Aisuru Botnet combina recorde de 11,5 tbps ddos ??ataque com 300.000 r

Data: 2025-09-16 10:24:02

Autor: Inteligência Against Invaders

O recém-identificado Botnet Aisuru, alavancando cerca de 300.000 roteadores comprometidos em

todo o mundo, foi identificado como a força por trás de um ataque de 11,5 TBPS distribuído (DDoS),

que desvie o recorde em setembro de 2025.

Esse ataque sem precedentes eclipsa o pico anterior de 5,8 Tbps visto no início do ano e ressalta uma escalada perigosa em escala e sofisticação de botnet.

Primeiro divulgado Por XLAB em agosto de 2024, Aisuru ressurgiu em março de 2025, quando o sistema de insight e análise de ameaças cibernéticas da XLAB (CTIA) começou a capturar amostras novas.

De acordo com um insider anônimo, o grupo é liderado por três operadores com codinome Snow (Desenvolvimento de Botnet), Tom (Pesquisa de Vulnerabilidade) e Forky (vendas de botnet).

Em abril de 2025, Tom orquestrou o compromisso de um servidor de atualização de firmware do roteador Totolink, plantando um script malicioso (T.SH) que redirecionou os dispositivos para baixar o malware aisuru.

Dentro de semanas, a botnet aumentou os 100.000 nós, chegando a aproximadamente 300.000 roteadores infectados em todo o mundo.

A CTIA do XLAB oferece forte visibilidade à infraestrutura da Aisuru, abrangendo a coleta de amostras, comando e controle Servidores C2e ataque de telemetria.

Referência cruzada Capturas de tela vazadas do painel de gerenciamento de botnet-apresentando mais de 30.000 nós chineses entre 300.000 totais-e os registros de mitigação de Cloudflare ajudaram a validar as reivindicações do membro privilegiado e a estabelecer a culpabilidade de Aisuru em vários ataques recordes.

Estatísticas de propagação e ataque

As amostras de Aisuru exploram uma variedade diversificada de vulnerabilidades para se propagar. Enquanto a maioria das infecções se espalhou por falhas de “n do dia n”, o botnet continua a alavancar um dia zero nos roteadores CNPILOT da Cambium Networks observados pela primeira vez em junho de 2024.

Rose para 672.588 globalmente dentro de um mês, provando que a campanha de infecção do grupo Aisuru foi muito bem -sucedida.

As vulnerabilidades abordadas incluem CVE-2017-5259 (CAMBiumNetworks), CVE-2023-28771 (dispositivos Zyxel), CVE-2023-50381 (Realtek Jungle SDK) e numerosas falhas de DVR e gateway datando de 2013.

Essa ampla tela de vulnerabilidade permite que o AISURU se infiltre um amplo espectro de dispositivos de roteador e IoT.

Os dados de ataque revelam campanhas diárias de DDOs direcionadas a centenas de organizações na China, Estados Unidos, Alemanha, Reino Unido e Hong Kong sem viés discernível do setor.

Notavelmente, Aisuru conduziu um ataque de 5,8 tbps que Cloudflare Mitigado em abril e depois aumentou até 11,5 TBPs em setembro, ampliando o tráfego através de túneis GREs configurados em quatro IPs C2 (151.242.2.22-25) e os dispositivos seqüestrados em todo o mundo.

Insights técnicos

A análise da amostra de Bot da versão 2 da Aisuru expõe medidas avançadas de anti-análise e evasão.

Na startup, os malware digitalizam nomes de processos e identificadores de hardware – por exemplo, “Wireshark”, “VirtualBox”E“ qemu ”-e sai se detectado para impedir a inspeção dinâmica. Desativa o OOM Killer do Linux escrevendo“ -1000 ”para /proc/self/oom_score_adjgarantindo a execução persistente mesmo sob pressão da memória.

Para resistir às táticas rivais de “matar”, os mapas binários compartilhavam bibliotecas de /lib/renomear -se para libcow.soe ofusca seu nome de processo como daemons comuns como “telnetd” e “dhclient”.

As rotinas de criptografia também divergem das implementações padrão. O algoritmo RC4 modificado da AISURU emprega uma chave fixa (“Pjbinbbeasdddfsc”), apresenta perturbações personalizadas durante a inicialização e integra um processo de geração de teclas sob medida que combina mudanças de estado baseado em sementes com operações bit-sise.

Essa variante descriptografa seqüências de comando e chaves de comunicação muito mais resilientemente do que a baunilha RC4, como demonstrado por uma mensagem de pós-decreção provocada incorporada na amostra.

A extração C2 mantém o método legado de decodificar registros TXT via XOR (abandonando o uso anterior do Chacha20), dividindo as cordas descriptografadas em ‘|’ | e ‘,’ para enumerar subdomínios.

As compilações recentes também incorporam um módulo de teste de velocidade de rede opcional-os pontos de extremidade do teste de velocidade-para relatar métricas de desempenho do nó de volta ao C2, facilitando o recrutamento de proxies de alta largura de banda para campanhas futuras.

O rápido crescimento, propagação multi-vetor de Aisuru e técnicas sofisticadas de evasão o posicionam como uma das botnets mais formidáveis ??da história.

As equipes de segurança devem priorizar as vulnerabilidades de roteador conhecidas, monitorar o estabelecimento anômalo do túnel GRE e examinar as anomalias registradas do DNS-TXT para

detectar e interromper as operações da Aisuru.

Encontre esta história interessante! Siga -nosLinkedIneXPara obter mais atualizações instantâneas.