TLP: CLEAR

Pesquisa de Cibersegurança

SAFEPAY - Evolução e Persistência (2025-2026)

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse a inteligência que produzimos sobre as Táticas, Técnicas e Procedimentos de determinados *Threat Actors*, análises de *malwares* emergentes no cenário de cibersegurança, análises de vulnerabilidades críticas e outras informações no *blog* da ISH Tecnologia, clicando na imagem abaixo.

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

LISTA DE TABELAS

LISTA DE FIGURAS

1. INTRODUÇÃO EXECUTIVA

O ***SafePay*** consolidou-se em 2025 como um dos **Top 10** grupos de *ransomware* mais ativos, representando uma ameaça de alto nível e persistente. O grupo opera sob um modelo de **negócio centralizado e fechado**, o que lhe confere maior controle e longevidade no cenário de ameaças, em contraste com os modelos de franquia mais comuns.

Estrategicamente, o risco é elevado. O ***SafePay*** direciona suas operações a organizações com alto potencial de retorno financeiro, independentemente do setor, mantendo maior incidência de ataques na **América do Norte** e **Europa Ocidental**. A tática de dupla extorsão, permanece como principal mecanismo de coerção e monetização.

Operacionalmente, o ***SafePay*** prioriza velocidade. O acesso inicial ocorre, em sua maioria, por meio de credenciais comprometidas, seguido pela rápida execução das etapas subsequentes do ataque, **muitas vezes em menos de 24 horas**. A natureza do ataque exige uma defesa focada na detecção precoce de atividades anômalas, como o uso de ferramentas legítimas para fins maliciosos (***Living-off-the-Land***) e a rápida identificação de ferramentas de acesso remoto não autorizadas.

2. PERSISTÊNCIA E ESCALADA GLOBAL

2.1 CONTEXTO E EVOLUÇÃO DO SAFEPAY

O grupo ***SafePay*** emergiu no final de 2024, sendo inicialmente documentado como uma ameaça emergente que utilizava fragmentos de código do **LockBit 3.0**. Para uma compreensão mais técnica deste ator, recomenda-se a leitura do relatório anterior:

- Detalhes da operação do Ransomware SafePay

Enquanto o **relatório de 2024** destacou uma análise inicial do binário, **este documento de 2026** serve como uma Análise de Maturidade e Persistência. Observamos que, embora o comportamento principal não tenha sofrido alterações estruturais drásticas, a eficiência operacional e a escala global do grupo atingiram um novo patamar de profissionalismo. O ***SafePay*** deixou de ser uma "nova variante" para se tornar um pilar de estabilidade no ecossistema de *ransomware*, provando que um modelo centralizado e fechado pode ser mais resiliente do que os modelos **RaaS** tradicionais.

2.2 CONSOLIDAÇÃO NO CENÁRIO GLOBAL

A consolidação do ***SafePay*** no cenário global é evidenciada pela constância de suas operações ao longo do tempo. Esse ritmo de atuação contribui diretamente para o espaço que o grupo vem ocupando entre os **principais atores de *ransomware***.

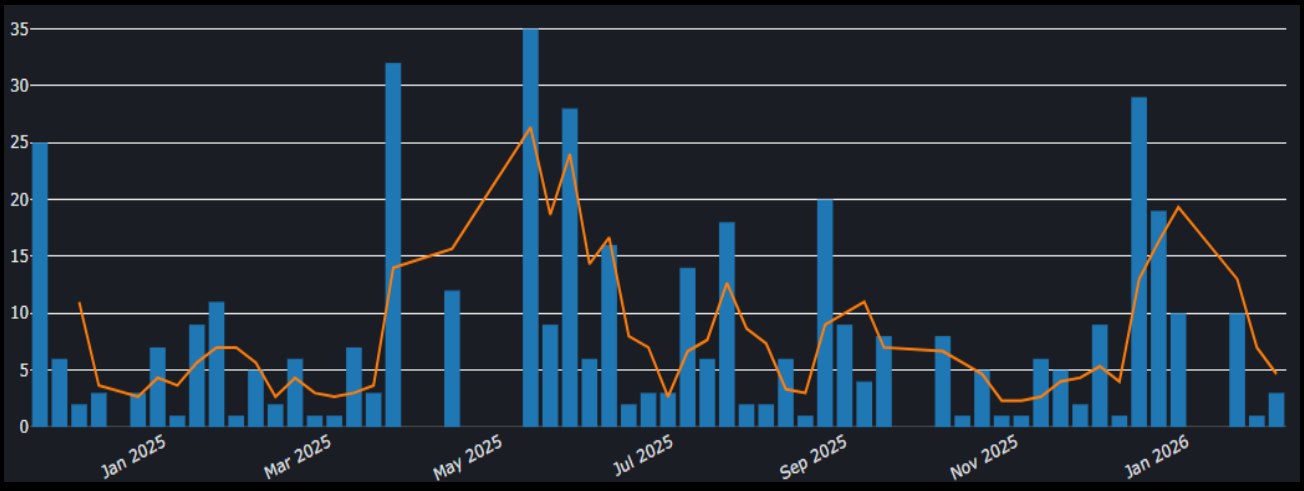

Figura 1 - Atividade do grupo

O grupo direciona suas operações a organizações com **alto potencial de retorno financeiro e impacto operacional**. Essa lógica se reflete em uma distribuição setorial diversificada, com predominância dos setores de **manufatura**, **tecnologia**, **educação**, **saúde** e **serviços empresariais**.

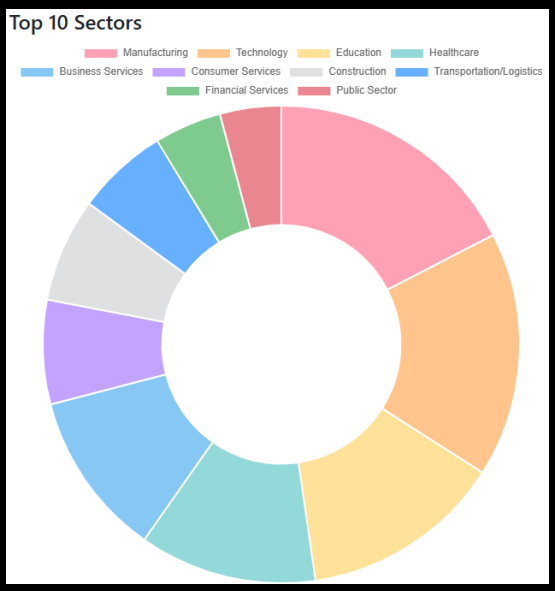

Figura 2 - Top 10 setores mais afetados por atividades do grupo SafePay

2.3 Panorama Regional: Alerta para a América Latina

A análise de vitimologia do ***SafePay*** entre 2025 e 2026 revela um movimento estratégico de expansão para além dos eixos tradicionais da América do Norte e Europa. Embora o grupo ainda concentre o maior volume de ataques fora da América do Sul, a identificação de incidentes em países vizinhos sinaliza que a infraestrutura operacional do grupo já está apontada para a região.

Panorama na América do Sul

O número de vítimas sul-americanas confirmadas serve como um indicador de alerta precoce para organizações locais.

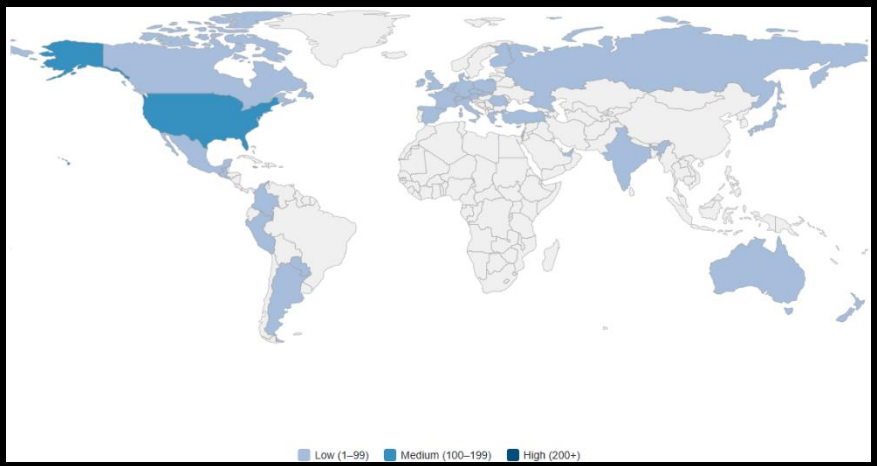

Figura 3 - Distribuição de vítimas do SafePay

Dando um zoom nos países alvos na América do Sul, temos:

- **Argentina:** 9 vítimas
- **Colômbia:** 6 vítimas
- **Peru:** 3 vítimas
- **Paraguai:** 1 vítima

O Risco Iminente para o Mercado Brasileiro

O **Brasil** configura-se como um **possível próximo alvo** dentro da progressão observada nas operações do ***SafePay***, sobretudo em função de sua relevância econômica regional. A ausência de ataques confirmados em território nacional até o momento **não deve ser interpretada como um indicativo de exclusão**, mas sim como uma **janela de oportunidade estratégica** para que organizações brasileiras antecipem a adoção de controles de detecção comportamental e de fortalecimento dos mecanismos de acesso remoto.

2.4 Vantagem Competitiva do Modelo Centralizado

A decisão do ***SafePay*** de operar como um **grupo fechado**, em vez de adotar o modelo de ***Ransomware as a Service***, representa uma escolha estratégica com impacto direto em sua resiliência operacional. Esse modelo confere ao grupo maior controle sobre todas as etapas da operação, **reduzindo dependências externas e pontos de exposição**.

- **Controle total** sobre os processos de intrusão, criptografia e extorsão;
- **Retenção integral dos lucros**, sem divisão com afiliados;
- **Redução do risco operacional**, ao evitar a fragmentação e a visibilidade excessiva típicas de ecossistemas **RaaS** baseados em afiliados.

3. MITRE ATT&CK – TTPs

A tabela abaixo consolida as Táticas, Técnicas e Procedimentos (TTPs) observadas nas campanhas do ***SafePay***.

Tática	Técnica	Procedimento
Acesso Inicial	Valid Accounts - **T1078**	Uso de credenciais comprometidas (RDP/VPN) compradas de corretores ou via brute-force
	External Remote Services - **T1133**	Exploração de VPNs e gateways RDP sem MFA ou com configurações fracas
Execução	Command and Scripting Interpreter - **T1059**	Execução de scripts PowerShell como ShareFinder.ps1 e comandos via cmd.exe
	Service Execution - **T1569.002**	Uso de PsExec para execução remota de processos
Persistência	Boot or Logon Autostart Execution - **T1547**	Instalação do backdoor QDoor para manter acesso persistente
	External Remote Services - **T1133**	Uso de ferramentas legítimas de acesso remoto como ScreenConnect
Privilege Escalation	Abuse Elevation Control Mechanism - **T1548.002**	Bypass de UAC via interface COM CMSTPLUA para elevar privilégios
Defense Evasion	Indicator Removal on Host - **T1070**	Uso do argumento -selfdelete para remover o executável após a criptografia
	Impair Defenses - **T1562.001**	Encerramento de processos de segurança (Sophos, Veeam) e deleção de Shadow Copies via vssadmin
	Obfuscated Files or Information - **T1027**	Uso de DLLs com timestamps falsos e argumentos de execução obrigatórios (-pass=)
Discovery	Network Share Discovery - **T1135**	Uso do script Invoke-ShareFinder para identificar compartilhamentos de rede
	System Language Discovery - **T1614.001**	Kill Switch: Verificação de layout de teclado cirílico para evitar execução em países da CEI
Lateral Movement	Remote Services - **T1021**	Movimento lateral via RDP, PsExec e WinRM utilizando ferramentas legítimas (LotL)
Exfiltration	Archive Collected Data - **T1560**	Uso de WinRAR e 7-Zip para compactar dados com exclusão de extensões não essenciais
	Exfiltration Over Web Service - **T1048**	Transferência de dados via FileZilla e Rclone para servidores controlados
Impact	Data Encrypted for Impact - **T1486**	Criptografia intermitente (AES/ChaCha20) com extensão .safepay

Tabela 1 - Tabela MITRE ATT&CK

4. INDICADORES E DETALHES TÉCNICOS

4.1 COMPORTAMENTO DA PAYLOAD E ARTEFATOS DE HOST

O ***SafePay*** é frequentemente entregue como uma **DLL PE32** nativa, executada via **rundll32.exe** ou **regsvr32.exe**. Um diferencial crítico é a exigência de argumentos de linha de comando para ativação, o que dificulta a análise automatizada em *sandboxes*.

Principais Artefatos de Execução:

- **Argumentos Obrigatórios**: O parâmetro **-pass=** é mandatório para decodificar *strings* e configurações internas do *malware*. Sem ele, a *payload* permanece inerte.
- **Mutexes de Controle**: O *malware* utiliza ***Mutexes*** para garantir que apenas uma instância de criptografia esteja ativa.
- **Manipulação de Serviços**: O ***SafePay*** possui uma lista "*hardcoded*" de mais de 50 processos e serviços que tenta encerrar.

4.2 LÓGICA DE CRIPTOGRAFIA E ANTI-RECUPERAÇÃO

O ***SafePay*** utiliza um esquema de criptografia híbrido e otimizado para velocidade, visando maximizar o dano antes de qualquer intervenção.

1. **Criptografia Intermitente**: Em vez de criptografar o arquivo inteiro, o malware criptografa apenas blocos específicos. O usuário pode definir a porcentagem via argumento -enc= (ex: -enc=5 para 50%). Isso torna o processo extremamente rápido e dificulta a detecção por soluções que monitoram alta taxa de I/O de escrita.
2. **Proteção de Chaves (x25519)**: Para cada arquivo, é gerada uma chave simétrica única (**AES** ou **ChaCha20**). Esta chave é então protegida usando o algoritmo de curva elíptica **x25519** (**ECDH**) ou **RSA**, e o resultado é anexado ao final do arquivo criptografado.
3. **Destruição de Backups Locais**: O *malware* executa comandos agressivos para impedir a recuperação sem o pagamento:
    a. **vssadmin delete shadows /all /quiet**;
    b. **wmic shadowcopy delete**;
    c. bcdedit /set {default} recoveryenabled no.

4.3 Estratégias de Detecção e Hunting

Para uma defesa eficaz contra o ***SafePay***, as organizações devem focar em detecção comportamental e correlação de eventos.

Lógica de Detecção Sugerida:

Alvo de Monitoramento	Lógica de Detecção / Alerta
Execução de Processo	rundll32.exe ou regsvr32.exe chamando DLLs em diretórios não convencionais, com argumentos como -pass= ou -enc=, etc.
Comportamento de Backup	Execução de vssadmin.exe ou wmic.exe com comandos para deletar shadow copies originados de processos não administrativos usuais.
Atividade de Rede	Conexões de saída para endereços IP desconhecidos ou serviços de armazenamento em nuvem não usuais.
Scripts PowerShell	Execução do script Invoke-ShareFinder ou qualquer script que utilize NetShareEnum para descoberta de rede em massa.

Tabela 2 - Insumos para detecção

5. CONCLUSÃO

O ***SafePay*** se consolidou como um ator de ameaça maduro e resiliente em 2025, operando com um modelo centralizado e fechado que reduz riscos operacionais e sustenta a dupla extorsão como principal mecanismo de monetização. Essa abordagem reforça sua posição entre os principais grupos de *ransomware* do cenário atual.

A evolução tática do grupo, com o uso de mecanismos de persistência como o ***backdoor QDoor*** e melhorias no processo de criptografia, evidencia a limitação de defesas baseadas apenas em assinatura e reforça a necessidade de capacidades de detecção comportamental e resposta.

A tendência é que o ***SafePay*** permaneça ativo em 2026, mantendo foco em organizações com exposição de acesso remoto, especialmente ambientes com RDP ou VPN mal protegidos e uso inadequado de MFA. O maior ponto de atenção defensiva deve estar nas fases pós exploração, com ênfase no abuso de ferramentas legítimas e *scripts* de descoberta.

Para mitigar o risco, é fundamental adotar uma defesa em profundidade, priorizando o fortalecimento do acesso remoto com MFA efetivo e visibilidade de *logs*, o monitoramento comportamental via EDR ou XDR para identificar uso anômalo de ferramentas administrativas e ***PowerShell***, além de uma gestão contínua de vulnerabilidades em dispositivos de borda frequentemente explorados para acesso inicial.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- **PYCUS**
- **RANSOMWARE.LIVE**
- **RANSOMLOOK**

AUTORES

Gustavo Jatene de Oliveira - Security Researcher

heimdall
security research
A DIVISION OF ISH