Relatório de Threat Intelligence – Hash de Arquivo `58968266f92ea06e3f064e23e58d689cc9d6841082581e06876d36d4a14228ca`

> **Fonte dos dados**: VirusTotal, AlienVault OTX, URLHaus, YARAify, Malware Bazaar, Hybrid Analysis, Threat Fox. **Timestamp da Análise**: 2026-02-14T13:06:00.874453.

1. Resumo Executivo

O arquivo com hash SHA-256 `58968266f92ea06e3f064e23e58d689cc9d6841082581e06876d36d4a14228ca` é um executável ELF 32-bit malicioso para sistemas Linux/embarcados, identificado como pertencente à família de malware **Mirai/Gafgyt/BASHLITE**. Está ativamente associado a campanhas de botnet voltadas para dispositivos IoT, com o objetivo principal de recrutar dispositivos vulneráveis para formar redes de bots usadas em ataques de Negação de Serviço Distribuído (DDoS) e execução remota de comandos. Foi detectado por múltiplos motores de antivírus (33/76 no VirusTotal) e catalogado em feeds de inteligência como MalwareBazaar e URLhaus. Os comportamentos observados incluem ofuscação de comunicação, tentativas de persistência e funcionalidades de backdoor. Os principais Indicadores de Comprometimento (IOCs) são o próprio hash, os nomes de arquivo evasivos (`s-h.4-.dick`, `4zr6d.exe`) e os endereços de distribuição associados.

---

2. Análise de Comportamento

Fonte	Evidência	Interpretação
VirusTotal	33 detecções de 76 motores. Classificado como `Backdoor.Linux.Mirai`, `Trojan.Linux.Gafgyt`. Reputação negativa (-11).	Confirmação sólida de maliciosidade por engines consolidadas. O arquivo é um backdoor conhecido para IoT.
AlienVault OTX	Incluído no pulse "Malware | Feb 15, 2026" com 576 hashes relacionados. Tags: `malwarebazaar`.	Indica que o hash faz parte de uma coleção ampla de malware ativo, compartilhada pela comunidade de inteligência.
URLHaus	Arquivo classificado como **Mirai**. URLs de distribuição: `http://16.171.140.194/s-h.4-.dick` e `http://definitely-not.gay/s-h.4-.dick`.	Confirma a natureza de botnet e fornece IOCs de infraestrutura de distribuição (URLs e IP).
YARAify	Detectado por múltiplas regras YARA para famílias **Mirai, Torii, Gafgyt**. Strings XORadas contendo "Mozilla/5.0".	Evidencia técnicas de ofuscação de comunicação com servidores de comando e controle (C2), padrão em botnets.

Fonte	Evidência	Interpretação
Malware Bazaar	Classificado como `Mirai/Gafgyt`. Tipo: `elf`. Primeira seen: 2026-02-15. Vínculo com URLhaus confirmado.	Corrobora a identificação da família, data de atividade recente e associação com infraestrutura de entrega.
Hybrid Analysis	Veredito: **Malicious**. Família: `Trojan[Backdoor]/Linux.Gafgyt`. Vinculado ao IP `16.171.140.194`.	Análise comportamental suplementar que classifica o arquivo como backdoor e associa a um IP malicioso.
Threat Fox	Consulta sem resultados (`no_result`).	A ausência nesta fonte específica não descarta a maliciosidade, amplamente atestada por outras.

Comportamentos Maliciosos Identificados:

- **Backdoor / Botnet:** O arquivo fornece funcionalidades de backdoor, permitindo controle remoto do dispositivo infectado e sua integração a uma rede de bots (botnet).
- **Comunicação com C2:** Utiliza protocolos de rede (possivelmente HTTP/DNS) para se comunicar com servidores de comando e controle, com strings ofuscadas para evitar detecção.
- **Propagação e Ataques DDoS:** Típico da família Mirai, o malware pode escanear e explorar vulnerabilidades em outros dispositivos para propagação e é utilizado para lançar ataques de negação de serviço.

Táticas/Procedimentos (MITRE ATT&CK) Observados:

- **T1071.001 – Application Layer Protocol: Web Protocols:** Uso de HTTP para download do payload e comunicação C2.
- **T1027 – Obfuscated Files or Information:** Ofuscação de strings (ex: "Mozilla/5.0") via XOR.
- **T1095 – Non-Application Layer Protocol:** Potencial uso de protocolos raw socket para ataques DDoS.
- **T1583.001 – Acquire Infrastructure: Virtual Private Server:** Utilização de servidores (IP `16.171.140.194`) para hospedagem do payload.
- **T1547.013 – Boot or Logon Autostart Execution: Unix Shell Configuration Modification:** Regras Yara sugerem tentativas de persistência via arquivos de shell.

---

3. Informações de Campanha Associada

Campo	Valor
Nome de Arquivos	`s-h.4-.dick`, `4zr6d.exe`
Tipo	Executável (ELF 32-bit LSB)
Classe	Botnet, Backdoor, DDoS Trojan
Grupo/Família	Mirai / Gafgyt / BASHLITE
Alvo	Dispositivos Linux embarcados e servidores (especialmente IoT com credenciais padrão ou vulnerabilidades conhecidas)

Campo	Valor
Localização	Infraestrutura de distribuição global (IPs associados a diversos provedores).
Objetivos	Recrutamento de dispositivos para botnet, execução de ataques DDoS, execução remota de comandos.

4. Domínios e IPs Relacionados (IOCs)

- **URLs de Distribuição:**
  - `http://16.171.140.194/s-h.4-.dick`
  - `http://definitely-not.gay/s-h.4-.dick`
- **Endereço IP Malicioso:**
  - `16.171.140.194`
- **Hashes Relacionados (Exemplos do Pulse OTX):** O hash analisado está contido em um pulse com 576 hashes semelhantes, indicando uma coleção ampla de amostras da mesma campanha ou família.

---

5. Recomendações de Ações de Investigação

1. **Bloqueio Proativo:** Adicione o hash SHA-256 `58968266f92ea06e3f064e23e58d689cc9d6841082581e06876d36d4a14228ca` e os IOCs relacionados (URLs, IP `16.171.140.194`) às listas de bloqueio em ferramentas de segurança (EDR, antimalware, firewall, proxies).
2. **Threat Hunting em Redes IoT/Embarcadas:** Procure por tráfego de rede incomum (escanes, tentativas de login em massa em portas SSH/Telnet) originado de dispositivos Linux internos, especialmente para os IPs e URLs listados.
3. **Busca por Artefatos:** Em ambientes Linux críticos, busque por arquivos com os nomes `s-h.4-.dick` ou `4zr6d.exe`, ou por processos suspeitos consumindo recursos de rede de forma anômala.
4. **Análise de Logs de Firewall/Proxy:** Revise os logs para identificar tentativas de acesso ou download a partir dos URLs maliciosos mencionados.
5. **Enriquecimento de IOC:** Consulte o IP `16.171.140.194` em feeds de ameaças para identificar outras campanhas ou malwares associados, determinando seu ASN e histórico de maliciosidade.
6. **Monitoramento de Sub-redes Vulneráveis:** Como o Mirai explora credenciais padrão, verifique a existência de dispositivos IoT com senhas fracas ou não alteradas na rede.

---

6. Conclusão

O arquivo analisado é **definitivamente malicioso**, representando uma ameaça concreta e ativa para ambientes baseados em Linux, particularmente dispositivos IoT e servidores embarcados. Sua associação comprovada à família de botnets Mirai/Gafgyt o classifica como um risco de **alto impacto**, com potencial para causar interrupções de serviço via DDoS e comprometer a segurança de redes internas. Recomenda-se tratá-lo com prioridade alta, implementando as ações de bloqueio e investigação recomendadas, dada sua natureza de propagação automática e uso em campanhas criminosas.