unit42.paloaltonetworks.com /cloud-based-gift-card-fraud-campaign/

Jingle Thief: Inside a Cloud-Based Gift Card Fraud Campaign

Stav Setty, Shachar Roitman ⋮ ⋮ 10/22/2025

Executive Summary

We investigated a campaign waged by financially motivated threat actors operating out of Morocco. We refer to this campaign as Jingle Thief, due to the attackers' modus operandi of conducting gift card fraud during festive seasons. Jingle Thief attackers use phishing and smishing to steal credentials, to compromise organizations that issue gift cards. Their operations primarily target global enterprises in the retail and consumer services sectors. Once they gain access to an organization, they pursue the type and level of access needed to issue unauthorized gift cards.

The activity related to this campaign is tracked by Unit 42 as cluster CL-CRI-1032. The threat actors behind the activity target organizations that primarily rely on cloud-based services and infrastructure. They then exploit Microsoft 365 capabilities to conduct reconnaissance, maintain long-term persistence and execute large-scale gift card fraud. We assess with moderate confidence that the activity cluster we track as CL-CRI-1032 overlaps with the activity of threat actors publicly tracked as Atlas Lion and STORM-0539 [PDF].

What makes the threat actor behind this activity particularly dangerous is the ability to maintain a foothold inside organizations for extended periods — sometimes over a year. During this time, they gain deep familiarity with the environment, including how to access critical infrastructure — making detection and remediation especially challenging. In April and May 2025, the threat actor behind the Jingle Thief campaign launched a wave of coordinated attacks across multiple global enterprises.

This article presents an end-to-end analysis of the Jingle Thief campaign lifecycle, based on real-world incident telemetry and detections. We provide a clear view of the methods involved in this activity, and practical guidance for mitigating identity-based threats — attacks that target user accounts and credentials — in cloud environments. As identity increasingly replaces the traditional perimeter, understanding campaigns like Jingle Thief is essential to securing modern enterprise infrastructure.

This activity was identified through behavioral anomalies detected by Cortex User Entity Behavior Analytics (UEBA) and Identity Threat Detection and Response (ITDR). Customers are better protected from this activity with the new Cortex Advanced Email Security module.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **Phishing**, Smishing

Who Is Behind the Jingle Thief Campaign?

We assess with moderate confidence that the Jingle Thief campaign was created by financially motivated Morocco-based attackers who have been active since 2021. Their operations primarily target global enterprises in the retail

and consumer services sectors. Although not affiliated with a nation-state, the activity we track as CL-CRI-1032 includes advanced tactics, persistence and operational focus.

Unlike threat actors who rely on commodity malware or endpoint exploitation, the attackers behind CL-CRI-1032 operate almost exclusively in cloud environments once they obtain credentials through phishing. They exploit cloud-based infrastructure to impersonate legitimate users, gain unauthorized access to sensitive data and carry out gift card fraud at scale.

Anatomy of the Jingle Thief Campaign

In a campaign that we observed, threat actors maintained access for approximately 10 months and compromised over 60 user accounts within a single global enterprise. The activity involved the use of Microsoft 365 services, including SharePoint, OneDrive, Exchange and Entra ID. This demonstrated a high degree of adaptability and operational patience. Detecting this approach requires close observation of adversaries' actions over an extended period. The threat actors behind the Jingle Thief campaign often align their activity with holiday periods, increasing operations during times of reduced staffing and heightened gift card spending.

Having gained initial access, the threat actors conducted reconnaissance to map the environment, moved laterally to access more sensitive areas, and identified opportunities to execute large-scale financial fraud. Figure 1 illustrates the end-to-end attack lifecycle across Microsoft 365, highlighting how the threat actors progressed from phishing-based entry to persistent access through device registration.

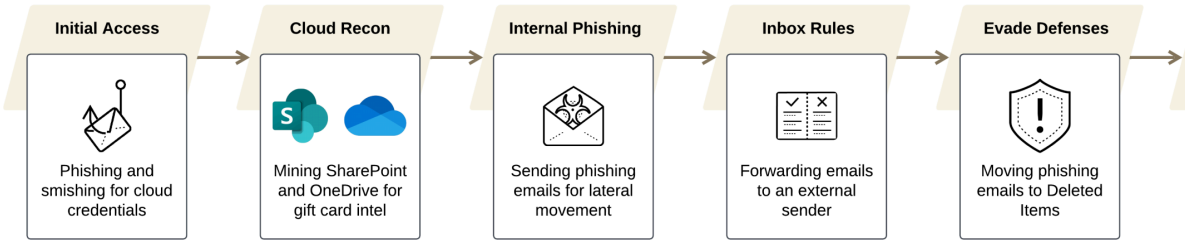

Figure 1. Jingle Thief phishing attack chain across Microsoft 365.

The final attack step of device registration creates a foothold that the threat actors exploit to issue gift cards, which they then leverage for monetary gain.

Why Gift Cards? The Prey of Choice

Gift cards are highly attractive to financially motivated actors due to their ease of redemption and rapid monetization. Threat actors resell gift cards on gray-market forums at discounted rates, enabling near-instant cash flow.

Additional factors that make gift cards attractive include:

- Minimal personal information required for redemption
- Difficult to trace, making fraud harder to investigate or recover
- Accepted widely, often indistinguishable from legitimate use
- Useful for low-risk money laundering, especially across jurisdictions
- Frequently issued through systems with weak access controls, broad internal permissions, and limited monitoring or logging

Retail environments are particularly vulnerable to this type of attack, as gift card systems are often accessible to a wide range of internal users, such as store employees. These systems may support multiple vendors or programs, making access pathways broader and more difficult to control.

Gift card fraud combines stealth, speed and scalability, especially when paired with access to cloud environments where issuance workflows reside. To exploit these systems, the threat actors need access to internal documentation and communications. They can secure this by stealing credentials and maintaining a quiet, persistent presence within Microsoft 365 environments of targeted organizations that provide gift card services.

In the campaign we observed, the attackers made repeated access attempts against multiple gift-card issuance applications. They tried to issue high-value cards across different programs in order to monetize them, and possibly to use the cards as collateral in money-laundering schemes — effectively turning digital theft into untraceable cash or

short-term loans. These operations were staged in a way that minimizes logging and forensic traces, reducing the chance of rapid detection.

Highly Targeted and Tailored Attacks

The threat actors behind the Jingle Thief campaign invest heavily in reconnaissance before launching attacks. They gather intelligence on each target, including branding, login portals, email templates and domain naming conventions. This allows them to craft highly convincing phishing content that appears authentic to both users and security tools.

Phishing URLs often include the organization's name, a trusted third-party tool or software, and landing pages that closely mimic legitimate login screens. This highly customized social engineering approach increases the likelihood of compromise and highlights the actors' use of sophisticated techniques.

Figure 2 shows a credential phishing page crafted by the threat actors to impersonate a legitimate Microsoft 365 login portal, tailored to the victim organization's branding.

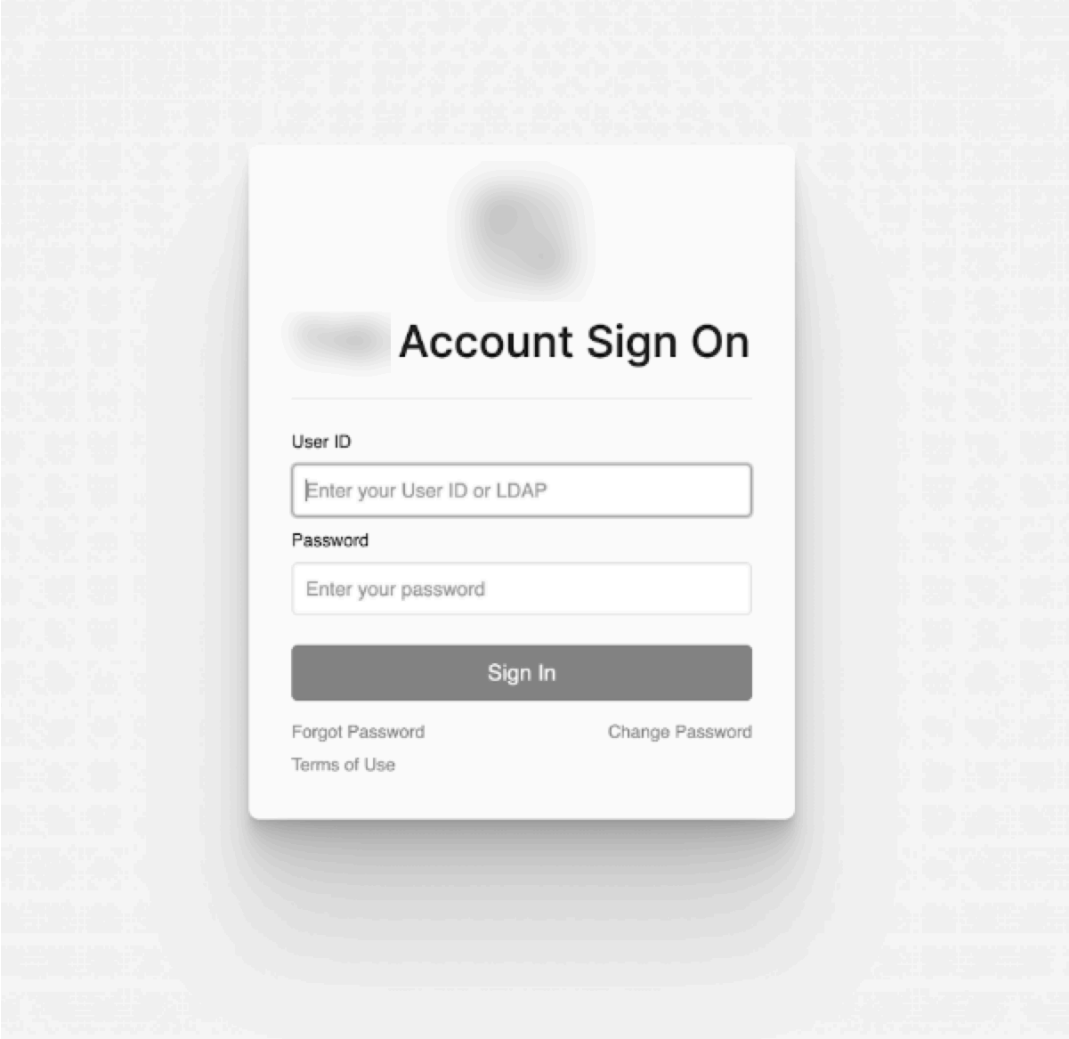

Figure 2. Fake Microsoft 365 login page tailored to the target organization.

Initial Access: Phishing and Smishing for Cloud Credentials

The threat actors behind the Jingle Thief campaign typically begin their operations with tailored phishing or SMS-based smishing attacks. These messages lure victims to counterfeit Microsoft 365 login portals that mimic legitimate sign-in pages. Some lures impersonate nonprofits or non-governmental organizations (NGOs), likely to give the appearance of credibility and increase victim engagement.

Notably, many messages are delivered using self-hosted PHP mailer scripts, often sent from compromised or hijacked WordPress servers, which obscure the attackers' origin and improve delivery.

The threat actors also employ deceptive URL formatting, such as:
https://organization[.]com@malicious.cl[/]workspace

While the URL above appears to point to the legitimate organization's domain (organization[.]com), browsers interpret everything before the @ as user credentials, and actually navigate to the domain after it (malicious.cl). This tactic helps disguise the true destination of the link and increases the likelihood of victims clicking.

After harvesting credentials in the campaign that we observed, the attackers authenticated to Microsoft 365 directly and began navigating the environment, with no malware required. Figure 3 shows a smishing attempt used to harvest credentials, captured from a malicious PHP email send log from the attackers' infrastructure. The message originated from a Moroccan IP address, and was sent to a Verizon SMS gateway (vtext.com).

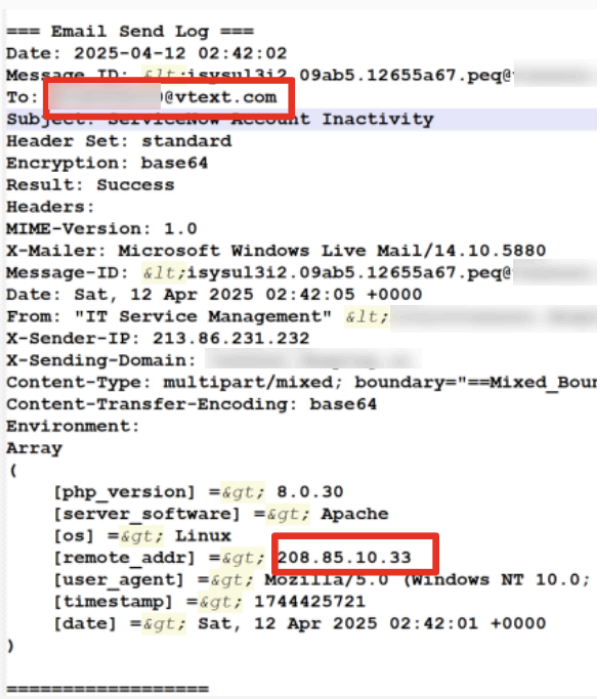

Figure 3. Credential phishing via smishing, logged from attackers' infrastructure.

Cloud Reconnaissance: Mining SharePoint and OneDrive for Gift Card Intel

After initial access, the attackers behind Jingle Thief perform extensive reconnaissance within the Microsoft 365 environment, particularly focusing on SharePoint and OneDrive. These services frequently contain internal documentation related to business operations, financial processes and IT workflows.

The threat actors search for:

- Gift card issuance workflows
- Ticketing system exports or instructions
- VPN configuration and access guides
- Spreadsheets or internal tools used to issue or track gift cards
- Organizational virtual machines, Citrix environments

Figure 4 shows SharePoint files accessed by the threat actors after account compromise, revealing their focus on internal documentation tied to gift card workflows and remote access infrastructure.

Figure 4. Internal SharePoint files accessed by Jingle Thief post-compromise.

Rather than escalating privileges, the threat actors build situational awareness by accessing readily available data on compromised users. This discreet approach helps evade detection while laying the groundwork for future fraud.

Internal Phishing for Lateral Moves

Instead of deploying malware or post-exploitation frameworks, Jingle Thief relies on internal phishing to expand their foothold within target environments. In an attempted attack against one of our customers, after compromising a user's Microsoft 365 account, the attackers sent phishing emails from the legitimate account to personnel inside the same organization. These messages mimicked IT service notifications or ticketing updates, often leveraging information gathered from internal documentation or previous communications to appear legitimate.

Common lures:

- Fake ServiceNow alerts: *"INCIDENT REQ07672026 Has been completed"*
- IT access notifications: *"ServiceNow Account Inactivity Notice"*
- Generic approval prompts: *"Incident pending your review"*

These emails link to fake login portals branded with the organization's identity, leveraging internal trust to evade suspicion and spread laterally.

Figure 5 shows an internal phishing email sent from a compromised account, spoofing a ServiceNow inactivity notice to trick users into entering credentials.

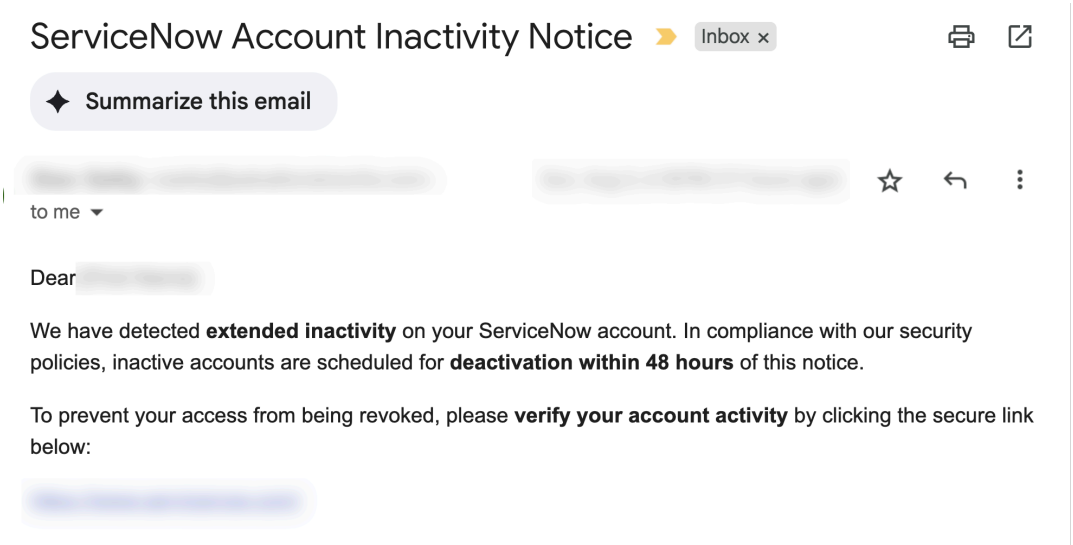

Figure 5. Internal phishing email mimicking a ServiceNow notification.

Ruling the Inbox for Silent Email Exfiltration

To passively monitor internal communications, the attackers responsible for the Jingle Thief campaign often create inbox rules to automatically forward emails to attacker-controlled addresses.

They monitor:

- Gift card approvals
- Financial workflows
- IT ticketing or account changes

This approach reduces the need for active attacker interaction and helps maintain stealth. Figure 6 shows an alert flagging the creation of a malicious inbox forwarding rule, which is one of the stealth tactics employed by these threat actors to monitor internal communications.

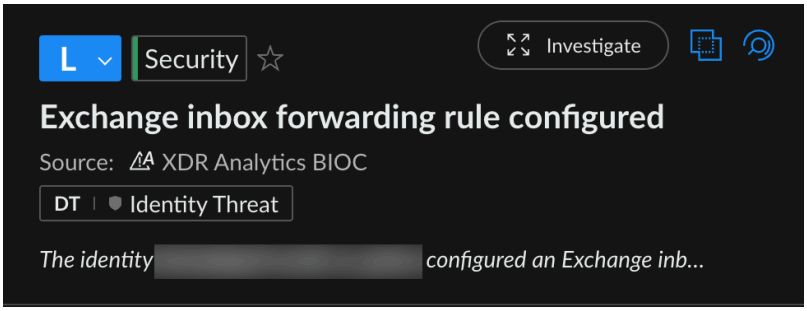

Figure 6. Cortex XDR alert showing automatic email forwarding rule set by threat actors.

Stealthy Email Activity: Hiding in Plain Sight

To cover their tracks, the attackers actively manage mailbox folders:

- Moving sent phishing emails immediately from Sent Items to Deleted Items
- Moving replies from users from Inbox to Deleted Items

This ensures that victims won't see the phishing messages or responses, delaying discovery by both victims and defenders.

The Exchange audit logs in Figure 7 show the attackers moving phishing email replies from the Inbox folder to the Deleted Items folder.

operation_name_orig	email_subject	folder	de
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\D
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\D
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\D
MoveToDeletedItems	Automatic reply: INCIDENT REQ07672026 Has been completed.	\Inbox	\D

Figure 7. Items moved from Inbox to Deleted Items.

Dominating Rogue Devices for Persistence

Most of the intrusions we observed in the Jingle Thief campaign relied on stolen credentials or session tokens for temporary access. However, the actors also demonstrated techniques for establishing longer-term persistence within compromised environments.

In some intrusions, the threat actors took control of identity infrastructure by misusing legitimate user self-service and device enrollment mechanisms in Microsoft Entra ID. These tactics allowed them to maintain access even after passwords were reset or sessions were revoked.

Tactics include:

- Registering rogue authenticator apps to bypass MFA
- Resetting passwords via self-service flows
- Enrolling attacker-controlled devices in Entra ID

Figure 8 shows the user interface for registering a device in Microsoft Entra ID using the Authenticator app. The attackers misused this legitimate process to silently enroll rogue devices and maintain MFA-resistant access.

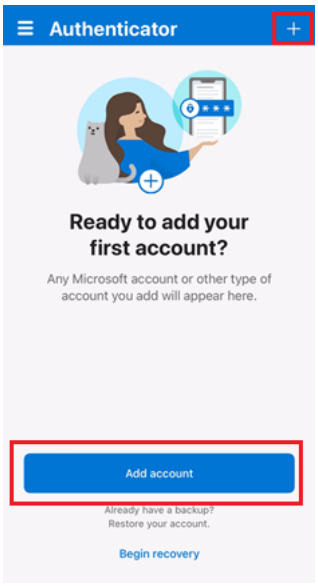

Figure 8. Device registration flow in Microsoft Entra ID.

The ultimate goal of these varied tactics – phishing, inbox control, mail exfiltration and rogue device registration – is to obtain and monetize gift cards at scale.

Tracing Jingle Thief's Moroccan Roots

The campaign activities that we observed almost exclusively originated from IP addresses geolocated in Morocco. Across incidents, Microsoft 365 logs showed recurring device fingerprints and login behaviors associated with these IP addresses. Unlike many actors who hide behind VPNs, these threat actors often made no attempt to obscure their origin, and only sometimes used Mysterium VPN when accessing compromised accounts.

Autonomous System Number (ASN) metadata from the connections also consistently matched Moroccan telecommunications providers, including:

- MT-MPLS
- ASMedi
- MAROCCONNECT

In addition to IP and ASN infrastructure, Jingle Thief reuses distinctive domain and URL structures across campaigns. These recurring patterns in domain naming and infrastructure further support attribution to a Morocco-based threat group.

Conclusion

The Jingle Thief campaign demonstrates a clear focus on major retailers' gift-card issuance systems. The attackers targeted multiple issuance applications to generate high-value cards, likely for resale on gray markets, or as fungible assets in money-laundering chains. Gift-card systems are often under-monitored and widely accessible internally, making them an attractive extension to identity-based attacks: By compromising the right accounts, threat actors can issue and steal gift cards, while leaving almost no trace of their malicious operations.

The cluster of activity behind the Jingle Thief campaign overlaps with the activity of threat actors publicly tracked as Atlas Lion. This cluster — tracked by Unit 42 as CL-CRI-1032 — favors identity misuse over malware, and leverages trusted cloud services rather than endpoint compromise. Their campaigns highlight how attackers can operate entirely within cloud environments, abusing legitimate features for phishing, persistence and fraud.

By understanding the tactics used in the Jingle Thief campaign, defenders can better prioritize identity-based monitoring and adapt to the industry's shift toward treating identity as the new security perimeter. Understanding user behavior, login patterns and identity misuse are increasingly essential for early detection and response.

Palo Alto Networks customers are better protected from this activity with the new Cortex Advanced Email Security module, as well as Cortex UEBA and ITDR.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 00080005045107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Moroccan Infrastructure (Attribution Signal)

- 105.156.109[.]227
- 105.156.234[.]139
- 105.157.86[.]136
- 105.158.226[.]49
- 105.158.237[.]165
- 160.176.128[.]242
- 160.178.201[.]89
- 160.179.102[.]157
- 196.64.165[.]160
- 196.65.139[.]51
- 196.65.146[.]114
- 196.65.172[.]48
- 196.65.237[.]97
- 196.74.125[.]243
- 196.74.183[.]81
- 196.77.47[.]232
- 196.89.141[.]80
- 41.141.201[.]19
- 41.250.180[.]114
- 41.250.190[.]104

Associated ASN Organizations (Geolocated to Morocco)

- MT-MPLS
- ASMedi
- MAROCCONNECT

U.S. Infrastructure (Potential Proxy or Compromised Hosts)

- 70.187.192[.]236
- 72.49.91[.]23

Phishing URL Patterns

- hxxps://*.com.ng/*[brand-name].com/home/
- hxxps://*.[brand-name].servicenow.*/*access
- hxxps://[brand-name].com@*.*/portal/
- hxxps://[brand-name].com@*.*/workspace
- hxxps://*/home
- hxxps://*/workspace/home

Cortex XDR/XSIAM Alerts on Jingle Thief Activity

Table 1 shows Cortex alerts for this activity, using Identity Analytics including behavioral indicators of compromise (BIOC) and the ITDR module.

Alert Name	Alert Source	MITRE ATT&CK Technique
Exchange inbox forwarding rule configured	XDR Analytics BIOC, Identity Threat Module (ITDR)	Hide Artifacts: Email Hiding Rules (T1564.008)

User moved Exchange sent messages to deleted items	XDR Analytics, Identity Threat Module (ITDR)	Indicator Removal: Clear Mailbox Data (T1070.008)
First connection from a country in organization	XDR Analytics BIOC, Identity Analytics	Compromise Accounts (T1586)
First SSO access from ASN in organization	XDR Analytics BIOC, Identity Analytics	Valid Accounts: Domain Accounts (T1078.002)
Impossible Traveler - SSO	XDR Analytics, Identity Analytics	Compromise Accounts (T1586)
A user connected from a new country	XDR Analytics BIOC, Identity Analytics	Compromise Accounts (T1586)
First SSO access from ASN for user	XDR Analytics BIOC, Identity Analytics	Valid Accounts: Domain Accounts (T1078.002)
A user connected to a VPN from a new country	XDR Analytics BIOC, Identity Analytics	Compromise Accounts (T1586)
VPN access with an abnormal operating system	XDR Analytics BIOC, Identity Analytics	Valid Accounts: Domain Accounts (T1078.002)
First VPN access from ASN in organization	XDR Analytics BIOC, Identity Analytics	Valid Accounts: Domain Accounts (T1078.002)
First SSO Resource Access in the Organization	XDR Analytics BIOC, Identity Analytics	Valid Accounts: Domain Accounts (T1078.002)
Suspicious SSO access from ASN	XDR Analytics BIOC, Identity Analytics	Valid Accounts: Domain Accounts (T1078.002)
A possible risky login to Azure	XDR Analytics BIOC, Identity Analytics	Compromise Accounts (T1586)
User attempted to connect from a suspicious country	XDR Analytics BIOC, Identity Analytics	Compromise Accounts (T1586)
SSO with new operating system	XDR Analytics BIOC, Identity Analytics	Valid Accounts: Domain Accounts (T1078.002)
Massive file downloads from SaaS service	XDR Analytics, Identity Threat Module (ITDR)	Data from Cloud Storage (T1530)

Table 1. Cortex XDR/XSIAM alerts on Jingle Thief campaign activity.