ALVAKA RECOVERS OVER 2 MILLION FILES THOUGHT TO BE LOST FOREVER

ALVAKA
CASE STUDY

Emergency Services Designed for the Rapid Recovery of Your Business!

Overview

A state government entity in the Midwest with 900 users needed to decrypt over 2,000,000 "double" and "triple" encrypted files that were crucial to its operations. The attack had exhausted the IT staff and brought day-to-day operations to a halt.

Challenges

The organization had been attacked by a ransomware group that used two unique ransomware variants to encrypt its irreplaceable files. While the victim paid the ransom and a leading forensics firm was hired to decrypt the data, they could not recover more than 24% of the files.

Unfortunately, while the threat actors had delivered some of the decryption keys, many of the file ID's remained buried under more layers of encryption. To make the situation worse, the organization did not have sufficient computing resources to decrypt the data in their environment.

After a month, the forensics firm and victim concluded that further efforts to decrypt data would be futile and that 75% of the data, representing years of irreplaceable work, was lost forever.

Luckily, the breach attorney, familiar with Alvaka's ransomware recovery expertise, contacted Alvaka in a last-ditch effort to recover the rest of the files.

At a Glance...

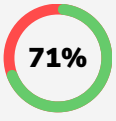
- State government entity
- 900 users impacted
- 2,000,000+ encrypted files
- Multiple layers of encryption
- 5-figure ransom
- GlobeImposter & MedusaLocker Ransomware variants

Before Alvaka

- Ransom paid
- Over a month of decryption effort
- 75% of files thought to be lost forever

Only 24% of files recovered after one month

After Alvaka



71% of files recovered within 2 days

99%+ of files ultimately recovered

Solutions

With prior experience with a wide range of Ransomware variants, Alvaka was able to develop a custom decryption method within 24 hours. Within 48 hours, it had successfully decrypted 71% of files. Initially, the client had hoped to only recover a few critical files, but Alvaka eventually decrypted over 99% of the files, thought to be lost forever.

To accelerate the recovery, Alvaka placed their proprietary Ransomware R.E.S.C.U.E. Kit onsite in the client's environment. The R.E.S.C.U.E. Kit is a powerful toolset that helps to rapidly and efficiently recover and rebuild servers and workstations infected by ransomware. Alvaka was able to seamlessly integrate into the client's environment without impacting the performance of their production systems, significantly reducing the timeframe for recovery.

Benefits

Alvaka's team works tirelessly around the clock, logging every step in detail to ensure complete transparency and understanding of how we are recovering your operations. Our services are tailored to your unique situation so that your organization's operations become fully functional again.

Results

Alvaka delivered positive results within 24 hours and recovered over 2,000,000 files that had been encrypted in multiple layers by two ransomware variants. The client was able to return to normal operations within three weeks of hiring Alvaka.

*"The R.E.S.C.U.E. Kit drastically **reduced restoration times** and assured the success of the recovery" - Kevin McDonald, COO & CISO of Alvaka*

About Us

Alvaka provides a portfolio of technologies and services that ensure the integrity of your network, 24 hours a day, 365 days a year. We provide the necessary talent, tools, and resources your business needs so that you can focus on what truly matters. Since the 1990s, Alvaka has been helping clients build and manage the fast and secure networks they need for the new world of non-stop business.

Alvaka's Network Operations Center in Irvine, California, is staffed by US Based engineers ready to meet your needs at any time of day or night. Detailed information about Alvaka and the services we offer are available on our website, www.alvaka.net

If you have any questions please reach out at **(949) 428-5000** or **sales@alvaka.net**. We operate **24x7x365** with all US based personnel.