# Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack

By Lawrence Abrams

Published: 2021-01-26 · Archived: 2026-04-05 19:42:42 UTC

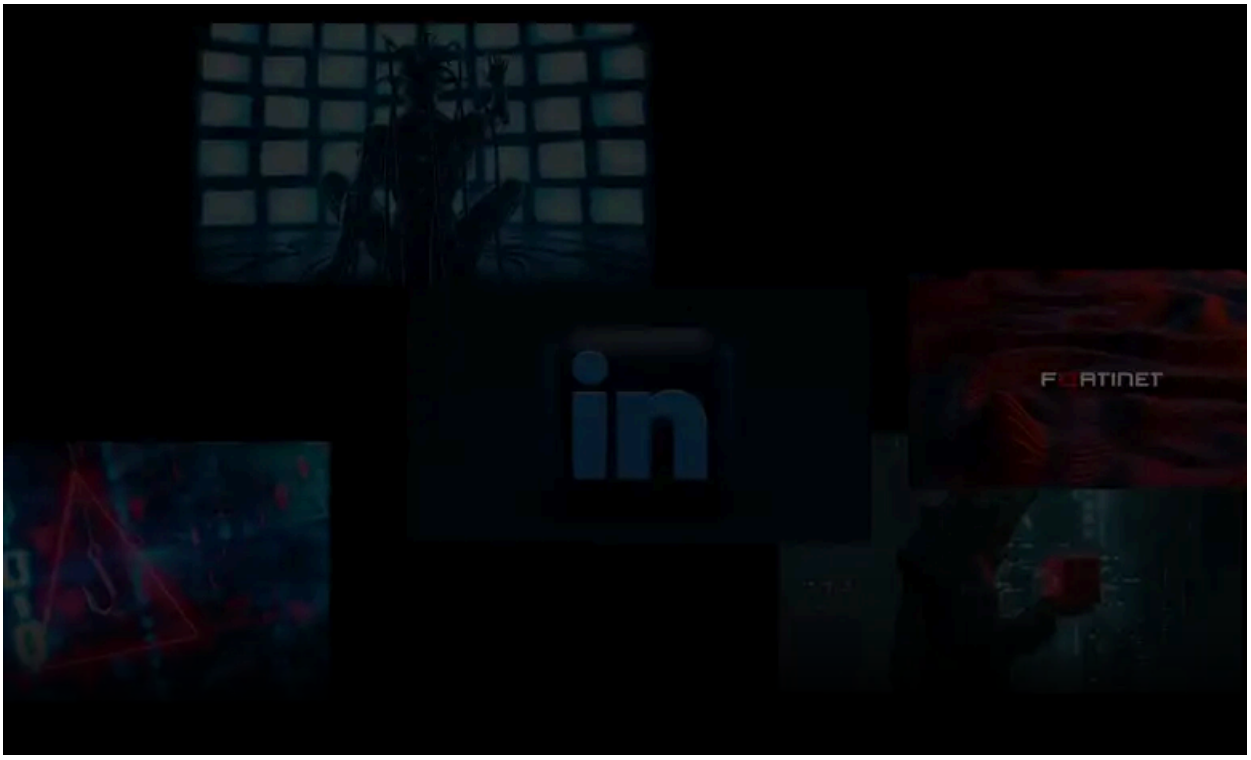
Massive pan-Asian retail chain operator Dairy Farm Group was attacked this month by the REvil ransomware operation. The attackers claim to have demanded a $30 million ransom.

The Dairy Farm Group operates over 10,000 outlets and has 230,000 employees throughout Asia. In 2019, the Dairy Farm Group's total annual sales exceeded $27 billion.

The group operates numerous grocery, convenience store, health and beauty, home furnishing, and restaurant brands in Asian markets, including Wellcome, Giant, Cold Storage, Hero, 7-Eleven, Rose Pharmacy, GNC, Mannings, Ikea, Maxims, and more.

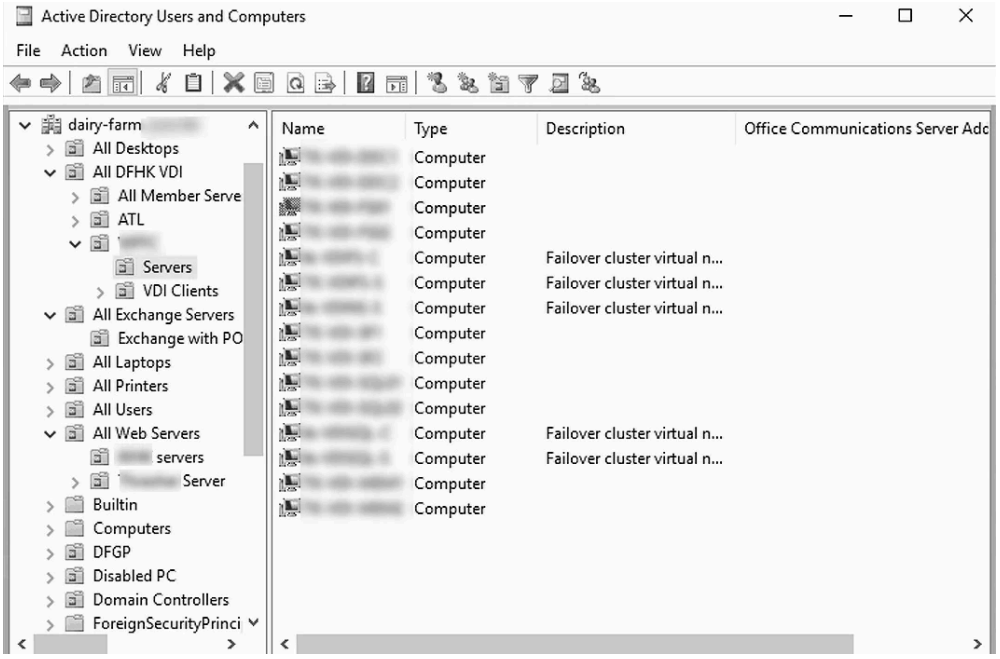
## REvil ransomware attack on Dairy Farm

This week, BleepingComputer was contacted by a threat actor who stated that the REvil ransomware group had compromised Dairy Farm Group's network and encrypted devices around January 14th, 2021.


FORTINET

BleepingComputer was told that the ransom demand is $30 million but has not independently confirmed this amount.

To prove they had access to the Dairy Farm network, the threat actor shared a screenshot of the Active Directory Users and Computers MMC.




**A leaked screenshot of the Dairy Farm Windows domain**

Redacted by BleepingComputer

The attackers claim to still have access to the network seven days after the attack, including full control over Dairy Farm's corporate email, which they state will be used for phishing attacks.

"They cannot shut down their network because their business will stop. There is a group of revil partners who are still attacking this company, there are more than 30k hosts there," the threat actor told BleepingComputer.

Dairy Farm confirmed to BleepingComputer that they suffered a cyberattack this month but said that less than 2 percent of all company devices were affected.

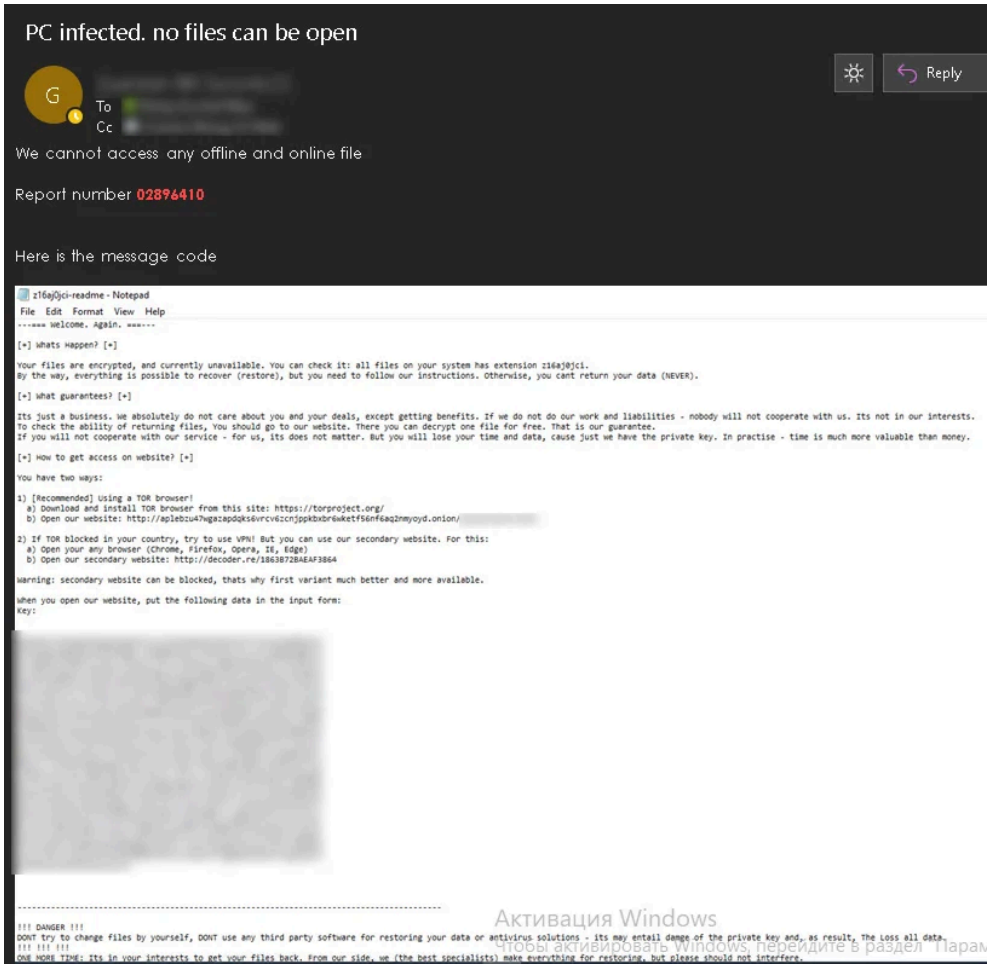
"At Dairy Farm , the protection of our systems is a top priority. On Thursday, we identified an incident that impacted less than 2 per cent of our business servers. These were taken offline and isolated. As an additional precaution, we initiated a full and thorough investigation with the support of an external security specialist, introduced additional security measures and strengthened our monitoring systems further."

"All of our stores are open, trading and serving our customers across all markets, and are only closed where there are COVID-19 restrictions put in place by national or local governments," Dairy Farm told BleepingComputer via email.

In a later phone conversation with Dairy Farm, BleepingComputer informed the company that the threat actors claim to still have access and are allegedly still downloading data from the network.

The company stated that they were not aware of any data being stolen during the attack, even though screenshots seen by BleepingComputer show that the threat actors continued to have access to email and computers after the attack.

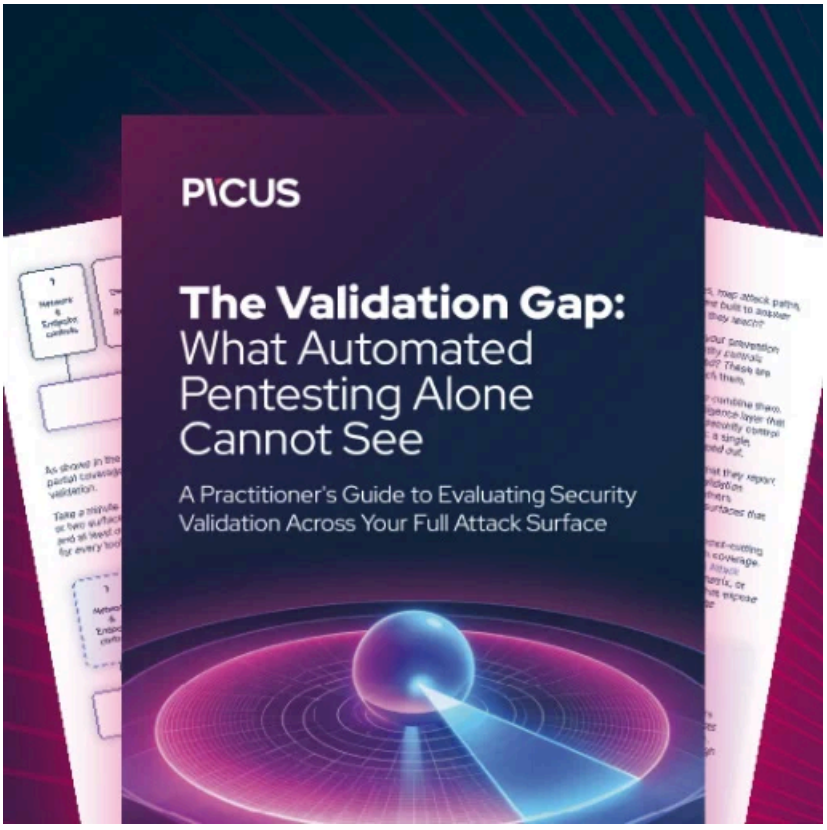
For example, below is a internal Dairy Farm email about the cyberattack leaked by the attackers.




**Internal email about the ransomware attack**
Redacted by BleepingComputer

As REvil is known for stealing data during an attack and then threatening to release it if a ransom is not paid, it would come as no surprise to find that stolen data was leaked at a later date.

Since the Christmas holidays, ransomware gangs appeared to be taking a break from large scale attacks. Unfortunately, this break is now over, and large enterprise attacks are increasing again, as was seen with the Dairy Farm attack and an ongoing global cyberattack against crane manufacturer Palfinger.




## Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revil-ransomware-attack/