O SystemBC Botnet compromete 1.500 VPs todos os dias para alugar para

Data: 2025-09-19 06:27:18

Autor: Inteligência Against Invaders

O SystemBC, uma rede de malware resiliente Socks5, vista pela primeira vez em 2019, desenvolveu drasticamente sua infraestrutura de proxy, comprometendo uma média de 1.500 servidores privados virtuais (VPS) todos os dias.

Essa mudança de dispositivos residenciais para os nós VPS em larga escala concede a ameaças que os atores de largura de banda e longevidade sem precedentes do tráfego malicioso, permitindo operações sustentadas de negação de serviço distribuída (DDOs) e forças brutas, enquanto evitam limitações típicas de rede de proxy.

Os proxies tradicionais de botnet dependem de roteadores domésticos, dispositivos IoT ou terminais residenciais com largura de banda restrita.

Labs Black Lotus na Lumen Technologies recentemente descoberto Uma assembléia de mais de 80 servidores de comando e controle, alimentando esse botnet, quase 80 % dos quais alavancam os fornecedores de VPS comercial de alta capacidade.

O tráfego excessivo através desses dispositivos geralmente interrompe a atividade legítima do usuário e desencadeia uma rápida detecção. Por outro lado, o SystemBC aproveita os poderosos sistemas VPS capazes de sustentar transferências de dados em escala de gigabytes sem alertar os provedores de hospedagem ou usuários finais.

A análise da telemetria global revelou médias diárias de 1.500 sistemas implantados como proxies, incluindo 300 que se sobrepõem à botnet de forçante bruta e bruta.

Quase 40 % dessas infecções persistem por mais de um mês, ressaltando a resiliência da rede e o desrespeito dos atacantes por furtividade em favor de um volume.

Os servidores de vítimas exibem uma impressionante variedade de vulnerabilidades não patches – em média vinte por servidor, com alguns sistemas abrigando mais de 160 CVEs conhecidos.

Os atores maliciosos exploram essas falhas sondando a porta 443 para acesso inicial e utilizando retornos de chamada da porta 80 para baixar scripts de shell cometidos por russo que implantam mais de 180 amostras de malware simultaneamente.

O Proxy Pipeline resultante direciona o tráfego do usuário de portas de entrada de alto número por meio de hosts VPS infectados para os alvos finais, conforme ilustrado nos processos de configuração e criptografia decodificados da amostra Linux-Variant.

Ecossistema criminal e serviços de procuração

O Black Lotus Labs observou proxies SystemBC integrados a vários serviços criminais. Duas plataformas de procuração baseadas na Rússia e uma vietnamita redirecionam esses bots, comercializando conjuntos de IPs de alto volume para clientes indiferentes à lista negra.

Quase 100 % desses proxies baseados em VPS acabam surgindo em locais de blocos, mas os operadores priorizam a capacidade de tráfego sobre a evasão.

Também vemos uma vida útil média de infecção extremamente longa, onde quase 40% permanecem infectados por mais de um mês.

Entre os usuários mais proeminentes está o Proxy REM, que aluga aproximadamente 80 % da rede SystemBC. O REM Proxy também agrega 20.000 roteadores Mikrotik comprometidos e descobriu livremente proxies abertos, oferecendo pacotes em camadas-mix-speed, mix-mix e mix-economy-para cumprir reconhecimentocolheita de credenciais e necessidades direcionadas de exploração.

Grupos de ransomware, como Morfeu e Avoslocker, alavancam o proxy REM para tudo, desde campanhas de phishing a pipelines de exfiltração, demonstrando o papel integral do serviço em vários vetores de ataque.

O maior uso da botnet é pelos próprios operadores do SystemBC, usando sua própria rede para forçar as credenciais do WordPress.

Os dados do Global NetFlow confirmam que os usuários de proxy REM se conectam a quase cem entradas de usuário Servidores C2que, em seguida, canaliza solicitações para os hosts SystemBC e Mikrotik. Triagem diária através de um domínio auxiliar, Honipsiops[.]In, identifica novos endereços IP acessíveis e alimenta aproximadamente 2.500 proxies examinados na rede.

Interrupção e medidas defensivas

Em resposta a essas revelações, a Lumen Technologies possui tráfego de roteamento nulo para toda a infraestrutura de proxy SystemBC e REM conhecida em sua espinha dorsal global.

Os indicadores de compromisso (COI) foram publicados para facilitar os esforços de defesa da comunidade e a cortar os fluxos de receita de criminoso Serviços de proxy.

O Black Lotus Labs reconhece a colaboração de parceiros do setor, incluindo Spur e InfoBlox, por apoiar esta pesquisa.

Os defensores da rede devem monitorar as tentativas anômalas de login dos intervalos de IP VPS, implementar regras de firewall de aplicativos da web para bloquear as IOCs identificadas e verificar a postura de segurança de servidores hospedados em nuvem por meio de serviços como Censys.

Os consumidores e os usuários finais de pequenos escritórios devem atualizar e segmentar regularmente os roteadores Soho, desativar as credenciais padrão e restringir o acesso administrativo.

À medida que o cenário de botnet muda para a infraestrutura de nível comercial, os defensores

devem se adaptar, priorizando a detecção baseada em volume e o gerenciamento proativo de vulnerabilidades para proteger contra a crescente ameaça de redes de proxy alimentadas por VPS.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.