



# Relatório De Pesquisas WEB Exploitation

A ilusão do Arquivo Seguro – Análise da

**CVE-2023-38831**

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!



Acesse as análises produzidas pela ISH Tecnologia sobre Táticas, Técnicas e Procedimentos (TTPs) de Threat Actors, malwares emergentes, vulnerabilidades críticas e outros temas relevantes em cibersegurança. Clique na imagem abaixo para conferir nosso blog.



ISH —  
**ALERTA HEIMDALL! HTTP2 RAPID RESET, IMPACTOS E DETECÇÃO DA CVE-2023-44487**

Falhas de negação de serviço (DoS) não são apenas interrupções técnicas. Elas representam riscos reais à continuidade do negócio, à confiança dos clientes e à reputação da marca. Nisto temos a vulnerabilidade CVE-2023-44487, conhecida como HTTP/2 Rapid Reset.

[BAIXAR](#)



ISH —  
**ALERTA HEIMDALL! BABUK2 EM 2025: RETORNO LEGÍTIMO OU COPYCAT ESTRATÉGICO**

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, temos o ransomware Babuk2.

[BAIXAR](#)



ISH —  
**ALERTA HEIMDALL! A ANATOMIA DO RANSOMWARE AKIRA E SUA EXPANSÃO MULTIPLATAFORMA**

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e ganhando bastante popularidade. Nesse contexto, temos o ransomware Akira.

[BAIXAR](#)

## SUMÁRIO

Introdução EXECUTIVA .....	5
1 ESTRATÉGICO .....	5
1.1 Introdução sobre a vulnerabilidade.....	5
1.2 Vitimologia e Ataque .....	6
1.3 Inteligência Complementar .....	6
2 TÁTICO .....	7
2.1 Mapeamento de Exposição e Modus Operandi .....	7
3 Operacional .....	8
3.1 Sequência de Exploração .....	8
3.2 Recomendações .....	8
MITRE ATT&CK - TTPS .....	9
4 Conclusão .....	9
Referências .....	10
Autores.....	10

## LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK. ....	9
--------------------------------------	---

## LISTA DE FIGURAS

Figura 1 - EPSS Score .....	5
Figura 2 - Inclusão KEV CISA .....	6

# 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.

## 1 ESTRATÉGICO

### 1.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

A **CVE-2023-38831** é uma falha lógica crítica de Execução Remota de Código (RCE) no software de compactação **WinRAR (versões anteriores à 6.23)**. A vulnerabilidade surge de uma divergência na forma como o software processa nomes de arquivos que contêm espaços em branco e pastas com nomes idênticos dentro de um arquivo compactado (ZIP ou RAR).

Diferente de *buffer overflows* complexos, esta falha permite que um atacante execute código arbitrário no momento em que a vítima clica para abrir um arquivo aparentemente inofensivo (como uma imagem .JPG ou um documento .PDF) dentro da interface do **WinRAR**.



Figura 1 - EPSS Score

A CVE em questão, também foi incluída nos alertas de vulnerabilidades exploradas - **Known Exploited Vulnerabilities (KEV)** da **CISA** o que implica em uso da mesma em campanhas maliciosas, com um crescente **aumento no seu EPSS (Exploit**

*Prediction Scoring System*) visto no mês de julho de 2025 como podemos visualizar nas imagens disponibilizadas com ajuda do [cvefind](#).

### **CISA KEV (Known Exploited Vulnerabilities)**

**Vulnerability name :** RARLAB WinRAR Code Execution Vulnerability

**Required action :** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

**Known To Be Used in Ransomware Campaigns :** Known

**Added :** 2023-08-23 22h00 +00:00

**Action is due :** 2023-09-13 22h00 +00:00

Figura 2 - Inclusão KEV CISA

## 1.2 VITIMOLOGIA E ATAQUE

Devido à onipresença do *WinRAR* em ambientes corporativos e domésticos, a superfície de ataque é massiva.

- **Setor Financeiro e Traders:** Historicamente, os primeiros vetores de ataque observados focaram em fóruns de investimento, disfarçando *payloads* como planilhas e documentos de estratégia financeira.
- **Ambientes Corporativos:** O vetor de entrada via e-mail (*Phishing*) com anexos maliciosos torna qualquer colaborador com o software desatualizado um ponto de entrada potencial para *Ransomware* e *Infostealers*.

## 1.3 INTELIGÊNCIA COMPLEMENTAR

A vulnerabilidade possui alta criticidade pois já foi observada sendo explorada *in-the-wild* (em ambiente real) por diversos grupos de ameaça (*Threat Actors*) antes mesmo da divulgação pública do patch, classificando-a como um *0-day* na época de sua descoberta. Grupos como **DarkCasino** e **APT's patrocinados por estados** já incorporaram esse *exploit* em seus arsenais.

## 2 TÁTICO

---

### 2.1 MAPEAMENTO DE EXPOSIÇÃO E MODUS OPERANDI

A análise tática revela que o sucesso da CVE-2023-38831 depende fortemente de Engenharia Social combinada com ofuscação técnica. O atacante não precisa de acesso prévio à rede; ele precisa apenas que o arquivo chegue ao *endpoint* e seja aberto pelo WinRAR.

Elementos Chave:

- **Spoofing de Extensão:** O ataque é eficaz porque a interface *do WinRAR* esconde a verdadeira natureza do arquivo executável, mostrando ao usuário apenas o ícone e a extensão do arquivo "isca" (ex: `relatorio.pdf`).
- **Evasão de Análise Estática:** Como o arquivo compactado em si não está corrompido (é um arquivo RAR estruturalmente válido), muitas soluções de *gateway* de e-mail e antivírus tradicionais podem falhar na detecção inicial, vendo apenas arquivos compactados contendo imagens ou textos.
- **Persistence:** Frequentemente, após a execução inicial, o *script* malicioso instala mecanismos de persistência (como chaves de registro *Run*) para manter o acesso mesmo após o fechamento do *WinRAR*.

## 3 OPERACIONAL

---

### 3.1 SEQUÊNCIA DE EXPLORAÇÃO

A mecânica do ataque abusa de uma falha de "Path Confusion" (Confusão de Caminho).

1. **Estruturação:** O atacante cria uma estrutura de pastas onde existe um arquivo isca (ex: nota\_fiscal.pdf com um espaço no final) e uma pasta com o mesmo nome (nota\_fiscal.pdf/). Dentro desta pasta, reside o executável malicioso (.cmd, .bat ou .exe).
2. **Interação:** Quando o usuário clica duas vezes no arquivo isca na interface do WinRAR, o software tenta processar o arquivo.
3. **O "Glitch":** Devido ao espaço em branco no nome, o WinRAR se confunde e, em vez de abrir apenas o PDF, ele varre a pasta de mesmo nome e executa o conteúdo executável que estiver lá dentro.
4. **Execução:** O *script* do atacante roda, muitas vezes abrindo o documento original (para não levantar suspeitas) enquanto, em segundo plano, baixa e executa o *malware* final (Beacon, RAT, etc.).

### 3.2 RECOMENDAÇÕES

Diante da facilidade de exploração da **CVE-2023-38831**, a atualização é **mandatória e urgente**.

- **Atualização de Software:** Atualizar imediatamente o **WinRAR para a versão 6.23 ou superior**, onde a lógica de tratamento de caminhos foi corrigida.
- **Bloqueio de Extensões:** Caso o update não seja possível no momento tentar ao máximo bloquear o recebimento de arquivos compactados (.rar, .zip) diretamente por e-mail, forçando o uso de links de compartilhamento gerenciados.

- **Educação do Usuário:** Treinar colaboradores para desconfiarem de arquivos compactados que solicitam senhas ou que venham de fontes desconhecidas, mesmo que pareçam conter PDFs ou imagens.
- **Monitoramento EDR:** Configurar alertas para processos filhos suspeitos (como cmd.exe, powershell.exe) originados pelo processo pai winrar.exe.

## MITRE ATT&CK - TTPS

Este tópico apresenta as **TTPs** identificadas 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
Execution	<b>T1204</b> - <i>User Execution: Malicious File</i>	O usuário executa o código ao abrir o arquivo isca no Winrar
Defense Evasion	<b>T1027.004</b> – <i>Obfuscated Files or Information: Fileless Storage</i>	Uso da estrutura de pastas para ocultar o script real.

Tabela 1 – Tabela MITRE ATT&CK.

## 4 CONCLUSÃO

A exploração da **CVE-2023-38831** representa um marco na evolução das ameaças que visam o usuário final, demonstrando que vulnerabilidades lógicas em softwares de produtividade podem ser tão prejudiciais quanto falhas complexas em sistemas operacionais. A eficácia desta técnica reside na subversão de um hábito comum e aparentemente seguro: a visualização de documentos dentro de arquivos compactados.

## REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- CTI Purple Team *by* ISH Tecnologia
- [MITRE ATT&CK](#)
- [NVD - CVE-2023-38831](#)
- [CVEFIND – CVE-2023-38831](#)

## AUTORES

---

- Lucas Andrade – Security Researcher



heimdall  
security research

A DIVISION OF ISH