Arkose Labs | SOLUTION BRIEF

Arkose Phishing Protection

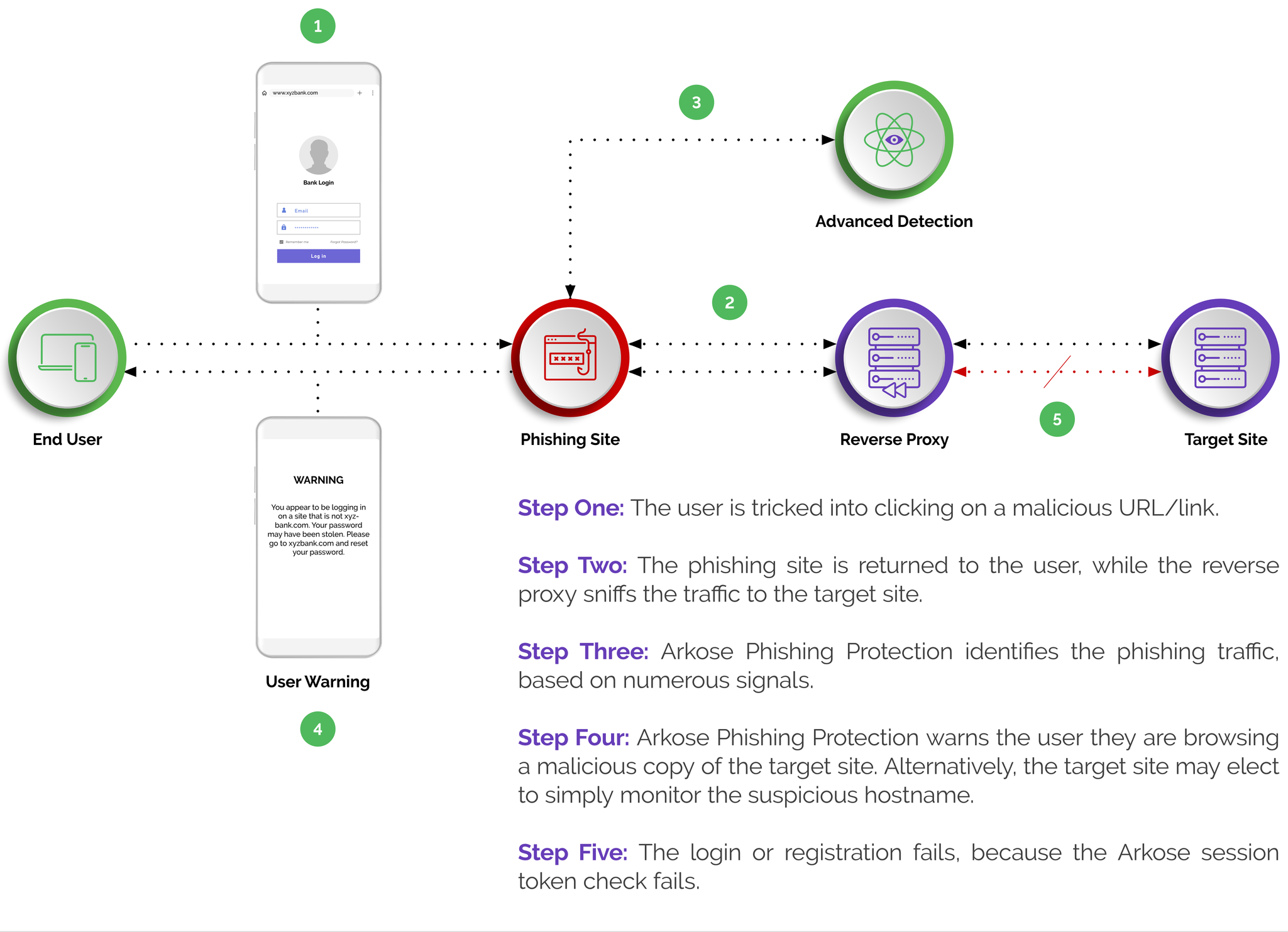
Safeguard Your Business from Powerful Reverse-Proxy Phishing Attacks

Phishing attacks have soared recently, due to the rise of sophisticated proxy phishing frameworks and new attack platforms operating as PhaaS (phishing as a service). With low deployment barriers and detection-avoidance capabilities like anti-bot protection and short-lived domains, your business faces a dangerous adversary. Unfortunately, traditional solutions struggle to detect and defend against adversary-in-the-middle (AITM) and reverse-proxy phishing campaigns. These "after-the-fact" solutions rely on offline analysis, and the phishing event or website is usually discovered only days later, after significant damage is done. This new breed of cybercrime calls for a proactive, adaptive approach.

Arkose Phishing Protection

Arkose Phishing Protection is a powerful solution designed to effectively counter reverse-proxy phishing attacks and safeguard login and MFA credentials from theft. It offers essential features that cater to the needs of product security teams, providing them with the necessary configurability and intelligence to protect their applications and users. With real-time detection capabilities, it identifies and mitigates reverse-proxy phishing attacks using both client- and server-side signatures. The solution includes managed phishing detection rulesets, hostname allow and deny lists, and immediate end-user warning messages, and it supports both active interception and monitor-only modes.

How It Works



Step One: The user is tricked into clicking on a malicious URL/link.

Step Two: The phishing site is returned to the user, while the reverse proxy sniffs the traffic to the target site.

Step Three: Arkose Phishing Protection identifies the phishing traffic, based on numerous signals.

Step Four: Arkose Phishing Protection warns the user they are browsing a malicious copy of the target site. Alternatively, the target site may elect to simply monitor the suspicious hostname.

Step Five: The login or registration fails, because the Arkose session token check fails.

Why Add Phishing Protection to Your Arkose Labs' Deployment

- Detect reverse-proxy phishing attacks in real time
- Protect users and block credential theft
- Prevent interception of MFA/2FA codes
- Warn users with customized alerts

Superior Reverse-Proxy Attack Detection	Traditional solutions rely on static indicators and known phishing URLs. Arkose Phishing Protection builds on the unmatched bot detection and mitigation technology of Arkose Bot Manager to stop reverse-proxy attacks and prevent the theft of login and MFA credentials.
Real-Time Mitigation	Catch phishers in the act. Our solution includes real-time detection of reverse-proxy phishing attacks (using client- and server-side signatures), in-the-moment end user warning messages, and immediate visibility of phishing sessions in the portal.
Flexible Deployment Options	In "active" mode, suspicious hostnames are captured and anti-phishing pressure activates, displaying a warning message to the end user and blocking verification. Alternatively, businesses may choose "monitor" mode to capture and report on potentially malicious activity.
Ease of Integration	The solution is easy to deploy, with no new integration points or engineering work required. Arkose Phishing Protection complements your incumbent solutions to provide well-rounded protection against phishing attacks.

Based on early trials, customers can flag hundreds of thousands of reverse-proxy phishing sessions during initial deployment and block dozens of previously undetected phishing domains within a week of activation.

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as the 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M warranties for credential stuffing and SMS toll fraud. With 20% of our customers being Fortune 500 companies, our AI-powered platform combines powerful risk assessments with dynamic threat response to undermine the strategy of attack, all while improving good user throughput. Headquartered in San Mateo, CA, with offices in London, Costa Rica, and Brisbane, Australia, Arkose Labs protects enterprises from cybercrime and abuse.

Request a 1:1 demo with your CSM today