Account Takeover – Chronology of an Attack



PART 1 The landscape

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

22 billion

15

3,932

user records exposed in 2020¹

41,857 credentials stolen per minute

average months to discover and report credential spills² PART 2

Preparing the attack



data breaches in 2020³

\$2,999 price to purchase 3.8M credentials

cost \$6-\$50 files

cost of software, configuration files, and proxies

to run a mass-scale automated attack

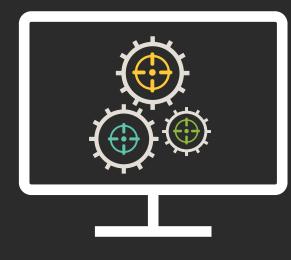


PART 3 The attack

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.

20/6 success rate from testing sets of

username and passwords at login.⁴





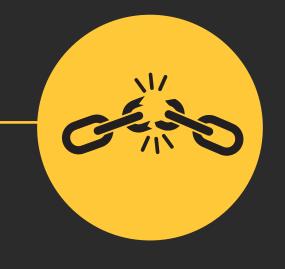
of attacks are automated.4

Based on NuData Analytics

PART 4 The aftermath



32% of victims of ATO never do business with that merchant again.⁵



Credential testing



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

Account takeover

1 in 3

login attempts in 2020 were high-risk traffic attempting to take over an account.

Mass-scale attacks

+4M

high-risk login attempts at a U.S. login page in 48 hours.

\$6.0 billion lost

to ATO in 2020 in the U.S.⁶

The cost of data breaches is projected to hit

\$5 trillion globally by 2024⁷



How you can change the story with NuDetect for ATO



NuDetect for ATO blocks all high-risk automated attacks in real time

Blocks +99%

of automated credential testing and account takeover attempts



Protects your pre-authentication interface to avoid future fraud

Here's how one digital goods company changed their story



... and so have several fortune 500 companies.

Click Here to read their stories

¹ ITP.net, 2021
² Shape Security, 2019
³ GovTech.com, 2021
⁴ NuData Security Network, 2021
⁵ Mastercard, 2021
⁶ Javelin Strategy & Research, 2021
⁷ Juniper Research, 2019

