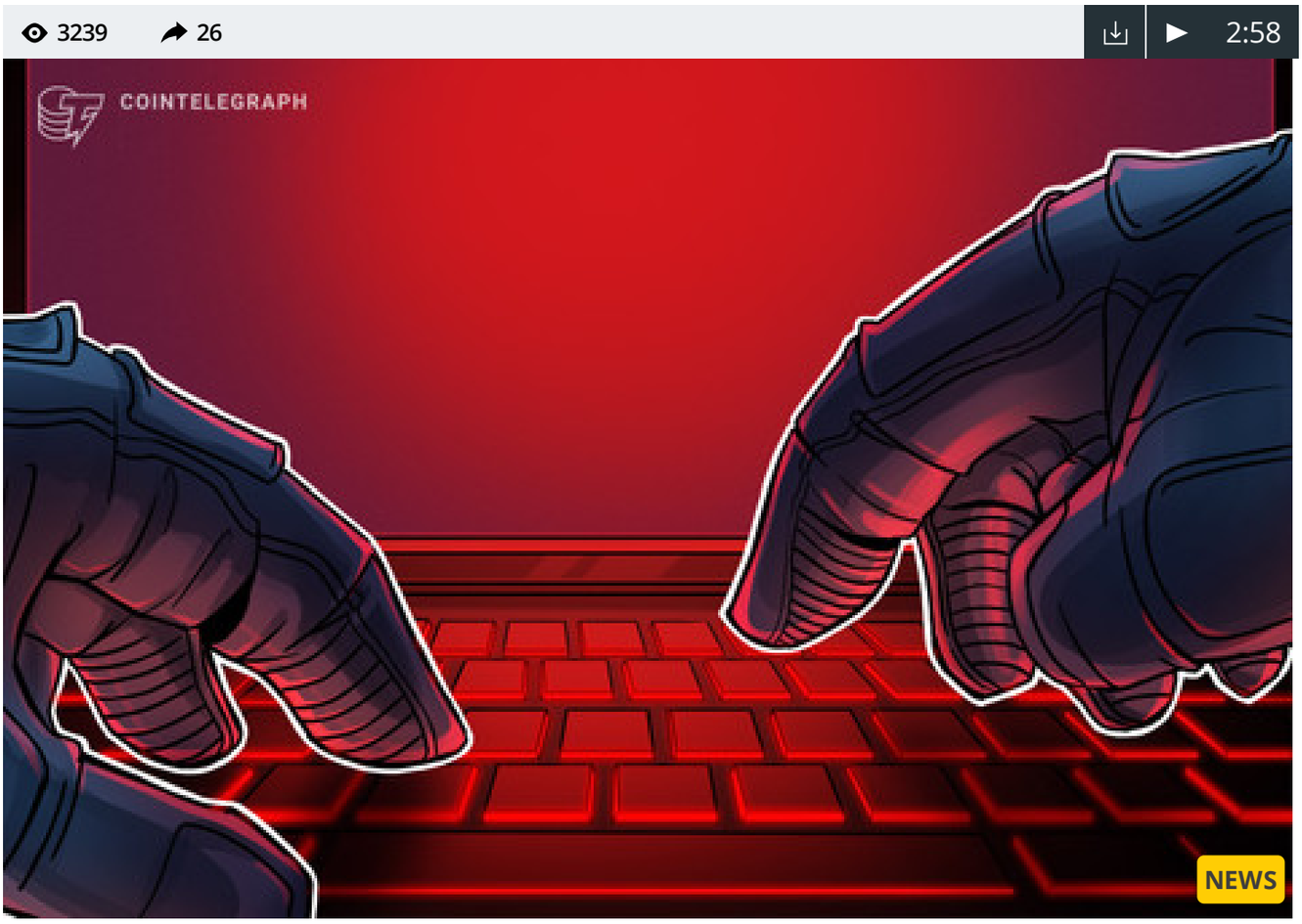
Australian Beverage Giant Faces Monero Ransom Demand of Nearly $1M

Ransomware gang REvil launched a second attack on an australian drink manufacturer.



Another ransomware attack has hit the Australia-based drinks manufacturer, Lion. This is the second attack on the company in less than one week. The cybercriminals behind the attack are threatening to double the ransom amount if Lion does not pay by the specified date. The currency of choice for the particular attack is Monero (XMR).

A report published by The Sydney Morning Herald on June 18 said that Lion's staff were informed that the attack had disrupted its IT infrastructure.

Initially, REvil has asked for a ransom of $800,000, to be paid in Monero. If Lion fails to send this amount before June 19, the group will double the ransom to $1,600,000.

Second ransomware attack in June against Lion

The first attack suffered by the Australian beverage giant was on June 9. Since then, the company has provided a number of updates on its official website, with the latest published on June 15.

Lion reportedly contacted a multinational professional services company, Accenture, seeking help in their recovery efforts.

Further details on the second attack were not disclosed as of press time. In a statement provided to news outlet iTWire, a spokeswoman of Lion commented:

> "We have confirmed that Lion was the victim of a cyber attack, caused by ransomware. We are not in a position to provide any further comment."

Modus operandi of REvil in its ransomware attacks

Speaking with Cointelegraph, Brett Callow, threat analyst and ransomware expert at malware lab, Emsisoft, said:

> "Ransomware groups frequently create backdoors which, unless remediated, provide them with access to the target network after the initial encryption event."

Callow also spoke about another recent case where REvil targeted an insurance company. The gang maintained post-attack access to the company's network and was able to monitor its response to the incident. They were even able to access emailed transcripts of telephone conversations.

Recommendations for Ransomware's victims

The data that was obtained during this continued period of access was subsequently posted online, along with an insinuation that the company was committing insurance fraud, Callow adds. He also provided some recommendations for ransomware victims:

> "Post-incident, companies need to rebuild their networks and infrastructure rather than simply decrypting their data or restoring it from backups. This is the only way to eliminate the possibility of a second attack."

Lion currently employs 7,000 workers. Its 2015 revenue was $ 5.6 million, according to figures shown by Wikipedia.

Recently, REvil launched another series of attacks targeting three companies in the U.S. and Canada. They have leaked data from two companies and threatened to disclose sensitive data from the third.

The companies are well-known Canadian accounting firm, Goodman Mintz LLP, licensed real estate broker Strategic Sites LLC, and ZEGG Hotels & Store, a duty-free store.