Os hackers exploram a Amazon SES para explodir mais de 50.000 e -mails

Data: 2025-09-08 18:38:19

Autor: Inteligência Against Invaders

Uma sofisticada campanha de ataque cibernético, onde os atores de ameaças exploraram credenciais comprometidas da AWS para seqüestrar o serviço de email simples da Amazon (SES), lançando operações de phishing em larga escala capazes de enviar mais de 50.000 e-mails maliciosos diariamente.

A equipe de pesquisa do Wiz identificado Esta campanha alarmante de abuso de SES em maio de 2025, destacando uma tendência preocupante, onde os cibercriminosos estão armando serviços de nuvem legítimos para realizar operações de fraude em escala sem precedentes.

O ataque demonstra como as chaves comprometidas da AWS de acesso podem ser transformadas em poderosa infraestrutura de phishing, ignorando as defesas tradicionais de segurança por e -mail enquanto mudam custos e danos à reputação para vítimas inocentes.

A campanha sofisticada começou com os invasores obtendo chaves de acesso à AWS comprometidas por meio de vetores desconhecidos, provavelmente incluindo exposição pública acidental em repositórios de código ou roubo das estações de trabalho do desenvolvedor.

Uma vez armados com essas credenciais, os atores de ameaças imediatamente realizaram reconhecimento para avaliar suas capacidades.

Seu primeiro passo envolveu uma solicitação simples de getCallerIdentity, que revelou que a chave de acesso comprometida continha “SES-” em seu nome, indicando que foi originalmente provisionado com as permissões do SES. Essa descoberta se tornou a base para toda a sua operação.

Os atacantes então aumentaram seu reconhecimento ao investigar o SES diretamente através do getSendQuota e GetAccount Chamadas, projetadas para revelar o estado de configuração atual e determinar se a conta permaneceu restrita aos limites da caixa de areia.

Essa fase de avaliação inicial ocorreu em segundos, demonstrando a natureza automatizada de sua abordagem.

Se libertar de restrições de segurança

Amazon O SES opera no modo “Sandbox” por padrão, restringindo contas a enviar apenas 200 mensagens por dia a endereços verificados a uma taxa máxima de uma mensagem por segundo.

Para desbloquear todo o potencial do serviço para empresas legítimas, as contas devem fazer a transição para o modo de “produção”, o que eleva a cota para normalmente 50.000 e -mails por dia e permite enviar para destinatários arbitrários.

Em uma nova técnica não documentada anteriormente em pesquisas de segurança, os atacantes lançaram uma explosão coordenada de solicitações PutAccountDetails em todas as regiões da AWS em apenas dez segundos.

Essa abordagem multi-regional aparece projetada para maximizar as cotas de envio específicas da região, evitar possíveis restrições ou criar redundância em diferentes locais geográficos.

Para justificar sua solicitação de transição, os atacantes enviaram uma explicação cuidadosamente criada, mas genérica, referenciando um site da empresa de construção que não tinha conexão com a vítima ou as identidades usadas posteriormente para phishing.

Apesar de sua natureza de caldeira, a solicitação foi polida o suficiente para passar no processo de revisão da AWS e obter aprovação para acesso ao modo de produção.

Não satisfeitos com a cota padrão de 50.000 emontes por dia, os atores de ameaças tentaram expandir ainda mais suas capacidades através de vários caminhos.

Eles tentaram abrir um ticket de suporte programaticamente usando a API CreateCase para solicitar limites mais altos, uma abordagem incomum que serve como um forte indicador de atividade suspeita, pois os usuários legítimos normalmente usam o console da AWS.

Quando essa tentativa falhou devido a permissões insuficientes, os atacantes tentaram escalar seus privilégios, criando uma política de IAM chamada “SES-support-policy” e tentando anexá-la ao usuário comprometido.

Esse esforço também falhou, deixando -os com a cota de produção padrão, que se mostrou suficiente para os objetivos da campanha.

Com o modo de produção ativado, os invasores começaram a estabelecer sua infraestrutura de phishing, adicionando vários domínios como identidades verificadas através da API CreateEmailIdentity.

Sua estratégia de domínio incluía domínios de propriedade do atacante e domínios legítimos com proteções fracas do DMARC, facilitando a falsificação ou o envio de e-mails sem ser bloqueado pelos controles de segurança.

O lançamento da campanha de phishing

Uma vez que a infraestrutura deles foi estabelecida, o cibercriminosos Lançou uma ampla campanha de phishing direcionada a várias organizações sem foco geográfico ou do setor claro.

Os e -mails maliciosos referenciados em 2024 formulários fiscais com assuntos como “seus formulários de impostos 2024 estão agora prontos para visualizar e imprimir” e “alerta de informação: os registros fiscais contêm anomalias”.

Esses e -mails direcionaram os destinatários a sites de roubo de credenciais escondidos por trás dos

redirecionamentos fornecidos pelos serviços de análise de tráfego comercial.

Essa técnica, comumente usada em campanhas de marketing legítimas, foi reaproveitada para ignorar os scanners de segurança, fornecendo visibilidade dos atacantes nas taxas de cliques de vítimas.

A natureza leve e oportunista da campanha sugere que foi conduzida principalmente para ganho financeiro, embora os pesquisadores não o vinculem a nenhum grupo de ameaças rastreado publicamente.

As operações de roubo de credenciais podem facilitar várias atividades maliciosas, incluindo compromisso por e -mail de negócios e esquemas adicionais de fraude.

Esta campanha de abuso de SES representa mais do que apenas um incômodo com custos insignificantes. O ataque destaca várias preocupações críticas de segurança para as organizações usando serviços em nuvem.

Os riscos de reputação e negócios são substanciais, pois os invasores podem enviar e -mails de domínios verificados, permitindo o phishing que parece se originar de organizações legítimas. Esse recurso facilita o spearphishing, a fraude, o roubo de dados e o disfarce em processos de negócios, potencialmente causando danos significativos na marca.

O risco de compromisso se estende além do abuso por e -mail, pois a exploração do SES raramente ocorre isoladamente. Serve como um indicador claro de que os adversários já controlam válidos Credenciais da AWS Isso pode ser expandido para ações mais impactantes em toda a infraestrutura em nuvem.

Os riscos operacionais incluem o potencial de spam ou atividade de phishing para desencadear queixas de abuso à AWS, resultando em casos de abuso apresentados em contas de vítimas. Tais incidentes podem interromper as operações comerciais e exigir recursos significativos para resolver.

Estratégias de prevenção

Os especialistas em segurança recomendam várias medidas para reduzir o risco de abuso de SES. As organizações devem implementar políticas de controle de serviços da AWS para bloquear inteiramente o SES em contas onde não é necessário, enquanto audita regularmente e gira as chaves do IAM para evitar compromissos a longo prazo.

A aplicação dos princípios de menor privilégio garante que apenas funções designadas possam verificar novos remetentes ou solicitar acesso à produção.

O registro e o alerta abrangentes da atividade do SES através do CloudTrail podem ajudar a detectar chamadas suspeitas de API e picos de uso.

O monitoramento de indicadores de ataque específicos identificados nesta campanha se mostra crucial, incluindo rajadas multi-regionais de solicitações de putaccounddetails, invocação não console da API CreateCase e criação rápida de domínios e identidades de email.

Plataformas de segurança como o Wiz Defend desenvolveram regras de detecção específicas para identificar esses padrões de ataque no início da cadeia de mortes.

Ao monitorar comportamentos como tentativas multi-regionais de deixar o modo de caixa de areia do SES, o uso da chave de acesso ao IAM após longos períodos de inatividade e chamadas de API de vários países dentro de curtos prazos, as equipes de segurança podem responder antes que as campanhas atinjam a escala completa.

A campanha ressalta a importância crítica de monitorar o uso de serviços em nuvem quanto a picos repentinos e manter a vigilância em torno da segurança da credencial.

À medida que os atores de ameaças continuam evoluindo suas técnicas para explorar serviços legítimos em nuvem, as organizações devem adaptar suas estratégias de defesa para abordar esses vetores de ataque emergentes.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.