TrendAI™ Helps Drive Global Takedown of Tycoon 2FA MFA-Bypass Phishing Service

Long-term intelligence tracking and cross-industry coordination disrupt a major identity–based cybercrime operation

DALLAS, March 4, 2026 /PRNewswire/ -- TrendAI™, the enterprise AI security leader fromTrend Micro Incorporated (TYO: 4704; TSE: 4704), has played a key role in the global disruption of Tycoon 2FA, a leading phishing-as-a-service platform designed to bypass multi-factor authentication and enable large-scale account compromise.

To read a copy of the report, Europol, Microsoft, TrendAI™ and Collaborators Halt Tycoon 2FA Operations, please visit: https://www.trendmicro.com/en_us/research/26/c/tycoon2fa-takedown.html

Working in coordination with Europol and a coalition of industry partners, including Cloudflare,Coinbase, Crowell, eSentire, Health-ISAC, Intel471, Microsoft, Proofpoint, Resecurity, Shadowserver and SpyCloud, TrendAI™ provided threat intelligence, infrastructure tracking, and actor attribution that directly supported enforcement action.

Tycoon 2FA first emerged inAugust 2023 as a subscription-based phishing toolkit built around adversary-in-the-middle techniques. Rather than simply harvesting usernames and passwords, the platform intercepted live authentication sessions, capturing credentials, one-time passcodes, and active session cookies in real time. Those session cookies could then be replayed to gain access to accounts, effectively bypassing MFA protections relied upon by enterprises worldwide.

At the time of disruption, Tycoon 2FA had approximately 2,000 users and had leveraged more than 24,000 domains since launch, with campaigns primarily targeting Microsoft 365 and other cloud services.

TrendAI™ threat researchers had been tracking the platform's infrastructure, campaigns, and operator behavior over an extended period. By November 2025, researchers had linked the operation to an actor using the monikers SaaadFridi and MrXaad, assessed to be the developer and primary operator behind the service. Historical activity showed earlier involvement in web defacement before pivoting to phishing kit development at scale. Detailed intelligence on tooling, infrastructure patterns, and operational behaviour was shared with Europol to support coordinated action.

"This was not a single phishing campaign. It was an industrialized service built to make MFA bypass accessible to thousands of criminals," said **Robert McArdle, Director for Cybercrime Research at TrendAI™.** "Identity is now the primary attack surface. When session hijacking can be packaged and sold as a subscription, the risk shifts from isolated incidents to systemic exposure."

Phishing-as-a-service platforms such as Tycoon 2FA are often viewed as secondary to ransomware. In practice, they frequently serve as the entry point. Credentials and live session tokens harvested through adversary-in-the-middle campaigns are resold in established criminal marketplaces or passed to access brokers. That access can then be monetized through business email compromise, data theft, or ransomware deployment.

By lowering the technical barrier to entry, Tycoon 2FA expanded the pool of attackers capable of launching sophisticated identity-based attacks. Its disruption represents a significant setback for that ecosystem, but it does not eliminate the underlying threat.

The operation underscores the value of sustained intelligence tracking combined with cross-industry coordination. Phishing platforms operate across borders, rely on distributed infrastructure, and serve thousands of criminal customers. No single organization has full visibility. Disruption at this scale requires actionable intelligence and aligned execution.

TrendAI™ will continue monitoring for attempts to rebuild or rebrand the service under new infrastructure and is supporting follow-on investigation into identified users and administrators. Previously stolen credentials and session cookies may remain in circulation, reinforcing the need for continued vigilance.

What Organizations Should Do Now:

The takedown reinforces a clear message: MFA alone is not sufficient against adversary-in-the-middle phishing.

TrendAI™ recommends that organizations:

- Adopt phishing-resistant authentication mechanisms and enforce strict conditional access controls.
- Deploy advanced email and collaboration security capable of detecting lateral phishing and brand impersonation.
- Enable real-time URL inspection and web content analysis to identify fake login infrastructure.
- Monitor identity risk posture continuously and enforce rapid response actions when anomalous session behaviour is detected.
- Conduct regular phishing simulations and targeted security awareness training to reduce human risk exposure.

"The disruption of Tycoon 2FA shows what is possible when intelligence is acted on, not just observed," added **Robert McArdle at TrendAI™**. "We will continue to track the actors, the infrastructure, and the users behind these services to protect our customers and raise the cost of operating in this ecosystem."

About TrendAI™
TrendAI™, a global leader in AI security, empowers enterprises to innovate fearlessly by securing AI, cloud, networks, endpoints, and data across the modern attack surface. At the core is TrendAI Vision One™, a unified cybersecurity platform that centralizes cyber risk exposure management and security operations to protect the entire AI lifecycle from infrastructure to models to users. The platform is fueled by world-class threat intelligence and insights that protect organizations from hundreds of millions of threats every day. With 6,000 TrendAI™ experts across 75 countries, TrendAI™ empowers security leaders to stay ahead of threats, driving proactive security outcomes across the entire attack surface. This includes critical environments like AWS, Google, Microsoft, and NVIDIA. AI Fearlessly.

SOURCE TrendAI

For further information: Trend Micro Communications: 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2026-03-04-TrendAI-TM-Helps-Drive-Global-Takedown-of-Tycoon-2FA-MFA-Bypass-Phishing-Service