HUMAN

Are You Prepared for CARDING ATTACKS?

What Are Carding Attacks?

Carding is an attack in which cybercriminals use bots to **test stolen credit card and debit card data by making small purchases** on e-commerce sites. **Validated cards are used to make subsequent fraudulent purchases** of products or gift cards, which are then converted into high-value goods and resold online. Gift card cracking is a type of carding where cybercriminals validate gift card numbers in a brute force attack.

It is Cheap and Easy to Run Carding Attacks

There are more than **4 million** **credit card details for sale** on the dark web

The average price of a **credit card number is** **10 dollars**

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

Carding Attacks Are On the Rise

2021

2020

Carding attacks **increased** **112%** YoY from 2020 in 2021 in terms of total normalized requests

Card-not-present fraud is **81% more likely** than point-of-sale fraud

Carding Attacks Cause Financial Losses

Digital card-not-present fraud is predicted to hit **$130B by 2023**

2020 2021 2022

Every dollar in fraud **costs merchants** **$3.36** due to chargebacks, fees and replacement of lost merchandise

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 Carding 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

Lawsuits and regulatory **fines**

Dive in stock prices

How Can You Stop Carding Attacks?

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

The key to preventing carding attacks is to switch from profiling environments to focusing on behavioral anomalies and characteristics. HUMAN Bot Defender leverages machine learning, behavioral analysis and predictive analytics to detect and stop sophisticated carding attacks with unparalleled accuracy.

> "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; PerimeterX: Automated Fraud Benchmark Report; FinTech Report: Over 4 Million Credit Card Details for Sale on the Dark Web; Javelin: Identity Fraud Report; Juniper Research: Online Payment Fraud: Emerging Threats, Segment Analysis and Market Forecasts 2021-2025; LexisNexis Risk Solutions: True Cost of Fraud Study: e-Commerce/Retail Edition; PreciseSecurity: Credit Card Frauds Top the List of US Identity Theft Crime; Trend Micro Research: Shifts in Underground Markets: Past, Present, and Future.

Learn more at www.humansecurity.com