ARKOSE LABS™

THE GLOBAL SCAMDEMIC: THREAT ACTOR BEHAVIOR EXPOSED

More than $1 trillion was lost to scams globally in 2024. A Data-Driven Analysis of Threat Actor Behavior analyzes nearly 20 billion malicious attack traffic patterns to uncover the where, how and when of scammers' devastating campaigns.

VULNERABLE ENTRY POINTS

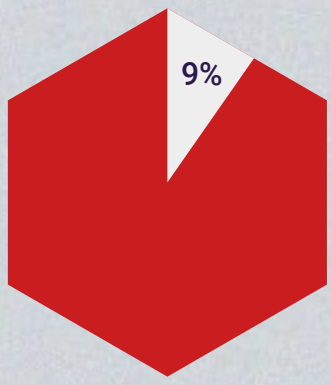
of scams started through account sign-up flows

ESCALATING ATTACK TYPES

Fake account creation surged from

of all attacks

SMS SURGE



of all attacks were SMS toll fraud by year's end, more than double the percentage at the beginning of the year.

WEAPONIZED ATTACK MECHANISMS

2,046%
Q2oQ1↑
Relentless Attack Automation Services

957%
Q2oQ1↑
Coordinated Fraud Farms

556%
Q4oQ3↑
Shape-Shifting Advanced Bots

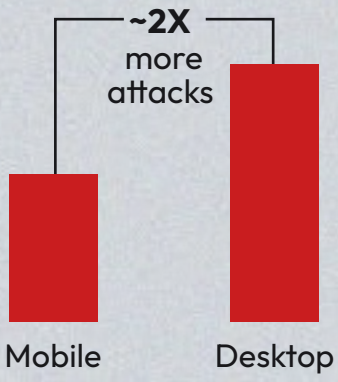
173%
Q4oQ3↑
Bots

SCAMMER SALARY

Scammers in El Salvador might make 20x more attacking gaming companies, versus working a software developer job

POPULAR ATTACK DEVICES

ACCOUNT TAKEOVERS



ATTACK TIMING TRENDS

60%

of attacks originating in El Salvador occur between **4 p.m. to 12 a.m.** Local Time (Central Standard Time)

SCAMMERS TOOK A BREATHER

Among the target industries in this report, August and September malicious traffic accounted for less than 1% of all annual malicious traffic

ARKOSE LABS™

Talk to Our Experts