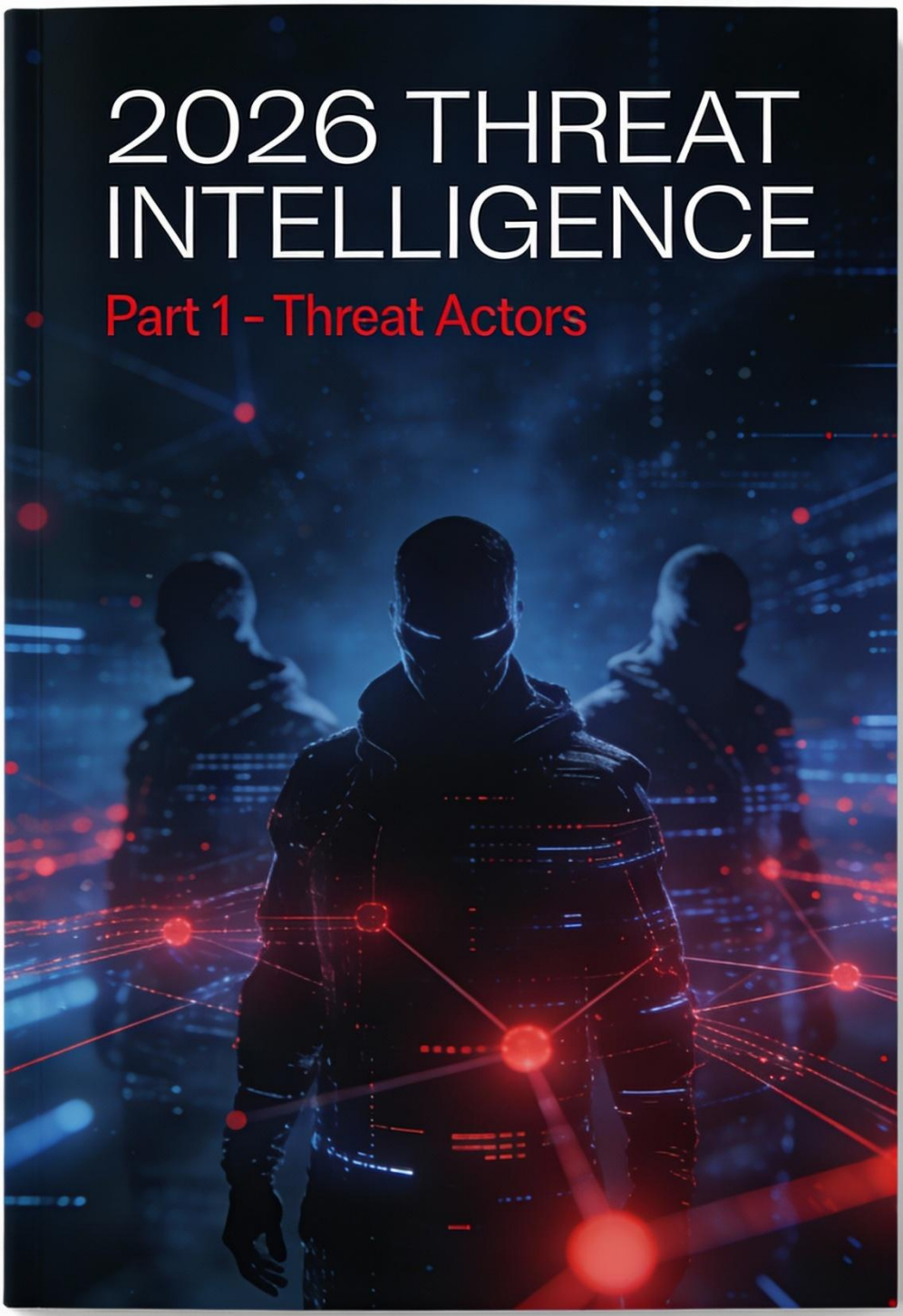
2026 THREAT INTELLIGENCE

Part 1 - Threat Actors



2026 Threat Intelligence

Part 1 - Threat Actors

Santosh Pandit

London, 16 December 2025

"If you know the enemy and know yourself, you need not fear the result of a hundred battles."

- Sun Tzu, *The Art of War*

Contents

Important Disclaimers:

Dear Friends, Followers and Readers,

All views in this article are based on my independent research and the experience of managing my own infrastructure.

My views may not be necessarily shared by my past or current employers. Errors and omissions are solely mine.

I do not expect fellow professionals to agree with my identification of threat actors and forecasts such as re-emergence of GOATs. However, I would request you to conduct your own analysis and identify threat actors that are most relevant to your own industry (e.g. healthcare or power plants).

I would prefer you produce a different list than doing no research at all. Feedback is welcome and DMs are always open.

Eternally yours,

Santosh Pandit

Glossary

CNI (Critical National Infrastructure): Essential systems like power plants, utilities, and transportation critical to national security.

GOAT (in cyber threat context): Greatest Of All Time; refers to highly resilient, long-lasting threat actors like Emotet.

IAB (Initial Access Broker): Actor selling or providing initial network access to other cybercriminals.

N-Day attacks: Exploitation of known vulnerabilities that have existing patches available.

RaaS (Ransomware-as-a-Service): Business model where ransomware tools and infrastructure are rented to affiliates.

Supply Chain Compromise: Attack targeting third-party vendors or software to indirectly breach primary targets.

Threat Actor: Individual or group conducting cyber attacks.

TLPT (Threat-Led Penetration Testing): Simulated attacks based on specific real-world threat actors' TTPs.

TTPs (Tactics, Techniques, and Procedures): Methods and processes used by threat actors in attacks.

Zero-Day attacks: Exploitation of undisclosed vulnerabilities with no available patch.

2026 Forecast

Over the last five years, global authorities have coordinated, arrested, and disrupted a number of criminal gangs. But there have been resurrections, consolidations and arrival of new, younger and linguistically proficient threat actors.

The volume of attacks on my own infrastructure was low in the first three quarters of 2025 but has picked up in Q4. There were signs of greater sophistication and opportunistic probes throughout the year.

I expect 2026 to be a year of accelerated attacks. While Zero-Day attacks will continue to test the depth of our multi-layer cyber defences, my bigger worry is about N-Day attacks. Every healthcare, defence, aerospace, power or other critical business, will be forced to revise their patching and vulnerability management practices.

In this Part 1 report, I have tried to identify which cyber groups pose the greatest disruptive potential over the next year (or two), ranked by estimated impact based on 2025 activity, adaptability, and trends like AI integration. Top risks stem from resilient Ransomware-as-a-Service (RaaS) operators like LockBit and Qilin, alongside emerging destructive actors.

This list is not exhaustive but provides a prioritised framework for threat-focused defence planning. Without identifying and ranking potential adversaries, the asymmetric nature of cyber threats makes effective defence significantly harder.

Methodology

This prioritisation is based on 2025 activity patterns, adaptability indicators, operational resilience following law enforcement actions, and emerging trends such as AI integration. The goal is to help friends and followers focus defensive resources where they matter most.

Priority Threat Actors

Tier 1: Critical Priority

LockBit (Fifth Generation)

2025 Activity: Despite major law enforcement action in 2024, LockBit resurfaced in 2025 with its fifth iteration, declaring intent to target critical infrastructure including power plants. The group has emphasised supply chain compromises and demonstrated remarkable resilience, with affiliates continuing operations post-takedowns.

2026 Forecast: LockBit has consistently risen from disruption attempts by authorities. In 2026, all critical national infrastructure (CNI) should test defences against cumulative LockBit tactics, techniques, and procedures (TTPs) and monitor for innovation, especially AI-enhanced lateral movement. High disruptive potential due to proven resilience and critical infrastructure focus.

Qilin

2025 Activity: The most active group in June and July 2025, Qilin introduced innovative psychological tactics including a "Call Lawyer" feature. The group was notably exploited by a North Korean state actor and targeted by Europol for supply-chain attacks. Over 700 attacks recorded, with activity escalating amid RansomHub disruptions.

2026 Forecast: Qilin will likely continue aggressive operations in 2026, potentially incorporating AI for victim negotiation and data prioritisation. Expect continued innovation in psychological pressure tactics.

Lazarus Group

2025 Activity: This North Korean-linked actor blends cybercrime (for revenue generation) with espionage and sabotage. Notably observed exploiting Qilin ransomware in 2025, showcasing a hybrid criminal-state tactic involving both financial and espionage sectors.

2026 Forecast: A critical consideration for every Threat-Led Penetration Testing (TLPT) exercise, especially in AI arms race contexts. The convergence of state-sponsored capabilities with ransomware operations represents a concerning evolution.

Tier 2: High Priority

RansomHub

2025 Activity: Ended 2024 as the top ransomware group with 736 victims, attracting elite affiliates from LockBit and BlackCat. Activity decreased significantly in early 2025 with few victims after April, though the group's infrastructure remained involved in affiliate migrations.

2026 Forecast: Despite arrests and disruption, RansomHub's previous success suggests continued operations, possibly under rebranded identities. The group represents a resilient threat actor network that may splinter but not disappear.

Cl0p

2025 Activity: Master of large-scale zero-day exploits, notably the MOVEit vulnerability. Responsible for over one-third of attacks in H1 2025, though activity fluctuated dramatically quarter-to-quarter.

2026 Forecast: As long as organisations continue using vulnerable file transfer applications, Cl0p will remain active. The continued prevalence of internet-facing file transfer services provides an abundant attack surface. Monitor port scans on your own infrastructure as an early warning indicator.

Akira

2025 Activity: Extremely active and profitable throughout 2025 with no signs of slowing. Part of the industrialised RaaS ecosystem with consistent victim acquisition.

2026 Forecast: As long as vulnerable firewalls and VPNs remain deployed, Akira (or its successors) will continue operations. The group has demonstrated effective exploitation of edge security devices.

Tier 3: Elevated Watch

DragonForce

2025 Activity: Rapidly rising threat with attacks surging 212.5% in June 2025. Aggressively recruits affiliates on dark web forums, demonstrating strong operational growth.

2026 Forecast: Expect continued rise with potential AI adoption for recruitment and targeting operations. The group's aggressive expansion suggests ambitions to join the top tier of ransomware operators.

Anubis

2025 Activity: Features destructive file-wiping capabilities with "Robin Hood" style public shaming. Unlike profit-motivated groups, Anubis prioritises ideological destruction over financial gain.

2026 Forecast: In an increasingly polarised world, ideologically driven destruction poses unique risks. Unlike financially motivated actors requesting ransom, Anubis may cause irreversible damage without offering decryption.

Play

2025 Activity: Known for targeting government agencies and critical infrastructure in Latin America and Europe. Activity dropped 31.8% in June 2025 but maintains focus on geopolitically sensitive targets.

2026 Forecast: Likely to remain active with potential escalation in hybrid warfare contexts, particularly in regions of geopolitical tension.

Scattered LAPSUS$ Hunters (SLH)

2025 Activity: Despite arrests in 2025, diffused alliances effectively continue the legacy of Scattered Spider (aka UNC3944, Octo Tempest), LAPSUS$, and ShinyHunters. Notable for human supply chain coercion tactics.

2026 Forecast: As long as IT service desks remain vulnerable to social engineering by native English speakers, these domestic threat actors will persist. The "Trojan Horse" approach of exploiting trusted internal processes remains effective.

Emotet (Modern Iteration)

2025 Activity: Operating in the background as an Initial Access Broker (IAB), supporting botnet operations and providing entry points for other threat actors.

2026 Forecast: One of the most resilient threat actors over the past two decades. It is in my view a GOAT and I say that without glorifying what they do. While currently playing a supporting role, Emotet could return to frontline operations. Don't underestimate this established botnet infrastructure.

Emerging Trends for 2026

AI Acceleration: Threat actors will deploy AI agents for autonomous attacks, compressing attack timelines from days to hours. Defenders must counter with AI-driven security operations to maintain detection capabilities.

Industrialisation and Convergence: Cybercrime continues evolving into enterprise-scale operations, merging with fraud and trafficking networks. The 50% ransomware increase validates this trend toward professionalisation.

Critical Infrastructure Focus: Geopolitical tensions will drive increased attacks on utilities, transportation, and communication infrastructure. Resilience planning becomes essential.

Supply Chain, Zero-Day and N-Day Exploitation: Continued targeting of third-party relationships and vulnerability exploitation, as evidenced throughout 2025 advisories.

Threat Actor Comparison Matrix

Threat Actor	2025 Activity Level	Key Target Sectors	2026 Impact Forecast
LockBit	High (affiliate migrations)	Critical Infrastructure, Supply Chain	Critical
Qilin	Very High (700+ attacks)	Multi-sector, Supply Chain	Critical
Lazarus	High (hybrid operations)	Espionage, Financial	Critical
RansomHub	Decreased but resilient	Multi-sector	High
Cl0p	High (1/3 of H1 attacks)	File Transfer Applications	High
Akira	Very High	Firewalls, VPNs	High
DragonForce	Rapidly Rising (212.5% growth)	Multi-sector	Medium-High
Anubis	Emerging	Ideological Targets	Medium-High
Play	Medium (31.8% decrease)	Government, CNI (LatAm/Europe)	Medium
SLH Alliance	Persistent	IT Service Desks	Medium
Emotet	Medium (IAB role)	Access Brokerage	Medium

Annex: References and Citations

(Note: All links were working on 16 Dec 2025, except where stated. If you are unable to access original articles, please use the Internet Archive, Google dork, or 404wayback.)

Threat Actor Profiles and 2025 Activity

Primary Threat Actors Referenced

LockBit (Fifth Generation)

- Breached.co. (2025, November 16). The Ransomware-as-a-Service Ecosystem in Late 2025: From LockBit's disruption to the rise of Qilin, Akira, and beyond. Retrieved from https://breached.company/
- Quorum Cyber. (2025, January 30). LockBit ransomware operation disrupted by global law enforcement agencies - Operation Cronos. Retrieved from https://www.quorumcyber.com/insights/lockbit-ransomware-operation-disrupted-by-global-law-enforcement-agencies/
- UK National Crime Agency (NCA), FBI, Europol, et al. (2024). Operation Cronos: Global disruption of LockBit ransomware infrastructure. Retrieved via international law enforcement coordination announcements. https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos .

Qilin

- Industrial Cyber. (2025, October 26). Qilin ransomware escalates rapidly in 2025, targeting critical sectors with 700+ attacks and AMTI implications. Retrieved from https://industrialcyber.co/ransomware/qilin-ransomware-escalates-rapidly-in-2025-targeting-critical-sectors-with-700-attacks-ami/
- Moody, R., Comparitech. (2025). (Note: They have many related articles. Here is one link). https://www.comparitech.com/news/qilin-ransomware-stats-on-attacks-ransoms-data-breaches/

Lazarus Group

- Brand Defense. (2025, October 16). The Lazarus Group: Espionage, Sabotage, and Cybercrime Under State Sponsorship. Retrieved from https://brandefense.io/blog/lazarus-group/
- Cyble. (2025). They have many articles on Lazarus including this one. https://cyble.com/threat-actor-profiles/lazarus-group/

RansomHub

- Trend Micro. (2024, December 19). Ransomware Spotlight: RansomHub - Attack chains, initial access vectors, and operational tactics. (Cautionary note: I cannot include links to Trend Micro articles as my browser and antivirus are giving me a warning. I suggest you use Google dork in a sandboxed browser. Trend Micro has tons of useful articles).
- AttackIQ. (2025, March 6). Emulating the Relentless RansomHub Ransomware: RaaS model analysis and attack graph development. Retrieved from https://www.attackiq.com/2025/03/06/emulating-ransomhub/

Cl0p

- ORX. (2025, February 28). MOVEit Transfer Data Breaches Deep Dive: SQL injection zero-day exploitation campaign analysis. Retrieved from https://orx.org/resource/moveit-transfer-data-breaches
- Cybersecurity News. (2025, September 19). Top Zero-Day Vulnerabilities Exploited in the Wild in 2025. Retrieved from https://cybersecuritynews.com/popular-zero-day-vulnerabilities/

Akira

- Wikipedia. (2024, October 14). Akira (ransomware). Retrieved from https://en.wikipedia.org/wiki/Akira_(ransomware)
- DeepStrike. (2025, December 7). Ransomware Statistics 2025: Trends, Costs, and Key Threats. Retrieved from https://deepstrike.io/blog/ransomware-statistics-2025

DragonForce

- PointWild. (2025, October 16). DragonForce Ransomware: Threat intelligence analysis and operational capabilities. Retrieved from https://www.pointwild.com/threat-intelligence/dragonforce-ransomware
- Check Point. (2025, May 7). DragonForce Ransomware: Redefining Hybrid Extortion in 2025 - Analysis of white-label services and Ransom Bay infrastructure. Retrieved from https://blog.checkpoint.com/security/dragonforce-ransomware-redefining-hybrid-extortion-in-2025/
- Check Point. (2025, November 12). The State of Ransomware – Q3 2025: Data leak site analysis and monthly victim trends. Retrieved from https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/

Anubis

- Thai CERT. (2025, June 18). Anubis Ransomware Encrypts and Wipes Data, Making Recovery Impossible Even After Ransom Payment. Retrieved from https://www.thaicert.or.th/en/2025/06/18/anubis-ransomware-encrypts-and-wipes-data-making-recovery-impossible-even-after-ransom/
- Trend Micro. (2025). https://www.trendmicro.com/pt_br/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html and related articles. (Note: switch language to English if needed)

Play

- Wikipedia. (2023, June 16). Play (hacker group). Retrieved from https://en.wikipedia.org/wiki/Play_(hacker_group)
- Cybersecurity News. (2025, September 19). Top Zero-Day Vulnerabilities Exploited in the Wild in 2025: Play ransomware group operational activity. https://cybersecuritynews.com/popular-zero-day-vulnerabilities/

Scattered LAPSUS$ Hunters (SLH)

- Picus Security. (2025, October 16). Scattered LAPSUS$ Hunters: 2025's Most Dangerous Cybercrime Supergroup - Analysis of supergroup

formation and integrated attack tactics. Retrieved from https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup

- ReliaQuest. (2025, June 4). Scattered Spider Cyber Attacks Using Phishing and Social Engineering: Help-desk exploitation and managed service provider targeting. Retrieved from https://reliaquest.com/blog/scattered-spider-cyber-attacks-using-phishing-social-engineering-2025/
- ZeroFox. (2025, November 20). Flash Report: Powerful New RaaS from Scattered Lapsus$ Hunters - ShinySp1d3r development and RaaS platform capabilities. Retrieved from https://www.zerofox.com/intelligence/flash-report-powerful-new-raas-from-scattered-lapsus-hunters/

Emotet

- Radware. (2024, December 31). The Emotet Threat in 2025: Anatomy, Attack Examples & Defense - Initial Access Broker role and botnet infrastructure. Retrieved from https://www.radware.com/cyberpedia/bot-management/emotet-anatomy-examples-and-defense/

Emerging Trends and 2026 Forecasts

AI in Cybercrime

- Intelligence X. (2025, December 1). How Artificial Intelligence Weaponized Cybercrime in 2025: PromptLock, agentic AI, and autonomous attack systems. Retrieved from https://blog.intelligencex.org/ai-powered-ransomware-attacks-2025-artificial-intelligence-cybercrime

Supply Chain Attacks

- Industrial Cyber. (2025, November 6). Software Supply Chain Attacks Surge: Ransomware groups escalate targeting, with industrial sectors facing elevated exposure. Retrieved from https://industrialcyber.co/reports/software-supply-chain-attacks-surge-as-ransomware-groups-escalate-and-industrial-sectors-face/
- Cyble. (2025, December 1). Cyble's 2025 Threat Predictions Proven True: 2026 Insights - Supply chain targeting expansion and geopolitical

drivers. Retrieved from https://cyble.com/knowledge-hub/cybles-2025-threat-predictions/

Critical Infrastructure Targeting

- Dataminr. (2025, December 10). Dataminr's 2026 Cyber Predictions: What We See Coming - Systemic disruption forecasts and logistics/manufacturing focus. Retrieved from https://www.dataminr.com/resources/blog/dataminrs-2026-cyber-predictions-what-we-see-coming/

Vulnerability Exploitation Trends

- Cybersecurity News. (2025, September 19). Top Zero-Day Vulnerabilities Exploited in the Wild in 2025: Zero-day exploitation velocity and sophisticated attack chains. Retrieved from https://cybersecuritynews.com/popular-zero-day-vulnerabilities/
- DeepStrike. (2025, October 7). Vulnerabilities Statistics 2025: CVE Surge & Exploit Speed - Weaponization timelines and patch Tuesday effectiveness analysis. Retrieved from https://deepstrike.io/blog/vulnerability-statistics-2025

Ransomware Statistics and Impact

- DeepStrike. (2025, December 7). Ransomware Statistics 2025: Trends, Costs, and Key Threats - Attack volume surge, payment rate decline, and recovery cost analysis. Retrieved from https://deepstrike.io/blog/ransomware-statistics-2025
- Check Point. (2025, November 12). The State of Ransomware – Q3 2025: Data leak site metrics and long-term law enforcement impact assessment. Retrieved from https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/

2026 Cybersecurity Forecasts

Fortinet Cyberthreat Predictions

- Fortinet. (2025). Cyberthreat Predictions for 2026 - Acceleration, industrialization, and AI-enabled autonomous cybercrime agents. Retrieved from https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-predictions-2026.pdf

- LinkedIn. (2025, October 1). Fortinet & Cybersecurity Challenges Going Into 2026 - AI/ML-driven detection and prevention requirements. Retrieved from https://www.linkedin.com/pulse/fortinet-cybersecurity-challenges-going-2026-insoftservices-gzqqc

Google Cloud Cybersecurity Forecast 2026

- Google Cloud. (2025, December 14). Google Cloud's 2026 Forecast: AI to Amplify Cyber Threats and Defenses - AI-enhanced attacks, identity threats, and defender capabilities. Retrieved from https://www.webpronews.com/google-clouds-2026-forecast-ai-to-amplify-cyber-threats-and-defenses/
- Mandiant & Google Security Teams. (2025). Cybersecurity Forecast 2026: Insights on nation-state operations, virtualized environments, and blockchain targeting. (Related pdf is here)

Cyble 2025-2026 Predictions

- Cyble. (2025, December 1). Cyble's 2025 Threat Predictions Proven True: 2026 Insights - Accurate forecasts on ransomware adaptation, cloud targeting, and infrastructure attacks. Retrieved from https://cyble.com/knowledge-hub/cybles-2025-threat-predictions/

Industry References

ENISA (European Union Agency for Cybersecurity)

- ENISA. (2025, October). ENISA Threat Landscape 2025. Retrieved from https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf

Copyright and License