Muddled Libra: Why Are We So Obsessed With You?

By Richard Emerson

Published: 2025-08-06 · Archived: 2026-04-05 19:12:43 UTC

Why Do We Talk So Much About Muddled Libra?

Many articles and presentations have covered the tactics, techniques and procedures of the group that Unit 42 tracks as Muddled Libra. Known for social engineering tactics, the group recently attacked organizations in industries including government, retail, insurance and aviation. There's an undeniable impact for the group's victims, but I've also been pondering why this group seems to receive more media attention than other groups that also partner with Ransomware-as-a-Service (RaaS) programs.

There are other affiliates that heavily target English-speaking countries, and that are just as fast and impactful. Reading Trend 3 of our recent 2025 Unit 42 Global Incident Response Report, for example, there are fast attacks in incident response cases related to a variety of threat groups.

Here are some thoughts on why Muddled Libra has been a particular focus for the media:

Distinct Playbook, Industry Targeting

Even though Muddled Libra often uses publicly available tools and known techniques, their playbook is pretty consistent and their vishing is somewhat unique. This may make it easier to identify this group of hackers across cases versus other hacking teams. Muddled Libra has also attacked companies in waves by industry, which puts companies in those industries on high alert. It's one thing to know that your organization may be attacked at any time, it's another to know a specific threat actor is successfully targeting your peers and you may be getting attacked right now and not even know it. For other intrusions involving a RaaS affiliate, many of these groups have such similar techniques that it makes it difficult to differentiate them, and their targeting more opportunistic across industries, so there is not as coherent a story to tell.

Successful Tactics

Just looking at our cases in 2025 involving this threat actor this year, 50% of cases led to DragonForce ransomware deployment and data exfiltration, showing that Muddled Libra's attacks are frequently successful. Granted, we don't know how many calls to Help Desks go nowhere for this group, so it may be harder to measure them against their "peers." But the urgency of requests from organizations express palpable fear of Muddled Libra, as if executives were really worried they simply could not stop this threat actor.

The Power of Language

The really differentiating factor for me for this group is the English-speaking fluency that they are able to employ. It's not really possible to screen malicious calls and protect your help desk from ever receiving them. This may allow Muddled Libra to more surgically pick and choose which targets to go after within a victim environment.

Seeing the success of this language fluency and these social engineering tactics makes me wonder what will happen as AI capabilities continue to mature. Could we see every RaaS affiliate gain the capability to act like Muddled Libra?

Studying the Group Is Key to Defending Against It

As described in our Muddled Libra Threat Assessment, we've seen organizations disrupt Muddled Libra through properly implementing Conditional Access Policies. There are many other recommendations that can make a difference to stopping or slowing this threat actor. For example, gathering information that can point to suspicious activities and intelligently making connections with it (with capabilities such as those of Cortex XSIAM) can help identify incidents that need a response.

Focused study of Muddled Libra and sharing information around it helps us all stay aware of the sorts of defenses that could make a difference, against this threat actor and many others. Knowing what's worked for organizations who have successfully stopped the group can show all organizations that there is hope for defense, even against persistent and successful threat actors.
