A nova botnet explora falhas simples do DNS que levam a um ataque ciber

Data: 2025-09-20 18:28:56

Autor: Inteligência Against Invaders

Os pesquisadores de segurança cibernética descobriram uma sofisticada operação de botnet russa que alavancou incrustações incorretas do DNS e comprometiu os roteadores Mikrotik para entregar malware por meio de campanhas enormes de spam.

A descoberta revela como os atores de ameaças exploraram erros simples do DNS para ignorar as proteções de segurança por email e distribuir cargas úteis maliciosas em escala global.

A investigação começou em novembro de 2024, quando os pesquisadores identificaram uma campanha MALSPAM com faturas de remessas fraudulentas que se representam DHL Express.

A campanha foi entregue Arquivos ZIP Contendo JavaScript ofuscado que executou scripts do PowerShell, estabelecendo conexões com um servidor de comando e controle localizado no endereço IP 62.133.60[.]137, associado à atividade de ameaça russa na infraestrutura de rede de soluções de conectividade global.

Mikrotik Botnet alimenta o ataque cibernético global

Análise dos cabeçalhos de e -mail revelado Uma ampla rede de aproximadamente 13.000 dispositivos Mikrotik seqüestrados operando como uma botnet coordenada.

Os roteadores comprometidos abrangem várias versões de firmware, incluindo lançamentos recentes, sugerindo a exploração contínua de vulnerabilidades conhecidas e explorações potencialmente de dia zero.

Os atacantes transformaram esses dispositivos em proxies de Socks4, criando efetivamente um sistema de retransmissão aberta que mascara origens maliciosas do tráfego e fornece anonimato para operações de ameaças.

As principais características da infraestrutura de botnet incluem:

- Configuração do proxy SOCKS4, permitindo o anonimato de roteamento de tráfego.
- Suporte para dezenas de milhares de máquinas comprometidas adicionais.
- Exploração de firmware de várias versões nas gerações do roteador.
- Distribuição global que fornece uma extensa cobertura geográfica.
- A acessibilidade aberta do relé permite o uso de atores de ameaças de terceiros.

A configuração do botnet permite dezenas ou centenas de milhares de máquinas comprometidas adicionais para rotear o tráfego através desses nós de proxy, ampliando exponencialmente a escala

e o impacto da infraestrutura de ataque.

Essa abordagem distribuída permite várias atividades maliciosas, incluindo ataques distribuídos de negação de serviço, exfiltração de dados, operações de recheio de credenciais e campanhas generalizadas de distribuição de malware.

O método de compromisso provavelmente envolve explorar Vulnerabilidades de transbordamento de buffer Nos roteadores Mikrotik, particularmente direcionando dispositivos com credenciais administrativas padrão.

Muitos roteadores historicamente enviados com contas de administração codificadas usando senhas em branco, criando vulnerabilidades de segurança persistentes, mesmo após atualizações de firmware.

SPF misconfigs Ative o desvio de segurança por email

O sucesso da campanha dependia de explorar registros de políticas de remetente de remetente em aproximadamente 20.000 domínios legítimos.

Enquanto esses domínios implementados SPF Proteções, eles foram configurados incorretamente com sinalizadores “+all” em vez das opções seguras “-ver” ou “~ all”.

Essa configuração incorreta crítica autorizou essencialmente qualquer servidor em todo o mundo a enviar e-mails em nome desses domínios, derrotando completamente as finalidades anti-spoofing do SPF.

Vulnerabilidades críticas de configuração do DNS identificadas:

- Os registros do SPF usando sinalizadores “+all” permissivos em vez de “-odos” restritivos.
- Recursos de falsificação de domínio em 20.000 organizações legítimas.
- Bypass de segurança por email, permitindo altas taxas de sucesso de entrega.
- Erros administrativos em potencial ou compromissos de conta de registrador maliciosos.
- CONVOLVENÇÃO COMPLETA DE MECANISMOS DE PROTEÇÃO DE ANTI-SPAM.

Os registros SPF configurados corretamente devem especificar servidores de email autorizados e negar remetentes não autorizados usando a sintaxe como “v = spf1 incluem: exemplo.com -all”.

No entanto, os domínios comprometidos usados ??”v = spf1 incluem: exemplo.com +all”, que permite que qualquer servidor envie e -mails falsificados que aparecem legítimos aos servidores de correio do destinatário.

Essas configurações incorretas podem resultar de erros administrativos acidentais ou modificações maliciosas por atores de ameaças com acesso à conta do registrador.

Independentemente da origem, a conseqüência permite operações maciças de falsificação por e-mail que ignoram as proteções tradicionais anti-spam e aumentam as taxas de sucesso de entrega de carga útil maliciosa.

Implicações e recomendações defensivas

Essa descoberta ressalta a sofisticação em evolução das operações de botnet e a importância crítica do gerenciamento de configuração DNS adequado.

A combinação de infraestrutura de roteador comprometida e equívocas de DNS criou uma tempestade perfeita, permitindo que a distribuição de malware em larga escala com probabilidade reduzida de detecção.

As organizações devem auditar imediatamente seus registros DNS SPF para garantir a configuração adequada e revisar regularmente as configurações de segurança do dispositivo, principalmente os roteadores e equipamentos de rede voltados para a Internet.

A campanha demonstra como os erros de configuração aparentemente menores podem permitir grandes violações de segurança e enfatizar a necessidade de monitoramento abrangente de segurança nos sistemas de gerenciamento de rede e de gerenciamento de DNS.

A natureza contínua dessa ameaça requer vigilância sustentada, pois a infraestrutura de botnet identificada permanece capaz de apoiar várias atividades maliciosas além das campanhas observadas do MALSPAM.

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