TLP: CLEAR

BOLETIM DE SEGURANÇA

Dispositivos MikroTik e domínios web no centro de uma nova botnet

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 SEGMENTO DE MERCADO

Os segmentos de mercado potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Provedores de Serviços de Internet (ISPs)*
- *Empresas de Logística e Transporte*
- *Setor Financeiro*
- *Comércio Eletrônico e Varejo*
- *Setor de Tecnologia da Informação e Comunicações (TIC)*

2.2 IMPACTO FINANCEIRO POTENCIAL

- *Aumento dos custos com recursos em infraestrutura e mitigação de ataques*
- *Perdas financeiras por roubo de dados e movimentação lateral em redes*
- *Custos com resposta a incidentes e forense digital*

2.3 OBJETIVO DA AMEAÇA

A ameaça descrita nesta relatório visa explorar uma configuração incorreta de DNS em dispositivos MikroTik para distribuir malware por meio de uma botnet. Os atacantes utilizam um erro de digitação na configuração do DNS para redirecionar o tráfego da Internet para servidores maliciosos, permitindo a entrega de cargas úteis maliciosas com o objetivo final de comprometer dispositivos e integrá-los à botnet para atividades maliciosas, como roubo de dados e ataques DDoS.

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

Uma botnet composta por 13.000 dispositivos **MikroTik** tem explorado entradas **SPF mal configuradas** para espalhar malware. Esses dispositivos são utilizados para contornar proteções de e-mail, aproveitando o nome de aproximadamente 20.000 domínios para o envio de mensagens maliciosas. A estratégia baseia-se na exploração de configurações inadequadas nos registros SPF dos DNS, permitindo o envio não autorizado de e-mails. A ameaça utiliza dispositivos MikroTik configurados como proxies **SOCKS4**, facilitando diversas atividades maliciosas, como mascaramento de tráfego, ataques DDoS e exfiltração de dados. A estrutura da botnet aproveita vulnerabilidades conhecidas em dispositivos MikroTik, incluindo falhas de autenticação e exploração de portas expostas, como a porta 8291, para comprometer dispositivos adicionais.

Além disso, a configuração de proxies permite que os operadores ocultem a origem do tráfego, tornando as operações mais difíceis de rastrear. A botnet demonstra uma capacidade significativa de escalabilidade, utilizando ferramentas automatizadas para expandir sua rede, comprometendo outros dispositivos vulneráveis e garantindo persistência nos ambientes afetados. A botnet também apresenta uma versatilidade impressionante em suas operações, sendo utilizada para diversos fins maliciosos, como o envio massivo de campanhas de phishing, fraudes por cliques e roubo de credenciais. Ao operar como uma rede de dispositivos comprometidos, ela proporciona aos agentes maliciosos a infraestrutura necessária para executar ataques complexos e coordenados, enquanto utiliza os dispositivos MikroTik para maximizar a eficiência e o impacto dessas ações. Essa abordagem permite que diferentes etapas da cadeia de ataque sejam realizadas de forma distribuída e discreta, dificultando a detecção e a interrupção da operação como um todo.

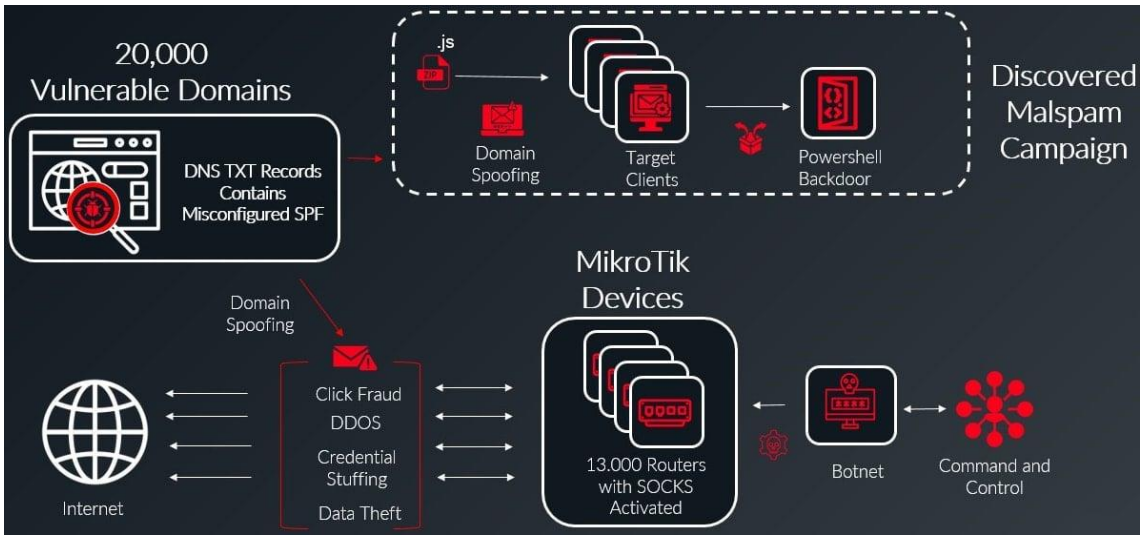

Figura 1 – Visão geral da operação da botnet

3.2 VULNERABILIDADES EXPLORADAS

A botnet MikroTik explorou uma série de vulnerabilidades e configurações inadequadas para comprometer milhares de dispositivos e viabilizar suas operações maliciosas. Entre as principais fraquezas identificadas, destaca-se o uso generalizado de **credenciais administrativas padrão**, como o usuário "admin" com senha vazia. Embora versões recentes do RouterOS tenham introduzido notificações para alterar essas configurações, uma grande quantidade de dispositivos continua exposta devido à negligência em adotar práticas básicas de segurança. Outro ponto crítico foi a ampla exposição de interfaces de gerenciamento, como Webfig e Winbox, e o uso de portas vulneráveis, como a 8291. Essas portas foram frequentemente exploradas por ataques de força bruta, permitindo que os atacantes obtivessem controle remoto dos dispositivos. Além disso, versões desatualizadas do RouterOS, particularmente as anteriores à 6.49.8, apresentavam a vulnerabilidade CVE-2023-30799, que possibilitava a escalada de privilégios de administradores para superadmin. Esse acesso irrestrito permitiu a execução de comandos arbitrários e o uso dos roteadores como parte da infraestrutura maliciosa.

Paralelamente, a botnet também se aproveitou de configurações permissivas nos registros DNS SPF de aproximadamente 20.000 domínios. A utilização da opção +all nesses registros permitiu que os atacantes enviassem e-mails fraudulentos em nome desses domínios, contornando mecanismos de proteção de e-mail e facilitando a disseminação de malware em campanhas de malspam. Essa abordagem não apenas aumentou a eficácia dos ataques, mas também dificultou sua detecção.

3.3 Operação e Capacidade da Ameaça

A operação da botnet composta por dispositivos MikroTik demonstra uma capacidade avançada de execução de atividades maliciosas em larga escala, explorando não apenas vulnerabilidades técnicas, mas também configurações inadequadas de segurança. Essa ameaça é capaz de comprometer infraestruturas críticas por meio de campanhas de malspam, ataques DDoS, exfiltração de dados e mascaramento de tráfego, o que dificulta a detecção e a mitigação. A capacidade de configurar dispositivos comprometidos como proxies SOCKS4 amplia significativamente o alcance das operações, permitindo que os atacantes ocultem suas ações e utilizem a botnet para diversos fins, como envio de phishing, fraudes por cliques e roubo de credenciais. Além disso, a exploração de registros DNS SPF mal configurados evidencia a habilidade dos operadores em manipular sistemas externos para contornar proteções de e-mail e maximizar o impacto de suas campanhas. A escalabilidade da botnet é outro fator crucial, pois a automação dos processos de exploração e comprometimento permite a rápida expansão da rede de dispositivos sequestrados. Essa capacidade de integrar novos dispositivos, independentemente da versão do firmware ou da complexidade das proteções existentes, reforça a ameaça como uma das mais abrangentes e difíceis de combater no cenário atual.

3.4 Tabela MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Initial Access	T1133 External Remote Services	Os atacantes exploram serviços remotos mal configurados nos dispositivos MikroTik para obter acesso inicial.
Execution	T1204.001 User Execution: Malicious Link	Os invasores induzem vítimas a clicar em links maliciosos que levam ao comprometimento.
Persistence	T1098 Account Manipulation	Criação ou modificação de configurações para manter o controle dos dispositivos.
Defense Evasion	T1562.001 Impair Defenses: Disable or Modify Tools	Os atacantes desativam mecanismos de segurança para evitar detecção.
Command and Control	T1071.004 Application Layer Protocol: DNS	Uso de DNS para comunicação com os servidores de comando e controle (C2).

Tabela 1 – Tabela MITRE ATT&CK

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento listados, podem ser adotadas medidas para mitigar o impacto e prevenir a exploração dos dispositivos MikroTik e de registros DNS mal configurados, como por exemplo:

Aplicar atualizações de firmware imediatamente

- Certifique-se de que todos os dispositivos MikroTik estejam rodando a versão mais recente do RouterOS, idealmente 6.49.8 ou uma versão estável da série 7.x, conforme indicado pela documentação oficial.

Alterar credenciais padrão

- Remova o usuário administrativo padrão “admin” e configure novos usuários com senhas fortes e únicas. Isso reduz drasticamente o risco de comprometimento por ataques de força bruta.

Restringir o acesso remoto

- Desative o acesso às interfaces Webfig e Winbox pela internet e restrinja o gerenciamento dos dispositivos a redes internas ou específicas, utilizando listas de controle de acesso (ACL).

Configurar corretamente registros DNS SPF

- Revise os registros SPF de todos os domínios gerenciados para garantir que a opção configurada seja “-all” em vez de “+all”, limitando o envio de e-mails apenas a servidores autorizados.

Monitorar portas expostas

- Verifique regularmente dispositivos expostos em portas críticas, como a 8291, e considere bloquear essas portas em firewalls sempre que possível, permitindo apenas conexões essenciais.

Implementar autenticação robusta

- Configure dispositivos para exigir autenticação multifator (MFA) sempre que disponível e desabilite métodos de autenticação vulneráveis, como senhas simples.

Realizar auditorias regulares de segurança

- Monitore logs de dispositivos para identificar atividades suspeitas, como tentativas repetidas de login, e verifique a integridade das configurações periodicamente para identificar alterações não autorizadas.

5 OPERACIONAL

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

5.1 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de IPs e Domínios	
IP	62.133.60[.]137

Tabela 2 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Bleepingcomputer**
- **VulnCheck**
- **InfoBlox**
- **NVD**

7 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH