

Protect Your Online Business from Credential Stuffing

Stay Ahead of Threats with Advanced Bot Management Technology



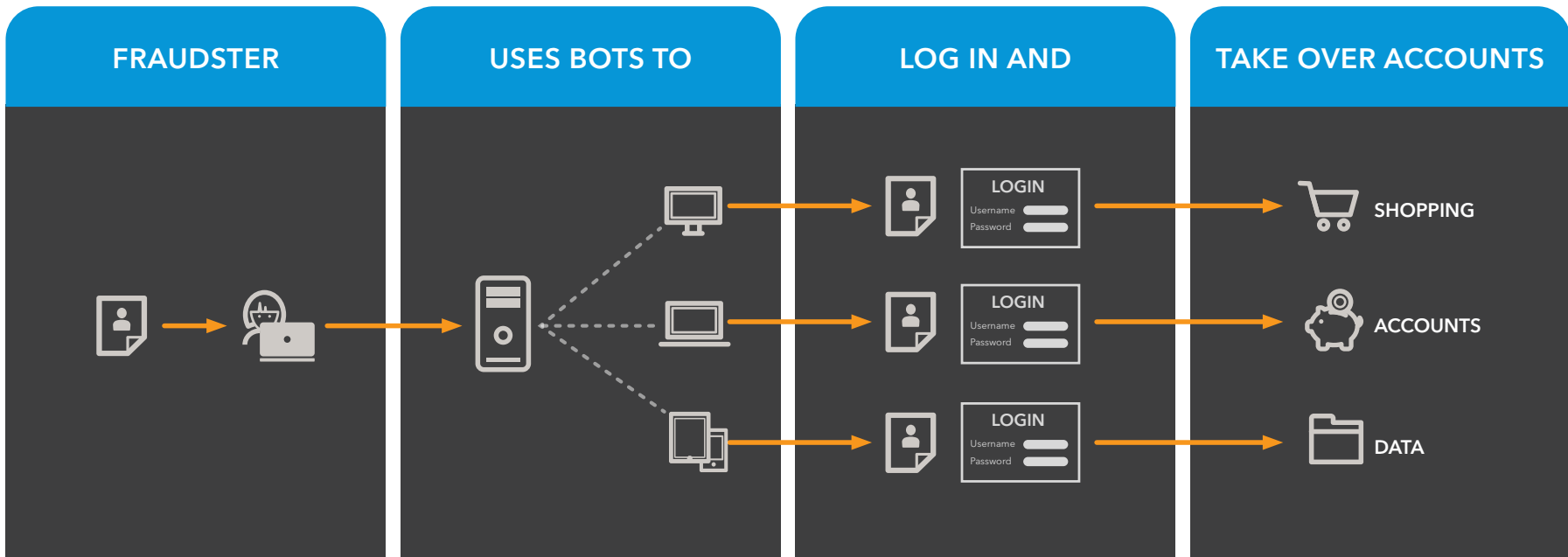
“

The total cost associated with credential stuffing – including fraud-related losses, operational security, application downtime, and customer churn – can range from \$6 million to \$54 million annually.”

Source: The Cost of Credential Stuffing, Ponemon Institute

CREDENTIAL STUFFING

ACCOUNT TAKEOVER



How Credential Stuffing Works

An attacker uses bots to continuously ping your website pages (usually the login or account page) with user credentials purchased from the dark web. The attacker keeps track of which credentials work, then sells the validated credentials to other fraudsters who use them to log into your site and take over customer accounts, buy

merchandise, or commit other fraudulent activity – usually taking in a hefty profit for their efforts. And their profit is your loss. You lose revenue, customers, reputation ... you might even suffer more monetary losses if you are not in compliance with regulations and have to pay penalties and legal fees.




With the proliferation of online applications, most users don't practice good internet hygiene – often repurposing the same login credentials across multiple accounts. That makes every online business with a login page a potential target for credential stuffing, whether you've had a data breach or not.

Your network and data can be properly secured, but your business is still exposed to fraud if you can't see and stop credential stuffing before a successful combination is found. In a survey by Ponemon Institute, more than half of respondents reported credential stuffing as a significant security challenge for their companies. Additionally, *nearly 70% of respondents said they did not feel (or were unsure if) their companies had adequate visibility into these attacks.*

This makes sense, because recent industry estimates indicate there are *billions of stolen credentials (usernames, passwords, and email addresses) currently circulating on the dark web.*

**Akamai observed
26.95 billion
credential stuffing
attempts during
Q1 2020 –
a 256% increase
from the amount
observed in
Q1 2019.**





Akamai notes that bots are responsible for 30% to 70% of total traffic to websites.

Credential Stuffing Is Automated – Bot Management Is Your Best Defense

Unfortunately, login requests resulting from credential stuffing do not have patterns you can easily identify and block. Verified credentials are valid requests – the login information is legitimate, but the entity attempting to authenticate into an account is not – making them nearly impossible to spot.

Fortunately, credential stuffing is not likely to be accomplished manually. Validation is typically automated, which makes bot management the best defense against this problem.

Your ability to stop credential stuffing attacks depends on how well you can detect and mitigate bots.



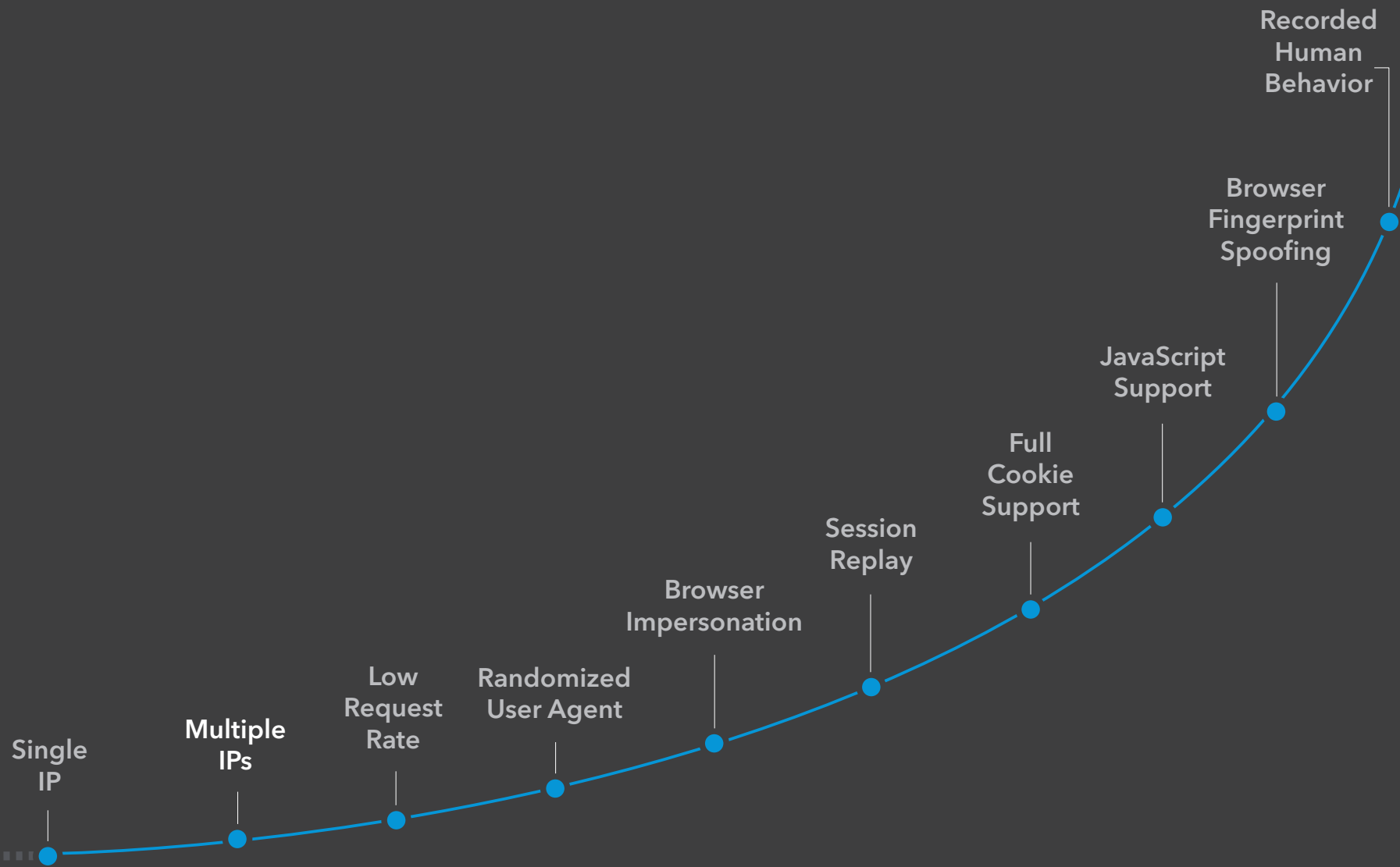
Bot management software allows you to:

- More easily identify automated abuse, since login requests generated by bots are easier to catch than account takeovers involving humans
- Lower the incidence of account takeover attempts by reducing the number of validated credentials available to fraudsters
- Make your website less attractive to fraudsters, who often move on to less-protected targets

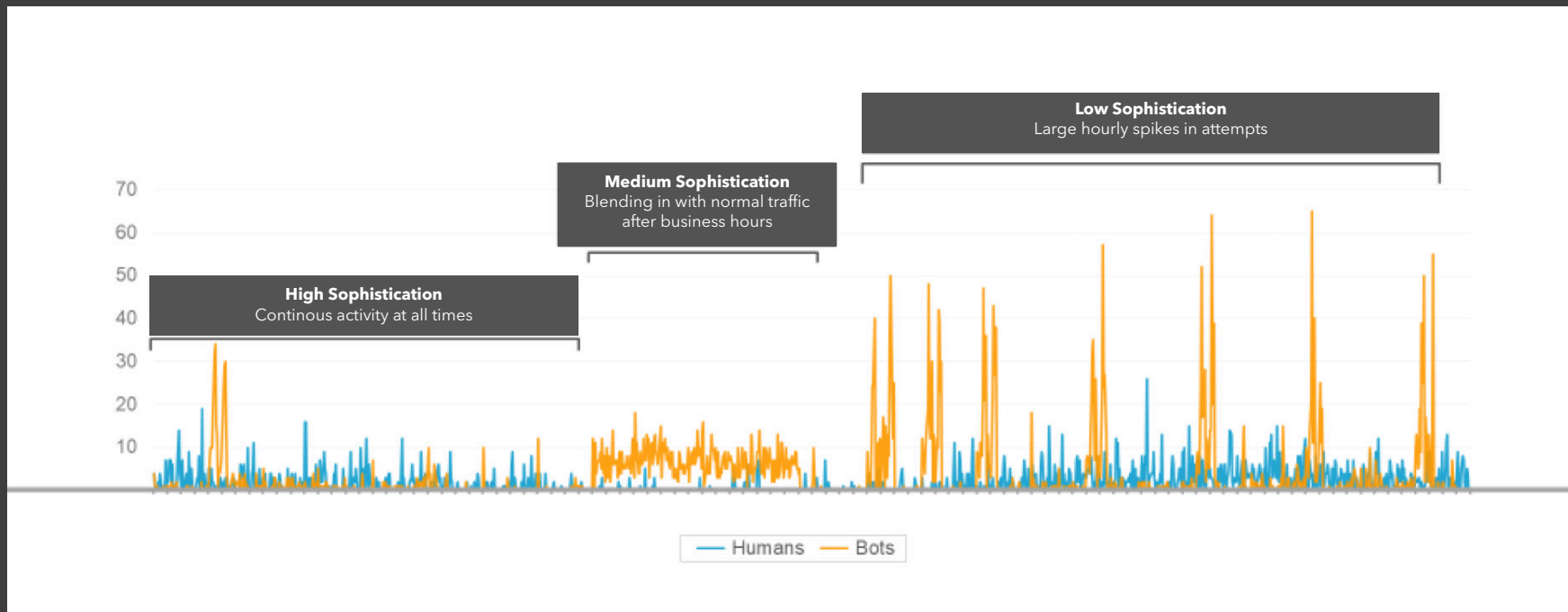
If a fraudster sees that you've found the bot, they will try to figure out how you detected it, then update the software to avoid the original detection and try again. Because of the significant profit opportunities, credential stuffing attracts some of the most sophisticated bot operators and has a fast rate of bot evolution. Protecting your organization and your customers means evolving as quickly as the bots are.

**Bots are smart
and persistent –
your bot
management needs
to keep up with
evolving threats.**





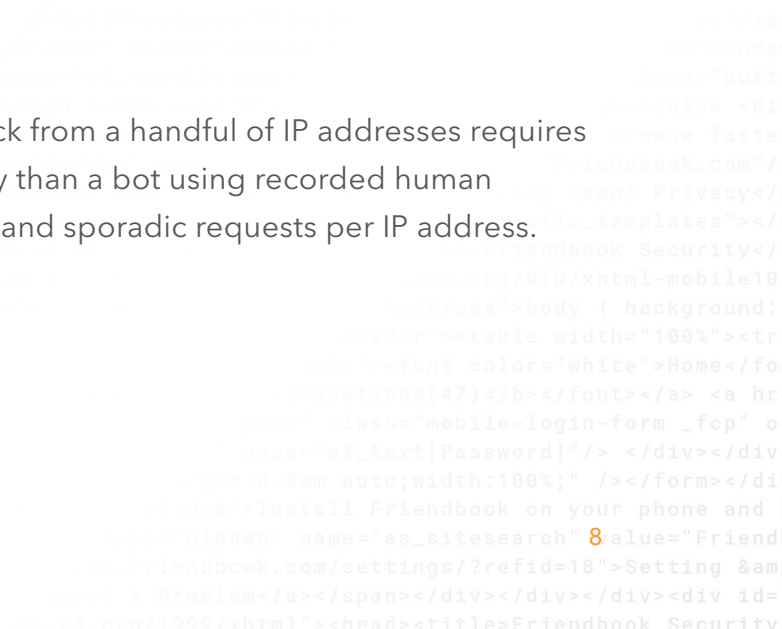
Looking at bot technologies and capabilities in escalating sophistication



Looking at bot sophistication by traffic pattern with a variety of levels detected in a 24-hour period

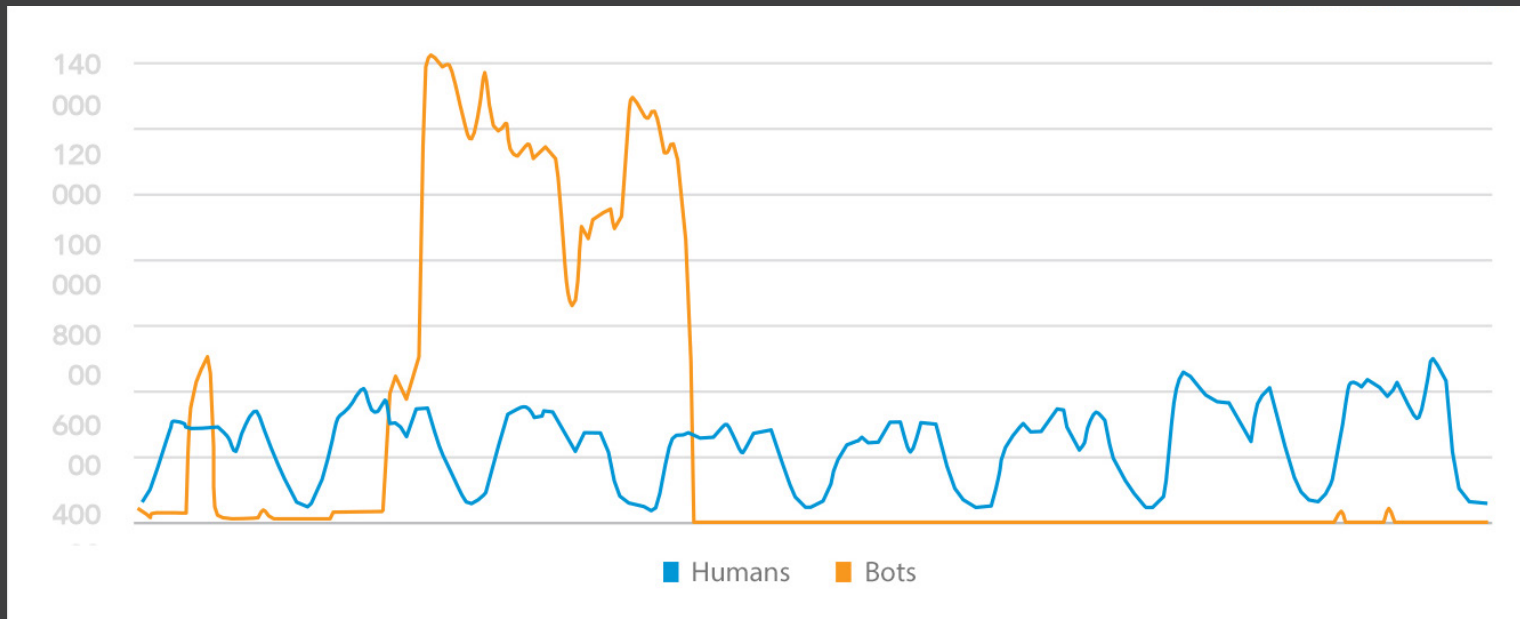
And it's not just the bot itself, but its attack approach. For example, if you're only looking for big spikes in login attempts, much more serious activity can go undetected. Most websites interact with a range of threats every day – from obvious automation to the most evasive bot behavior.

A brute-force attack from a handful of IP addresses requires a different strategy than a bot using recorded human behavior with few and sporadic requests per IP address.



CASE STUDY

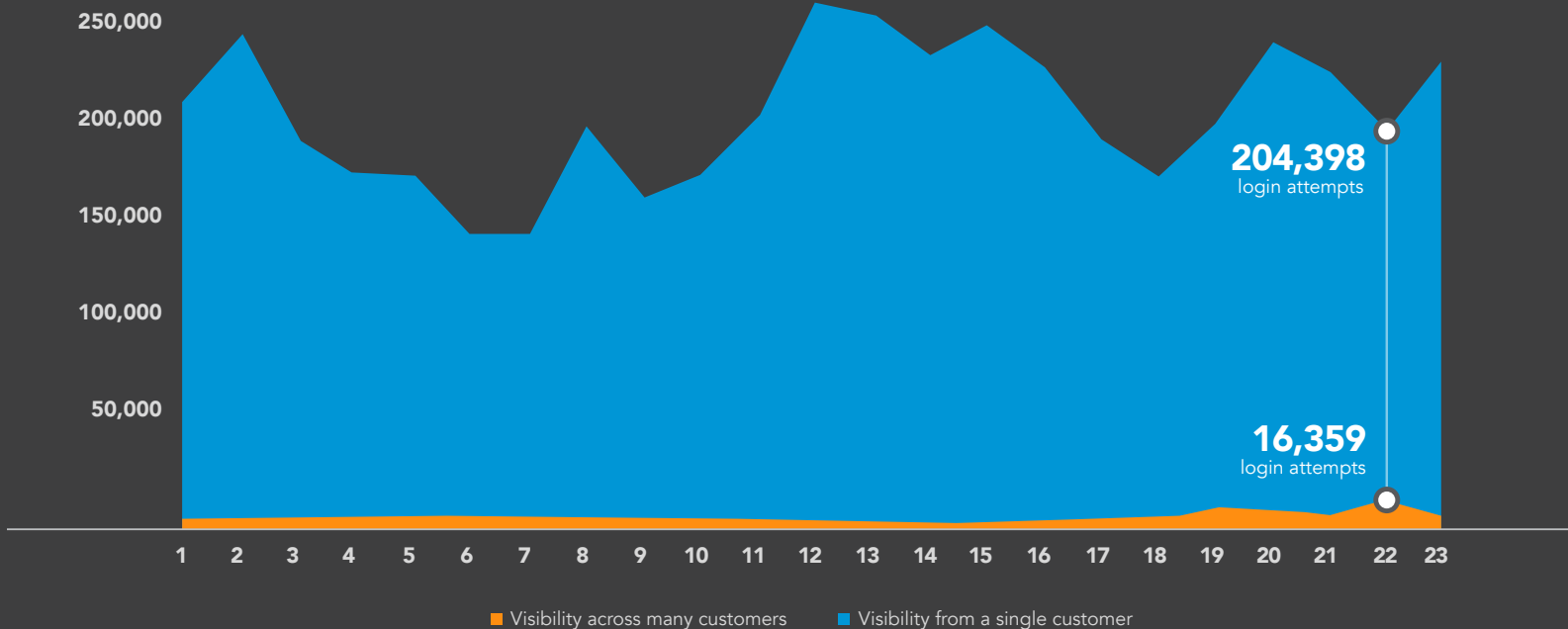
After a large attack peaking at more than 131,000 requests per hour, a leading fashion retailer began to block bot traffic with Akamai Bot Manager Premier. Not only did the detected bot login traffic fall to a statistically insignificant amount, but the level of human login traffic did not change.



The number of login attempts made by humans and bots to a login page for a leading fashion retailer over an 8-day period

CASE STUDY

A Global 500 financial services group found its pensions site, which typically processes 20,000 invalid login attempts per day, began receiving 50,000 invalid login attempts every five minutes. During the attack, the infrastructure struggled as users received session timeouts or were unable to log in to their accounts. Quick deployment of Akamai Bot Manager Premier immediately halted the attack and prevented the bot operator from taking out fraudulent loans against actual customer accounts.



■ A larger snapshot of internet traffic illuminates more sophisticated bot activity

Deny Bot Logins Without Sacrificing Customer Experience

More than 70% of Ponemon Institute survey respondents agreed that preventing credential stuffing attacks is difficult because fixes that curtail criminals may diminish the web experience of legitimate users.

Advanced machine-learning technology and behavior anomaly analysis used against these more sophisticated threats lead to better accuracy. The more finely tuned the algorithm, the more precise the analysis to minimize performance impact and false positives that can inadvertently block legitimate user logins.

Calculate the Financial Impact of Credential Stuffing

You can estimate the impact by quantifying the scope of activity and tying it to known metrics like:

- Money lost to fraud – the average value of fraudulent transactions using stolen credentials
- Cost of prevented fraud – reducing the incidence of compromised accounts lowers the cost of anti-fraud solutions your organization may be using
- Remediation cost – notifying customers to change their credentials costs less than assigning a representative to a fraud investigation
- Value of a lost customer – customers who suffered account takeovers are unlikely to stay with your organization



If 20 of your user accounts are compromised every month, your company stands to lose \$576,000 in one year.

Average based on following assumptions:

- 1,000,000 fraudulent login attempts / month
 - 20 compromised accounts / month
 - \$.01 per lookup for anti-fraud solutions
 - \$500 average fraudulent transaction value
 - \$1,000 remediation costs / account
 - \$2,000 average customer lifetime value
 - 20% attrition rate attributed to compromised accounts
- $1,000,000 \times \$0.01 = \$10,000$ reduced fraud prevention cost / month
 - $20 \times \$500 = \$10,000$ prevented fraud costs / month
 - $20 \times \$1,000 = \$20,000$ prevented remediation costs / month
 - $20 \times 20\% \times 2,000 = \$8,000$ lost customer value / month
- $\$10,000 + \$10,000 + \$20,000 + 8,000 = \$48,000$ total value / month



Consider the Akamai Difference

With a significant portion of all web traffic traversing its network daily, including some of the largest and most frequently attacked sites in the world, Akamai is uniquely positioned for deep visibility into legitimate application use as well as the constantly evolving attack behaviors of malicious bots. It has the latest bot detection technologies that are proven to identify the most sophisticated bots today.

Its complete online security portfolio is designed to help customers manage bot traffic on the Akamai cloud delivery platform at the network edge, before reaching their websites and infrastructure. Akamai can help enterprises manage the business and IT impacts of bot traffic to protect customers, company, and brand.



In one credential abuse attack, Akamai observed a botnet of nearly 13,000 IP addresses, with each member averaging one login attempt every two hours. Altogether, the botnet sent 167,039 login attempts over 24 hours, and 123,909 unique accounts were targeted."

Source: Improving Credential Abuse Threat Mitigation

Learn more about how to manage and mitigate bot threats such as credential stuffing at akamai.com/bots.

[Contact us](#) to find out how Akamai's new advanced bot management technologies can enhance your online security strategy.



Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or [@Akamai](#) on Twitter. You can find our global contact information at akamai.com/locations. Published 07/20.