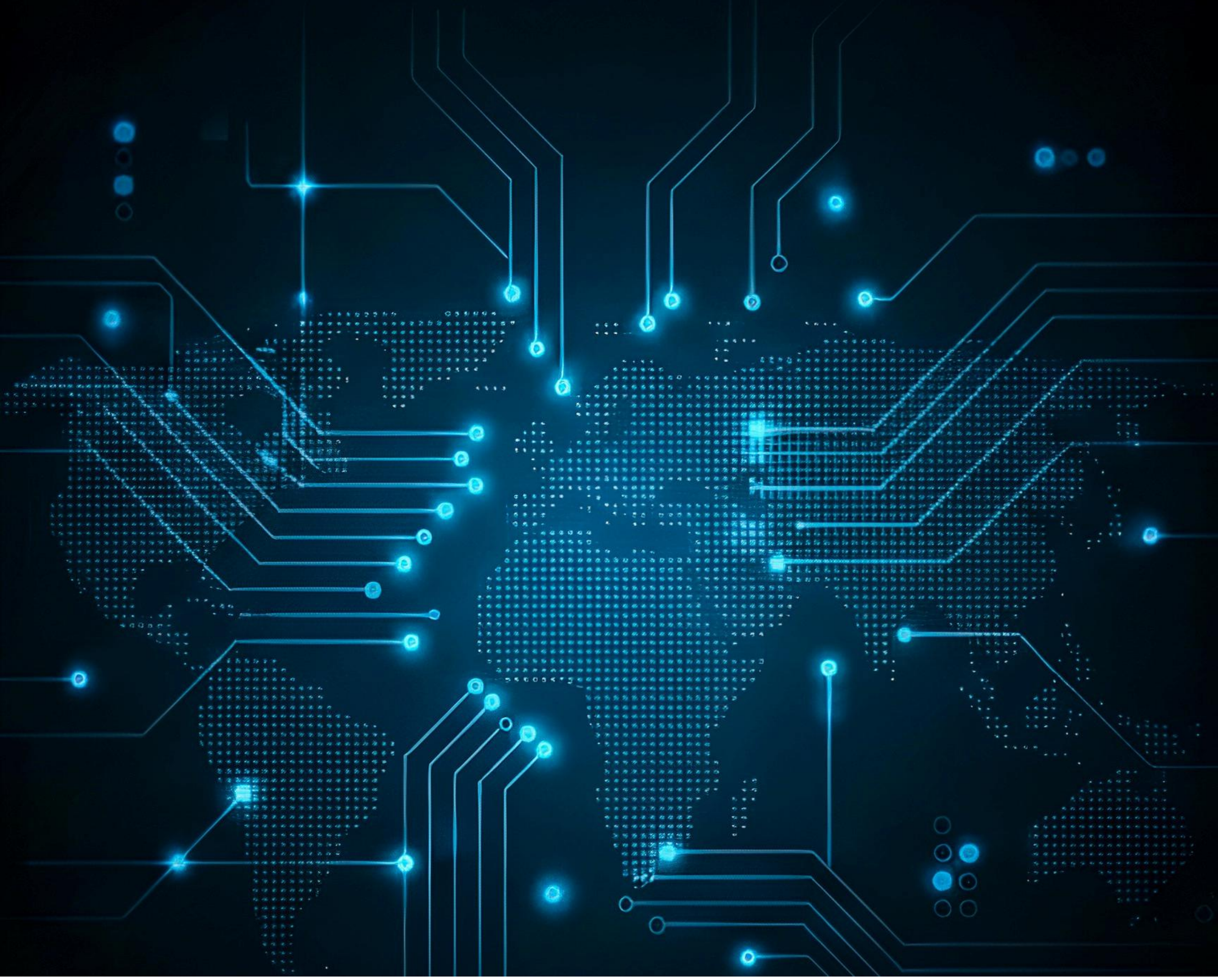
2026 THREAT INTELLIGENCE

Part 2 - Innovations in TTP Systems



2026 Cyber Threat Intelligence

Part 2 - Innovations in TTP Systems

Santosh Pandit

London, 20 December 2025

"If you know the enemy's tactics, you can adapt before the battle begins."

- *Adapted from 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 the professionalisation of reputational extortion. However, I would request you to conduct your own analysis and identify threat actors and TTP systems that are most relevant to your own industry (e.g., healthcare, power plants, financial services, supply chain vendors).

This is what I truly believe. Failure to anticipate your enemy's evolution is plan to fail.

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

Agentic AI: Autonomous AI systems executing multi-step attacks with reasoning capabilities, adaptive decision-making, and minimal human intervention. Distinct from orchestrated script automation.

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

Deepfake: Synthetic media (audio/video) created using generative AI to impersonate real individuals.

EDR (Endpoint Detection and Response): Security software that monitors endpoints for malicious behaviour and responds to threats.

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.

LotC (Living Off the Cloud): Techniques leveraging cloud-native features and API abuse for attacks without deploying traditional malware.

MTTR (Mean Time to Respond): Average time from detection to containment of a security incident.

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.

Snow Features: Small, seemingly harmless code additions designed to poison machine learning models in security tools. Think of the reduced visibility when you are driving under snowfall.

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.

TTP (Tactics, Techniques, and Procedures): Methods and processes used by threat actors.

TTP System: Integrated combinations of TTPs forming coherent, resilient attack chains deployed by sophisticated threat actors.

VaaS (Vishing-as-a-Service): Voice phishing services using AI voice-cloning for impersonation and social engineering.

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

2026 Forecast

In Part 1 of this report, "2026 Threat Intelligence Part 1 - Threat Actors," I identified 11 threat actors posing the greatest disruptive potential in 2026: Akira, Anubis, Cl0p, DragonForce, Emotet, Lazarus, LockBit, Play, Qilin, RansomHub, and SLH. While Part 1 told you who the enemy is, Part 2 tells you the weapons they will bring to the battlefield.

In technical terms, the exam question for Part 2 is: **What will these threat actors actually do?** How will their tactics, techniques, and procedures (TTPs) evolve?

Of course, anyone can map the TTPs used by any threat actor and construct the MITRE ATT&CK Matrix for Enterprise. However, I do not adopt that approach for two reasons.

First, complexity without clarity: The MITRE framework now contains 250+ techniques - not counting 3–5x more sub-techniques. Each threat actor typically uses approximately 25 techniques when the full attack chain is mapped from Initial Access Broker through negotiation phases. Presenting the entire ATT&CK framework offers little practical value to defenders.

Second, outdated thinking: Over the past decade, we have assumed threat actors to be relatively specialised - each leveraging a particular set of techniques in isolation. This thought process is becoming obsolete and in my opinion is already inadequate. The sophistication, industrialisation, and AI acceleration of 2026 demands a shift in perspective.

Part 2 is therefore dedicated to forecasting the "TTP Systems" that threat actors will deploy in 2026.

A **TTP System** is not a single technique like DNS poisoning or phishing. Instead, it is an **integrated combination of tactics, techniques, and procedures forming a coherent, resilient attack chain** - one that can adapt, persist, and multiply pressure on targets.

2026 will see TTP Systems evolve with AI acceleration, shifting from scripted to agentic attacks, cloud-native extortion, and multi-pronged reputational pressure tactics. Key risks include:

- **Agentic AI compressing timelines**: Autonomous reasoning reducing Time-to-Exploit from days to hours.
- **Identity-centric intrusions via deepfakes**: Synthetic media weaponised for credential theft and social engineering.
- **Reputational extortion professionalisation**: Multi-vector pressure targeting organisations with poor disclosure practices and amplifying past vulnerabilities.
- **Supply chain weaponisation**: Deliberately targeting weak links in disclosure chains to accelerate cascading pressure.

While N-Day exploits remain the dominant attack vector, emerging threats - zero-days, adversarial ML, and cloud-native techniques - are evolving rapidly. The threat landscape in 2026 is not simply "more of the same." It is qualitatively different. Like a game of chess, we need to think like criminals that attack us, we need “TTP Systems”. I have tried to show one way and hope it is useful to your own brainstorming.

Methodology

This prioritisation of TTP innovations is based on:

- **2025 operational patterns**: Analysis of observed threat actor behaviour, deployment frequency, and success rates.
- **AI adoption indicators**: Evidence of machine learning and generative AI integration into attack chains.
- **Resilience following disruption**: How threat actors have adapted post-law enforcement action.
- **Supply chain vulnerability amplification**: Targeting of organisations with known disclosure weaknesses to maximise reputational damage.
- **Emerging technical vectors**: Cloud-native exploitation, identity attacks, and model poisoning.

The goal is to help defenders and leaders **think in systems** rather than isolated techniques - and to enhance TTP-based thinking toward integrated **TTP Systems** that reflect how threats actually operate in 2026.

Priority TTP Innovations

This prioritisation focuses on **integrated TTP Systems** - combinations of tactics, techniques, and procedures forming resilient attack chains - based on 2025 patterns, AI adoption rates, and adaptability indicators.

In naming certain Threat Actors in this chapter, I am conscious that new Threat Actors are constantly emerging and speed of copying TTPs is increasing. Of course, nobody has a monopoly on any TTP.

Tier 1: Critical Priority

1. The Rise of "Agentic" Attack Chains

Primary Threat Actors: LockBit, Lazarus, RansomHub (adopting), others in transition

Current State (2025 Observations)

The most significant shift emerging for 2026 is the transition from **scripted automation to Agentic AI**. Unlike traditional bots or orchestration tools, agentic AI agents exhibit autonomous reasoning and adaptive decision-making:

- **GenAI for automated evasion**: 2025 activity shows threat actors integrating generative AI for dynamic payload generation, sandbox evasion, and anti-analysis techniques.
- **Lateral movement reasoning**: Early indicators show agents learning network topology and making adaptive choices rather than following predefined paths.
- **Lifecycle management**: Automated response to defensive measures (network blocks, signature updates, containment attempts).

2026 Forecast

By 2026, we expect widespread adoption of agentic AI by Tier 1 ransomware and espionage actors:

- **Autonomous reconnaissance and lateral movement**: Attackers deploy agents that perform network reconnaissance, identify high-value targets, and laterally move without human direction between detection windows.
- **Adaptive evasion**: If an agent encounters a firewall rule blocking a known exploit path, it does not simply fail. Instead, it queries its knowledge base for alternative CVEs, tests lateral routes, and selects the highest-probability path - all autonomously and in real time.
- **Time-to-Exploit compression**: Current MTTR baselines for critical infrastructure average 4–6 days from breach to containment. **By Q3 2026, agentic AI could compress Time-to-Exploit to 8–16 hours**, creating a window too narrow for traditional SOC response cycles. Your own estimates could vary – but you and I can agree that the 10-day SLA to patch Critical vulnerabilities would be suicidal in the N-Day world, where differential lines of code can quickly become exploits thanks to AI!

- **Confidence level**: High for Tier 1 actors (LockBit, Lazarus) by mid-2026; medium adoption by smaller RaaS affiliates by late 2026.

Actor-to-TTP Mapping:

- **LockBit (Fifth Generation)**: Early adopter (Q1–Q2 2026). Emphasis on agentic lateral movement in supply chain compromises.
- **Lazarus**: Concurrent adoption with LockBit. Blending agentic AI with state-sponsored espionage for dual-revenue streams.
- **RansomHub**: Following by late 2026 as API access improves.
- **Akira, Cl0p**: Selective adoption on high-value targets; cost-benefit analysis limits widespread deployment.

Defensive Implications: Organisations must shift from signature-based and static behavioural detection to **AI-driven anomaly detection** and real-time behavioural modelling. Traditional EDR signatures will be insufficient. Layered defences must include network segmentation, behavioural analytics at scale, and automated response orchestration. Critical infrastructure should treat MTTR as a key strategic metric - baseline current response times before agentic AI adoption becomes widespread.

2. Professionalisation of Reputational Extortion

Primary Threat Actors: Qilin, Anubis, LockBit, RansomHub

Why "Evolution" Rather Than "Innovation"

Multi-vector extortion is not new. Groups like REvil (pre-2021 disruption) and others deployed DDoS alongside data leaks as early as 2020–2021. What has changed is **industrialisation, coordination, and targeting precision**.

In 2025, groups like Qilin and Anubis began formalising what was previously ad hoc:

- Dedicated "Media Relations" or "Negotiation" teams
- Automated spam campaigns against customer bases
- Scheduled DDoS campaigns with operational discipline
- Preliminary data suggesting multi-vector victims settle 3–4x faster than encryption-only victims (payment rates increasing in reputational cases)

During my research, I did not find evidence whether non-payment of ransom leads to a drop on ransom demands. The anecdotal evidence of increased ransomware cases in Q4:2025 makes me believe that ransom demands will continue to increase in 2026.

2026 Forecast: Weaponising Supply Chain Disclosure Weaknesses

In 2026, threat actors will deliberately target organisations - particularly in supply chains - that are notorious for poor quality disclosure practices. This represents a **profound evolution** of the reputational extortion system:

- **Supply chain targeting**: Threat actors will identify and prioritise vendors, third-party service providers, and integration partners known to have weak disclosure protocols, delayed vulnerability patches, or poor public communication.
- **Cascading pressure**: By breaching a weak link in the supply chain, actors trigger simultaneous pressure on the primary target (who must disclose), the vendor (who faces regulatory/customer backlash), and downstream customers (who discover exposure indirectly).
- **Regulatory weaponisation**: Threat actors will file proactive regulatory complaints to financial authorities (SEC, FCA, ECB) or data protection bodies (ICO, CNIL, Garante) before victim negotiation, forcing organisations into crisis mode before they even know they've been breached.

Important note: You are no doubt aware that authorities across the world have taken a variety of positions on payment of ransom. My personal view is that in an extreme scenario where (1) if it were my business and my employees, (2) my immutable backups have completely failed and, (3) there is absolutely no way to recover even with pro help, I would take the risk and pay ransom. But this topic is so sensitive you cannot imagine. When it comes to ransom payment, the world is more polarised it could be during a cricket match between India and Pakistan or a football game between Liverpool and Manchester. If Shakespeare were to write Othello and Ransomware Attack, he would start with “To Pay or Not To Pay” as the existential question. You could well decide not to pay and shutdown your business – that’s your funeral not mine.

- **Media amplification**: Coordinated outreach to financial press, sector analysts, and affected customers via automated calling or email campaigns - creating reputation damage independent of encryption.
- **Residual vulnerability exploitation**: Prior unpatched vulnerabilities or known weak points in target organisations' disclosure processes will be weaponised as proof of systemic negligence, amplifying reputational damage beyond the breach itself.

Why This Matters for Financial Services and Regulated Entities:

Organisations operating under FSMA, PCI-DSS, DORA, or SOX face compounded risk. Reputational extortion forces disclosure before containment is complete, triggering:

- Regulatory inquiries
- Customer notification obligations (GDPR, PCI-DSS breach notification)
- Shareholder disclosures (SOX Item 8.01)
- Compliance audit triggers

This transforms ransomware from an "IT incident" to a **multi-stakeholder crisis** requiring coordination across legal, PR, regulatory, and executive teams.

Actor-to-TTP Mapping:

- **Qilin**: Leading adopter. The "Call Lawyer" feature (2025) evolves to formalised regulatory reporting and media coordination.
- **Anubis**: Already emphasises ideological destruction and public shaming; will formalise multi-vector coordination.
- **LockBit**: Supply chain focus (stated in Part 1) makes this TTP System natural evolution.
- **RansomHub**: Following Qilin's playbook; scaling automated pressure campaigns.

Defensive Implications: Ransomware is now a **PR and regulatory crisis first, and an IT security incident second**. Organisations must:

- Establish cross-functional incident response teams (Security, Legal, PR, IR, Regulatory Affairs)
- Develop disclosure response playbooks for multi-vector attacks (what to communicate, to whom, and when)
- Monitor supply chain partners' disclosure practices and patch management - poor practices in vendors become organisational risk
- Prepare regulatory narratives and customer communications *before* incidents occur
- Consider cyber insurance that covers reputational/regulatory costs, not just ransom negotiation

3. Lazarus Group: State-Sponsored AI-Enhanced Hybrid Operations

Primary Threat Actor: Lazarus Group (North Korean-linked)

Current State (2025 Observations)

Lazarus has demonstrated a unique hybrid model blending:

- **Cybercrime** (ransomware, theft for revenue generation)
- **Espionage** (APT style targeting of financial institutions and critical sectors)
- **Sabotage** (destructive operations against geopolitical adversaries)

In 2025, Lazarus was observed exploiting Qilin ransomware infrastructure - a remarkable convergence of state-sponsored capabilities and criminal-for-hire tactics.

2026 Forecast

Lazarus will accelerate agentic AI adoption *earlier and more aggressively* than commercial RaaS operators:

- **Dual-revenue fusion**: Simultaneous espionage (stealing intelligence for state use) and ransomware (generating hard currency). Agentic AI enables parallel objective pursuit within the same intrusion.
- **AI arms race leadership**: As a well-resourced state actor, Lazarus will likely field agentic AI capabilities 1–2 quarters *before* commercial RaaS groups, creating a competitive advantage in TTPs.
- **Supply chain dominance**: Expect Lazarus to target financial services, aerospace, and critical infrastructure via supply chain compromises - combining state espionage objectives with lucrative ransomware extraction.
- **Confidence level**: Very high. Lazarus's 2025 behaviour demonstrates both capability and intent.

Actor-to-TTP Mapping:

- **Lazarus**: Concurrent with or potentially *preceding* LockBit in agentic AI deployment. Primary adopter of AI + reputational extortion fusion.

Defensive Implications: Organisations in financial services, aerospace, defence, and critical infrastructure must assume Lazarus intrusions are **dual-objective threats**: loss of data to state actors AND ransomware extortion. Standard ransomware response (negotiate, pay, restore) may be insufficient if espionage objectives have been achieved. Threat-Led Penetration Testing (TLPT) exercises must model Lazarus-specific TTPs and assume exfiltrated intelligence will be strategically weaponised (not just sold).

Tier 2: High Priority

1. "Living Off the Cloud" (LotC) and API Hijacking

Primary Threat Actors: Cl0p, Akira, Lazarus, LockBit (emerging)

Current State (2025 Observations)

As organisations migrate to cloud-native architectures, threat actors are evolving equally. The MOVEit vulnerability (Cl0p's 2025 focus) demonstrated how attackers target file transfer services - but the evolution goes deeper.

- **Zero-day chains in cloud APIs**: 2025 saw fluctuating high activity on cloud platforms (AWS, Azure, GCP).
- **Credential theft from cloud environments**: Compromised IAM keys and service account tokens enable direct access to cloud infrastructure.
- **Native cloud service abuse**: Using legitimate cloud features (S3 encryption, IAM policies, backup snapshots) for attack purposes.

2026 Forecast

Instead of deploying ransomware to servers, actors will abuse stolen API credentials and cloud-native features to deny access or exfiltrate data at scale:

- **API-driven encryption**: Using stolen AWS IAM credentials or Azure service principals, attackers trigger cloud-native encryption (e.g., AWS KMS key rotation, enabling S3 bucket encryption with attacker-controlled keys) to deny the victim access to their own data.
- **IAM permission revocation**: Systematically removing the victim organisation's own IAM permissions while maintaining attacker access, creating a "trapped infrastructure" scenario.
- **Cloud backup poisoning**: Encrypting or deleting cloud backup snapshots before victims realise they've been compromised, eliminating recovery options. The quality of immutable backup solutions in the market has definitely improved in 2025. What I am not sure is their capacity to withstand extremely sophisticated attacks – especially when criminals are happy to hire their ex-employees[1].
- **Data exfiltration at scale**: Leveraging cloud data transfer quotas and legitimate APIs to exfiltrate terabytes of data with minimal malware deployment - leaving no traditional EDR signatures.
- **Confidence level**: High for Cl0p and Akira by mid-2026; adoption by others accelerating by late 2026.

[1] Hiring ex-employees as a TTP is not only relevant to backup systems; but also everything including file-transfer-applications (FTAs), firewalls, routers and switching equipment and other hardware/software.

Why LotC Bypasses Traditional Defence:

- **No malware signatures**: EDR tools expect executable payloads. Cloud API abuse generates only legitimate-looking API calls.
- **Difficult to detect**: Cloud logging may exist, but aggregating and correlating API patterns requires behavioural analytics. Many organisations lack cloud-specific SIEM coverage.
- **Persistent access**: Unlike malware that can be removed, compromised API credentials remain valid until explicitly rotated - and attackers can maintain multiple backdoors.

Actor-to-TTP Mapping:

- **Cl0p**: Pioneer (MOVEit zero-days lead to cloud API exploitation). Scaling in 2026.
- **Akira**: High adoption expected; proven success with network edge compromise enables cloud credential theft.
- **Lazarus**: Selective deployment on high-value espionage targets.
- **LockBit**: Late 2026 adoption as supply chain focus shifts to cloud-native targets.

Defensive Implications:

- Shift from **malware-centric to identity-centric and API-centric monitoring**.
- Implement cloud-native security monitoring (AWS CloudTrail, Azure Activity Log, GCP Audit Logs) with behavioural analytics to detect anomalous API patterns.
- Enforce principle of least privilege for IAM roles and credential rotation policies for service accounts.
- Maintain offline, encrypted backup copies independent of cloud platforms.
- Treat cloud credentials (API keys, service principals, tokens) with the same rigor as on-premises root credentials.

2. Vishing-as-a-Service (VaaS) and Generative Identity Impersonation

Primary Threat Actors: SLH (Scattered LAPSUS$ Hunters), DragonForce, emerging RaaS affiliates

Current State (2025 Observations)

AI voice-cloning technology has matured significantly in 2025. Initial proof-of-concepts and limited operational deployments have demonstrated:

- Real-time voice synthesis indistinguishable from authentic speaker
- Integration with social engineering workflows
- High success rates in help desk exploitation

2026 Forecast

Vishing will professionalise and scale as a formalised service within RaaS ecosystems:

- **Voice-cloned CEO/CTO fraud**: Threat actors use AI voice-cloning to impersonate IT directors, CEOs, or third-party vendors during calls to help desks or security teams, requesting MFA token resets, emergency access provisioning, or credential resets.
- **Deepfake video augmentation**: Combined with deepfake video for video conferencing scenarios, creating plausible impersonation across multiple modalities.
- **Help desk becomes primary target**: For organisations claiming "Zero Trust" architecture, the help desk remains the most accessible human interface - and the only entity authorised to override automated access policies.
- **Rebranding as "Identity Social Engineering"**: The threat will be reframed from simple phishing to sophisticated **identity compromise at the authentication layer**.
- **Confidence level**: High adoption by SLH and DragonForce by Q2 2026; mainstream RaaS adoption by H2 2026.

Why VaaS Is Effective:

- **Defeats technical controls**: MFA, conditional access policies, and passwordless authentication all depend on human-authorised exceptions.
- **Exploits organisational trust**: Help desks are trained to be helpful; urgency and authority bypass their scepticism.
- **Low cost for high impact**: Once initial access is gained, lateral movement and privilege escalation become trivial.

Actor-to-TTP Mapping:

- **SLH**: Native English speakers with social engineering expertise; likely leading adopters. Help-desk targeting aligns with 2025 "Trojan Horse" tactics.
- **DragonForce**: Rapidly growing; will adopt VaaS to augment affiliate recruitment.
- **Emerging RaaS affiliates**: VaaS will become a standardised initial access vector sold as a service within dark web forums.

Defensive Implications:

- Help desk becomes a **critical security perimeter** - not an IT function.
- Implement mandatory voice verification protocols for MFA resets and emergency access requests (callback verification, secondary authentication, pre-established code phrases).
- Deploy behavioural analysis on help desk interactions to detect anomalous access requests.
- Conduct regular TLPT exercises specifically targeting help desks with AI-voiced impersonation.

- Consider help desk consolidation to fewer, highly trained, security-aware personnel rather than decentralised IT support.

Tier 3: Elevated Watch

1. Adversarial ML: Poisoning the Defenders

Primary Threat Actors: Lazarus, Emotet, state-sponsored actors

Current State (2025 Observations)

As defenders increasingly adopt machine learning for threat detection (anomaly detection, EDR behavioural analytics, SIEM correlation), threat actors have begun developing counterstrategies:

- **Model poisoning research**: Academic and underground communities publishing techniques for adversarial examples that fool ML classifiers.
- **Supply chain ML attacks**: Early indicators of threat actors targeting training datasets for security tools.

2026 Forecast (theoretical threat with operational potential; medium confidence)

Threat actors will operationalise model poisoning - deliberately crafting malware or attack patterns that exploit weaknesses in EDR and SIEM machine learning models:

- **"Snow Features" injection**: Threat actors introduce small, seemingly harmless code additions or behavioural patterns that retrain or "poison" a company's EDR machine-learning models. Over time, these patterns teach the security system that specific malware signatures or lateral movement techniques are "normal" behaviour.

Important note: This component is highly speculative on my part and not supported by currently available evidence. The NIST provides theoretical framework but not operational evidence. You choose whether you share my paranoid confidence in Threat Actors or await real life attacks!

- **Silent model degradation**: Rather than a sudden detection failure, the model gradually loses fidelity - making it appear as a normal drift in false positive rates rather than a deliberate attack.
- **Model Integrity Breach**: By 2026, we will likely see the first major incident where an organisation's AI defence system is silently transformed into an **insider threat** - actively suppressing detection of real attacks.
- **Confidence level**: Medium-high for state-sponsored actors by late 2026; low adoption by cybercriminals (requires technical sophistication).

Why Model Poisoning Is Dangerous:

- **Asymmetric impact**: A single successful poisoning can undermine months of model training and tuning.
- **Invisible failure mode**: Organisations may not realise their AI defences have been compromised until a catastrophic breach occurs.
- **Trust erosion**: As ML-based security becomes mainstream, successful model poisoning will force defenders to reconsider trust in ML models altogether.

Actor-to-TTP Mapping:

- **Lazarus**: High sophistication; likely to field model poisoning attacks by late 2026.
- **Emotet**: If operationalised as a modern botnet with AI capabilities, potential adoption for reconnaissance and defence mapping.
- **State-sponsored actors (other)**: Primary adopters; likely to focus on critical infrastructure sectors.

Defensive Implications:

- Implement **model integrity monitoring** for all ML-based security tools. Detect unexpected changes in model decision boundaries or performance metrics.
- Maintain offline, air-gapped validation datasets to periodically verify ML model behaviour against ground truth.
- Combine ML-based detection with rules-based detection - do not rely entirely on ML for critical threat identification.
- For critical security functions, require explainable AI (XAI) models where decision rationale can be audited and verified.

2. Supply Chain Compromise (punishing bad behaviours)

Primary Threat Actors: LockBit, Cl0p, Qilin, Lazarus

Current State (2025 Observations)

Supply chain targeting has been a consistent theme throughout 2025. However, the sophistication is increasing:

- Attackers are not simply seeking initial access via vendors; they are strategically selecting vendors with **known weak disclosure practices** to amplify reputational damage.
- Breach notification delays and poor vulnerability management by third parties create cascading disclosure obligations for primary targets.

2026 Forecast

I must emphasise that I do not support any criminal activity. Period. There is a cynic in me however that smiles when a reckless and opaque vendor hides vulnerabilities and creates a bigger problem for the rest of the world. Criminals will teach them the hard lessons that their business customers can't. I will not name bad vendors but you can use the super prompt I created for you (link here).

Supply chain attacks will become **deliberately weaponised against organisations with poor disclosure practices**:

- **Vendor pre-vetting by attackers**: Threat actors could research and prioritise vendors known for delayed patch cycles, weak incident response, or history of SEC/regulatory fines related to security. I have split thoughts on this point. Based on CISA KEV, CTP designations, HBOM/SBOM and other sources it is fairly easy to identify vendors as targets. I also think any Threat Actor who needs to undertake such research is probably a noob. You decide whether it is worth debating Threat Actors' research capability!
- **Cascading disclosure**: Breaching a poorly managed vendor triggers simultaneous disclosure obligations for the vendor, the primary target, and downstream customers - maximising organisational chaos.
- **Residual vulnerability amplification**: Attackers will exploit vendors' known, documented vulnerabilities that should have been patched months ago - evidence of systemic negligence that amplifies regulatory and customer pressure.
- **Confidence level**: Very high. This is already visible in 2025 targeting patterns and will accelerate in 2026.

Actor-to-TTP Mapping:

- **LockBit**: Supply chain focus (stated in Part 1) makes this natural evolution. Q1 2026 adoption expected.
- **Cl0p**: Targeting file transfer and integration partners; perfect vector for supply chain exploitation.
- **Qilin**: Already pursuing multi-vector pressure; will add strategic vendor targeting.
- **Lazarus**: Espionage objectives may prioritise supply chain vendors for intelligence gathering, creating dual-objective breaches.

Defensive Implications:

- Implement **vendor security audits** focused on disclosure practices, patch management timelines, and incident response maturity.
- Establish **supply chain risk scoring** that explicitly weights vendors' vulnerability management and disclosure reputation.
- Develop **contractual disclosure coordination agreements** with critical vendors to ensure synchronised, controlled breach notifications.
- Monitor vendors' vulnerability disclosure and patch release patterns - deviations may signal compromise or emerging risk.

Emerging Trends for 2026

While the five TTP Systems above represent the most significant threats, several cross-cutting trends will amplify their impact:

AI as a Universal Accelerant

Agentic AI is not confined to initial intrusion. It will accelerate reconnaissance, lateral movement, data exfiltration, and even extortion negotiation. Organisations must assume that 2026 attacks will be **faster, more adaptive, and harder to interrupt** than 2025 equivalents.

Identity as the New Perimeter

Deepfakes, VaaS, API hijacking, and credential theft all target identity infrastructure rather than network perimeters. Organisations claiming "Zero Trust" will discover that identity remains the weakest link if not architected with extreme rigor.

Reputational Damage as a Primary Objective

Encryption was the ransomware weapon of choice in 2020–2024. In 2026, **reputational damage and regulatory pressure** become co-equal objectives - sometimes superseding ransom demands. Organisations must prepare for scenarios where paying the ransom does *not* stop media campaigns or regulatory action.

Disclosure Weaponisation

Poor disclosure practices will become an organisational liability. Threat actors will deliberately target vendors and partners known for weak communication, transforming supply chain relationships into sources of amplified damage rather than operational dependency.

TTP Systems: Comparison Matrix

Traditional TTP (2023–2024)	**Innovative TTP System (2026)**	**Primary Driver**	**Key Threat Actors**	**2026 Impact Forecast**
Phishing Emails	AI Voice/Video Cloning (VaaS)	Generative AI Maturity	SLH, DragonForce	High
Malware Payloads (EDR Evasion)	Living Off the Cloud (LotC) & API Abuse	Cloud Maturation	Cl0p, Akira, Lazarus	High
Manual Lateral Movement	Autonomous AI Agents (Agentic AI)	AI Reasoning Capabilities	LockBit, Lazarus, RansomHub	**Critical**
Encryption-Only Extortion	Multi-Vector Reputational Pressure (targeting disclosure weaknesses)	Business Logic / Regulatory Weaponisation	Qilin, Anubis, LockBit	**Critical**
Static EDR Detection	Adversarial ML Poisoning (Snow Features)	AI Arms Race	Lazarus, Emotet, State Actors	Medium–High
Random Vendor Targeting	Strategic Supply Chain Exploitation (poor disclosure practices)	Intelligence Optimisation	LockBit, Cl0p, Qilin, Lazarus	High

Actor-to-TTP System Adoption Matrix

This matrix clarifies which Part 1 threat actors are adopting which Part 2 TTP Systems in 2026. Note that my timelines are highly speculative and drafted to help prioritisation and sequencing:

Threat Actor	**Agentic AI**	**Reputational Extortion (Supply Chain Focus)**	**Living Off Cloud**	**VaaS**	**Adversarial ML**	**Supply Chain Exploitation**
LockBit	Early Adopter (Q1–Q2)	Native (Q1+)	Emerging (Q3–Q4)	No	No	Leading (Q1+)
Lazarus	Concurrent (Q1–Q2)	Selective (Q3+)	Selective (High value)	No	Leading (Q2–Q3)	Leading (Intelligence-driven)
Qilin	No (too mature)	**Leading** (Q1+)	No	No	No	Adopting (Q2–Q3)
Anubis	No	Ideological Focus	No	No	No	No
Cl0p	No	No	**Pioneering** (MOVEit→APIs)	No	No	**Leading** (File Transfer)
Akira	Limited (Q3–Q4)	Emerging	**High Adoption** (Q1–Q2)	No	No	Opportunistic
RansomHub	Following (Q3–Q4)	Following (Q2–Q3)	No	No	No	No
DragonForce	No	Emerging	No	**Adopting** (Q2–Q3)	No	No

Threat Actor	**Agentic AI**	**Reputational Extortion (Supply Chain Focus)**	**Living Off Cloud**	**VaaS**	**Adversarial ML**	**Supply Chain Exploitation**
SLH	No	No	No	**Leading** (Q1–Q2)	No	Targeted (Help Desk)
Play	No	No	No	No	No	Geopolitical (LatAm/Europe)
Emotet	Potential (if modernised)	No	No	No	Potential (ML Poisoning)	N/A (IAB Role)

Key Observations:

- **LockBit dominance**: Multi-TTP adoption makes it the most versatile threat actor in 2026.
- **Lazarus uniqueness**: State-sponsored hybrid model positions it ahead in agentic AI and adversarial ML.
- **Specialisation by actor**: Qilin excels at reputational pressure; Cl0p at cloud exploitation; SLH at identity compromise.
- **Supply chain as universal vector**: All major actors will exploit this weakness - but via different means.

Defensive Implications: Layered Response Framework

To counter 2026 TTP Systems, we should implement a **layered defence approach that recognises TTP systems**:

Layer 1: AI-Driven Detection and Response

- Deploy behavioural anomaly detection for network traffic, endpoint behaviour, and API activity.
- Implement AI-powered SOC automation to compress detection-to-response timelines.
- For critical infrastructure: target MTTR < 4 hours to outpace agentic AI latency.

Layer 2: Identity-Centric Security

- Implement voice verification MFA for help desk functions (callback verification, pre-established code phrases).
- Deploy deepfake detection tools for video conferencing and communications.
- Conduct regular TLPT exercises targeting identity compromise vectors (VaaS, deepfakes, API hijacking).

Layer 3: Cloud-Native Defence

- Monitor and alert on anomalous API patterns (unusual IAM role changes, encryption operations, backup modifications).
- Implement cloud backup isolation (offline copies, secondary regions, air-gapped recovery).
- Enforce principle of least privilege for cloud credentials; rotate service account keys regularly.
- Use cloud-native SIEM and behavioural analytics to detect LotC attacks.

Layer 4: Supply Chain Risk Management

- Establish vendor security scorecards explicitly rating disclosure practices, patch management, and incident response maturity.
- Develop pre-negotiated disclosure coordination agreements with critical vendors.
- Monitor vendors' public vulnerability disclosures for anomalies (delays, incomplete patches, regulatory concerns).
- Assume multi-vector pressure from supply chain breaches; prepare cross-functional incident response teams.

Layer 5: ML Integrity Verification

- For all security ML models, implement offline validation datasets to periodically verify model performance.
- Monitor ML model decision boundaries for unexpected drift or changes.
- Combine rule-based detection with ML-based detection - never rely entirely on ML for critical functions.
- Maintain explainable AI (XAI) models where decision rationale can be audited.

Layer 6: Organisational Resilience

- Establish cross-functional incident response teams (Security, Legal, PR, IR, Regulatory Affairs).
- Develop disclosure response playbooks for multi-vector attacks with regulatory coordination.
- Prepare shareholder and customer communication templates pre-incident.
- Conduct tabletop exercises simulating reputational extortion scenarios.
- Consider cyber insurance that covers reputational and regulatory costs, not just ransom negotiation.

2026 Preparedness Checklist for Security Leaders

- **Agentic AI Readiness**: Have you baselined current MTTR for critical systems? Do you have AI-driven SOC capabilities or roadmap?
- **Reputational Crisis Planning**: Do you have cross-functional incident response teams (Legal, PR, Regulatory)? Pre-drafted disclosure statements?
- **Cloud Security**: Have you implemented cloud-native monitoring (CloudTrail, Activity Logs, Audit Logs) with behavioural analytics? API key rotation policies?
- **Identity Defence**: Have you implemented voice verification MFA for help desks? Conducted TLPT with VaaS scenarios?
- **Supply Chain Intelligence**: Have you audited critical vendors' disclosure practices and patch management? Pre-established disclosure coordination agreements?
- **ML Model Security**: Have you implemented model integrity monitoring for your ML-based security tools? Offline validation datasets?
- **Threat-Led Penetration Testing**: Are your TLPT exercises updated to include 2026 TTP Systems (agentic AI, LotC, VaaS, reputational extortion)?

Conclusion

The threat landscape in 2026 is not simply "more sophisticated" which was indeed the case for 2025. The next year represents a **qualitative shift** in how threat actors think, plan, and execute attacks. The integration of AI, cloud-native exploitation, identity compromise, and professionalised reputational pressure creates attack surfaces that are fundamentally different from 2025.

The key insight from Part 1 remains applicable: **Know your threat actors**. But Part 2's contribution is equally critical: **Know the TTP Systems they will deploy**.

Organisations that prepare for 2026 by:

- Compressing incident response timelines
- Shifting from perimeter-centric to identity-centric defence
- Implementing cloud-native monitoring and API security
- Building organisational resilience against reputational pressure
- Updating TLPT exercises to model 2026 threat actors and TTPs

...will be significantly better positioned than those treating 2026 as an incremental evolution of 2025 threats.

The future of cybersecurity is not about building higher walls. I never believed in throwing lawbooks, rules, regulations, and standards as the effective means of establishing security. It is about understanding the attackers, their tools, their systems, and - most importantly - how they will adapt faster than your defences, unless you intentionally design for that speed.

Think like a criminal, but stay on the right side of law.

Best wishes,

Santosh

Annex 1: References and Citations

(Note: All links were working on 20 Dec 2025, except where stated. If you are unable to access original articles, please use the Internet Archive, Google dork, or 404wayback.)

Agentic AI and Autonomous Attack Systems

1. **LevelBlue. (2025, December 15). "Predictions 2026: Surge in Agentic AI for Attacks and Defenses."**
   Link: https://levelblue.com/blogs/levelblue-blog/predictions-2026-surge-in-agentic-ai-for-attacks-and-defenses/
   Focus: Agentic AI adoption by threat actors and defenders.

2. **eSecurity Planet. (2025, December 19). "AI Agent Attacks in Q4 2025 Signal New Risks for 2026."**
   Link: https://www.esecurityplanet.com/artificial-intelligence/ai-agent-attacks-in-q4-2025-signal-new-risks-for-2026/
   Focus: Early indicators of AI agent-based attacks in late 2025.

3. **Stellar Cyber. (2025, December 11). "Top Agentic AI Security Threats in 2026."**
   Link: https://stellarcyber.ai/learn/agentic-ai-securiry-threats/
   Focus: Technical implications of agentic AI for threat detection.

4. **Splunk. (2025, December 16). "Security Predictions 2026: What Agentic AI Means for the People Running the SOC."**
   Link: https://www.splunk.com/en_us/blog/leadership/security-predictions-2026-what-agentic-ai-means-for-the-people-running-the-soc.html
   Focus: Operational impact of agentic AI on security operations centres.

5. **IBM. (2025, December 19). "Cybersecurity trends: IBM's predictions for 2026."**
   Link: https://www.ibm.com/think/news/cybersecurity-trends-predictions-2026
   Focus: Enterprise perspective on emerging threats including AI acceleration.

Reputational Extortion and Multi-Vector Pressure Tactics

6. **Concentric AI. (2025, June 16). "5 Ransomware Predictions for 2026."**
   Link: https://concentric.ai/ransomware-predictions-for-2026-what-experts-are-forecasting/
   Focus: Ransomware evolution including extortion pressure tactics.

7. **Breached Company. (2025, December 5). "The Ransomware Revolution: How Attack Economics Are Reshaping the Threat Landscape Entering 2026."**
   Link: https://breached.company/the-ransomware-revolution-how-attack-economics-are-reshaping-the-threat-landscape-entering-2026/
   Focus: Business model evolution and professionalisation of ransomware operations.

8. **Mexico Business News. (2025, November 26). "Ransomware and Extortion Threat to Persist in 2026."**
   Link: https://mexicobusiness.news/cybersecurity/news/ransomware-and-extortion-threat-persist-2026
   Focus: Global ransomware trends and extortion tactics.

9. **Check Point. (2025, November 12). "The State of Ransomware – Q3 2025: Data leak site metrics and long-term law enforcement impact assessment."**
   Link: https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/
   Focus: Ransomware activity metrics and emerging threat patterns.

10. **MSSP Alert. (2025, December 2). "2026 Security Predictions: Are You Prepared?"**
    Link: https://www.msspalert.com/perspective/why-backup-and-recovery-are-now-central-to-every-msps-ransomware-strategy
    Focus: Ransomware resilience and recovery strategies.

Vishing, Voice Cloning, and Identity-Based Attacks

11. **ThreatLocker. (2025, September 26). "AI voice cloning and vishing attacks: What every business must know."**
    Link: https://www.threatlocker.com/blog/ai-voice-cloning-and-vishing-attacks-what-every-business-must-know
    Focus: Operational risk of AI voice cloning in social engineering.

12. **Kymatio. (2025, July 18). "Phishing Trends 2026: AI-Phishing, QRishing & Voice Deepfakes."**
    Link: https://kymatio.com/blog/phishing-trends-ai-phishing-qrishing-and-voice-attacks
    Focus: Convergence of deepfake and phishing tactics.

13. **Dark Reading. (2025, September 30). "AI-Powered Voice Cloning Raises Vishing Risks."**
    Link: https://www.darkreading.com/cyberattacks-data-breaches/ai-voice-cloning-vishing-risks
    Focus: Voice cloning as emerging attack vector.

14. **Group-IB. (2025, August 6). "The Anatomy of a Deepfake Voice Phishing Attack."**
    Link: https://www.group-ib.com/blog/voice-deepfake-scams/
    Focus: Technical and operational aspects of deepfake phishing.

15. **Breacher.ai. (2025, December 11). "How CISOs Can Tackle Deepfakes and AI-Powered Attacks in 2026."**
    Link: https://breacher.ai/blog/ciso-guide-deepfakes/
    Focus: Defence strategies for deepfake and AI-powered social engineering.

16. **IBM. (2025). "What's Behind the Rise in Vishing Incidents?"**
    Link: https://www.ibm.com/think/insights/rise-of-vishing
    Focus: Vishing attack proliferation and threat landscape.

17. **TechNewsWorld. (2025, October 1). "Researchers Mount Vishing Attacks With Real-Time Voice Cloning."**
    Link: https://www.technewsworld.com/story/researchers-mount-vishing-attacks-with-real-time-voice-cloning-179945.html
    Focus: Real-time voice cloning techniques and operational deployment.

Living Off the Cloud (LotC) and Cloud API Exploitation

18. **Cy5.io. (2025). "Cloud Security Threats 2025–2026: Top Risks & Fixes."**
    Link: https://www.cy5.io/blog/cloud-security-threats-2025-2026/
    Focus: Emerging cloud security threats and mitigation strategies.

19. **Google Cloud. (2025, December 14). "Cybersecurity Forecast 2026 report."**

    Note: Accessing this report requires free registration and I think it is worth it. A very good report. : https://cloud.google.com/security/resources/cybersecurity-forecast

    Focus: Cloud-native threat landscape and defence approaches.

20. **SecurityWeek. (2025, December 17). "Five Cybersecurity Predictions for 2026: Identity, AI and the Collapse of Perimeter Thinking."**

    Link: https://www.securityweek.com/five-cybersecurity-predictions-for-2026-identity-ai-and-the-collapse-of-perimeter-thinking/

    Focus: Identity-centric threats and cloud perimeter collapse.

Supply Chain Attacks and Strategic Vendor Targeting

21. **Industrial Cyber. (2025, November 6). "Software Supply Chain Attacks Surge: Ransomware groups escalate targeting, with industrial sectors facing elevated exposure."**

    Link: https://industrialcyber.co/reports/software-supply-chain-attacks-surge-as-ransomware-groups-escalate-and-industrial-sectors-face/

    Focus: Supply chain targeting escalation and industrial sector risk.

22. **Cyble. (2025, December 1). "Cyble's 2025 Threat Predictions Proven True: 2026 Insights."**

    Link: https://cyble.com/knowledge-hub/cybles-2025-threat-predictions/

    Focus: Supply chain targeting expansion and geopolitical drivers.

23. **Dataminr. (2025, December 10). "Dataminr's 2026 Cyber Predictions: What We See Coming."**

    Link: https://www.dataminr.com/resources/blog/dataminrs-2026-cyber-predictions-what-we-see-coming/

    Focus: Systemic disruption forecasts and logistics/manufacturing targeting.

Adversarial ML and Model Poisoning

24. **LastPass. (2025, December 16). "AI Model Poisoning in 2026: How It Works and the First Line of Defense."**

    Link: https://blog.lastpass.com/posts/model-poisoning

    Focus: Technical mechanisms of model poisoning and defences.

25. **Kratikal. (2025, December 13). "2026 Will Be the Year of AI-based Cyberattacks."**

    Link: https://kratikal.com/blog/2026-will-be-the-year-of-ai-based-cyberattacks-how-can-organizations-prepare/

    Focus: AI-enabled attacks and organisational preparedness.

26. **LinkedIn. (2025, November 25). "The First Adversarial AI 'Tarpit' Attack Causes a Major Breach (2026)."**

    Note: People from stone age may require a LinkedIn account. I like Oliver's "Tarpit Attack" explanation. : https://www.linkedin.com/pulse/scenario-first-adversarial-ai-tarpit-attack-causes-major-rochford-umggf

    Focus: Scenario-based analysis of adversarial AI attacks.

Threat Actor Profiles and 2025 Activity (Referenced from Part 1)

27. **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."**
    Note: If you are unable to access the article easily, use Google dork.
    https://breached.company/the-ransomware-as-a-service-ecosystem-in-late-2025-from-lockbits-disruption-to-the-rise-of-qilin-akira-and-dragonforce/
    Focus: RaaS ecosystem evolution and threat actor landscape.

28. **Industrial Cyber. (2025, October 26). "Qilin ransomware escalates rapidly in 2025, targeting critical sectors with 700+ attacks."**
    Link: https://industrialcyber.co/ransomware/qilin-ransomware-escalates-rapidly-in-2025-targeting-critical-sectors-with-700-attacks-ami/
    Focus: Qilin operational escalation and targeting patterns.

29. **Brand Defense. (2025, October 16). "The Lazarus Group: Espionage, Sabotage, and Cybercrime Under State Sponsorship."**
    Link: https://brandefense.io/blog/lazarus-group/
    Focus: Lazarus hybrid operational model and state-sponsored nexus.

30. **Cyble. (2025). "Lazarus Group Threat Actor Profile."**
    Link: https://cyble.com/threat-actor-profiles/lazarus-group/
    Focus: Lazarus operational capabilities and targeting.

31. **ORX. (2025, February 28). "MOVEit Transfer Data Breaches Deep Dive: SQL injection zero-day exploitation campaign analysis."**
    Link: https://orx.org/resource/moveit-transfer-data-breaches
    Focus: Cl0p's MOVEit exploitation and API attack vector.

32. **Check Point. (2025, May 7). "DragonForce Ransomware: Redefining Hybrid Extortion in 2025."**
    Link: https://blog.checkpoint.com/security/dragonforce-ransomware-redefining-hybrid-extortion-in-2025/
    Focus: DragonForce's emerging threat profile and tactical innovation.

33. **Thai CERT. (2025, June 18). "Anubis Ransomware Encrypts and Wipes Data, Making Recovery Impossible Even After Ransom Payment."**
    Link: https://www.thaicert.or.th/en/2025/06/18/anubis-ransomware-encrypts-and-wipes-data-making-recovery-impossible-even-after-ransom/
    Focus: Anubis destructive capabilities and ideological motivation.

34. **Picus Security. (2025, October 16). "Scattered LAPSUS$ Hunters: 2025's Most Dangerous Cybercrime Supergroup."**
    Link: https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup
    Focus: SLH formation and integrated attack tactics.

35. **Radware. (2024, December 31). "The Emotet Threat in 2025: Anatomy, Attack Examples & Defense."**
    Note: “Tips from the Expert (Dhanesh Ramachandran) are very good.
    : https://www.radware.com/cyberpedia/bot-management/emotet-anatomy-examples-and-defense/
    Focus: Emotet's evolving IAB role and resilience indicators.

Vulnerability Exploitation and N-Day/Zero-Day Trends

36. **Cybersecurity News. (2025, September 19). "Top Zero-Day Vulnerabilities Exploited in the Wild in 2025."**
    Link: https://cybersecuritynews.com/popular-zero-day-vulnerabilities/
    Focus: Exploitation velocity and sophisticated attack chains.

37. **DeepStrike. (2025, October 7). "Vulnerabilities Statistics 2025: CVE Surge & Exploit Speed."**
    Link: https://deepstrike.io/blog/vulnerability-statistics-2025
    Focus: Weaponisation timelines and patch effectiveness analysis.

38. **DeepStrike. (2025, December 7). "Ransomware Statistics 2025: Trends, Costs, and Key Threats."**
    Link: https://deepstrike.io/blog/ransomware-statistics-2025
    Focus: Attack volume, payment rates, and recovery cost analysis.

General 2026 Cybersecurity Forecasts and Industry Predictions

39. **CISecurity. (2025, December 12). "7 CIS Experts' 2026 Cybersecurity Predictions."**
    Link: https://www.cisecurity.org/insights/blog/7-cis-experts-2026-cybersecurity-predictions

40. **SecurityWeek. (2025, December 17). "Five Cybersecurity Predictions for 2026: Identity, AI and the Collapse of Perimeter Thinking."** *(Duplicate emphasis)*
    Link: https://www.securityweek.com/five-cybersecurity-predictions-for-2026-identity-ai-and-the-collapse-of-perimeter-thinking/
    Focus: Identity-centric threats and perimeter evolution.

41. **Cybersecurity Ventures. (2025, November 17). "Official 2026 Cybersecurity Market Report: Predictions And Statistics."**
    Link: https://cybersecurityventures.com/official-2026-cybersecurity-market-report-predictions-and-statistics/
    Focus: Market-wide predictions and statistical trends.

42. **Vanta. (2025, December 17). "Top 6 AI security trends for 2026---and how companies can prepare."**
    Link: https://www.vanta.com/resources/top-ai-security-trends-for-2026
    Focus: AI-driven security trends and preparedness strategies.

43. **DTEX Systems. (2025, December 16). "2026 Cybersecurity Predictions: Insider Risk, AI Security, and the Collapse of Perimeter Thinking."**
    Link: https://www.dtexsystems.com/blog/2026-cybersecurity-predictions/
    Focus: Insider risk and AI security integration.

44. **Solutions Review. (2025, December 19). "140+ Cybersecurity Predictions from Industry Experts for 2026."**
Link: https://solutionsreview.com/security-information-event-management/cybersecurity-predictions-from-industry-experts-for-2026/
Focus: Comprehensive aggregation of industry expert predictions.

45. **Forbes. (2025, December 12). "Ten Cybersecurity Predictions That Will Define 2026."**
Link: https://www.forbes.com/sites/emilsayegh/2025/12/12/ten-cybersecurity-predictions-that-will-define-2026/

46. **UpGuard. (2025, December 19). "Cybersecurity Predictions for 2026: Human Risk, AI Data Leaks, and More."**
Link: https://www.upguard.com/blog/cybersecurity-predictions-2026-human-risk-ai-data-leaks
Focus: Human risk factors and data exposure trends.

47. **Google Cloud. (2025, December 12). "Cloud CISO Perspectives: Our 2026 Cybersecurity Forecast report."**
Note: Francis deSouza refers to AI Fluency and Model Armor that Debian/AppArmor users like myself will find appealing. : https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-our-2026-cybersecurity-forecast-report
Focus: Cloud-centric security perspectives and forecasts.

48. **Fortinet. (2025). "Cyberthreat Predictions for 2026."**
Link: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-predictions-2026.pdf
Focus: Enterprise-scale threat predictions and AI-enabled autonomy.

49. **Integrity360. (2025, October 8). "5 core trends redefining MDR in 2026."**
Note on slide 10 the authors have identified the increasing AI adoption by Defenders and asks the right question “But can they win the race?”: https://info.integrity360.com/hubfs/Integrity360-webinar-slides-Core-trends-redefining-MDR-in-2026.pdf

50. **Taylor Wessing. (2025, December 1). "Digital resilience in 2026: key trends and predictions."**
Link: https://www.taylorwessing.com/en/interface/2025/predictions-2026/digital-resilience-in-2026-key-trends-and-predictions
Focus: Organisational resilience and digital risk management.

Financial Services and Regulatory Context

51. **Yash. (2025, December 15). "Cybersecurity Priorities 2026 Part 2: Essential Leadership Guide."**
Link: https://www.yash.com/blog/cybersecurity-strategic-priorities-for-2026-part-2-resilience-patching-identity-defense/
Focus: Leadership priorities including regulatory and compliance context. Also, highlights the need for speed in patching.

52. **ENISA (European Union Agency for Cybersecurity). (2025, October). "ENISA Threat Landscape 2025."**
Note: I suggest your read Chapters 7 to 9 for a broader coverage. For example I have not covered hacktivism in my series. : https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf
Focus: Although the publication is designed for EU-specific threat landscape and regulatory implications, in my view these threats are global and the observations are equally valid for all countries.

Annex 2: My Favourite Sources

I find the following sources to be extremely valuable. In some cases, registration is required; but that should be free. You may like to combine these with your list of favourites.

1. **AttackIQ** (https://www.attackiq.com/)
2. **Brand Defense** (https://brandefense.io/)
3. **Breached.co** (https://breached.company/)
4. **Check Point Research** (https://research.checkpoint.com/)
5. **CIS** (https://www.cisecurity.org/)
6. **Comparitech** (https://www.comparitech.com/)
7. **Cyber Rescue** (https://www.linkedin.com/company/cyber-rescue-alliance/)
8. **Cyble** (https://cyble.com/)
9. **Cybersecurity News** (https://cybersecuritynews.com/)
10. **Dataminr** (https://www.dataminr.com/)
11. **DeepStrike** (https://deepstrike.io/)
12. **ENISA** (https://www.enisa.europa.eu/)
13. **Fortinet** (https://www.fortinet.com/)
14. **Google Cloud Security** (https://cloud.google.com/security)
15. **Industrial Cyber** (https://industrialcyber.co/)
16. **Intelligence X** (https://blog.intelligencex.org/)
17. **LevelBlue** (https://levelblue.com/)
18. **ORX** (https://orx.org/)
19. **Picus Security** (https://www.picussecurity.com/)
20. **Quorum Cyber** (https://www.quorumcyber.com/)
21. **ReliaQuest** (https://reliaquest.com/) — Social engineering and help desk exploitation

If I have missed on any other valuable sources, please send me a DM and I will include them in future research.

Copyright and License

No Warranty: This work is provided "as is" without warranty of any kind, express or implied. The author shall not be liable for any damages arising from the use of this information.