BEYOND IDENTITY

The Top 10 MFA Bypass Hacks

Multi-factor authentication (MFA) breaches are becoming alarmingly commonplace, with cyberattacks no longer necessitating advanced skills or deep knowledge to bypass these security measures.

The scale at which multi-factor authentication (MFA) is being compromised is a testament to its vulnerabilities. Increasingly, hackers are leveraging easily accessible tools and techniques, such as purchasing stolen credentials from Initial Access Brokers (IABs) on the dark web. Coupled with simple strategies like social engineering, they can effortlessly sidestep MFA, leaving organizations exposed to data theft and ransomware attacks.

Read on to learn about ten of the most significant MFA bypass hacks that have hit major organizations.

Uber

The notorious Lapsus$ group's hackers breached Uber's IT systems through "MFA fatigue". Having illicitly gained an Uber contractor's password details, the attackers kept trying to log in, bombarding this individual with MFA push notifications.

Eventually, the contractor approved one, giving the hackers access to Uber's systems. No sensitive data was stolen, but the attack caused disruption and embarrassment for Uber.

Okta

Hackers recently bypassed the multifactor authentication (MFA) defenses of multiple Okta customers (including MGM resorts) by convincing their IT service desk personnel to reset the MFA of privileged users. They used social engineering tactics, possibly presenting legitimate credentials or manipulating the authentication flow. This gave them privileged access to the victims' systems.

Slack

Private source code was downloaded from Slack's Github repository by hackers. They used stolen employee tokens they'd illicitly obtained to bypass MFA defenses and gain access. This could have been very damaging for Slack, but fortunately, none of the repositories accessed by the attackers contained customer data or the company's primary codebase.

Microsoft

A massive phishing spree targeted over 10,000 organizations using Microsoft Office 365. The attackers set up fake Office 365 login pages to trick users, capture their login details, and hijack the MFA process.

Some victims were led to these fake pages through phishing emails with HTML attachments. After obtaining victims' credentials and session cookies, the attackers accessed their email accounts and then used them to scam yet more organizations.

Cisco

In another example of "MFA fatigue", hackers attacked Cisco by first using stolen credentials to get into an employee's personal Google account, which had synced Cisco credentials. They then wore down the employee with numerous MFA requests and voice notes pretending to be support agents. They eventually accepted one of these requests, allowing the hackers to get into Cisco's systems and infect it with ransomware that stole over three thousand files, which included NDAs.

Deutsche Bank

Deutsche Bank suffered the theft of customer data due to a data breach at one of its third-party service providers, Majorel Germany. The Russia-backed Clop ransomware gang exploited an SQL injection vulnerability in the MOVEit software Majorel Germany was using. This allowed the attackers to breach the cybersecurity defenses and obtain thousands of customer names and account numbers.

EA

Hackers bypassed EA's MFA defenses using social engineering methods, allowing them to steal a staggering 780 GB of data. The attackers used stolen cookies they'd purchased online to gain access to an internal EA Slack channel. They then messaged EA's IT department pretending to be an employee who'd lost their phone.

The hackers successfully tricked the IT staff into giving them a MFA token, allowing them to access EA's corporate network. Once inside, they extracted this huge quantity of data, which included source code for FIFA 21.

Bangkok Airways

Bangkok Airways suffered a ransomware attack by the LockBit gang, with the hackers claiming to have stolen over 200GB of data belonging to the company, including sensitive data like passport and credit card information. The group also claimed that the airline's password was "P@ssw0rd", enabling them to easily bypass their MFA defenses.

Twilio

Hackers impersonated Twilio's IT department and sent SMS phishing messages to employees, claiming there were issues with their passwords. The messages contained links to fake Twilio login pages, which harvested these employees' credentials. Using the stolen credentials, the attackers breached Twilio's MFA-protected systems, accessing data belonging to at least 125 customers.

Roblox

Hackers bypassed the MFA defenses of Roblox, an online game creation platform, by targeting an employee with "highly personalized" social engineering tactics. This phishing attack resulted in 4GB of internal documents being stolen.

Honorable mention: Twitch

Twitch suffered a huge data breach, which exposed at least 128GB of sensitive data, due to a server configuration error. A "hacktivist"— motivated by hatred of Twitch—exploited this misconfiguration to bypass the company's MFA defenses, access the company's servers, and leak the data.

How to stop MFA bypass attacks

The reality is that traditional MFA simply can't protect your organization. Cybercriminals have developed too many methods to bypass it. To stop such cyberattacks, Zero Trust Authentication is absolutely essential.

Beyond Identity is the leading innovator in secure authentication. Our passwordless, phishing-resistant MFA prevents credential breaches and offers a seamless user experience. See how we can help your organization and get a demo today.

BEYOND IDENTITY

Beyond Identity is revolutionizing digital access for organizations looking to improve protection against cyber attacks and deliver the highest levels of security for their workforces, customers and developers. Its suite of passwordless, phishing-resistant, and zero trust authentication solutions improves security and user experience. The platform delivers continuous risk-based authentication incorporating signals from the zero trust ecosystem to ensure only valid users and secure devices gain or maintain access to critical resources. Companies like Snowflake, Unqork, and Roblox rely on Beyond Identity's highly available cloud-native platform to thwart attacks and advance their zero trust strategies. To learn more about Beyond Identity's FIDO-2 certified multi-factor authentication (MFA) solutions, visit beyondidentity.com and stay connected with us on Twitter, LinkedIn, and YouTube.