DATA SHEET

# Backups

## The Age of Ransomware

In years past, the primary threats to backups were natural disasters – tornadoes, earthquakes – physically destroying data. To achieve resilient backups, organizations rotated tapes and other storage media to offsite storage, replicated data between geographically dispersed brick-and-mortar data centers, and later shifted to the cloud.

Today, criminals that leverage ransomware intentionally corrupt or erase backups to increase the odds of their victims paying the ransom. This technique is effective and deployed frequently. Achieving resilient backups now requires implementing countermeasures to protect backups from this threat.

### Protecting Against Ransomware

MOXFIVE has observed the three scenarios below significantly impact organizations which are unprepared for an attacker targeting their backups.

- An attacker obtains privileged access to internal resources, including backups.
- Leveraging that access, an attacker deletes, modifies, or corrupts the backups.
- Valid backups of data prior to ransomware encryption exist but are subsequently overwritten by post-ransomware-execution encrypted data.

When faced with two difficult options, one being to pay the ransom, and the other to reconstruct entire swaths of IT from scratch, it's easy to see why organizations pay. If viable backups are not available, reconstruction may not even be a viable option – the business disruption may be too severe to consider.

### Attacker obtains access to backups

There are many security measures that make gaining privileged access difficult, but none are perfect. Given the severity of business disruption that can occur in a ransomware attack that also corrupts backups, assume that an attacker will bypass defenses, gain access to the internal network (and, if applicable, cloud resources), and achieve privileged access on par with that of IT administrators.

## Benefits of working with MOXFIVE

### IT & Security Expertise On-Demand

With a deep understanding of both IT operations and security, MOXFIVE Technical Advisors can provide the expertise you need and help determine the most efficient and cost-effective solution.

### Access to Experts at Scale

MOXFIVE maintains an ecosystem of the industry's best technology experts and service providers so we can quickly assemble the right team with the skills you need.

### Streamlined Process

MOXFIVE manages the selection, implementation and procurement processes to keep projects on schedule and minimize disruption.

### Resilient Outcomes

MOXFIVE identifies gaps between business, IT and security objectives to build a more resilient environment.

To mitigate backup-disrupting scenarios, ensure that solely having privileged access within Active Directory is not sufficient to administer the backup system. Leave the backup server off the domain with a separate set of credentials required to administer it, so that domain credentials won't provide access. Better yet, require multifactor authentication to access the server(s) and administrative portals that control the backup infrastructure.

### Attacker corrupts backups

For maximum resilience, further assume that the attacker may gain the ability to delete or corrupt 'online' backups leveraging their administrator level access (sometimes through vulnerabilities). Mitigating this capability requires backup tooling that has been designed to provide 'immutable' storage, meaning that even privileged users cannot modify it.

For particularly important data, periodically creating a copy that is stored offline can also mitigate a worst-case scenario. If all else fails and primary backups are corrupted, a month-old offsite backup can open more options than no backups at all.

### Valid backups are overwritten

This scenario differs from the prior two in that it can occur even if an attacker does not corrupt backups intentionally. Depending on the backup method and timing, differential backups of post-ransomware-execution encrypted data may occur frequently. If the victim organization does not identify the attack promptly, many differential backups may be taken. If limited storage space has been allocated to store those differential backups, old (valid) backups may be completely deleted by the system to make room for the new (ransomware encrypted) ones.

To avoid this scenario, ensure that your ransomware response playbook includes a triage step to ensure that this is not occurring in your environment.

### Plan for a rainy day

Common threads running through many of MOXFIVE's ransomware cases include IT organizations being unaware of attackers specifically targeting backups, configurations that exposed those backup systems to attackers once they gained internal privileged access, lack of immutable storage, and lack of redundancy for business-critical systems and data.

MOXFIVE can assist your organization in preparing for these challenges – whether through tabletop exercises simulating ransomware attacks, hands-on testing to identify weaknesses, or procuring resilient backup tools.

Check out MOXFIVE's previous blog posts on this topic for additional context and case studies: Backups: Ahh! To Zzz and Ransomware Recovery Tales: Protect the Kingdom.



www.moxfive.com
(833) 568-6695
info@moxfive.com



MOXFIVE