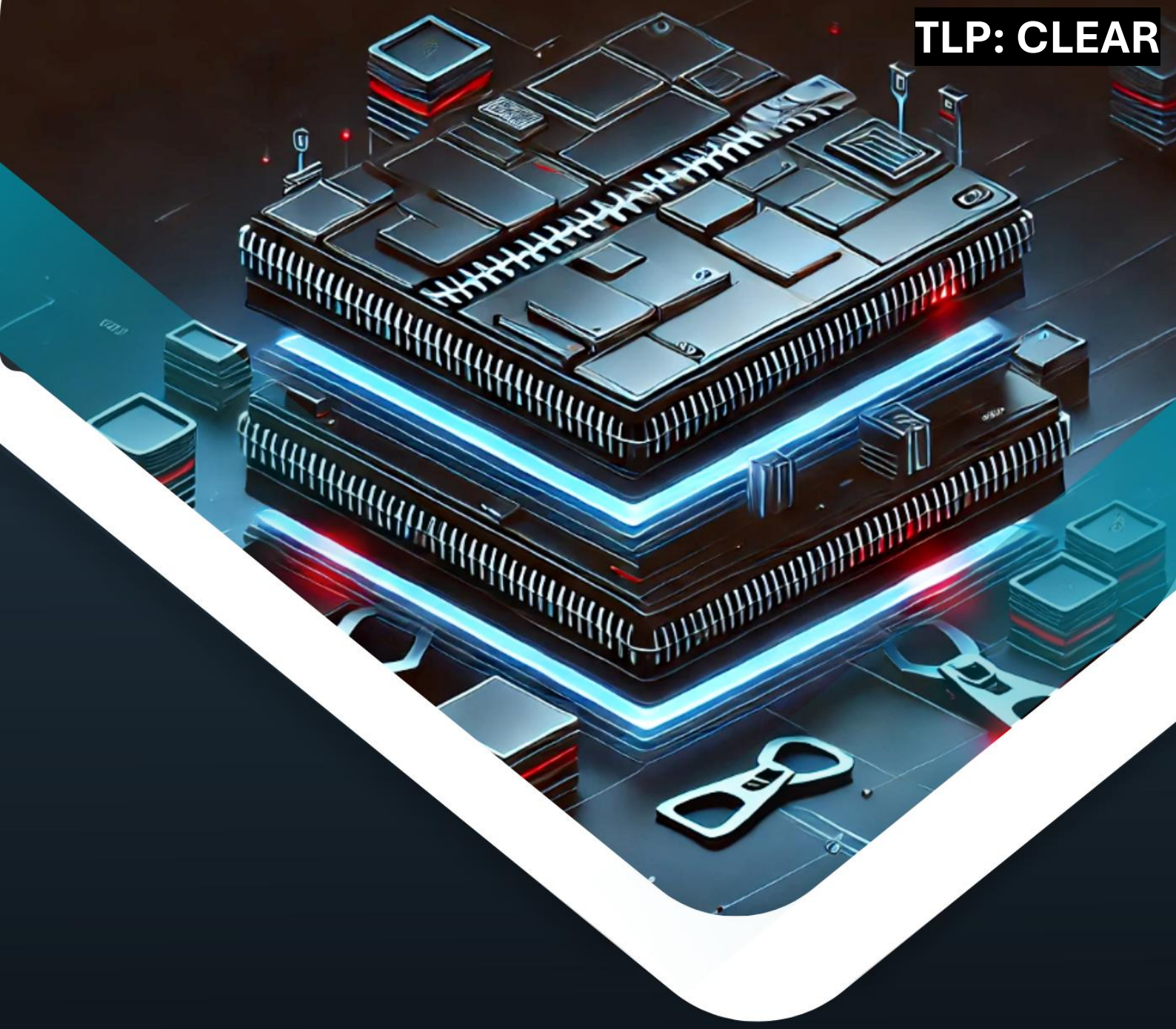
TLP: CLEAR



RELATÓRIO DE PESQUISAS

WinRAR: Um Vetor silencioso de comprometimento em ambientes corporativos

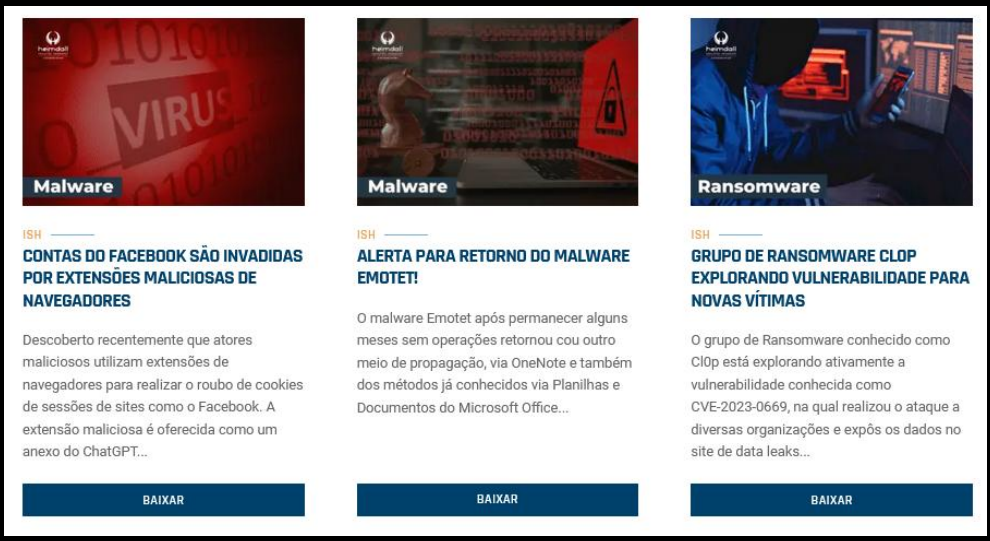
heimdall
security research

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

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência **Heimdall da ISH Tecnologia**, 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 INTRODUÇÃO SOBRE A AMEAÇA

A exploração de vulnerabilidades no **WinRAR**, especialmente as falhas **CVE-2023-38831**, **CVE-2023-40477**, **CVE-2024-33899** e o recente **CVE-2025-8088**, consolidou-se como um dos vetores de entrada preferenciais tanto por **cibercriminosos** quanto por **atores estatais (APT)** ao longo dos últimos anos.

O fator crítico reside no comportamento natural dos usuários: arquivos compactados são vistos como itens inofensivos e rotineiros, utilizados em processos corporativos legítimos (RH, financeiro, contratos, auditoria, logística, engenharia etc.). Isso cria um cenário ideal para operações maliciosas fundamentadas em **engenharia social**, onde o simples ato de visualizar um arquivo dentro de um **.zip/.rar** pode desencadear a execução de código sem o conhecimento da vítima.

A ameaça assume caráter estratégico por três pilares principais:

1. **Alcance global e transversal**
   - O WinRAR possui base instalada gigantesca e heterogênea. Isso aumenta exponencialmente a superfície de ataque.
2. **Persistência do risco**
   - O WinRAR não possui atualização automática, fazendo com que versões vulneráveis permaneçam operacionais por anos, mesmo após a divulgação de patches.
3. **Adoção por atores sofisticados**
   - Atores governamentais integraram o vetor de exploração em campanhas direcionadas de espionagem, enquanto grupos de crime organizado utilizam a técnica para fraudes financeiras e roubo de credenciais em massa.

Assim, a ameaça transcende o nível técnico e se caracteriza como um risco estratégico para a continuidade de negócios, afetando confidencialidade, integridade e disponibilidade de ativos críticos.

2.2 VITIMOLOGIA E SEGMENTOS AFETADOS

A exploração das vulnerabilidades do WinRAR afeta **múltiplos setores**, mas os mais sensíveis apresentam padrões claros de vitimização. As campanhas observadas indicam dois grandes blocos:

Setores preferencialmente alvejados por Atores Estatais (APT)

Esses grupos utilizam o WinRAR para obter acesso estratégico visando espionagem, comprometimento prolongado e exfiltração de dados confidenciais.

Setor	Motivo do Interesse
Governo/ Defesa/ Relações Exteriores	Obtenção de inteligência estratégica, roubo de documentos e monitoramento de decisões políticas.
Energia, Petróleo e Gás	Interesse em infraestrutura crítica e informações de capacidade energética.
Manufatura e Aeroespacial	Furto de propriedade intelectual, segredos de engenharia e protótipos.
Think Tanks e ONGs Internacionais	Coleta de informação geopolítica e influência narrativa.
Fornecedores da cadeia de suprimentos	Alvos indiretos para pivotamento e infiltração lateral.

Tabela 1 – Setores alvos e motivos de interesses APT's.

Setores prediletos por Cibercriminosos e Grupos Financeiros

Esses operadores focam em **ganho financeiro**, usando as falhas do WinRAR para instalar infostealers, RATs e backdoors com alto potencial de **fraude.**

Setor	Motivo do Interesse
Financeiro/ Bancário/ Trading	Roubo de credenciais, contas de corretoras, carteiras digitais e manipulação de transações.
E-commerce e varejo	Furto de dados de cartão, credenciais administrativas e acesso a gateways de pagamento.
Tecnologia e SaaS	Comprometimento de credenciais privilegiadas e movimentação lateral para outros clientes.
Saúde	Acesso a dados sensíveis e extorsão por ransomware.
Educação e Pesquisa	Pontos vulneráveis utilizados como salto para entidades de maior valor.

Tabela 2 – Setores alvos e motivos de interesses Cibercrminosos.

2.3 IMPACTO ESTRATÉGICO NA ORGANIZAÇÃO AFETADA

A exploração do WinRAR compromete diretamente:

- **Confidencialidade**: roubo de credenciais, documentos, propriedade intelectual.
- **Integridade**: adulteração de informações financeiras, contratos ou folhas de pagamento.
- **Disponibilidade**: casos em que o ataque culmina em ransomware ou exclusão lógica.
- **Confiança**: danos reputacionais pela exposição a espionagem ou fraudes massivas.

O vetor possui alto potencial para causar prejuízo financeiro, operações fraudulentas e espionagem corporativa de longo prazo, justificando sua permanência como ameaça estratégica prioritária.

3 TÁTICO

3.1 VISÃO GERAL DO WINRAR COMO SUPERFÍCIE DE ATAQUE

O **WinRAR** é um software de compressão amplamente usado em estações Windows e outras plataformas, com suporte a RAR, ZIP, 7z, entre outros. Ele frequentemente é instalado manualmente, fora de mecanismos centralizados de gestão de software, o que:

- Dificulta o inventário;
- Prejudica o patch management;
- Faz com que versões vulneráveis permaneçam em uso por anos.

Além disso, o WinRAR possui integração profunda com o **explorador de arquivos**, atalhos e o mecanismo de execução nativo do Windows. Isso significa que falhas na lógica de extração, abertura automática de arquivos ou manipulação de metadados podem ser exploradas como vetores para executar binários, scripts ou cargas maliciosas sem interação direta do usuário. Essa combinação alta adoção, baixa governança e interação nativa com o sistema operacional torna o WinRAR um alvo recorrente em ataques que exploram arquivos compactados para movimentação lateral, persistência ou *initial access* em ambientes corporativos.

4 VULNERABILIDADES RELEVANTES NO WINRAR

4.1 CVE-2023-38831 - EXECUÇÃO DE CÓDIGO AO VISUALIZAR ARQUIVOS "BENIGNOS"

No WinRAR antes da versão 6.23 permite execução arbitrária de código quando o usuário tenta visualizar um arquivo considerado benigno dentro de um arquivo ZIP (por exemplo, uma .JPG). O arquivo ZIP pode conter:

- Um arquivo benigno (ex.: imagem.jpg)
- Uma pasta com o mesmo nome (imagem.jpg\) contendo conteúdo malicioso (ex.: *.cmd, .bat, .exe*).

Durante a tentativa de abrir apenas o arquivo benigno, o conteúdo da pasta também é processado e executado.

Impacto:

- Execução de malware (infostealers, RATs, backdoors) após um simples duplo clique em um arquivo supostamente seguro.
- Vetor altamente adequado a spear phishing e campanhas temáticas (documentos de treinamento, convites para eventos, relatórios, etc.).

4.2 CVE-2023-40477 - Remote Code Execution com Interação do Usuário

Vulnerabilidade de RCE em WinRAR associada a validação incorreta de entrada do usuário; apesar de exigir interação (abrir/extração de arquivo específico), pode ser explorada remotamente via conteúdo entregue por e-mail/ download.

Também reforça o padrão: arquivos compactados maliciosos + engenharia social - execução de código.

4.3 CVE-2025-8088 - Zero-day de Path Traversal

Uma vulnerabilidade de **path traversal** que afeta a versão para Windows do WinRAR permite que atacantes executem código arbitrário criando arquivos compactados maliciosos.

Campanha observada:

- **Alvos:** setores financeiro, manufatura, defesa e logística em vários países;
- **Grupo:** RomCom (Storm-0978/ Tropical Scorpius / UNC2596), alinhado à Rússia;
- **Carga útil:** backdoors Mythic, SnipBot, RustyClaw/MeltingClaw, com forte foco em espionagem e roubo de informação.

4.4 Atores de Ameaça Envolvidos

Cybercrime e Fraude Financeira

Campanhas contra traders e usuários de plataformas financeiras usando arquivos ZIP/WinRAR mascarados como estratégias de trading, robôs, sistemas de investimento, etc.

- Entrega de infostealers (Rhadamanthys, outros) e trojans que visam:
  - Roubo de credenciais de corretoras, bancos e carteiras;
  - Desvio de fundos/ fraude transacional.

Atores Estatais/ APTs

Múltiplos grupos governamentais explorando CVE-2023-38831, incluindo:

- FROZENBARENTS (SANDWORM)
- FROZENLAKE (APT28)
- Grupos ligados à China, como ISLANDDREAMS (APT40), mirando governos.

Esses grupos usam o WinRAR como vetor para:

- Distribuir backdoors customizados;
- Garantir persistência e movimento lateral;
- Realizar espionagem em setores de energia, defesa, think tanks e governo.

4.5 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	T1566.001 Spearphishing Attachment	Envio de arquivos .zip/.rar maliciosos contendo documentos falsamente benignos.
Execution	T1204.002 Malicious File	Execução automática do payload ao abrir o arquivo no WinRAR.
Persistence	T1547.001 Startup Folder	Criação de LNK maliciosos na pasta de inicialização do usuário.
Defense Evasion	T1036 Masquerading	Uso de arquivos com nomes, ícones ou extensões falsas para enganar a vítima.
Credential Access	T1555 Credentials from Password Stores T1552 Unsecured Credentials	Coleta de credenciais por infostealers instalados após exploração.
Command and Control	T1071.001 Web Protocols	Conexões HTTPS para servidores controlados pelo atacante.
Exfiltration	T1041 Exfiltration Over C2	Extração de dados sensíveis via canal de comando e controle.

Tabela 3 – Tabela MITRE ATT&CK.

5 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção da referida *ameaça*, como por exemplo:

- Implementar política corporativa para atualização ou remoção do WinRAR, priorizando a substituição por ferramentas de compressão que possuam mecanismos de atualização automática e melhor integração com ambientes corporativos.
- Reforçar filtros de e-mail, para bloquear ou colocar em quarentena anexos compactados (.rar/.zip) provenientes de remetentes externos desconhecidos ou pouco confiáveis, especialmente quando associados a temas recorrentes de engenharia social.
- Configurar o EDR para monitorar comportamentos pós-extração, incluindo a criação de arquivos executáveis, DLLs e atalhos (.lnk) após a abertura de arquivos compactados, bem como a execução de intérpretes de comandos (cmd, PowerShell, WScript, MSHTA).
- Adotar processos de sandboxing, para análise dinâmica de arquivos .rar/.zip suspeitos antes da disponibilização ao usuário final, principalmente em fluxos de e-mail e download externo.
- Conduzir campanhas de conscientização de usuários, destacando golpes recorrentes baseados em currículos, notas fiscais, propostas comerciais e documentos corporativos enviados em arquivos compactados.
- Estabelecer controles de Application Control/ Allowlisting, restringindo a execução de binários, scripts e DLLs extraídos de diretórios temporários, pastas de usuário ou caminhos frequentemente abusados por malware.
- Estruturar ou fortalecer uma capacidade dedicada de Cyber Threat Intelligence (CTI), responsável por monitorar continuamente a exploração ativa de vulnerabilidades, campanhas emergentes, TTPs de atores relevantes e indicadores de comprometimento, garantindo que informações acionáveis sejam integradas aos processos de detecção, resposta a incidentes e priorização de riscos.
- Implementar monitoramento comportamental específico para ferramentas de compressão, correlacionando eventos de abertura de arquivos compactados com atividades suspeitas subsequentes, como criação de persistência ou conexões de rede anômalas.
- Incorporar o WinRAR e ferramentas similares ao processo formal de Gestão de Vulnerabilidades, com inventário contínuo, definição de SLAs de correção e priorização baseada em inteligência de ameaças (CVEs exploradas ativamente).

6 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.

6.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	391325100384964325ed4ace788c8bc2
sha1:	371a5b8ba86fbcab80d4e0087d2aa0d8ffddc70b
sha256:	2a8fafa01f6d3863c87f20905736ebab28d6a5753ab708760c0b6cf3970828c3
File name:	Adverse_Effect_Medical_Records_2025.rar

Indicadores do artefato	
md5:	df9cfd04d8cda6df8f7263af54f9e5b1
sha1:	f77dba76010a9988c9ceb8e420c96aebc071b889
sha256:	107f3d1fe28b67397d21a6acca5b6b35def1aeb62a67bc10109bd73d567f9806
File name:	eli-rosenfeld-cv2-copy-10.rar

Indicadores do artefato	
md5:	4c458b976b583cda61aa8fa2827ab2cc
sha1:	ae687bef963cb30a3788e34cc18046f54c41ffba
sha256:	e0cbe8f18315a2ee781de48565dc8a087a1564557c42c66067f65c267120c894
File name:	4c458b976b583cda61aa8fa2827ab2cc.ex_

Indicadores do artefato	
md5:	2dd4c9139bf6361e561216280266592d
sha1:	9830b9e650d473e4d6f88d928256ea97b6a9f365
sha256:	61f88c557364657bfa12e1f145cc53d186686ac503b30b55c74d5e9020b64d95
File name:	my-foto-progect.rar

Indicadores do artefato	
md5:	9b6cf97a3bba6cf218fd560b18fdd97b
sha1:	8c23dff5daf28237fb4f74584ca841a457422102
sha256:	c620ba7b6dfe81c6b6bf54a3e6a98bbca7b77e0c3f75586b900af326b8fd7cfe
File name:	Passport.rar

Tabela 4 – Indicadores de Comprometimento.

Indicadores de IPs e Domínios

Indicadores de IPs e Domínios	
Domínio	87iavv[.]com trssp05923[.]com corialopolova[.]com mmnedgeggrrva[.]com
IP	162.19[.]175[.]44 194.36[.]209[.]127 85.158[.]108[.]62 185.173[.]235[.]134

Tabela 5 – Indicadores de Comprometimento.

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.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- **Group-ib**
- **Vicarius.io**
- **Welivesecurity**
- **KEV-CISA**
- **MITRE ATT&CK**

8 AUTORES

- **Ismael Rocha – Threat Intelligence Specialist**
- **Thiago Cesar Maciel da Paixão – Threat Intelligence Analyst**

heimdall
security research
A DIVISION OF ISH