GreyNoise detecta aumento de 500% nas varreduras direcionadas aos por

Data: 2025-10-04 20:03:52

Autor: Inteligência Against Invaders

GreyNoise detecta aumento de 500% nas varreduras direcionadas aos portais da Palo Alto Networks

A GreyNoise viu um aumento de 500% nas varreduras nos portais de login da Palo Alto Networks em 3 de outubro de 2025, o maior em três meses.

A empresa de segurança cibernética GreyNoise relatou um aumento de 500% nas varreduras direcionadas aos portais de login da Palo Alto Networks em 3 de outubro de 2025, marcando a maior atividade em três meses.

Em 3 de outubro, os pesquisadores observaram que mais de 1.285 IPs escanearam os portais de Palo Alto, contra os 200 usuais. Os especialistas relataram que 93% dos IPs eram suspeitos, 7% maliciosos.

A maioria se originou nos EUA, com clusters menores no Reino Unido, Holanda, Canadá e Rússia.

A GryNoise definiu o tráfego direcionado e estruturado, voltado para os portais de login de Palo Alto e dividido em clusters de varredura distintos.

As varreduras tiveram como alvo perfis emulados de Palo Alto, concentrando-se principalmente nos sistemas dos EUA e do Paquistão, indicando reconhecimento coordenado e direcionado.

A GreyNoise descobriu que a varredura recente de Palo Alto reflete a atividade do Cisco ASA, mostrando clustering regional e impressões digitais TLS compartilhadas vinculadas à infraestrutura da Holanda. Ambos usaram ferramentas semelhantes, sugerindo possíveis infraestruturas ou operadores compartilhados. A sobreposição segue um aumento de varredura do Cisco ASA que precede a divulgação de duas vulnerabilidades de dia zero.

*“Tanto o Cisco ASA quanto o tráfego de varredura de login de Palo Alto nas últimas 48 horas compartilham uma impressão digital TLS dominante vinculada à infraestrutura na Holanda.*reportado*um surto de varredura do ASA antes da divulgação da Cisco de dois dias zero do ASA.” lê o* relatório *publicado pela Grey Noise. “Além de uma possível conexão com a verificação contínua do Cisco ASA, a GreyNoise identificou surtos simultâneos nos serviços de acesso remoto. Embora suspeitos, não temos certeza se essa atividade está relacionada.*

A GreyNoise observou em julho que picos nas varreduras de Palo Alto às vezes precediam novas falhas 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.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,portais da Palo Alto Networks)