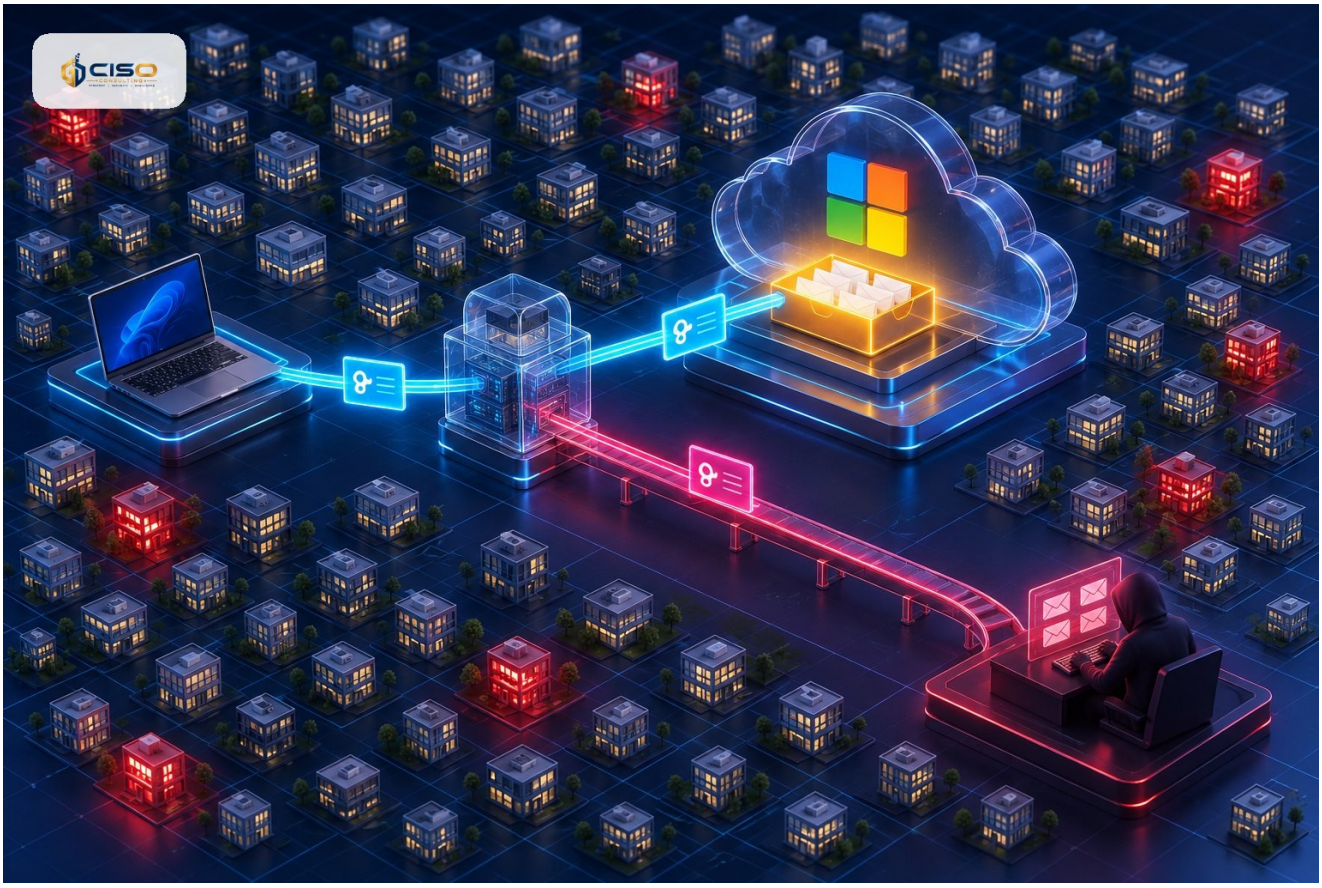
Token-replay campaign hits 97 Microsoft 365 accounts at 79 organizations



Huntress reports an adversary-in-the-middle campaign that captured Microsoft 365 sessions and replayed stolen tokens to access email at 79 organizations between July 14 and September 22, 2026.

- The campaign uses an adversary-in-the-middle (AitM) relay to capture sign-in sessions.
- Stolen tokens are then replayed to break into email accounts.
- Huntress observed the activity between July 14 and September 22, 2026.
- The headline figures are 97 compromised accounts at 79 organizations.
- Huntress detected 497 successful Microsoft 365 sign-in events; the source excerpt does not give further detail.

What was reported

Researchers have disclosed a Microsoft 365 campaign in which attackers place an adversary-in-the-middle (AitM) relay between the user and the sign-in service. The relay captures the sign-in session, and the attackers then replay the stolen tokens to get into email accounts.

Huntress observed the activity between July 14 and September 22, 2026. According to the report, 97 accounts at 79 organizations were compromised, and Huntress detected 497 successful Microsoft 365 sign-in events.

Why it matters

Token replay works on a session that has already been authenticated. For that reason, a password alone is not the only thing at stake, and a sign-in that looks legitimate in logs may still be attacker activity. The source excerpt available to us does not describe the lures used, the sectors targeted or any specific mitigations, so we do not extend the findings beyond what was reported.

What to do next

Institutions using Microsoft 365 should review how sessions and tokens are protected and how unusual successful sign-ins are detected. The actions below are general good practice and are not drawn from the report itself.

What to do now

1. Review Microsoft 365 sign-in logs for successful sign-ins from unusual locations, devices or timing, covering July to September 2026.
2. Check mailboxes of any suspicious accounts for new forwarding or inbox rules.
3. Revoke active sessions and tokens and reset credentials for accounts showing suspicious activity.
4. Assess whether your multi-factor authentication methods resist session relay, and prioritize stronger methods for privileged and finance users.
5. Brief staff and the SOC on AitM phishing and add token-replay scenarios to incident response playbooks.