RANSOMWARE THREAT LANDSCAPE REPORT

2023 RANSOMWARE RESURGENCE

EMERGING TRENDS, THREAT ACTORS, AND CYBERSECURITY STRATEGIES

A BLACK KITE RESEARCH REPORT

RANSOMWARE PREVENTION AND RESPONSE RECOMMENDATIONS FOR ORGANIZATIONS

INTERNAL SECURITY MEASURES FOR RANSOMWARE PREVENTION

MONITOR YOUR RANSOMWARE INDICATORS

Keep track of your ransomware indicators to avoid being on the radar of ransomware groups. Regularly check for open critical ports, leaked credentials, email security configurations, and phishing/fraudulent domains.

PATCH MANAGEMENT

Ensure all systems, applications, and software are up-to-date with the latest patches, focusing on those with known remote code execution vulnerabilities.

NETWORK SECURITY

Restrict remote access to your network by closing unnecessary ports, using VPNs, and employing strong authentication methods like multi-factor authentication (MFA).

DATA AND SYSTEM BACKUP

Regularly back up critical data and systems to allow for quick recovery in the event of an attack. Store backups both on-site and off-site, and consider using air-gapped storage for added protection. Test your backup and recovery processes periodically to ensure their effectiveness.

ENDPOINT SECURITY

Implement strong endpoint security measures, including antivirus and anti-malware software, and consider deploying advanced solutions like micro VMs to prevent malware from spreading.

INCIDENT RESPONSE PLAN

Develop and maintain a comprehensive incident response plan to address potential ransomware attacks, including clear roles and responsibilities, communication protocols, and recovery strategies.

EMAIL SECURITY

Strengthen your email security by implementing SPF, DKIM, and DMARC records, and conduct regular security awareness training to educate employees on how to identify and report phishing attempts.

By implementing these internal security measures, you can reduce the likelihood of falling victim to a ransomware attack and minimize the potential damage if an attack does occur.

MITIGATING THIRD-PARTY RANSOMWARE RISK

TO MITIGATE THE RISK OF RANSOMWARE ATTACKS DUE TO THIRD-PARTY VENDORS, ORGANIZATIONS SHOULD:

- Evaluate the cybersecurity posture of third-party vendors using tools like Black Kite's Ransomware Susceptibility Index™ (RSI™).
- Require vendors to adhere to industry best practices and implement robust cybersecurity measures.
- Perform regular audits of vendors' security practices and provide guidance for improvement if necessary.
- Foster a culture of collaboration and information sharing among vendors to enhance overall cybersecurity.

RESPONDING TO A RANSOMWARE ATTACK

STEPS TO TAKE WHEN HIT BY A RANSOMWARE ATTACK INCLUDE:

- Isolate affected systems to prevent the spread of the ransomware.
- Notify relevant authorities and stakeholders.
- Engage with cybersecurity experts to assess the situation and explore potential remediation options.
- Preserve evidence and document the incident for future reference and potential legal actions.

POST-ATTACK RECOVERY

AFTER A RANSOMWARE ATTACK, IT IS CRUCIAL TO LEARN FROM THE EXPERIENCE AND STRENGTHEN DEFENSES. POST-ATTACK STEPS INCLUDE:

- Conduct a thorough analysis of the incident to identify root causes and vulnerabilities.
- Implement recommended security measures to prevent similar attacks in the future.
- Review and update your incident response plan based on the lessons learned.
- Share information about the attack with relevant parties and collaborate with industry peers to improve overall cybersecurity.