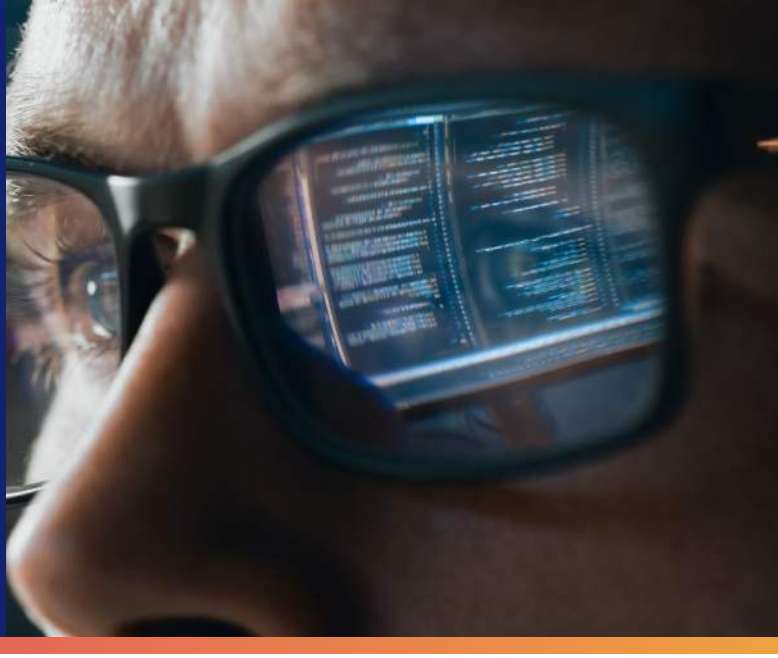
covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

CASE STUDY

A Ragnor Locker Ransomware Attack

When a major manufacturer of medical equipment suffered a ransomware attack in 2023, they were able to recover quickly thanks to a unique feature of their Veeam backups with Covenco.



Customer

An established medical equipment manufacturer based in the UK with global warehouse and office locations.

Industry

Medical, scientific, and veterinary equipment for clinical trials, diagnostics and critical care.

Operations

IT operations in the UK, with centralised data management across a global network.

Covenco Solutions

- Covenco Backup as a Service.
- Covenco Ransomware Recovery Service.
- Veeam Cloud Connect.
- Covenco Disaster Recovery Service.

The client was fortunate to have Veeam Cloud Connect and offsite backups with Covenco. They are now actively investigating the addition of immutable backups.

A rude awakening

On an August morning in 2023, the IT director of a major manufacturer of medical equipment in the UK was making his first cup of coffee and looking at the backup report from the previous night.

"I had just logged into our Veeam portal to check the status of the backups from the night before. I do it every morning, and it's always my priority," says the client, "but, I knew something wasn't right straight away."

Our client noticed that his nightly backups had not run. Not only that, but they had been stopped by someone with administrator privileges.

"I knew immediately that we had a major problem, likely due to a malicious attack, because the only person that could stop a backup was me," explained the client.

His natural reaction was to attempt to log into the system remotely. "My login failed, and I realised that the entire network was blocked to any user access. My heart sank as I realised, we were likely looking at a breach of our systems and a possible ransomware attack".

He immediately went to the office to access the client's data room. Once on-site, he could see ransomware demands and other evidence that indicated the company had indeed fallen foul of a ransomware attack.

"I took screen shots of everything pertinent," says the client. "I then disconnected every single bit of kit from the network and powered everything down. We were facing a crisis that would have massive implications for the business".

The sequence of events that he undertook is a play-book of an IT manager's action upon discovering a ransomware attack or other malicious breach of a company network. He had the presence of mind and the experience to know that you must act decisively - while remaining calm. He also had a detailed policy in place that would guide him in taking the proper steps, which included an immediate call to the backup team at Covenco.

Covenco's Backup-as-a-Service

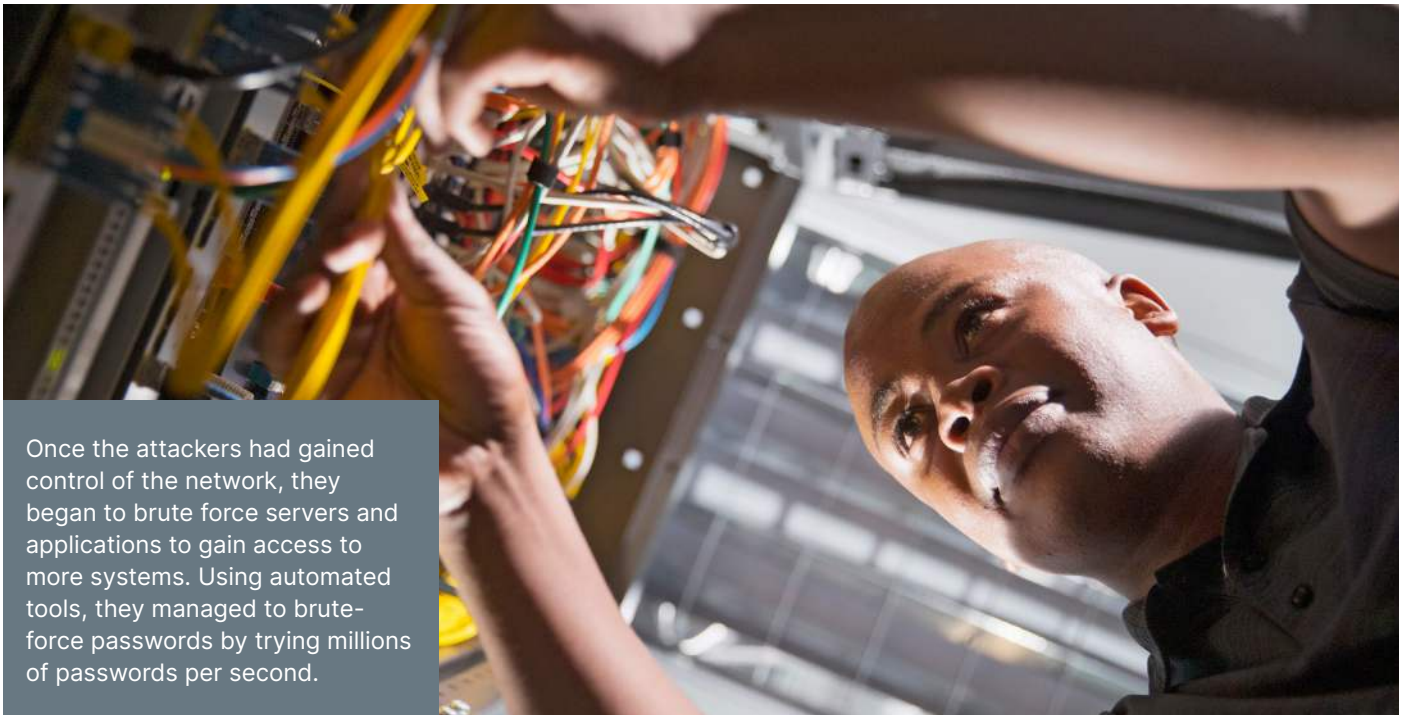
Since 2019, our client has used Veeam's Cloud Connect solution to backup data to Covenco's servers every night.

The Covenco Backup-as-a-Service gives our clients a monitored and reliable off-site backup solution that meets its critical data management requirements.

> "The Covenco backup service helps us maintain off-site data should a disaster strike. This might be anything from a fire at our offices to a power outage or - as in this case - a malicious attack."

"The service runs on the Veeam Cloud Connect solution and gives us a powerful set of tools and analytics that help us ensure that our data is

© Copyright Covenco Limited 2023.



Once the attackers had gained control of the network, they began to brute force servers and applications to gain access to more systems. Using automated tools, they managed to brute-force passwords by trying millions of passwords per second.

protected, accurate and available at all times. The most impressive feature is 'Insider Protection', which catches any attempts to delete data from the Cloud Backup Repository."

The client informed the Covenco team of the situation. He asked for a copy of the backups to be made available online so he could attempt to restore them to the existing infrastructure. However, Covenco's advice was to take a different path... "My advice is always to restore to clean hardware that hasn't been a part of the attack," says Gurdip Sohal, Director of Data Management Services at Covenco. "If you erase your infected hardware and attempt to restore to it, you could cause two issues:

1. You are erasing vital evidence that could help you understand how the attackers gained access to your network and how they managed to transition from machine to machine.

2. You may be restoring data to infected hardware. Although you can erase the drives, the infection can still reside in other hardware, including network devices, storage and servers. The perpetrators will assume this is what you will attempt to do – and they will have injected back-doors and hidden triggers that will reignite the infection, setting off a cascade of further infection."

Gurdip and the Covenco team immediately investigated the status of the off-site Cloud Backup Repository. They discovered that their entire backup had been deleted and was residing within the Veeam Insider Protection zone.

They then contacted the client and engaged in a Comprise Assessment to determine how the threat actors entered the Network and, more importantly, establish an accurate timeline. The Covenco team discovered that the Ransomware deployment began just before the scheduled off-site backup jobs.

The team then restored the data from the Veeam Insider Protection zone to a suite of emergency servers held in a staging area at Covenco, ready for immediate deployment to customer sites.

"Our disaster recovery solutions include ship-to-site hardware that is made ready for deployment 24/7/365," explains Gurdip.

"We restored the latest good backups to a SAN immediately and, along with a Server acting as a HyperV Host, sent them with our engineers to the clients office for commissioning".

Once on-site, Covenco's engineers and the client worked to restore the business's network and availability of data for their staff. The team worked tirelessly to give access to specific data so that the client's customers would not be disrupted. After 24 hours, the business was almost fully operational, albeit on loaned hardware from Covenco.

What was the attack?

By 9am on the morning of 24th August, it was clear that the Ragnor Locker ransomware gang had attacked the company.

Ragnor Locker is a type of ransomware that first emerged in early 2023. It was a relatively new ransomware strain, but it quickly became one of the most active and dangerous ransomware threats to businesses worldwide. Ragnor Locker is known for its aggressive infection vectors and its ability to encrypt a wide range of file types.

Ragnor Locker typically gains access to networks through phishing emails or exploit kits, although in this case, it gained access via an undetected vulnerability in a router. Once the ransomware is on a network, it spreads quickly through shared drives and network shares. Ragnor Locker then encrypts all the files on the infected system, making them inaccessible to the victim.

© Copyright Covenco Limited 2023.

Ragnor Locker operators normally demand a ransom payment in Bitcoin in exchange for the decryption key. If the victim does not pay the ransom, the ransomware operators threaten to leak the victim's data.

In September 2023, the Ragnor Locker group was disrupted by a joint operation between the FBI, Europol, and law enforcement agencies in several countries. The process resulted in the arrest of several group members and the seizure of servers used to control the ransomware operation.

The disruption of the Ragnor Locker group is a significant victory for law enforcement and a blow to the ransomware ecosystem. However, it is important to note that ransomware groups are constantly evolving and adapting. The Ragnor Locker threat will not have gone away; it has most likely transitioned to new ownership, where it will be enhanced further.

What did the attack actually do?

The Ragnor Locker attack on the client exploited an unknown vulnerability in the company's primary router. Although the router was patched and up to date, the attackers were able to discover a vulnerability that allowed them access. Enterprise routers are often assumed to be invulnerable regarding security, but they can be a significant entry point for the most sophisticated attackers.

In this case, the attackers used router hijacking to access the router's configuration and then changed its settings to allow it to take complete control. Once the attacker had control of the router, they used it to launch attacks against the other devices on the network.

Once the attackers had gained control of the network, they began to brute force servers and applications to gain access to more systems. Using automated tools, they managed to brute-force passwords by trying millions of passwords per second.

The safety Net: Veeam Protection Zone

Once the attackers had access to the full system, they started to encrypt data and simultaneously delete all of the backups, including those on the Veeam Cloud Connect servers at Covenco. The client would undoubtedly have faced a much larger disaster if this had been successful.

> "The Veeam Insider Protection Zone within the Cloud Connect saved us a world of pain," says the client. "Without the excellent tools from Veeam and configuration from Covenco, we might still be in recovery today".

The Veeam Insider Protection Zone acts like a recycle bin for backups by storing deleted backup files for a specified period. This prevents ransomware attackers from being able to delete backups completely.

When a backup file is deleted from Veeam, the file is not completely deleted from the storage system. Instead, the file is moved to the Insider Protection Zone, which is a separate storage location and only visible to Covenco as a Veeam Cloud Service Provider.

When a ransomware attack occurs, the attacker will always attempt to delete backups; they can only delete the backup files stored in the production storage location. Because the deleted backups are stored in a completely different location, they are entirely protected from deletion.

The Veeam Insider Protection Zone (SPZ) is valuable for protecting backups from ransomware attacks. By storing deleted backup files in a separate storage location, the Insider Protection feature can help organisations recover their data quickly and easily in the event of a ransomware attack.

Here are some of the benefits of using the Veeam Insider Protection Zone to protect backups from ransomware attacks:

- Prevents backups from being deleted completely: Even if a ransomware attacker can delete backup files from the production storage location, the backup files will still be stored in the Protection Zone and can be restored.
- Reduces the risk of data loss: By preventing backups from being deleted completely, the Veeam Protection Zone minimises the risk of data loss in a ransomware attack.
- The Veeam Insider Protection Zone provides a backup of backups, which can be used to restore data if the production storage location and the Protection Zone are both compromised by a ransomware attack.

© Copyright Covenco Limited 2023.

The client was confident in the Veeam system and knew that the Insider Protection Zone could be his saving grace.

“I knew the SPZ was in place and working because I regularly test it with Covenco as a part of our backup-as-a-service arrangement. I was over the moon when the Covenco team confirmed that we still had clean backups we could restore from.”

Follow-up actions.

Once Covenco’s ship-to-site hardware was up and running, the client could return to ‘business as usual’. But their major challenges had only just begun. The client worked with their insurance-appointed security team to conduct a complete post-attack analysis.

“We had to discover exactly how the attackers had gained access, and we had to trace back through every part of the system to find evidence of the attack and which vulnerabilities they exploited - so we could learn how to prevent it from ever happening again”.

The team created a detailed analysis and report demonstrating exactly how servers and firewalls were breached and how the router was the first point of failure.

The client also had all the due diligence tasks to perform, including notifying the information commissioner’s office and law enforcement.

“Fortunately, we know that the attackers had not managed to exfiltrate any data during their attack,” explained the client. “The security and law enforcement teams thought that the attack had been triggered around the same time that Interpol and the FBI were closing in on the Ragnor Locker gang. They didn’t have time to trigger the exfiltration of our data”.

Only after the security team’s report was completed could the client set about restoring their servers and storage systems.

“Every disk was forensically erased to give us a fresh platform to start again,” says the client. “It was a good experience, and gave the company confidence that every application, license and hardware item was up to date, configured correctly, and running clean data”.

> “We also added further security measures, including SentinelOne endpoint protection.
>
> We know we need further protection for our backups, and we are working with Covenco to engage their Off-site/Offline backup copies, along with an immutable copy for complete peace of mind.”

Are you ready to protect your data?

Contact the Covenco Ransomware Recovery team to discuss your security measures.

We can guide you on the latest best practice tools and techniques to ensure your ransomware survival.

Call: 01753 732 000

Email: sales@covenco.com

Visit: covenco.com

About Covenco

With more than 30 years of experience in the IT industry across a range of technologies, Covenco specializes in purchasing, selling and renting new and refurbished IBM, HP, Dell and NetApp computing hardware, storage and supporting software. Today, Covenco provides cloud and hosting solutions, disaster recovery, maintenance, virtualization, backup and high-availability services.

Solution and services used

Covenco Backup as a Service.

Covenco Ransomware Recovery Service.

Veeam Cloud Connect.

Covenco Disaster Recovery Service.

Contact Covenco

Covenco
Unit 3-4, MXL Centre
Lombard Way
Banbury
Oxfordshire
OX16 4TJ
United Kingdom

Telephone: 01753 732000
Email: sales@covenco.com

www.covenco.com

covenco
DATA MANAGEMENT & INFRASTRUCTURE 365

© Copyright Covenco Limited 2023.