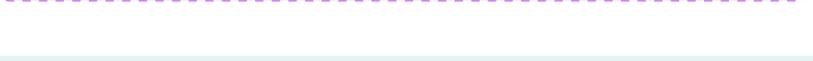
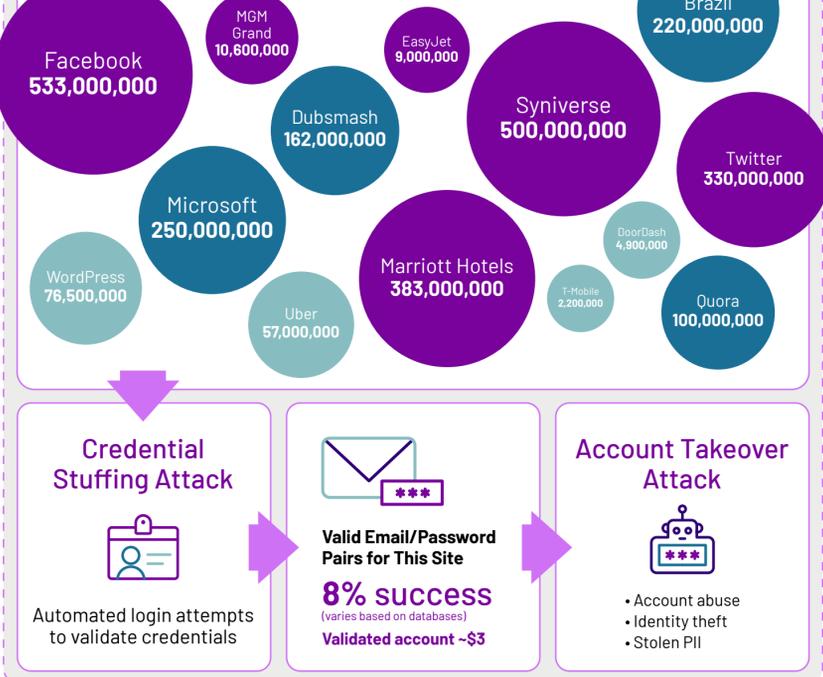


# Are You Prepared for CREDENTIAL STUFFING ATTACKS?

## What is Credential Stuffing?

Credential stuffing is an attack in which **cybercriminals use bots to attempt logins on popular sites using stolen usernames and passwords**. If a login is successful, the validated credential pair is used by the cybercriminals to **commit account takeovers or sold on the dark web**.



## It is Cheap and Easy to Run Credential Stuffing Attacks

There are more than **26 billion** credentials up for sale on the dark web

Lists of **billions of credentials** can cost as little as **2 dollars**

To rent a botnet for use in carding attacks, it can cost **only \$9 per hour**

## Credentials Are a Renewable Resource

**66%** of people reuse passwords across multiple online accounts



**60%** of account takeover victims use the compromised password across multiple online accounts



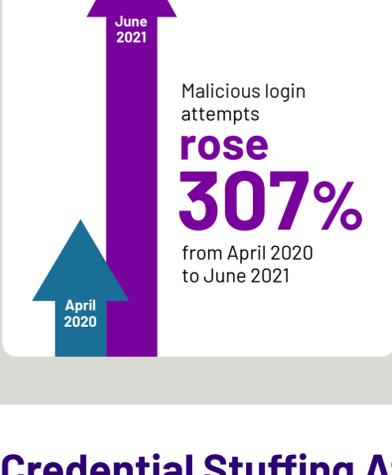
## Why Credential Stuffing Attacks Are So Difficult to Detect

It is **very easy to launch a highly distributed campaign with bots** that pretend to be browsers. Because the number of requests from a single source is small and doesn't exceed the limit of requests from an IP address, bot **Credential Stuffing attacks fly under the radar**.

**366,000** login attempts  
**>1,000** different IP addresses  
**10,000** attempts per hour

**77%** of these attacks would go **undetected** by volumetric detection

## Credential Stuffing Attacks are On the Rise



Malicious login attempts averaged **82% of all login attempts** in the **second half of 2021** (up from **75%** in the **first half of 2021**)

Malicious login attempts account for up to **94% of total login attempts** during credential stuffing attack peaks

## Credential Stuffing Attacks Cause Financial Losses

When cybercriminals launch successful credential stuffing attacks, they can take over users' accounts and commit fraud. **This has a lasting impact on businesses and consumers.**

ATO losses are up **72%** year over year

U.S. businesses lose nearly **\$7 billion** annually due to **ATO attacks**

Up to **80%** of e-commerce operational costs are **negatively affected by bad bots**

Malicious bots **negatively impact 18-23%** of e-commerce revenue

## Business Impact of Credential Stuffing Attacks

- High operational costs** for infrastructure and bandwidth
- Increased demand** for customer resources
- Damage to brand reputation** and consumer trust
- Burden on IT** to manage bad bots
- Refunds, chargebacks** and make goods
- Law suits and regulatory **fin**es
- Dive** in stock prices

## How Can You Stop Credential Stuffing Attacks?

**HUMAN Bot Defender** leverages machine learning, behavioral analysis and predictive analytics to detect and stop sophisticated credential stuffing bot attacks with unparalleled accuracy.

**HUMAN Credential Intelligence** prevents the use of compromised credentials on your site, providing an early warning system that flags stolen usernames and passwords for mitigating action, before fraud occurs.

Advanced bot detection and mitigation services can **reduce the negative impact of malicious bots by more than 50%** at times of peak bot traffic.



**" I found HUMAN to be the ultimate vendor with [an] amazing support team, great vision, and an ever-growing hunger for success. "**

– Reference Customer from the Forrester Wave™: Bot Management, Q2 2022

SOURCES: Aberdeen Strategy & Research: Quantifying the Impact of Bad Bots on E-commerce Merchant Profitability; Account Takeover 2021 Annual Report; Prevalence, Awareness and Prevention; Digital Shadows: From Exposure to Takeover: The 15 Billion Stolen Credentials Allowing Account Takeover; Forrester: The Forrester Wave™: Risk-Based Authentication; Google/Harris Poll: The United States of P@ssw0rd\$; Javelin Strategy & Research: Identity Fraud Report; New York State Office of the Attorney General: Attorney General James G. Graney's Call to Action on Identity Theft; Identity Theft; PerimeterX: Automated Fraud Benchmark Report; Sift: Q3 2021 Digital Trust & Safety Index; Threatpost: Billions of Passwords Offered for \$2 in Cyber-Underground; Trend Micro Research: Shifts in Underground Markets: Past, Present, and Future.