ATO Threat Monitoring is an advanced security solution that continuously monitors an organization's domains, BINs or emails to protect against credential stuffing attacks, card testing, and account compromise by fraudsters and bad actors.

ATO Threat MONITORING

With *ATO Threat Monitoring,* you tell us the domains, emails, and/or BINs to monitor and we'll alert you to bad actor traffic/malicious activity so you know what is being attacked, how frequently, and how successfully. This service is provided as an annual subscription that covers one or multiple BINs or domains.

Domain Monitoring

We monitor traffic running through myNetWatchman proxies to detect when your organization's domains are being actively targeted by a credential stuffing attack—whether via the web, APIs, a portal, your login page, or elsewhere. *ATO Threat Monitoring* alerts you when the attacks are occurring and provides information such as the targeted email addresses/usernames and passwords, IP address of the attack source, timestamp, and URL where the attack is being attempted.

These alerts provides you with actionable insights that enable your organizations to thwart the attack and to determine remediation actions, such as identifying which impacted users need to be notified. Detecting these attacks often alerts organizations to other issues as well, including failures in bot protection and ATO controls, or deficient application/edge security.

Credit Card BIN Monitoring

Our cutting-edge technology detects compromised card information to provide unparalleled protection of financial data. Real-time alerts enable payment card issuers to quickly respond to

Get alerts when bad actors are actively and successfully, testing credentials or credit cards and know exactly what they are testing

threats and maintain the trust of cardholders. When a BIN range is actively being tested, you can increase scrutiny on all transactions attempted with cards falling within the BIN. As soon as a suspect payment card is fraudulently tested, you can lock down the card and proactively issue a new one, before a fraudulent transaction occurs.

- Know when credential stuffing attacks are targeting your web domain(s).
- Know when employees or contractors using your email domain are targeted with ATO or credential stuffing on external sites or systems.
- Protect cardholders by detecting when their cards are being tested to prevent future fraudulent transactions.
- Know when your BOT and ATO controls to secure credentials aren't working as intended.

15 MILLION
newly-compromised credentials pairs added daily to our ever-expanding database

100	THOUSAND NEW CARDS ADDED DAILY TO OUR EVER-EXPANDING DATABASE
5	MILLION CARD TESTS DETECTED ON 2 MILLION DISTINCT COMPROMISED PAYMENT CARDS
1.5	MILLION WEB DOMAINS TRACKED MONTHLY TO UNCOVER ATTACKS FUELED BY BREACH DATA

BUSINESS USE CASES

Know When and Where Credential Stuffing Attacks Occur

Credential stuffing attacks target consumer and workplace accounts, login pages, APIs and apps. Your organization needs to know when and where these attacks are occurring and respond with corrective action. *ATO Threat Monitoring* alerts you when you are being attacked and tells you where the attack is happening, while simultaneously providing data about the attack. As a result, you're not only aware of the attack, but have the information you need to quickly assess the damage and actively work to stop it.

The insights provided with *ATO Threat Monitoring* not only help your organization stop credential stuffing attacks against your domain(s) and login pages, but these insights also reveal the specific accounts that were targeted and when the attacks were successful so you can promptly notify impacted accounts and/or require them to change their compromised passwords.

Find and fix gaps in user credential security, prioritize attack investigations, and triage mitigation response

Know When Your BINs or Cards Are Being Used

Compromised payment card data is often packaged and sold in BIN/IIN ranges, which fraudsters then test to identify active cards they can use for much larger fraudulent purchase attempts. Your institution can protect cardholders by knowing when there is high frequency use of BINs. Because testing of many cards with the same BIN is critical information that benefits transaction risk-scoring models, *ATO Threat Monitoring* provides continuous monitoring of attempted use of payment cards or BINs and flags this testing. Because successfully tested cards are likely to be used for more significant transactions in the near future, your institution can escalate anti-fraud measures and decline suspicious transaction attempts from these cards. Further, when a card is successfully tested, you can also decide to proactively issue a new payment card and primary account number (PAN) to the impacted cardholder—often at a reduced cost compared to emergency card replacement.

Know When Employees or Contractors Are Being Targeted with ATO or Credential Stuffing Attacks Against Your Email Domain

Too many employees and contractors use a shared password to access multiple systems or services. To protect against this insecure practice, *ATO Threat Monitoring* not only monitors credential stuffing attacks against your website domains, but also observes the credentials being used or attempted. *ATO Threat Monitoring* alerts your organization when there is an ATO attempt

or credential stuffing attack that presents a username or login email under your organization's domain as part of the login credential. This provides confirmation that employees or contractors are being targeted with ATO and reports if the attacks were successful, so you can notify the impacted users to change the compromised passwords anywhere they may be using them.

So easy, you can be up and running in one day...no messy integration work, lengthy rollout, or complex training

1 Diamond Causeway
Suite 21-246
Savannah, GA 31406
+1 678-624-0924

contactus@mynetwatchman.com
mynetwatchman.tech

© 2025 myNetWatchman, LLC. All Rights Reserved.