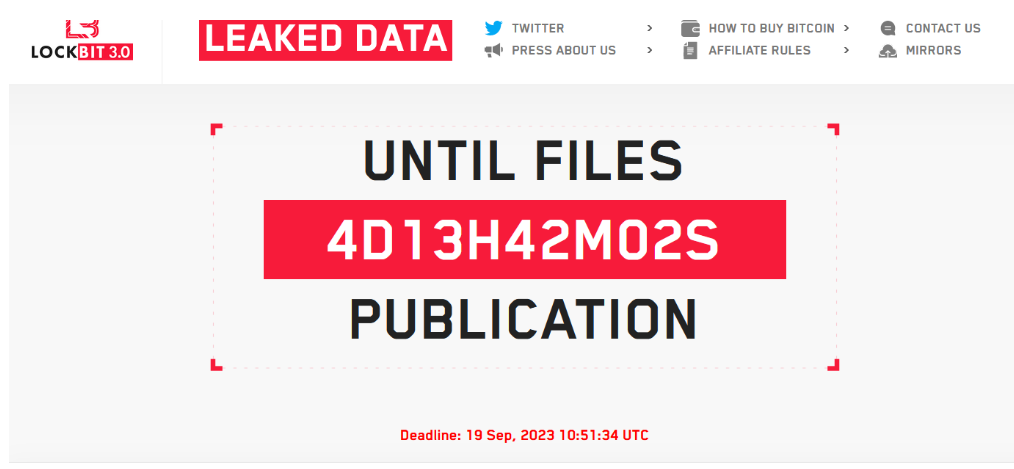
The Claxton-Hepburn Medical Center said this week that it would keep canceling outpatient appointments at clinics and doctor's offices this week due to the serious nature of the situation there, according to The Record Media.



<https://www.facebook.com/ClaxtonHepburn/posts/823893659743045?ref=embed_post>

The hospitals have now been included to the LockBit ransomware gang's Tor leak site. If the victims don't pay the ransom, the gang allegedly plans to disclose the allegedly stolen material by September 19, 2023.

The gang has not yet made any samples of the allegedly stolen material public as evidence of the attack.



<https://i0.wp.com/securityaffairs.com/wp-content/uploads/2023/09/image-23.png?ssl=1>

The Lockbit gang and its associates have attacked hospitals before. The LockBit ransomware group officially apologized for the attack on the Hospital for Sick Children (SickKids) in January and provided the hospital with a free decryptor.

It is well known that the organisation forbids its affiliates from striking healthcare institutions. Its policy prohibits encrypting networks at companies where a breach could result in fatalities.

The gang claimed that one of its associates attacked SickKids in violation of the organization's guidelines, leading to the affiliate's blocking.

Other healthcare institutions have also been targeted by members of the Lockbit gang in the past; in early December 2022, a cyberattack on the Hospital Centre of Versailles was blamed on the gang. The cyberattack forced the Hospital Centre of Versailles, which houses the Despagne Retirement Home, Andre-Mignot Hospital, and Richaud Hospital, to suspend operations and move some patients.

The Center Hospitalier Sud Francilien (CHSF), a hospital southeast of Paris, was attacked by the gang in August. The incident forced the hospital to refer patients to other facilities and hampered the emergency services and procedures. Threat actors, according to local media, demand a $10 million ransom in exchange for the decryption key needed to restore encrypted data.