CYBERMINUTE

Alberta Cybersecurity Insights

TLP: WHITE

LockBit exfiltrates data in cyber-attack targeting London Drugs

On April 28th, 2024, following the detection of malicious activity within its network, London Drugs was prompted to temporarily cease operations and close stores to contain the incident. Pharmacists were placed on standby to deliver any urgent care to customers who required it. A third-party cybersecurity team was also enlisted to help remediate any impact and conduct a forensic investigation, which discovered the company had been the victim of a ransomware attack.

A period of gradually re-opening stores began on May 4th, with the last remaining stores returning to normal business operations as of May 9th, marking a total of 11 days of downtime for some stores. Their main website has also been brought back online, although this took significantly longer, with BleepingComputer reporting that it was still down as of May 21st.

The LockBit ransomware gang claimed the compromise on May 21st, posting London Drugs as a victim on their Data Leak Site (DLS) and setting a 48-hour deadline to pay a $25 million ransom. Payments are typically demanded by ransomware gangs to supposedly secure assurance that all stolen data will be deleted once the ransom is received. Such claims are increasingly harder to believe and should not be trusted.

Posting victims on a DLS is a common technique used by ransomware groups to apply pressure to their targets. In this scenario, it was also highly likely in response to failed negotiations, with LockBit alleging that London Drugs were only willing to pay $8 million as ransom (although this claim should also not be trusted). London Drugs decided to not pay

the ransom, a decision that was met with high praise for their apparent willingness to resist the demands of cyber criminals.

London Drugs likely had some understanding of the nature of the stolen data, as evidenced by offering all employees two years of credit monitoring and identity theft protection services prior to the deadline. London Drugs claims this offer was made "out of an abundance of caution". LockBit delivered on their threat, and the stolen data—which did contain employee information—was leaked by them on May 23rd.

In the immediate aftermath of a cyberattack resulting in a data leak, any implicated individuals or organizations should reset account credentials and enable multi-factor authentication whenever possible. Any identified vulnerabilities that were exploited as part of the attack should also be patched or mitigated.

Organizations should also be on high alert for any follow-up attempts from either the same or other threat actors to conduct further compromise. Threat actors have leveraged breaches in the past as context for phishing attacks, often impersonating some sort of system recovery function or IT support team.

Click Here to Read More!

Cybersecurity Incident in British Columbia

Through late April to early May 2024, the Government of British Columbia (BC) identified a series of sophisticated cybersecurity incidents involving its networks. BC Premier David Eby announced there was a high degree of confidence a state or state-sponsored actor

Cybersecurity Threats on the Rise: Global Increase in DDoS Attacks

A Cloudflare report has shown a significant increase in Distributed Denial-of-Service (DDoS) attacks globally in 2024. In their first quarter report, Cloudflare has indicated their automated defences mitigated 4.5 million DDoS attacks during the first three months

attempted to breach government systems. In a separate announcement, Public Safety Minister and Solicitor General Mike Farnworth also stated that no ransom demand had been received. The Government of BC is working closely with the Canadian Centre for Cyber Security (CCCS) and other agencies to determine the extent of the incidents and implement additional measures to safeguard data and information systems.

At the time of writing, no evidence has been brought forward that would indicate that sensitive information had been compromised; however, the investigation is still ongoing. The government informed the Office of the Information and Privacy Commissioner about the cyberattack. The province's chief information officer was also informed and directed public service employees to change their passwords to ensure the security of the organization's email systems. The public was assured that the protection of data and networks is a top priority for the government.

This incident serves as a stark reminder of the growing seriousness of cybersecurity threats in the modern world. Organizations of all sizes must take proactive steps to protect their digital assets and reduce the risk of falling victim to cyberattacks. Maintaining healthy firewalls, keeping software and systems up-to-date, and ensuring sensitive data is encrypted are crucial elements to protecting an organization's cyber posture. However, they are not the only protections that can be put

of the year, representing a 50 per cent year-over-year increase. DNS-based DDoS attacks increased by 80 per cent year-over-year and remain the most prominent attack vector.

DDoS attacks can severely disrupt essential services and infrastructure. With these attacks being driven by political and economic motivations, their frequency is rising exponentially. As such, enhancing defences against these attacks is becoming ever more crucial to maintaining an organization's security, stability, and operationality.

Near the end of May 2024, the websites of two Canadian airports were allegedly the victim of DDoS attacks. In tandem, HackNeT and the People's CyberArmy, Russian cybercriminal groups, purportedly targeted Winnipeg's James Armstrong Richardson International Airport and Ottawa's Macdonald-Cartier International Airport websites, causing disruption in their abilities to provide services.

The tactics and technologies utilized by cyberattackers has been growing and evolving to match the rapid changes to the global digital landscape, underscoring the increasing importance of strong cybersecurity measures to protect against such attacks.

In the realm of cybersecurity, prevention is always better than the cure, and to aid with this the CCCS provides comprehensive guidelines to defend against DDoS attacks.

in place. Some strategies that can also help include people focused protections such as regular employee training on cybersecurity best practices and encouraging employees to set and maintain secure passwords. Administrative controls—such as conducting regular audits, employing the principle of least privilege, and implementing well defined access control measures can also help mitigate the impact of a cyberattack.

The BC government's experience underscores the importance of robust cybersecurity measures. By learning from this incident and implementing these strategies, organizations can better protect themselves against future cyber threats.

Click Here to Read More!

Emphasis is placed on the importance of implementing scalable and resilient multilayered DDoS protection solutions. This can include measures such as the installation of a Web Application Firewall to filter traffic based on general or organization specific rules, blackhole routing to turn away malicious traffic, and even something as simple as educating employees on recognizing and reporting indicators of a DDoS attack. Collectively, these strategies can contribute to enhancing an organization's resilience against DDoS attacks.

For organizations with limited cybersecurity resources, the CCCS recommends engaging with an external subject matter expert, such as a managed service provider, specializing in cybersecurity. These experts can provide knowledge, technological assistance, and monitoring services, allowing for DDoS attacks to be detected early, which is crucial in mitigating the scope of their attacks.

Click Here to Read More!