Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

The Gift Card Grinch Uncovered in the Jingle Thief Campaign

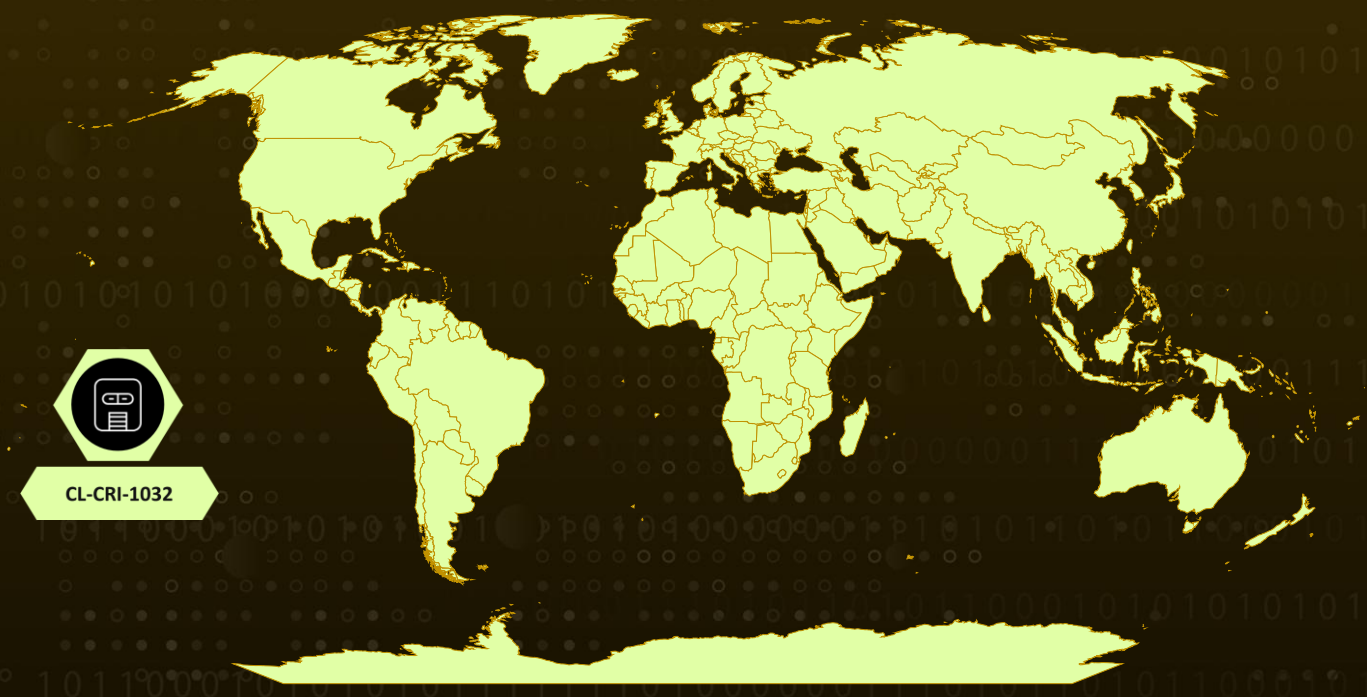
Date of Publication	Admiralty Code	TA Number
October 29, 2025	A1	TA2025329

Summary

Active Since: 2021
Campaign: Jingle Thief
Threat Actor: CL-CRI-1032
Targeted Region: Worldwide
Targeted Industries: Retail, Consumer Services

Attack: The Jingle Thief campaign, led by the Morocco-based threat group CL-CRI-1032, exploits Microsoft 365 cloud environments to execute large-scale gift card fraud through sophisticated phishing and smishing attacks. Active since 2021 and overlapping with Atlas Lion and STORM-0539, the group maintains long-term access within targeted retail and consumer service organizations, often remaining undetected for over a year.

Attack Regions



Attack Details

#1 The new campaign, known as Jingle Thief, derives its name from the attackers' method of executing large-scale gift card fraud. These cybercriminals use phishing and smishing techniques to steal credentials and compromise organizations that issue gift cards. Their operations primarily target businesses in the retail and consumer services sectors.

#2 The financially motivated threat group, operating out of Morocco and tracked as CL-CRI-1032, has been active since 2021. Their activity overlaps with other threat actors publicly identified as Atlas Lion and STORM-0539. CL-CRI-1032 focuses on organizations that rely heavily on cloud-based infrastructure, exploiting Microsoft 365 environments to conduct reconnaissance, establish persistence, and carry out large-scale gift card fraud.

#3 A major concern is their ability to maintain long-term access to compromised networks, often for more than a year. After obtaining credentials through phishing, the attackers operate almost exclusively in cloud environments, impersonating legitimate users to gain unauthorized access to sensitive data and perform fraudulent transactions at scale.

#4 The group performs in-depth reconnaissance on each target, collecting details such as branding, login portals, email templates, and domain naming conventions. This enables crafting of persuasive phishing emails and fake login pages that appear authentic to both users and security systems.

#5 To evade detection, the attackers carefully manage mailbox folders, deleting sent phishing messages and moving user replies from inboxes to deleted folders. In some cases, they register rogue authenticator applications to bypass multi-factor authentication (MFA) and even enroll their own devices in Entra ID. This ensures continued access even after password resets or session token revocations.

#6 The primary goal of the Jingle Thief campaign is monetary profit. Stolen gift cards are converted into cash, typically resold on gray markets. Gift cards remain a preferred target due to their ease of redemption, minimal verification requirements, and difficulty in tracing. With the holiday season approaching, organizations should prepare for an increase in phishing campaigns and gift card fraud attempts associated with the Jingle Thief operation.

Recommendations

Enhance Email Security and User Awareness: Implement advanced phishing filters to detect spear-phishing attempts and malicious attachments. Encourage verification of requests that appear to come from authoritative sources. Implement advanced phishing detection and anti-spam filters across all corporate email systems. Enable URL scanning and attachment sandboxing to block malicious links and payloads before they reach users.

Segment Critical Networks and Limit Access: Implement strict network segmentation to isolate high-value assets. Apply least-privilege access controls and regularly review permissions to minimize potential lateral movement.

Monitor for Anomalous Cloud Activity: Continuously monitor Microsoft 365 and other cloud environments for suspicious behavior such as unusual login patterns, new device enrollments, and privilege escalations. Use behavioral analytics to identify deviations from normal user activity.

Harden Entra ID and Cloud Configurations: Regularly review Entra ID (Azure AD) configurations to detect unauthorized device enrollments or app registrations. Implement conditional access policies to restrict access from unapproved devices or regions.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0040 Impact	**TA0043** Reconnaissance	**TA0042** Resource Development	**T1589** Gather Victim Identity Information
T1564 Hide Artifacts	**T1564.008** Email Hiding Rules	**T1070** Indicator Removal	**T1070.008** Clear Mailbox Data

T1586 Compromise Accounts	**T1078** Valid Accounts	**T1078.002** Domain Accounts	**T1530** Data from Cloud Storage
T1566.002 Spearphishing Link	**T1566** Phishing	**T1078.004** Cloud Accounts	**T1057** Process Discovery
T1087.003 Email Account	**T1087** Account Discovery	**T1556.006** Multi-Factor Authentication	**T1556** Modify Authentication Process
T1098 Account Manipulation	**T1036** Masquerading	**T1496** Resource Hijacking	**T1591** Gather Victim Org Information
T1598 Phishing for Information	**T1588** Obtain Capabilities	**T1189** Drive-by Compromise	**T1199** Trusted Relationship
T1531 Account Access Removal			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	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,

TYPE	VALUE
IPv4	196[.]89[.]141[.]80, 41[.]141[.]201[.]19, 41[.]250[.]180[.]114, 41[.]250[.]190[.]104, 70[.]187[.]192[.]236, 72[.]49[.]91[.]23
URL*	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, hxxps[:]//organization[.]com[@]malicious[.]cl[/]workspace

References

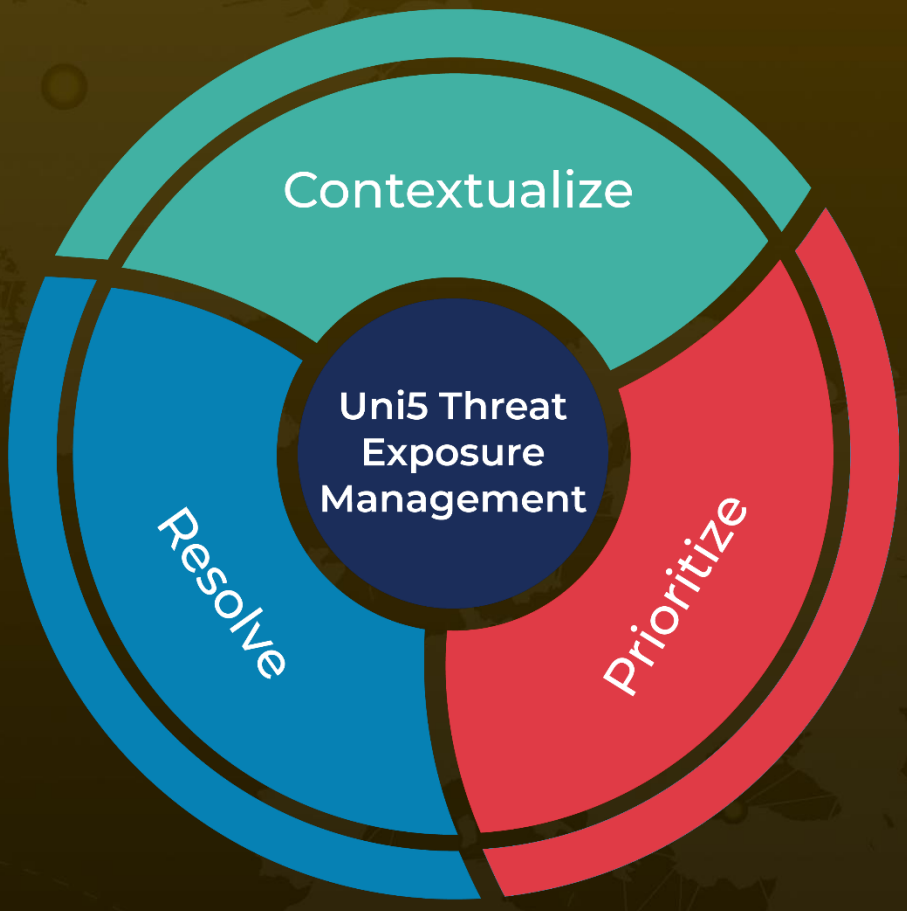
https://unit42.paloaltonetworks.com/cloud-based-gift-card-fraud-campaign/

**These are phishing URL patterns used in the Jingle Thief campaign.*

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 29, 2025 • 7:30 AM

More at www.hivepro.com