CASE STUDY

Recovering from Phobos Ransomware Attack on Exchange Environment

Restoring Critical Infrastructure and Ensuring Business Continuity

Introduction:

In February 2024, a global IT product-based company confronted a severe ransomware attack by Phobos, which critically impacted their entire Exchange Server environment and also affected their Active Directory (AD) infrastructure. This case study delves into the comprehensive recovery efforts undertaken to restore functionality and mitigate operational disruptions.

Background:

The company operated a robust infrastructure with three Exchange servers configured in a Database Availability Group (DAG). This setup was pivotal in ensuring high availability and redundancy, essential for maintaining seamless email communication and collaboration across departments.

Impact on the Business:

The ransomware attack compromised two out of three Exchange servers running on Exchange Server 2016 CU21. To contain the threat, these servers were promptly shut down. In addition to Exchange servers, the company's file server and SharePoint environment also fell victim, severely affecting critical file sharing and collaborative services. The attack extended to their Active Directory (AD) infrastructure, causing a complete system crash that disrupted user authentication and access controls.

Attempted Solutions:

- IInitially, containment efforts focused on isolating infected servers to prevent further spread and data encryption. Given the extent of the damage and encryption of data on affected servers, a comprehensive recovery strategy was initiated.

Confidential

IT Product Based Company

Statement from the customer:

"The Phobos ransomware attack severely disrupted our Exchange Server and critical infrastructure. Thanks to Stellar Repair for Exchange for recovery efforts, we swiftly restored operations and bolstered our security. We truly appreciate the dedicated support that made this recovery possible."

IT Manager

Client

- IT Manager

Business Need

- Ensuring uninterrupted email communication and seamless collaboration across departments.

Solution and Benefits

Rebuilding Active Directory:

- The company manually recreated user accounts and rebuilt the AD infrastructure to restore crucial user authentication and permissions.
- Performed an Active Directory backup restore using Windows Backup

Deployment of New Exchange Server:

- Implemented a new Exchange Server 2016 environment, meticulously applying cumulative updates and reinforcing security configurations to fortify against potential future threats.

Data Recovery and Conversion:

- Utilized Stellar Repair for Exchange to extract unaffected EDB files directly to Live Exchange, ensuring the preservation of email data integrity.
- Prioritized higher management's accounts for export to Live Exchange, followed by importing PST files into users' Outlook, including archive mailboxes, and local and external contacts.
- Successfully restored all emails, calendar events, and tasks, receiving positive feedback from users. Stellar's technical support was instrumental in facilitating these efforts.

Restoration of File Server and SharePoint:

- Leveraged backup copies to restore critical data and conducted rigorous integrity checks to verify the completeness and accuracy of recovered files and documents.

Conclusion:

Through decisive and coordinated efforts, the company successfully restored critical Exchange Server functionality and mitigated the disruptive impact of the ransomware attack. The deployment of a new Exchange environment, coupled with robust data recovery measures and meticulous AD reconstruction, enabled them to swiftly resume normal operations and maintain business continuity.

Challenges

- Addressing the extensive impact of ransomware on critical infrastructure components, including Exchange Server, file server, SharePoint, and Active Directory.

Stellar Repair for Exchange

Benefits

The rapid and effective recovery facilitated by Stellar Repair for Exchange and the comprehensive rebuilding efforts not only restored business continuity but also enhanced resilience against future cybersecurity threats, underscoring our commitment to safeguarding organizational operations and data integrity.