SISA

MFA Brute Forcing Attack

The Menace of MFA Brute Force Attacks

MFA is bypassed in 30% of attacks

SMS-based MFA was the most common type of MFA used, and the least secure.

32.5% companies were targeted by brute-force attacks in one month alone.

What is MFA Brute Force Attack?

A Brute-Force Attack to gain unauthorized access to protected accounts, through -

Endless login attempts.

Cracking login credentials, encryption keys, and hidden URLs.

Detective Controls to Prevent MFA Brute Force Attacks

Enrich public IP with Geo location, ASN (Autonomous System Numbers) value for remote application logs.

Identify unknown ASN from login origin, to assess use of VPN by the user.

Use a long tail analysis graph/dashboard of the Geo to identify any login attempt from a different Geo.

Train ML to link user with Geo and ASN and generate anomaly if the user logs in from a different Geo or ASN.

Preventive Controls to Combat MFA Brute Force Attacks

Configure the MFA to OTP-based authorization.

Configure the application to be disabled if the user has rejected a push notification three times within a short period.

Configure the remote application to reject authentication of users connecting from a different geo.

Train employees on a continuous basis to reinforce best practices of

- Not sharing OTPs.
- Not authorizing MFA to push notification unless authorized by user.
- Informing IT and Infosec team on receipt of unauthorized OTP or push notifications.

To learn more about emerging trends, threat exploits, intruder tactics and SISA's top learnings from breach investigations, register for a **Forensics Learning Session**