Jingle Thief: Cloud Identity Tradecraft in Microsoft 365

Stav Setty | Principal Researcher, Palo Alto Networks

An analysis of modern financially motivated cloud intrusions and identity misuse

TROOPERS26

Let’s Play a Game…

How would you find the attacker if the user already let them in?

About Me

Stav Setty

Principal Security Researcher

Palo Alto Networks

Tel Aviv, Israel

UEBA / ITDR Team

Overview

Atlas Lion

Financially motivated Moroccan threat actor operating sophisticated fraud schemes.

Cloud-First Targeting

Exploits cloud-first enterprises through advanced phishing and smishing campaigns.

Microsoft 365 Abuse

Weaponizes M365 services for reconnaissance, persistence, and gift card operations.

Extended Operations

Demonstrates exceptional operational patience with months-long intrusions for impact.

Who is Atlas Lion?

Moroccan cybercrime group

Financially-motivated threat actor

- Active since 2021 with evolving techniques
- Specializes in targeting **gift card issuance systems**
- Focus on large online retailers, insurance, and financial services
- Demonstrates advanced operational security and patience

Past Campaign Impact

222

Phishing Sites

Active infrastructure identified between February 2023 and June 2024 by Intel471 research

$100K

Daily Theft Volume

Peak fraudulent activity reported by Microsoft during active campaign periods

30%

Activity Surge

Significant operational increase observed by Microsoft during holiday periods

FBI reports specifically highlighted Atlas Lion's systematic targeting of gift card departments at major **U.S. retailers**

Campaign Overview

10+

Month Duration

Single enterprise intrusion timeframe

60+

Compromised Accounts

User accounts successfully breached

4

M365 Services

SharePoint, OneDrive, Exchange, Entra ID

Campaign activity is strategically aligned with holiday shopping periods to maximize operational advantage and blend with legitimate high-volume transactions.

Temporary Users & Holiday Surges

Seasonal Staffing

Massive influx of temporary workers with high turnover rates.

Short Lifespans

Accounts created for weeks, leading to "stale" identity sprawl.

Heightened Spending

Gift card issuance volume spikes during holidays

Increased Operations

SOC teams face higher alert volumes and slower response times

Why Gift Cards?

Liquid Assets

Easily resold at discounted rates through underground markets

Minimal Verification

Require minimal personally identifiable information for redemption

Weakly Secured Systems

Frequently issued through systems with weak access controls, broad internal permissions, and limited monitoring or logging

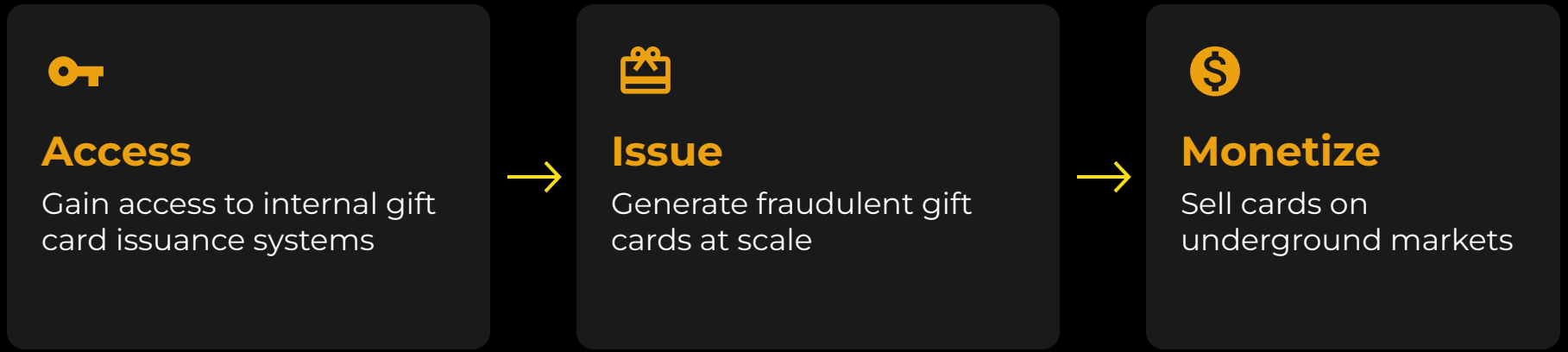
Anonymous Transactions

Largely untraceable and maintain transaction anonymity

Money Laundering

Provide discreet pathways for financial crime operations

Gift Card Issuance Flow



Identity = Money?

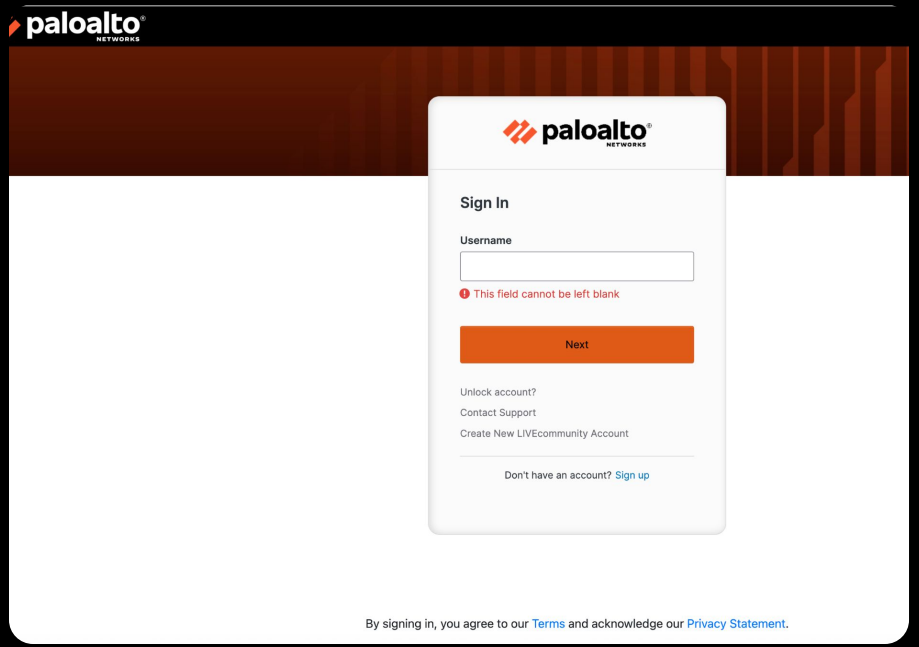
Atlas Lion Attack Lifecycle

- Reconnaissance
- Initial Access
- Discovery/Collection
- Persistence
- Lateral Movement
- Defense Evasion
- Privilege Escalation
- Exfiltration

Phase 01:
Reconnaissance

Highly Targeted Attacks

- Brand Intelligence
- Infrastructure Mapping
- Template Replication



Phase 02:
Initial Access

Initial Access: Threat Vectors

SMS Phishing (Smishing)

Mobile-targeted campaigns leveraging urgent messaging and trusted sender impersonation.

Email Phishing with AiTM

Adversary-in-the-Middle phishing pages designed to harvest credentials and session tokens.

Credential & Session Theft

Attackers relay victim credentials to MFA systems while capturing authenticated sessions.

MFA Bypass

Victims unknowingly approve MFA prompts, providing attackers with authenticated session access.

Initial Access: External Phishing

“ServiceNow Account Inactivity Notice” Phishing Campaign

External phishing emails from the domain **despleg.ar** - April 2025

sender	subject	recipient_count
[redacted]despleg.ar	ServiceNow Account Inactivity Notice	1106
[redacted]despleg.ar	ServiceNow Account Inactivity Notice	247
[redacted]	ServiceNow Account Inactivity Notice	4
[redacted]service-now.com	ServiceNow Account Inactivity Notice	1
[redacted]	ServiceNow Account Inactivity Notice	1
[redacted]despleg.ar	ServiceNow Account Inactivity Notice	1

DETECTIVE BRIEFING

Email Header Investigation Challenge

Can you spot the interesting email header?

```
MIME-Version: 1.0
X-MS-Exchange-CrossTenant-OriginalArrivalTime
11 Apr 2025 18:37:44.1596 (UTC)
Content-Type: text/html; charset="UTF-8"
X-PHP-Script: domain.ar/attache/index.php
Content-Transfer-Encoding: quoted-printable
```

DETECTIVE BRIEFING

Email Header Investigation

Can you spot the interesting email header?

```
MIME-Version: 1.0
X-MS-Exchange-CrossTenant-OriginalArrivalTime
11 Apr 2025 18:37:44.1596 (UTC)
Content-Type: text/html; charset="UTF-8"
X-PHP-Script: domain.ar/attache/index.php
Content-Transfer-Encoding: quoted-printable
```

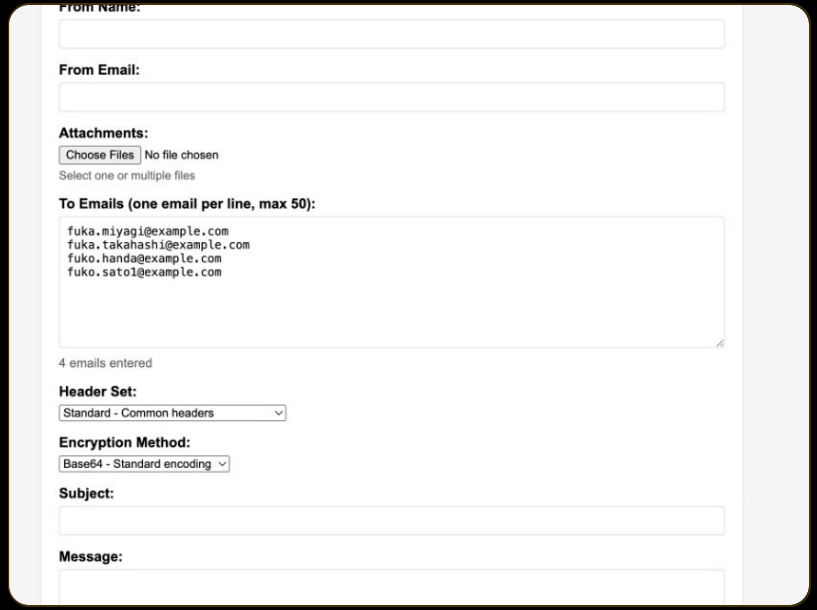
INVESTIGATION LOG

PHP Email Sender Discovery

Our email header investigation uncovered the attacker's infrastructure!

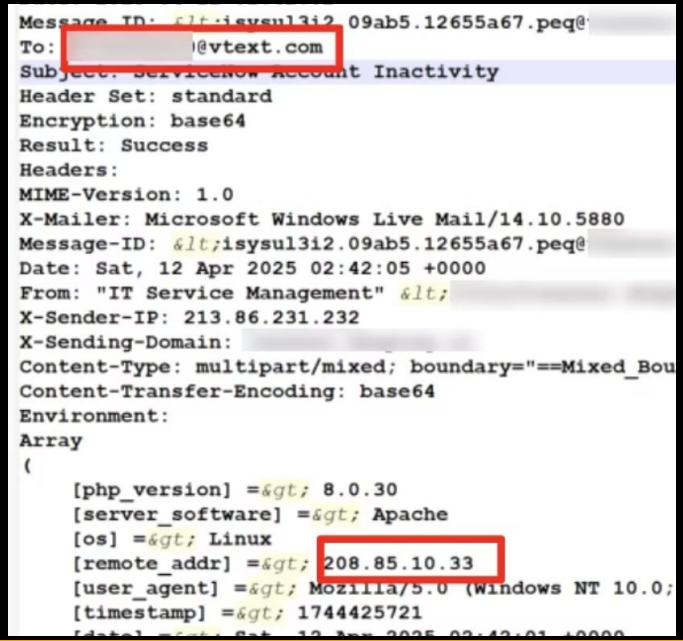
We found it by looking at the **X-PHP-Script** header of the email logs.

```
X-PHP-Script:
<attacker_domain>/attache/index.php
```



DETECTIVE BRIEFING

PHP Email Send Logs



Extensive email send logs revealed clear indicators of **SMS phishing (smishing)** activities.

Target: Individual Users

"Bill doesn't read email headers... don't be Bill."

Phase 03: Discovery/Collection

Discovery + Collection

Atlas Lion mines SharePoint and OneDrive for sensitive corporate workflows, including:

VPN Infrastructure

- VPN test cases
- MFA token installation guides
- Device registration documentation

Gift Card Systems

- Catalog procedures
- Issuance guides
- Platform documentation

Remote Access

- VDI migration plans
- Remote Desktop guides
- Workspace configuration documentation

Discovery + Collection - Examples

https:// com/sites/Systems_Engineering_and_Operations/SiteAssets/SitePages/Global-Protect-VPN-Test-cases/**Global-Protect-VPN-Test-cases.xlsx**
https:// .com/sites/RSA/RSA Installation Guides/**Instructions to install and import RSA token on smartphone.pdf**
https:// com/sites/RSA/RSA Installation Guides/RSA-MFA-guide/ **RSA SecurID Authenticate Device Registration Overview.pdf**
https:// .com/sites/ _IT_Support/SiteAssets/SitePages/**Way-to-connect-to-the-VPN/2 -anyconnect1.png**
https:// .com/sites/ IT_Support/SitePages/**Way to Use Citrix.aspx**
https:// .com/sites/ /**ariba-giftcard-order-catalog.pdf**
https:// .com/sites/ /ContactCenterResources/SiteAssets/SitePages/**Training Resources/Gift-Card-Integration_Huddle-Guide.pdf**
https:// .com/sites/CustomerCare /**Citrix VDI Migration.pdf**
https:// com/sites/ Shared Documents/Apps(1)/Viva Engage/**CREDIT PROMO SIGN CARD.pdf**

Email Collection

The compromised accounts showed extensive email access patterns, indicating systematic collection of corporate communications.

Log analysis revealed **high-volume mail item access** across multiple user mailboxes.

MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	2	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	4	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	10	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	10	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104
MailItemsAccessed	11	MT-MPLS	41.250.190.104

Phase 04:
Exfiltration

Exchange Inbox Rules

Automatic actions in Microsoft Exchange/Outlook that help organize, filter, and manage emails without manual intervention.

Conditions

Define triggers like sender, subject patterns, or keywords.

Actions

Move, forward, delete, or flag matching messages.

Exceptions

Exclude specific scenarios from rule execution.

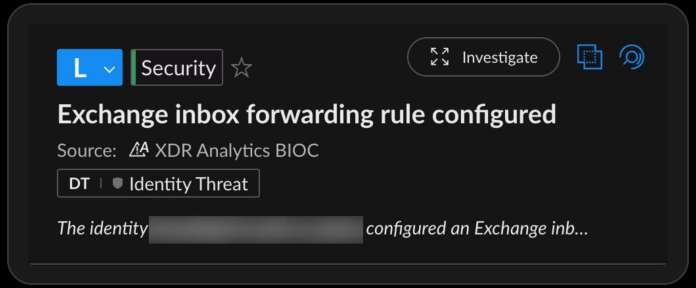
Most Common Abuse: Move or forward emails by regex pattern matching in subject or body content.

Mailbox Display Name	Rule Name	Conditions Configured	Actions Configured	Exceptions Configured
Enola Holmes	Move to Junk	Subject Contains Words, Subject or Body C...	Move To Folder, Apply category, Send Text ...	Except Subject Contains Words, Ex
Jennnifer Longbottom	FowardingAttachmentsRule	Subject Contains Words, Subject or Body C...	Apply category, Forward as Attacment To, ...	Except Subject Contains Words, Ex
Jennnifer Longbottom	ForwardingRule	Subject Contains Words, Subject or Body C...	Apply category, Forward To, Send Text Mes...	Except Subject Contains Words, Ex

Email Exfiltration Mechanism

The threat actor established persistent data exfiltration channels through **malicious inbox rules**.

These rules automatically forwarded incoming emails to attacker-controlled external addresses, enabling continuous intelligence collection.

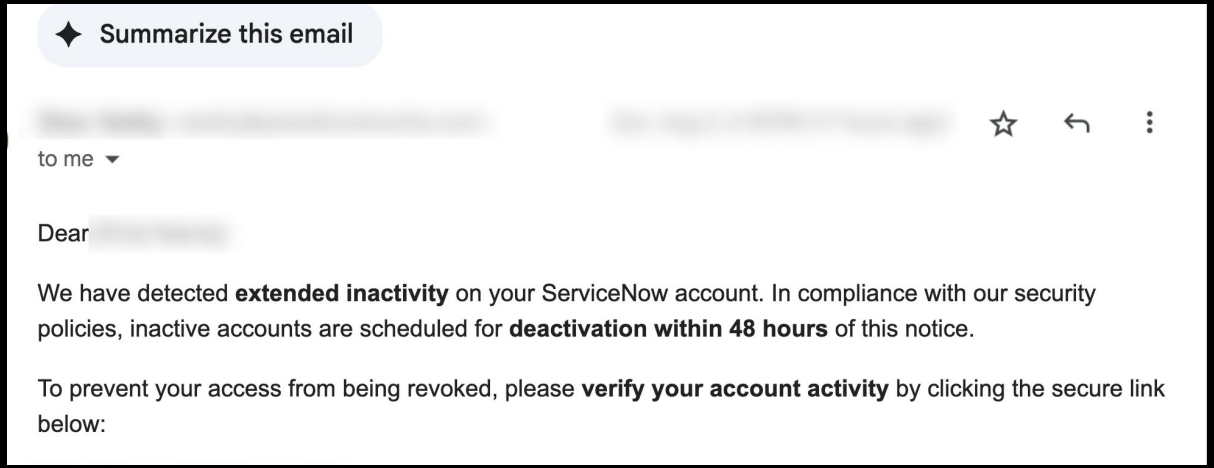


This technique provides continuous access to corporate communications without requiring persistent system access.

Phase 05:
Lateral Movement

Lateral Movement

Internal Phishing



Key Insight: Internal phishing significantly increases success rates due to implicit trust in sender authenticity.

Phase 06:
Defense Evasion

Defense Evasion Tactics

Email Cleanup

Phishing emails systematically moved from **Sent Items** to **Deleted Items** to avoid detection by security teams.

Deleted Phishing Campaign Examples:

- "INCIDENT REQ07672026 Has been completed"
- "ServiceNow Account Inactivity Notice"
- "Incident pending your review"

User moved Exchange sent messages to deleted items	The user [redacted] moved many sent email messages to \Deleted Items in Exchange. A total of 11 messages were moved in a span of 10 minutes. The messages moved: FW: ServiceNow Account Inactivity Notice, FW: ServiceNow Account Inactivity Notice,ServiceNow Account Inactivity Notice, Re: Service Now email?, ServiceNow Account Inactivity Notice

Inbox Cleanup Operations

Defense Evasion Tactics

Beyond sent item cleanup, the attacker systematically deleted incoming emails from user inboxes to eliminate forensic evidence and prevent victim awareness.

Automatic reply: INCIDENT REQ07672026 Has been completed

Re: TSC Incident pending your review

RE: Phishing attempt

operation_name_orig	email_subject	folder	dest_folder
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	RE: Phishing attempt	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: TSC Incident pending your review	\Inbox	\Deleted Items
MoveToDeletedItems	Re: TSC Incident pending your review	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: TSC Incident pending your review	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\Deleted Items
MoveToDeletedItems	Automatic reply: TSC Incident pending your review	\Inbox	\Deleted Items

Phase 07:
Persistence

Persistence Mechanisms

Advanced Persistence Tactics

MFA Bypass
Registering rogue authenticator apps to circumvent multi-factor authentication controls

Password Reset Abuse
Exploiting self-service password reset flows to maintain account access

Device Registration
Enrolling attacker-controlled devices in Azure AD for persistent authentication

Phase 08:
Privilege Escalation

Privilege Escalation

Legitimate Infrastructure Abuse

The threat actor leveraged **ServiceNow's** legitimate ticketing system to request elevated permissions.

To security teams monitoring access requests, this seemed like **standard IT operations**.

No More Tricks

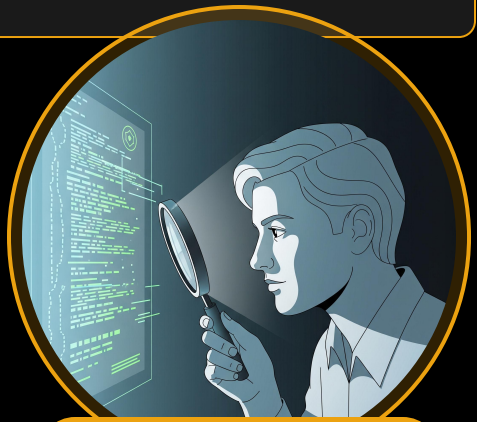
Closing the curtain on attacker TTPs

Detection!

Detection: Inbox Forwarding Rules

Monitoring Suspicious Mailbox Operations

```
(Operation_name_orig IN (NEW_INBOX_RULE, SET_INBOX_RULE)
AND ExchangeParameters CONTAINS (FORWARD_TO,
FORWARD_AS_ATTACHMENT_TO, REDIRECT_TO))
OR (Operation_name_orig = UPDATE_INBOX_RULES
AND ExchangeProperties CONTAINS FORWARD
AND ExchangeParameters CONTAINS (ADD_MAILBOX_RULE,
MODIFY_MAILBOX_RULE))
AND ForwardingAddress MATCHES EMAIL_REGEX
```



DETECTION LOGIC

Detecting Inbox Forwarding Rules

New/Set Inbox Rules

Operation_name_orig in:

- NEW_INBOX_RULE
- SET_INBOX_RULE

AND ExchangeParameters contains:

- FORWARD_TO
- FORWARD_AS_ATTACHMENT_TO
- REDIRECT_TO

Update Rules

Operation_name_orig = UPDATE_INBOX_RULES

AND ExchangeProperties like FORWARD

With:

- ADD_MAILBOX_RULE
- MODIFY_MAILBOX_RULE

Regex Matching

ForwardingAddress matching email regex:

```
[\w._%+-]+@[\w.-]+\.[\\w]{2,}$
```

BEHAVIORAL ANALYSIS

Profiling Normal Activity

Filter legitimate activity by establishing behavioral baselines:

User Frequency

How many forwarding rules does this user typically create monthly?

Target Scope

How many other users has this account performed operations on?

Domain History

How long has the forwarding destination domain been seen in the org?

Domain Type

Is the destination a public email domain (Gmail, Yahoo, etc.)?

HIGH-CONFIDENCE SIGNALS

Stronger Identifiers - Forwarding Rule Detection

Rule Content Analysis

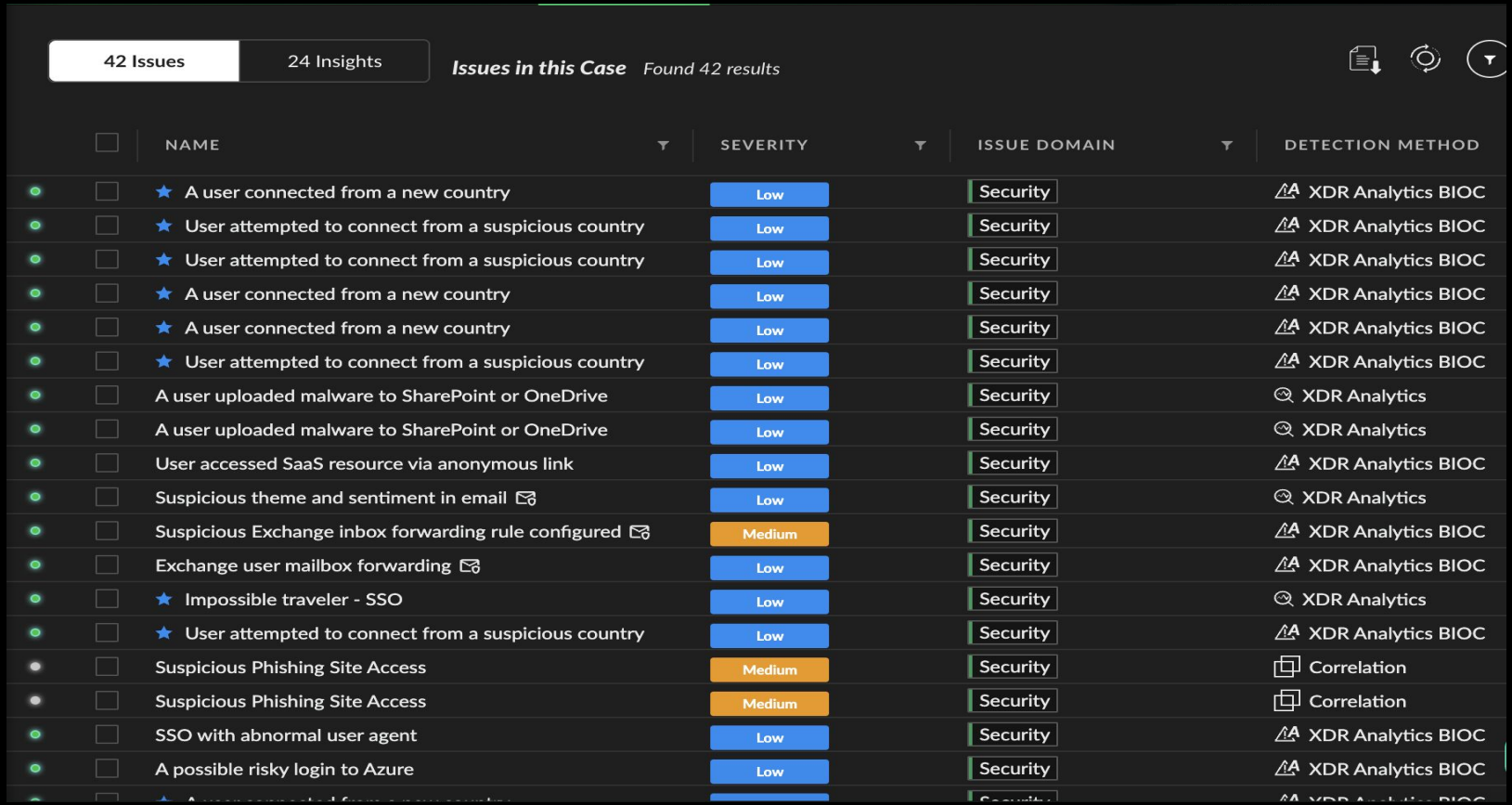
Flag rules containing suspicious keywords that indicate malicious intent:

wire transfer

MFA

Domain Length

Flag domains exceeding 25 characters in length—a common pattern in attack infrastructure.


42 Issues
24 Insights
Issues in this Case
Found 42 results
NAME
SEVERITY
ISSUE DOMAIN
DETECTION METHOD
A user connected from a new country
Low
Security
XDR Analytics BIOC
User attempted to connect from a suspicious country
Low
Security
XDR Analytics BIOC
User attempted to connect from a suspicious country
Low
Security
XDR Analytics BIOC
A user connected from a new country
Low
Security
XDR Analytics BIOC
A user connected from a new country
Low
Security
XDR Analytics BIOC
User attempted to connect from a suspicious country
Low
Security
XDR Analytics BIOC
A user uploaded malware to SharePoint or OneDrive
Low
Security
XDR Analytics
A user uploaded malware to SharePoint or OneDrive
Low
Security
XDR Analytics
User accessed SaaS resource via anonymous link
Low
Security
XDR Analytics BIOC
Suspicious theme and sentiment in email
Low
Security
XDR Analytics
Suspicious Exchange inbox forwarding rule configured
Medium
Security
XDR Analytics BIOC
Exchange user mailbox forwarding
Low
Security
XDR Analytics BIOC
Impossible traveler - SSO
Low
Security
XDR Analytics
User attempted to connect from a suspicious country
Low
Security
XDR Analytics BIOC
Suspicious Phishing Site Access
Medium
Security
Correlation
Suspicious Phishing Site Access
Medium
Security
Correlation
SSO with abnormal user agent
Low
Security
XDR Analytics BIOC
A possible risky login to Azure
Low
Security
XDR Analytics BIOC

Threat Intelligence

Attack IOCs - ASNs

Morocco-Based Infrastructure

Primary Threat Indicators:

- MT-MPLS
- ASMedi
- MAROCCONNECT

Strongest indicators of malicious activity

US-Based Infrastructure

Secondary Indicators:

- ASN-CXA-ALL-CCI-22773-RDC (70.187.192.236)
- FUSE-NET (72.49.91.23)

Legitimate ASNs with evidence of malicious use

THREAT INTELLIGENCE

Phishing URL Patterns

Many phishing URLs are hosted on legitimate domains, likely through compromised WordPress sites.

Note: Many URLs use "@" notation to appear more legitimate; the browser ignores everything before the "@".

Common Observed Patterns

`https://*.com.ng/*[brand-name].com/home/`

`https://*.[brand-name].servicenow.*/*access`

`https://[brand-name].com@*.*/portal/`

`https://[brand-name].com@*.*/workspace`

`https://*/home` `https://*/workspace/home`

KEY FINDINGS

Key Takeaways

Identity-Centric Attacks

Identity misuse serves as the primary attack vector, bypassing traditional perimeter defenses

Cloud-Native Evasion

Attackers abuse cloud services and SaaS environments to move laterally and avoid traditional detection

Gift Card Monetization

Easy access to gift cards enables rapid, low-trace cash-outs through commonly permitted retail workflows

Behavioral Detection Required

Detecting these attacks requires monitoring unusual user behaviors, not just static indicators

Jingle Thief Campaign

Unit 42 Blog Post Analysis

TROOPERS26

Thank You

Questions?

Stav Setty

ssetty@paloaltonetworks.com