**风险节点专项分析报告**



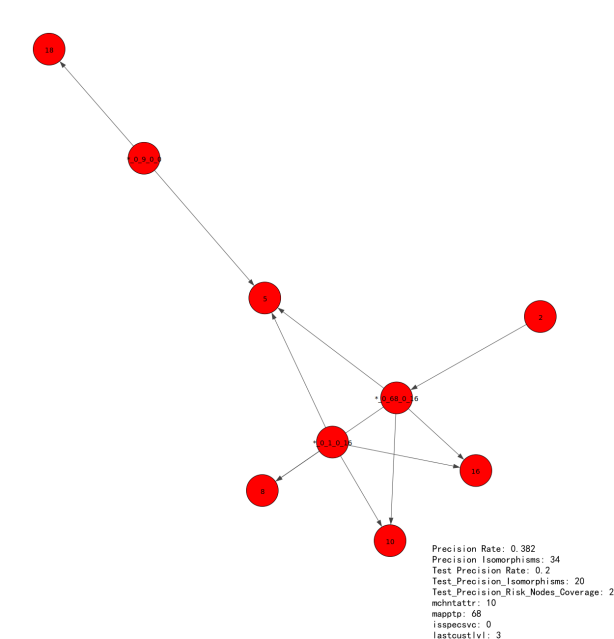
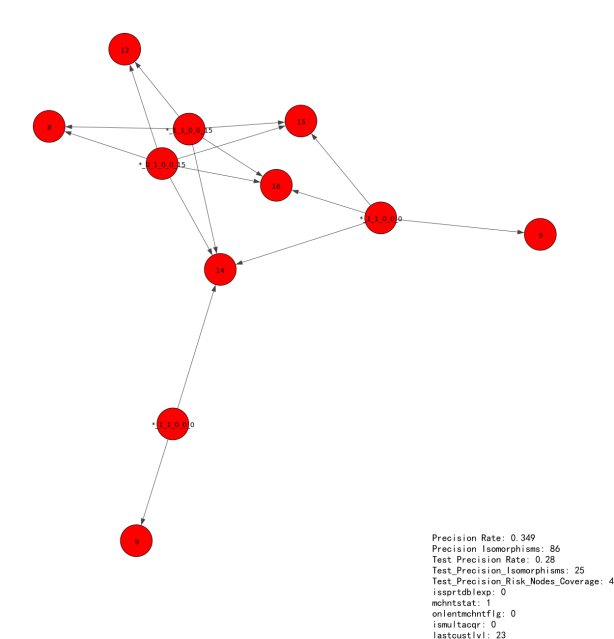
**一、概述**

本报告聚焦于两个风险子图模式，旨在系统解析其潜在风险。通过分析覆盖这两个风险子图模式的星型拓扑结构，揭示了风险传导机制及隐蔽性特征。具体而言，模式一以应用节点1为中心，辐射其他节点，表明应用节点1可能为核心节点，其他节点通过不同的属性与之相连，符合星型拓扑结构的特点。模式二同样采用星型拓扑结构，以用户节点1为中心，其他节点围绕其分布，表明用户节点1在地理位置上是中心节点，其他节点通过不同的属性与之相连。这些星型结构的风险节点显示出高度一致的属性和地理位置，暗示可能存在统一控制或关联，特别是涉及敏感服务或高价值交易时，这种风险信号更加显著。通过风险矩阵分析，发现模式一和模式二均存在不同程度的同质化特征，其中模式一的风险评级为A级（高风险），模式二的风险评级为B级（中风险）。针对高风险节点，建议建立冗余机制与实时监控，加强身份验证和访问控制，定期进行安全审计和漏洞扫描，以减少潜在的安全威胁；针对中风险节点，则建议建立冗余机制与实时监控，并定期进行压力测试，以确保不同级别的用户能够平稳运行，同时监控不同地理位置的性能差异。

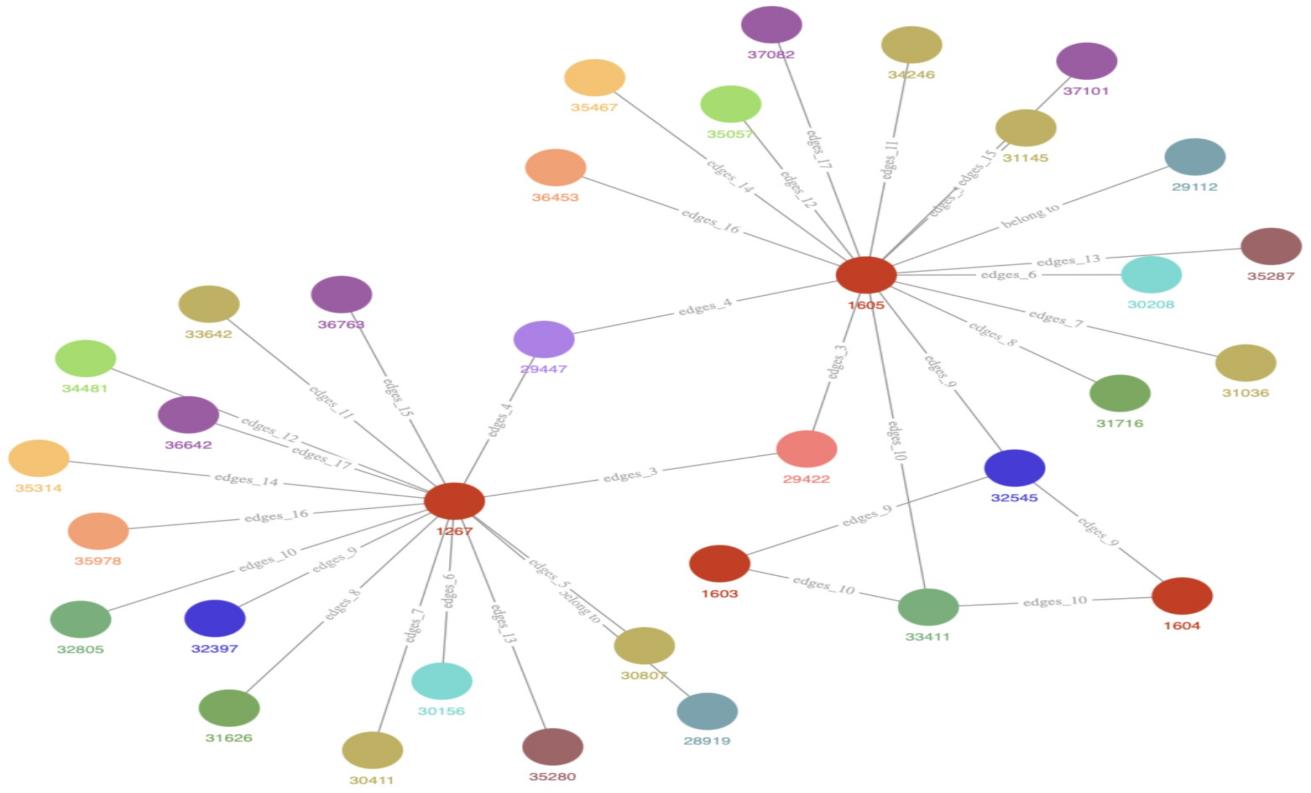


**二、风险子图模式规则信息**

**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为枢纽辐射其他应用节点。理由：应用节点1与其他应用节点（2、3、4）之间存在多个共同属性（如省、市、县等），表明应用节点1在地理位置上是中心点，其他应用节点围绕它分布。同时，应用节点1与其他应用节点之间的关系较为紧密，符合星型拓扑结构的特征。

 **关键属性**：

商户状态与地理位置的一致性。详细分析：在给定的风险子图中，多个应用节点（应用节点1、2、3和4）具有相同的商户状态（正常）和地理位置（省、市、县相同）。特别是应用节点2和应用节点4之间不仅省、市、县相同，结算账户也相同，这可能暗示这些商户之间存在某种关联或统一管理。此外，应用节点1、2、3和4的最后客户等级虽然不同（普通和试用），但它们的其他属性（如是否支持双币卡、在线商户标志和是否多收单机构）均相同，且地理位置高度一致。这种高度一致的属性和地理位置可能表明这些商户背后可能存在统一控制实体，或者存在欺诈行为。

 **风险特征**：

该行业环境中，多个用户节点（1、2、3和4）具有相同属性（正常状态）和地理位置（省、市、县），表明这些用户之间可能存在某种形式的关联或联合管理。同时，用户节点1与其他用户节点（2、3、4）之间存在多个相同属性（如省、市、县），表明用户节点1在地理位置上是中心节点，其他节点围绕其分布。此外，用户节点1与其他用户节点之间的关系较为紧密，符合扇形分布结构的要求。鉴于此，建议建立基于扇形分布结构的防火墙机制，并确保中心节点1的实时监控与压力测试，以防止不同级别用户的异常行为，同时监控不同地理位置的功能差异。

 **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，并定期进行压力测试，以确保不同级别的用户能够平稳运行，同时监控不同地理位置的性能差异。

**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进行跨境交易以规避监管 |
| 商户状态 | 正常 | 占比100% | 正常状态下的商户更容易进行合法合规操作 |
| 在线商户标志 | 未知 | 占比100% | 未知状态可能被用于隐藏真实身份或状态 |
| 是否多收单机构 | 否 | 占比100% | 单一收单机构更容易被监管，多收单机构可能规避集中监管 |
| 最后客户等级 | 普通/试用 | 占比50% | 试用或普通等级客户可能被用于测试或规避特定规则 |

**2. 模式二：法人资质与服务等级异常**

 **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与应用节点2和应用节点3之间有多个共同属性，表明应用节点1可能是核心节点，其他节点通过不同的属性与之相连。这种连接方式符合星型拓扑结构的特点，其中应用节点1作为中心节点，其他节点作为外围节点。

 **关键属性**：

商户发展方集中。详细分析：观察到应用节点1和应用节点2，以及应用节点1和应用节点3之间的商户发展方(dvlpsd)完全一致，且这些节点的结算账户(stl\_acc)、联系人(mchnt\_con)、县(county)也相同。这表明这些节点可能属于同一商户发展方或紧密相关的商户群体。这种高度一致的特征可能暗示存在统一控制或关联，增加了潜在的风险，特别是在涉及敏感服务或高价值交易时。

 **风险特征**：

分析显示，关键风险指标主要集中在会员发送渠道中，且这些渠道的计算代理、交互人数和县区等属性一致，暗示可能存在统一管理或关联性，这种高度一致的风险信号可能源于同一会员发送渠道或安全相关的会员群体。网络结构采用星型结构，以会员1为枢纽节点与其他节点连接，表明会员1可能是中心节点，其他节点通过不同的属性与之相连。这种连接方式符合星型网络结构的特点，其中会员1作为中心节点，其他节点作为外围节点。建议建立基于星型结构的防火墙机制与统一管理策略，并加强实时监控与动态调整，以减少运行中的安全成本。

 **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，加强身份验证和访问控制，定期进行安全审计和漏洞扫描，以减少潜在的安全威胁。

**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** |
| 商户属性 | 普通商户 | 占比100% | 无明显规避手段 |
| 商户应用类型 | 在线旅游,娱乐,零售 | 占比33.33% | 无明显规避手段 |
| 是否特殊服务商户 | 否 | 占比100% | 无明显规避手段 |
| 最后客户等级 | 定制,普通 | 占比50% | 无明显规避手段 |



**四、风险评级与管控建议**

高风险节点（评级A）的核心发现是存在显著的安全威胁。建议采取以下管控措施：建立冗余机制与实时监控，加强身份验证和访问控制，定期进行安全审计和漏洞扫描，以有效减少潜在的安全风险。  
  
中风险节点（评级B）的核心发现是系统在不同用户级别和地理位置上的运行稳定性有待提高。建议采取以下管控措施：建立冗余机制与实时监控，并定期进行压力测试，以确保不同用户级别的稳定运行，并监控不同地理位置的性能差异，从而提升整体系统的运行可靠性。



**五、结论**

关键风险指标主要集中在会员发送渠道中，且这些渠道的计算代理、交互人数和县区等属性一致，暗示可能存在统一管理或关联性，这种高度一致的风险信号可能源于同一会员发送渠道或安全相关的会员群体。网络结构采用星型结构，以会员1为枢纽节点与其他节点连接，表明会员1可能是中心节点，其他节点通过不同的属性与之相连。这种连接方式符合星型网络结构的特点，其中会员1作为中心节点，其他节点作为外围节点。建议建立基于星型结构的防火墙机制与统一管理策略，并加强实时监控与动态调整，以减少运行中的安全成本。  
  
在该行业环境中，多个用户节点（1、2、3和4）具有相同属性（正常状态）和地理位置（省、市、县），表明这些用户之间可能存在某种形式的关联或联合管理。同时，用户节点1与其他用户节点（2、3、4）之间存在多个相同属性（如省、市、县），表明用户节点1在地理位置上是中心节点，其他节点围绕其分布。此外，用户节点1与其他用户节点之间的关系较为紧密，符合扇形分布结构的要求。鉴于此，建议建立基于扇形分布结构的防火墙机制，并确保中心节点1的实时监控与压力测试，以防止不同级别用户的异常行为，同时监控不同地理位置的功能差异。