O malware SystemBC transforma sistemas VPS infectados em uma rodovi

Data: 2025-09-18 16:23:14

Autor: Inteligência Against Invaders

Os operadores do botnet proxy SystemBC estão procurando servidores virtuais privados (VPS)

comerciais vulneráveis e mantêm uma média de 1.500 bots todos os dias que fornecem uma rodovia

para tráfego malicioso.

Os servidores comprometidos estão localizados em todo o mundo e têm pelo menos uma vulnerabilidade crítica não corrigida, alguns deles sendo atormentados por dezenas de problemas de segurança.

O SystemBC existe desde pelo menos 2019 e tem sido usado por vários agentes de ameaças, incluindo várias gangues de ransomware, para entregar cargas úteis.

Ele permite que os invasores roteiem o tráfego mal-intencionado pelo host infectado e ocultem a atividade de comando e controle (C2) para dificultar a detecção.

Clientes da SystemBC

De acordo com pesquisadores do Black Lotus Labs da Lumen Technology, a rede proxy SystemBC é construída para volume, com pouca preocupação com furtividade. Ele também alimenta outras redes de proxy criminosas e tem “tempos médios de infecção extremamente longos”.

Com base nas descobertas dos pesquisadores, nem os clientes nem os operadores do SystemBC se preocupam em manter um perfil discreto, uma vez que os endereços IP dos bots não são protegidos de forma alguma (por exemplo, por meio de ofuscação ou rotação).

O SystemBC tem mais de 80 servidores de comando e controle (C2), que conectam clientes a um servidor proxy infectado e alimentam outros serviços de rede proxy.

Um serviço malicioso chamado REM Proxy depende de cerca de 80% dos bots do SystemBC, fornecendo serviços em camadas a seus clientes, dependendo da qualidade do proxy necessária.

Um grande serviço russo de raspagem da web é outro cliente significativo do SystemBC, juntamente com uma rede proxy baseada no Vietnã chamada VN5Socks ou Shopsocks5.

[IMAGEM REMOVIDA][IMAGEM REMOVIDA]

Todos os servidores infectados têm várias vulnerabilidades “fáceis de explorar”, sendo a média de

20 problemas de segurança não corrigidos e pelo menos um de gravidade crítica.

Os pesquisadores também encontraram um sistema no Alabama, que a plataforma de inteligência de internet e o mecanismo de busca Censys listaram como tendo 161 vulnerabilidades de segurança.

[IMAGEM REMOVIDA]relatório compartilhado com o BleepingComputer.

Com base na telemetria IP global da empresa, um endereço, 104.250.164[.]214, parece estar no centro da atividade de recrutamento de vítimas e também hospeda todas as 180 amostras de malware SystemBC.

De acordo com a análise dos pesquisadores, um servidor recém-infectado baixa um script de shell, que tem comentários em russo e direciona o bot para executar todas as amostras do SystemBC ao mesmo tempo.

A rede proxy está ativa há muito tempo e resistiu até mesmo a operações de aplicação da lei, como Endgame, que visava os droppers de malware para vários botnets, incluindo SystemBC.

O Black Lotus Labs fornece uma análise técnica detalhada do malware proxy SystemBC, juntamente com indicadores de comprometimento, para ajudar as organizações a identificar tentativas de comprometimento ou interromper a operação.

Ionut Ilascu

Ionut Ilascu é um escritor de tecnologia com foco em todas as coisas de segurança cibernética. Os tópicos sobre os quais ele escreve incluem malware, vulnerabilidades, exploits e defesas de segurança, bem como pesquisa e inovação em segurança da informação. Seu trabalho foi publicado pela Bitdefender, Netgear, The Security Ledger e Softpedia.

Você também pode gostar: