

Relatório de Threat Intelligence – Hash de Arquivo

4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7

Fonte dos dados: VirusTotal, AlienVault OTX, URLHaus, YARAify, Malware Bazaar, Hybrid Analysis, Threat Fox. **Timestamp da Análise:** 2026-02-17T13:27:24.442712.

1. Resumo Executivo

O arquivo com hash [4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7](#) é um executável malicioso ELF para a arquitetura MIPS (dispositivos IoT/embarcados Linux), amplamente detectado como uma variante das famílias de botnets **Mozi** e **Mirai**. A ameaça apresenta detecção massiva (49/72 motores no VirusTotal) e está ativamente associada a campanhas de recrutamento de botnets para ataques DDoS e exploração de vulnerabilidades. A análise de comportamento revela técnicas sofisticadas de evasão (packer UPX modificado, detecção de sandbox), persistência agressiva (modificação de serviços `systemd` e `rc.local`), comunicação C2 criptografada e tentativas de roubo de credenciais de metadados de nuvem. Os indicadores de comprometimento (IOCs) são abundantes e vinculam o arquivo a uma extensa infraestrutura de distribuição global, com centenas de milhares de URLs e IPs maliciosos, principalmente na Ásia. O risco é classificado como **ALTO**, representando uma ameaça operacional persistente para dispositivos Linux e IoT expostos.

2. Análise de Comportamento

Fonte	Evidência	Interpretação
VirusTotal (Detecção)	49/72 motores marcam como malicioso. Reputação: -210. Famílias: Trojan.Linux.Mirai , Backdoor.Linux.Mozi .	Consenso elevado na comunidade de antivírus sobre a natureza maliciosa do artefato, associando-o a botnets de IoT conhecidas.
VirusTotal (Comportamento)	Comunicação HTTPS com IPs suspeitos (ex: 185.125.188.59). Tentativa de conexão com endpoint de metadados da nuvem (169.254.169.254:80). Parada de serviço <code>snapd.socket</code> .	Padrão claro de C2 e coleta de informações sensíveis. Comportamento de desabilitação de serviços de segurança/atualização para estabelecer controle.
VirusTotal (Zenbox/ATT&CK)	Táticas mapeadas: Defense Evasion (T1027 - UPX packing), Discovery (T1518.001 - detecção de software de segurança), Persistence (criação de serviços <code>systemd</code>), Command and Control (T1071.001 - HTTPS).	Malware evasivo que busca se entrincheirar no sistema, coletar informações do ambiente e estabelecer canal de comunicação persistente com atacantes.

Fonte	Evidência	Interpretação
AlienVault OTX	Associado a 50+ <i>Pulses</i> . Vinculado a campanhas ativas de força bruta SSH e Apache. Fontes como MalwarePatrol o listam em feeds diários.	O artefato está em uso ativo por atores de ameaça, sendo distribuído em campanhas de exploração e comprometimento inicial.
URLHaus	Mais de 720 mil URLs de distribuição associadas, muitas ainda online. IPs de hospedagem primariamente na China (ex: 61.53.81.9 , 115.48.36.132).	Infraestrutura de distribuição massiva e resiliente, indicando uma operação de botnet madura e de larga escala.
Hybrid Analysis	Erros consistentes de análise (FILE_TYPE_BAD_ERROR) em múltiplos SOs. 1510 tentativas de análise falhadas.	Forte indicativo de técnicas anti-análise e ofuscação deliberada para impedir a detecção dinâmica em sandboxes.
Outras Fontes	(Malware Bazaar) Nome comum: Mozi.m . (YARAify) Ativo desde fev/2023. Packer UPX "patched".	Confirma a associação específica à botnet Mozi e a evolução contínua do malware para evitar detecção estática.

Táticas/Procedimentos (ATT&CK) Observados:

- T1027 – Obfuscated Files or Information:** Empacotado com UPX modificado ("patched").
- T1518.001 – Software Discovery:** Chama `uname` e lê `/proc` para identificar o ambiente.
- T1543.002 – Create or Modify System Process (`systemd`):** Cria ou modifica serviços `systemd` para persistência.
- T1071.001 – Application Layer Protocol (HTTP/HTTPS):** Comunicação C2 via HTTPS em portas diversas.
- T1573 – Encrypted Channel:** Uso de HTTPS para ofuscar a comunicação.
- T1110 – Brute Force:** Associado a campanhas de força bruta SSH (conforme OTX).
- T1486 – Data Encrypted for Impact:** Vinculado a campanhas de ransomware em *pulses* relacionados.
- T1595 – Active Scanning:** Comportamento de varredura de rede típico do Mirai/Mozi.

3. Informações de Campanha Associada

Campo	Valor
Nome de Arquivos	Mozi.m , bin.sh , 115.50.4.8257595 (IP embutido no nome)
Tipo	Executável (ELF)
Obfuscation	Packer UPX modificado/remendado ("patched UPX")
Classe	Botnet, Backdoor, DDoS Trojan
Grupo/Família	Mozi (derivado da família Mirai)

Campo	Valor
Alvo	Dispositivos IoT (roteadores, câmeras IP, DVRs) e servidores Linux com credenciais fracas ou vulnerabilidades não corrigidas.
Localização	Distribuição global, com forte concentração de infraestrutura na Ásia (especialmente China).
Objetivos	Recrutamento de dispositivos para uma botnet (zumbificação) para realização de ataques de Negação de Serviço Distribuído (DDoS), mineração de criptomoedas, exfiltração de dados e propagação lateral.

4. Domínios e IPs Relacionados

A ameaça está associada a uma vasta infraestrutura. Abaixo, os IOCs mais críticos e recorrentes:

- **IPs de Comando e Controle (C2) e Distribuição:**
 - 185.125.188.59:443 (C2 via HTTPS, citado no VT)
 - 61.53.81.9 (Distribuição, citado no URLHaus)
 - 115.48.36.132 (Distribuição, citado no URLHaus)
 - 23.192.228.84, 23.215.0.136, 23.215.0.138 (IPs associados em *pulses* da OTX)
- **Endpoints de Distribuição Comuns:** Padrões de URL como `/i`, `/bin.sh` em portas não padrão (ex: `:8080`, `:8443`).
- **Endereço de Metadados de Nuvem:** 169.254.169.254:80 (Alvo de tentativa de conexão para roubo de credenciais).
- **Hash Relacionados (IOCs de Arquivo):**
 - **MD5:** 59ce0babab11893f90527fc951ac69912
 - **SHA1:** 5857a7dd621c4c3ebb0b5a3bec915d409f70d39f
 - **Nomes suspeitos:** Qualquer arquivo nomeado `Mozi.m`, `bin.sh`, ou contendo padrões de IP como nome (ex: `[IP].[PORTA]`).

Observação: A lista completa de IOCs (milhares de URLs e IPs) está disponível nos *pulses* do AlienVault OTX e no banco de dados do URLHaus associados a este hash.

5. Recomendações de Ações de Investigação

1. **Bloqueio Proativo de IOCs:** Implemente bloqueios imediatos em firewalls, proxies e soluções de segurança de endpoint para os IPs de C2 e distribuição listados, bem como para os hashes de arquivo conhecidos (SHA256, MD5).
2. **Threat Hunting em Dispositivos Linux/IoT:** Busque ativamente nos ativos de rede por:
 - Processos com os nomes suspeitos (`Mozi.m`, `bin.sh`).
 - Conexões de saída para as portas e IPs listados.
 - Modificações suspeitas em arquivos de inicialização (`/etc/rc.local`, `/etc/init.d/`) ou criação de novos serviços `systemd`.
 - Tentativas de acesso ao endpoint de metadados 169.254.169.254 a partir de servidores internos.
3. **Análise de Logs de Autenticação:** Revise logs de serviços expostos (SSH, Apache, outros) por tentativas massivas de força bruta, que são o vetor primário de infecção para este malware.

4. **Enriquecimento de Monitoramento:** Configure alertas no SIEM para qualquer tráfego de saída para os IPs de C2 identificados ou para padrões de comunicação HTTPS incomuns em portas altas a partir de dispositivos IoT ou servidores Linux.
 5. **Análise de Artefatos em Sandbox Corporativa:** Submeta amostras de arquivos suspeitos coletados no ambiente para análise dinâmica em sandbox, observando especificamente os comportamentos de persistência e C2 documentados.
 6. **Monitoramento de Feeds de Inteligência:** Inscreva-se ou consulte regularmente feeds de ameaças (como OTX, URLHaus) que listam IOCs relacionados às famílias Mirai e Mozi para atualizar as listas de bloqueio.
-

6. Conclusão

O arquivo analisado ([4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7](#)) é **definitivamente malicioso** e representa uma ameaça operacional de alto risco. Trata-se de um componente ativo da botnet **Mozi**, que herda e evolui as capacidades destrutivas da família **Mirai**. Sua sofisticação é evidenciada pelas técnicas de evasão, persistência agressiva e pela infraestrutura de distribuição massiva e resiliente.

A ameaça é projetada para transformar dispositivos comprometidos em zumbis sob o controle de um operador malicioso, primariamente para a realização de ataques DDoS em larga escala. A persistência da atividade ao longo de anos e a associação constante a campanhas ativas de exploração demandam que organizações com ativos Linux e IoT expostos tratem este indicador com máxima prioridade, implementando as ações de investigação e contenção recomendadas.