CASE STUDY

ATTACKED WITH THE ROBINHOOD RANSOMWARE VIRUS, A CLIENT RECOVERS WITHIN AN ASTONISHING ONE WEEK

THE CLIENT

A nationwide insurance company that provides coverage in over 40 states.

THE CHALLENGE

The RobinHood ransomware crypto virus penetrated a Sirius client's Windows®-based IT ecosystem, rendering the infrastructure (over a petabyte of data) inaccessible. RobinHood ransomware is a complex encryption algorithm that infects all files on a Windows system, leaving it useless unless a ransom is paid or a full system recovery performed. All Windows infrastructure data was impacted for this client, including data for webservers, accounting, claims, payroll, and human resources.

THE SOLUTION

Just months before the attack, Sirius designed and implemented new data protection systems for the client to safeguard against cyberattacks, hardware and software failures, data corruption, and natural disasters. The relatively new systems and policies allowed Sirius to recover business-critical systems within hours, and to fully restore the primary production site within one week.

"The data protection systems that the clients invested in with us allowed them to ignore a ransom demand, to fully restore, and avoid regulatory fines for data loss."
Sirius Solutions Architect

THE RESULTS

- The solution successfully protected a hybrid Nutanix™ Acropolis and VMware® environment for one of the largest insurance providers in the United States.
- Day-one recovery of critical systems such as webservers and payroll allowed the client to remain operational and open for business while the recovery effort on the affected environment was taking place.
- In one week, every instance of Windows in the client environment was restored. The client avoided hefty fines by maintaining government-regulated file retention.

www.siriuscom.com
800.460.1237

THE RECOVERY BEGAN BEFORE THE ATTACK

The odyssey began with a jarring phone call in June 2019. A Sirius client had just experienced complete data loss in a RobinHood ransomware attack. The virus infected every Windows instance in the client's environment. Their entire infrastructure, including backup proxy servers and backup consoles, were encrypted with the virus and therefore inaccessible.

The Sirius solution architect—who designed and implemented the backup and recovery environment a few months prior to the attack—was able to immediately assure the client that all the Nutanix Acropolis and VMware data backed up with Veeam to Dell EMC PowerProtect DD appliance would be recoverable. This was one of the scenarios the agnostic solution was built to withstand.

Here's how it works: Veeam integrates the PowerProtect DD appliances as a backup repository. It leverages DD Boost to restrict access to the PowerProtect DD appliance via an encrypted lockbox that stores the PowerProtect DD system information, including credentials for the DD Boost user. When used as a Common Internet File System (CIFS) backup repository, PowerProtect DD also restricts the access to the CIFS shares by users and groups for an additional protection layer. In addition, the PowerProtect DD operating system is a closed Linux®-based shell, so it is not penetrable to Windows-based malware. During backups, Veeam stores metadata with backup data onto the PowerProtect DD Backup Repository. As a last line of defense, daily snapshots are also performed on the PowerProtect DD appliance. If the appliance was lost due to malware, a snapshot prior to the date of infection could be used to restore the appliance to a healthy state.

Knowing all this, Sirius accessed the backup data with the client to confirm and prove that the PowerProtect DD appliance was not compromised. Given that the Veeam backup server and proxies were infected (since they were Windows Servers), they needed to be re-imaged before Veeam Backup and Replication could be re-installed. Once the Veeam Backup Server was installed, the Veeam Config Backup was imported, and credentials were reestablished from the new backup servers to the PowerProtect DD appliance. It was then confirmed that all backup jobs were disabled.

Finally, restores were initiated for the Acropolis and VMware infrastructures. The restore performance was dictated by the number of backup servers and proxies for each cluster, for the AHV environment, and by the number of physical and virtual proxies for the VMware environment. Once servers were restored, the client made sure all instances of Windows were up to date, and then loaded Windows Defender antivirus software on each machine to ensure they were protected from future infections or attacks.

Restoration of the client's environment to a healthy state was completed in an astonishing one-week timeframe. "It's similar to a chess game; hackers are constantly finding new attack strategies, and we're constantly coming up with different approaches for protection. This is an example of how we proactively protect clients leveraging system design, technologies and policies, " said the Sirius solutions architect.

ABOUT SIRIUS

From evaluation and design to implementation, financing and managed services, Sirius can help you develop a successful data protection strategy to optimize application and service delivery, while safely migrating, managing and running applications for the purposes of data protection, recoverability and resiliency. Contact us to learn more about how Sirius' Data Protection & Information Management team can help you implement a comprehensive, efficient and effective data protection strategy.

SOLUTION COMPONENTS

- Dell EMC® PowerProtect DD Boost for Veeam®, for VMware® backups
- Veeam for Nutanix AHV, for backups to the PowerProtect DD appliance
- Veeam retention policies fulfilling recovery point and recovery time objectives (RPO/RTO)
- Daily PowerProtect DD snapshots

SSTA_ROBRANSOM_042020