Armored Likho: Análise de um Grupo de Ameaça Persistente Avançada com Duplo Foco em Espionagem Cibernética e Fraude Financeira

Vitor Mallmann[1], Rodrigo Caio Koelln Alfonsin[1]

[1]Itaipu Parquetec, Foz do Iguaçu, Paraná, Brasil (mallmannvictor@gmail.com)

Resumo: O trabalho analisa o Armored Likho, grupo de ameaça persistente avançada identificado pela Kaspersky em julho de 2026 e associado ao agrupamento Eagle Werewolf. O grupo combina espionagem cibernética contra órgãos governamentais e o setor elétrico na Rússia, Cazaquistão e Brasil com fraude financeira contra indivíduos, usando o infostealer BusySnake. Descrevem-se os vetores de infecção, a arquitetura do malware e seu mapeamento ao MITRE ATT&CK.

Palavras-chave: APT; infostealer; MITRE ATT&CK; phishing; segurança cibernética.

INTRODUÇÃO

Em julho de 2026, pesquisadores da Kaspersky divulgaram, por meio da plataforma de inteligência de ameaças Securelist, a identificação de um grupo de ameaça persistente avançada até então não documentado, ao qual atribuíram o codinome Armored Likho (Kaspersky, 2026). O grupo distingue-se de boa parte dos agentes de ameaça monitorados por operar simultaneamente em duas frentes: campanhas de espionagem cibernética contra organizações governamentais e do setor de energia elétrica, e operações financeiramente motivadas contra indivíduos (Kaspersky, 2026). A abrangência geográfica confirmada das vítimas inclui Rússia, Cazaquistão e Brasil, o que caracteriza o grupo como uma ameaça de alcance global e torna sua análise particularmente relevante para organizações brasileiras dos setores elétrico e governamental.

A pesquisa da Kaspersky associa o grupo, com base em evidências circunstanciais, ao agrupamento que a empresa russa de segurança BI.ZONE rastreia sob o codinome Eagle Werewolf, ativo desde pelo menos maio de 2023 e historicamente voltado a organizações estatais, empresas industriais e indivíduos ligados à fabricação e engenharia de drones (BI.ZONE, 2026). Essa sobreposição de identidade é sustentada por similaridades estruturais entre ferramentas previamente atribuídas a cada um dos agrupamentos.

O achado técnico central do relatório da Kaspersky é o BusySnake Stealer, um infostealer baseado em Python, até então inédito, projetado para sistemas Windows e equipado com múltiplas camadas de evasão. A campanha ativa no momento da publicação também chamou atenção por evidências de que os *loaders* de primeiro estágio do malware foram gerados com apoio de ferramentas de inteligência artificial, uma tendência que dificulta a análise de atribuição por complicar a identificação de padrões de codificação característicos do grupo (Kaspersky, 2026).

Este trabalho tem como objetivo consolidar as informações técnicas disponíveis sobre o Armored Likho, apresentar o histórico do grupo e sua associação ao Eagle Werewolf, descrever os vetores de infecção inicial e a arquitetura do BusySnake Stealer, discutir as evidências técnicas de atribuição, mapear as táticas, técnicas e procedimentos (TTPs) ao framework MITRE ATT&CK, e propor recomendações práticas de detecção e mitigação para organizações expostas a esse tipo de ameaça.

MATERIAL E MÉTODOS

A pesquisa baseou-se em revisão qualitativa e documental de relatórios técnicos primários de inteligência de ameaças, priorizando fontes de empresas de segurança com acesso direto a amostras de malware e telemetria, em detrimento de coberturas jornalísticas secundárias. As duas fontes primárias centrais foram o boletim da Kaspersky Securelist sobre o Armored Likho e o BusySnake Stealer (Kaspersky, 2026) e o relatório da BI.ZONE sobre a campanha do agrupamento Eagle Werewolf, publicado em março de 2026 (BI.ZONE, 2026). Essas fontes foram complementadas pelo boletim trimestral de vulnerabilidades e exploits da própria Kaspersky, referente ao primeiro trimestre de 2025, no qual a vulnerabilidade ZDI-CAN-25373 foi originalmente documentada (Kolesnikov, 2025), e pela matriz pública do framework MITRE ATT&CK Enterprise (MITRE, 2025).

O processo de análise seguiu três etapas. Na primeira, extraíram-se dos relatórios primários os elementos descritivos do comportamento do grupo —

vetores de infecção, mecanismos de persistência, técnicas de evasão e de exfiltração — organizando-os cronologicamente e por fase da cadeia de ataque. Na segunda etapa, cada trecho descritivo foi mapeado ao identificador de técnica correspondente no MITRE ATT&CK, seguindo abordagem de classificação por evidência textual semelhante à empregada em trabalhos acadêmicos de extração estruturada de TTPs a partir de relatórios de inteligência de ameaças, como o método CAPTAIN, que utiliza sequenciamento de TTPs extraídas de relatórios para apoiar a atribuição de grupos de ameaça persistente avançada (Rani et al., 2024). Na terceira etapa, consolidaram-se as evidências de atribuição relatadas pelas fontes primárias, sem reinterpretação especulativa, preservando o nível de confiança (média, no caso da atribuição da Kaspersky) originalmente atribuído pelos pesquisadores.

Como limitação metodológica, reconhece-se que a análise depende integralmente de relatórios de terceiros, sem acesso direto às amostras de malware ou à infraestrutura ofensiva do grupo, o que é uma limitação comum a trabalhos de síntese de inteligência de ameaças baseados em fontes públicas.

RESULTADOS E DISCUSSÃO

O Armored Likho foi identificado durante atividades de monitoramento contínuo de ameaças conduzidas pela Kaspersky, que classificou o agrupamento como híbrido: parte de suas operações mira indivíduos com finalidade financeira, enquanto outra parte é dedicada à espionagem cibernética contra organizações (Kaspersky, 2026). O arsenal do grupo inclui Trojans de acesso remoto (RATs) modulares e ofuscados, infostealers projetados especificamente para dificultar a análise dinâmica, além de ferramentas mais simples como o Go2Tunnel, utilizado para acesso remoto e tunelamento de rede (Kaspersky, 2026). Em fevereiro de 2026, a BI.ZONE documentou uma campanha na qual três agrupamentos distintos — Paper Werewolf, Versatile Werewolf e o próprio Eagle Werewolf — distribuíram malware disfarçado de serviços de registro de dispositivos Starlink e de aplicativos de treinamento para pilotos de drones, operando de forma autônoma, sem evidências de coordenação direta entre eles (BI.ZONE, 2026). Especificamente quanto ao Eagle Werewolf, a BI.ZONE relata o comprometimento de um canal de Telegram voltado à comunidade de operadores de drones, utilizado para distribuir um dropper em Rust disfarçado de lista de verificação para ativação de dispositivos Starlink, que por sua vez decriptografa um segundo dropper em Go responsável por registrar a vítima na infraestrutura de comando e controle e implantar o AquilaRAT (BI.ZONE, 2026).

O principal vetor de acesso inicial do Armored Likho continua sendo o phishing. O grupo envia e-mails de spear-phishing com temas que variam entre comunicados governamentais oficiais e programas de assistência social, distribuindo anexos maliciosos em arquivos compactados com nomes que remetem a testes psicológicos ou solicitações de ajuda humanitária (Kaspersky, 2026). Dois padrões de infecção distintos foram documentados. No primeiro, o arquivo compactado contém um dropper executável construído com o Nullsoft Scriptable Install System (NSIS), que exibe uma aplicação-isca — em um caso documentado, um falso teste psicológico — para dissipar suspeitas, enquanto grava em disco um executável legítimo e injeta código malicioso em sua memória para executar um *loader*. Esse *loader* busca arquivos compactados adicionais hospedados em repositórios do GitHub, cujo processo de publicação é automatizado, permitindo rotação rápida tanto dos *payloads* quanto dos próprios repositórios (Kaspersky, 2026).

No segundo padrão, o anexo malicioso é um arquivo de atalho do Windows (.lnk) nomeado de forma a mimetizar o tema da isca de phishing. Para conduzir essa infecção, o grupo explora a vulnerabilidade identificada como ZDI-CAN-25373, documentada pela Kaspersky em seu relatório trimestral de vulnerabilidades e exploits do primeiro trimestre de 2025 (Kolesnikov, 2025). Trata-se de uma falha na forma como o Windows Explorer exibe os parâmetros especificados no campo de destino de atalhos: ao inserir caracteres adicionais, como espaços ou quebras de linha, após um caminho aparentemente legítimo, seguidos de comandos maliciosos, o Explorer exibe apenas a primeira parte do caminho, ocultando o restante do comando executado. Essa falha, posteriormente catalogada como CVE-2025-9491, foi corrigida pela Microsoft em dezembro de 2025 — quase um ano após ter sido reportada pela Zero Day Initiative em março de 2025 —, mas já vinha sendo ativamente explorada por diversos agentes de ameaça havia anos no momento em que a Kaspersky documentou a exploração pelo Armored Likho (Kolesnikov, 2025).No caso do Armored Likho, a execução do atalho dispara um comando ofuscado que aciona uma instrução PowerShell responsável por baixar e executar o *loader*, que por sua vez exibe um documento-isca em DOCX enquanto inicializa variáveis de ambiente necessárias para a instalação do stealer (Kaspersky, 2026). Um aspecto notável observado pelos pesquisadores é que o código-fonte dos *loaders* contém comentários extensos e emojis em formato de marcadores, estilo atípico para malware desenvolvido por humanos e forte indício do uso de modelos de linguagem na geração dos *payloads* (Kaspersky, 2026).

Arquitetura do BusySnake Stealer. O payload principal entregue por ambos os vetores é um infostealer baseado em Python ao qual a Kaspersky atribuiu o nome BusySnake Stealer. Seu código-fonte é ofuscado e criptografado com a ferramenta comercial PyArmor Pro, versão 9.2.0, que decriptografa o *bytecode* dinamicamente apenas no momento exato em que uma função é chamada, recriptografando os dados imediatamente após o uso — o que dificulta consideravelmente a análise estática (Kaspersky, 2026). O malware é executado como arquivo .pyw, rodando em segundo plano sem abrir janela de console visível. A Tabela 1 resume os principais *handlers* identificados na análise da Kaspersky.

Tabela 1. Principais *handlers* do BusySnake Stealer (Kaspersky, 2026).

Handler	Função
single_instance_lock	Impede múltiplas instâncias simultâneas do stealer via bloqueio por arquivo não convencional
start_key_clipboard_logger	Coleta contínua de dados da área de transferência
start_inventory_background	Enumera arquivos do sistema e registra metadados em banco SQLite local
extract_hex64_from_file	Varre arquivos em busca de sequências hexadecimais de 64 caracteres compatíveis com chaves privadas
start_send_documents_priority_background	Localiza e envia documentos de Área de Trabalho, Documentos e Downloads ao C2
take_screenshot/archive_pngs	Captura e arquiva capturas de tela periódicas, removendo temporários já enviados
poll_task	Mantém laço contínuo de comunicação com o C2 aguardando comandos
ensure_schtask	Verifica e recria a tarefa agendada de persistência caso ausente

O servidor de C2 transmite comandos na forma de nomes de função, cobrindo capacidades que vão de captura de tela e keylogging até extração de credenciais de navegadores, cookies, segredos de autenticação de dois fatores, arquivos de carteiras de criptomoedas, dados de sessão do Telegram e tunelamento SSH reverso (Kaspersky, 2026). Uma capacidade sensível é o controle remoto: caso a ferramenta legítima RustDesk esteja instalada, o stealer pode reiniciá-la para forçar a vítima a reinserir credenciais, capturando a tela nesse momento. Para navegadores Chromium, o stealer localiza a chave mestra de criptografia protegida pela DPAPI e a decriptografa no contexto do próprio usuário; no Firefox, quando o perfil não está protegido por senha mestra — cenário frequente em ambientes corporativos —, o próprio mecanismo de criptografia do navegador permite a decriptografia sem interação adicional (Kaspersky, 2026). Cookies de sessão são extraídos tanto diretamente dos bancos de dados dos navegadores quanto por meio de uma extensão maliciosa instalada via um módulo complementar obtido do GitHub. O tunelamento SSH reverso, antes provido pela ferramenta independente Go2Tunnel, foi incorporado como recurso nativo do stealer.

EA Kaspersky identificou uma versão mais recente do stealer, mantendo o mesmo método de distribuição e ofuscação estática, mas com alterações significativas nas TTPs. Em vez de criar tarefas agendadas via chamadas diretas ao utilitário schtasks, a nova versão utiliza a biblioteca win32com.client para interagir diretamente com o objeto COM Schedule.Service, mecanismo de persistência menos detectável (Kaspersky, 2026). Foi adicionada também uma função que pausa a execução antes de disparar rotinas maliciosas, dificultando a análise em sandbox, além de um sistema de gerenciamento de tarefas com identificador único e estado operacional dinâmico por tarefa recebida do C2. Uma das capacidades mais relevantes dessa evolução é uma classe dedicada à execução de scripts Python arbitrários recebidos do C2, que instala dependências via pip e executa o código diretamente em memória, sem gravação em disco (Kaspersky, 2026).

A Kaspersky atribui a campanha ao Armored Likho com confiança média, fundamentada em três linhas de evidência. Primeiro, o grupo já utilizava o Go2Tunnel para túneis SSH reversos; a funcionalidade equivalente incorporada ao BusySnake recebe comandos e chaves do mesmo tipo de servidor de C2, com argumentos SSH idênticos entre as duas ferramentas. Segundo, o grupo já empregava historicamente o RAT AquilaRAT, que compartilha estrutura semelhante ao BusySnake: ambos recebem tarefas de um servidor C2 e delegam sua execução a *handlers* dedicados, utilizando endpoints similares para reportar conclusão de tarefas. Terceiro, ambas as ferramentas mantêm persistência registrando tarefas agendadas disfarçadas de utilitários legítimos da Microsoft — o AquilaRAT como MicrosoftOfficeUpdate, o BusySnake como WindowsHelper (Kaspersky,

2026). Essa mesma convenção de mascaramento também aparece no histórico do AquilaRAT associado ao Eagle Werewolf pela BI.ZONE, reforçando a hipótese de sobreposição entre os dois agrupamentos (BI.ZONE, 2026).

Até o momento da publicação do relatório os alvos e escopo geográfico, haviam sido identificadas na Rússia, no Cazaquistão e no Brasil, com ataques concentrados nos setores governamental e de infraestrutura elétrica (Kaspersky, 2026). O histórico do Eagle Werewolf documentado pela BI.ZONE aponta ainda um padrão de vitimização voltado a organizações estatais, empresas industriais e indivíduos ligados à fabricação e engenharia de drones, desde pelo menos maio de 2023 (BI.ZONE, 2026). A combinação desses dois padrões — infraestrutura crítica de energia e órgãos governamentais, de um lado, e setor industrial e de defesa ligado a sistemas não tripulados, de outro — reforça a avaliação de que o Armored Likho/Eagle Werewolf representa uma ameaça relevante para organizações de infraestrutura crítica para além das fronteiras da Rússia, alcançando também a América Latina.

Mapeamento ao MITRE ATT&CK. A Tabela 2 consolida as principais TTPs identificadas.

Tabela 2. TTPs do Armored Likho mapeadas ao MITRE ATT&CK..

Técnica	ID	Uso observado
Spearphishing com anexo	T1566.001	Distribuição de droppers EXE/LNK disfarçados de documentos oficiais
Interpretador de comandos e scripting	T1059.001	PowerShell para baixar e executar loaders
Exploração para acesso inicial	T1203	Abuso da falha ZDI-CAN-25373
Tarefa agendada	T1053.005	Persistência via tarefa disfarçada de utilitário Microsoft
Ofuscação de arquivos ou informação	T1027	Ofuscação do bytecode Python com PyArmor Pro
Credenciais de stores de senhas	T1555.003	Extração via DPAPI e NSS
Roubo de cookies de sessão web	T1539	Extração direta e via extensão maliciosa
Protocolo de camada de aplicação (proxy)	T1090/T1572	Tunelamento SSH reverso
Captura de área de transferência	T1115	Monitoramento contínuo do clipboard para dados sensíveis e chaves de dois fatores
Captura de tela	T1113	Capturas periódicas e sob demanda, arquivadas e exfiltradas ao C2

Para detecção e mitigação no perímetro de e-mail, recomenda-se bloqueio ou quarentena de anexos compactados contendo executáveis e atalhos LNK provenientes de remetentes externos, com políticas restritivas para extensões historicamente associadas a esse tipo de campanha. Embora a vulnerabilidade ZDI-CAN-25373 (CVE-2025-9491) já tenha recebido correção formal da Microsoft em dezembro de 2025, sua longa janela de exploração ativa por múltiplos grupos de ameaça — e o fato de campanhas como a do Armored Likho continuarem sendo documentadas mesmo após a correção estar disponível — reforça a necessidade de que organizações mantenham seus sistemas atualizados e, complementarmente, restrinjam a execução de arquivos LNK recebidos por e-mail ou mídia removível, monitorando a execução de rundll32.exe e cadeias de PowerShell disparadas a partir de atalhos (Kolesnikov, 2025; Kaspersky, 2026). No nível de endpoint, equipes de segurança devem configurar alertas para execução não usual de interpretadores Python, sobretudo quando associados a acesso a arquivos de credenciais de navegadores, ao diretório tdata do Telegram, ou a varreduras em busca de chaves criptográficas, além de monitorar conexões SSH de saída originadas de estações que normalmente não iniciariam esse tráfego. Tarefas agendadas com nomes que imitam utilitários legítimos da Microsoft, como WindowsHelper ou MicrosoftOfficeUpdate, devem ser tratadas como indicadores de comprometimento a serem auditados regularmente (Kaspersky, 2026). Quanto à proteção de credenciais armazenadas, uma vez que o BusySnake explora diretamente a ausência de senha mestra no Firefox, organizações devem migrar contas de alto valor para gerenciadores de senha dedicados com múltiplos fatores de autenticação, reduzindo a dependência de mecanismos nativos dos navegadores. Por fim, dado que ambos os vetores de infecção dependem da ação da vítima, programas de simulação de phishing devem incorporar cenários

com temas de comunicados governamentais, programas sociais e documentos de ajuda humanitária, refletindo as iscas efetivamente observadas nas campanhas do grupo.

CONCLUSÃO

O Armored Likho representa um exemplo relevante da convergência entre espionagem cibernética voltada a infraestrutura crítica e operações financeiramente motivadas dentro de um mesmo agrupamento de ameaça. A sobreposição técnica identificada entre suas ferramentas e o histórico do agrupamento Eagle Werewolf, documentado independentemente pela BI.ZONE desde 2023, sugere continuidade operacional de médio a longo prazo, ainda que a atribuição definitiva permaneça classificada com confiança apenas circunstancial e média. Do ponto de vista técnico, a campanha evidencia uma tendência mais ampla no cenário de ameaças: o uso de ferramentas de inteligência artificial para geração de *loaders* de primeiro estágio, o que reduz o tempo de desenvolvimento de novas variantes e dificulta a atribuição baseada em estilo de codificação. Somado a isso, a longa janela de exploração da vulnerabilidade ZDI-CAN-25373 (CVE-2025-9491) — corrigida pela Microsoft somente em dezembro de 2025, quase um ano após sua divulgação pela Zero Day Initiative — reforça a importância de tratar arquivos de atalho do Windows como uma superfície de ataque ativa e não apenas teórica, além de destacar a relevância de manter os ambientes corporativos com os patches de segurança em dia. Organizações do setor governamental e de energia elétrica, em particular na América Latina, devem considerar o Armored Likho um agente de ameaça relevante para seus modelos de risco, priorizando controles de e-mail, monitoramento comportamental de endpoints e restrição ao uso de arquivos de atalho, complementados por programas de conscientização direcionados aos temas de engenharia social especificamente observados nas campanhas do grupo.

REFERÊNCIAS

BI.ZONE. Unholy trinity: werewolves target law enforcers. BI.ZONE Expertise Blog, 2026.

KASPERSKY. Armored Likho's new weapon: BusySnake Stealer. Securelist, 2026.

KOLESNIKOV, A. Vulnerability landscape analysis for Q1 2025. Securelist, 2025.

MITRE CORPORATION. MITRE ATT&CK Enterprise Matrix. MITRE, 2025.

RANI, N.; SAHA, B.; MAURYA, V.; SHUKLA, S. K. Chasing the shadows: TTPs in action to attribute advanced persistent threats. arXiv preprint arXiv:2409.16400, 2024.