Amazon interrompe hackers russos APT29 visando o Microsoft 365 - Agai

Data: 2025-09-01 23:54:37

Autor: Inteligência Against Invaders

Pesquisadores interromperam uma operação atribuída ao grupo de ameaças patrocinado pelo

Estado russo Midnight Blizzard, quebuscou acesso a contas e dados do Microsoft 365.

Também conhecido como APT29, o grupo de hackers comprometeu sites em uma campanha para redirecionar alvos selecionados “para infraestrutura maliciosa projetada para induzir os usuários a autorizar dispositivos controlados por invasores por meio do fluxo de autenticação de código de dispositivo da Microsoft”.

O agente da ameaça Midnight Blizzard foi vinculado ao Serviço de Inteligência Estrangeira da Rússia (SVR) e é bem conhecido por seus métodos inteligentes de phishing que recentemente impactaram Embaixadas europeias, Hewlett Packard Empresae TeamViewer.

Seleção aleatória de alvo

A equipe de inteligência de ameaças da Amazon descobriu os nomes de domínio usados na campanha watering hole depois de criar uma análise para a infraestrutura do APT29.

Uma investigação revelou que os hackers comprometeram vários sites legítimos e ofuscaram códigos maliciosos usando a codificação base64.

Ao usar a randomização, o APT29 redirecionou cerca de 10% dos visitantes do site comprometido para domínios que imitam as páginas de verificação do Cloudflare, como *EncontrarCloudFlare[.]com*ou *Cloudflare[.]parceiros de redirecionamento[.]com*.

[IMAGEM REMOVIDA]Explica em um relatório sobre a ação recente, os agentes de ameaças usaram um sistema baseado em cookies para impedir que o mesmo usuário fosse redirecionado várias vezes, reduzindo a suspeita.

As vítimas que acessaram as páginas falsas do Cloudflare foram guiadas para um fluxo de autenticação de código de dispositivo malicioso da Microsoft, na tentativa de induzi-las a autorizar dispositivos controlados por invasores.

[IMAGEM REMOVIDA]domínios que se fazem passar por AWS ou engenharia social tentam contornar a autenticação multifator (MFA) enganando os alvos para que criemsenhas específicas do aplicativo.

Recomenda-se que os usuários verifiquem as solicitações de autorização do dispositivo, habilitem a autenticação multifator (MFA) e evitem executar comandos em seu sistema que são copiados de páginas da Web.

Os administradores devem considerar desabilitar falhas desnecessárias de autorização de dispositivo sempre que possível, impor políticas de acesso condicional e monitorar de perto eventos de autenticação suspeitos.

A Amazon enfatizou que esta campanha APT29 não comprometeu sua infraestrutura nem impactou seus serviços.

Bill Toulas

Bill Toulas é redator de tecnologia e repórter de notícias de segurança da informação com mais de uma década de experiência trabalhando em várias publicações online, cobrindo código aberto, Linux, malware, incidentes de violação de dados e hacks.

Você também pode gostar: