04.03.2026 – 17:00 Uhr

TrendAI™ unterstützt weltweite Takedown-Operation von MFA-Bypass-Plattform Tycoon2FA

TrendAI™ unterstützt weltweite Takedown-Operation von MFA-Bypass-Plattform Tycoon2FA

Langfristige Bedrohungsanalyse und branchenübergreifende Zusammenarbeit legen eine der grössten identitätsbasierten Cybercrime-Operationen lahm

Wallisellen, 04. März 2026 – TrendAI™, ein Geschäftsbereich von Trend Micro, einem der weltweit führenden Anbieter von Cybersicherheitslösungen, war massgeblich an der weltweiten Zerschlagung von Tycoon2FA beteiligt. Die führende Phishing-as-a-Service-Plattform war darauf ausgelegt, Multi-Faktor-Authentifizierung zu umgehen und Kontoübernahmen im grossen Stil zu ermöglichen.

In Zusammenarbeit mit Europol und einem Verbund von Branchenpartnern – darunter Cloudflare, Coinbase, Crowell, eSentire, Health-ISAC, Intel471, Microsoft, Proofpoint, Resecurity, Shadowserver und SpyCloud – lieferte TrendAI™ Threat Intelligence, Infrastruktur-Tracking und Täterattribution, die unmittelbar zur Strafverfolgung beitrugen.

Tycoon2FA tauchte erstmals im August 2023 als abonnementbasiertes Phishing-Toolkit auf, das auf Adversary-in-the-Middle-Techniken setzte. Die Plattform fing nicht nur Benutzernamen und Passwörter ab, sondern kaperte aktive Authentifizierungssitzungen, einschliesslich Anmeldedaten, Einmalpasswörtern und aktiver Session-Cookies, in Echtzeit. Diese Cookies liessen sich anschliessend wiederverwenden, um Zugang zu Konten zu erlangen und so MFA-Schutzmechanismen zu umgehen, auf die Unternehmen weltweit vertrauen.

Zum Zeitpunkt der Zerschlagung zählte Tycoon2FA rund 2.000 Nutzer und hatte seit dem Start mehr als 24.000 Domains eingesetzt. Die Kampagnen zielten primär auf Microsoft 365 und andere Cloud-Dienste ab.

Die Bedrohungsforscher von TrendAI™ beobachteten die Infrastruktur, Kampagnen und das Verhalten der Betreiber über einen längeren Zeitraum. Im November 2025 konnten die Forscher die Operation einem Akteur zuordnen, der unter den Pseudonymen SaaadFridi und Mr_Xaad agierte. Nach ihrer Einschätzung handelt es sich dabei um den Entwickler und Hauptbetreiber des Dienstes. Frühere Aktivitäten deuteten auf eine Vergangenheit im Bereich Web Defacement hin, bevor der Akteur zur grossangelegten Entwicklung von Phishing-Kits wechselte. Detaillierte Erkenntnisse zu eingesetzten Tools, Infrastrukturmustern und operativem Verhalten gab TrendAI™ an Europol weiter, um koordinierte Massnahmen zu ermöglichen.

„Das war keine einzelne Phishing-Kampagne. Es war ein industrialisierter Dienst, der MFA-Bypass für Tausende von Kriminellen zugänglich machte“, erklärt Robert McArdle, Director für Cybercrime Research bei TrendAI™. „Identität ist heute die primäre Angriffsfläche. Wenn Session Hijacking als Abo-Modell angeboten wird, verschiebt

sich das Risiko von Einzelfällen hin zu systemischer Bedrohung."

Phishing-as-a-Service-Plattformen wie Tycoon2FA werden oft als nachrangig gegenüber Ransomware betrachtet. In der Praxis dienen sie jedoch häufig als erstes Einfallstor. Zugangsdaten und aktive Session Tokens, die über Adversary-in-the-Middle-Kampagnen erbeutet werden, landen auf etablierten kriminellen Marktplätzen oder werden an Access Broker weitergegeben. Dieser Zugang lässt sich anschliessend durch Business E-Mail Compromise (BEC), Datendiebstahl oder Ransomware-Angriffe monetarisieren.

Durch die Senkung der technischen Einstiegshürde erweiterte Tycoon2FA den Kreis der Angreifer, die in der Lage sind, ausgefeilte identitätsbasierte Attacken durchzuführen. Die Zerschlagung bedeutet einen erheblichen Rückschlag für dieses Ökosystem, beseitigt jedoch nicht die grundlegende Bedrohung.

Die Takedown-Operation unterstreicht den Wert einer nachhaltigen Bedrohungsanalyse in Kombination mit branchenweiter Koordination. Phishing-Plattformen operieren grenzüberschreitend, setzen auf verteilte Infrastrukturen und bedienen Tausende krimineller Kunden. Keine einzelne Organisation hat vollständige Transparenz. Eine Zerschlagung in diesem Ausmass erfordert deshalb verwertbare Erkenntnisse und abgestimmtes Handeln.

TrendAI™ wird auch in Zukunft mögliche Versuche beobachten, den Dienst unter neuer Infrastruktur wiederaufzubauen oder umzubenennen, und unterstützt Folgeermittlungen gegen identifizierte Nutzer und Administratoren. Zuvor gestohlene Zugangsdaten und Session-Cookies könnten weiterhin im Umlauf sein, weshalb Wachsamkeit auch weiterhin wichtig ist.

Was Unternehmen jetzt tun sollten:

Die Zerschlagung unterstreicht eine klare Botschaft: MFA allein reicht gegen Adversary-in-the-Middle-Phishing nicht aus.

TrendAI™ empfiehlt Unternehmen folgende Massnahmen:

- **Phishing-resistente Authentifizierungsmechanismen** einführen und strenge Conditional-Access-Richtlinien durchsetzen.
- **Erweiterte E-Mail- und Collaboration-Sicherheit** implementieren, die Lateral Phishing und Unternehmens-Impersonation erkennt.
- **URL-Prüfung und Web-Content-Analyse in Echtzeit** aktivieren, um gefälschte Login-Infrastrukturen zu identifizieren.
- **Identitätsrisiken kontinuierlich überwachen** und bei anomalem Sitzungsverhalten schnelle Gegenmassnahmen einleiten.
- **Regelmässige Phishing-Simulationen und gezielte Security-Awareness-Trainings** durchführen, um das Risiko durch menschliche Fehler zu reduzieren.

„Die Zerschlagung von Tycoon2FA zeigt, was möglich ist, wenn nicht nur beobachtet, sondern auch gehandelt wird", ergänzt Robert McArdle von TrendAI™. „Wir werden die Akteure, die Infrastruktur und die Nutzer hinter diesen Diensten weiterverfolgen, um unsere Kunden zu schützen und die Kosten für den Betrieb im cyberkriminellen Ökosystem zu erhöhen."

Weitere Informationen

Die vollständige Studie *Europol, Microsoft, TrendAI™ and Collaborators Halt Tycoon 2FA Operations* finden Sie hier: https://www.trendmicro.com/en_us/research/26/c/tycoon2fa-takedown.html.

Pressestelle Trend Micro Schweiz
c/o BRAND AFFAIRS AG

Mischa Keller / MSc Business Administration
Partner

Telefon: +41 44 254 80 00
E-Mail: trendmicro-media@brandaffairs.ch
Mühlebachstrasse 8 / 8008 Zürich / Switzerland

Medieninhalte

Robert McArdle, Director für Cybercrime Research bei TrendAI™.