ARBITIUM INSIGHTS | TECHNICAL

MFA Is Not Enough: The Anatomy of a Modern Identity Takeover

Arbitium Engineering | April 1, 2026

MFA Is Not Enough: The Anatomy of a Modern Identity Takeover

Last week, SentinelOne published its 2026 Annual Threat Report. The headline finding was not subtle: threat actors have moved beyond initial breaches to systematically abuse trusted identity systems, infrastructure, and the automation pipelines that power modern enterprises. Around the same time, the 2026 Sophos Active Adversary Report landed with a similar conclusion: 67% of all incidents investigated by their teams were rooted in identity-related attacks.

The uncomfortable truth sitting behind these numbers is that multi-factor authentication, the security control most widely deployed to protect identity, is no longer the hard stop it once was. This article explains why, technically, and what a modern automated defense looks like in response.

How MFA Gets Bypassed: The Session Cookie Problem

MFA is designed to prove you are who you claim to be at login time. Once you authenticate successfully, the browser or application stores a session token: a cryptographic credential that says, in effect, "this user already proved their identity, let them through." That token is valid until it expires or is explicitly revoked.

Infostealers, the malware family at the heart of the modern credential economy, do not need your password. They do not need to intercept your OTP. They harvest the session cookies already sitting in your browser profile directory, post-authentication, MFA already cleared, access already granted.

The Infostealer Pipeline at Scale

The 2026 Identity Breach Report documents what happens when you industrialize this capability. Researchers processed 51.7 million infostealer packages in 2025, representing 24.8 million unique infected devices. Each package is a structured archive: harvested browser cookies, saved passwords in plaintext, autofill data, session tokens for SaaS platforms, VPN credentials, and anything else the browser knew.

The report also documents a 261% year-over-year increase in plaintext credentials found in these logs, with 68.89% of all breached passwords arriving in clear text. This is not because encryption got worse. It is because the theft is happening after decryption, at the browser layer, where the user experience requires credentials to be readable.

A simplified version of the pipeline looks like this:

1. Phishing email or malvertising delivers infostealer payload to endpoint. 2. Infostealer executes in user context, reads browser profile directory. 3. Cookies, saved passwords, and session tokens

exfiltrated to C2 or sold via underground markets. 4. Attacker loads harvested session cookie into their browser. 5. Target application accepts the cookie as a valid session; no login required, no MFA prompt.

The attacker is now authenticated. Not as someone impersonating you. As you. With your permissions, your access level, your trusted device fingerprint.

The Automation Asymmetry

What makes this particularly dangerous in 2026 is not the individual attack technique. It is the velocity. Attackers are running automated pipelines: harvesting credentials at scale, testing them programmatically, chaining scanning, credential replay, and exploitation tools into continuous, high-throughput operations.

Defenders, meanwhile, are responding with ticket queues, analyst triage, and Change Advisory Board approvals before taking containment action. The Sophos report found that identity weaknesses played a material role in nearly 90% of incident response investigations. The 2026 Constella Identity Breach Report describes this explicitly as "the industrialization of identity": machine-scale pipelines designed to weaponize human identities at speeds that human-paced security operations cannot match.

When the attacker's pipeline runs in milliseconds and your response runs in hours, the detection signal is not the bottleneck. The bottleneck is the gap between signal and action.

What Automated Defense Actually Requires

Closing this gap requires rethinking what security automation is for. Most automation in security operations today focuses on alert enrichment and investigation support: gathering context, correlating signals, suggesting next steps. These are useful. They are not sufficient.

Closing the session hijacking loop specifically requires systems capable of:

Detecting session anomalies in real time, not at next-business-day alert review. This means behavioral signals: impossible travel, device fingerprint mismatch, concurrent session from two geographic locations.

Executing token revocation automatically when anomaly confidence crosses a defined threshold, without waiting for a human to approve the action.

Triggering endpoint quarantine or network isolation for the affected device before the attacker can pivot to additional resources.

Logging the full action chain for human review post-execution, maintaining auditability without sacrificing speed.

The key insight is that session hijacking attacks compress the time between compromise and damage to a window that human response cannot reliably close. Automated detection is only half the equation. Automated execution is the other half.

Technical Audit: What to Check Right Now

Here is a practical checklist your team can run this week against your current identity security posture:

1. Session token lifetimes: Are your SSO and SaaS application session tokens expiring within 8 hours for privileged access? Tokens with 30-day lifetimes are a wide-open window for session hijacking.

2. Concurrent session detection: Does your IdP or SIEM alert on simultaneous sessions from geographically impossible locations? If you cannot answer this in under 60 seconds, the answer is probably no.

3. Infostealer indicators on endpoints: Pull your EDR telemetry for reads of browser profile directories (AppData\Local\Google\Chrome\User Data on Windows, ~/Library/Application Support/Google/Chrome on macOS) by any process that is not the browser itself.

4. MFA bypass vectors: Audit which of your SaaS applications support session persistence that bypasses MFA on re-authentication. Legacy OAuth tokens and remember-me cookies are common gaps.

5. Revocation pipeline: Time how long it takes from "analyst identifies suspicious session" to "session token revoked." If that number is over 15 minutes, you have an automation gap.

A simple detection query for your SIEM to surface high-risk concurrent sessions:

```
# Pseudo-logic for impossible travel / session clone detection SELECT user_id, session_id, source_ip, geo_country, timestamp FROM auth_events WHERE session_id IN ( SELECT session_id FROM auth_events GROUP BY session_id HAVING COUNT(DISTINCT geo_country) > 1 AND MAX(timestamp) - MIN(timestamp) < 3600 -- within 1 hour ) ORDER BY timestamp DESC;
```

Run the audit items above and map the results to your current detection and response pipeline. Specifically, identify which of the five checks has a fully automated response path and which ones still require human action to close the loop. That gap, framed as time-to-revocation, is the metric worth presenting to your security leadership. To discuss autonomous response architectures for identity threats, visit ***arbitium.com/contact****.*

Arbitium Engineering publishes technical content on autonomous security execution, agentic AI architectures, and the engineering challenges of closing the gap between detection and response. arbitium.com

Sources

SentinelOne Annual Threat Report 2026. Press release, March 24, 2026. sentinelone.com

Sophos Active Adversary Report 2026. "Identity Attacks Dominate." sophos.com, March 2026.

Constella Intelligence. "2026 Identity Breach Report: The Industrialization of Identity." constella.ai

Darktrace Annual Threat Report 2026. "AI-enabled credential abuse." industrialcyber.co

Help Net Security. "One stolen credential is all it takes to compromise everything." February 2026.

Security Boulevard. "Top 5 Learnings from the 2026 Identity Breach Report." February 2026.

Sophos Incident Response data: 90% of IR investigations include identity weakness. 2026.