

Warning signs of predatory, extortionist, and cult style networks

Union of Saints

Below is a broad check list of 200 common tactics and characteristics observed in groups like 764, and in similar predatory or cult style networks. Many items overlap or reinforce each other, this may be used as a practical **red flag list**.

Devoid of humanity, their goals are to harm, destabilize society and to profit off of other's pain and suffering. Somehow, they inspire.

We hope to inspire also, rule of law, redress, correction and consequence.

List of Harms:

1. Targeting children aged ~8-17 as primary victims.
2. Use of popular gaming platforms/social media (e.g., Roblox, Minecraft, Discord) for recruitment.
3. "Love-bombing" or friendly approach at first to build trust.
4. Deception: pretending to be peer, friend, romantic interest.
5. Gradual escalation: initial benign contact leading to more extreme demands.
6. Sextortion: obtaining compromising images/videos of victims.
7. Blackmail and threats if victims refuse to comply.
8. Forcing self-harm (cutting, mutilation, carving symbols).
9. Forcing abuse of animals or pets to prove loyalty or as punishment.
10. Using "branding" or "cutsigns" (victims carve abuser's alias into their body).
11. Use of violent or shocking content as currency within the group.
12. Encouraging or celebrating real-world violent acts, including murders.
13. Use of extremist ideology (neo-Nazism, satanism, nihilism) intertwined with the group narrative.
14. Use of symbolism, rituals, or aesthetic signs to create identity and belonging.
15. Creating an "us vs them" mentality, a distinct identity separate from mainstream society.
16. Targeting vulnerable individuals (mental health issues, minority status, isolated youth).

17. Encouraging victims to recruit other victims or perform “tasks”.
18. Hosting “watch parties” where disturbing content is shared among members.
19. Decentralised structure: many offshoots, splinter groups, names change to avoid detection.
20. Use of encrypted or niche platforms (Telegram, Discord channels, etc).
21. Emphasis on notoriety, clout, status within network for committing worse acts.
22. Violations escalate: from online acts to real-world violence, bomb threats, swatting.
23. Use of doxxing (revealing personal data) or swatting (false police reports) for intimidation.
24. Use of “gamification” of abuse – points, hierarchy, rewards for violence.
25. Manipulation of victim’s sense of identity, self-worth (e.g., “you are special”, “you belong”). (inferred by grooming pattern)
26. Isolation of the victim from other supportive relationships (friends, family). (common in abusive/cult contexts)
27. Coercive control: forcing compliance under threat, overstretching boundaries. (general principle)
28. Blame shifting: victims made to feel complicit (thus trapped). (common tactic)
29. Silence and secrecy: victims instructed not to speak, under threat of exposure. (logical extension of blackmail)
30. Use of peer pressure within the group to enforce conformity and escalation. (fits list)
31. Encouraging shame and humiliation as a tool of control. (humiliation tactic)
32. Use of symbols or tattoos to mark members or victims (‘branding’).
33. Encouraging self-destructive behaviours (cutting, suicide attempts) to deepen entrapment.
34. Targeting the family/friends of victims as leverage. (some mention of threats to victims’ families)
35. Use of live streaming to escalate terror and status.
36. Co-optation of youth culture (gaming, social media) to make recruitment seamless. (fits pattern)
37. Escalation in demands: what starts small becomes extreme quickly. (already included as #6)
38. Use of anonymity and pseudonyms so perpetrators feel safe. (common)
39. Use of shock and gore to desensitise participants and victims.

40. Messaging suggesting rebellion, anti-societal goals (“bring down society”, chaos).
41. Use of trauma bonding: linking victim’s suffering to loyalty to the group. (inferred)
42. Creating dependency: victim becomes dependent on abuser for “acceptance”. (inferred)
43. Blurring of boundaries between victim and perpetrator (victims turned recruiters).
44. Targeting multiple jurisdictions globally, crossing borders.
45. Use of digital currency or dark-web transactions (for CSAM or extortion).
46. Use of “lorebooks” or manuals to recruit and incite violence.
47. Use of extremist ideology as a veneer—but underlying motivation often sadism or power.
48. Affiliation with other extremist groups/networks for legitimacy or structure.
49. Encouraging victims to commit crimes (hacking, bomb threats, weapons) as proof of loyalty.
50. Use of peer-ranking or status lists (“who has done the worst act”). (implied)
51. Encouraging escape from normal moral constraints (“we are beyond good & evil”). (deduced from nihilistic framing)
52. Exploiting moral disengagement (“It’s just a game”, “It’s just online”) to normalise abuse. (common)
53. Use of manipulation of trauma or vulnerability (victim’s prior abuse, isolation) to recruit.
54. Promoting self-harm or suicide ideation among victims to keep them compliant.
55. Use of threats of exposure (public shame, posting images) to control victims.
56. Using branding (victim marks, group tags) so victims carry permanent reminder of group. (#11/#33)
57. Encouragement of hatred of society/institutions, anti-authority messages.
58. Use of live streaming or real-time videos to heighten terror and evidencing. (#36)
59. Adoption of multi-media content (videos, images, chat, games) to reinforce message. (fits pattern)
60. Use of chilling or shocking rituals (animal killing, self-mutilation) to bond members. (#10, #34)
61. Elevating the worst acts to insider status; “badge of honor” for cruelty.
62. Victims often come from oppressed/minority backgrounds or mental-health issues. (#17)

63. Use of peer competition (who can do more) to escalate harm. (#22/#51)
64. Use of internet and digital anonymity to facilitate abuse, avoid physical presence. (#40)
65. Encouraging infiltration of mainstream youth spaces (gaming, chat) rather than obvious extremist channels. (#37)
66. Strategic use of fear and shame rather than overt physical force (initially). (common grooming pattern)
67. Use of legal or quasi-legal threats (exposure, police, media) for compliance. (#8)
68. Use of facilitator/leaders who remain hidden or protected behind layers of chat/alias. (#20)
69. Rapid evolution of group identity/name to avoid crackdown. (#20)
70. Promotion of chaotic worldview; denial of meaning or morals (nihilism). (#48)
71. Use of peer communities to normalise and reinforce behaviour (group culture). (common)
72. Use of self-harm or abuse as rite of passage for member admission. (#34)
73. Encouraging victims to become perpetrators, thus internalising the culture. (#44)
74. Use of trophying: storing graphic content as proof of compliance.
75. Engagement in real-world terror plots or violence beyond sexual abuse. (#23, #50)
76. Use of past mass-casualty attacks and extremist iconography for inspiration. (#41)
77. Use of covert communication (hidden servers, encrypted chats). (#21)
78. Cultivation of charismatic “leaders” or figureheads (even if young) who lure others. (cult-pattern)
79. Use of rituals or pseudo-religious elements to deepen control. (#14/#15)
80. Use of network effect: each member recruits or influences others. (#18)
81. Use of shame/guilt to trap victims (“you owe us now”, “you betrayed the group”). (common)
82. Use of false empowerment of victim (“you are part of something powerful”) to gain loyalty. (grooming)
83. Use of technology to bypass spatial boundaries—global spread, asynchronous abuse. (#45)
84. Use of private communities that glorify horror, elevate cruelty as status. (#22/#62)
85. Use of blackmail data or CSAM as a currency of control. (#7/#46)
86. Use of “norms” within the group that reward cruelty, punish disobedience. (implied)

87. Use of moral inversion—evil is framed as good, or strength, while normalcy is weak. (common in extremist/cult)
88. Use of hierarchical structures even if informal—who's "in", who's "out". (cult pattern)
89. Use of external-looking symbols (tattoos, logos, aliases) to cement identity. (#15/#33)
90. Encouraging victims' cut ties with family/support (isolation). (#27)
91. Use of directed content creation by victims (forcing them to produce videos/images). (#7/#8)
92. Use of peer-reinforced propaganda (group members share deviant content to normalise). (#60)
93. Use of monitoring of victims to ensure compliance (threat of exposure). (#30)
94. Use of escalation loops: each new act must be worse to satisfy group. (#38/#22)
95. Use of internal ideology that includes destruction of societal norms/institutions. (#41)
96. Use of manipulation of trauma and psychological vulnerabilities to recruit and control. (#54)
97. Use of fear of being exposed, punished, or abandoned by the group as coercion. (#26/#82)
98. Use of ambiguous or shifting ideology so that beliefs are secondary to obedience. (#48)
99. Use of "safe spaces" façade (gaming, fun) to hide predation behind normal activities. (#37)
100. Grooming online.

List of 100: Similar but with other details of interest.

1. Secrecy around membership and activities.
2. Heavy emphasis on absolute loyalty to leaders.
3. Leader worship, unquestioned authority.
4. Rapid escalation from friendly contact to intense pressure.
5. Love bombing followed by withdrawal.
6. Isolation of members from outside friends and family.
7. Encouraging dependence on the group for identity.
8. Frequent use of guilt and shame to control behavior.
9. Gaslighting, denying reality to undermine confidence.

10. Rewriting or distorting past events to control narrative.
11. Recruiters who target vulnerable people.
12. Grooming through incremental commitments.
13. Financial exploitation of members.
14. Mandatory donations or payment tiers.
15. Pay to participate events or trainings.
16. Hidden fee structures and surprise fines.
17. Debt bondage and coerced labor.
18. Confiscation or strong pressure to hand over documents.
19. Coerced signatures on contracts or NDAs.
20. Legal threats used to silence critics.
21. Frequent use of gag orders or intimidation letters.
22. Use of private investigators to follow targets.
23. Organized doxxing of opponents.
24. Smear campaigns to discredit dissenters.
25. Coordinated online harassment and trolling.
26. Sock puppet accounts to manufacture support.
27. Astroturfing, fake grassroots campaigns.
28. Controlled or captive media channels.
29. Pressuring mainstream journalists, threatening lawsuits.
30. Creating front organizations or charities.
31. Shell companies to hide ownership.
32. Money laundering through opaque transactions.
33. Use of offshore accounts and complex corporate webs.
34. Reliance on cryptocurrency or untraceable transfers.
35. Fake credentials, bogus experts, and staged endorsements.
36. Rapid promotion of insiders with little transparency.
37. Rituals or ceremonies that enforce belonging.
38. Use of coded language to exclude outsiders.
39. Blackmail using private or fabricated information.

40. Encouraging members to spy on each other.
41. Compartmentalization of tasks and knowledge.
42. Frequent, long meetings that exhaust members.
43. Sleep and nutrition disruption used to lower resistance.
44. Frequent public confessions to control narrative.
45. Loyalty tests and public shaming for failure.
46. Threats to members' families to enforce obedience.
47. Recruiting children or using minors as leverage.
48. Sexual exploitation framed as loyalty or ritual.
49. Sexual relationships dictated by leadership.
50. Medical coercion or pressuring members about care.
51. Surveillance, both digital and physical.
52. Mandatory apps, trackers, or reporting systems.
53. Phone and computer monitoring, requested passwords.
54. Extreme secrecy about financing and budgets.
55. Selective transparency to insiders only.
56. Punishments that escalate for speaking out.
57. Cultivating paranoia about the outside world.
58. Claims of unique, exclusive truth or mission.
59. Framing critics as enemies or traitors.
60. Recruiting through deception or false job offers.
61. Fake job postings to funnel people in.
62. Training that normalizes unethical conduct.
63. Exploiting legal loopholes and regulatory gaps.
64. Strategic litigation to drain resources of opponents.
65. Capture or targeted influence of local officials.
66. Bribery and corruption to secure protection.
67. Infiltration of nonprofits, schools, and institutions.
68. Grooming journalists and influencers to spread narratives.
69. Covert partnerships with other bad actors.

70. Creating dependency on group controlled services.
71. Withholding vital services as punishment.
72. Shifting blame to scapegoats within or outside group.
73. Rapid turnover of policies to confuse outsiders.
74. Collecting compromising material for leverage.
75. False flag operations to justify retaliation.
76. Staging crises to bond members and raise funds.
77. Recruiting through appeals to fear and scarcity.
78. Promises of elite status for recruits who comply.
79. Promoting paranoia, suggesting external conspiracy.
80. Use of cult of victimhood to generate sympathy.
81. Training members to lie or evade investigators.
82. Normalizing small illegal acts that escalate over time.
83. Reinterpretation of laws to suit group aims.
84. Intentionally creating plausible deniability.
85. Use of proxy actors to distance leadership from harm.
86. Violence or threats as an implied enforcement tool.
87. Encouraging members to sever legal counsel ties.
88. Rapid rebranding when exposed.
89. Controlling narrative after exits, coercing retractions.
90. Encouraging members to report on private conversations.
91. Creating rivalries to distract and divide.
92. Rewarding informants within the group.
93. Selective charity used as reputation laundering.
94. Myth making about founders to legitimize power.
95. Tactical use of religion or ideology to justify acts.
96. Training in manipulation and persuasion techniques.
97. Recycling rhetoric to recruit imitators and expand reach.
98. Profit motives entwined with political or social aims.
99. Inspiring copycats who replicate tactics elsewhere.

100. Obfuscating accountability so penalties remain insufficient.