Proven Data Restores PowerHost's VMware Backups After SEXi Ransomware Attack

By Jane Devry

Published: 2024-05-31 · Archived: 2026-04-05 17:14:17 UTC

The rise of sophisticated cyberattacks and increasingly brazen attackers is a well-established threat. Businesses and organizations need to take action and be aware of the risks cyberattacks and data breaches pose to their daily functions, financial statements, and reputation. A recent ransomware incident involving IxMetro PowerHost, a Chilean data center and hosting provider with operations spanning the USA, South America, and Europe, is a stark reminder of these dangers.

The ransomware deployed by a threat actor group known as “SEXi” was specifically designed to target ESXi environments, a choice reflected in the group’s name, which is an anagram of ESXi. This suggests a deliberate focus on these systems, leveraging specific vulnerabilities or misconfigurations common in such setups. Once inside the network, the ransomware likely utilized scripts or automated processes to locate and encrypt ESXi server data systematically, rendering the virtual machines (VMs) and their associated data inaccessible. This method ensures a high-impact disruption, as each encrypted ESXi server simultaneously affects multiple clients and services.

The Attack History

April 2024 saw the emergence of the SEXi ransomware gang, which launched a strategic attack on PowerHost's VMware ESXi servers hosting their clients' virtual private servers (VPS). The ransomware, specifically crafted to exploit vulnerabilities in ESXi systems, spread rapidly across the network. It systematically encrypted data on the servers and backups, crippling the virtual machines (VMs) and rendering crucial data inaccessible.

SEXi's method was particularly devastating because it focused on centralizing multiple virtual environments within single physical servers. This strategy maximized disruption by encrypting a limited number of high-value targets, significantly impacting PowerHost's clients. This approach demonstrates an evolution in ransomware tactics, where attackers aim to negate the victim's ability to recover independently, thus strengthening their leverage.

It encrypted terabytes of data, effectively rendering numerous websites and services hosted on these servers inaccessible. The ransomware gang demanded a ransom of two bitcoins per victim, which would have amounted to an astronomical $140 million.

Mitigation and Recovery

As customers began experiencing service outages, PowerHost's IT team swiftly identified the ransomware infection. Recognizing the severity of the situation, they enlisted the expertise of Proven Data's cybersecurity specialists. Simultaneously, PowerHost's CEO, Ricardo Rubem, coordinated with law enforcement agencies across multiple countries to gain insights and formulate a response strategy. The clear consensus from these agencies was to refrain from paying the ransom.

Despite encrypting both primary data and backups, PowerHost and Proven Data worked tirelessly to restore services. Leveraging advanced decryption techniques and cutting-edge recovery tools, the joint effort resulted in successful data recovery for IxMetro PowerHost. This critical intervention saved the company from the staggering $140 million ransom demand and minimized operational downtime and financial losses.

While the recovery process is still ongoing, PowerHost has offered affected VPS customers the option to set up new VPS systems, enabling some customers to resume online operations.

Results

PowerHost's collaboration with Proven Data cybersecurity experts and law enforcement agencies was crucial and underscored the importance of collective efforts in combating cyber threats. This collaborative approach was a testament to the strength of the cybersecurity community and its commitment to protecting businesses and organizations.

It also outlines the importance of transparent and timely communication with customers, which is vital in maintaining trust and managing the fallout from such attacks.

Lessons Learned

The ransomware attack on PowerHost is a critical lesson for businesses worldwide about the necessity of robust cybersecurity measures. By learning from PowerHost's experience, other companies can fortify their defenses and

better protect themselves against the ever-growing ransomware threat. The incident highlights the strength of the cybersecurity community and its unwavering commitment to safeguarding businesses and their operations.

About Bogdan Glushko

Bogdan Glushko is the Chief Information Officer of Proven Data. Glushko actively leverages his years of experience restoring thousands of critical systems after incidents. Glushko is a trusted voice guiding organizations on resilient data strategies, ransomware response protocols, and mitigating evolving cyber threats. Through proven leadership, he continues delivering cutting-edge data preservation and recovery solutions that fortify business resilience against breaches, outages, and data loss from modern cyber attacks.

Join our LinkedIn group Information Security Community!
