Healthcare CAPTCHA: The Cure that's Worse than the Disease

Customer Story

CUSTOMERS OUT. CRIMINALS IN.

"This is not who we are," muttered the CIO of one of the largest health insurance companies in the world as he looked over the report.

The digital team had decided to add a CAPTCHA to the site's login page. As a direct result, older patients were struggling to access their accounts. 70% of this patient demographic had been driven off the website and pharmacy orders were also down a shocking 70%. The call center was swamped at 130% of typical call volume with site users struggling to pass the visual puzzles.

What's worse? The automation attacks this CAPTCHA was set up to defend against was being easily bypassed by cybercriminals.

Putting the cart before the horse– driving innovation without considering security

The seeds of this customer experience calamity were planted with good intensions.

The global healthcare insurer had introduced an innovative Health Rewards program that was hailed as a bold "gamification of wellness". The program rewarded patients with points for achieving preventive medical milestones, such as scheduling wellness checkups, screening for bone density, and getting flu shots. Patients even received points for volunteering or participating in nutrition classes—activities that were good for their social and mental health and community bonding. The program was encouraging conscientious behavior with personal rewards.

The reward points themselves had no cash value but could be redeemed in the insurer's online mall for gift cards from retailers like Amazon and Walmart. Those gift cards did have monetary value of course and proved a juicy target for gift-card crackers.

THE DEPARTMENT OF HEALTH AND HUMAN SERVICES ANNOUNCED IN 2021 ALONE, OVER 27 MILLION INDIVIDUALS WERE AFFECTED BY HEALTHCARE INDUSTRY BREACHES CLASSIFIED AS "HACKING/IT INCIDENT".

Cue the credential-stuffing attacks

Almost immediately, cybercriminals began launching credential-stuffing attacks at the login page of the insurance company's rewards program. Credential stuffing is the act of testing millions of previously breached username and password combinations against a website with the knowledge that there will be a certain percentage of valid credentials. Success rates for an individual credential-stuffing login vary between 0.1 - 2.0% depending on the client population.

The Department of Health and Human Services announced in 2021 alone, over 27 million individuals were affected by healthcare industry breaches classified as "Hacking/IT Incident".

That may seem low, but attackers are able to scale their attempts into the millions via *automation*—scripted programs called “bots.” Modern bots look very much like human users to a target computer. Telling them apart is one of the most difficult problems in modern computer science. A 1% success rate in a credential-stuffing attack is a reasonable statistical estimate; one million leaked credentials will yield 10,000 successful logins against a third party, leading to account takeovers by the attacker and resulting monetization schemes. Learn more about the costs and incentives behind cyber attacks in this Attacker Economics Report.

How to Detect Automated Attacks

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. 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.

Figure 1: How do you know if you are being attacked? There are four important ways to start diagnosing automated attacks on your organization.

Attackers were able to successfully breach thousands of the healthcare customer’s accounts and access the rewards program. They consolidated reward points and converted them into gift cards, from which they exfiltrated the real cash value. The resulting fraud loss from gift card cracking wasn’t this customer’s top concern. The CIO and IT team wanted first and foremost to protect their customers and their data.

> **“We were much more anxious about the PII exposure than the fraud loss.”**
> **–Global Health Insurer CIO**

Fortunately, the attackers appeared to be ignoring the Personally Identifiable Information (PII) associated with the cracked accounts in favor of getting the rewards points, but the exposure was alarming and could not be ignored.

The security team turned reactively to their Content Delivery Network (CDN) vendor for help. The CDN’s “bot management” solution put a CAPTCHA into the user login process in a failed attempt to stop the automation.

CAPTCHA Stops Customers, Not Criminals

Human success rates for CAPTCHAs are as low as 15% for certain demographics. The tests have become increasingly more difficult because computers have gotten so good at solving them. For elderly users who are often visually impaired, CAPTCHA success rates are even lower. One would be hard-pressed to devise a worse user experience than CAPTCHA for an aging population trying to access their health insurance information.

CAPTCHAs are only a speed bump for motivated attackers while introducing considerable friction for legitimate customers.

Immediately after the CDN put their CAPTCHA in place, login success rates plummeted. Seven out of ten elderly users could no longer access their accounts, the rewards program, or prescription renewals online. Frustrated patients started reaching out to customer support for help.

Online pharmacy orders plunged by 70%.

Meanwhile, the attackers were easily bypassing the “bot management” solution through one of the many affordable underground services that enable simple and effective CAPTCHA solving at scale. Read this blog for more on how cybercriminals bypass CAPTCHA with ease.

Now the criminals were the only ones earning rewards from this new loyalty program. The CAPTCHA was adding to the problem it was intended to solve for. Not only was this insurer still suffering from fraud loss and exposed PII, but CAPTCHA had also added user friction, call center costs, and a negative customer experience into the mix.

F5 Steps in to Remove Automation *and* Friction

F5 DETECTS UP TO TWO MILLION MALICIOUS AUTOMATED LOGIN ATTEMPTS PER DAY FOR HEALTHCARE CUSTOMER THAT THEIR EXISTING SOLUTION WAS MISSING.

After an introduction from another F5 customer, the CIO reached out to us to remedy the situation. F5's XC Bot Defense was deployed quickly and went right into monitoring mode to analyze the attack traffic patterns. F5 came in behind the health insurer's CDN solution so we were able to show exactly how much credential stuffing and gift cracking they were missing—sometimes up to two million automated attempts per day!

While the attackers had been smart enough to "hide" their traffic spikes within the diurnal patterns associated with human logins, they were not otherwise trying to disguise their traffic. They connected through proxies, sometimes through a partner healthcare insurer, and even once through a financial aggregator.

Once in mitigation mode, F5 was able to block the automation and fight attackers as they retooled in an attempt to get around our defenses. Within weeks a vast majority of the attackers gave up the fight, resulting in a 90% decrease in overall traffic.

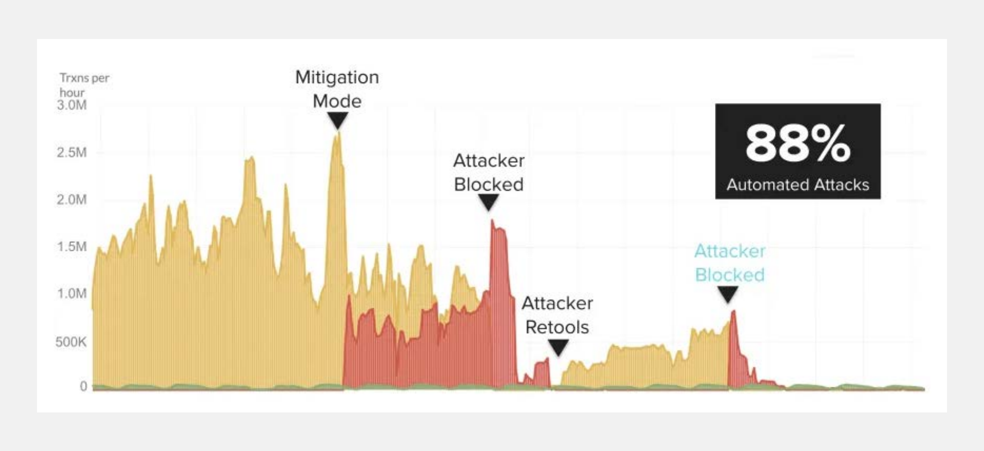

Figure 2: Once F5's XC Bot Defense was deployed, the attacker quickly retooled.

F5 completely displaced the CDN for bot management at the health insurer's web property and the CAPTCHAs were removed from two dozen entry points. We quickly began work to protect their mobile property as well.

CUSTOMERS IN. CRIMINALS OUT!

Knowing that attackers often retarget to mobile after being blocked on web, F5 quickly got in line to defend this customer's mobile application. After about a month, we were able to add additional value by leveraging the same technology to remember legitimate users. F5 cut the health insurer's legitimate "forgot password" transactions in half.

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.

Steady State Unlocked

F5 XC Bot Defense now protects the healthcare insurer's website and has replaced every damaging CAPTCHA that once sat in front of their pharmacy, account profiles, and rewards program. F5 is also integrated with nearly all the mobile platforms that the insurer reports.

As a result, the online pharmacy is easily accessible to all customers again and call volumes have dropped to levels not seen since before the CAPTCHA crisis. Attackers and aggregators continue to probe the insurer's web and mobile properties. F5 continues to block the attackers. The health insurer is notified of the aggregators and encourages them to use authorized API gateways.

By replacing CAPTCHA with F5 XC Bot Defense, this healthcare company was able to:

- Drastically reduce account takeover attacks and gift card cracking fraud on web and mobile applications.
- Remove login friction and improve user experience.
- Cut legitimate customer "forgot password" transactions in half.
- Reduce call center costs.
- Provide aggregator management capabilities.

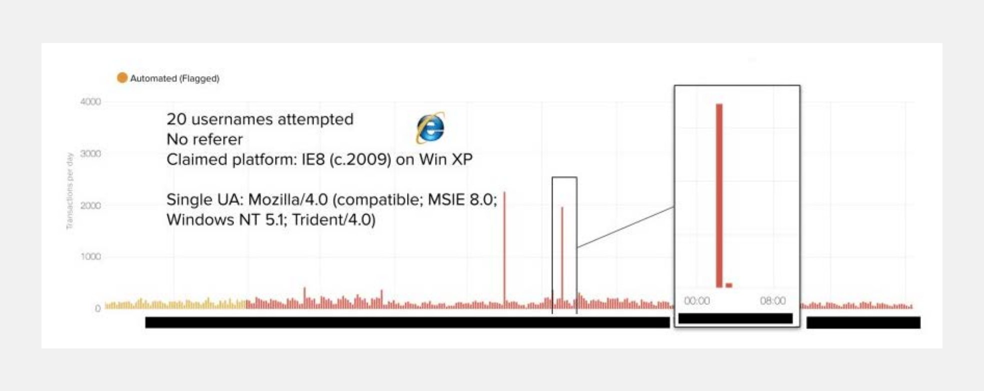

Figure 3: Attackers continue to probe (unsuccessfully) today.

With balance restored, this healthcare insurer was able to return their focus to innovating new programs and driving value for their customers.

Learn more about how F5 stops fraud without friction.