Insights on identity attacks and trends continued

Introduction Nation-state threats Ransomware

<1%

of attacks

Fraud Identity and social engineering DDoS attacks

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

_

More than 99% of identity attacks are password attacks

Breach replay

Password spray

Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

Less than 1% combined

MFA attacks

SIM swapping

MFA fatique

AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.



Post-authentication attacks

Token theft

Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.



Infrastructure compromise

Often silently executed by professional groups or nation-statebacked threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.



Fragmented solutions lead to

- Unnecessary data transfers
- Duplicate copies of data
- Inconsistent data classification
- Redundant alerts
- Siloed investigations
- Exposure gaps

- Increased implementation complexity
- Longer deployment times
- Greater management burden
- | Higher costs
- Worse security outcomes