Muddled Libra's Strike Teams: Amalgamated Evil

By Kristopher Russo

Published: 2025-08-12 · Archived: 2026-04-05 17:24:55 UTC

Many From One

It's disingenuous to consider Muddled Libra like a traditional monolithic attack group, one with defined structure and clear lines of leadership. Muddled Libra, Scattered Spider, Octo Tempest or any of the many other names the group is labeled with is not an organized entity but a loose collaboration of like-minded cybercriminals, or personas, with common interests tethered by social chat applications.

Interrelated Strike Teams

Muddled Libra personas converge into strike teams, each with their own unique skillsets, tradecraft and objectives in tow. Since late 2022, Unit 42 has tracked at least seven distinct teams. Though in reality distinction means very little as personas enter, exit and flow from team to team. Instead, what defines a team is the combination of what they're after and the unique ways in which they go after it.

While the fluidity of this model complicates tracking, it also creates unique opportunities for threat researchers. Unlike the homogeneous, mostly faceless operations of traditional cybercrime groups, members of these small teams inherently leave their fingerprints on each attack; distinct fingerprints that become signature tradecraft.

Over time successful tradecraft is shared, learned and incorporated by other personas into their own fingerprints. By studying incident response engagements, threat intelligence researchers can walk this development back and begin profiling personas and their interdependent relationships. This allows the creation of predictive models, ultimately leading to effective controls and mitigations against future attacks.

Theory in Practice

In the teams we track related to this attack cluster, we find patterns not only in tradecraft but also objective. That is not to say these teams' tradecraft and objectives remain static, but that they tend to evolve in a predictable way that indicates relatively consistent and known personas.

Most early teams were hyper-focused on cryptocurrency theft and have never wavered, while others started out with cryptocurrency in mind but shifted to less complex and more volume-friendly objectives. The supply chain for the cryptocurrency industry is far-reaching and includes business process outsourcing, mass marketing, telecommunications, authentication providers and many other verticals. Many organizations in these industries have essentially been collateral damage along the way as strike teams identified and hunted cryptocurrency "whales" – large, valuable targets.

With each success, teams have learned, matured and multiplied. New personas enter the fray and others are arrested or fade away. Attack teams have expanded far from cryptocurrency and into a staggering breadth of industries.

- There are strike teams focused on stealing unique intellectual property for bragging rights that have targeted media and software development firms.
- Extortion-oriented teams use common ransomware-as-a-service affiliate playbooks with widespread asset destruction and encryption. These teams typically target organizations in high-availability verticals like retail and entertainment.
- Some teams simply aim to harvest credentials directly from consumers that can be quickly flipped on the dark web; low-complexity attacks like these frequently target individuals.
- A few teams are engaging in mass information harvesting. Valuable personal data is stolen that can later be stitched together to invasively profile high-value targets. Attackers focus on organizations that have unique and highly private data like those in the financial, retail and transportation industries.

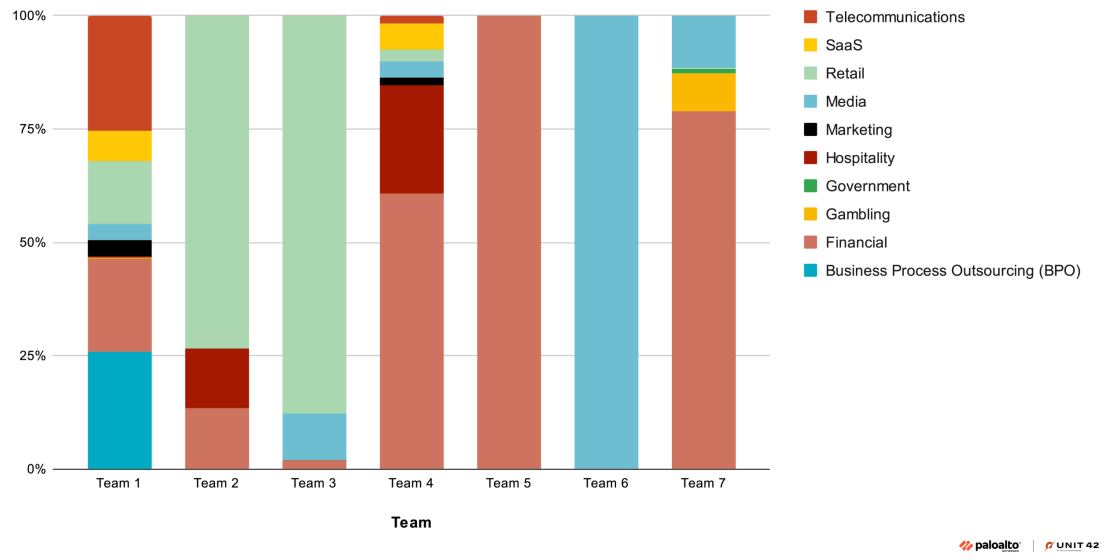

Figure 1. Seven teams associated with Muddled Libra and the differences in their targeting.

The fluid nature of Muddled Libra attack teams make it a fool's errand to predict what industry will be targeted next. Instead, defenders should focus on what they have that the group is likely to be after and who might be impacted.

For example, consider data theft or direct extortion and work backward from there. If your organization has troves of personal data, take a deep look at how to classify and protect it appropriately based on its value. Restrictive access control, data retention policies, data loss prevention and segmentation all go a long way toward ensuring your data is not used as a weapon against you.

Extortionists typically threaten to leak stolen data, disrupt critical business operations, or both. Effective business continuity and disaster recovery planning can help shield key business assets from destruction or ransomware.

If your organization is consumer facing, consider how you can better authenticate your customers and protect them from having their credentials compromised and used against them.

Strike teams will continue to form, developing new techniques and branching into new industries. Don’t lose sight of the forest (a broader goal of a robust security program based on risk and defense-in-depth strategies) for the sake of analyzing the trees (the specific tactics, techniques and procedures or targets currently popular with individual Muddled Libra strike teams).

If your organization could benefit from assistance evaluating your readiness, consider reaching out for a Cyber Risk Assessment or other proactive services from Unit 42.

Updated on Aug. 28, 2025, at 2:34 p.m. PT to add missing data to Figure 1.
