Varredura de portais de Palo Alto aumenta 500%

Data: 2025-10-06 11:00:00

Autor: Inteligência Against Invaders

Especialistas em segurança observaram um aumento maciço na atividade de reconhecimento

direcionada a portais de login para produtos da Palo Alto Networks.

O provedor de inteligência em tempo real GreyNoise disse que viu cerca de 1300 endereços IP direcionados à sua tag Palo Alto Networks Login Scanner em 3 de outubro. Por outro lado, os volumes diários raramente ultrapassaram 200 IPs nos 90 dias anteriores.

A empresa disse que a atividade é direcionada e “provavelmente derivada” de varreduras públicas ou originadas por invasores.

Cerca de 91% dos IPs estavam localizados nos EUA, com clusters menores no Reino Unido, Holanda, Canadá e Rússia. A grande maioria (93%) deles é classificada como “suspeita”, com 7% confirmada como maliciosa.

Leia mais sobre ameaças da Palo Alto Networks: Hackers Exploram em Cadeia Três Falhas de Firewall da Palo Alto Networks

O aumento de 500% é o maior observado pela GreyNoise para portais de login de Palo Alto em três meses.

“A pesquisa da GreyNoise em julho descobriu que os surtos de atividade contra as tecnologias de Palo Alto foram, em alguns casos, seguidos por novas divulgações de vulnerabilidades em seis semanas”, continuou a empresa.

“No entanto, os surtos contra a tag Palo Alto Networks Login Scanner da GreyNoise não mostraram essa correlação. A GreyNoise continuará monitorando caso essa atividade preceda uma nova divulgação de Palo Alto, o que representaria um sinal aditivo à nossa pesquisa de julho.”

Cisco também visava

A GreyNoise também detectou aumentos na verificação de outros serviços de acesso remoto, incluindo os produtos SonicWall, Ivanti, Pulse Secure e Cisco ASA.

“A análise da GreyNoise mostra que esse surto de Palo Alto compartilha características com a varredura do Cisco ASA ocorrida nas últimas 48 horas. Em ambos os casos, os scanners exibiram sobreposição de agrupamento regional e impressão digital nas ferramentas usadas “, afirmou.

“Tanto o tráfego de verificação de login do Cisco ASA quanto o de Palo Alto nas últimas 48 horas compartilham uma impressão digital TLS dominante vinculada à infraestrutura na Holanda. Isso ocorre depois que a GreyNoise relatou inicialmente um aumento de varredura do ASA antes da

divulgação da Cisco de dois dias zero do ASA.

No entanto, a GreyNouse não pôde dizer com certeza se a atividade foi realizada pelo mesmo operador e/ou com a mesma intenção.

Os produtos de segurança continuam sendo um alvo popular para os agentes de ameaças. A semana passada *Segurança da informação* reportadoum aumento nos ataques do grupo de ransomware Akira com o objetivo de sequestrar dispositivos SonicWall SSL VPN.

A IA também está ajudando os grupos a ampliar os esforços de reconhecimento e exploração.

O NCSC alertou em um relatório de maio: “Os agentes de ameaças cibernéticas quase certamente já estão usando a IA para aprimorar as táticas, técnicas e procedimentos (TTPs) existentes no reconhecimento de vítimas, pesquisa de vulnerabilidades e desenvolvimento de exploits, acesso a sistemas por meio de engenharia social, geração básica de malware e processamento de dados exfiltrados. “