TLP: CLEAR

Pesquisa de Cibersegurança
Cyber Threat Actors

LOCKBIT:

Raio-X e Linha do Tempo

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

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

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO EXECUTIVO: CONHECENDO A AMEAÇA

Em seis anos, **o LockBit** consolidou-se como a operação de *Ransomware* mais prolífica e resiliente do cibercrime global. Surgido em 2019 sob o nome "ABCD Ransomware", evoluiu rapidamente para um modelo de *Ransomware-as-a-Service* (**RaaS**), no qual os administradores forneciam *malware*, infraestrutura e canais de extorsão, enquanto afiliados independentes conduziam os ataques e negociações. Essa estrutura escalável transformou o grupo em uma espécie de "franquia" do cibercrime, permitindo sua atuação em mais de 100 países e o ataque a setores críticos como saúde, energia, finanças, educação e governo.

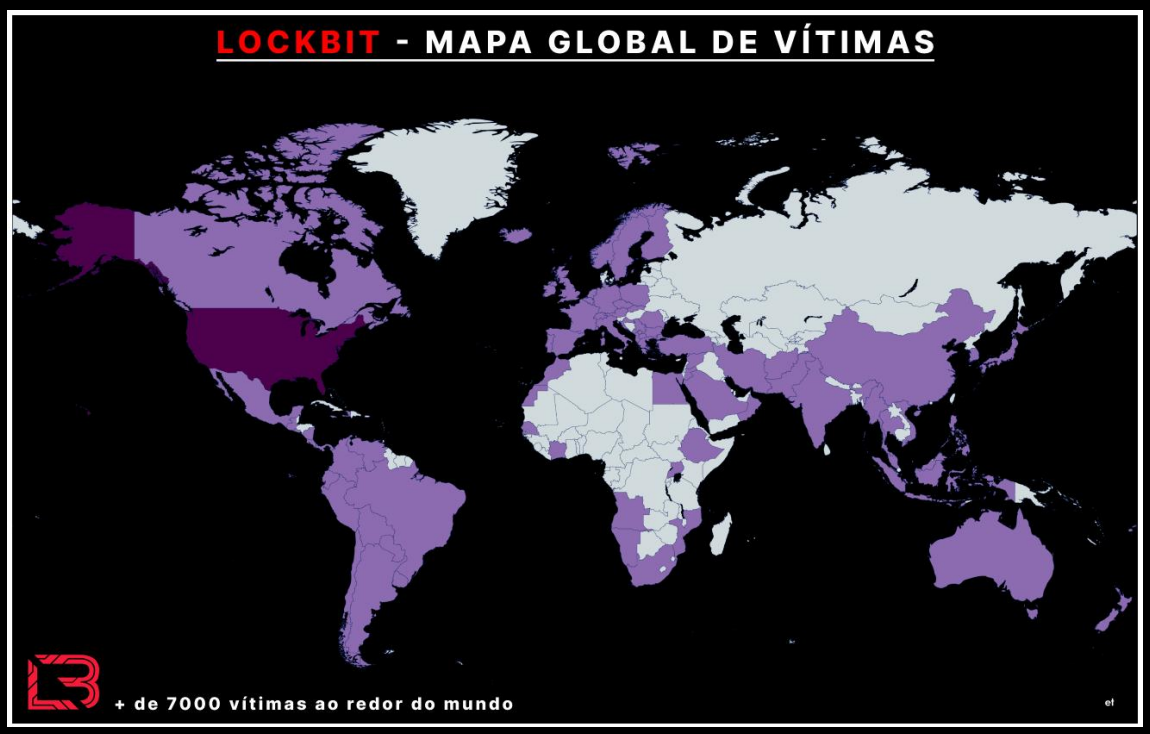

Figura 1 - Mapa Global de Vítimas

O crescimento meteórico do **LockBit** resultou de uma combinação de inovação constante, *marketing* agressivo em fóruns clandestinos e reputação de confiabilidade entre afiliados, que recebiam sua parte dos resgates antes dos administradores. O grupo se destacou por iniciativas inéditas, como um ***bug bounty*** para seu próprio *Ransomware*, competições técnicas de recrutamento e campanhas de autopromoção que incluíram até pagamentos para quem tatuasse seu logotipo. Essa mistura de profissionalismo e propaganda consolidou o **LockBit** como uma das marcas mais fortes do ecossistema cibercriminoso.

Operacionalmente, o **LockBit** foi pioneiro no modelo de extorsão dupla, criptografando arquivos e vazando dados sensíveis, e evoluiu para a extorsão tripla ao incorporar ataques **DDoS**, ampliando a pressão sobre as vítimas. Suas versões Red (2.0), Black (3.0) e Green (derivada do **Conti**) trouxeram avanços em velocidade, evasão e exfiltração. O vazamento do builder do **LockBit 3.0**, em 2022, impulsionou uma onda de ataques independentes, evidenciando os riscos da descentralização desse ecossistema.

Apesar de sua força, o **LockBit** foi alvo da Operação Cronos, uma das maiores ações conjuntas já realizadas. em fevereiro de 2024, liderada pela **NCA britânica**, **FBI** e **Europol**. A operação derrubou servidores centrais, apreendeu mais de mil chaves de descriptografia, congelou milhões em criptomoedas e revelou o suposto líder, **Dmitry Khoroshev**. Mesmo enfraquecido, o grupo reagiu e anunciou, em setembro de 2025, o **LockBit 5.0**, cercado por suspeitas de que a marca estaria sendo usada por imitadores ou como um possível *honeypot* da aplicação da lei.

Figura 2 - Infraestrutura derrubada pelo Operação Cronos

Em termos de impacto econômico, estima-se que apenas nos Estados Unidos o grupo tenha arrecadado mais de 90 milhões de dólares em resgates pagos entre 2020 e 2023, com mais de 7 mil ataques documentados globalmente até a disrupção da ***Operação Cronos***. O setor de saúde foi um dos mais atingidos, com mais de mil hospitais e clínicas afetados, evidenciando a ausência de barreiras éticas consistentes, apesar das declarações públicas do grupo. Curiosamente, o **LockBit** manteve a política de não atacar países da *Comunidade de Estados Independentes* (**CEI**), revelando motivações políticas implícitas por trás de sua suposta neutralidade.

O impacto do **LockBit** vai além da técnica: o grupo definiu padrões operacionais para o cibercrime, influenciando rivais como **BlackCat/ALPHV**, **Akira** e **RansomHub** com sua eficiência e modelo de monetização. Há ainda indícios de que lidera um movimento de "cartelização" do *Ransomware*, ao lado de grupos como **DragonForce** e **Qilin**, visando coordenar ataques e maximizar lucros. Caso confirmado, esse alinhamento marcaria um novo estágio na organização do crime digital, ampliando os riscos para governos e empresas globalmente.

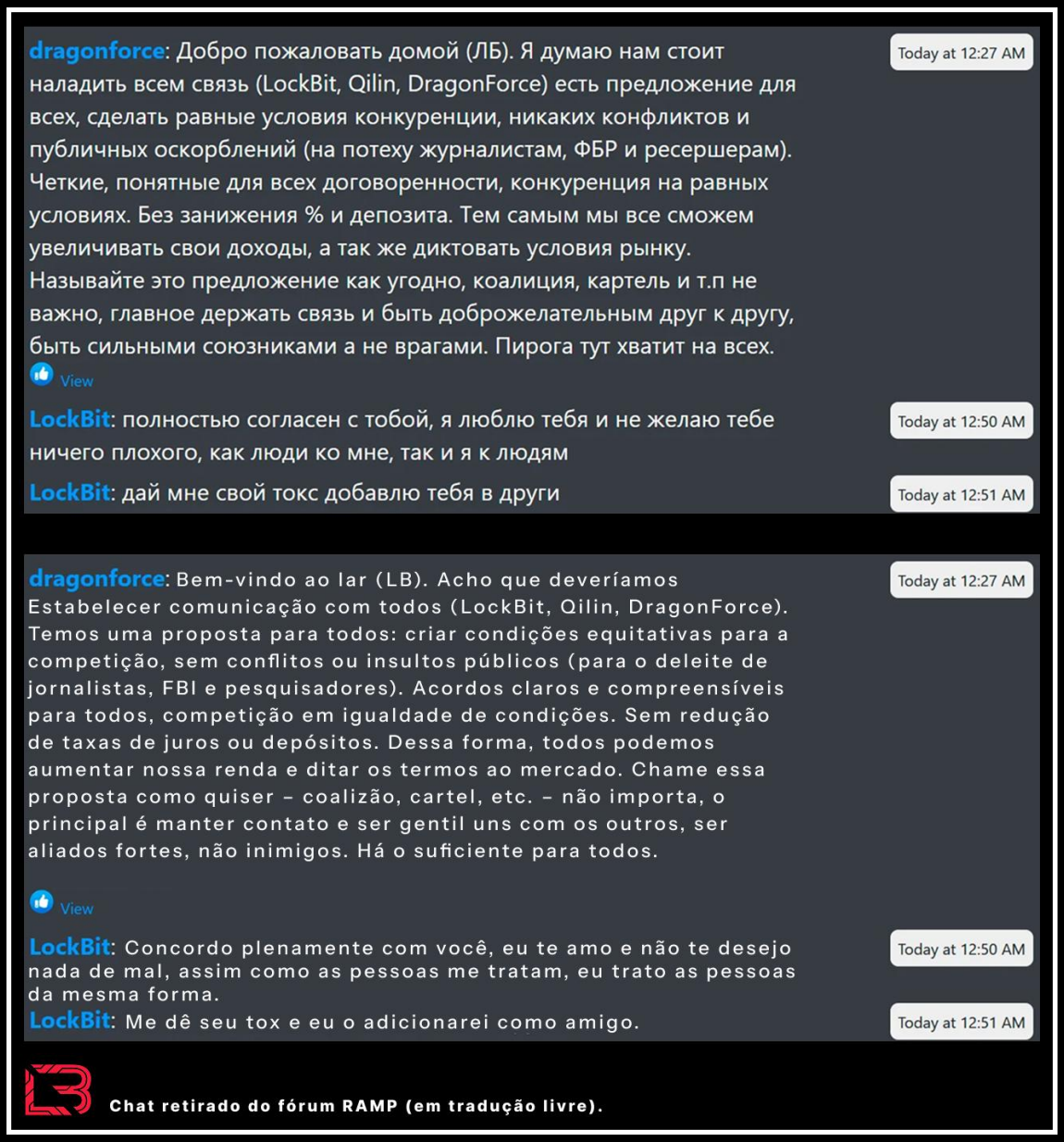

Figura 3 - Imagem do Chat (Fórum RAMP)

Em síntese, o **LockBit** representa não apenas um caso de estudo sobre resiliência cibercriminosa, mas também um marco na profissionalização e na "corporativização" do *Ransomware*. Apesar dos esforços de disrupção internacional, o grupo demonstra que operações descentralizadas, baseadas em programas de afiliação robustos e em forte identidade de marca, têm alta capacidade de sobrevivência. O risco que permanece para executivos é duplo: de um lado, a ameaça imediata de ser vítima direta de suas campanhas; de outro, a perspectiva mais ampla de um mercado cibercriminoso que se organiza em moldes de cartel, aumentando o poder de barganha e a previsibilidade dos ataques. Nesse contexto, entender a trajetória do **LockBit** e monitorar seus desdobramentos é essencial não apenas para as áreas de segurança, mas também para a gestão estratégica de riscos corporativos e governamentais.

INTELIGÊNCIA ESTRATÉGICA – CONHECENDO OS IMPACTOS

O **LockBit**, ao longo dos últimos anos, consolidou-se não apenas como uma das mais agressivas operações de ransomware já observadas, mas também como um ecossistema multifacetado que reflete a maturidade da economia cibercriminosa. A trajetória desse grupo ilustra uma mudança significativa no paradigma do crime digital: a transição de operações fragmentadas e oportunistas para estruturas organizadas, com modelo de negócio, hierarquia, incentivos financeiros e até mesmo estratégias de marketing que rivalizam com empresas legítimas. A análise de inteligência estratégica desse ator revela pontos críticos que transcendem o impacto imediato das campanhas de extorsão, ajudando a entender sua resiliência e capacidade de adaptação.

Figura 4 - Página do Decryptor do Lockbit

Primeiramente, a evolução contínua do **LockBit** demonstra um entendimento sofisticado de dinâmica de risco e recompensa. O grupo desenvolveu sucessivas versões do seu *Ransomware*, cada uma projetada não apenas para aumentar a eficácia técnica das infecções, mas também para mitigar a exposição a esforços de detecção e resposta. Esse ciclo de inovação tecnológica indica que o grupo adota uma mentalidade de *pesquisa e desenvolvimento*(**P&D**) similar à de organizações legítimas, mas com foco na maximização de ganhos ilícitos. A introdução de recursos como criptografia mais veloz, mecanismos de auto propagação e técnicas de evasão de segurança reforça essa noção de que o **LockBit** opera de forma corporativa, reinvestindo continuamente em sua infraestrutura criminosa.

Outro ponto estratégico de destaque é o modelo de afiliação, o chamado *Ransomware-as-a-Service* (**RaaS**), que transformou o **LockBit** em uma plataforma global. Essa abordagem descentraliza o risco operacional ao mesmo tempo em que amplia o alcance da ameaça. Ao permitir que afiliados independentes utilizem sua infraestrutura em troca de uma participação nos lucros, o grupo não apenas multiplica a escala de ataques possíveis, mas também cria um mercado de talentos criminosos, atraindo operadores especializados em intrusão, movimentação lateral e negociação. Essa lógica de terceirização e parceria revela um posicionamento estratégico: o **LockBit** *não é apenas um grupo, mas um hub de criminalidade organizada, capaz de agregar diferentes perfis e competências*.

Do ponto de vista de reputação e influência, o **LockBit** também demonstra uma inteligência estratégica rara no submundo cibernético. Diferente de grupos mais anárquicos ou erráticos, o **LockBit** cultiva uma imagem de eficiência e confiabilidade entre seus pares. Sua comunicação pública, seja em fóruns clandestinos ou em comunicados em sites de vazamento, reforça constantemente a mensagem de profissionalismo: prazos cumpridos, promessas mantidas e até mesmo "códigos de conduta" informais para afiliados. Essa aura de previsibilidade dentro do mercado clandestino funciona como um diferencial competitivo, fortalecendo sua marca e aumentando a adesão de afiliados. Ao mesmo tempo, a postura agressiva contra vítimas, frequentemente acompanhada de ameaças públicas de vazamento e campanhas midiáticas, cria uma dualidade estratégica: respeito no submundo e medo no mundo corporativo.

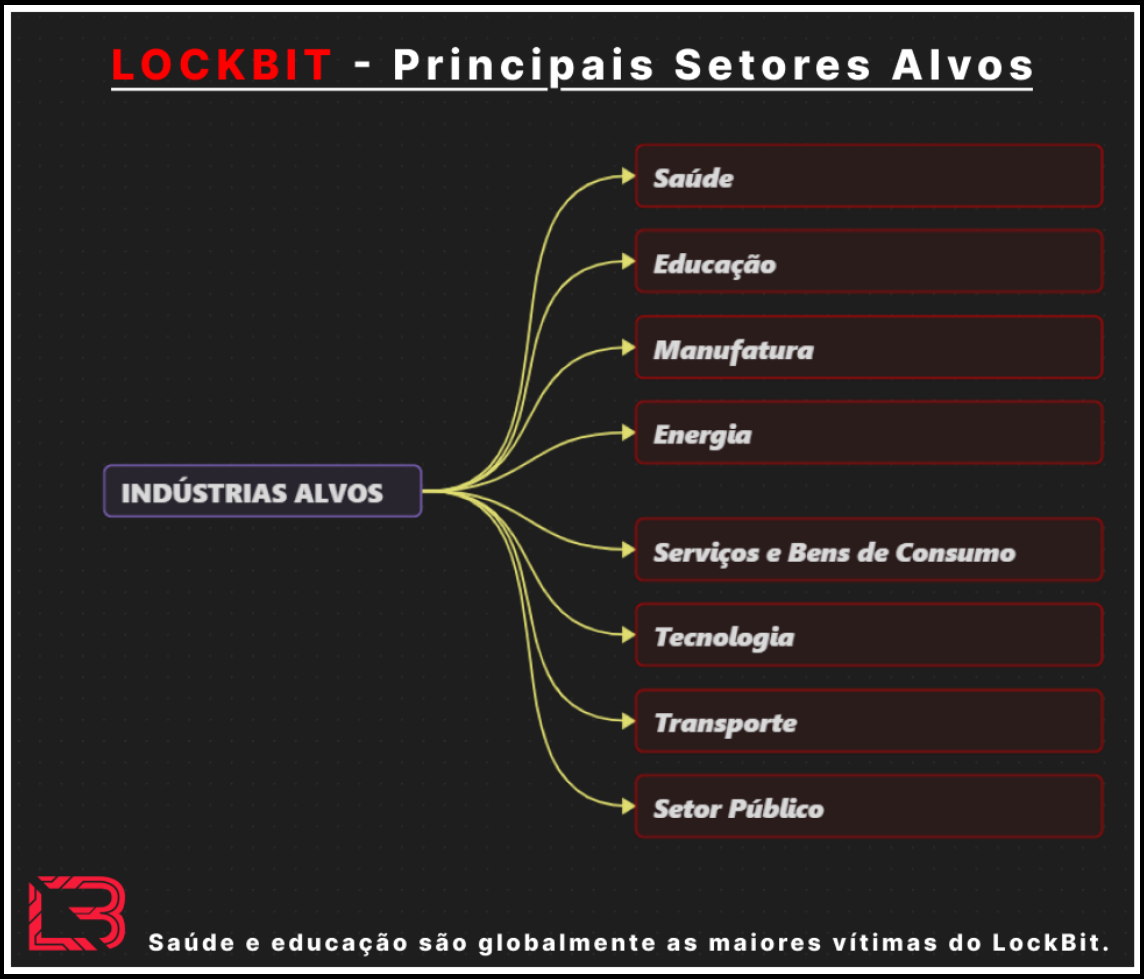

Figura 5 - Indústrias Alvo

Por fim, é preciso destacar a capacidade adaptativa do **LockBit** frente à pressão de forças de defesa globais. Investigações policiais internacionais, desmantelamentos parciais e sanções financeiras foram respondidos com agilidade surpreendente pelo grupo, que rapidamente recriou infraestruturas, mudou mecanismos de pagamento e diversificou canais de comunicação. Essa resiliência é um indicativo de que o **LockBit** opera com redundância e planejamento antecipado, elementos que demonstram uma inteligência estratégica madura. Enquanto muitos grupos de *Ransomware* desapareceram após operações de repressão, o **LockBit** continua ativo, reinventando-se em ciclos curtos e ajustando sua estratégia para manter-se relevante e lucrativo.

Em suma, sob a ótica da inteligência estratégica, o **LockBit** *deve ser interpretado não apenas como uma ameaça técnica, mas como uma entidade corporativa criminosa altamente adaptável, orientada por lógica de mercado e capaz de operar em longo prazo*. A sua longevidade e relevância decorrem justamente dessa combinação de inovação técnica, descentralização operacional e gestão de reputação, fatores que, quando somados, tornam o grupo um dos adversários mais implacáveis para governos, empresas e instituições em escala global.

HISTÓRICO E EVOLUÇÃO DO LOCKBIT

O **LockBit** surgiu em 2019 como mais um entre vários grupos de *Ransomware* que se aproveitavam do modelo emergente de *Ransomware-as-a-Service* (**RaaS**). À primeira vista, não chamava atenção frente a atores mais consolidados, como **REvil** ou **Ryuk**. No entanto, desde o início apresentou sinais de diferenciação: velocidade de criptografia acima da média, foco em automação e uma postura quase "corporativa" em sua comunicação. Essa fundação inicial seria o ponto de partida para uma das mais longas e bem-sucedidas operações de *Ransomware* já vistas.

Ano / Versão	Info Técnica	Info Estratégica	Impacto
2019 – LockBit 1.0	Foco em **criptografia rápida** e automação de infecção. Ferramenta ainda simples comparada a concorrentes.	Posicionamento inicial no submundo. Apostava em agilidade para aumentar taxa de pagamento.	Chamou atenção por reduzir tempo de resposta das vítimas, aumentando pressão.
2021 – LockBit 2.0	Melhorias no algoritmo de criptografia, evasão de segurança e módulos mais estáveis.	Expansão do **programa de afiliação (RaaS)**, com marketing agressivo em fóruns.	Passou a competir com **REvil** e **Ryuk**, atingindo empresas de saúde, governo e indústria.
2022 – LockBit 3.0 (Black)	Introdução de mecanismos de **dupla/tripla extorsão**, uso de DDoS e maior sofisticação técnica.	Lançamento do **primeiro "bug bounty" criminoso**. Ampliação de métodos de pagamento.	Tornou-se a operação mais ativa do mundo. Consolidação da **marca LockBit** no crime.
2022 – LockBit Green	Baseado no **código vazado do Conti**, adaptado ao ecossistema LockBit.	Demonstra pragmatismo: absorção de código externo para aumentar capacidades.	Expansão do arsenal, mostrando resiliência e flexibilidade do grupo.
2023–2024	Diversificação constante: melhorias anti-detection, uso de ferramentas legítimas (**LOLbins**).	Rapidez na reconstrução de infraestrutura após operações policiais.	Mantém protagonismo mesmo sob pressão internacional.
2025 – Atualidade	Operações mais descentralizadas, maior foco em afiliados de alta capacidade.	Estratégia de longo prazo, redundância e resiliência.	Segue como o **grupo de ransomware mais prolífico da década**.

Tabela 1 - Histórico do Lockbit Ransomware

A primeira versão, conhecida retroativamente como **LockBit 1.0**, já demonstrava a filosofia que o grupo carregaria ao longo dos anos: eficiência operacional e facilidade de uso para afiliados. Embora tecnicamente mais simples, destacava-se pela rapidez em criptografar

grandes volumes de dados, reduzindo a janela de resposta das vítimas. Isso colocava o **LockBit** em posição de vantagem estratégica, forçando empresas a reagirem sob forte pressão temporal, aumentando a probabilidade de pagamento.

A virada ocorreu em 2021 com a introdução do **LockBit 2.0**. O grupo já havia absorvido lições do mercado e observado o declínio de concorrentes derrubados por operações internacionais. O **LockBit 2.0** trouxe melhorias técnicas: algoritmos mais robustos e mecanismos de evasão de segurança, e reforçou a infraestrutura de afiliação. Ampliou o marketing no submundo, ofereceu suporte técnico a afiliados e programas de "recrutamento" em fóruns clandestinos, prometendo repasse de lucros vantajosos. *Foi nessa fase que o **LockBit** ganhou notoriedade internacional*, com ataques de alto perfil em setores críticos, incluindo saúde, governo e infraestrutura.

O auge veio com o **LockBit 3.0 (Black),** lançado em meados de 2022. Essa versão consolidou a posição do grupo como referência no ecossistema de *Ransomware*. Introduziu um programa de *bug bounty* criminoso, convidando *hackers* a reportar falhas em troca de recompensas financeiras; diversificou métodos de pagamento, incluindo criptomoedas alternativas; e aplicou extorsão dupla e tripla, como **DDoS** e divulgação pública de dados. Essa fase ampliou o impacto técnico e demonstrou habilidade em marketing agressivo, algo raro no submundo. *A imagem de profissionalismo e inovação passou a fazer parte da identidade do **LockBit***.

Figura 6 - Página com regras de Bug-Bounty do LockBit

Em paralelo, o grupo adotou a cooptação de código externo, evidenciada no **LockBit Green**, baseado no código vazado do **Conti**. Essa adaptação expandiu o arsenal técnico e simbolizou a mentalidade pragmática: absorver rapidamente capacidades externas e integrá-las ao modelo de negócio. Essa plasticidade explica a longevidade do **LockBit**, enquanto tantos outros grupos desapareceram diante da pressão de autoridades.

Apesar de operações de repressão internacionais, que derrubaram temporariamente parte da infraestrutura, o **LockBit** demonstrou resiliência. Reconstruíram painéis, migraram servidores e ajustaram canais de comunicação, mantendo o fluxo de ataques. Esse jogo de "gato e rato" consolidou a percepção de que o **LockBit** não é apenas um *malware*, mas uma organização criminosa resiliente, com redundância operacional e visão de longo prazo.

Nos anos recentes, o grupo expandiu escopo geográfico e setorial, mirando desde pequenas empresas até conglomerados multinacionais. A popularidade do programa de afiliação fez o **LockBit** responsável por uma parcela significativa dos incidentes de *Ransomware* globais, ultrapassando rivais históricos e tornando-se o *Ransomware* mais prolífico da última década.

Em síntese, a linha do tempo do **LockBit** não é apenas uma cronologia de versões de *malware*, mas a evolução de uma entidade que opera com mentalidade corporativa. Da simplicidade do 1.0 à sofisticação do 3.0 e Green, o grupo demonstrou capacidade de aprender, adaptar-se e expandir-se, mesmo diante de intensa pressão internacional. Essa trajetória reafirma o **LockBit** como um dos atores mais resilientes, inovadores e perigosos do cenário cibercriminosa contemporâneo.

TTPs – Comportamento Operacional do LockBit

O *playbook* operacional do **LockBit** costuma se desenrolar em fases reconhecíveis, ainda que existam variações entre afiliados e entre versões do *Ransomware*. Essas fases compreendem:

- Acesso Inicial
- Persistência e Escalada de Privilégios
- Movimentação Lateral e Coleta
- Exfiltração
- Preparação para Impacto (limpeza/antiforense)
- Criptografia e Extorsão Pública.

Em cada etapa, o grupo emprega um conjunto de técnicas reconhecíveis e recorrentes.

Tática (MITRE)	Técnica (ID)	Descrição Executiva	Impacto para a Vítima
Initial Access	*Spearphishing / Exploit Public-Facing App (**T1566/T1190**)*	Uso de e-mails maliciosos e exploração de sistemas expostos.	Quebra da primeira camada de defesa, ponto de entrada sigiloso.
Execution	*PowerShell / Scripts (**T1059**)*	Execução de *payloads in-memory* via scripts.	Bypass de defesas tradicionais (AV/EDR)
Persistence	*Scheduled Task / Services (**T1053/T1543**)*	Criação de tarefas agendadas e serviços persistentes.	Mantém o acesso mesmo após reboot.
Privilege Escalation	*Credential Dumping (**T1003**)*	Coleta de credenciais via LSASS, Mimikatz etc.	Acesso administrativo total.
Lateral Movement	*SMB/Remote Services (**T1021**)*	Uso de ferramentas nativas para se mover na rede.	Expansão rápida no ambiente corporativo.
Exfiltration	*Data Encrypted for Impact (**T1486**)*	Roubo e criptografia de dados críticos.	Pressão dupla: indisponibilidade + chantagem.
Impact	*Multi-Extortion (DDoS, vazamento)*	Ameaças públicas, ataques DDoS, exposição em "blogs".	Pressão máxima para forçar pagamento.

Tabela 2 - TTPs do Lockbit

Acesso inicial — o **LockBit** explora múltiplos vetores para entrar em ambientes alvo. Entre os vetores observados em campanhas documentadas estão exposição de serviços remotos, credenciais comprometidas adquiridas em mercados de acesso, campanhas de *phishing* direcionado e exploração de vulnerabilidades em *gateways* e *appliances*. Em muitas operações, a cadeia de entrada combina elementos automatizados, como varreduras e tentativas de acesso em massa, com ações personalizadas de engenharia social quando necessário.

Persistência e Escalada — uma vez dentro, os operadores buscam aumentar privilégios e estabilidade de acesso. Procedimentos observados incluem o uso de ferramentas de roubo de credenciais para obter credenciais de nível elevado e a criação de mecanismos para manter persistência no ambiente. Ferramentas/ofuscadores comerciais e de código aberto, assim como binários legítimos reutilizados para fins maliciosos, aparecem frequentemente no repertório. A combinação de técnicas visa reduzir o tempo até se obter controle suficiente para operações subsequentes.

Movimentação Lateral e Coleta — após consolidar privilégios, a operação tipicamente se espalha lateralmente por servidores e estações relevantes, visando repositórios de dados críticos. Os atacantes empregam protocolos e métodos nativos do ambiente corporativo para se mover, bem como *frameworks* de pós-exploração comerciais e containerizados que facilitam a execução remota e o gerenciamento de cargas úteis. Nesta fase, há foco em identificar locais de alto valor (bases de dados, arquivos corporativos, *backups*) para subsequente coleta de dados.

Exfiltração — uma característica definidora nas campanhas **LockBit** é a exfiltração de dados anterior à encriptação. A operação já foi associada tanto a soluções proprietárias de extração automatizada (**StealBit**) quanto a *uploads* para serviços de armazenamento em nuvem ou infraestrutura de terceiros. O propósito é estruturar uma ameaça de dupla extorsão: tornar indisponíveis os dados via criptografia e, simultaneamente, ganhar alavanca adicional por meio da ameaça de vazamento público.

Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

Figura 7 - Velocidade de Download do Stealbit (Fonte: KELA/Twitter)

Antiforense e preparação do Impacto — antes de executar a fase de impacto, operadores do **LockBit** costumam realizar ações destinadas a reduzir a capacidade de recuperação e investigação: manipulação de *shadow copies*, tentativas de interromper processos de *backup* ou de desabilitar proteções identificáveis, e ações de limpeza de *logs*. Essas medidas têm a finalidade explícita de maximizar o custo e o dano gerado pela ação quando a criptografia for aplicada.

Criptografia e extorsão — a entrega do *payload* de criptografia é concebida para causar impacto rápido e visível. Versões evoluídas do **LockBit** demonstraram técnicas para otimizar velocidade de encriptação e, em alguns casos, criptografar seletivamente para

acelerar o efeito disruptivo. Paralelamente, a infraestrutura de extorsão pública, como *websites* de vazamento, painéis de gerenciamento e canais de comunicação para negociação, é utilizada para pressionar alvos a pagar, muitas vezes com mensagens públicas que maximizam pressão reputacional e operacional.

Ferramentas e ecossistema — historicamente, o arsenal associado a campanhas **LockBit** inclui tanto componentes desenvolvidos especificamente para o *Ransomware* quanto um conjunto de ferramentas de terceiros reutilizadas. *Frameworks* de **C2** comerciais, utilitários de pós-exploração e ferramentas para manipulação de arquivos foram correlacionados em diversas investigações. Além disso, a estrutura **RaaS** implica que afiliados distintos podem introduzir variações operacionais, o que resulta em heterogeneidade nos artefatos observáveis entre incidentes.

Artefatos e sinais observáveis — a operação deixa diversos vestígios que, de forma consistente, reaparecem em relatos públicos e *dumps* vazados: mudanças maciças no padrão de criação/alteração de arquivos durante a fase de criptografia; evidências de transferências de dados para endpoints externos; e artefatos relacionados a manipulação de serviços de *backup* e *logs*. Também emergem indícios administrativos, como a criação de contas com privilégios, e traços de uso de ferramentas de *Credential-dumping*.

Comportamento organizacional — além das TTPs técnicas, o **LockBit** se destaca por práticas organizacionais que influenciam seu impacto: modelo **RaaS** que delega atividades operacionais a afiliados; investimentos em **P&D** criminal (evidenciado pelo lançamento de versões, *builders* e iniciativas públicas como *bug-bounties* no passado); e práticas de comunicação pública e de mercado que reforçam sua "marca" no ecossistema criminoso. Isso cria heterogeneidade nas campanhas, mas mantém um núcleo de procedimentos reconhecíveis.

Por fim, é importante perceber que as **TTPs** do **LockBit** constituem um conjunto dinâmico: à medida que a aplicação da lei e a indústria de segurança evoluem, o ator adapta sua cadeia operacional, incorpora capacidades de outras famílias de malware e altera práticas de afiliação. Este retrato contextual das **TTPs** serve como fundamento para o aprofundamento técnico subsequente, que deverá detalhar atributos específicos por versão, amostras e artefatos técnicos identificáveis em logs e telemetria.

Modelo de Negócio e Programa de Afiliados

O modelo **RaaS** se organiza como uma cadeia de valor onde o fornecedor central (no caso, o **LockBit**) projeta, mantém e atualiza o produto (o *Ransomware*, painéis, *builder*, infraestrutura de *leak* e canais de pagamento). Do outro lado, existem afiliados, que são operadores independentes que compram/arrendam o direito de usar o produto para executar intrusões, lateralizar, exfiltrar e disparar a criptografia. Entre esses polos emergem intermediários especializados: *brokers* de acesso inicial (**IABs**) que vendem *logins* e acessos a redes comprometidas; negociadores que lidam com vítimas; e serviços adjacentes (mixers/convertidores de cripto, *hosts bulletproof*, infraestrutura de **C2** terceirizada).

Do ponto de vista de oferta e demanda, o **LockBit** atua como um *market-maker*: produz um produto padronizado e replicável (builds configuráveis, documentação, painel de gestão) e cria incentivos para que operadores de campo, muitos com habilidades variadas, o empunhem. *Isso reduz a barreira técnica de entrada para criminosos menos sofisticados e amplia a capacidade de ataque da rede* **LockBit** *sem aumento linear de risco operacional para o núcleo*.

Papel / Ator	Função Principal	Observações
Núcleo (desenvolvedores / administradores)	Desenvolvimento do *malware*, manutenção do painel, políticas de afiliação.	Centraliza R&D criminoso e controla infraestrutura crítica.
Afiliados / Operadores	Intrusão, pós-exploração, exfiltração e disparo do *ransomware*.	Escalabilidade de ataques; variabilidade tática entre afiliados.
Brokers / IABs	Venda de acessos iniciais e credenciais.	Mercado secundário que alimenta o pipeline de ataques.
Negociadores	Contato com vítima, gestão de pagamento.	Especialistas em extração de valor sem necessariamente executar intrusão.
Serviços auxiliares	Mixers de cripto, *bulletproof hosting*, serviços de DDoS.	Permitem operacionalização financeira e técnica da extorsão.
Moderadores / suporte	Onboarding de afiliados, resolução de disputas, "suporte" técnico ao produto.	Incrementa confiança e reduz atrito comercial na comunidade criminosa.

Tabela 3 - Modelo de Negócio do Lockbit

Ciclo de Vida do Afiliado: Onboarding, Operação e Churn

O processo de transformação de um estranho em afiliado segue uma lógica quase corporativa: identificação/recrutamento (via fóruns, indicações), *vetting* (uma checagem de antecedentes para evitar infiltrações operacionais), acesso a *builders*/painéis, e suporte contínuo. Afiliados recebem documentação, versões do *builder*, e em muitos casos "suporte técnico" para configurar implantações. Em troca, o modelo financeiro prevê uma divisão dos lucros, que foi historicamente reportada em diversas fontes como uma fatia majoritária para o afiliado (por exemplo, faixas comuns de 60–80% para o

operador, 20–40% para o operador central), embora isso varie por contrato e por versão do painel.

O *churn* (taxa de evasão) de afiliados é gerenciado por incentivos: garantia de pagamento, reputação do operador central (cumprimento de promessas), e benefícios exclusivos (acesso a builds mais eficientes, bug-bounties, sessões de treinamento). Ao mesmo tempo, o núcleo impõe regras informais e políticas, que funcionam como mecanismos de governança e mitigam riscos geopolíticos.

PRODUTOS E SERVIÇOS COMERCIALIZADOS INTERNAMENTE

O "portfólio" comercial do ecossistema **LockBit** inclui:

- Builders configuráveis (geradores de *payload* com parâmetros customizáveis);
- Painéis de gestão para monitoramento de campanhas, lista de vítimas e negociações;
- Sites de vazamento/*leak* que servem a dupla função de pressionar vítimas e catalogar ativos monetizáveis;
- Ferramentas de exfiltração integradas (módulos para *upload* automático a *clouds* ou servidores externos);
- Suporte/gestão de crise (negociadores e "garantia" de pagamento em alguns arranjos);

Algumas dessas ofertas foram objeto de "inovação de produto": por exemplo, o anúncio de *bug-bounties* (incentivo para terceiros encontrarem falhas no próprio *malware*) ou a disponibilidade de painéis *user friendly* que diminuem a curva de aprendizado para afiliados.

GOVERNANÇA, REGRAS E NORMAS INTERNAS

Embora anárquico à primeira vista, o ecossistema apresenta elementos de governança: políticas tácitas (por exemplo, evitar atacar organizações e países específicos), termos informais de serviço, mecanismos de resolução de conflitos e requisitos de reputação para participar do programa. Essas normas funcionam como filtros de gestão de risco, manter a operação fora de pontos de maior atrito político ou reduz pressões de aplicação da lei local, até certo ponto.

Também há evidência de instrumentos financeiros internos: registros, *wallets* e procedimentos para dividir pagamentos; quando essas estruturas vazam, como em dumps de painéis, fornecem uma janela direta para entender o fluxo financeiro e a lógica econômica por trás das operações.

ECONOMIA, INCENTIVOS E ALAVANCAS DE CRESCIMENTO

A arquitetura econômica do **RaaS** gera incentivos claros:

- Para afiliados: acesso à tecnologia sofisticada sem necessidade de desenvolvê-la, potencial de lucro rápido, suporte e reputação para facilitar negociações.

- Para o núcleo: escala sem exposição proporcional, receita recorrente via cortes/fees, capacidade de reinvestir em **P&D** criminoso.

Esse arranjo reduz o custo marginal de cada ataque para o núcleo e transforma os afiliados em multiplicadores de alcance. Além disso, a existência de intermediários (**IABs**) cria um mercado paralelo que acelera a entrega de potenciais vítimas ao afiliado, fechando um ciclo econômico eficiente e lucrativo.

Riscos, fragilidades e adaptação estrutural

Apesar da aparente robustez, o modelo **RaaS** apresenta fragilidades estratégicas que também explicam por que operações de aplicação da lei podem ter impacto material: a centralização da infraestrutura crítica (painéis, *leak sites*, *builders*) cria pontos de alavancagem para ações disruptivas. A necessidade de confiança entre atores (para garantir pagamentos e evitar infiltrações) cria *vetting* e procedimentos que, quando vazados, expõem a cadeia, e a dependência de serviços externos (hospedagem, conversores de cripto) introduz vetores adicionais de risco operacional.

Em contrapartida, o ecossistema compensa com redundância operacional (painéis múltiplos, *builds* vazados, replicação do modelo por imitadores), recuperação rápida e fragmentação, são fenômenos observados após operações de repressão, quando o núcleo se dispersa e partes do conhecimento técnico alimentam novos atores.

Dinâmica concorrencial e sinais de cartelização

A evolução da competição entre **RaaS** revelou um nível de profissionalização que torna o setor mais parecido com um mercado oligopolístico: grupos dominantes competem por talento, adoção de afiliados e portfólios de serviços. Indícios recentes de coordenação entre grupos, como menções a acordos tácitos, divisão de áreas geográficas/temáticas e até propostas públicas de coalizão, sugerem uma tentativa de cartelização do mercado criminal, onde vantagens estratégicas (evitar competição direta, padronizar métodos de pagamento, coordenar preços de resgate) podem aumentar a eficiência e a previsibilidade das operações. Essa possível consolidação altera não apenas o volume de ataques, mas também o perfil tático e a escala de impacto, ao concentrar poder em clubes de elite criminosos.

O modelo de negócio do **LockBit** exemplifica a profissionalização do crime cibernético: uma operação que combina produto, mercado e governança para transformar capacidades técnicas em receita recorrente. O programa de afiliados funciona como a alavanca de escala, onde ao delegar execução a atores diversos, o núcleo maximiza alcance e lucros enquanto tenta modular risco por meio de governança e infraestrutura proprietária. Entender essa arquitetura é essencial para interpretar a dinâmica observada de ataques massivos, o fenômeno de rápida propagação de técnicas e a formação de cadeias econômicas que sustentam a persistência do grupo no longo prazo.

CONCLUSÃO

O **LockBit** consolidou-se como um marco na história do cibercrime moderno, simbolizando a transição definitiva do *Ransomware* de uma ameaça técnica isolada para um modelo de negócio estruturado, global e autossustentável. Sua longevidade e adaptabilidade demonstram que a cibercriminalidade opera hoje sob lógicas corporativas, com pesquisa e desenvolvimento, parcerias, marketing e reinvestimento, em uma escala que desafia fronteiras técnicas e jurídicas.

Mais do que um simples grupo de ataque, o **LockBit** representa um ecossistema descentralizado que combina inovação tecnológica, eficiência operacional e estratégia de mercado. A capacidade de sobreviver a operações internacionais, reconstruir infraestrutura e manter uma base ativa de afiliados evidencia a maturidade de sua governança interna e o grau de profissionalização alcançado pelo crime digital.

Para governos e organizações, o aprendizado é inequívoco: o enfrentamento desse tipo de ameaça exige mais do que tecnologia; requer coordenação, inteligência compartilhada e visão estratégica de longo prazo. A desarticulação de um núcleo não implica o fim de um ecossistema, apenas o início de um novo ciclo, mais adaptado e, muitas vezes, mais perigoso.

O **LockBit** é, portanto, um lembrete de que o cibercrime evolui em simetria com a própria cibersegurança. E compreender sua trajetória não é apenas uma questão de análise técnica, mas de antecipação estratégica, sendo essencial para quem busca defender o futuro digital com realismo e eficácia.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- TrendMicro – Ransomware SpotLight: LockBit
- Barracuda - The Rise and Fall of LockBit Ransomware
- SearchLight Cyber – Operation Cronos and LockBit
- Daily Dark Web – LockBit Ransomware Group Unveils Version 5.0
- CISA.gov – Understanding Ransomware Threat Actors: LockBit

AUTORES

- **Gustavo Santos – Security Researcher**

heimdall
security research
A DIVISION OF ISH