Your IT Company

Mirai Botnet e Seus Spinoffs

1. Objetivo

Este documento foi desenvolvido e fundamentado nas documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são mundialmente conhecidas na área de cibersegurança como modelos de padronização das melhores práticas de segurança, pesquisa de metodologias de ataques, defesa cibernética e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

2. Mirai Botnet e Seus Spinoffs.

2.1 Ataque DDoS Globais

Pesquisas recentes revelam que **spinoffs** da infame **mirai botnet** estão causando uma nova onda de ataques de **negação de serviço distribuída (DDoS)** ao redor do mundo. Esses ataques, que começaram no final de 2024, exploram falhas críticas em dispositivos de **Internet das Coisas (IoT)**, comprometendo-os para criar vastas redes de **botnets** capazes de sobrecarregar organizações e redes em uma escala global.

2.2 Murdoc_Botnet: Uma Nova Ameaça Surge.

Uma das principais botnets dessa nova onda é a **Murdoc_Botnet**, um **spinoff do Mirai** que iniciou suas operações em julho de 2024. Pesquisadores da **Qualys** recentemente descobriram detalhes sobre as atividades do Murdoc, que já infectou mais de **1.300 endereços IP ativos**. A botnet explora vulnerabilidades em **câmeras IP da Avtech e roteadores Huawei HG532**, que são suscetíveis a **execução remota de código (RCE) e injeção de comandos sem autenticação**.

A propagação do Murdoc envolve a exploração dessas falhas para injetar **scripts maliciosos** e arquivos **ELF** em dispositivos IoT comprometidos. Uma vez infectados, os dispositivos começam a se comunicar com os servidores de **comando e controle (C2)** da botnet, que propagam o **malware Mirai** ainda mais pela rede.

Pesquisadores da Qualys identificaram mais de **100 conjuntos distintos de servidores** envolvidos na campanha, que desempenham um papel crucial na organização das atividades e na manutenção da botnet em operação em **diversos países**, com os maiores números de IPs encontrados em **Malásia**, seguidos de **Tailândia**, **México** e **Indonésia**.

2.3 Ataques DDoS Globais: Uma Campanha de Grande Escala.

Outra botnet, composta por variantes do **Mirai** e **Bashlite**, está explorando falhas de segurança e credenciais fracas em dispositivos IoT para amplificar ataques DDoS. Segundo pesquisadores da **Trend Micro**, essa botnet tem realizado ataques de grande escala desde o final de 2024, inicialmente focados em organizações no Japão, incluindo grandes corporações e bancos. No entanto, a campanha rapidamente se expandiu para a **América do Norte**, **Europa** e **Ásia**.

Os dispositivos-alvo dos ataques incluem **roteadores sem fio** e **câmeras IP** de marcas populares como **TP-Link, Zyxel** e **Hikvision**. Estes dispositivos são vulneráveis devido a falhas de **execução remota de código (RCE)** ou **credenciais fracas**.

Os **vetores de ataque** usados por essa botnet são variados, mas os pesquisadores destacaram dois tipos principais de ataques DDoS:

1. **Ataques de Inundação:** Sobrecarga a rede enviando um volume massivo de pacotes, causando congestionamento e interrupção do serviço.

2. **Exaustão de Sessões:** Esgota os recursos do servidor estabelecendo muitas conexões, levando a falhas no servidor e falta de resposta.

Em alguns casos, os atacantes usaram uma combinação desses dois tipos de ataques, permitindo uma sobrecarga simultânea da rede e do servidor.

2.4 Como Se Defender de Ataques DDoS.

Com as variantes do Mirai continuando a gerar novas botnets para lançar ataques DDoS cada vez mais amplos, é crucial que as organizações possam identificar e proteger suas redes contra esse tráfego indesejado. Os pesquisadores recomendaram diversas estratégias de mitigação, adequadas aos dois tipos de ataques observados:

2.5 Para Ataques de Inundação:

- Utilize firewalls ou roteadores para bloquear endereços IP específicos ou protocolos, restringindo o tráfego malicioso.
- Colabore com provedores de serviços de comunicação para filtrar o tráfego DDoS na rede de backbone ou borda.
- Atualize o hardware dos roteadores para lidar com volumes maiores de pacotes e evitar sobrecarga.

2.6 Para Ataques de Exaustão de Sessões:

- Implemente limitação de taxa para restringir o número de requisições que podem ser feitas por um endereço IP dentro de um determinado período.
- Utilize serviços de mitigação DDoS de terceiros para separar o tráfego de ataque e processar o tráfego legítimo.
- Realize monitoramento em tempo real para identificar e bloquear endereços IP com um número elevado de conexões, sinalizando um ataque em andamento.

Além disso, pesquisadores da Qualys enfatizaram a importância de monitorar processos suspeitos e execuções de scripts ou binários não confiáveis em dispositivos IoT, alertando as organizações para a cautela ao lidar com scripts shell provenientes de fontes não confiáveis.

Essa nova onda de ataques DDoS alimentada por spinoffs do Mirai botnet é um alerta sobre como as ameaças evoluem e como dispositivos IoT vulneráveis continuam a ser uma superfície de ataque crítica. Implementando as medidas de mitigação recomendadas, incluindo a atualização de dispositivos, o monitoramento constante de tráfego e o uso de ferramentas de mitigação de DDoS, as organizações podem proteger suas redes e reduzir o impacto de futuros ataques.

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Harley José Maria Araújo - Consultor de Resposta à Incidentes Pleno