VERITAS

CASE STUDY

Veritas Helps Minimize and Mitigate the Impacts of a Major Ransomware Attack

In the wake of the crippling attack, a global restaurant chain worked with Veritas to recover data without paying the ransom and to redesign data protection to be even more secure.

Challenge

A company that runs restaurants around the world suffered a ransomware attack that deleted all its on-premises backups. Fortunately, the company still had cloud-based instances of many backups. Management decided not to pay a ransom, but instead engaged a Veritas services team to assist with the recovery of its lost data.

Solution

Working closely with Veritas, the internal incident response team created a cloud recovery server to restore data back to the on-premises environment. They rebuilt the company's entire backup infrastructure, including its containerized appliances, and brought back the available backups. The new infrastructure includes additional protections that the company's legacy data protection environment did not offer.

Outcome

The ransomware incident ended up being costly for the company, but much less expensive than it could have been. Through their rapid response, the internal security team helped minimize and mitigate the damage. And through their ongoing partnership with Veritas, they have helped reduce the risk that a future attack will impact the business at all.

INDUSTRY

Food & Beverage

EMPLOYEES

Tens of thousands

HEADQUARTERS

United States

The company's quick response, partnership with Veritas, and—most important—ability to recover data via robust cloud-based backups all combined to reduce the ransomware incident's impact on its business.

Zero-Day Malware Gets Through Cyber Defenses

There is nothing like a ransomware attack to focus the executive team's attention on cybersecurity—as one multinational restaurant chain learned firsthand last year. Using highly sophisticated techniques, bad actors gained unauthorized access to certain of the company's systems, then locked down those systems in hopes of receiving a ransom payment. Hundreds of restaurant locations had to be closed temporarily as the organization struggled to contain the threat and remediate the damage.

> *Because the restaurant company defeated the attack without paying a ransom, it may be less likely to experience similar incidents in the future. Research indicates 80% of organizations that pay ransom demands will face a re-attack.*

Thanks to the rapid response of the corporate cybersecurity team, all the company's restaurants were soon back in business. However, in responding, the security team discovered that some employees' personal data had been exfiltrated. And recovery from the incident was expensive.

Management decided not to pay the ransom, but other costs added up quickly. In addition to working with local law enforcement, the company engaged leading digital forensics and restoration teams to investigate what had happened. The organization also offered impacted employees two years' worth of credit monitoring, as well as access to an insurance policy that would protect them if the corporate breach were to lead to identity theft.

The entire experience was disappointing for a security team that prided themselves on being prepared. They had in place well-defined data protection processes, a stable of best-of-breed security solutions, and a security operations center (SOC)—yet the company still suffered damage. In addition to the direct costs of the incident, some of which continue to play out, the business faces a class-action lawsuit from impacted employees who claim the company was not running adequate cybersecurity and took a reckless approach to data storage.

Robust Backup Architecture Saves the Day

One significant factor that increased the attack's impact was the attackers' ability to cut off access to backup data and then delete the entire backup system from the restaurant company's on-premises servers. Master servers, backup hardware appliances, and data stored on-premises were all wiped clean, as the bad actors awaited payment.

Fortunately, most of the company's on-premises backups were replicated to an instance of Veritas NetBackup™ in the Azure cloud, which was unaffected by the attack. As soon as the company decided not to pay the ransom, its incident response team partnered with Veritas experts to begin recovery efforts. Together, they created a cloud recovery server to restore data back to the on-premises data protection systems.

Essentially, the company had to rebuild its entire backup infrastructure, including its containerized, on-premises appliances. The Veritas recovery team leveraged their extensive experience and deep expertise in attack forensics to help streamline the process and ensure the new infrastructure would be more secure than ever before.

Working with the Veritas team, the restaurant company's internal security group built into the new backup configuration preventative measures that are designed to keep data safe in the event of a future ransomware attack. They implemented multilayer protections across the entire data protection infrastructure, including multifactor authentication (MFA), a "write once, read many" (WORM) procedure, role-based access control policies, anomaly detection capabilities, and even broader replication to a second cloud-based backup environment.

In parallel, the Veritas field security team conducted a comprehensive ransomware-resilience assessment, which identified risks and additional areas for improvement, including some gaps unrelated to the ransomware incident. They worked with the company's internal security team to develop a two-year security roadmap covering all the organization's locations around the world. Veritas experts also suggested improvements to the company's data protection policies and processes, paving the way for a strengthened, comprehensive security strategy throughout the organization.

Mitigating the Impact of a Serious Cyberattack

Although the company continues to spend money dealing with the repercussions of the ransomware attack, its quick response, partnership with Veritas, and—most important—ability to recover data via robust cloud-based backups all combined to reduce the ransomware incident's impact on its business. Restaurant operations were interrupted in only one market, and for a short time. Were the company unable to recover data from backups, its business would likely have incurred far more significant downtime, with much larger impacts to operations and, ultimately, the organization's financials.

Moreover, because the restaurant company defeated the attack without paying a ransom, it may be less likely to experience similar incidents in the future. Research indicates 80% of organizations that pay ransom demands will face a re-attack, as bad actors presumably see the willingness to pay up one time as an opportunity to score additional paydays.

The restaurant company continues to enhance its cyber resilience along several angles outlined in its security roadmap. It is working to better integrate its internal infrastructure and security teams. It is developing new disaster recovery strategies and improving its governance structure. And it continues to foster a tight working relationship with its partners at Veritas.

The ransomware incident could have been much worse, but it is impossible to deny that it had significant business impacts. Through its ongoing relationship with Veritas, the restaurant company intends to ensure that, should it be hit again, any future attack will have even less of an impact.

For More Information

Please contact your local Veritas Sales Representative or Business Partner.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V2108 4/24