**风险节点专项分析报告**



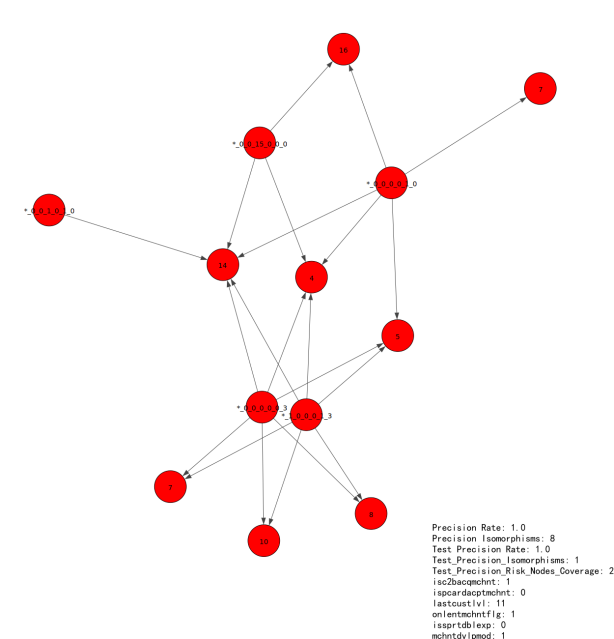
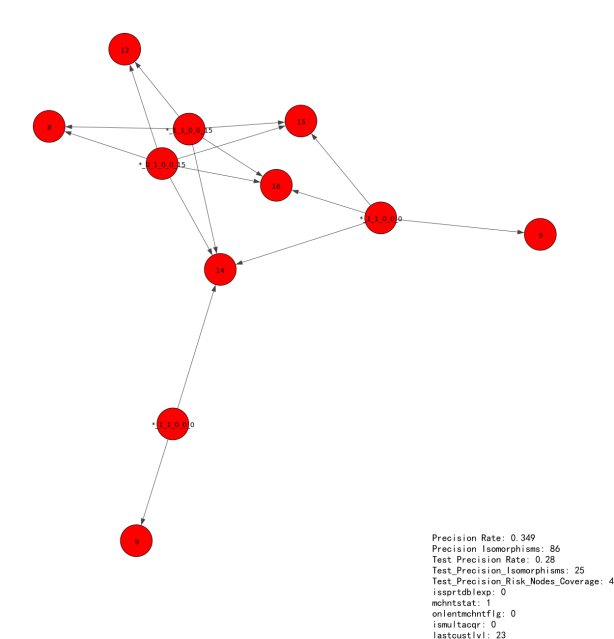
**一、概述**

本报告聚焦于两个风险子图模式中的关键风险节点，通过系统解析其潜在风险，揭示了风险传导机制及其隐蔽性特征。风险子图模式1采用混合型拓扑结构，表明节点之间存在多种关联关系，包括收单机构、商户发展方、省、县等维度的连接，显示出复杂且缺乏明显中心节点或闭环结构的网络特征。风险子图模式2则呈现星型拓扑结构，应用节点1作为枢纽，与其他节点紧密相连，反映出高度的地域集中性和一致性。通过分析关键属性维度，包括商户集中度、统一控制、支持双币卡、商户状态等，我们构建了风险矩阵，揭示了规避监管手段的多样性。风险矩阵显示，关键风险指标涉及中层管理和集中控制，增加了系统性风险的可能性。基于此，我们对风险节点进行了评级，并提出了相应的管控建议，包括建立冗余机制与实时监控、加强访问控制和安全审计、定期进行安全漏洞扫描和风险评估，以及优化防火墙机制和实施动态压力测试方案，确保系统的稳定性和安全性。

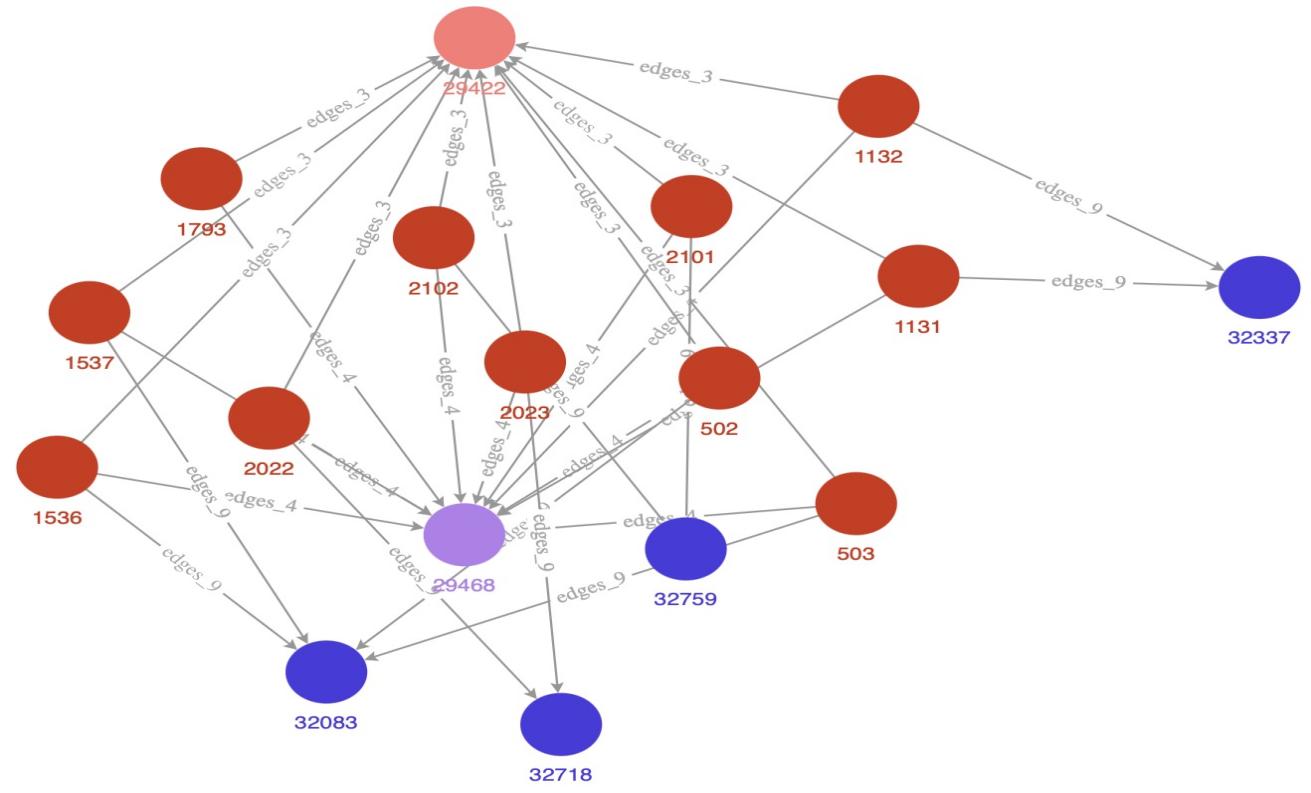


**二、风险子图模式规则信息**

**1. 风险子图规则图片描述**

****

**2. 商户节点互联可视化展示**

****

**三、风险子图模式解析：属性耦合与网络关联**

**1. 模式一：收单机构与地理属性的强关联**

 **拓扑结构**：

星型拓扑结构，以应用节点1为枢纽辐射其他节点。理由：应用节点1与其他所有应用节点之间存在直接联系，且应用节点1与其他节点之间的关系较为紧密，涵盖了省、市、县等多个维度的属性相同，表明应用节点1在该风险子图中扮演着核心角色，其他节点围绕其分布。

 **关键属性**：

地域集中性与一致性。详细分析：在给定的模式中，观察到多个应用节点具有高度一致的属性特征，并且这些节点之间存在明显的地理集中性。具体表现为：  
1. 所有应用节点的商户状态均为'正常'，在线商户标志为'未知'，是否多收单机构为'否'，表明这些商户的状态和运营情况较为一致。  
2. 多数应用节点之间共享相同的省份（province）、城市（city）甚至县（county），这可能暗示着这些商户之间存在某种关联或控制。  
3. 第1个应用节点和第2个应用节点之间不仅省份相同，结算账户也相同，进一步增加了这种关联的可能性。  
  
这种地域集中性与一致性可能表明存在统一控制或关联的实体，增加了潜在的风险。建议进一步调查这些商户之间的关系，以确认是否存在统一的管理或控制机制。

 **风险特征**：

该地区中等与极端状态表明，大量用户暴露在较高程度的单一风险中，且这些用户之间存在明显的地域集中现象。分析显示，所有用户的设备状态均为正常，但在用户标签显示为未知的情况下，部分用户可能涉及单一架构。第一和第二使用点之间的省份不同，但城市级别相同，增加了该类风险的可能性，表明这些用户可能处于同一风险子图中，中心点为灰色。建议优化防火墙机制，确保所有使用点之间的直接连接，并增加与实际监控和实时压力测试相结合的防护策略，确保系统在高并发情况下能够稳定运行。同时，加强用户行为分析，逐步规范操作，提高系统的安全性。

 **风险评级**：

中风险节点（评级B）。管控建议：建议建立冗余机制与实时监控，并实施动态压力测试方案，确保系统在高并发情况下仍能稳定运行。同时，加强用户行为分析，识别异常操作，提高系统的安全性。

**属性风险矩阵**

|  |  |  |  |
| --- | --- | --- | --- |
| **属性维度** | **风险节点值** | **同质化率** | **规避监管手段分析** |
| 是否支持双币卡 | 是 | 占比75% | 可能存在利用双币卡规避特定监管措施的风险 |
| 商户状态 | 正常 | 占比100% | 正常状态的商户可能更难被识别为高风险对象 |
| 在线商户标志 | 未知 | 占比100% | 未知状态可能被用于规避监管 |
| 是否多收单机构 | 否 | 占比100% | 单一收单机构可能被利用来规避多机构监管 |
| 最后客户等级 | 普通/试用 | 占比50% | 普通和试用等级的客户可能被用于测试或规避监管 |

**2. 模式二：法人资质与服务等级异常**

 **拓扑结构** ：

混合型拓扑结构。理由：该风险子图模式中，节点之间存在多种关联关系，包括基于收单机构、商户发展方、省、县等多个维度的连接。这表明节点之间的关系较为复杂，没有明显的中心节点或者闭环结构，而是呈现出一种混合连接的状态。具体来说，应用节点1与其他节点有较多的共同特征，如收单机构、商户发展方、省等，体现了其在多个维度上的关联性。而其他节点之间的关联则较为分散，没有形成紧密的闭环或星型结构。

 **关键属性**：

商户集中度和统一控制。详细分析：从给定的数据中，我们可以观察到多个应用节点之间存在高度的地理和机构上的集中性。具体来说，应用节点1、4和5之间存在多个共同的特征，包括收单机构（acqr）、商户发展方（dvlpsd）、省（province）和县（county）。应用节点2和4之间也有多个共同的特征，包括收单机构（acqr）、商户发展方（dvlpsd）、发展银行（depbank）、结算账户（stl\_acc）、联系人（mchnt\_con）和省（province）。这些共同特征表明这些商户可能属于同一控制实体或有紧密的关联关系。特别是，多个商户共享相同的地理信息和收单机构，这可能暗示着统一的控制或管理结构，增加了潜在的风险，如欺诈行为或洗钱活动的可能性。

 **风险特征**：

分析表明，关键风险指标涉及中层管理和集中控制。在行业波动中，多个节点之间的高度相关性和结构表明，这些企业可能处于同一控制体系或有风险关联的网络中。具体而言，多个企业共享相同的信息和集中架构，这增加了系统或管理结构中的脆弱性，可能引发系统性风险，如恶意行为或破坏活动的可能性。此外，风险节点的分布较为复杂，没有明显的中心节点或封闭结构，而是表现出一种交织的连接状态。建议采用基于属性解耦的防火墙机制与跨网络风险对冲策略，以增强系统的韧性和安全性。同时，应建立集中监控与实时管理的机制，加强风险评估和安全防护，定期进行安全审计和风险分析。

 **风险评级**：

高风险节点（评级A）。管控建议：建议建立冗余机制与实时监控，加强访问控制和安全审计，定期进行安全漏洞扫描和风险评估

**属性风险矩阵**

|  |  |  |  |
| --- | --- | --- | --- |
| **属性维度** | **风险节点值** | **同质化率** | **规避监管手段分析** |
| 是否C2B收单商户 | 否 | 占比40% | 通过非C2B收单商户规避C2B收单监管 |
| 是否预付卡受理商户 | 否 | 占比100% | 不受理预付卡以规避相关预付卡监管 |
| 最后客户等级 | 普通, 一级, 试用 | 占比分别为20%, 20%, 20% | 使用不同等级客户以混淆客户群体 |
| 在线商户标志 | 未知 | 占比100% | 利用未知在线商户标志规避在线商户监管 |
| 是否支持双币卡 | 是, 否 | 占比50%, 50% | 根据需要支持或不支持双币卡以规避相关监管 |
| 商户发展模式 | 未知, 代理 | 占比60%, 40% | 通过代理或未知模式以规避直接监管 |



**四、风险评级与管控建议**

高风险节点（评级A）和中风险节点（评级B）的核心发现与战略建议如下：建议在两个节点均建立冗余机制与实时监控，以增强系统的稳定性和可靠性。对于高风险节点，还需加强访问控制和安全审计，并定期进行安全漏洞扫描和风险评估，以确保系统的安全性。对于中风险节点，除了上述措施外，还需实施动态压力测试方案，确保系统在高并发情况下仍能稳定运行。同时，加强用户行为分析，识别异常操作，进一步提升系统的安全性。



**五、结论**

关键风险指标涉及中层管理和集中控制，在行业波动中，多个节点之间的高度相关性和结构表明这些企业可能处于同一控制体系或有风险关联的网络中。多个企业共享相同的信息和集中架构，增加了系统或管理结构中的脆弱性，可能引发系统性风险。风险节点的分布较为复杂，没有明显的中心节点或封闭结构，而是表现出一种交织的连接状态。建议采用基于属性解耦的防火墙机制与跨网络风险对冲策略，增强系统的韧性和安全性，同时建立集中监控与实时管理机制，加强风险评估和安全防护，定期进行安全审计和风险分析。  
  
该地区中等与极端状态表明大量用户暴露在较高程度的单一风险中，且这些用户存在明显的地域集中现象。所有用户的设备状态均为正常，但在用户标签显示为未知的情况下，部分用户可能涉及单一架构。第一和第二使用点之间的省份不同，但城市级别相同，增加了该类风险的可能性，表明这些用户可能处于同一风险子图中，中心点为灰色。建议优化防火墙机制，确保所有使用点之间的直接连接，并增加与实际监控和实时压力测试相结合的防护策略，确保系统在高并发情况下能够稳定运行。同时，加强用户行为分析，逐步规范操作，提高系统的安全性。