Aumento maciço de varreduras direcionadas aos portais de login da Palo

Data: 2025-10-04 15:29:37

Autor: Inteligência Against Invaders

Um aumento nas varreduras suspeitas direcionadas aos portais de login da Palo Alto Networks

indica esforços claros de reconhecimento de endereços IP suspeitos, alertam os pesquisadores.

A empresa de inteligência de segurança cibernética GreyNoise relata um aumento de 500% nos endereços IP focados nos perfis Palo Alto Networks GlobalProtect e PAN-OS.

A atividade culminou em 3 de outubro com mais de 1.285 IPs únicos envolvidos na atividade. Normalmente, as varreduras diárias não excedem 200 endereços, diz a empresa.

A maioria dos IPs observados estava geolocalizada nos EUA, enquanto clusters menores estavam baseados no Reino Unido, Holanda, Canadá e Rússia.

Um grupo de atividades concentrou seu tráfego em alvos nos Estados Unidos e outro no Paquistão, dizem os pesquisadores, observando que ambos tinham “impressões digitais TLS distintas, mas não sem sobreposição”.

De acordo com a GreyNoise, 91% dos endereços IP foram classificados como suspeitos. Outros 7% foram marcados como maliciosos.

“Quase todas as atividades foram direcionadas aos perfis emulados de Palo Alto da GreyNoise (Palo Alto GlobalProtect, Palo Alto PAN-OS), sugerindo que a atividade é direcionada por natureza, provavelmente derivada de varreduras públicas (por exemplo, Shodan, Censys) ou originadas por invasores que identificam dispositivos Palo Alto”, explica GreyNoise.

[IMAGEM REMOVIDA]avisou anteriormente que essa atividade de varredura geralmente indica preparação para ataques usando novos exploits para falhas de dia zero ou n dias.

A empresa de segurança cibernética emitiu um alerta recentemente sobre Aumento das varreduras de rede visando dispositivos Cisco ASA. Duas semanas depois, surgiram notícias sobre umVulnerabilidade de dia zeroexplorado em ataques visando o mesmo produto da Cisco.

No entanto, a GreyNoise diz que a correlação observada é mais fraca para as varreduras recentes com foco nos produtos da Palo Alto Networks.

Grafana também é alvo

Os pesquisadores também notaram um aumento nas tentativas de exploração de uma

vulnerabilidade de travessia de caminho antigo no Grafana. O problema de segurança é identificado como CVE-2021-43798 efoi explorado em dezembro de 2021em ataques de dia zero.

CinzaRuídoobservado 110 IPs maliciosos exclusivos, a maioria deles de Bangladesh, lançando ataques em 28 de setembro.

Os alvos foram baseados principalmente nos Estados Unidos, Eslováquia e Taiwan, com os ataques mantendo uma proporção de destino consistente, dependendo da origem específica, o que normalmente indica automação.

[IMAGEM REMOVIDA]

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: