Aumento de 500% nas varreduras direcionadas aos portais de login da Pa

Data: 2025-10-05 02:31:52

Autor: Inteligência Against Invaders

boletim de segurança da informação

8 segundos atrás
Alerta, Internacional

Em 3 de outubro de 2025, a GreyNoise observou um aumento de 500% nas varreduras direcionadas aos portais de login da Palo Alto Networks, o maior nível de atividade em três meses. Os pesquisadores descobriram que mais de 1.285 IPs escanearam os portais de Palo Alto, um aumento em relação aos 200 típicos. Eles observaram que 93% desses IPs eram suspeitos, enquanto 7% eram maliciosos.

A maioria se originou nos EUA, com clusters menores no Reino Unido, Holanda, Canadá e Rússia. O GryNoise teve como alvo o tráfego específico destinado aos portais de login de Palo Alto, organizados em clusters de varredura separados.

As varreduras se concentraram em perfis emulados de Palo Alto nos sistemas dos EUA e do Paquistão, mostrando esforços organizados de reconhecimento.

A GreyNoise descobriu que a varredura recente de Palo Alto se assemelha à atividade do Cisco ASA, indicando agrupamento regional e impressões digitais TLS compartilhadas relacionadas à infraestrutura na Holanda. Ambos utilizaram ferramentas semelhantes, sugerindo potencial infraestrutura ou operadores compartilhados. Essa sobreposição ocorre após um aumento na varredura do Cisco ASA antes que duas vulnerabilidades de dia zero fossem reveladas.

“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 na varredura do ASA antes da divulgação da Cisco de dois dias zero do ASA.uo; lê o relatório publicado pela Grey Noise. “Além de uma possível conexão com a verificação contínua do Cisco ASA, a GreyNoise identificou picos simultâneos nos serviços de acesso remoto. Embora suspeitos, não temos certeza se essa atividade está relacionada. “

A GreyNoise observou em julho que os aumentos nas varreduras de Palo Alto às vezes aconteciam antes que novas falhas aparecessem em seis semanas; Os especialistas estão monitorando se o último aumento sinaliza outra divulgação.

“A GreyNoise está desenvolvendo uma lista de bloqueio de IP dinâmica aprimorada para ajudar os defensores a tomar medidas mais rápidas em ameaças emergentes”, conclui o relatório.