

Weekly Intelligence Summary

Report Date: 16.06.2025

Intelligence Cut-off Date: 13.06.2025

Weekly Focus: Open-source tool 'TeamFiltration' used in large-scale Entra ID account takeover campaign

A widespread account takeover (ATO) campaign has targeted 80,000 Microsoft Entra ID accounts, exploiting open-source penetration testing tools to compromise enterprise cloud environments at scale.

A coordinated account takeover campaign has reportedly targeted approximately 80,000 Microsoft Entra ID accounts (formerly Azure Active Directory), with evidence suggesting the use of open-source penetration testing tools to exploit common identity misconfigurations.

TeamFiltration, an open-source tool designed for cross-platform security assessments of Microsoft 365 tenants, automates account enumeration, password spraying, token extraction, and persistence mechanisms. Activity consistent with this functionality has been observed in suspected malicious contexts.

The tool integrates FireProx, an AWS API Gateway-based utility that rotates IP addresses to evade rate limiting and detection during password spraying. This technique uses a small number of common passwords across many accounts, minimising account lockouts and reducing detection probability.

Observed activity linked to TeamFiltration has included use of an outdated Microsoft Teams user-agent, OAuth access attempts from incompatible device profiles, user-agent spoofing, and client IDs known to be hardcoded in the tool to harvest family refresh tokens. These artefacts align with public configurations of TeamFiltration and support a high-confidence assessment that the tool is being abused in ongoing campaigns.

Why It Matters...

Targeting Entra ID accounts allows threat actors to potentially obtain persistent, high-privilege access to enterprise cloud environments without the need for exploits. These campaigns rely on predictable weaknesses, unenforced MFA, continued use of legacy protocols, and weak or recycled credentials.

Without strong authentication policies, real-time access monitoring, and strict credential hygiene, organisations remain exposed. Preventing compromise requires the elimination of structural weaknesses that such tools are explicitly designed to exploit.

Threat actors are inherently opportunistic, constantly adapting to improved defences, which often leads to leveraging the weaknesses presented by the lack of user awareness and education, or poor policy implementation.

Intelligence Overview

Ransomware

Interlock compromised Kettering Health, exfiltrating 941 GB of sensitive data, including patient records and ID documents. Charting systems and call centres were disrupted.

Sensata confirmed that ransomware encrypted systems after network access was gained in March. Exfiltrated data includes extensive employee PII. No group has claimed responsibility. Operations remain partially impacted.

Education Sector

Mastery Schools reported a ransomware attack affecting 37,031 individuals. DragonForce claims to have stolen 171 GB of sensitive data, including PII, financial, medical, and student records.

Service Disruption

Erie Insurance experienced major disruption due to a confirmed cyberattack. Policy access, payments, and claims systems remain affected. The nature of the attack is unconfirmed.

UNFI took systems offline following a network breach. Customer orders were impacted. Full details are pending, with ongoing remediation supported by third-party cyber specialists.

Data Breach

TxDOT confirmed a breach of its Crash Records system. Nearly 300,000 crash reports were downloaded via a compromised account. Exposed data includes names, licence numbers, and injury details.