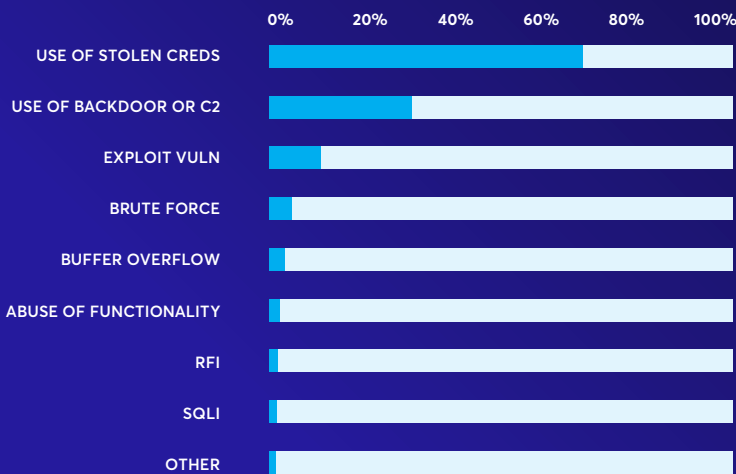# STOPPING ACCOUNT TAKEOVER ATTACKS

How hackers are increasing their success rates, and what you can do about it

01 – SCOPE OF THE PROBLEM

Top hacking action varieties

Source: Verizon 2019 Data Breach Investigations Report

	0%	20%	40%	60%	80%	100%
USE OF STOLEN CREDS						
USE OF BACKDOOR OR C2						
EXPLOIT VULN						
BRUTE FORCE						
BUFFER OVERFLOW						
ABUSE OF FUNCTIONALITY						
RFI						
SQLI						
OTHER						

$290 Out-of-Pocket Costs

Victims of credential theft pay on average $290 in out-of-pocket costs and spend 16 hours to resolve the incident.

– Javelin Strategy & Research

$48 Billion Lost

Organizations are expected to lose $48 billion by 2023 due to fraudulent online transactions.

– Juniper Research

No.1 Attack Vector

Credential theft was the number one attack vector used by hackers to get into web applications.

– Verizon 2019 Data Breach Investigations Report

02 – THE ANATOMY OF ACCOUNT TAKEOVER ATTACKS

1 DATA HARVESTING

2 CREDENTIAL VALIDATING

3 EXPLOITING CREDENTIALS

Account takeover attacks have three phases:

1. Harvesting the Data – to generate a list of credentials to work with.

2. Validating the Credentials – to identify good username/password combinations (password spraying) and see which ones work (credential stuffing).

3. Exploiting the Credentials – to login and download personal data, complete transactions, disrupt service, or gain access to other resources to carry out further attacks.

Castle

4 TACTICS ATTACKERS ARE USING TO INCREASE ACCOUNT TAKEOVER SUCCESS RATES

Traditional success rates of account takeover attacks have been approximately **.1%**, but over the past year, new attack patterns have emerged that increased success rates up to **20-30%.**
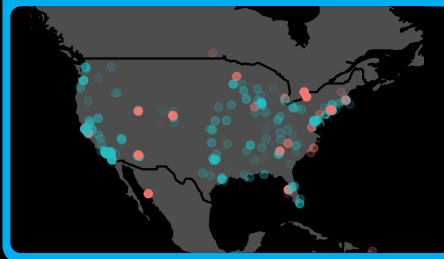
– Castle Research

The following are **four** tactics that attackers are leveraging, uncovered by Castle research:
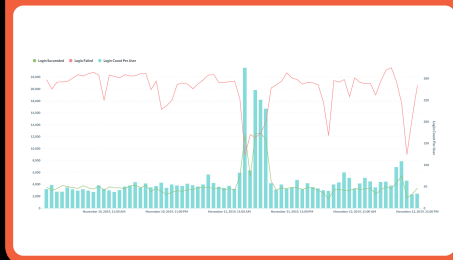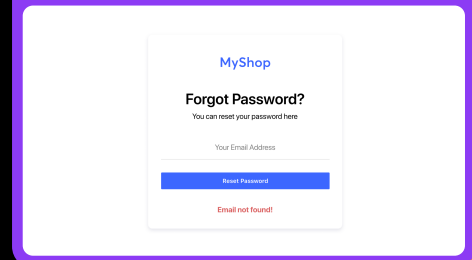
TACTIC 1
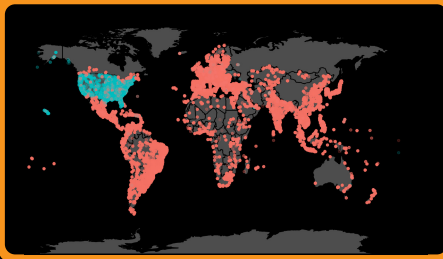
Appear larger by using more IPs

TACTIC 2

Appear local by using local IPs

TACTIC 3

Appear better by using fake accounts to improve reputation

TACTIC 4

MyShop

Forgot Password?
You can reset your password here

Your Email Address

Reset Password

Email not found!

Appear legitimate by using registration and password resets

What You Can Do to Defend Your Digital Business from Account Takeover Attacks

The best ways to protect your digital business from account takeover attacks is to look for the following features:

• Real-time anomaly and attack detection
• Pre and post-login protection
• Real-time user analytics and insights
• Automated account recovery
• Risk-based authentication
• Custom risk-based user journeys

To learn more about these tactics and how to protect your site and online service, check out this ebook.

Castle