Amazon derruba a infraestrutura russa APT29 direcionada aos usuários

Data: 2025-08-30 11:48:27

Autor: Inteligência Against Invaders

A equipe de segurança cibernética da Amazon interrompeu com sucesso uma sofisticada campanha

de buracos de água orquestrada pela APT29, um notório grupo de hackers ligado ao serviço de

inteligência estrangeira da Rússia.

A operação de agosto de 2025 representa o capítulo mais recente em uma batalha de guerra cibernética em andamento entre gigantes da tecnologia e atores de ameaças patrocinados pelo Estado que buscam se infiltrar em redes globais e colher credenciais sensíveis.

Shift do APT29: domínios para hacks de sites

A unidade cibernética russa, também conhecida como Midnight Blizzarddemonstrou uma adaptabilidade notável em suas metodologias de ataque ao longo de 2024 e 2025.

Esta última campanha marca uma mudança tática significativa das operações anteriores, mostrando a capacidade do grupo de evoluir sob pressão dos defensores da segurança cibernética.

Ao contrário da campanha de outubro de 2024, que se baseou na representação do domínio da AWS para distribuir arquivos de protocolo de desktop remotos maliciosos, a mais nova abordagem do APT29 envolveu comprometer sites legítimos e injetar código JavaScript ofusco.

Os atacantes redirecionaram estrategicamente apenas 10% dos visitantes do site para evitar a detecção, demonstrando uma abordagem calculada para maximizar o impacto e minimizar a exposição.

As principais melhorias táticas incluídas:

- Usando técnicas de randomização para redirecionar apenas uma pequena porcentagem de visitantes.
- Empregando a codificação base64 para ocultar código malicioso de sistemas de detecção.
- Definir cookies para evitar redirecionamentos repetidos do mesmo visitante.
- Girando rapidamente para uma nova infraestrutura quando os domínios existentes foram bloqueados.

A sofisticação técnica do grupo ficou evidente no uso de várias técnicas de evasão, permitindo que eles mantenham a segurança operacional enquanto lançava uma rede mais ampla para possíveis vítimas.

Microsoft Auth Flow direcionado

O objetivo final da campanha centrou -se na exploração do sistema de autenticação de código de dispositivos da Microsoft, um recurso legítimo que permite aos usuários autorizar novos dispositivos para acesso à conta.

Apt29 criou páginas de verificação de cloudflare falsas convincentes em domínios como findcloudflare[.]com, projetado para induzir os usuários a autorizar dispositivos controlados por atacantes através do fluxo de trabalho de autenticação da Microsoft.

A equipe de inteligência de ameaças da Amazon descobriu a operação por meio de análises especializadas projetadas para detectar padrões de infraestrutura APT29.

A investigação revelou que os agentes russos haviam comprometido com sucesso vários sites legítimos, transformando -os em armas involuntárias em sua campanha de coleção de inteligência.

Fundamentalmente, Amazon confirmado que nenhum sistema da AWS foi comprometido durante a operação e não houve impacto direto nos serviços ou infraestrutura da AWS.

Quando a Amazon e seus parceiros se mudaram para interromper a infraestrutura inicial, o APT29 rapidamente se adaptou pela migração de operações para provedores alternativos de nuvem e registrando novos domínios, como Cloudflare[.]RedirectPartners[.]com.

Este jogo de gato e rato destacou a natureza persistente das operações cibernéticas patrocinadas pelo Estado e a necessidade de vigilância contínua dos defensores da segurança cibernética.

A colaboração aumenta a defesa cibernética

A resposta da Amazon demonstra a importância crítica das parcerias públicas-privadas no combate a ameaças cibernéticas sofisticadas.

Ao descobrir a campanha, a Amazon imediatamente coordenou com vários parceiros do setor, incluindo Cloudflare e Microsoft, para isolar sistemas comprometidos e compartilhar a inteligência de ameaças.

A empresa também trabalhou para interromper os domínios dos atacantes e forneceu informações cruciais para ajudar outras organizações a proteger seus usuários.

Os especialistas em segurança recomendam que as organizações implementem medidas de proteção robustas, incluindo obrigatórias Autenticação multifatorialverificação cuidadosa das solicitações de autorização do dispositivo e monitoramento aprimorado de eventos de autenticação.

Os administradores de TI são aconselhados a revisar a orientação de autenticação de dispositivos da Microsoft e considerar desativar o recurso, se desnecessário para operações comerciais.

A interrupção bem -sucedida desta campanha ressalta a evolução contínua das táticas de guerra cibernética e a necessidade de adaptação constante pelos profissionais de segurança cibernética.

À medida que o APT29 continua a refinar seus métodos, a comunidade de segurança cibernética deve manter o compartilhamento de inteligência colaborativo e a caça proativa de ameaças para ficar à frente desses adversários persistentes.

Encontre esta notícia interessante! Siga -nosGoogle NewsAssim,LinkedIneXPara obter atualizações instantâneas!