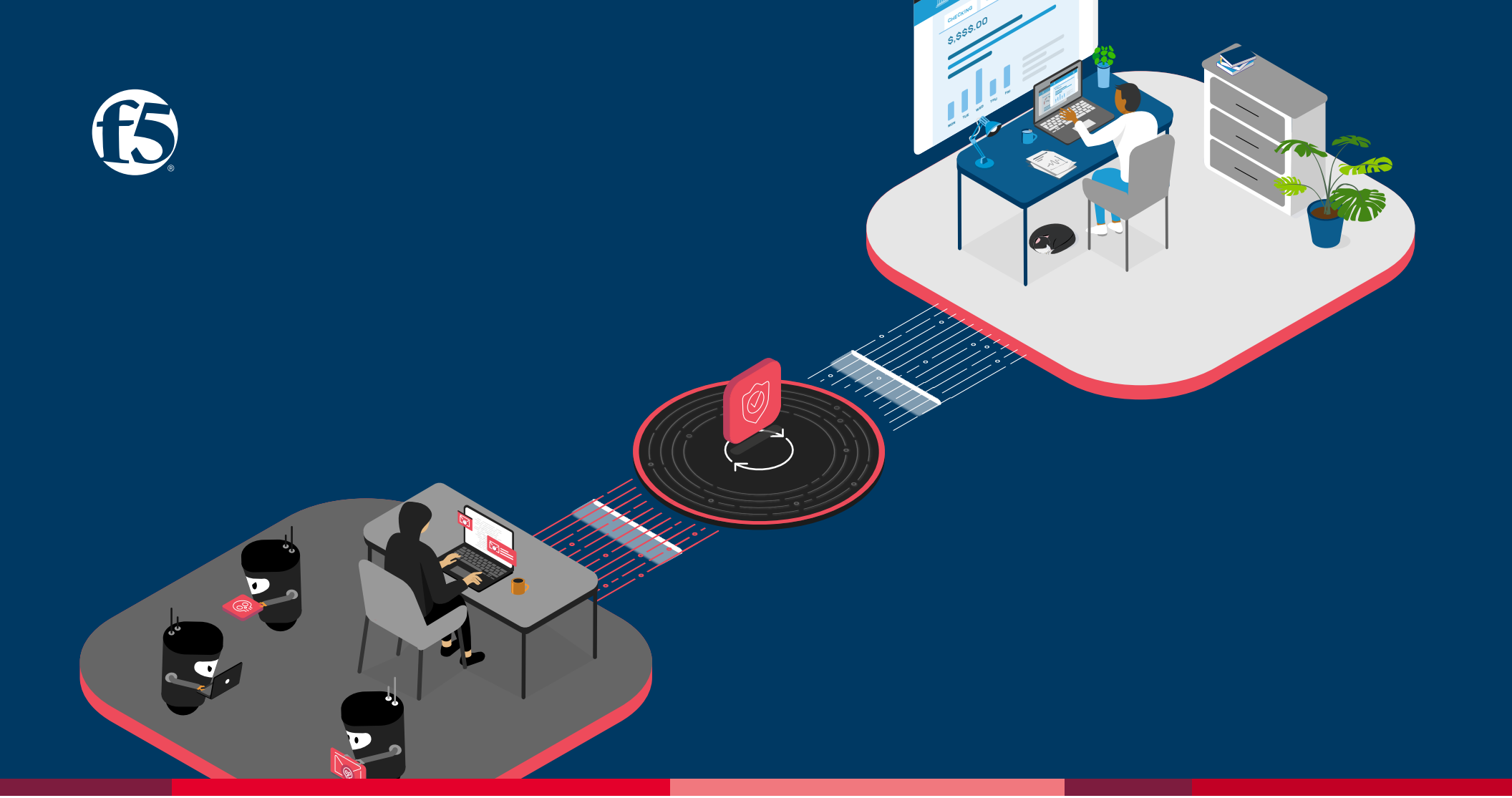


The New Era of Fraud: An Automated Threat

Introduction

Digital innovation has changed everything: the money is behind apps, so every online business is a potential target for fraud.

Banks and financial institutions used to be the primary targets of fraud. Why banks? "Because that's where the money is," to quote the notorious American bank robber Willie Sutton. While banks remain firmly in the crosshairs of fraudsters, the speed of digital transformation has made every company susceptible.

In the new digital economy, every business with an online presence is a potential target for fraud. The same technology that helps us find airfare deals, sweet concert seats, or the best prices on the hottest Jordan shoes—that is, automation—can now be used by criminals to scale and adapt their attacks.

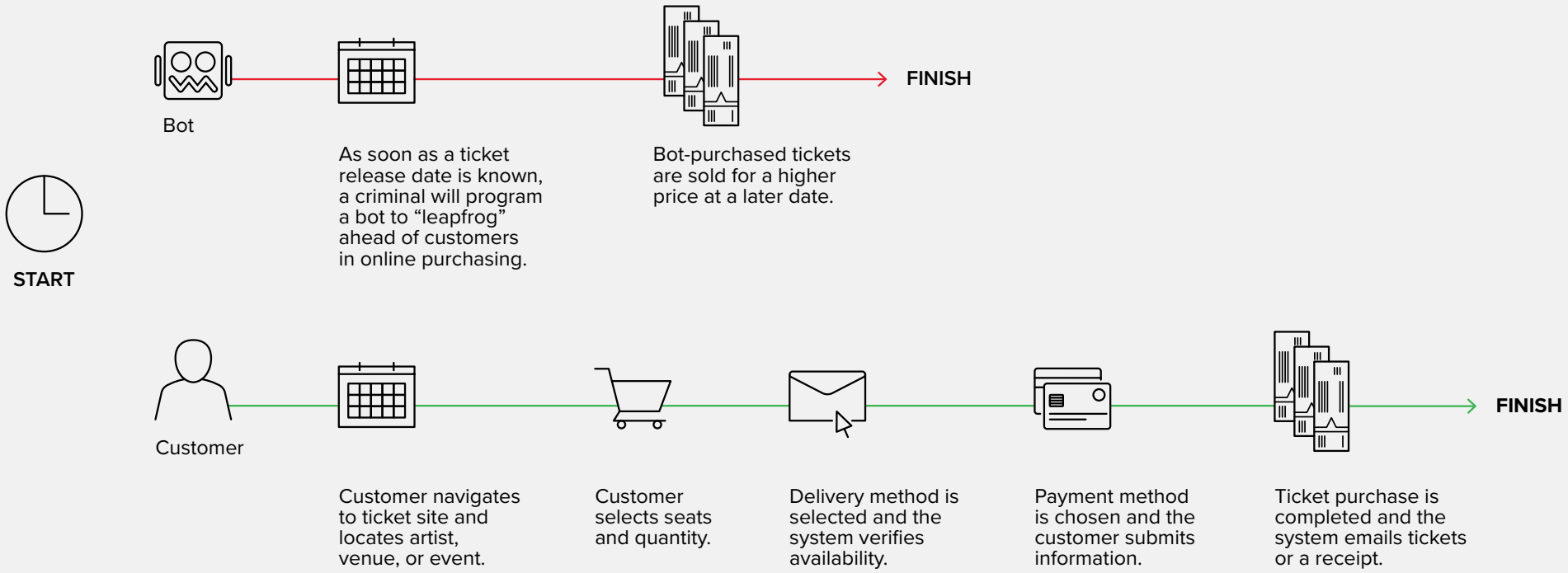
Fraudsters employ bots and automated attacks that scour apps looking for any opportunity to hijack business logic, take over customer accounts, and extract their value. And since fraud targets your business processes beyond industry-known weaknesses or vulnerabilities, you may not know when it is happening or have the best tools to protect your customer accounts, revenue, and brand.

If your application has a login for end customers, **expect it to be targeted** by credential stuffing.[1]

Customers vs. Bots

In this online ticket purchasing scenario, the deck is stacked against a legitimate customer trying to get to the finish line of making an online purchase before a bot can grab tickets. When the tickets are sold out, a fraudster can sell them later at a higher price. The result is a frustrated customer and potentially longstanding damage to brand loyalty.

The Race for Online Tickets



Know Your Enemy: The Many Faces of Fraud

Your ability to identify and thwart fraud will be perpetually tested by a wide range of creative, complex, and stealthy tactics that criminals use to evaluate, exploit, and evade digital processes. Being knowledgeable about fraud—and how bots and automation are employed to facilitate it—is a good first step on the road to effective detection and mitigation.

Business logic attacks

Not necessarily the result of flaws in code, these attacks take advantage of how an application works or how you do business. For example, attackers may try making small purchases on a web app (for example, ordering a pizza) to validate stolen credit card numbers. Or they might register in a coffee shop's rewards program 365 times to collect a free "birthday coffee" every day of the year. Increasingly, fraudsters are targeting critical endpoints like logon, create account, and add to cart that facilitate business logic processes underpinning your entire digital business.

Credential stuffing and account takeover

Often powered by bots, these attacks leverage readily available tools and compromised data from active data breaches or the dark web to gain access to customer accounts. Automated login requests using stolen username and password combinations can lead to account takeover (ATO) and provide a beachhead for fraud.

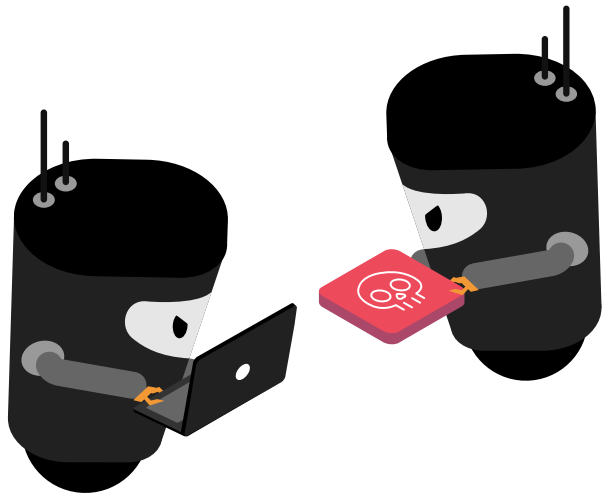
Bank accounts, online gaming accounts, and even hotel rewards points accounts are typical targets because fraudsters can gain financially from these accounts.

Content scraping

Web scrapers traverse your digital properties to steal and repurpose intellectual property and content such as pricing information, published articles, and other such assets. This stolen content can be used by the fraudster to undercut pricing, poach potential visitors, or harvest customer information.

Gift card cracking

Attackers check millions of number variations on a gift card balance lookup app or endpoint to identify card numbers that hold value. In some cases, the attacker will visit a retail location to identify numeric patterns in gift cards to assist with efforts to crack them using automation. Because after all, this is a game of large numbers.



Scalping and inventory hoarding

These bots purchase, hoard, and resell goods and services that are typically limited in supply such as concert tickets or in-demand sneakers. Scalpers buy up as much as they can so they can later resell the acquired goods for a substantial profit. Allowing or ignoring this kind of behavior can alienate your true customer base because customers will not be able to purchase directly from you, which acts as a denial of service and tarnishes your reputation as a reliable source.

Marketing fraud and click fraud

Often powered by botnets of compromised computers, these tools mimic human behavior to facilitate a variety of purposes such as registering for accounts and clicking on ads, which falsely increases ad revenue. More advanced tools of this nature can defeat traditional security challenges and spoof controls used to delineate humans from bots and automation.

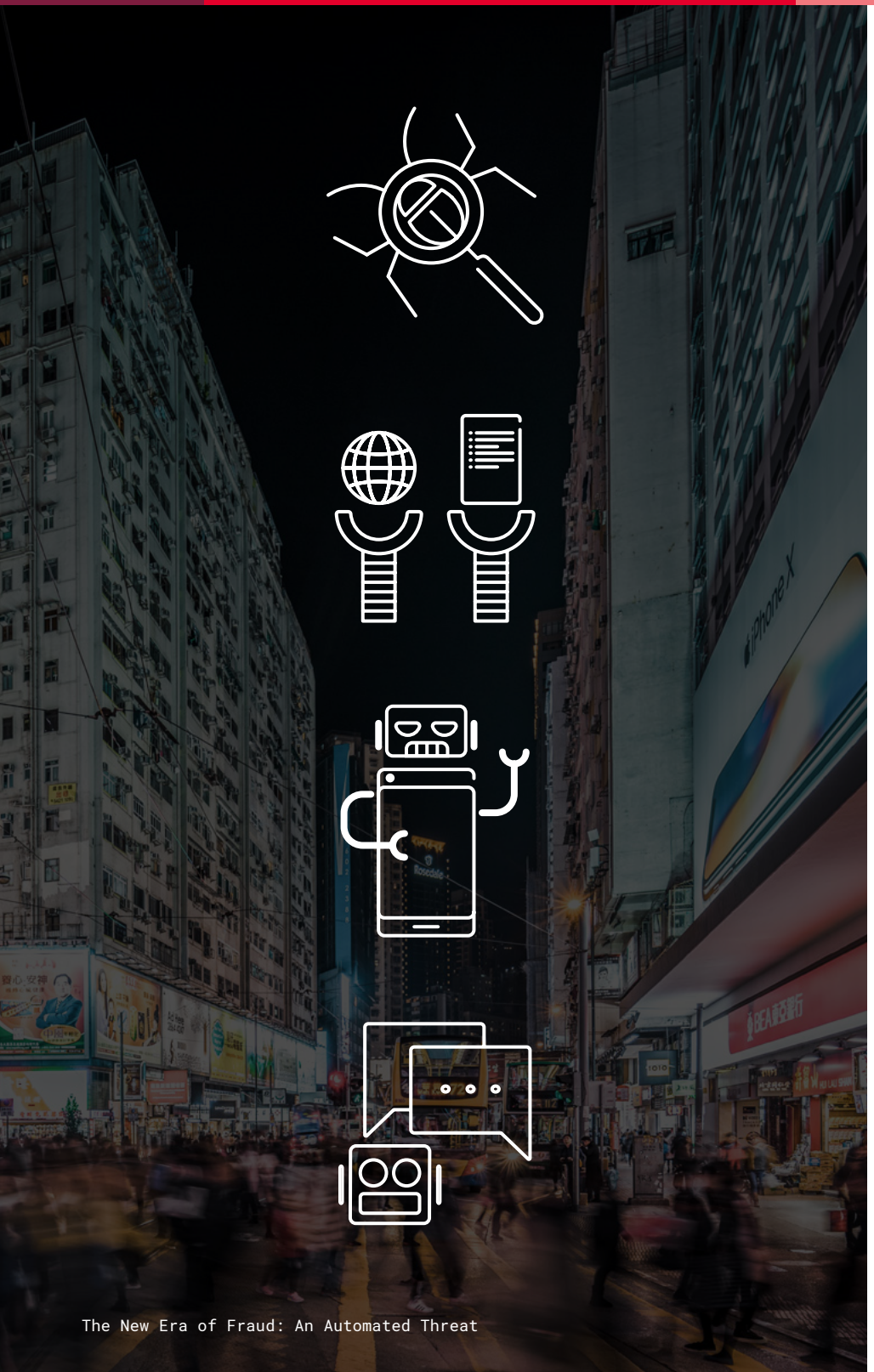
Fake accounts/new account opening fraud

Bad actors automate the creation and use of fake accounts to generate content spam, create fake product or service reviews, or commit financially motivated attacks such as discount, promotion, or reward abuse on retail sites and money laundering via online banking.

Aggregator abuse

Fraudsters leverage aggregators as a backdoor into banks to steal information, check account balances, and launder money. The risk is increasing as consumers demand personalized experiences and all-up account views.

Online fraud losses are projected to exceed **$48 billion** per year by 2023.[2]



Bots, Bots, Bots!

Bot-generated internet traffic has long surpassed human traffic.[3] Part of the reason for this is that customers are increasingly finding utility in automation, which allows them to engage brands through real-time chat and digital interactions, index and search the internet, find the best travel deals, and fetch relevant content to display in our favorite web hangouts. As Siri, Alexa, and Google make bots available as personal assistants ready to respond to our commands, bots have become an essential tool for both businesses and consumers alike.

However, bots are also the fraudster's best friend. They are efficient and effective, and they don't ask questions, making them indispensable for the execution of malicious campaigns. Often the same technology that powers our favorite apps also enables fraud.

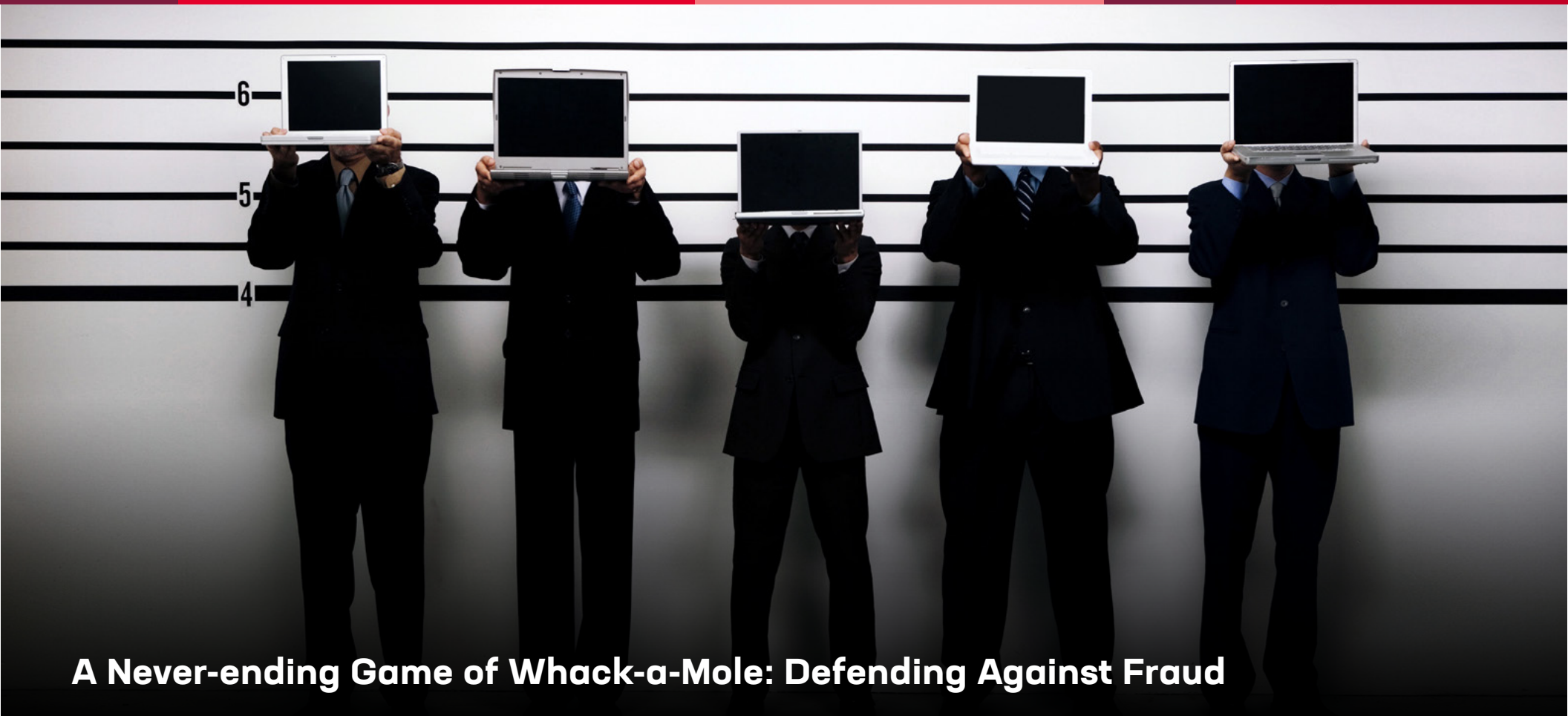
Some bots are designed to pass themselves off as humans. Fraudsters use these social bots to promote products and services, and even manipulate public opinion via social media, discussion groups, product reviews, and public forums.[4]

Not all bots are leveraged for deception. Some autonomous programs crawl the internet looking for web application vulnerabilities to exploit. These are typically web applications that have not been properly updated or patched and unaddressed information leakage can make the identification of these relatively easy. Once the apps and vulnerabilities have been identified, the attackers can plan their exploits and use automation to carry them out at scale. This is an important part of fraudsters' industrialized attack lifecycle because vulnerability exploits often lead to data breaches that expose PII—which can then be used in automated attacks and credential stuffing.

The most common attacks, however, are attackers that leverage bots, automated tools, and compromised data to maximize the ROI of their efforts to commit account takeover (ATO) and fraud. Credential stuffing has become the most popular attack as the success rate is attractive and the payout is potentially astronomical. In 2021, access attacks, that is, attacks against user-facing authentication surfaces, were the single most frequent cause of breaches.[1]

These attacks do not exploit application vulnerabilities or software weaknesses, but instead abuse human psychology (password re-use) and digital interfaces such as login forms. As such, bots are increasingly used to abuse critical business logic and commit commercial and retail fraud.[6] Attacker frameworks are predicted to evolve even further to leverage trained AI models to bypass security, as the industrialized attack lifecycle begins with automation and end with fraud.[7]

"**Credential stuffing** will be a threat so long as we require users to log in to accounts online."[5]



A Never-ending Game of Whack-a-Mole: Defending Against Fraud

Fighting fraud can feel like a never-ending game of whack-a-mole. Because fraudsters can be evasive and relentless, your defense must make success so difficult and impractical that their ROI becomes unattractive. While you will never achieve complete invulnerability, implementing security countermeasures that make your applications a more challenging target will greatly increase the probability that criminals will focus their attention and efforts elsewhere.

The best deterrence is specialized bot defense that can be integrated seamlessly into your existing architecture—whether through an application proxy, application platform, or content delivery network (CDN). These are key insertion points for gaining visibility and for blocking malicious bots, advanced automation, and anomalous behavior indicative of fraud.

Because attackers constantly retool to circumvent security countermeasures, there are several factors to consider when choosing a solution. First, your solution needs to see diverse traffic patterns from numerous customers and environments to obtain the large data sets needed to accurately recognize attacks and anomalies. It should also leverage durable telemetry collection and machine learning models to analyze network, device, environmental, and behavioral signals, and employ continuous monitoring by a security operations center (SOC).

Bot Management

Bot management protects web and mobile applications and API endpoints from sophisticated attacks that would otherwise result in large-scale fraud. A specialized bot management service can determine in real time if an application request is from a fraudulent source and then take an enterprise-specified action such as blocking, redirecting, or flagging the request. This provides resilient protection without assisting with the attacker's reconnaissance efforts, as the most skilled criminals will attempt to bypass security countermeasures and evade detection.

"Bot management **protects web and mobile applications and API endpoints** from sophisticated attacks that would otherwise result in large-scale fraud."

Collective defense

The diversity of traffic that is seen by a bot management service combined with accuracy of detection is critical to effectively mitigating bots—especially the sophisticated bots that lead to fraud. By modeling threat intelligence across similar attack profiles and risk surfaces, security countermeasures can be deployed autonomously for maximum effectiveness, no matter how an attacker retools in the attempt to bypass defenses. And when this collective defense network includes web, mobile, and API footprints of the world's most valuable brands, new attack techniques observed on one customer trigger immediate protection for all other customers.

Accurate and durable telemetry

Telemetry signals containing device, network, environmental, and behavioral signals can be used to filter unwanted automation in order to distinguish between a real customer and a fraudster. Durable and accurate telemetry coupled with closed AI models trained on large data sets of traffic and historical fraud records bolster defenses by detecting anomalous behavior used in fraud. This can include copying and pasting activity, screen toggling, odd screen real estate usage, device affinity, environmental spoofing, and attempts to anonymize identity. Because motivated attackers constantly retool and may pivot to bypass anti-automation defenses, it is imperative to anticipate all potential tactics and protect against them. In other words, if your solution can effectively collect the right signals, you'll have more than a simple anti-bot solution.

Artificial intelligence and machine learning

Using comprehensive telemetry signals, AI trained by attack profile, risk surface, and historical fraud records, along with supervised and unsupervised machine learning, attacks can be detected without manual intervention, relaxing the burden on security and fraud teams. Real-time protection is augmented with AI-based retrospective analysis and security operations oversight to ensure the right outcome is being delivered.

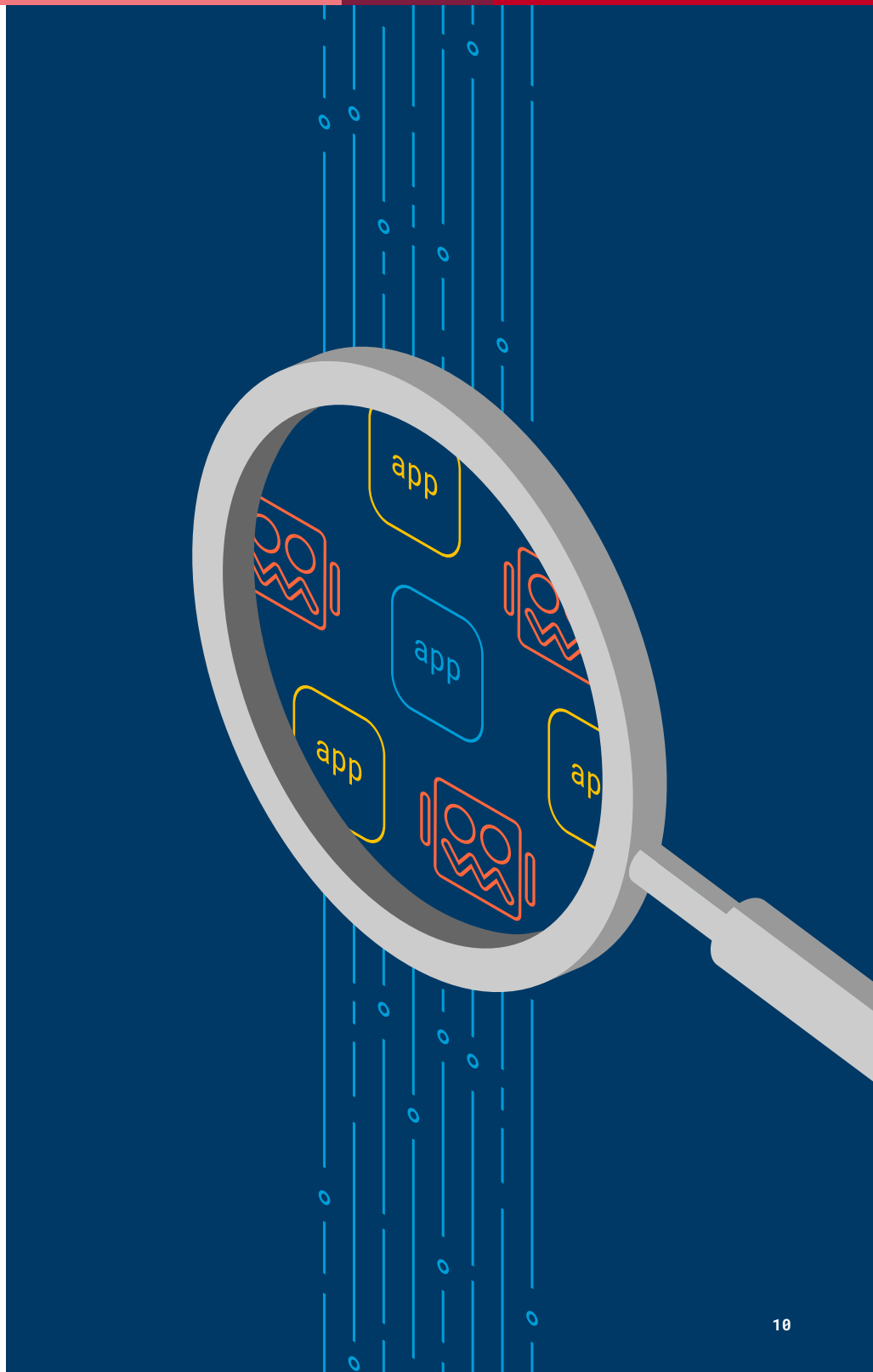
Automated security to combat retooling

Disrupting the attack ROI by making success impractical, or at least too costly to be feasible, is an effective deterrent. Skilled attackers adapt to security countermeasures by using advanced tools and manual interactions to spoof anti-automation algorithms. As such, security countermeasures must be continuously and autonomously deployed to provide resilient protection and long-term efficacy against attackers that retool, in part by using their own playbook—deception. For example, monitoring—but not blocking—the canary accounts fraudsters create to study how a web application works helps you stay one step ahead.

Frictionless authentication

Effective defenses do not rely on vague risk scores and complex authentication rules, releasing security and fraud teams from the operational burden of manual oversight and freeing users from the friction imposed by intrusive mitigations such as CAPTCHA and multi-factor authentication (MFA).

Real-time verification and retrospective analysis can be performed on protected resources by leveraging intelligence from the collective defense network, machine learning models, and SOC monitoring. This provides insight that enables organizations to block requests from devices affiliated with a compromised account, identities that previously exhibited suspicious behavior, and blatant attempts to use known stolen credentials without needlessly challenging legitimate customers.



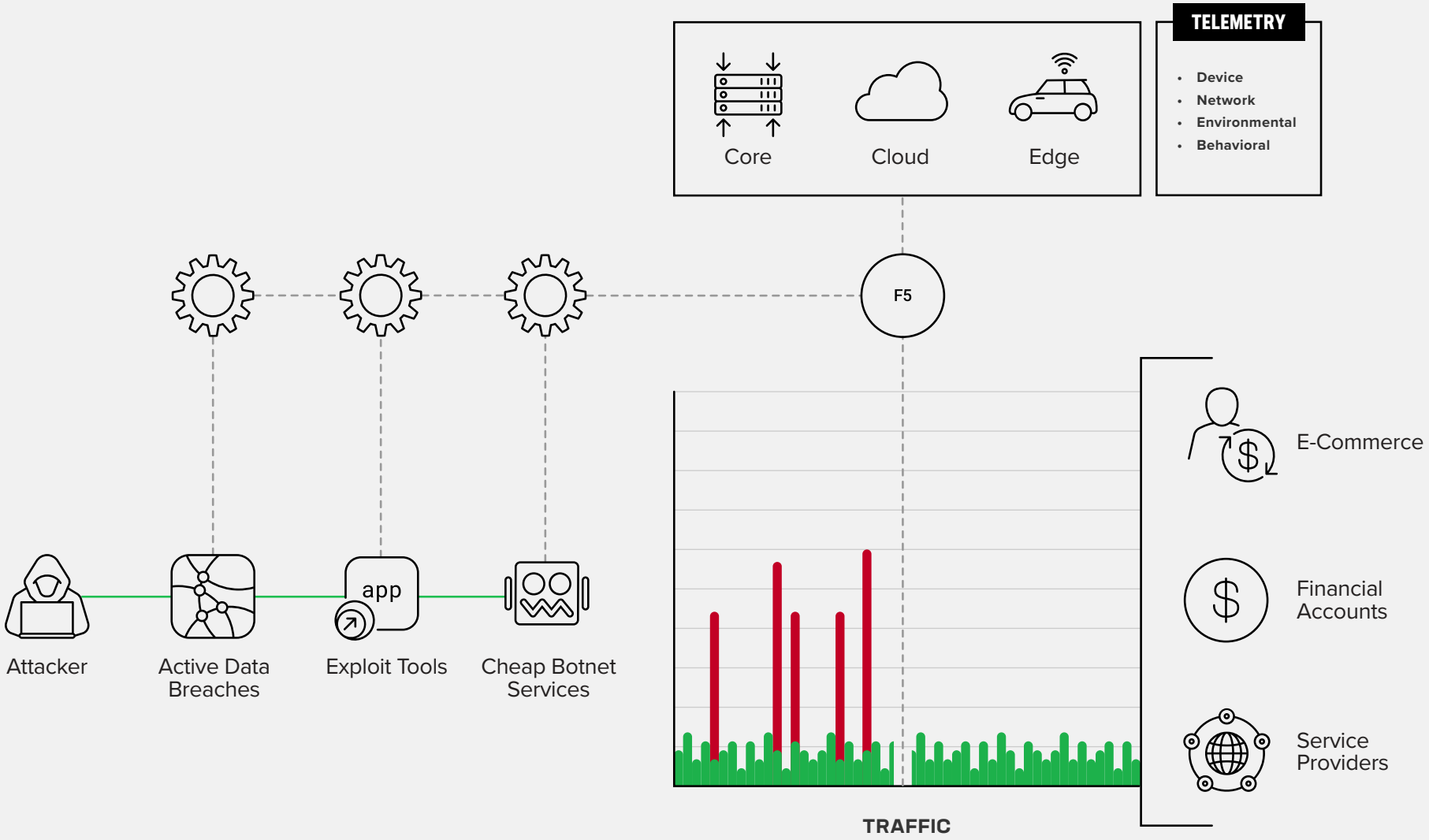


Figure 1: F5 solutions leverage durable, obfuscated telemetry for accurate detection and maintain resilience to deter malicious automation and attacker retooling.

Fraud: The Best Defense Is a Holistic Defense

Addressing fraud requires the right combination of strategy, technology, and diligence. While there is no simple solution to eliminate fraud, using specialized bot management to protect your apps and customers from automated attacks and abuse that can lead to fraud is paramount. Insertion points to connect bot management into your environment help you apply the right protections right where you need them—regardless of architecture.

The combination of visibility, accurate detection, adaptive protection, threat intelligence, machine learning, and mature security operations gives you the tools you need to shut down fraudulent activity—before it can take a toll on your business.

Appendix

[1] Sander Vinberg and Raymond Pompon, 2022 Application Protection Report: In Expectation of Exfiltration (F5 Labs, February 15, 2022), https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-in-expectation-of-exfiltration

[2] Susan Morrow and Nick Maynard, Online Payment Fraud: Emerging Threats, Segment Analysis & Market Forecasts 2021-2025 (April 26, 2021), https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report

[3] April Glaser, Internet Traffic from Bots Surpassed Human-Generated Traffic in 2016 (May 31, 2017), https://www.vox.com/2017/5/31/15720396/internet-traffic-bots-surpass-human-2016-mary-meeker-code-conference

[4] Alex Hern, Facebook and Twitter Are Being Used to Manipulate Public Opinion (June 19, 2017), https://www.theguardian.com/technology/2017/jun/19/social-media-proganda-manipulating-public-opinion-bots-accounts-facebook-twitter

[5] Sander Vinberg and Jarrod Overson, 2021 Credential Stuffing Report (February 9, 2021), https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

[6] Council to Secure the Digital Economy, International Botnet and IoT Security Guide 2020 (November, 2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf

[7] Kyle Roberts, How Attacks Evolve from Bots to Fraud – Part 1 (December 6, 2021), https://community.f5.com/t5/technical-articles/how-attacks-evolve-from-bots-to-fraud-part-1/ta-p/286685

ABOUT F5

F5 stops fraud without friction, so you can deliver differentiated, high-performing, and secure digital experiences.

Learn more about bot management at
f5.com/solutions/application-security/bot-management

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