Account Takeover – Chronology of an Attack



PART 1

The landscape

Bad actors have more stolen credentials available on the dark web than ever before.

15 billion

user records exposed in 2019

28,538

credentials stolen per minute

15

average months to discover and report credential spills

7,098

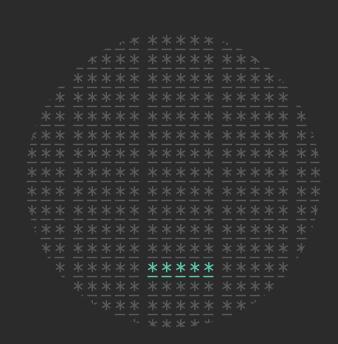
data breaches in 2019



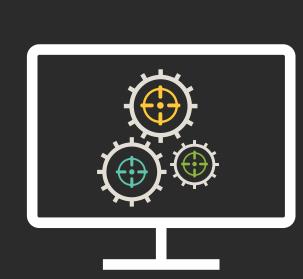
PART 3

The attack

These mass-scale credential testing and account takeover attacks can take place for the next days, weeks and even months. The working credentials are used for purchases.



1 2 0 6 success rate from testing sets of username and passwords at login.



90% of attacks are automated.

Based on NuData Analytics

Credential testing

82%

of automated high-risk activity at login comes from credential testing attacks.

Account takeover

43%

increase in ATO during COVID lockdowns compared to the same period in 2019.

Mass-scale attacks

+41

high-risk login attempts at a U.S.

login page in 48 hours.

PART 2

Preparing the attack



price to purchase 3.8M credentials



cost of software, configuration files, and proxies



to run a mass-scale automated attack

PART 4

The aftermath



32% of victims of ATO never do business with that merchant again

\$6.8 billion lost

to ATO in 2019 in the U.S. alone

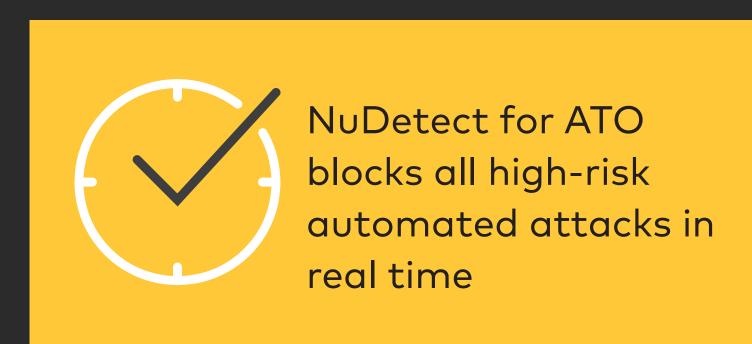
The cost of data breaches is projected to hit

\$5 trillion globally by 2024





How you can change the story with NuDetect for ATO



Blocks +99%

of automated credential testing and account takeover attempts



Here's how one digital goods company changed their story



10,000 attacks stopped per day

Saved nearly \$500,000 within a year.

... and so have several fortune 500 companies.

Click Here to read their stories