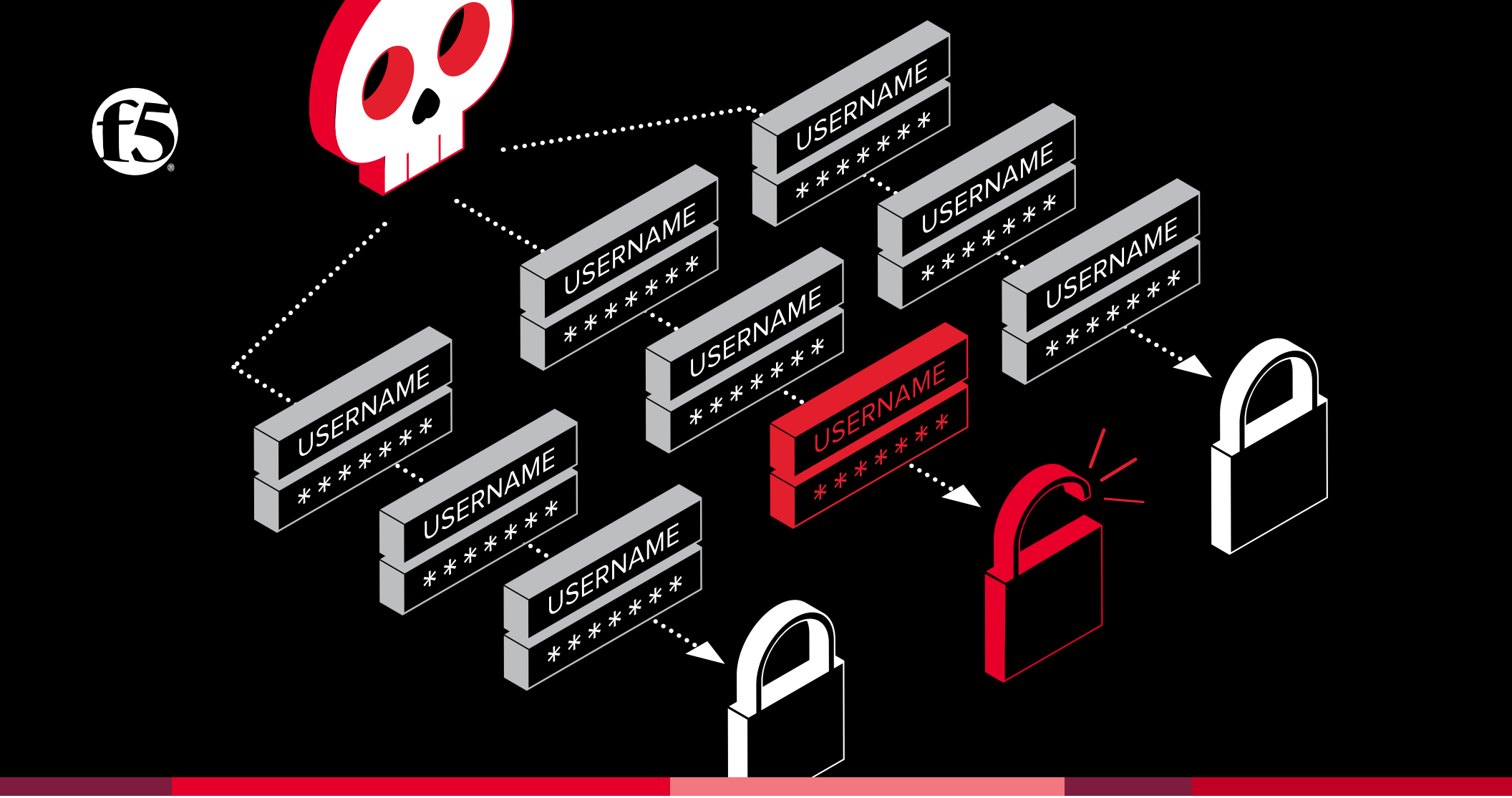


Credential Stuffing 2022: The Latest Attack Trends and Tools

Understand and disrupt sophisticated attackers who retool against your countermeasures.

Introduction

From the stereotypical loner in the basement to organized criminal gangs and nation states, attackers have become increasingly sophisticated over the past decade. They have the same skills, tools, and services at their fingertips as your IT teams do. This includes the ability to use artificial intelligence (AI) and machine learning (ML) to create sophisticated campaigns that adapt to your mitigation efforts. These dynamic attack methods keep evolving as the cost versus value equation continues to deliver extraordinary ROI for attackers. In particular, credential stuffing has evolved from attractive to downright lucrative.

Back in the day, a simple cURL tool could siphon website data. Companies added defenses like CAPTCHA, and in response, attackers adapted their attack methods to utilize CAPTCHA solvers and scriptable consumer browsers to imitate human behavior. These shifts were all an effort to capitalize on the growing value of their targets.

Today, attackers can gather a dossier on their targets using the same technologies that organizations leverage to protect their applications. The attackers gain insight into weaknesses in ways similar to those used by security and fraud teams as they seek information about attackers. With an even playing field, how can security and fraud teams stay ahead? The key lies in using automation, machine learning, and AI to create a security deterrent—maintaining resiliency and efficacy as attackers retool and adapt to security countermeasures in order to disrupt the ROI of an attack.

Credential Stuffing Is the Top Enterprise Attack

Credential stuffing attacks have become incredibly easy and inexpensive. The calculation below illustrates why these attacks have become so popular—and so profitable.

$0 : 2.3 billion credentials
$50 : for tool configuration
$139 : for 100,000 CAPTCHAs
$10 : for 1,000 global IPs

} Less than $200 for 100,000 ATO attempts

Even if you think you have credential stuffing under control, it's important to understand the trajectory these attacks are taking as attackers continually pivot. F5 Labs threat intelligence identified access-based attacks such as credential stuffing as the number one attack method leading to data breaches.[1] This form of abuse is spreading beyond your login pages to a variety of components of critical applications.

In 2019 alone, more than 80% of attacks on web applications involved using stolen credentials.[2] In addition, attacks on web apps were a part of 43% of breaches, more than double the results from the previous year. The risk surface for each organization varies, and so do the attackers' motives, so it's important to understand the intention behind these attacks.

Incentives and Adversity

The tension between incentives and adversity drives evolution. Adversity—the difficulty of an attack, including the investment necessary to compromise sensitive information or customer accounts—is dropping due to readily available tools, infrastructure, and compromised data. At the same time, a rapid shift to online commerce increases the potential value in customer accounts and thus the attackers' incentive. This is where opportunity thrives for attackers.

Over 80% of hacking-related breaches involve brute force or the use of lost or stolen credentials.[2]

Adversity also comes into play when organizations layer on defenses, driving up the cost of entry and the price of operationalizing an attack. At this point, attackers ask themselves: Is it worthwhile to pivot into the next generation of tools required to carry out an attack? Or can I target some easier, low-hanging fruit?

Unfortunately, there's a catch-22. The rise of AI, cloud, automation, and the tools companies use to do more with less are the exact same types of technologies that attackers use to lower their cost of entry and weaponize attacks. Evolution occurs when attackers shift to more sophisticated methods to obtain higher-value assets. Once they reach this next generation, you want to have enough defenses in place for the age-old cost versus value question to tip in your favor and encourage attackers to move on to easier targets.

But even if you reach that nirvana state of being too costly to attack, it won't last forever. Skilled attackers will typically attempt to retool and start a new attack as soon as new countermeasures are deployed. The most sophisticated attackers may abandon automation toolkits and launch manual attacks that bypass mitigations designed to detect non-human automation. Organizations should operate with the mentality that all defenses have been or imminently will be bypassed.

From lost revenue to regulatory fines, reputation damage, remediation costs, and chargeback losses, attacks continue to wreak havoc on organizations in every market sector. A new study found that businesses in the e-commerce, airline ticketing, money transfer, and banking industries will cumulatively lose over $200 billion to online payment fraud between 2020 and 2024,[3] losses driven by the increased sophistication of attackers and the rising number of attack vectors.

Why Economics Are in the Attackers' Favor

Accessing consumer credentials used to be a tough game. Attackers had to create their own breach, find a zero-day exploit, or travel in the right (read: wrong) circles. Now, anyone can get a credential list for free or for a nominal fee. Lists are available on the dark web, but they can also be accessed through mainstream sites like Twitter or various online forums. Some services are even designed to sell verified credentials and digital fingerprints from individuals impacted by a data breach.

For example, Genesis is an advanced browser plug-in, marketplace, and malware that attackers attempt to plant on a victim's device. It scrapes all the user's login data and delivers it back to the marketplace for sale to attackers. Even worse, the malware updates the marketplace when the user changes their passwords, and it scrapes the browser and environment data to generate both fingerprint and device characteristics, so the attack always appears to be coming from the infected user's browser.

To scale and adapt, attackers need tools to automate their operations. Today, you don't even need to have programming skills; CAPTCHA solvers, anti-fingerprinting, and other tools can do the technical work for you. And if you don't have time to configure all the services, you can find a gun-for-hire through freelance marketplaces who will configure your attack for a fee.

The next logical step is to operationalize the attack. As in the earlier phases, there are many ways to bypass rudimentary defenses like CAPTCHA. Cloud services make it easy to infiltrate web apps with hacking as a service and to distribute traffic across the globe. Tools designed to perform penetration testing as part of software quality assurance can be used for nefarious purposes, such as emulating network, device, and human behavior in order to bypass anti-automation defenses.

Attackers can also use AI-enabled malware programs to perform reconnaissance and profiling, studying an organization's environment, its update lifecycle, communication protocols, and system vulnerabilities and employees.[4]

Additionally, mobile apps and third-party integrations through APIs are becoming more essential, further increasing the threat surface, as APIs are also susceptible to credential stuffing.

Put these steps together and you have a cheap, automated, globally distributed attack with a high probability of success. The cost to enter and operationalize can be close to nothing, and the returns can be astronomical, based on the balance of automation and manual work.

The e-commerce, airline ticketing, money transfer, and banking industries will cumulatively lose over **$200 billion** to online payment fraud between 2020 and 2024.[3]

Generational Shifts in Attack Methods

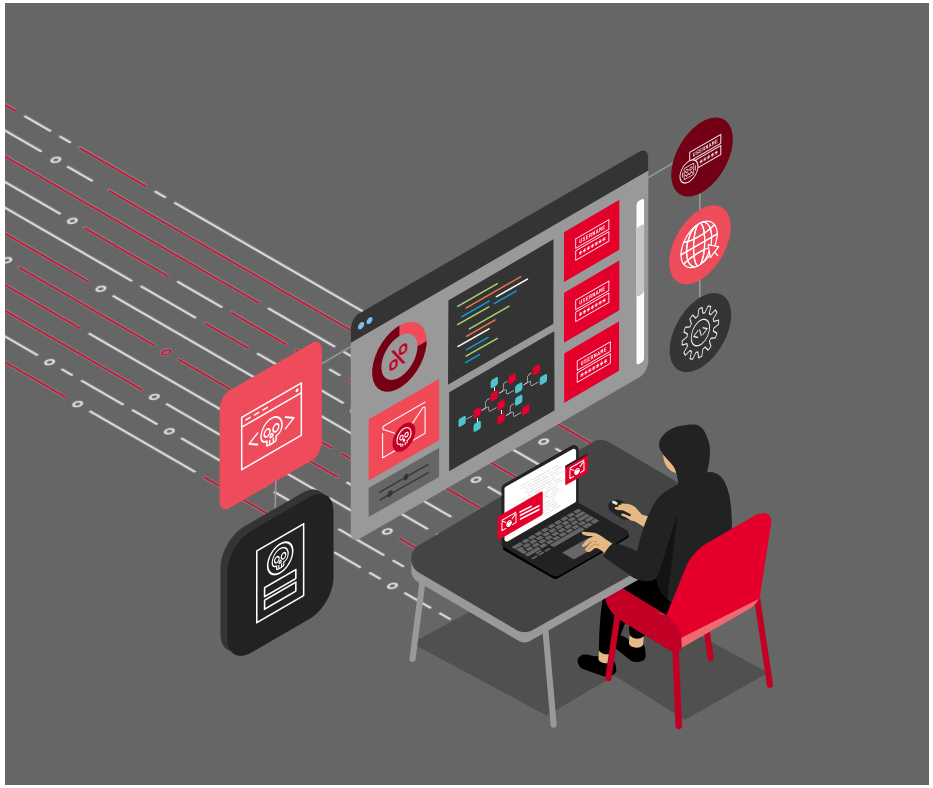
Even the best defenses won't keep attackers at bay for long because they innovate just as we do. They began with cURL and moved on to create tools designed specifically to automate attacks. Companies tried to detect these anomalies with rate limiting or denylists, but these are easily overcome. These first generation attacks resulted in a tactical shift for security defenses.

The emergence of CAPTCHA added a new layer of defense. Unfortunately, millions of companies adopted it on the free price tag alone. But for an attacker, CAPTCHA is easily defeated. A broad array of CAPTCHA solvers quickly became available to infiltrate this widely-used solution. Simply enter "CAPTCHA solvers" into your web browser and you'll immediately find hundreds of options and services.

The next tactical shift? Browser challenges through JavaScript injection. Second generation attacks pivoted to defeat these new schemes using the same tools that IT organizations rely on every day for testing their web applications, including Phantom JS and Trifle JS.

In third generation attacks, traffic more accurately imitates human behavior, so security teams need to find innovative ways to identify attack traffic. They also need to have more visibility into the nuances of human emulation. For example, tactical defenses work by checking header and environment data. Examining this kind of nuance can help you to better understand your traffic.

As hackers more accurately disguise their behavior as valid, human interactions, your IT team needs to sharpen its ability to distinguish between human and automated actions. For example, attackers can use anti-fingerprinting tools to randomize data sources, as well as tools such as Bablosoft's Fingerprint Switcher to cycle through real browser fingerprint data, including canvas, audio, and webGL data, video card properties, do not track signals, audio settings, browser language, touch support, geolocation, and much more.



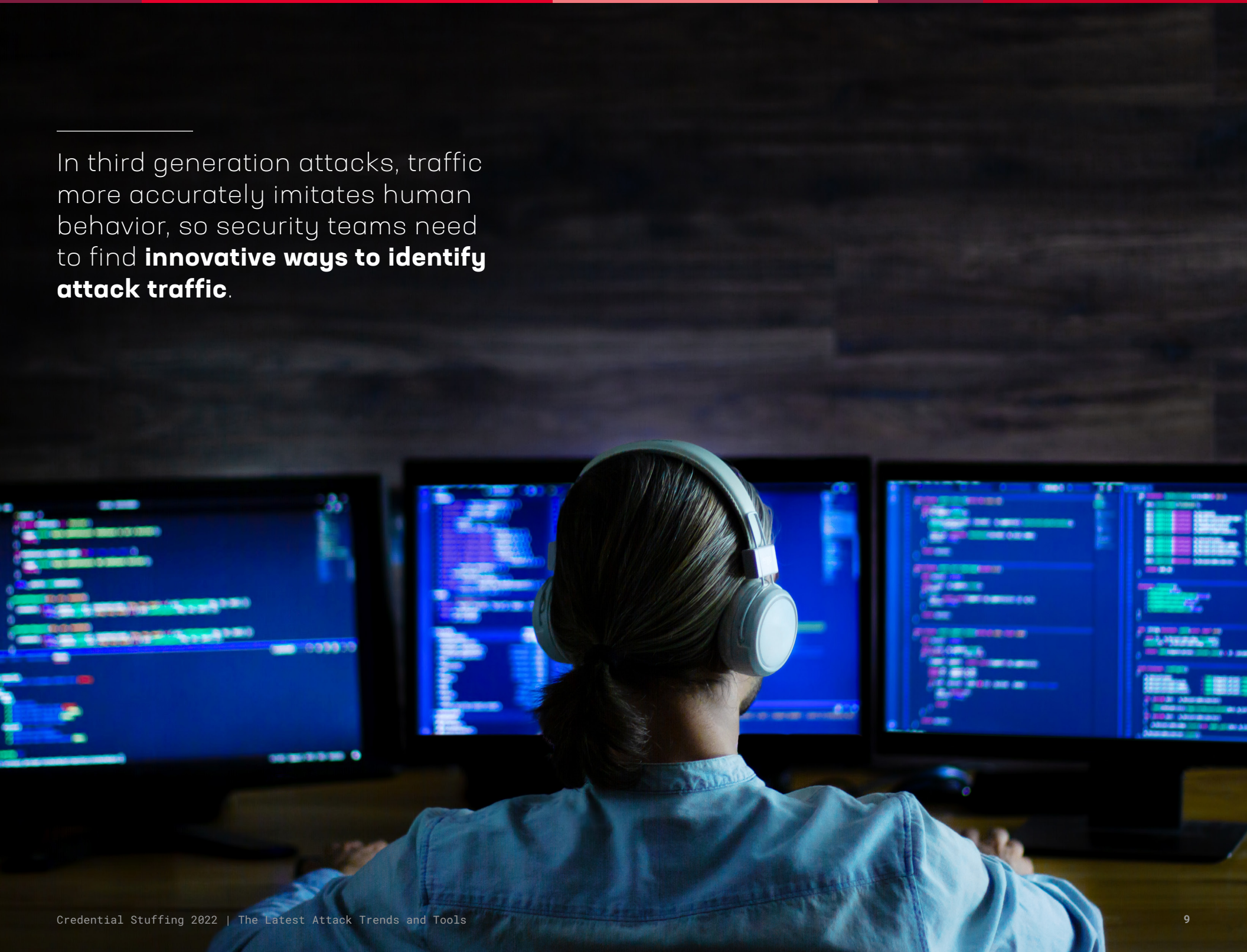
Appearing Just Human Enough

Credential stuffing is a cat-and-and mouse game. Companies create new defenses, hackers develop cheap and widely available tools to bypass these safeguards, and the cycle continues. Today, attackers use automated tools and algorithms to produce human-like behavior that bypasses behavioral analytics. Traditional products simply can't detect this kind of attack without generating an unacceptable level of false positives. In addition to the risk of false positives, CAPTCHA and multi-factor authentication (MFA) challenges can frustrate real users and lead to customer abandonment. On the other hand, the worst-case scenario—a false negative—can lead to data breach, account takeover, a damaged brand, and more commonly, fraud.

Attacks that imitate human behavior to bypass risk scoring and behavior analysis tools are called "imitation attacks," and they're designed to blend in. The end goal is to mimic legitimate network, device, and human behavior. Imitation attacks may or may not be automated.

Ultimately, whether attacks leverage tools to imitate human behavior or are actually conducted by humans with bad intent, they're increasingly difficult to prevent without introducing unacceptable friction for legitimate users.

In third generation attacks, traffic more accurately imitates human behavior, so security teams need to find **innovative ways to identify attack traffic**.



Where Do We Go from Here?

The value in customer accounts will continue to rise as commerce continues to shift online, so attackers will continue to develop more reliable ways to compromise them, jeopardizing strategic business imperatives and pressuring the top and bottom lines. The best-protected companies put resilient defenses in place to increase the investment required for a successful attack, raising the cost enough to prompt attackers to divert their attacks elsewhere.

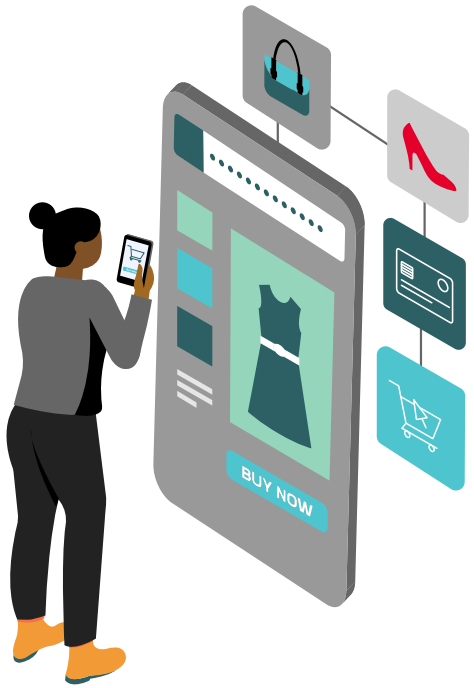
Attack the economic

Hacking is an economic problem, not solely a technical one—and there are no airtight defenses against criminals who are motivated to monetize your data. Sophisticated credential stuffing can lead to account takeover and fraud. It's gone far beyond simple automation. Security teams often lack the time and resources to identify and mitigate this problem until it's far too late, often resulting in significant fraud losses, chargebacks, and loss of customer loyalty and trust. That's why they need to work closely with line-of-business teams to understand the problem, build solutions, and mitigate it more effectively.

Remember that imitation attacks are designed to blend in. It's critical to have deep visibility into transactions so you can accurately identify anomalous network, device, and environment patterns that potentially indicate an attack.

Finally, attackers are economically driven. In turn, you need to attack their economics, because any defense will fail to deter a sophisticated adversary if the value is high enough. These attackers and fraudsters will adapt to every countermeasure by retooling to bypass your defenses. You can't predict every future attack, so you need to adapt when you encounter them and maintain full security efficacy without introducing friction that can cause your real customers to abandon their interactions. The only viable defense is deterrence, disrupting attacker economics by making successful attacks too costly to be feasible.

For more information on how to stop credential stuffing attacks that lead to account takeover, and other bot-driven attacks, visit **f5.com/bots**



Sources

[1] 2019 Application Protection Report, F5 Labs https://www.f5.com/labs/articles/threat-intelligence/2019-application-protection-report

[2] Verizon 2020 Data Breach Investigations Report https://enterprise.verizon.com/resources/reports/dbir/

[3] "Online Payment Fraud Losses to Exceed $200 Billion over Next Five Years," Juniper Research (Feb 25, 2020) https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion

[4] "Artificial Intelligence as Security Solution and Weaponization by Hackers," CISO MAG (Dec 19, 2019) https://cisomag.eccouncil.org/hackers-using-ai/

ABOUT F5

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

For more information on how to stop credential stuffing attacks that lead to account takeover, and other bot-driven attacks, visit **f5.com/bots**

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

DC0122 | FUJ-CORP- 823942344