



Threat Intelligence Report

Date: 2024-12-24 | Report ID: TR-2024-001

Executive Summary

This test report verifies that threat cards and IOC boxes are not split across pages during PDF generation.

Threat #1: Phishing Campaign

Severity: HIGH

Description: A sophisticated phishing campaign targeting financial institutions has been detected. The campaign uses spoofed email addresses and fake login pages to steal credentials.

Affected Entities:

- Banking sector organizations
- Credit unions
- Financial service providers

Recommendations:

- Implement multi-factor authentication
- Conduct user awareness training
- Deploy email filtering solutions

Indicators of Compromise (IOCs)

Malicious Domains:

- evil-bank-login[.]com
- secure-verify-account[.]net
- banking-update[.]org

IP Addresses:

- 192.168.1.100
- 10.0.0.50
- 172.16.0.25

Threat #2: Ransomware Attack

Severity: HIGH

Description: A new ransomware variant has been identified targeting healthcare organizations. The malware encrypts critical files and demands payment in cryptocurrency.

Attack Vector: Malicious email attachments and compromised RDP connections.

Mitigation Steps:

- Maintain offline backups
- Patch all systems regularly
- Disable unnecessary RDP access
- Monitor for unusual file encryption activities

File Hashes (SHA-256)

- a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6
- b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6a1

Threat #3: Data Breach

Severity: MEDIUM

Description: A misconfigured cloud storage bucket exposed sensitive customer data. Approximately 50,000 records were accessible without authentication.

Exposed Data:

- Customer names and email addresses
- Transaction history
- Partial payment information (last 4 digits)

Response Actions:

- Secure the storage bucket immediately
- Notify affected customers
- Review access controls on all cloud resources
- Implement monitoring for sensitive data exposure

Conclusion

This test verifies that all threat cards and IOC boxes remain intact on single pages without being cut across page boundaries. The PDF generation should preserve all styling and maintain readability.