Microsoft

Into the Lion's Den

Inside the Growing
Risk of Gift Card Fraud

30%

In May 2024, Microsoft observed a 30%
increase in activity from Storm-0539, a threat
actor focused on gift-card-related cybercrime,
compared to the preceding two months.

May 2024

Cyber Signals

A Microsoft Threat Intelligence Report

Introduction

In an age where digital transactions and online shopping have become integral parts of our daily lives, the threat of cybercrime looms. Among these threats, gift and payment card fraud, which include both gift cards from credit card companies or retailers, is pervasive and evolving. Criminals using increasingly sophisticated methods to compromise gift card portals before turning them into near-untraceable cash.

This edition of Cyber Signals delves into the tactics, techniques, and procedures of a cybercrime threat actor Microsoft calls Storm-0539, also known as Atlas Lion, and its activities in the realm of gift card theft, the intricacies of its methods, and the implications for individuals, businesses, and the cybersecurity landscape.

Storm-0539 has stayed relevant throughout the years, adapting to the ever-changing criminal landscape. Through a labyrinthine network of encrypted channels and underground forums, they orchestrate illicit ventures exploiting technological loopholes and deploying clever social engineering campaigns to scale their operation.

Although many cybercrime threat actors take the path of least resistance to quick profits and focus on scale, Storm-0539 shows a quiet, productive focus on compromising gift card systems and transactions. This adversary relentlessly targets gift card issuers by adapting techniques to keep pace with changes across retail, payment, and other related industries.

We are all defenders.

Security Snapshot

Historically, Storm-0539 increases its attack activity ahead of major holiday seasons. Between March and May 2024, ahead of the summer holiday season, Microsoft observed a 30% increase in intrusion activity from Storm-0539. Between September and December 2023, we observed a 60% increase in attack activity, coinciding with fall and winter holidays.

30%

Increase in Storm-0539 intrusion activity, between March and May 2024

60%

Increase in Storm-0539 intrusion activity, between September and December 2024

Threat briefing

## Attackers Refine Gift and Payment Card Heists

Storm-0539 operates out of Morocco and is involved in financial crimes such as gift card fraud. Their techniques include phishing, smishing, registering their own devices to victim environments to gain persistent access, and leveraging access to target third-party organizations. They register devices so that multifactor authentication (MFA) prompts associated with a compromised victim account go to the attacker's device. Registering a device lets them wholly compromise an identity and persist in the cloud environment.

Active since late 2021, this cybercrime group represents an evolution of threat actors focused on attacking payment card accounts and systems. Attackers commonly compromised payment card data with point-of-sale (POS) malware in the past. Yet, as industries hardened POS defenses, Storm-0539 adapted their attack techniques to compromise cloud and identity services in the criminal targeting of gift card portals linked to large retailers, luxury brands, and well-known fast-food restaurants.

Historically, payment and gift card fraud is associated with sophisticated malware and phishing campaigns. However, this group leverages their deep knowledge of the cloud to conduct reconnaissance on an organization's gift card issuance processes, gift card portals, and employees with access to gift cards.

Typically, the attack chain includes the following actions:

- Using employee directories and schedules, contact lists, and email inboxes, Storm-0539 targets employees' personal and work mobile phones with smishing texts.

- Once an employee account at a targeted organization is infiltrated, the attackers move laterally through the network, trying to identify the gift card business process, pivoting toward compromised accounts linked to this specific portfolio.

- They also gather information on virtual machines, VPN connections, SharePoint and OneDrive resources, as well as Salesforce, Citrix, and other remote environments.

- After gaining access, the group creates new gift cards using compromised employee accounts.

- They then redeem the value associated with those cards, sell the gift cards to other threat actors on black markets, or use money mules to cash out the gift cards.
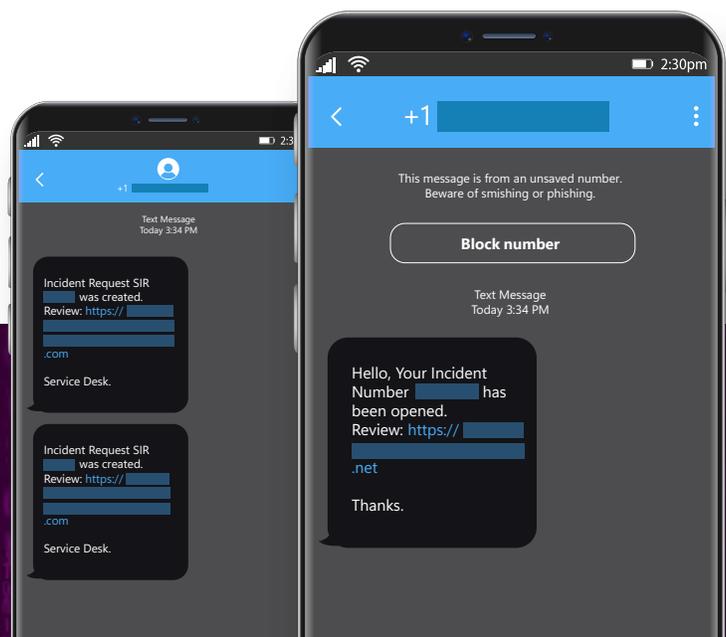
Storm-0539 smishing messages impersonating a targeted employee's company help desk.

Storm-0539's reconnaissance and ability to leverage cloud environments are similar to what Microsoft observes from nation-state-sponsored threat actors, showing how techniques popularized by espionage and geopolitical-focused adversaries are now influencing financially motivated criminals.
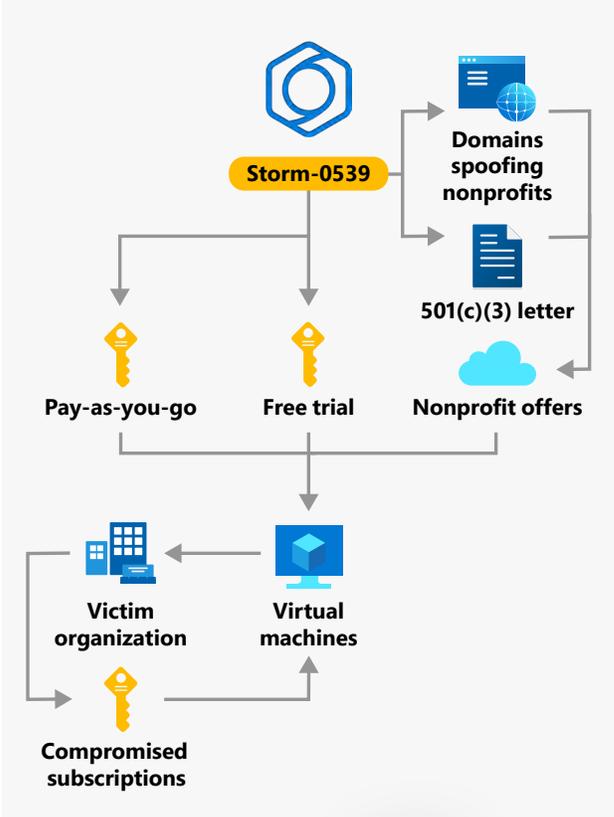
For example, Storm-0539 leverages their knowledge of cloud-based software, identity systems, and access privileges to target where gift cards are created, instead of focusing solely on the end-user. This activity is a trend that we're seeing among non-nation state groups like Octo Tempest and Storm-0539, which are tactically well-versed in cloud resources much like advanced state-sponsored actors.

To camouflage themselves and remain undetected, Storm-0539 presents themselves as legitimate organizations to cloud providers, in order to gain temporary application, storage, and other initial free resources for their attack activity.

As part of this effort, they create websites that impersonate charities, animal shelters, and other nonprofits in the United States typically with typosquatting, a deceptive practice where individuals register a common misspelling of an organization's domain as their own to trick users into visiting fraudulent sites and entering personal information or professional credentials.

To further expand their fraud toolkit, Microsoft has observed Storm-0539 downloading legitimate copies of 501(c)(3) letters issued by the Internal Revenue Service (IRS) from nonprofit organizations' public websites. Armed with a copy of a legitimate 501(c)(3) letter and a matching domain impersonating the nonprofit for which the letter was issued, they approach major cloud providers for sponsored or discounted technology services often given to nonprofits.

Storm-0539 operates from free trials, pay-as-you-go subscriptions, and compromised cloud resources. We also observed Storm-0539 impersonating legitimate nonprofits to obtain nonprofit sponsorship from several cloud providers.

Storm-0539

Domains spoofing nonprofits

501(c)(3) letter

Pay-as-you-go

Free trial

Nonprofit offers

Victim organization

Virtual machines

Compromised subscriptions

The group also creates free trials or student accounts on cloud service platforms typically providing new customers with 30 days of access. Within these accounts they create virtual machines from which to launch their targeted operations. Storm-0539's skill at compromising and creating cloud-based attack infrastructure lets them avoid common up-front costs in the cybercrime economy, such as paying for hosts and servers, as they seek to minimize costs and maximize efficiency.

Microsoft assesses that Storm-0539 carries out extensive reconnaissance into the federated identity service providers at targeted companies to convincingly mimic the user sign-in experience, including not only the appearance of the adversary-in-the-middle (AiTM) page, but also the use of registered domains that closely match legitimate services. In other instances, Storm-0539 has compromised legitimate recently registered WordPress domains to craft the AiTM landing page.

Recommendations:

Token protection and least privilege access: Use policies to protect against token replay attacks by binding the token to the legitimate user's device. Apply least privilege access principles across the entire technology stack to minimize the potential impact of an attack.

Adopt a secure gift card platform and implement fraud protection solutions: Consider switching to a system designed to authenticate payments. Merchants can also integrate fraud protection features to minimize losses.

Phishing-resistant MFA: Transition to phishing-resistant credentials that are immune to various attacks, such as FIDO2 security keys.

Require a secure password change when user risk level is high: Microsoft Entra MFA is required before the user can create a new password with password writeback to remediate their risk.

Educate employees: Merchants should train employees to recognize potential gift card scams and decline suspicious orders.

Defending against attacks

Weathering the Storm: Countermeasures Against Storm-0539

Gift cards are attractive targets for fraud because unlike credit or debit cards, there are no customer names or bank accounts attached to them. Microsoft sees an uptick in activity from Storm-0539 focused on this industry around seasonal holiday periods. Memorial Day, Labor Day, and Thanksgiving in the U.S., as well as Black Friday and winter holidays observed around the world, tend to be associated with increased activity from the group.

Typically, organizations set a limit on the cash value that can be issued to an individual gift card. For example, if that limit is $100,000, the threat actor will issue a card for $99,000 then send themselves the gift card code and monetize them. Their primary motivation is to steal gift cards and profit by selling them online at a discounted rate. We've seen some examples where the threat actor has stolen up to $100,000 a day at certain companies.

To defend against such attacks and prevent this group from gaining unauthorized access to gift card departments, companies issuing gift cards should treat their gift card portals as high-value targets. They should be closely monitored and continuously audited for any anomalous activity.

For any organization creating or issuing gift cards, implementing checks and balances to prevent quick access to gift card portals and other high-value targets, even if an account is compromised, can help. Continuously monitor logs to identify suspicious logins and other common initial access vectors that rely on cloud identity compromises and implement conditional access policies that limit sign-ons and flag risky sign-ins.

Organizations should also consider complementing MFA with conditional access policies where authentication requests are evaluated using additional identity-driven signals like IP address location information or device status, among others.

Another tactic that could help curb these attacks is a customer verification process for purchasing domains. Regulations and vendor policies may not consistently prevent malicious typosquatting around the world, meaning these deceptive websites can remain popular for scaling cyberattacks. Verification processes for creating domains could help curb more sites created solely for the purpose of deceiving victims.

In addition to misleading domain names, Microsoft has also observed Storm-0539 using legitimate internal company mailing lists to disseminate phishing messages once they gain a foothold in a company and understand its distribution lists and other norms of business.
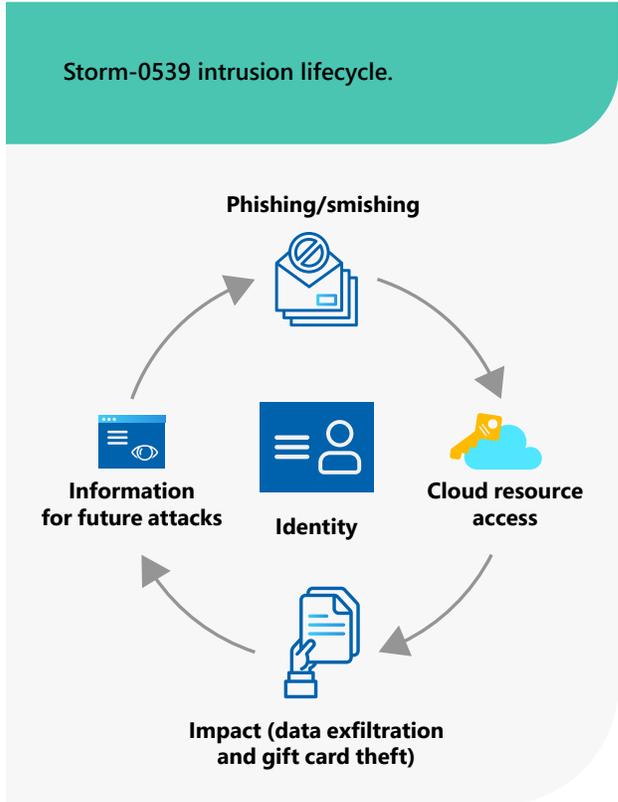
Not only does phishing through a valid distribution list add another layer of authenticity to malicious content, it also helps hone the targeting of content to more individuals with access to credentials, relationships, and information Storm-0539 relies on to gain persistence and reach.

When users click links contained in the phishing emails or texts, they are redirected to an AiTM phishing page for credential theft and secondary authentication token capture. Retailers are encouraged to teach staff how smishing/phishing scams work, how to identify them, and how to report them.

It's important to highlight that unlike noisy ransomware threat actors who encrypt and steal data then harass you to pay, Storm-0539 skates around in a cloud environment quietly gathering reconnaissance and abusing the cloud and identity infrastructure to achieve their end goals.

Storm-0539 operations are persuasive due to the actor's use of legitimate compromised emails and the mimicking of legitimate platforms used by the targeted company. For some companies gift card losses are recoverable. That requires a thorough investigation to determine which gift cards the threat actor issued.

Microsoft Threat Intelligence has issued notifications to organizations affected by Storm-0539. Partly because of this information-sharing and collaboration, we have observed an increase in major retailers' ability to effectively ward of Storm-0539 activity in recent months.

Storm-0539 intrusion lifecycle.

Phishing/smishing

Cloud resource access

Impact (data exfiltration and gift card theft)

Identity

Information for future attacks

Recommendations:

Reset passwords for users associated with phishing and AiTM activity: To revoke any active sessions, reset passwords immediately. Revoke any MFA setting changes made by the attacker on compromised accounts. Require re-challenging MFA for MFA updates as the default. Also, ensure mobile devices employees use to access corporate networks are similarly protected.

Enable zero-hour auto purge (ZAP) in Microsoft Defender for Office 365: ZAP finds and takes automated actions on the emails that are a part of the phishing campaign based on identical elements of known bad messages.

Update identities, access privileges, and distribution lists to minimize attack surfaces: Attackers like Storm-0539 assume they will find users with excessive access privileges they can compromise for outsized impact. Employee and team roles can change frequently. Establishing a regular review of privileges, distribution list memberships, and other attributes can help limit the fallout of an initial intrusion and make intruders' work more difficult.

Expert Profile

Alison Ali, Waymon Ho, Emiel Haeghebaert

Microsoft Threat Intelligence

Alison Ali, Waymon Ho, and Emiel Haeghebaert came to cybersecurity through very different paths. This group of analysts tracking Storm-0539 has a background that spans international relations, federal law enforcement, security, and government.

Waymon Ho first pursued a degree in computer science with a focus in software engineering but stumbled upon an internship with the Federal Bureau of Investigation (FBI). This changed his trajectory to pursue a cybersecurity career.

"At the FBI, I investigated cybercriminals as a computer scientist and joined Microsoft in 2022 as a senior hunt analyst on the Microsoft Threat Intelligence Center (MSTIC) team, focused on tracking threat actors," Waymon explains. He is currently a senior security research manager on Microsoft's Global Hunting, Oversight, and Strategic Triage (GHOST) team.

Waymon says what's notable about Storm-0539 is their persistence and knowledge of the gift card issuing process. "They identify employees managing gift card portals and locate internal guides outlining how to issue them. They issue cards just under the security limit to ensure authorization and that they remain undetected so they can return and repeat the process," he adds.

Emiel Haeghebaert's background spans both technology and international relations. Originally from Belgium, Emiel moved to the United States in 2018 to pursue a degree in security studies at Georgetown University. He's currently a senior hunt analyst with MSTIC, where he tracks Iranian state-sponsored cyberthreats targeting Microsoft customers and consumers.

Emiel also supports Microsoft incident response engagements related to both financially motivated and state-sponsored threat actors, supporting on-site teams and customers with attribution analysis, threat actor insights, and tailored briefings. With a background in international relations and cybersecurity, Emiel thrives at the intersection of these fields. "Working in cyberthreat intelligence, it's essential to have not only an understanding of technical matters related to cybersecurity, but also a comprehension of threat actors, their motivations, their priorities, and their sponsors' strategic objectives," he says. "My background in history and geopolitics helps me gain a more complete understanding of cybercriminal groups and state-sponsored threat actors."

Alison Ali came to security in a roundabout way, with a background in linguistics from Georgetown University. She began working at Microsoft in 2022 as a senior security researcher, where she works with teams across Microsoft Security to synthesize information for customers on significant cyberthreats, including financially motivated threat actors. Alison says, "Organizations across all industries are frequently dealing with users affected by large scale attacks like phishing or password sprays—what matters is security hardening measures that stop an initial foothold from becoming a major intrusion."

> " "
> What matters is security hardening measures that stop an initial foothold from becoming a major intrusion.