Arkose Labs

MFA Compromise: Reverse Proxy Phishing Solution

OTP Code Theft: A Weakness in MFA Defense

Man-in-the-middle (MITM) reverse proxy phishing attacks cost more than $2 billion each year globally and untold losses in diminished consumer trust. An MITM reverse proxy phishing attack involves software that acts as an intermediary between the user and the target site. Even multi-factor authentication (MFA) can't stop reverse proxy phishing attacks because bad actors bypass MFA safeguards.

In this type of attack, a user clicks on a malicious URL/link and is directed to a phishing site. This site functions as a reverse proxy, capturing traffic to the legitimate target site. When the user enters their credentials, including 2FA/MFA tokens, the reverse proxy captures and harvests these tokens for malicious use. The software accesses the target site programmatically, rewrites the traffic, and enters the stolen data without human involvement. This allows the reverse proxy to complete the transaction on the target site, effectively bypassing MFA protections.

Arkose Bot Manager Phishing Protection

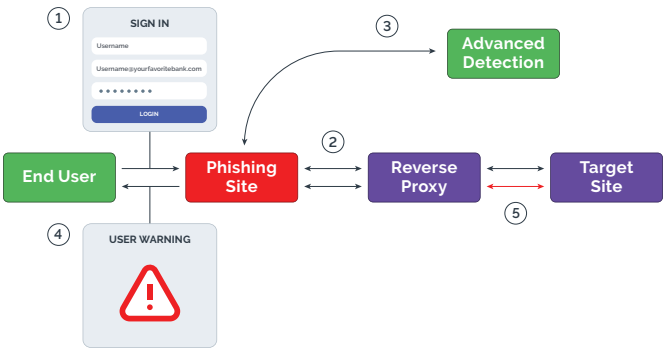
Protect your consumer experience and revenue-generating activities with an advanced threat detection system. Arkose Bot Manager's phishing protection effectively thwarts MITM advanced phishing attacks, also known as reverse proxy phishing or adversary-in-the-middle (AITM) attacks:

- Detect attacks in real time
- Deter credential theft
- Stop MFA/2FA code interception
- Prevent stolen authentication tokens
- Warn users with customized alerts

Arkose Bot Manager's phishing protection offers unmatched cyberattack detection and mitigation technology in real time to prevent the exploitation of login credentials, usernames and passwords, one-time passcodes (OTPs) and session tokens. Key capabilities include:

- Real-time attack detection using client- and server-side signatures
- Managed phishing detection rulesets
- Hostname allow and deny lists
- Immediate, configurable end-user warning messages
- Support for both active interception and monitor-only modes
- In-depth visibility and detailed reporting

MITM Reverse Proxy Phishing Detection



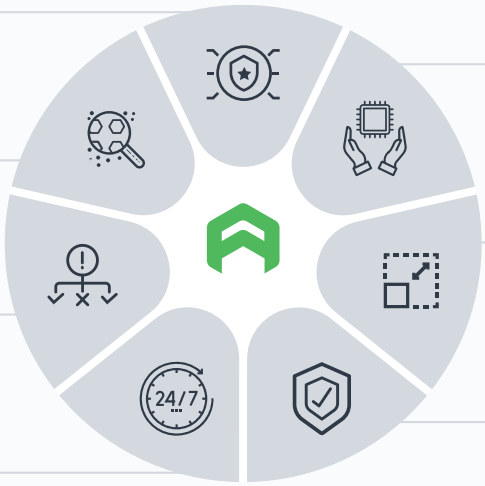
The Arkose Labs Advantage

Powerful collective impact
Global Intelligence Network data consortium for intelligence sharing

Unrivaled threat research
Dedicated threat-hunting, disarmament and enforcement

Transparent risk signals
Real-time threat and response visibility for downstream decisioning

Global, proactive support
24/7/365 SOC meets all cyber and privacy regulations



Pioneering technology
Proactively identifies attackers and effectively stops attacks

Proven at scale
Trusted by the world's largest B2C and global brands

Warranties
$1M warranties per event for cyberattacks

ACTIR and the Arkose Labs SOC

Arkose Labs operates as an extension of your team, rapidly countering attacks and providing actionable insights without overburdening your internal resources. The Arkose Cyber Threat Intelligence Research (ACTIR) unit conducts proactive threat hunting, risk intelligence gathering and other counterintelligence methods to provide vital, fresh intelligence. Meanwhile, the 24/7/365 Security Operations Center (SOC) team focuses on identifying and stopping large-scale attacks immediately.

The SOC continuously monitors for new threats and collaborates with ACTIR. This feedback loop ensures a seamless collaboration between the SOC and ACTIR, enhancing the overall accuracy, timeliness and effectiveness of your cybersecurity defense.

Arkose Bot Manager Takes On EvilProxy

EvilProxy is a sophisticated and widely used MITM phishing-as-a-service kit that allows attackers to bypass MFA. Traditional phishing detection tools miss a majority of EvilProxy attacks, but Arkose Bot Manager snares them. The proof: We conducted an analysis of requests on three login endpoints. Of 250 suspicious domains, 96% would have slipped past a traditional phishing detection method.

250 Suspicious Domains

Traditional Detection Method

→ **10/250** total suspicious domains detected

Arkose Labs Phishing Protection

→ **49** domains less than 60 days old (indicating they were likely created for attack)

→ **191** short-lived URLS (indicating they served their attack purpose and soon disappeared)

> "Brilliant product and great partners. Arkose Labs has a fantastic solution that ends all bulk attacks against your system, manual or automated. Their managed service provides peace of mind and effective management on top of their incredible technology."— **Sean H., CTO, Verified G2 User**

BOOK YOUR DEMO