2025 THREAT-LED DEFENSE

INDUSTRY-FIRST REPORT

TECHNIQUES, PROCEDURES & ADVERSARY CHANGE

TIDAL CYBER

Table of Contents

01
Introduction

This industry-first **Threat-Led Defense Report** puts real adversary behavior at the center of modern cyber defense. Grounded in **tens of thousands of observed techniques and procedures** collected directly in the Tidal Cyber platform and our **Procedures Library,** this report throws open a window into how we transform unstructured intelligence into structured, ATT&CK-aligned behaviors. With NARC, our AI engine that extracts procedure-level detail from raw threat data, we reveal the top techniques that are surging, which procedures recur across campaigns, and how adversary tradecraft is evolving in practice.

This is not the standard report that conveys what we already know by simply listing the top MITRE ATT&CK techniques. Nor is it another asset inventory, scan output, or patch backlog framed as risk. It is a data-driven picture of operational threat behavior rooted in real-world attacker action, revealing the top techniques that adversaries actually use, not theoretical exposure models. Tidal Cyber's Threat-Led Defense approach aligns defenses with how adversaries truly operate, giving security leaders clarity into true residual risk and which defensive efforts create the highest business value.

Traditional CTI reporting describes threats but rarely answers the most important question: ***"Can we defend against the behaviors that matter most?"***

By mapping TTPs directly to controls using MITRE ATT&CK, and other frameworks at the sub-technique and procedure level, we transform intelligence into prioritized defensive action and clearly reveal where protection is strong, weak, or missing entirely.

The 1st Annual 2025 Threat-Led Defense Report highlights the year's dominant techniques and behavioral patterns - not to re-catalog threats, but to show **how adversary tradecraft changed and what defenders must do next.** Our goal is to give CISOs, threat hunters, and engineers a defensible, behavior-led understanding of risk tied directly to threat-led resilience.

As we enter a future where defensive resilience must be demonstrated, one truth defines the path forward:

Strength will be measured by the adversary behaviors you can stop.
And that starts with how attackers operate and the exact techniques they use.

02 TTP Evolution

For years, defenders assumed IOCs changed fast but TTPs stayed stable. Our 2025 data disproves that. Adversaries are rapidly modifying procedures, testing new techniques, and shifting entire tactics across campaigns - meaning yesterday's coverage may no longer hold against today's behaviors.

Groups like **Scattered Spider** have demonstrated markedly different behaviors across multiple campaigns, while ransomware operators such as **Void Rabisu** and **Akira** have adopted significantly different tactics and procedures from one campaign to the next. These shifts illustrate that adversary TTPs are no longer fixed, rather they evolve quickly, repeat selectively, and demand constant reassessment. For defenders, this means yesterday's coverage may already be outdated and the need for granular, procedural-level understanding of attacker behavior is critical.

Findings & Methodology

All findings in this report are drawn from the Tidal Cyber Threat-Led Defense Platform. NARC, our AI engine, parses unstructured CTI and incident data into ATT&CK-aligned TTPs, transparently linked to sources, groups, campaigns, and software.

Our analysis tracks how adversary behaviors have evolved since their discovery and how changes in targeting, defenses, and broader motivations have driven increasingly sophisticated tactics and techniques.

Lastly, a **TTP Summary** is included for adversaries highlighted in this report based on findings discovered within the Tidal Cyber Threat-Led Defense platform and all sourced to Tidal Cyber and/or MITRE as follows:

- **Groups:** Groups and associated relationships.
- **Techniques:** Techniques used and linked relationships.
- **Procedures & Clusters:** Procedures describing exactly how adversary performed the technique(s) and groupings of similar procedures defined as Clusters.
- **Campaigns:** Specific operations attributed to adversary.
- **Software:** Tools, malware, frameworks, or utilities used to execute adversary operations.
- **References:** Evidence discovered validating adversary and their behaviors.

Tactic

Void Rabisu

Void Rabisu is a malicious actor (aka Tropical Scorpius and UNC2596) that was long thought to be driven by financial gain because of ransomware attacks. However, since the start of the war in Ukraine in 2022, APT actors that were not publicly reported on before, appear to have shifted from purely financial motives to geopolitical goals. Void Rabisu is a perfect example, an actor believed to be associated with Cuba ransomware and the RomCom backdoor for financial gain, even though its associated Cuba ransomware allegedly attacked the parliament of Montenegro in August 2022.

TTP Evolution

Void Rabisu represents a rare example of an adversary whose broader Tactic-level objectives have meaningfully shifted over time. Trend Micro researchers assess that since October 2022, the group's use of the RomCom backdoor in alleged attacks against Ukrainian government and military targets indicates an expanded mission that now includes espionage and intelligence collection alongside its traditional cybercrime activity. Normally, this type of campaign would be attributed to a nation-state actor, but in this case, multiple indicators point directly to Void Rabisu, with its TTPs aligning to RomCom-enabled, geopolitically motivated intrusions affecting Ukraine's government, military, energy and water utilities. The group has also targeted organizations outside Ukraine, including defense and IT service providers in Europe and the United States. Most notably, RomCom's methods have continued to evolve, with increasing emphasis on advanced detection-evasion techniques.

Tidal Cyber Discovery

TTP SUMMARY

59 Procedures &
40 Clusters
14 Techniques
9 References

7 Groups
2 Campaigns
9 Software

Techniques

Scattered Spider

Scattered Spider is a native English-speaking cybercriminal group active since at least 2022, initially targeting customer relationship management (CRM) providers, business process outsourcing (BPO) firms, and telecommunications and technology companies. Scattered Spider is a financially motivated group targeting companies through SIM-swapping and ransomware operations. Over time, the group has shifted to high-value industries such as retail, technology, and finance. The May 2025 cyberattack carried out by Scatter Spider used advanced social engineering techniques to compromise the organization's virtualization management platform to take control of its virtual infrastructure.

TTP Evolution

The various Scattered Spider campaigns tracked from 2022 thru 2025 feature unique Techniques. These shifts are likely largely reflections of targeting new and different technology platforms to continue to expand the scope of their attacks (certain ATT&CK Techniques are technology-platform specific).

- **SaaS Targeting (2023-2024):** Evolution of adversary TTPs focused on gaining wide access to victim SaaS applications such as Confluence, CRMs, and SharePoint and messaging applications like Slack and Teams, used for reconnaissance, data theft, and subsequent extortion purposes. Relevant Techniques include T1213.004, T1213.005, and T1567.002
- **CFO Targeting and Compromise (2025):** Increased use and targeting "virtualization" infrastructure and virtual machines (VMs) to move laterally and evade defenses. Relevant Techniques include T1651 and T1564.006

Tidal Cyber Discovery

TTP SUMMARY

225 Procedures &
94 Clusters
89 Techniques
22 References

7 Groups
3 Campaigns
46 Software

Procedures

Akira

Akira is a ransomware variant and ransomware deployment entity active since at least March 2023. Akira operations are associated with “double extortion” ransomware activity, where data is exfiltrated from victim environments prior to encryption, with threats to publish files if a ransom is not paid.

Akira is the ransomware group with **165 Procedure Sightings,** the most sightings in the Tidal Cyber knowledge base, underscoring the breadth of its capabilities. In some cases, evidence indicates Akira executing the exact same commands for the same purposes in intrusions years apart to delete Windows shadow copies via WMI to obstruct file recovery and inhibit system recovery after the ransomware attack.

Separately, the group has been seen using multiple distinct tools such as AdFind, net group, and SharpHound to perform Domain Group-focused discovery.

TTP Evolution

In 2025, the Akira ransomware variant continued to evolve as a highly adaptive Ransomware-as-a-Service (RaaS) operation, targeting organizations across sectors through VPN exploitation, credential compromise, and rapid encryption techniques. Its attacks caused widespread operational disruptions and data exfiltration, reinforcing Akira’s position as one of the most persistent and financially damaging ransomware threats of the year.

Tidal Cyber Discovery

The Tidal Cyber Threat-Led Defense platform observed and captured the following sightings:

- **Procedures Sighting:** In some cases, we have evidence of Akira executing the exact same commands for the same purposes in intrusions years apart to delete Windows shadow copies in order to inhibit system recovery after the ransomware attack.

- **Procedures Sighting:** But in many other instances, we see subtle or more significant shifts at the procedural level. For example, the group has also simply deleted administrator accounts to achieve the same overall goal. Or separately, the group has been seen using multiple distinct tools:
    - **AdFind:** Used AdFind.exe to query and retrieve information from Active Directory on Windows systems.
    - **Net group:** Used net group “Domain admins” /dom on Windows systems to enumerate administrator groups.
    - **SharpHound:** Used SharpHound, a component of the BloodHound toolkit, to collect data from Active Directory environments for privilege escalation and lateral movement planning on Windows systems.

Tidal Cyber’s Procedures Library highlights both patterns: actors reusing identical procedures over time and introducing subtle or significant procedural variations to accomplish the same operational objectives.

TTP SUMMARY

165 Procedures &
83 Clusters
28 Techniques
16 References

3 Groups
32 Campaigns
30 Software

03
2025 Cyber Themes

Insights from Tidal Cyber’s 2025 Threat-Led Report highlights four dominant themes shaping enterprise risk and defense priorities. These trends reflect an evolving threat landscape defined by advanced exploitation, human-centric targeting, hybrid ransomware operations, and state-driven cyber escalation. Collectively, they emphasize the growing importance of Threat-Led Defense, mapping defenses to the threats that matter and ensuring validation readiness against how adversaries actually execute techniques, not just what vulnerabilities exist.

We have also tracked how these adversaries have evolved since their discovery and the use of more sophisticated or different techniques based on changes in targeting.

In addition, throughout this report, we have highlighted existing, **Tidal Cyber-curated Threat Profiles** relevant to each major theme. These Profiles are available for all users of the Enterprise version of the Threat-Led Defense Platform, giving you the ability to immediately operationalize relevant, behavior-focused intelligence via Tidal Coverage Maps. Importantly, the Profiles are also kept continually up to date as the Adversary Intelligence team adds new relevant content to our knowledge base.

> “2025 redefined what it means to be proactive. Resilience is no longer patching vulnerabilities rather it’s about adversary behaviors.”

The 4 Key Themes Observed in 2025

1. Zero-Day Exploitation
2. Social Engineering Re-Emergence & AI Identity Attacks
3. The Ever-Shifting Ransomware Landscape
4. Cyber Implications of Geopolitical Conflict

ZERO-DAY Exploits

Once considered the exclusive domain of state-sponsored actors, zero-day exploitation has become a routine tool for a broader range of adversaries, including ransomware groups. In 2025, zero-day exploitation surged as both espionage and financially motivated actors increasingly targeted edge devices, remote access systems, and SaaS platforms - areas where visibility is weakest. Once the hallmark of state-sponsored groups, zero-days have become commoditized through exploit kits and AI-driven vulnerability discovery, shrinking defenders' response time from weeks to days and expanding their use across the full spectrum of adversaries.

> "Zero-days have become commodities.
> The first to exploit, wins."

Tidal Cyber's Threat-Led Defense platform has **discovered over 58 threat objects** tagged to a known or suspected exploit of a previously undisclosed (zero-day) vulnerability. This is highly significant because it demonstrates Tidal Cyber's ability to surface real-world adversary activity tied to true zero-day exploitation, something no other provider can replicate at a procedural depth.

By identifying these threat objects and associated exploits, we give our customers early visibility into how attackers are weaponizing unknown vulnerabilities before they're publicly disclosed or patched. This allows organizations to prioritize defenses based on validated adversary behavior and CVE publication cycles and retroactively tagging them if an organization wasn't aware through other channels. In effect, it bridges the intelligence-to-defense gap empowering security teams to harden configurations, tune detections, and validate controls against emerging attack patterns that traditional vulnerability or threat intelligence platforms cannot yet detect.

NOTABLE Groups & CAMPAIGNS

Here are some of the notable **zero-day campaigns** and groups Tidal Cyber has tracked with observations of more Zero-Day exploit abuse, including an expansion into use by cybercrime actors, not just APTs. A few most recent examples tracked in 2025 include:

1

SharePoint Vulnerabilities (ToolShell) Mass Exploit Campaign

Linked to multiple Chinese espionage groups, Zirconium and Threat Group -3390:

- **Zirconium:** A threat group operating out of China, this caught-in-the-wild exploit of CVE-2017,0005, a 0-Day attributed to Chinese APT31 known as Zirconium first observed in 2017 targeting individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community.
    - **TTP Evolution:** Since then, Zirconium has evolved from conducting traditional spear-phishing and espionage operations to using highly distributed proxy networks, compromised edge devices, and dynamic infrastructure that obscures attribution and enhances persistence across diverse global targets. This shift reflects a clear maturation in tradecraft, operational agility, and evasion tactics.

- **Threat Group -3390:** A Chinese threat group known as BRONZE UNION (formerly labeled TG-3390) has evolved from broad cyber-espionage campaigns focused on government and defense sectors to more targeted, stealthy operations leveraging living-off-the-land techniques, credential theft, and supply-chain compromises. Their shift toward fileless malware, cloud persistence, and exploitation of legitimate tools reflects a move toward greater operational sophistication and long-term access.

2 Ivanti VPN Zero-Day Exploit (CVE-2025-0282)

This is an identified zero-day exploit in the wild beginning mid-December 2024. Campaign linked to a “China-nexus”, espionage actor that previously exploited two vulnerabilities.

- **TTP Evolution:** By 2025 attackers were chaining that initial RCE into multi-stage intrusions, dropping web shells and persistence components, using multiple malware families, and showing more operational stealth and reuse by several China-nexus actors making detection and attribution harder.

3 Actor-Claimed Compromise & Exfiltration from Oracle Cloud Servers

A likely cybercrime, financially motivated campaign by a threat actor known as rose87168 allegedly claimed to be selling 6 million data records stolen from Oracle Cloud federated SSO login servers. Rather than simply exploiting a vulnerability and dumping data, the actor’s TTPs shifted from a one-off data sale to a blended extortion/market-making play. They threatened public leaks, bartered portions of the dump for zero-day exploits, and even stood up a site for victims to verify exposure (and pay for removal), indicating more structured monetization and victim targeting.

Zero-Day Exploit

Threat Profile

Zero-Day Exploit Threats:
A collection of Group objects labeled with the '0-Day Exploit' Tag, which tracks threats known or suspected of exploiting a previously undisclosed (zero-day) vulnerability.

Social Engineering & AI

2025 has also seen the resurgence of social engineering as a primary intrusion method and credential theft has once again become a frontline attack vector. Adversaries integrating AI-driven automation and synthesis technologies are doing so to enhance scale, realism, and success rates. Rather than "hacking in," adversaries are increasingly "logging in," often with stolen or manipulated identities. The rise of AI has lowered the barrier to executing convincing phishing, vishing, and SaaS-based social engineering campaigns, amplifying their impact. For defenders, this underscores the difficulty of stopping the initial technique, and the need to focus on detecting and disrupting the downstream behaviors these attacks enable.

> "Identity has become the new endpoint.
> And people, the new perimeter."

NOTABLE Groups & CAMPAIGNS

Tidal Cyber's Threat-Led Defense Platform and Procedures Library provide defenders with the ability to detect, validate, and respond to these evolving AI-enhanced social engineering techniques before they become widespread. **By mapping 35+ procedure sightings** tied to adversaries' use of large language models (LLMs) for reconnaissance, scripting, and deception, Tidal Cyber enables organizations to see exactly how threat actors operationalize AI, from synthetic voice generation to SaaS credential harvesting. This level of procedural visibility allows defenders to identify attack chains at the behavior level, rather than relying on static indicators or after-the-fact incident data.

For customers, this means a measurable advantage in anticipating adversary tradecraft. Through the Procedures Library's correlation of threat objects, techniques, and procedural patterns, organizations can test their defenses against the same AI-driven social engineering behaviors adversaries are deploying in the wild. This empowers them to validate controls tied to human and identity-based attack surfaces, transforming awareness into action, and ensuring their defenses evolve as fast as the attackers' AI does.

The fusion of AI and social engineering has lowered the barrier for sophisticated deception, enabling scalable, high-impact campaigns that outpace traditional awareness training and verification controls.

> "This level of procedural visibility lets defenders identify and disrupt an attack at the behavior level rather than reacting to indicators after the fact."

1 Luna Moth

Luna Moth (aka Silent Ransom Group) is a financially motivated actor active since 2022, known for "callback phishing" campaigns that trick victims into calling attacker-controlled numbers. Once connected, they use legitimate remote tools for network access, data theft, and extortion.

- **TTP Evolution:** Since 2022, the Luna Moth re-emerged in 2025 evolving to multi-channel social engineering operations that combine AI-generated lures, voice phishing, and data-exfiltration extortion. Their TTPs now emphasize persistence, credential theft, and lateral movement within SaaS environments, reflecting a shift from opportunistic campaigns to more tailored, business-focused intrusions.

2 UNC6040

A financially motivated threat cluster that specializes in voice phishing (vishing) campaigns to compromise organizations' Salesforce instances for data theft and extortion. They impersonate IT support personnel to trick employees into granting access or sharing credentials, facilitating data exfiltration from Salesforce and other cloud platforms.

- **TTP Evolution:** UNC6040 started with vishing + a rogue connected app to grab Salesforce data. Over 2025 it scaled the same core play but tightened targeting (privileged users), sped up exfiltration, extended into adjacent SaaS (Okta/M365), and professionalized its extortion cycle, all without relying on a Salesforce vulnerability. Multiple advisories and news reports in Sep–Oct 2025 note wider victim sets and coordinated extortion waves tied to the same cluster.

Adversaries are leveraging generative AI tools, such as LLMs, to amplify their targeting efforts. These models enable faster reconnaissance, more convincing social-engineering content, automated script generation, and limited assistance in developing malicious payloads.

3 Technique (T1588.007)

By utilizing a publicly available LLM, an adversary is essentially outsourcing or automating certain tasks to the tool. Using AI, the adversary may draft and generate content in a variety of written languages to be used in Phishing/Phishing for Information campaigns. The same publicly available tool may further enable vulnerability or other offensive research supporting Develop Capabilities. According to MITRE, AI tools may also automate technical tasks by generating, refining, or otherwise enhancing (e.g., Obfuscated Files or Information) malicious scripts and payloads. Finally, AI-generated text, images, audio, and video may be used for fraud, impersonation, and other malicious activities.

- **TTP Evolution:** The technique T1588.007 originally focused on using large-language models to draft phishing emails but basic social-engineering content has evolved into a full-lifecycle adversary capability. Attackers now chain AI/LLMs through reconnaissance, multi-language social engineering, exploit and payload generation, polymorphic obfuscation, and even synthetic media (voice/video) for fraud and impersonation, enabling faster, more convincing attacks at scale.

4 Contagious Interview

Contagious Interview is a North Korea–aligned threat group active since 2023. The group conducts both cyberespionage and financially motivated operations, including the theft of cryptocurrency and user credentials. Contagious Interview targets Windows, Linux, and macOS systems, with a particular focus on individuals engaged in software development and cryptocurrency-related activities.

- **TTP Evolution:** This group has since expanded and professionalized its playbook moving from simple fake apps and downloaders to supply-chain abuse (malicious npm packages and new loaders like XORIndex), the ClickFix/ClickFake tactics, and more sophisticated, multi-stage malware families. At the same time the operators have adopted AI and automation to scale credibility generating realistic resumes, interview scripts, and fake company personas to evade detection and increase success rates while broadening targets and opportunistic follow-on objectives (credential/crypto theft and lateral access).

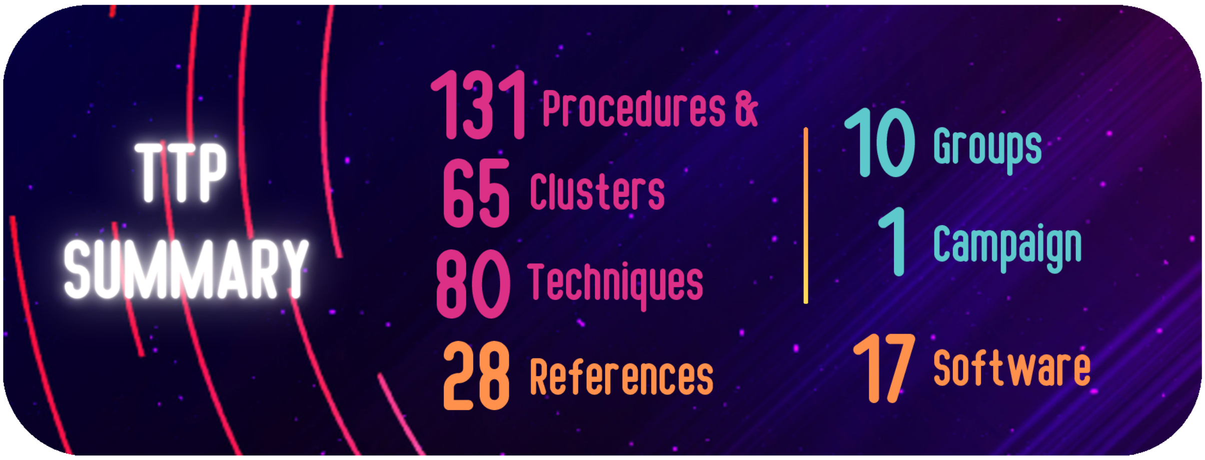
5 Magic Hound

An Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps. They have targeted European, U.S., and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), via complex social engineering campaigns since at least 2014.

- **TTP Evolution:** Since its discovery, Magic Hound has evolved from classic recruiter-style social-engineering campaigns into a highly professionalized espionage operator that now combines bespoke tooling and multi-stage malware (including custom loaders and supply-chain vectors), opportunistic use of public PoCs and N-day flaws, and sharper targeting of high-value accounts to achieve persistence and cross-platform lateral access. For defenders, Magic Hound’s shift into custom tooling, multi-stage malware, and opportunistic exploitation raises the bar for detection and validation. Playbooks tied to static IOCs or single-stage phishing flows will fail. Detection engineering must emphasize procedure-level coverage, cross-platform correlation, and validation of controls against the actual tactics Magic Hound now exhibits.

By 2024–2025 the group has integrated AI and automation to scale and refine social-engineering personas and lures, improving credibility and evasion while tightening operational tradecraft to accelerate exploitation and long-term collection.

Tidal Cyber Discovery



Social Engineering & AI

Threat Profile

Capability Type – Voice Phishing:
A collection of threats labeled with the “Voice Phishing” Tidal-curated Tag, which tracks adversaries known to use phone - or otherwise voice-based phishing/social engineering techniques.

Targeted Technology Tag - AI Threat:
A collection of threats labeled with the “AI Threat” Tidal-curated Tag, which tracks adversaries known to leverage AI technology to facilitate their operations.

Shifting Ransomware Landscape

The ransomware ecosystem continues to fragment and evolve at speed. Law enforcement pressure has disrupted some groups, but new actors have quickly filled the void, each adopting variations in techniques and procedures. The sheer volume of groups now active makes tracking difficult, and their willingness to rapidly shift playbooks only adds to the complexity. Defenders can no longer rely on static threat profiles. The challenge is not just identifying "who," but defending against "how" these groups operate.

> "Ransomware is no longer about encryption.
> It's about leverage."

In 2025, Tidal Cyber observed material cross-group procedure reuse, driven by shared affiliates and commodity toolchains. While precise global percentages aren't published, analysts characterize reuse as common and rising.

Tidal Cyber added 54 ransomware groups and software objects (and related TTP evidence) to our Procedures Library or knowledge base over the past year alone. In several cases, we've flagged these groups as emerging or trending threats before other trusted sources like CISA advisories or ATT&CK.

Threat-Led Defense shifts the focus from group names to procedures in use across campaigns. By tying ransomware profiles to ATT&CK techniques and procedures, defenders can align controls and validate coverage regardless of which group is behind the attack.

> "In several cases, we've flagged these groups as emerging or tending threats before other trusted sources like CISA advisories or ATT&CK."

Ransomware operations continued to fragment, with smaller, agile groups adopting advanced tradecraft and multi-extortion tactics. Groups like Medusa and Qilin demonstrated an ability to pivot quickly between sectors and exploit both legacy systems and cloud environments.

The Gentleman Threat Actor
Tidal Cyber AI was the first to identify "The Gentleman" threat actor from threat reporting, allowing users to link defensive capabilities with relevant Procedures and bring deep precision into their coverage

assessments. Our monthly process to identify emerging and trending ransomware threats (which routinely spotlights groups before they make headlines) surfaced a new extortion operation known as **“The Gentleman.”** The group only just started claiming victims in September 2025 but was described as “advanced” and “highly sophisticated”. And while the group displayed a few relatively uncommon behaviors, the Tidal Cyber analysis shows that the large majority are actually similar, if not identical to many commonly known ransomware TTPs (**92% of identified Tidal Procedures Sightings were “clustered” with previously observed Sightings**). Defenders can review their capabilities to confirm if existing defenses are relevant to these Procedures or identify opportunities for quick wins to bolster their defenses.

NOTABLE Groups & CAMPAIGNS

Ransomware has entered a new era, defined less by single malware families and more by rapidly evolving tradecraft. Modern groups like Medusa, Qilin, and Interlock no longer rely on simple phishing-and-encrypt playbooks. They operate as professionalized RaaS ecosystems that blend identity compromise, exploitation of unpatched appliances, multi-platform payloads, living-off-the-land techniques, cloud-service abuse, and increasingly sophisticated extortion workflows. Across campaigns, the shift is clear. Adversaries are scaling attacks by reusing reliable procedures, adopting affiliate models, and weaponizing public leak sites, while defenders are forced to harden identity, accelerate patching, and improve behavioral detection to keep pace with fast-moving, procedure-driven ransomware operations.

1 Medusa

Medusa is a ransomware operation that reportedly launched in June 2021. In 2023, the group launched a website used to publicize alleged victims. The group appears to be independent of the similarly named "MedusaLocker" operation. According to data collected by the ransomwatch project and analyzed by Tidal Cyber, Medusa actors publicly claimed around 90 victims through September 2023, **ranking it ninth out of the 50+ ransomware operations** in the dataset. These victims come from a wide variety of industry sectors and localities.

- **TTP Evolution:** Since its 2021 debut, Medusa has evolved from opportunistic phishing-and-encrypt operations into a more professionalized RaaS actor that combines credential-phishing and exploitation of unpatched software with living-off-the-land tactics, rapid data exfiltration for double-extortion, and a noisy public leak site to pressure victims, activity that scaled markedly in 2023–2025 and prompted joint FBI/CISA/MS-ISAC advisories.

2 Qilin (aka Agenda)

Qilin is a RaaS operation active since 2022 and attributed to Russian-speaking actors. It targets healthcare, government, and commercial sectors, recruiting affiliates via forums and providing tooling for a share of ransom proceeds, with a CIS kill-switch and English-language outreach pointing to likely Russian coordination.

- **TTP Evolution:** Qilin has shifted from basic phishing to a fully developed affiliate RaaS model, exploiting exposed RMM/VPNs and unpatched appliances before data theft, encryption, and extortion. Between 2023–2025, it expanded recruiting, adopted Rust/Golang variants, and added multi-platform support, fueling more destructive attacks and forcing stronger identity, patching, and segmentation defenses.

3 Interlock

Interlock is a ransomware operation first seen in September 2024, targeting organizations in North America and Europe with a double-extortion model. Actors use diverse initial-access techniques, such as drive-by downloads and ClickFix-style social engineering, and researchers note similarities to Rhysida ransomware.

- **TTP Evolution:** By early–mid 2025, Interlock expanded its capabilities using "FileFix" PowerShell lures, targeting both Windows and Linux/VMware systems, deploying stealers like LummaStealer and BerserkStealer, and abusing cloud tools such as AzCopy and Cloudflare tunnels. Combined with more polished leak-site and extortion operations, these upgrades fueled high-damage campaigns across sectors and pushed organizations to harden identity, segmentation, telemetry, and behavioral detection.

Emerging Ransomware

Threat Profile

Major & Emerging Ransomware and Extortion Threats: A regularly updated collection of ransomware and other extortion-focused threats, which are responsible for relatively many recent intrusions, growing numbers of attacks/claimed attacks, and/or which are frequently discussed in recent threat reporting.

Geopolitical Conflict

The cyber domain in 2025 has mirrored global instability. From state-sponsored campaigns to hacktivist operations, geopolitical conflict has consistently spilled over into cyberspace. Adversaries aligned with national or ideological causes have launched disruptive campaigns targeting both government and private sectors, creating an unpredictable threat environment. For defenders, the challenge lies in filtering through the noise of countless potential actors to focus on shared tools and behaviors that matter most when tensions escalate.

> “Geopolitical lines are digital and cyber is now the first move, not the last resort.”

Tidal Cyber has added many relevant objects and campaigns to its Procedures Library, not just at the “official” government level (e.g. state-sponsored groups retaliating against opposed countries) but increasingly with hacktivist groups that attack in support of particular countries.

The escalation of geopolitically driven cyber activity underscores the need for a threat-led defense grounded in understanding the specific adversaries, tools, and procedures most relevant to an organization’s attack surface. In an environment where nation-state and hacktivist operations blur together, defenders can no longer rely on static indicators or generic threat feeds. Threat-led defense enables continuous alignment of controls, detections, and validation efforts to the real behaviors adversaries use, allowing organizations to anticipate and reduce the probability of attacks tied to shifting geopolitical motives rather than reacting after impact.

RELEVANT NEW OBJECTS 2025

1 Handala Hack Team

This pro-Palestinian, and possibly Iranian-aligned threat actor, is known for using double-extortion tactics, targeting Israeli entities, and leaking significant data volumes. They also target emergency systems to broadcast alarms and propaganda. In July 2024 the Handala Phishing and Wiper Group sent lure emails containing malware to Israeli targets. The malware was a wiper designed to destroy files on the infected machine. After a period of relative quiet through much of the first half of the year, in June 2025 (days after an Israeli attack on Iranian nuclear facilities), the Handala Group claimed that it had compromised a large number of Israel-aligned entities, stealing data and granting access for potentially more destructive activity.

- **TTP Evolution:** In 2025, Tidal Cyber observed that Handala has moved beyond single-purpose wiper drops into more multi-stage campaigns that combine targeted phishing/smishing with initial access tooling (RATs/stealers and malware loaders), claimed data exfiltration and public leak/pressure activity, and wider targeting of journalists, energy and other critical-infrastructure sectors often operating alongside or as part of a broader hacktivist/IRGC-aligned “cluster.” These changes show a shift from noisy, one-off destructive attacks toward more persistent, intelligence-collection and reputational-pressure operations, though some public claims remain difficult to independently verify and researchers caution about attribution and exaggeration.

2 IT Army of Russia

Observed in July 2025, this new group is a pro-Russian hacktivist conducting data theft operations and DDoS attacks against Ukraine, primarily targeting Ukrainian digital infrastructure and small businesses. Interestingly, the group has been bold enough to attempt to recruit insiders at potential target organizations to facilitate access into those networks.

- **TTP Evolution:** Tidal Cyber has not found any reliable evidence that this group has publicly evolved significantly since its initial profile. What we do see in the broader pro-Russia hacktivist ecosystem is a shift toward targeting industrial OT/ICS environments rather than only web-fronts, as reflected in the Q3 2025 surge in infrastructure attacks. Also, the use of more stealth tactics and multifaceted campaigns (data theft, supply chain proxies, cloud/legit tools abuse) by Russian-aligned actors in general. Given these trends, it is reasonable to anticipate that the IT army of Russia may follow suit.

Geopolitical Conflict

Threat Profile

Iran-Attributed Threats + Hacktivists: Tidal Cyber's Adversary Intelligence team often curates ad hoc collections of objects in response to emerging landscape threats and events, such as increased hostilities in the Middle East in summer 2025 in this case.

Russia-Attributed Threats [similar Profiles exist for major adversarial nations]: A collection of recently updated (past year) threats linked to the subject country.

04

2025 SPOTLIGHT

Techniques

This section of the Annual Threat-Led Defense Report spotlights especially notable ATT&CK Techniques observed in our knowledge base from 2025. Rather than simply listing the top Techniques in terms of absolute number of observations (a list that remains largely static year-to-year), we've highlighted ones, based on quantitative data analysis, that saw a significant large uptick in observations this year, relative to 2024. This approach is designed to specifically shine a light on Techniques that defenders may not have on their radar so they can ensure their coverage around trending and emerging adversary behavior.

> "The power of a Threat-Led Defense approach is its ability to surface what's changing—not just what's common. We give defenders early insight into the behaviors that are gaining momentum across the threat landscape."

Tidal Cyber's Adversary Intelligence team continuously identifies and processes threat information from public sources like threat research and intelligence reports, government advisories, and independent blogs, and we heavily leverage our proprietary NARC AI solution to extract the adversaries, Tactics, Techniques, and Procedures, and relationships among them from these sources.

*Recently defined ATT&CK Techniques. Likely skews percent-change metrics.

Tidal Cyber 2025 SPOTLIGHT Techniques

Theme	Technique	Increase Monthly Observations (2024 v. 2025)	Context
Adversary Abuse of AI	Artificial Intelligence (T1588.007)	300%	**Threat Trends:** Adversaries are starting to use AI at various points in the attack chain, lowering the barrier to entry and potentially increasing the volume/pace of attacks. **Defensive Guidance:** Maintain awareness and train users on the latest AI-enabled phishing schemes. Ensure defense-in-depth around the post-exploit behaviors associated with adversaries who abuse AI.
Sophisticated Social Engineering	Spearphishing Voice (T15988.004) Impersonation (T1656) Acquire Infrastructure: Domains (T1583.001)	60% 54% 45%	**Threat Trends:** Innovative groups like Scattered Spider are successfully tricking employees to gain access, necessitating defense in depth. **Defensive Guidance:** Ensure help desk staff are trained on voice phishing risks and never grant system access to suspicious callers. Learn behavioral patterns of domain impersonation and proactively block against them.
Novel Attack Methods	Malicious Copy & Paste (T1204.004)	N/A*	**Threat Trends:** A new method that emerged and was quickly adopted by both e-crime and nation-state actors for wide-ranging compromises. **Defensive Guidance:** Monitor for evolving phishing lure schemes, disable user execution via "Run" dialog box, and hunt for known adversary execution chains.
Vulnerability Exploitation	Exploit Public-Facing Application (T1190) Network Devices (T1584.008)	31% 8%	**Threat Trends:** Adversaries are seeking access to new parts of the tech stack that may be less monitored but contain extremely valuable data. Review of access permissions, logging practices, and vendor risk management becomes more essential. **Defensive Guidance:** Defense-in-depth: ensure (and validate) robust defenses around common post-exploitation behaviors tied to known zero-day actors (and emerging ones).
SaaS Attacks	Data from Information Repositories (T1213) CRM Software (T1213.004)	N/A (not seen in 2024) N/A*	**Threat Trends:** Adversaries are increasingly exploiting "zero-day" (previously undisclosed) vulnerabilities, and ones that give access to less-monitored/defended technologies (routers, firewalls, and other "edge" devices). **Defensive Guidance:** Regularly validate that access permissions align with business needs. Explore opportunities to onboard additional application logs for proactive hunting & detection. Perform coverage assessments per business segments and – where possible – the supply chain.

05
The Tidal Cyber Difference

Going Beyond MITRE ATT&CK Techniques

Most organizations stop at technique-level mapping, which offers only a high-level view of adversary behavior. Tidal Cyber goes further by focusing on procedures, and the specific commands, tools, and tradecraft adversaries actually use in real attacks. This level of fidelity reveals the true behaviors behind the techniques, exposes variations and evolution over time, and enables security teams to align controls, detections, and validation readiness directly to how attackers actually operate. The result is a more precise representation of adversary capability and a sharper understanding of residual risk.

Tidal Cyber Procedures Library

By their design, Tactics, Techniques, and Sub-Techniques offer a high-level abstraction for describing adversary behavior. But in practice, practitioners need far more specificity to act. Tidal Cyber's industry-first Procedures Library enable analysts and defenders to immediately operationalize this Procedure-level threat intelligence for improved Threat-Led Defense. Procedures are designed to address traditional challenges by providing a granular level of adversary behavior detail, while also having relationships with many existing objects in our Knowledge Base, streamlining their use and operationalization.

NARC AI: Correlating Procedures to Threat Objects

Tidal Cyber's NARC engine accelerates Threat-Led Defense by automatically parsing unstructured intelligence and converting it into structured procedure objects linked to groups, campaigns, and software. By correlating behaviors to threat objects, NARC enables security teams to understand who uses a procedure, where it appears across campaigns, and how those behaviors connect to broader adversary patterns. This correlation transforms raw procedures into operational intelligence that drives prioritization, detection engineering, coverage mapping, and validation readiness at scale.

06
Looking Ahead to 2026

Top 7 Implications 2025

Across the diverse campaigns analyzed in this report from **Void Rabisu** and **Scattered Spider** to **Akira, Luna Moth, Medusa, Zirconium,** and **state-aligned or hacktivist groups,** a consistent set of patterns emerges.

Despite different motivations, regions, and tooling, these actors increasingly converge around the same strategic shifts: rapid and continuous TTP evolution, identity and cloud-layer targeting, AI-enabled social engineering, zero-day weaponization, hybrid criminal-espionage ecosystems, and geopolitical spillover that drives global collateral risk.

These shared observations reveal a fundamental change in the threat landscape as attackers adapt faster, automate more, blur operational boundaries, and exploit terrain where traditional detection and vulnerability-led models cannot keep up. As a whole, these implications point to a world where threat-led defense, based on aligning with adversary behavior, is the only defensible path forward.

1 Behavior Outplaces Detection: Rapid TTP Evolution

Adversaries are shifting procedures and tooling faster than traditional detection models can adapt, rendering technique-level and signature/IOC defenses increasingly ineffective.

2 AI Amplifies Social Engineering: Offensive Scale & Procedural Polymorphism

LLMs enable high-fidelity social engineering, automated reconnaissance, polymorphic payloads, and faster procedure iteration, dramatically lowering the barrier to advanced attacks.

3 Identity, SaaS, and Cloud Layers Become A Major Attack Surface

OAuth abuse, token theft, connected-app exploitation, and virtualization targeting represent some of the most persistent and highest-impact exposure points across ransomware, espionage, and cybercrime.

4 Democratization of Zero-Days Blurs Crime, Espionage, and Hacktivism

Zero-day exploitation is no longer confined to state actors. Crimeware groups increasingly weaponize new vulnerabilities within days, collapsing traditional actor distinctions and shortening defensive response times.

5 Ransomware Shifts to Stealth, Data Theft, and Multi-Stage Extortion

Modern ransomware prioritizes lateral movement, data theft, coercive extortion sites, and living-off-the-land tradecraft over mass encryption, requiring deeper behavioral telemetry and continuous mapping of control effectiveness.

6 Hybrid Adversary Ecosystems Accelerate Attack Chains

RaaS operators, access brokers, and cloud-focused threat groups increasingly collaborate or merge, building faster and more coordinated attack pipelines that span sectors and geographies.

7 Geopolitical Conflict Drives Blended Operations and Global Spillover

State units and hacktivist groups operate in overlapping campaigns combining espionage, and sabotage, influencing operations and creating widespread collateral risk for global enterprises and supply chains.

2026 Outlook: The New Reality of Threat-Led Defense

What We Can Expect in 2026

The threat landscape in 2026 will be defined by accelerating adversary innovation, AI-supercharged tradecraft, and the collapse of traditional boundaries between cybercrime, espionage, and hacktivism. Attackers will continue to shift procedures at unprecedented speed, using automation and LLM-driven tooling to generate new variations of commands, scripts, payloads, and social-engineering content. The result is behavior changes that outpace static detection, signature-based defenses, and vulnerability-led risk models.

Identity, SaaS, and cloud-control layers will become the primary battlegrounds. Token theft, OAuth abuse, virtualization escape paths, and cross-cloud privilege escalation will dominate intrusion chains, surfaces where many organizations lack telemetry, detections, or coverage mapping. Meanwhile, the democratization of zero-days will continue as ransomware groups and access brokers weaponize new exploits within days, leaving defenders with shrinking reaction windows.

Ransomware in 2026 will look less like encryption and more like multi-stage extortion, long-term persistence, and "living off the land" tradecraft that blends into normal IT activity. And as geopolitical tensions persist, organizations worldwide - even those far from conflict zones - will face increased collateral exposure from spillover attacks, wiper malware, and information-operations campaigns designed to disrupt trust, stability, and supply chains.

> "In short, 2026 will not reward organizations that defend against yesterday's TTPs. It will reward organizations that adapt as fast as attackers do."

To survive in this accelerating environment, CISOs must make a strategic shift from reactive, indicator-based defense to Threat-Led Defense grounded in adversary behavior. This means mapping controls, detection logic, and telemetry directly to the procedures attackers actually use, not generic techniques, not CVEs, and not compliance frameworks.

An Effective Defense in 2026

Behavioral Visibility at the Procedure Level

Organizations must understand exactly how adversaries execute attacks commands, tools, parameters, and variations. Technique-level mapping is no longer enough.

Identity and SaaS-Centric Detection Engineering

The security stack must expand to include telemetry, detection logic, and hardened workflow controls across OAuth, identity providers, cloud admin paths, and connected applications, the new center of gravity for attackers.

Continuous Validation of Controls and Coverage

Annual or point-in-time validation leaves organizations blind to rapid TTP shifts. Continuous, behavior-driven validation reveals whether defenses can stop the current version of an attack, not the one from six months ago.

Rapid Correlation Across Threat Objects

Linking procedures to threat groups, campaigns, and software provides early warning of shared tradecraft and cross-campaign behavioral reuse critical for prioritizing engineering work and preempting emerging threats.

Strategic Investment in Telemetry and Context

AI-driven attacks reduce the fidelity of traditional signals. Organizations must invest in deeper telemetry (identity, SaaS, cloud, network, and behavioral) and correlate it with adversary tradecraft to restore detection efficacy at scale.

Lead the Shift to Threat-Led Defense Based on Adversary Behavior

2026 will reward organizations that embrace behavior-driven **Threat-Led Defense *first*** where detections are mapped to real adversary tradecraft, controls are continuously mapped against evolving TTPs, and strategic investments align with how attackers actually operate. The path forward is clear:

- **Understand the behaviors.**
- **Map your defenses to them.**
- **Ensure your stack is validation-ready.**
- **Eliminate residual risk.**

Organizations that do this will not only withstand 2026's threat landscape, they   will build durable resilience that aligns operations, risk, and strategy around the realities of modern adversaries.

Tidal Cyber is the first true Threat-Led Defense platform built to flip the traditional defensive model by putting real adversary behavior at the center of your defense strategy. Threat-Led Defense maps techniques, sub-techniques, and procedures to ATT&CK, revealing exactly where you're exposed and how attackers operate.

It's a level of precision you've never had before, empowering your security team to proactively reduce risk and optimize high-impact security investments.

Threat-Led Defense is Tidal Cyber's unique implementation of Threat-Informed Defense, enhanced with procedure-level granularity to make CTI more relevant and actionable.

Shift to a proactive, continuous Threat-Led Defense *first.*

Learn More About Tidal Cyber at
contact@tidalcyber.com

References

TTP Evolution:

Scattered Spider:

https://cloud.google.com/blog/topics/threat-intelligence/unc3944-targets-saas-applications
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
https://web.archive.org/web/20250628050945/https:/reliaquest.com/blog/scattered-spiders-calculated-path-from-cfo-to-compromise/

Void Rabisu:

https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html

Akira:

https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/
https://www.trellix.com/blogs/research/akira-ransomware/
https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/

Themes:

Zero-Day

https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/
https://research.checkpoint.com/2021/the-story-of-jian/ https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/#storm-2603 https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/ https://research.checkpoint.com/2021/the-story-of-jian/
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

Social Engineering & AI

https://www.sygnia.co/blog/luna-moth-false-subscription-scams/
https://www.aha.org/system/files/media/file/2023/11/bi-tlp-clear-pin-ransomware-actors-continue-to-gain-access-through-third-parties-and-legitimate-system-tools-11-7-23.pdf
https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion
https://www.cybersecuritydive.com/news/fbi-warns-campaigns-salesforce-instances/760129/
https://www.knowbe4.com/hubfs/Phishing-Threat-Trends 2025_Report.pdf
https://www.validin.com/blog/inoculating_contagious_interview_with_validin/
https://www.recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat
https://securitylabs.datadoghq.com/articles/tenacious-pungsan-dprk-threat-actor-contagious-interview/

Ransomware Landscape

https://www.ic3.gov/CSA/2025/250312.pdf https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a https://www.bleepingcomputer.com/news/security/medusa-ransomware-gang-picks-up-steam-as-it-targets-companies-worldwide/ https://github.com/joshhighet/ransomwatch
https://blackpointcyber.com/wp-content/uploads/2025/08/Qilin.pdf
https://blog.barracuda.com/2025/07/18/qilin-ransomware-growing https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/ https://www.picussecurity.com/resource/blog/cisa-alert-aa25-203a-interlock-ransomware-analysis

Geopolitical Conflict

https://intelligence2risk.substack.com/p/the-retaliation-window
https://www.trellix.com/blogs/research/handalas-wiper-targets-israel/
https://www.intel471.com/blog/pro-russian-hacktivism-shifting-alliances-new-groups-and-risks
https://www.cyberdaily.au/security/12239-pro-palestinian-hackers-target-israel-in-wake-of-attack-on-iran

Learn More About Tidal Cyber at contact@tidalcyber.com

TIDAL CYBER