



Attacker Economics

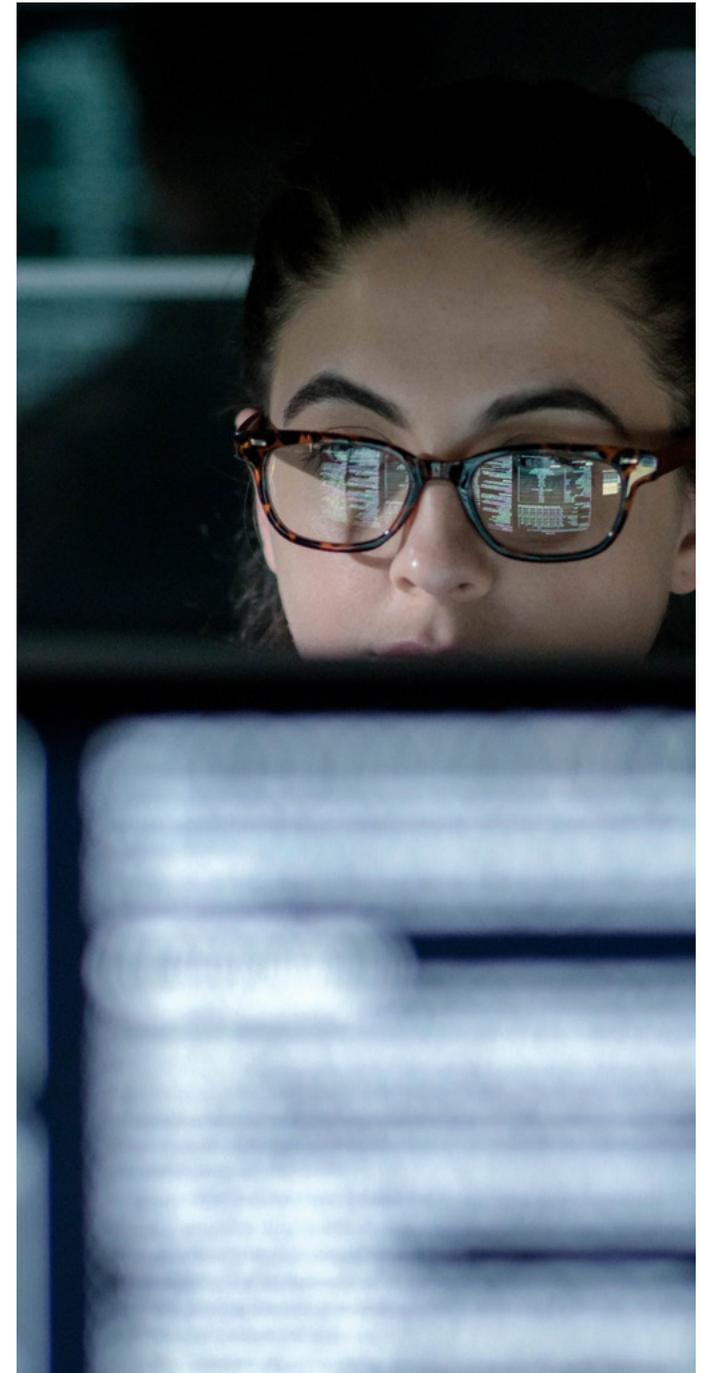
UNDERSTANDING THE ECONOMICS BEHIND CYBER ATTACKS—
WHAT MAKES YOUR COMPANY A PRIME TARGET?

INTRODUCTION

Automated attacks are proliferating against organizations around the globe. As the cost and investment of launching these attacks continues to plummet, companies are increasingly experiencing credential stuffing attacks that can lead to account takeover and fraud.

The ingredients required for these attacks—previously compromised consumer credentials found on the dark web, tools to orchestrate an attack, and botnets to execute the attack—are becoming less expensive to buy, or even rent. As a result, successful credential stuffing attacks can net an attacker a nice pay day. The decision to launch such an attack is a simple cost-benefit analysis that can all too easily tip in the attacker’s favor.

Just as you routinely evaluate the cost of a big purchase against its value, attackers must decide the best place to spend their time and resources. If the opportunity is cheap and the value is astronomical, the ROI is high and the decision is easy.



HOW MUCH DOES IT COST TO ATTACK YOU?

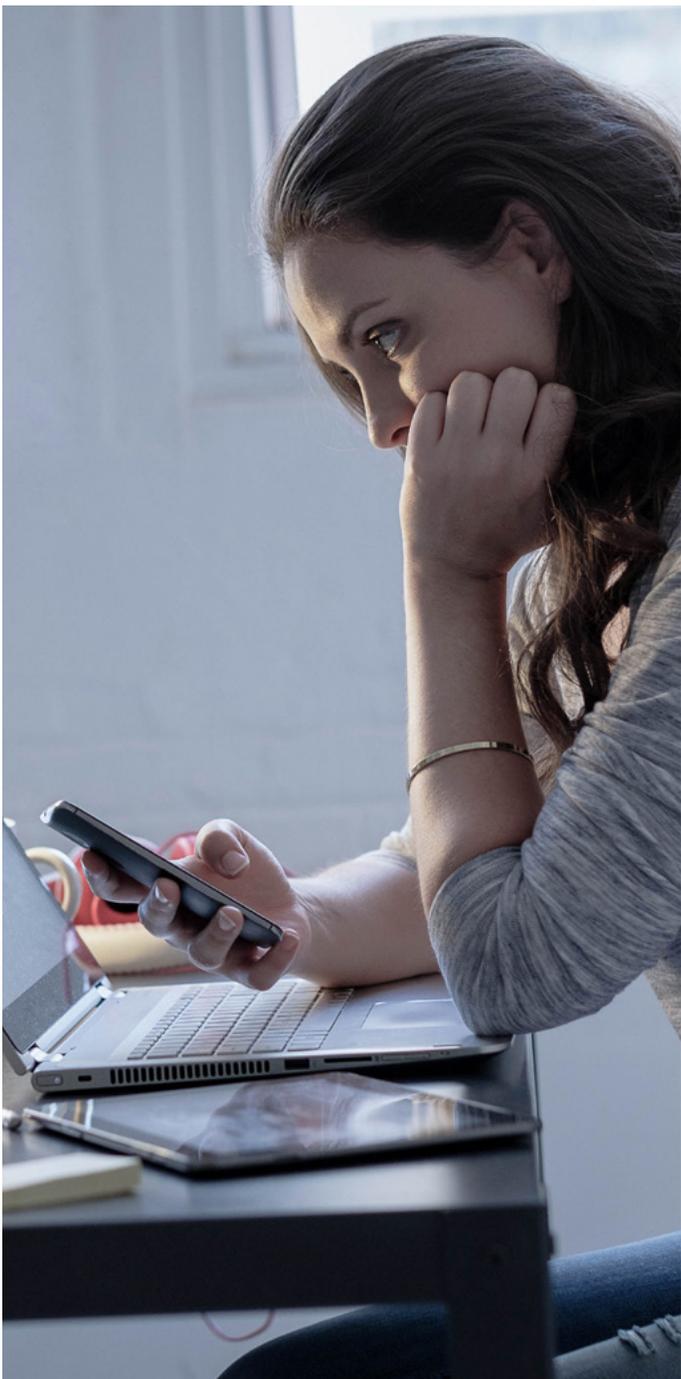
As attackers look for businesses to target, are you the low-hanging fruit? Does it cost less to attack your company than the one next door? Many IT professionals are expanding their knowledge of attack surfaces such as APIs that can be exposed on web and mobile applications.

The economics of mounting automated attacks against online applications are like buying a raffle ticket. Attackers weigh the cost to play against the chance of success and the value of the “prize.” It’s important to note that this prize will be different for every company depending on the value of the account and the attacker’s specific motivations—whether it be compromising accounts for monetary gain or

obtaining access to company data in order to manipulate pricing.

For example, an automated attack on a customer loyalty program may result in account takeover, draining of customer points, and resale for profit—fraud that can result in massive losses, customer abandonment, and a damaged brand.





THE LAW OF BIG NUMBERS

Automated attacks capitalize on the law of big numbers. Credential stuffing success rates typically hover between 0.2 and 2%—and attackers don't need a high success rate because billions of credentials are available for free or at nominal cost.¹

The calculation below illustrates why credential stuffing attacks have become cost-effective for cybercriminals. There's significant value in every successful account takeover (ATO). On the dark web, attackers can find the value of accounts for companies in specific industries or that share similar business models—and then tailor their attacks for maximum success.

| | |
|------------------------------|--|
| \$0: 2.3 billion credentials | } Less than \$200 for 100,000 ATO attempts |
| \$50: for tool configuration | |
| \$139: for 100,000 CAPTCHAs | |
| \$10: for 1,000 global IPs | |

Attackers want to make their job easier, so they typically consider how much it costs to set up the automated attack—including the credentials, automation tools, and botnets—versus the estimated return. These attacks can provide a solid ROI for cybercriminals even when the value per transaction is low.

THE ATTACKER EQUATION

Attackers leverage automation and bots in an attempt to access and take over user accounts to extract monetary value, but they also may be using them for other purposes such as validating gift cards or scraping important company data such as inventory or pricing. As attackers scale and aim their tools at multiple target applications or websites, the rate of return becomes far more attractive—especially if the cost and initial investment remain static. This is one reason why credential stuffing attacks have become increasingly common.

To determine the rate of return, multiply the **value of the attack** by the **chance of success**, and **divide by the cost**. Then subtract the **initial investment (100%)**.

$$\frac{\text{VALUE} \times \text{CHANCE OF SUCCESS}}{\text{COST}} - 100\% = \text{RATE OF RETURN}$$

If bad actors launch an attack on a business with only 100 users, they have little chance of financial success. Probably only one to two accounts will be compromised. But if they attack a major bank with 50 million customers, they can expect to compromise between 100,000 and 1 million accounts. That's a scary proposition.

The classic Las Vegas penny slots work on the same principle. Players happily keep feeding the slot machines with pennies (nickels and quarters today), even when the potential payout is minimal. This is a low-cost way to obtain even a small cash prize where the value outpaces the cost. The buy-in gets higher for table games, but so are the potential winnings.

The same principle applies to automated attacks that replay stolen consumer credentials against multiple e-commerce sites to gain account access, which can lead to large-scale account takeover. If there is value in the accounts and the attacker is skilled, chances are the outcome will be negative. Businesses in e-commerce,

airline ticketing, money transfer, and banking services will cumulatively lose an estimated \$200 billion to online payment fraud between 2020 and 2024, driven by the increased sophistication of credential stuffing, account takeover, and fraud—and the growing number of attack vectors.²

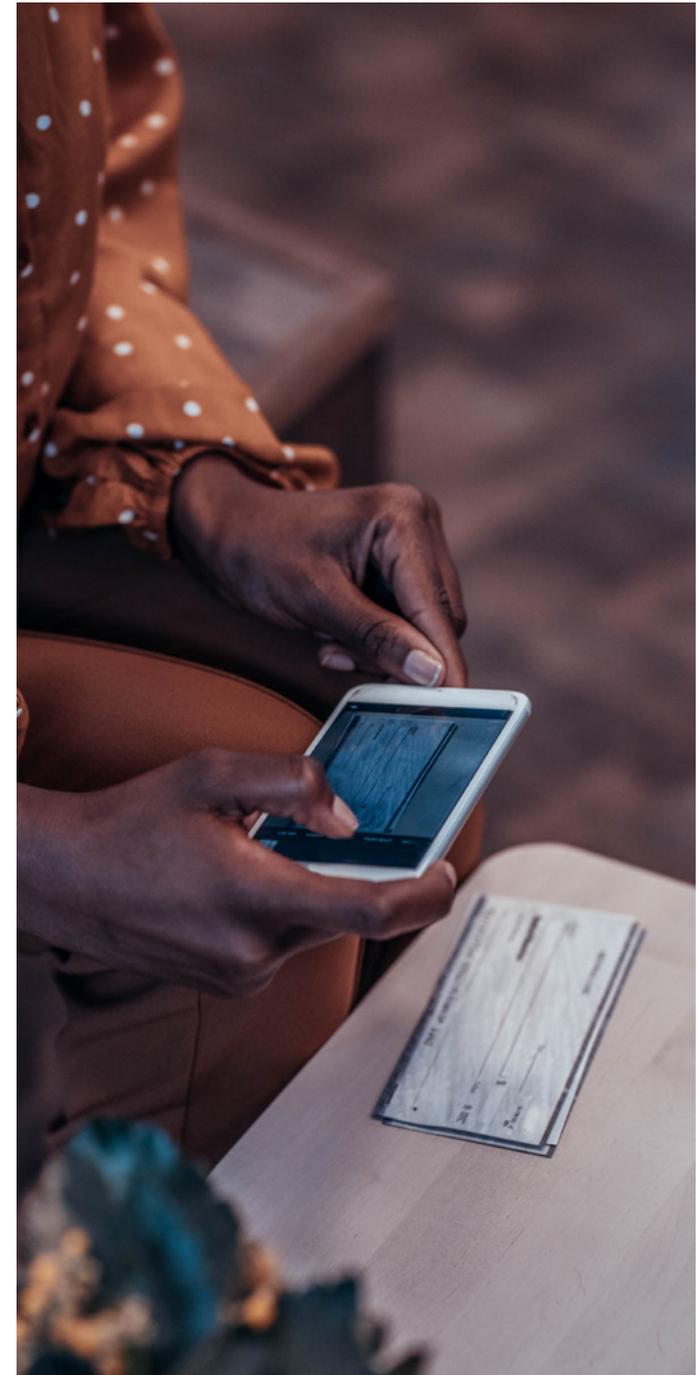
If credential stuffing attacks on your application have a high probability of success, you just gave attackers a golden ticket. On the flip side, if the chance of success drops due to the cost of penetrating the defense mechanisms you've put in place, this can severely diminish the ROI. The attacker may decide it's not worth the effort and target another company.

ATTACKS EXPLOIT APPLICATION LOGIC

Most companies understand that if attack costs are low and the financial rewards for cybercriminals are high, they're sitting ducks for attacks. Automated attacks such as credential stuffing that target bank, retail, or airline accounts are designed to steal money, period. Attacks of this kind are straight-up financial fraud—and the tools of the trade are increasingly less expensive.

Inevitably, the cost of entry to each generation of attacks will drop over time. You've probably watched the same pattern unfold across consumer technologies. For example, the cost of installing home solar panels dropped from \$2 per watt in 2010 to \$0.20 per watt in 2019.³ More dramatically, a 1-megabyte hard drive cost \$1 million in 1967.⁴ In 2017, the same capacity on a hard disk drive would have set you back by about two cents.

Even companies with seemingly airtight application security practices and tools eventually find themselves vulnerable to credential stuffing attacks. Readily available tools, infrastructure, and compromised credentials lower the investment required by the attacker at the same time the rapid shift to online commerce increases the value in customer accounts—resulting in attractive attacker economics. Most importantly, credential stuffing and other automated attacks abuse what could otherwise be securely coded applications. That's because instead of exploiting weaknesses or vulnerabilities in the application, cybercriminals are abusing application logic.





CREDENTIAL STUFFING IS A COMMON TYPE OF ATTACK

Usernames and passwords are commonly re-used across multiple applications. In fact, a recent password security report from LastPass shows that employees reuse a password an average of 13 times.⁵ Furthermore, even when consumers are notified that their accounts have been breached, only about a third change their passwords.⁶ Credential stuffing replays these pairs siphoned during large corporate breaches across consumer sites and services, including banks, retail sites, video and social media platforms, home automation services, and more. These attacks are effective because there's a high probability that passwords used on one site are repeated on another, and again, the economics are attractive for attackers.

A successful credential stuffing attack unfolds in four stages:

1. Get credentials

In the past, credentials were tricky for attackers to find. Now, they're readily available. Attackers can use sites such as RaidForums and Pastebin or find advertised lists on Twitter through accounts like @checkmydump. Fresh credentials—such as those stolen within the past one to two days—are more valuable and cost more for cybercriminals to buy. Stale credentials are less valuable because the chance of success using them is far lower.

2. Automate login

There are many different tools and frameworks available to help attackers automate the login process, and they all come with different price tags. Simple script-based tools, like cURL or Python, cost nothing, but are simple for security teams and tools to detect and block.

Sophisticated attackers use frameworks that more accurately simulate network, device, and user behavior. These attack tools become increasingly expensive to buy, rent, or use, but they're also more effective—and require more specialized security solutions to protect your applications.

3. Simulate relevant geography

Attackers know that sending billions of requests from one IP address will quickly raise flags. Proxy services make it both easy and affordable for attackers to ensure web traffic appears to be coming from local, relevant users. For example, a sudden flood of Ukraine-based traffic to a regional bank in New England would set off alarm bells. But when attackers can rent a botnet composed of U.S. and, even better, New England addresses, they're more likely to evade detection.

4. Defeat defenses

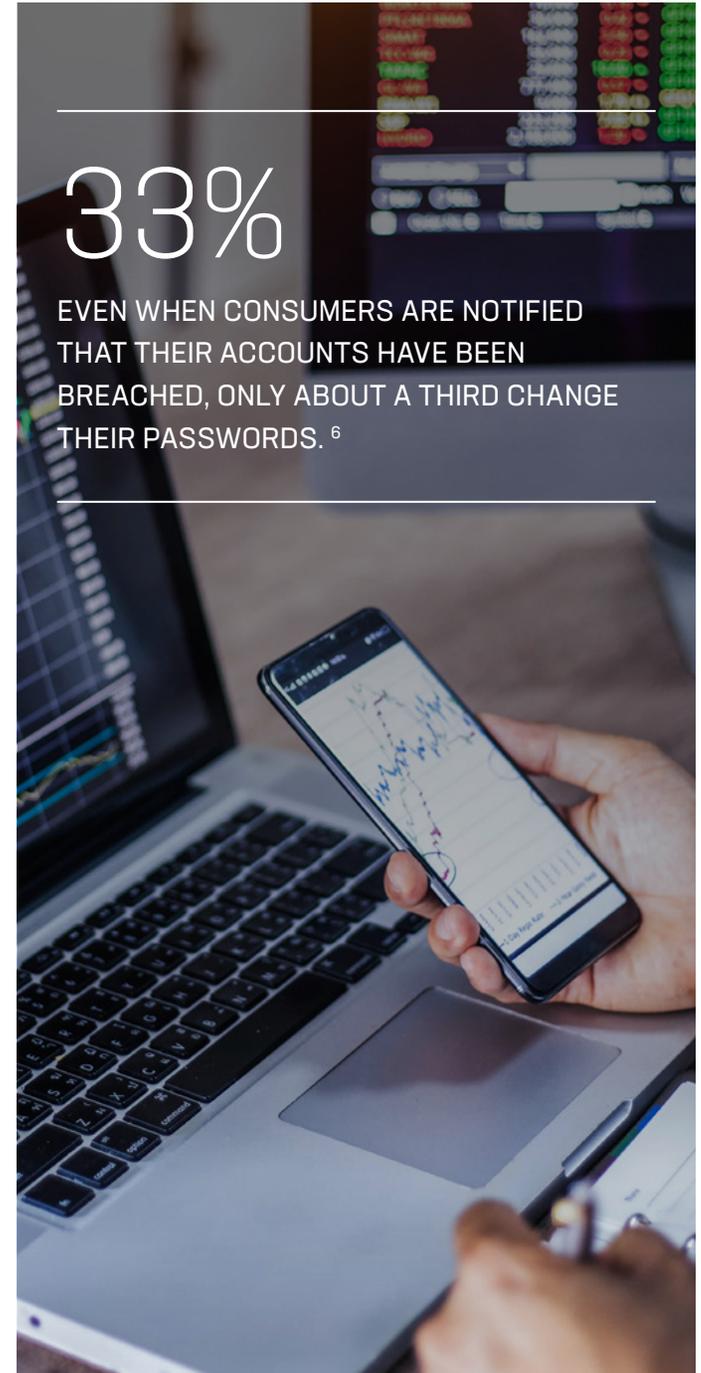
Generic solutions used by a wide range of companies are the easiest for attackers to defeat. For example, many organizations have tried to prevent automated attacks by implementing free or low-cost CAPTCHA solutions. In response, sites such as Death by

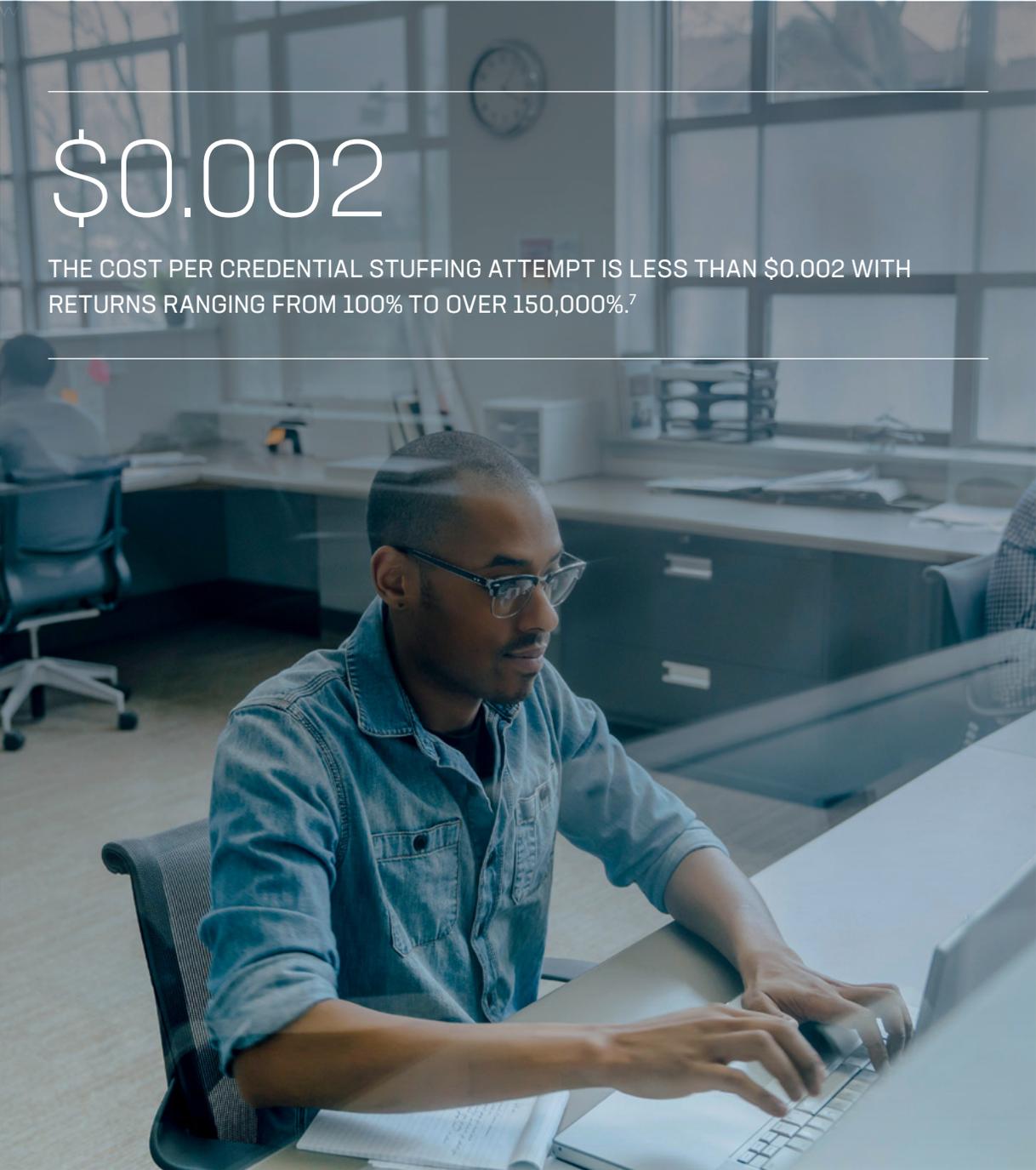
Captcha and XEvil have popped up to bypass these defenses. You don't even have to venture onto the dark web to find these tools; a quick browser search will surface hundreds of readily available tools.

Some companies believe multi-factor authentication (MFA) will stop the attacks, but it's not an ideal solution. Cybercriminals can still access accounts with a credential stuffing attack and gain MFA tokens using phishing, vishing, or other social engineering techniques. Plus, user challenges with MFA can frustrate legitimate users and lead to customer abandonment and lost revenue.

33%

EVEN WHEN CONSUMERS ARE NOTIFIED THAT THEIR ACCOUNTS HAVE BEEN BREACHED, ONLY ABOUT A THIRD CHANGE THEIR PASSWORDS. ⁶





\$0.002

THE COST PER CREDENTIAL STUFFING ATTEMPT IS LESS THAN \$0.002 WITH RETURNS RANGING FROM 100% TO OVER 150,000%.⁷

THE LADDER OF ATTACKER ECONOMICS

Financially motivated attackers will only invest as much as they need to reach their goal. If cybercriminals target an application with zero defenses and can successfully attack from their home IP address with a free cURL script and stale credentials from a dark web Pastebin, they will stay on this bottom rung. But if the app defenses block this attempt, the attackers will evolve to countermeasures and move up a rung. They might use slightly fresher, more costly credentials and tools that emulate device behavior.

If the next rung works, the attackers have no reason to move up the ladder and invest more money. But if the attack fails, they'll step up to better credentials and more sophisticated attack tools that emulate human behavior.

Understanding this ladder is the key to successfully defending your applications. Hardening your apps isn't the only solution because invasive security controls can frustrate users and jeopardize real customer interactions. Instead, you need to make it too expensive for attackers to get past your defenses. Force them to the top rung, where costs are so prohibitive that they give up and pick another target.

HOW TO DETECT AUTOMATED ATTACKS

How do you know if you are being attacked?

There are three important ways to start diagnosing automated attacks on your organization.

1. Examine application traffic patterns

Take a close look at your new account creation and login pages. These are the app pages that automated attacks and bots are most likely to attack. Even if the traffic looks normal, there's a good chance your applications are under siege.

2. Check your login success ratios

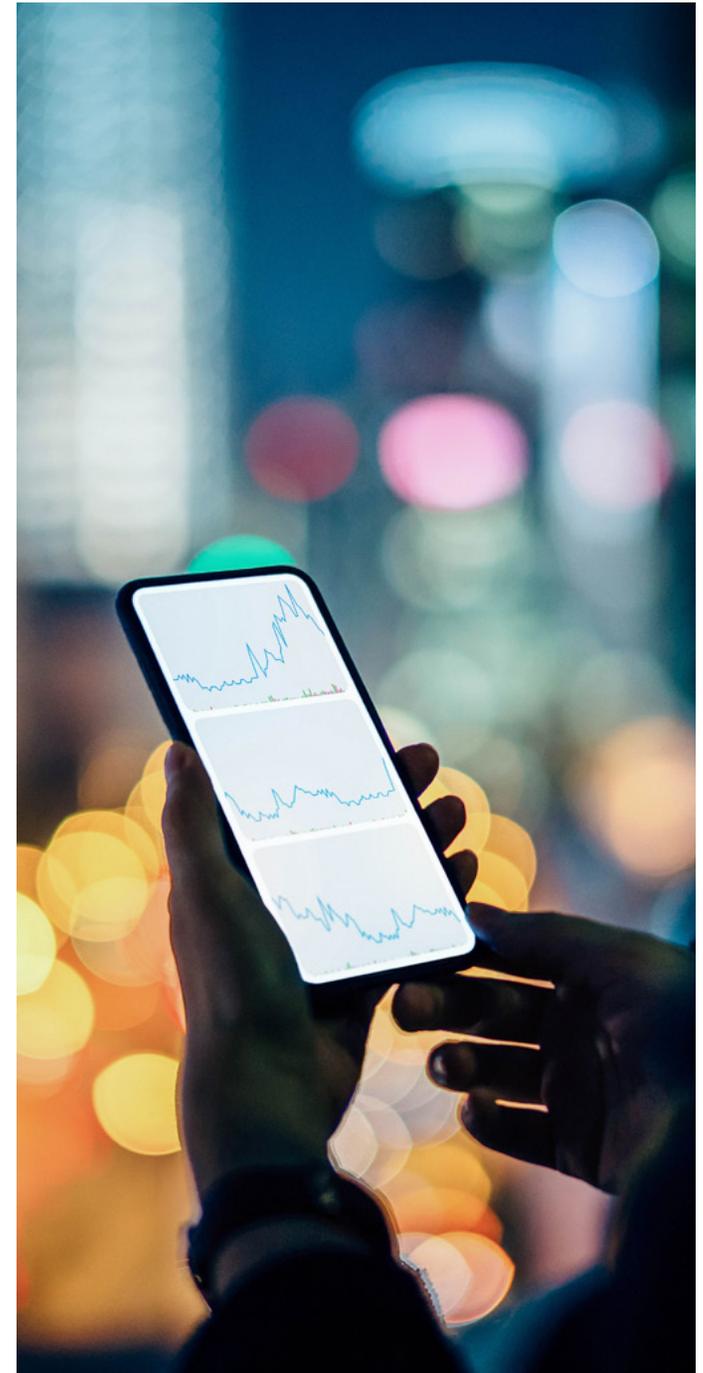
Across every industry, organizations can expect 60-85% login success rates.⁷ Higher or lower numbers are a sign that something is amiss, especially if the spike doesn't match discrete events such as promotions or viral marketing efforts.

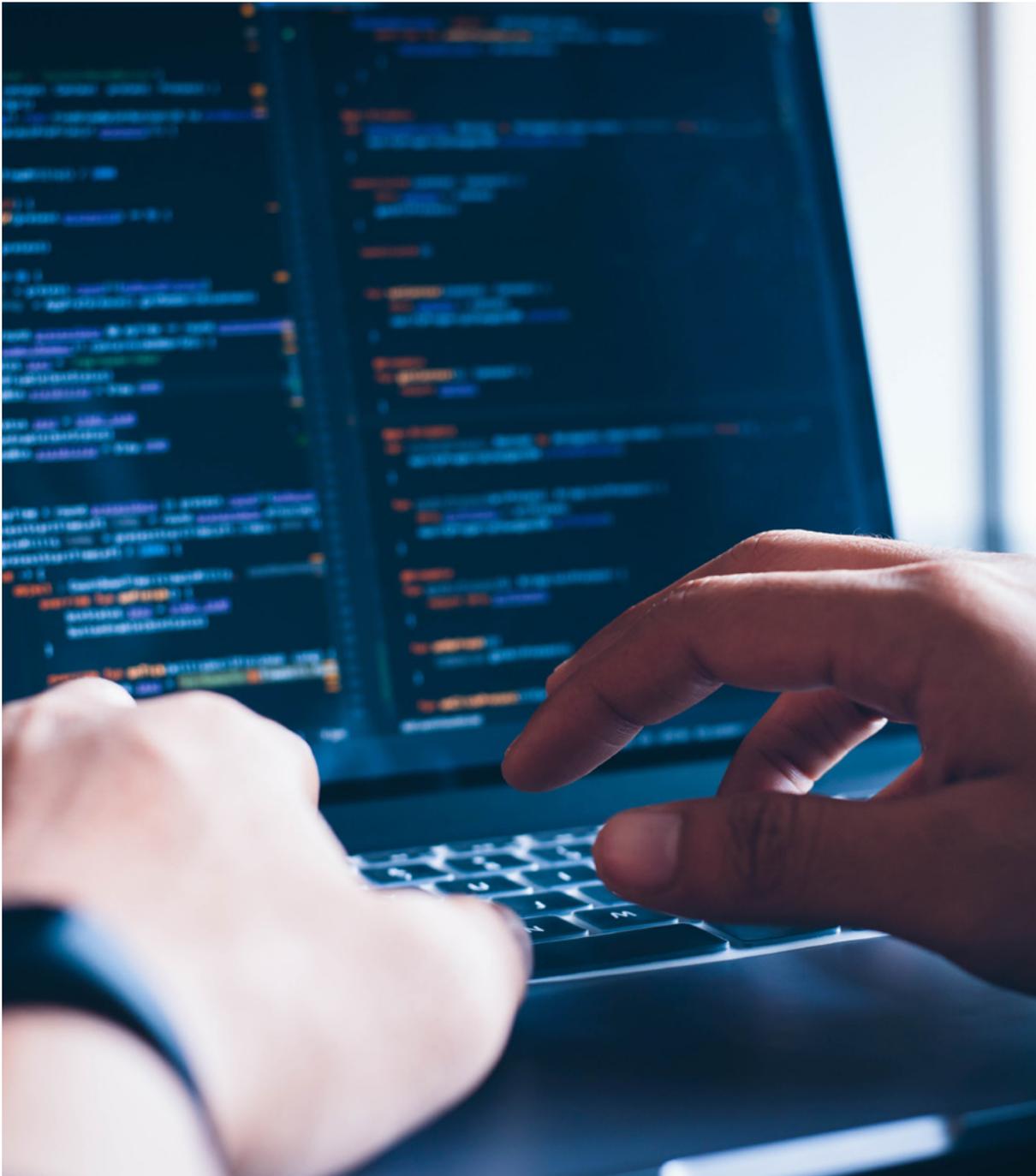
3. Look for diurnal patterns

Real, human traffic follows diurnal patterns: traffic begins to rise in the morning (for your local area or user base) and stays high during the day, then tapers off to hit a low point in the middle of a night. If you see random patterns, your organization might have a bot problem.

4. Check for attacker retooling

Have there been spikes in traffic followed by normal patterns? Has any anomalous behavior been detected by security or fraud teams during this time? If so, attackers may be retooling to adapt to your countermeasures. Remember, it is about economics and ROI. Retooling indicates the attackers are investing in order to bypass your security countermeasures - meaning there is real value in your accounts worth pursuing.





ASSUME YOU'RE GOING TO BE ATTACKED

In general, you should assume that every consumer-facing application you own will eventually be subjected to automated attacks—and prepare accordingly. It happens to even the most well-defended organizations with securely coded and patched apps. That's because attackers aren't exploiting flaws; they're abusing logic in order to commit fraud.

CONCLUSION

Even top cybersecurity teams struggle to defend organizations against the growing risk of attack and compromise. But automated attacks are more than a security issue; they represent a business challenge that must be properly addressed—for the sake of your customers and clients, your reputation, and your company's bottom line. By putting the right defenses in place, you can discourage these malicious attacks by making them cost-prohibitive, keeping the economics on your side.

For more information, watch the webinar, [Attacker Economics: Hacker Cost vs Value](#).



SOURCES

- ¹ F5, "What Your Login Success Rate Says About Your Credential Stuffing Threat," Aug. 23, 2019, <https://blog.shapesecurity.com/2019/04/23/what-your-login-success-rate-says-about-your-threat-surface/>
- ² Juniper Research, "Online Payment Fraud Losses to Exceed \$200 Billion Over Next 5 Years," Feb. 2020, <https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion>
- ³ Green Tech Media, "Solar Technology Got Cheaper and Better in the 2010s. Now What?" Dec. 17, 2019, <https://www.greentechmedia.com/articles/read/solar-pv-has-become-cheaper-and-better-in-the-2010s-now-what>
- ⁴ Computer World, "CW@50: Data storage goes from \$1M to 2 cents per gigabyte, (+ video)," March 23, 2017, <https://www.computerworld.com/article/3182207/cw50-data-storage-goes-from-1m-to-2-cents-per-gigabyte.html>
- ⁵ LastPass, "3rd Annual Global Password Security Report," <https://www.lastpass.com/business/articles/password-benchmark-report>
- ⁶ IEEE, "(How) Do People Change Their Passwords After a Breach?" <https://www.ieee-security.org/TC/SPW2020/ConPro/papers/bhagavatula-conpro20.pdf>
- ⁷ F5, "Attacker Economics: Hacker Cost vs Value," <https://www.shapesecurity.com/app-security-and-fraud-summit/attacker-economics>

ABOUT F5

F5 powers applications from development through their entire lifecycle, so you can deliver differentiated, high-performing, and secure digital experiences.

Find more banking and financial service resources at f5.com/solutions



US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

©2020 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.

Any other products, services, or company names referenced herein may be trademarks of the irrespctive owners with no endorsement or affiliation, expressed or implied, claimed by F5. EBOOK-BFSI-546894963