Microsoft

Na cova dos leões

Por dentro do risco crescente de fraude com cartões de presente

30%

Em maio de 2024, a Microsoft observou um aumento de 30% na atividade do Storm-0539, um agente de ameaças focado em crimes cibernéticos relacionados a cartões de presente, em comparação com os dois meses anteriores.

Maio 2024

Cyber Signals

Um Relatório de Inteligência de Ameaças da Microsoft

Introdução

Em uma era em que as transações digitais e as compras on-line se tornaram parte integrante de nossas vidas, a ameaça do cibercrime fica mais evidente. Entre esses riscos, a fraude de cartões de presente e pagamento, que incluem gift cards de empresas de cartão de crédito ou dos varejistas, está difundida e evoluindo com criminosos usando métodos cada vez mais sofisticados para comprometer portais de vale presente antes de transformá-los em dinheiro quase não rastreável.

Esta edição do Cyber Signals investiga as táticas, técnicas e procedimentos de um ator cibercriminoso que a Microsoft chama de Storm-0539, conhecido como Atlas Lion, e suas atividades no âmbito do roubo de cartões de presente, os meandros de seus métodos e as implicações para indivíduos, empresas e o cenário de segurança cibernética.

O Storm-0539 manteve-se relevante ao longo dos anos, adaptando-se ao cenário de crimes digitais, que está em constante mudança. Por meio de uma rede difusa de canais criptografados e fóruns subterrâneos, eles orquestram ações ilícitas explorando brechas tecnológicas e implantando campanhas inteligentes de engenharia social para escalar sua operação.

Embora muitos agentes de ameaças de crimes cibernéticos sigam o caminho de menor resistência a lucros rápidos e se concentrem em escala, o Storm-0539 mostra um foco silencioso e produtivo em comprometer sistemas e transações de 'gift cards'. Esse adversário visa implacavelmente aos emissores de cartões de presente, adaptando técnicas para acompanhar as mudanças no varejo, pagamentos e outros setores relacionados.

Somos todos agentes de defesa.

Retrato de segurança

Historicamente, o Storm-0539 aumenta sua atividade de ataque antes das principais temporadas festivas. Entre março e maio de 2024, antes da temporada de férias nos Estados Unidos, a Microsoft observou um aumento de 30% na atividade de intrusão do Storm-0539. Entre setembro e dezembro de 2023, a Microsoft observou um aumento de 60% na atividade de ataque, coincidindo com as festas de fim ano.

30%

aumento na atividade de invasões do Storm-0539, entre março e maio de 2024.

60%

aumento na atividade de invasões do Storm-0539, entre setembro e dezembro de 2024.

Criminosos refinam roubos de presentes e cartões de pagamento

A Storm-0539 opera a partir de Marrocos e está envolvida em crimes financeiros, como fraude de cartão de presente. Suas técnicas incluem phishing, smishing, registro de seus próprios dispositivos em ambientes de vítimas para obter acesso persistente e alavancar o acesso a organizações terceiras. Eles registram dispositivos para que os prompts de autenticação multifator (MFA) associados à conta da vítima sejam direcionados para o dispositivo do invasor. Registrar um dispositivo permite que eles comprometam totalmente uma identidade e persistam no ambiente de nuvem.

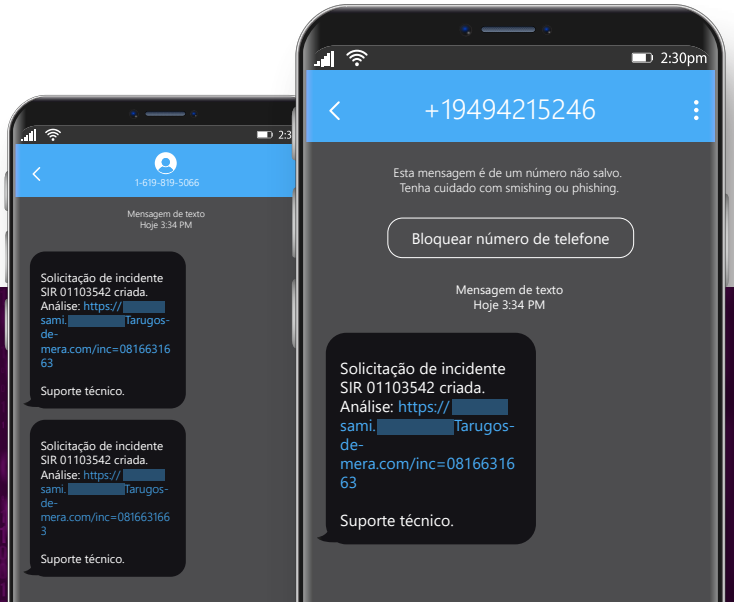
Ativo desde o final de 2021, este grupo de cibercrime representa uma evolução de agentes de ameaças focados em atacar contas e sistemas de cartões de pagamento. Os invasores geralmente comprometiam dados de cartões de pagamento com malware de ponto de venda (PDV) no passado. No entanto, à medida que as indústrias endureciam as defesas de PDV, o Storm-0539 adaptou suas técnicas de ataque para comprometer os serviços de nuvem e identidade no direcionamento criminoso de portais de cartões de presente ligados a grandes varejistas, marcas de luxo e restaurantes de fast-food conhecidos.

Historicamente, a fraude com cartão de pagamento está associada a malwares sofisticados e campanhas de phishing. No entanto, esse grupo aproveita seu profundo conhecimento da nuvem para realizar reconhecimento nos processos de emissão de cartões de presente de uma organização, portais de gift cards e funcionários com acesso a vale-presentes.

Briefing sobre ameaças

Normalmente, a cadeia de ataque inclui as seguintes ações:

- Usando diretórios e agendas de funcionários, listas de contatos e caixas de entrada de e-mail, o Storm-0539 tem como alvo os telefones celulares pessoais e de trabalho dos funcionários com mensagens de texto do tipo SMISHING.
- Uma vez que uma conta de funcionário em uma organização alvo é infiltrada, os invasores se movimentam pela rede, tentando identificar o processo de negócios do gift card, indo em direção a contas comprometidas vinculadas a esse portfólio específico. Eles também reúnem informações sobre máquinas virtuais, conexões VPN, recursos do SharePoint e do OneDrive, bem como Salesforce, Citrix e outros ambientes remotos.
- Depois de obter acesso, o grupo cria novos cartões de presente usando contas de funcionários comprometidas.
- Eles, então, resgatam o valor associado a esses cartões, vendem os gift cards para outros agentes de ameaças em mercados paralelos ou usam mulas de dinheiro para sacar os vale-presentes.



Mensagens smishing Storm-0539 representando o suporte técnico da empresa de um funcionário alvo.

O reconhecimento e a capacidade do Storm-0539 de alavancar ambientes de nuvem são semelhantes ao que a Microsoft observa de agentes de ameaças Estados-Nação, mostrando como técnicas popularizadas por espionagem e adversários com foco geopolítico agora estão influenciando criminosos com motivação financeira.

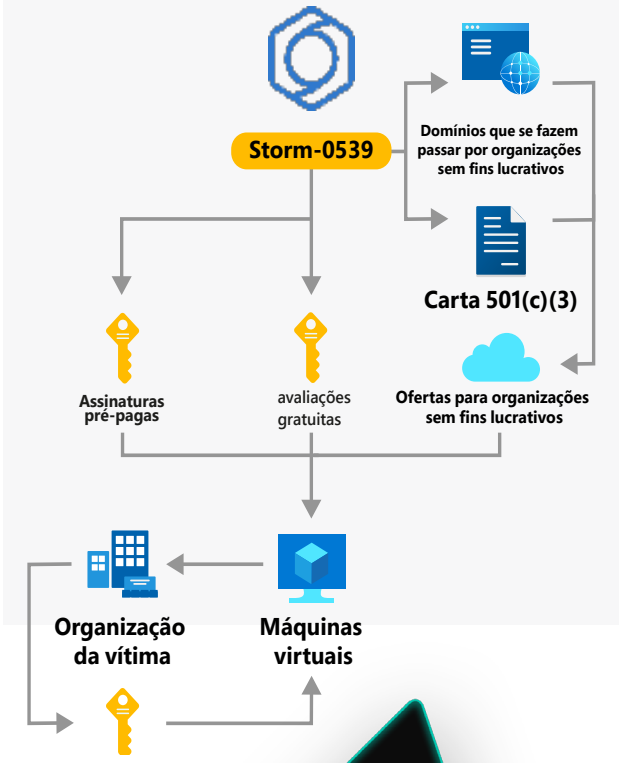
Por exemplo, o Storm-0539 aproveita conhecimento de software baseado em nuvem, sistemas de identidade e privilégios de acesso para direcionar onde os cartões de presente são criados, em vez de se concentrar apenas nos consumidores-final. Essa atividade é uma tendência que estamos vendo entre grupos de estados não nacionais, como Octo Tempest e Storm-0539, que são taticamente bem versados em recursos de nuvem ao lado de atores avançados patrocinados pelo Estado.

Para se camuflar e permanecer sem ser detectado, o Storm-0539 se apresenta como organizações legítimas para provedores de nuvem, a fim de obter aplicativos temporários, armazenamento e outros recursos gratuitos iniciais para sua atividade de ataque.

Como parte desse esforço, eles criam sites que se passam por instituições de caridade, abrigos de animais e outras organizações sem fins lucrativos nos Estados Unidos, normalmente com typosquatting, uma prática enganosa em que os indivíduos registram um erro de digitação comum do domínio de uma organização como seu para enganar os usuários a visitar sites fraudulentos e inserir informações pessoais ou credenciais profissionais.

Para expandir ainda mais seu kit de ferramentas de fraude, a Microsoft observou o Storm-0539 baixando cópias legítimas de cartas 501(c)(3) emitidas pelo Internal Revenue Service (IRS) de sites públicos de organizações sem fins lucrativos. Munidos de uma cópia de uma carta 501(c)(3) legítima e de um domínio correspondente que se passa pela organização sem fins lucrativos para a qual a carta foi emitida, eles abordam os principais provedores de nuvem para serviços de tecnologia patrocinados ou com desconto, muitas vezes dados a organizações sem fins lucrativos.

O Storm-0539 opera a partir de avaliações gratuitas, assinaturas pré-pagas e recursos de nuvem comprometidos. Também observamos o Storm-0539 se passando por organizações sem fins lucrativos legítimas para obter patrocínio de vários provedores de nuvem



O grupo também cria avaliações gratuitas ou contas de estudantes em plataformas de serviços em nuvem, normalmente fornecendo aos novos clientes 30 dias de acesso. Dentro dessas contas, eles criam máquinas virtuais a partir das quais iniciam suas operações de destino. A habilidade da Storm-0539 em comprometer e criar infraestrutura de ataque baseada em nuvem permite que eles evitem custos iniciais comuns na economia do crime cibernético, como pagar por hosts e servidores, à medida que buscam minimizar custos e maximizar a eficiência.

A Microsoft avalia que o Storm-0539 realiza um amplo reconhecimento nos provedores de serviços de identidade federados em empresas-alvo para imitar de forma convincente a experiência de entrada do usuário, incluindo não apenas a aparência da página do adversario en el medio (AiTM, em inglês), mas também o uso de domínios registrados que correspondem de perto aos serviços legítimos. Em outros casos, o Storm-0539 comprometeu domínios legítimos do WordPress recentemente registrados para criar a página de destino AiTM.

Recomendações:

Proteção de token e acesso a privilégios mínimos: use políticas para proteger contra-ataques de repetição de token, vinculando o token ao dispositivo do usuário legítimo. Aplique princípios de acesso de privilégios mínimos em toda a pilha de tecnologia para minimizar o impacto potencial de um ataque.

Adote uma plataforma segura de gift cards e implemente soluções de proteção contra fraude: considere mudar para um sistema projetado para autenticar pagamentos. Os comerciantes também podem integrar recursos de proteção contra fraude para minimizar perdas.

MFA resistente a phishing: faça a transição para credenciais resistentes a phishing que são imunes a vários ataques, como chaves de segurança FIDO2.

Exigir uma alteração de senha segura quando o nível de risco do usuário for alto: Microsoft Entra MFA é requirido antes que o usuário possa criar uma senha nova com write-back de senha para corrigir seu risco.

Educar os funcionários: os comerciantes devem treinar os funcionários para reconhecer possíveis golpes de cartões de presente e recusar pedidos suspeitos.

Defesa contra-ataques

Resistindo à tempestade: contramedidas contra o Storm-0539

Os cartões de presente são alvos atraentes para fraudes porque, ao contrário dos cartões de crédito ou débito, não há nomes de clientes ou contas bancárias anexadas a eles. A Microsoft vê um aumento na atividade do Storm-0539 focado neste setor em torno de períodos de férias sazonais. O Memorial Day, o Dia do Trabalho e o Dia de Ação de Graças nos EUA, bem como a Black Friday e os feriados de fim de ano observados em todo o mundo, tendem a estar associados ao aumento da atividade do grupo.

Normalmente, as organizações definem um limite no valor em dinheiro que pode ser emitido para um cartão-presente individual. Por exemplo, se esse limite for de US$ 100 mil, o agente da ameaça emitirá um cartão de US$ 99.000 e, em seguida, enviará a si mesmo o código do gift card e o monetizará. Sua principal motivação é roubar vale-presente e lucrar vendendo-os online a uma taxa com desconto. Vimos alguns exemplos em que o agente de ameaças roubou até US$ 100 mil por dia em certas empresas.

Para se defender de tais ataques e evitar que esse grupo obtenha acesso não autorizado aos departamentos de cartões de presente, as empresas emissoras de gift cards devem tratar seus portais de vale-presente como alvos de alto valor. Eles devem ser monitorados de perto e continuamente auditados para qualquer atividade anômala.

Para qualquer organização que crie ou emita cartões de presente, a implementação de verificações e saldos para impedir o acesso rápido a portais de gift cards e outros alvos de alto valor, mesmo que uma conta seja comprometida, pode ajudar. Monitore continuamente os logs para identificar logins suspeitos e outros vetores de acesso inicial comuns que dependem de comprometimentos de identidade na nuvem e implemente políticas de acesso condicional que limitam as entradas e sinalizam entradas arriscadas.

As organizações também devem considerar complementar a MFA com políticas de acesso condicional em que as solicitações de autenticação são avaliadas usando sinais adicionais orientados por identidade, como informações de localização de endereço IP ou status do dispositivo, entre outros.

Outra tática que pode ajudar a conter esses ataques é um processo de verificação do cliente para a compra de domínios. As regulamentações e as políticas do fornecedor podem não impedir consistentemente a exploração maliciosa de domínios com erros de digitação em todo o mundo, o que significa que esses sites enganosos podem permanecer populares para escalar ataques cibernéticos. Os processos de verificação para a criação de domínios podem ajudar a coibir mais sites criados exclusivamente com o propósito de enganar as vítimas.

Além de nomes de domínio enganosos, a Microsoft também observou o Storm-0539 usando listas de discussão internas legítimas da empresa para disseminar mensagens de phishing, uma vez que elas ganham uma posição em uma empresa e entendem suas listas de distribuição e outras normas de negócios.

O phishing por meio de uma lista de distribuição válida não apenas adiciona outra camada de autenticidade ao conteúdo mal-intencionado, mas também ajuda a aprimorar o direcionamento de conteúdo para mais indivíduos com acesso a credenciais, relacionamentos e informações nas quais o Storm-0539 depende para ganhar persistência e alcance.

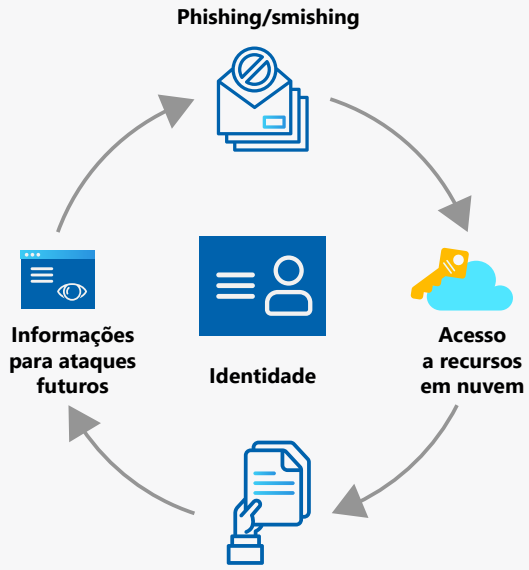
Quando os usuários clicam em links contidos nos e-mails ou textos de phishing, eles são redirecionados para uma página de phishing AiTM para roubo de credenciais e captura de token de autenticação secundária. Os varejistas são incentivados a ensinar aos funcionários como os golpes de phishing funcionam, como identificá-los e como denunciá-los.

É importante destacar que, ao contrário dos barulhentos agentes de ameaças de ransomware que criptografam e roubam dados e depois assediam você para pagar, o Storm-0539 patina em um ambiente de nuvem silenciosamente coletando reconhecimento e abusando da infraestrutura de nuvem e identidade para atingir seus objetivos finais.

As operações do Storm-0539 são persuasivas devido ao uso de e-mails legítimos comprometidos pelo ator e à imitação de plataformas legítimas usadas pela empresa visada. Para algumas empresas, as perdas com cartões de presente são recuperáveis. Isso requer uma investigação completa para determinar quais cartões de presente o agente da ameaça emitiu.

O Microsoft Threat Intelligence emitiu notificações para organizações afetadas pelo Storm-0539. Em parte, devido a esse compartilhamento de informações e colaboração, observamos um aumento na capacidade dos principais varejistas de efetivamente evitar a atividade do Storm-0539 nos últimos meses.

Ciclo de vida da intrusão Storm-0539.



Recomendações:

Redefinir senhas para usuários associados a phishing e atividades AiTM: para revogar quaisquer sessões ativas, redefina as senhas imediatamente. Revogar quaisquer alterações de configuração de MFA feitas pelo invasor em contas comprometidas. Exija um novo desafio de MFA para atualizações de MFA como padrão. Além disso, certifique-se de que os dispositivos móveis que os funcionários usam para acessar redes corporativas estejam protegidos da mesma forma.

Habilitar a limpeza automática de hora zero (ZAP, em inglês) no Microsoft Defender para Office 365: o ZAP localiza e executa ações automatizadas nos e-mails que fazem parte da campanha de phishing com base em elementos idênticos de mensagens incorretas conhecidas.

Atualize identidades, privilégios de acesso e listas de distribuição para minimizar superfícies de ataque: invasores como o Storm-0539 presumem que encontrarão usuários com privilégios de acesso excessivos que podem comprometer para um impacto descomunal. Embora as funções dos funcionários e da equipe possam mudar com frequência, estabelecendo uma revisão regular dos privilégios necessários (vs. excessivos ou desatualizados) de indivíduos, aplicativos e dispositivos, as associações à lista de distribuição e outros atributos podem ajudar a limitar as consequências de uma invasão inicial e dificultar o trabalho dos intrusos.

Perfil do Especialista

Alison Ali, Waymon Ho, Emiel Haeghebaert

Inteligência de ameaças da Microsoft

Alison Ali, Waymon Ho e Emiel Haeghebaert chegaram à cibersegurança por caminhos muito diferentes. Este grupo de analistas que acompanha o Storm-0539 tem um histórico que abrange relações internacionais, aplicação da lei federal, segurança e governo.

Waymon Ho primeiro se formou em ciência da computação com foco em engenharia de software, mas se deparou com um estágio no Federal Bureau of Investigation (FBI), nos Estados Unidos. Isso mudou sua trajetória para seguir uma carreira de cibersegurança.

"No FBI, investiguei cibercriminosos como cientista da computação e entrei na Microsoft em 2022 como analista sênior de caça na equipe do Microsoft Threat Intelligence Center (MSTIC), focada em rastrear atores de ameaças", explica Waymon. Atualmente, ele é gerente sênior de pesquisa de segurança na equipe Global Hunting, Oversight, and Strategic Triage (GHOST) da Microsoft.

Waymon diz que o que é notável sobre o Storm-0539 é sua persistência e conhecimento do processo de emissão do cartão-presente. "Eles identificam os funcionários que gerenciam portais de vale-presente e localizam guias internos descrevendo como emiti-los. Eles emitem cartões abaixo do limite de segurança para garantir a autorização e que não são detectados para que possam retornar e repetir o processo", acrescenta.

A experiência de Emiel Haeghebaert abrange tecnologia e relações internacionais. Natural da Bélgica, Emiel se mudou para os Estados Unidos em 2018 para se formar em segurança na Universidade de Georgetown. Atualmente, ele é analista sênior de caça da MSTIC, onde rastreia ameaças cibernéticas patrocinadas pelo Estado iraniano visando clientes e consumidores da Microsoft.

O Emiel também oferece suporte a compromissos de resposta a incidentes da Microsoft relacionados a agentes de ameaças patrocinados pelo Estado e financeiramente motivados, apoiando equipes e clientes no local com análises de atribuição, insights de agentes de ameaças e briefings personalizados. Com formação em relações internacionais e cibersegurança, Emiel prospera na intersecção desses campos. "Trabalhando em inteligência de ameaças cibernéticas, é essencial ter não apenas uma compreensão de questões técnicas relacionadas à segurança cibernética, mas também uma compreensão dos atores de ameaças, suas motivações e prioridades, e os objetivos estratégicos de seus patrocinadores", diz ele. "Minha formação em história e geopolítica me ajuda a obter uma compreensão mais completa de grupos cibercriminosos e atores de ameaças patrocinados pelo Estado."

Alison Ali chegou à segurança de forma rotunda, com formação em linguística pela Universidade de Georgetown. Ela começou a trabalhar na Microsoft em 2022 como pesquisadora sênior de segurança, onde trabalha com equipes de segurança da Microsoft para sintetizar informações para clientes sobre ameaças cibernéticas significativas, incluindo agentes de ameaças com motivação financeira. Alison diz: "Organizações de todos os setores estão frequentemente lidando com usuários afetados por ataques em grande escala, como phishing ou sprays de senha – o que importa são medidas de reforço de segurança que impeçam que um ponto de apoio inicial se torne uma grande invasão".

> "O que importa são medidas de reforço da segurança que impeçam que um ponto de apoio inicial se torne uma grande intrusão.

Metodologia: Os dados de estatísticas de snapshot e cover representam um aumento nas notificações e observações de nossos clientes do agente de ameaças Storm-0539. Esses números são reflexo do aumento de pessoal e recursos gastos no monitoramento desse grupo. O Azure Active Directory forneceu dados anônimos sobre atividades de ameaça, como contas de e-mail mal-intencionadas, e-mails de phishing e movimentação de invasores em redes. Informações adicionais são dos 78 trilhões de sinais de segurança diários processados pela Microsoft todos os dias, incluindo a nuvem, endpoints, a borda inteligente e a telemetria de plataformas e serviços da Microsoft, incluindo o Microsoft Defender.