**攻击者取证报告**



杭州安恒信息技术股份有限公司

${dateM}

目录

[1. 摘要及简报 3](#_Toc513645456)

[1.1. 攻击手段汇总 3](#_Toc513645457)

[1.2. 攻击事件回放 3](#_Toc513645458)

[2. 攻击者行为分析 3](#_Toc513645459)

[2.1. 攻击者信誉度 3](#_Toc513645460)

[2.2. 扫描探查 4](#_Toc513645461)

[2.3. 渗透攻击 4](#_Toc513645462)

[2.4. 获取权限 4](#_Toc513645463)

[2.5. 命令控制 5](#_Toc513645464)

[2.6. 资产破坏 5](#_Toc513645465)

[3. 攻击团伙分析 5](#_Toc513645466)

[3.1. 相似性IP 5](#_Toc513645467)

[3.2. 相似性取证信息 6](#_Toc513645468)

[4. 威胁情报分析 7](#_Toc513645469)

[4.1. 情报信息 7](#_Toc513645470)

[5. 分析结论与建议 8](#_Toc513645471)

[5.1. 分析结论 8](#_Toc513645472)

[5.2. 处置建议 8](#_Toc513645473)

1. **摘要及简报**

攻击者IP: ${attackerIp}

地理信息: ${LAN}

经纬度: ${longitude\_latitude}

运营商: ${operator}

取证周期: ${startdate}--${enddate}

* 1. **攻击手段汇总**

#table\_attackMeansSummary

* 1. **攻击事件回放**

#table\_attackEventPlayback

1. **攻击者行为分析**
   1. **攻击者信誉度**

${attacker\_creditworthiness}分

* 1. **扫描探查**

#table\_scanningProbing

* 1. **渗透攻击**

#table\_penetrationAttack

* 1. **获取权限**

#table\_obtainPermission

* 1. **命令控制**

#table\_commandControl

* 1. **资产破坏**

#table\_assetDestruction

1. **攻击团伙分析**
   1. **相似性IP**

#table\_similarityIP

* 1. **相似性取证信息**

攻击时间的展示如下：

#pic\_attackTime

攻击类型的展示如下：

#content\_attackTypeDisplay

1. **威胁情报分析**
   1. **情报信息**

#maliciousIP

#intelligence

1. **分析结论与建议**
   1. **分析结论**

攻击者IP**${analyzeIP}**在${analyzeStartdate}--${analyzeEnddate}进行了**${analyzeTotal}**次攻击，其中，扫描探查：**${analyzeScanningProbing}**次，渗透攻击：**${analyzePenetrationAttack}**次，获取权限：**${analyzeObtainPermission}**次，命令控制：**${analyzeCommandControl}**次，资产破坏：**${analyzeAssetDestruction}**次。进行的攻击类型多达**${analyzeType}**种。**${analyzeConclusion}**

* 1. **处置建议**

针对此次分析结果的建议如下：