WAFS ™ Versioning Feature Mitigates Effects of Ransomware

With the Help of WAFS's Versioning Features and Globalscape Support, Three Globalscape Customers Were Able to Reclaim Their Data Encrypted by Ransomware.

Introduction

What do a textile manufacturing company in the Greater New York Area, a global food supply company, and a global engineering firm have in common? All three organizations need to securely collaborate with offices in multiple locations, and all three were infected by ransomware.

As Globalscape's WAFS is a dynamic platform, each of the organizations use it in different ways to collaborate on files around the world. The textile manufacturing company uses WAFS to replicate their manufacturing templates, accounting and other critical data to manufacturing sites in China and the US; the food supply company uses WAFS to replicate sales and inventory data to share to multiple business offices; and the engineering company uses WAFS to transfer very large schematic files and blue prints.

These organizations had the issue that many do with maintaining multiple offices—how to securely share and collaborate on large files while maintaining the speed organizations on a LAN are accustomed to. In the case of the textile company and the engineering company, both require the need to collaborate on large design files, which had proved difficult before installing WAFS.

The Challenge

Ransomware restricts access to files stored on a local or mounted network drive using asymmetric keys. Once the files are encrypted, only the private key stored on the malware's control servers can decrypt the information. Organizations are asked to pay a fee, sometimes thousands of dollars, depending on the source of the ransom and the size of the organization to regain access to their information. If the organization does not pay the ransom within a certain period of time, the private key will expire and the critical company data will be rendered unintelligible forever.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

Copyright © 2014 GlobalSCAPE, Inc. All rights reserved. For more information about Globalscape, visit globalscape.com.

As any organizational security policy is only as strong as its weakest link, in these cases, each company had an employee fall victim to an attack. Prompted to visit a malicious site, these users downloaded a ransomware trojan. Once the employee's workstation was infected, the virus sought out and mapped each organization's network drives. Once there, the virus began to restrict access to critical files.

"We were very concerned when files were encrypted. Those files are our livelihood," said a representative from the engineering firm. "They are a significant portion of our business and represent countless man hours."

After clicking on a link in a malicious email, each of the organizations' systems were affected. Data stored in the Vault, WAFS's central data repository, became encrypted. Locked out of their mission-critical systems and with time running out, they came to Globalscape's support team to find a solution.

The Solution

When afflicted with ransomware, it's considered a best practice to not pay the ransom. Usually, the ransom is required to be paid in Bitcoins or other crypto-currencies that are untraceble. As such, organizations have no assurances that their data will be returned to its previous, plaintext state, or that the malware will not encrypt the files again. Each organizations turned to Globalscape's support team to solve their issue and return their data to its previous state.

The organizations differed in their implementation of WAFS and the degree to which their systems were compromised. Globalscape's support provided a case-by-case assessment of the situation to develop a solution.

For the textile manufacturing company, the Globalscape support technician was able to create a script that would parse through the Vault-stored data and convert the data to a previous revision not encrypted by the ransomware.

The food sales company had only a small subset of data encrypted. Globalscape's support technicians were able to walk the company representatives through the process of reverting data to a previous version stored within the vault.

The engineering firm was able to restore the Vault from a backup before the ransomware encryption occurred, which caused all Agents to download the previous versions that were uninfected by the ransomware.

Copyright © 2014 GlobalSCAPE, Inc. All rights reserved. For more information about Globalscape, visit globalscape.com.

The Result

In all three cases, the files were restored with the help of a script from Globalscape's support team and WAFS versioning feature.

In the wake of each incident, the customer reassessed their security policies. Without WAFS, the food sales company and the textile manufacturing company would have experienced a significant data loss as neither of the organizations had backup systems supporting their primary. The engineering firm did have a backup system to restore data from, but could have lost the most recent data acquired.

Globalscape support provided feedback to each customer to assist them in maintaining business continuity and to prevent future attacks, including:

» Implement a boundary connection with proxy servers to isolate their internal networks

» Deploy a backup system for organizations operating without one

» Limit the ability to download or transfer infected files

"We were relieved to be back in control of our data. The encrypted information represented a significant portion of our business," said a representative from the food sales company. "Globalscape customer support was very knowledgeable and quick to help us when time was of the essence. All things considered, they were able to help us turn around a potentially catastrophic experience."

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features Enhanced File Transfer™, the industry-leading enterprise file transfer platform that delivers military-grade security and a customizable solution for achieving best-in-class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments, and small businesses.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

Copyright © 2014 GlobalSCAPE, Inc. All rights reserved. For more information about Globalscape, visit globalscape.com.