网络安全威胁分析报告

生成时间: 2025-07-09 16:01:56
总事件数: 19843
分析维度: 威胁类别、严重程度、源IP、时间分布等

1. 威胁概览

威胁等级分布:
• severity_4: 15830 起 (79.8%)
• severity_1: 2848 起 (14.4%)
• severity_2: 661 起 (3.3%)
• severity_3: 451 起 (2.3%)
• severity_5: 53 起 (0.3%)

2. 威胁类别分析

• threat-intelligence-alarm: 15110 起 (76.1%)
• weird-behavior: 2545 起 (12.8%)
• tor-network-traffic: 647 起 (3.3%)
• scan: 384 起 (1.9%)
• encrypted-proxy: 303 起 (1.5%)
• trojan-activity: 261 起 (1.3%)
• covert-channel: 176 起 (0.9%)
• malicious-encrypted-traffic: 143 起 (0.7%)
• successful-recon-limited: 131 起 (0.7%)
• policy-violation: 79 起 (0.4%)

3. 常见威胁类型

• malicious-domain-dns-query: 15001 起
• remote-control-tool-identify: 2414 起
• tor-flow-identify: 647 起
• scan: 384 起
• vpn-flow-identify: 303 起
• trojan-remote-control: 216 起
• dns-tunneling: 176 起
• encrypted-traffic-analysis-traffic: 143 起
• successful-recon-limited: 131 起
• penetration-tool-identify: 131 起

4. 主要威胁源分析

涉及源IP总数: 1194

TOP 5 威胁源IP:

- 172.29.31.8: 11248 起
- 172.16.22.227: 3083 起
- 210.30.97.179: 622 起
- 172.29.22.212: 246 起
- 172.16.66.164: 205 起

5. 客户端威胁分析

前五频发的客户端源IP及其威胁统计:

IP: 172.29.31.8 (出现 11248 次)
- [severity_4] malicious-domain-dns-query: 11204
- [severity_3] trojan-mining: 14
- [severity_4] trojan-mining: 28
- [severity_1] remote-control-tool-identify: 2

IP: 172.16.22.227 (出现 3083 次)
- [severity_4] malicious-domain-dns-query: 3082
- [severity_1] scan: 1

IP: 172.29.22.212 (出现 246 次)
- [severity_4] tor-flow-identify: 244
- [severity_1] remote-control-tool-identify: 1
- [severity_3] tor-flow-identify: 1

IP: 172.16.66.164 (出现 205 次)
- [severity_4] trojan-remote-control: 205

IP: 192.168.79.87 (出现 65 次)
- [severity_5] penetration-tool-identify: 53
- [severity_1] remote-control-tool-identify: 11
- [severity_1] scan: 1

6. 服务端威胁分析

前五频发的服务端源IP及其威胁统计:

IP: 210.30.97.179 (出现 622 次)
- [severity_4] malicious-domain-dns-query: 621
- [severity_3] trojan-mining: 1

IP: 210.30.100.9 (出现 192 次)
- [severity_2] vpn-flow-identify: 14
- [severity_4] malicious-domain-dns-query: 84
- [severity_4] web-access-to-malicious-server: 42
- [severity_1] scan: 15
- [severity_1] remote-control-tool-identify: 21
- [severity_1] vpn-flow-identify: 12
- [severity_2] remote-control-tool-identify: 2
- [severity_4] tor-flow-identify: 2

IP: 210.30.97.173 (出现 37 次)
• [severity_1] remote-control-tool-identify: 7
• [severity_4] tor-flow-identify: 29
• [severity_3] tor-flow-identify: 1

IP: 210.30.97.78 (出现 29 次)
• [severity_2] vpn-flow-identify: 15
• [severity_1] vpn-flow-identify: 14

IP: 210.30.96.240 (出现 21 次)
• [severity_1] remote-control-tool-identify: 20
• [severity_2] remote-control-tool-identify: 1

7. 威胁时间分布

24小时威胁事件分布:
• 00:00-01:00: 1209 起
• 01:00-02:00: 1194 起
• 02:00-03:00: 1243 起
• 03:00-04:00: 1054 起
• 04:00-05:00: 1026 起
• 05:00-06:00: 963 起
• 06:00-07:00: 979 起
• 07:00-08:00: 1142 起
• 08:00-09:00: 1388 起
• 09:00-10:00: 1838 起
• 10:00-11:00: 1881 起
• 11:00-12:00: 1522 起
• 12:00-13:00: 1839 起
• 13:00-14:00: 1957 起
• 14:00-15:00: 608 起

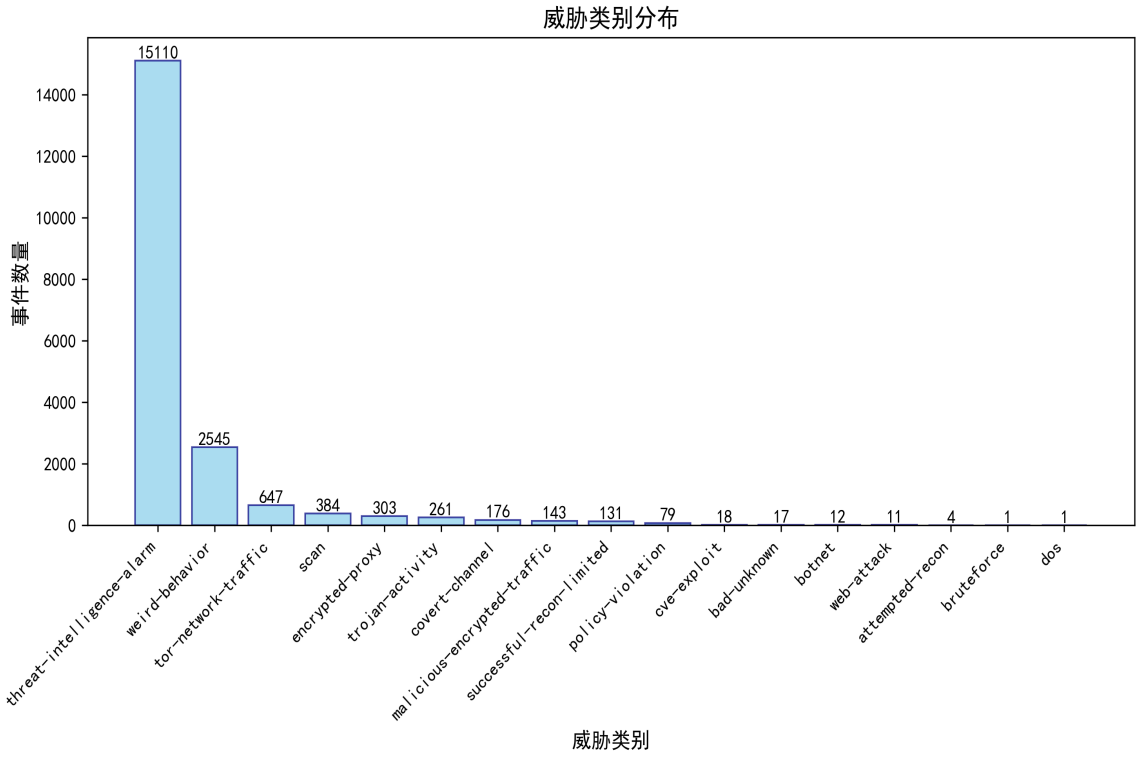
8. 协议与端口分析

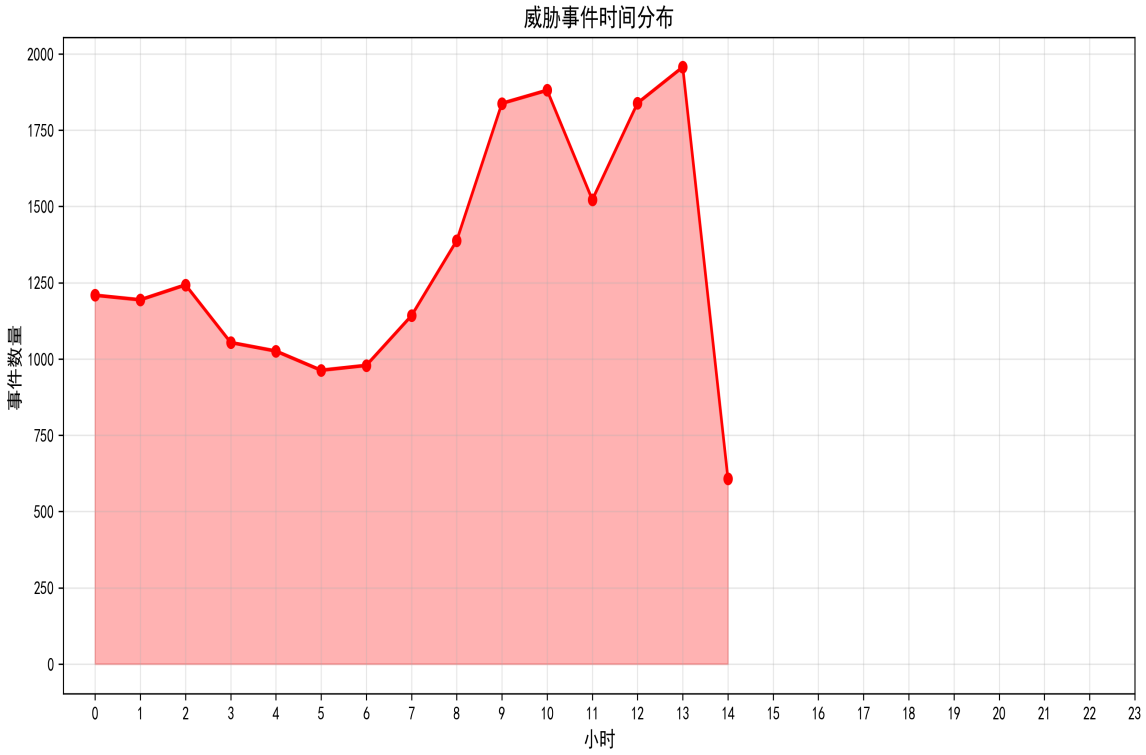
常用协议分布:
• dns: 16684 次
• other: 1324 次
• ssl: 1233 次
• http: 567 次
• pop3: 28 次
• imap: 4 次
• dcerpc: 2 次
• ssh: 1 次

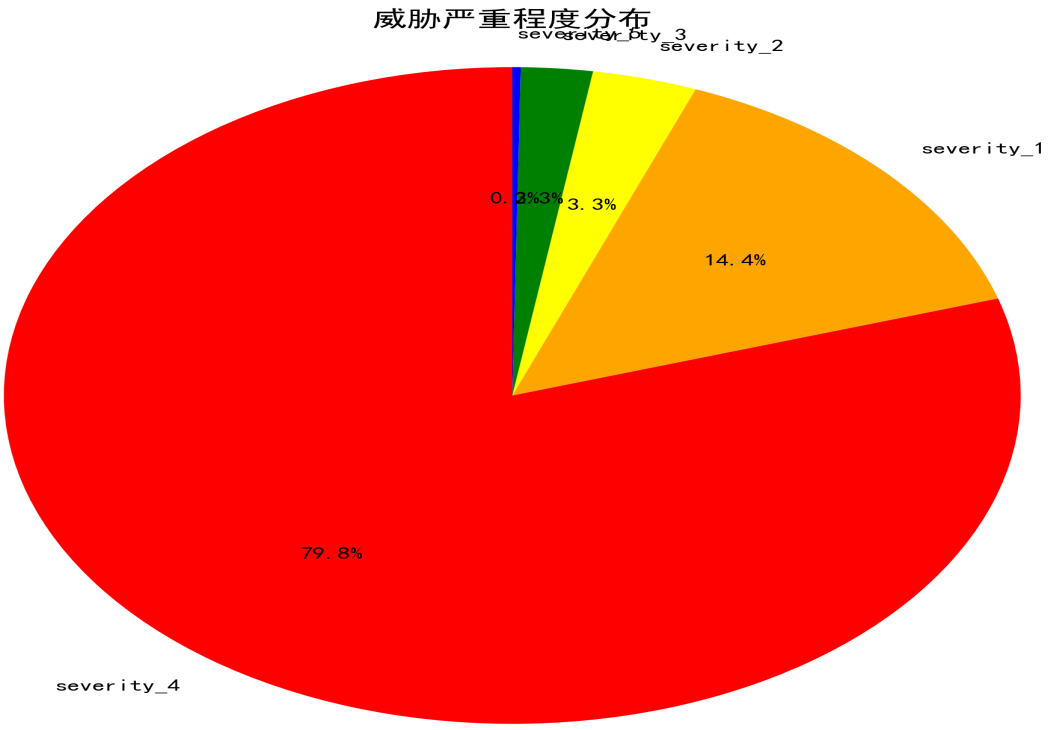
常见目标端口:
• 端口 53: 16684 次
• 端口 443: 1487 次
• 端口 62149: 245 次
• 端口 45: 216 次
• 端口 80: 188 次
• 端口 8081: 122 次

- 端口 19000: 96 次
- 端口 8443: 69 次
- 端口 5995: 58 次
- 端口 10012: 53 次

9. 数据可视化


威胁类别分布
事件数量
威胁类别
15110
2545
647
384
303
261
176
143
131
79
18
17
12
11
4
1
1
threat-intelligence-alarm
weird-behavior
tor-network-traffic
scan
encrypted-proxy
trojan-activity
covert-channel
malicious-encrypted-traffic
successful-recon-limited
policy-violation
cve-exploit
bad-unknown
botnet
web-attack
attempted-recon
bruteforce
dos


威胁事件时间分布
事件数量
小时


威胁严重程度分布
severity_3
severity_2
severity_1
0.3%
3.3%
14.4%
79.8%
severity_4