

ARX CYBER

RELATÓRIO DE PESQUISAS

LOCKBIT

Ransomware-as-a-Service, dupla extorsão e o retorno com a versão 5.0

SOBRE ESTE RELATÓRIO

O **LockBit** é um dos nomes mais conhecidos do cibercrime. Este relatório reúne contexto de inteligência, análise técnica e recomendações em três camadas, para que diferentes públicos da organização encontrem o nível de detalhe de que precisam.

ESTRATÉGICO

Para gestão e liderança: o que é a ameaça, quem ela atinge e qual o impacto no negócio.

TÁTICO

Para arquitetura e segurança: capacidades, cadeia de ataque, técnicas MITRE e análise do artefato.

OPERACIONAL

Para SOC e resposta a incidentes: indicadores de comprometimento e pontos de caça.

Resumo da publicação

Item	Informação
Tema	LockBit: RaaS, dupla extorsão e o retorno com a versão 5.0
Data de publicação	03 de novembro de 2026
Autoria	Equipe CTI - ARX CYBER
Classificação	TLP:CLEAR
Artefato analisado	7ea5afbc...c2277b82

SUMÁRIO

1 Introdução executiva 5

2 Estratégico 5

2.1 Introdução sobre a ameaça 5

2.2 Linha do tempo da ameaça 6

2.3 Modelo RaaS e dupla extorsão 6

2.4 Impacto estratégico 7

3 Tático 7

3.1 Visão geral do LockBit 5.0 7

3.2 Capacidades técnicas 8

3.3 Cadeia de ataque típica 8

3.4 Mapeamento MITRE ATT&CK 9

4 Análise do artefato 10

4.1 Instantâneo da amostra 10

4.2 Análise estática 11

4.3 Detecção por motores antivírus 11

5 Recomendações 13

6 Operacional 14

6.1 Indicadores de Comprometimento (IoC) 15

6.2 LockBit 5.0 ransomware 15

7 Referências 15

8 Autores 15

LISTA DE TABELAS

Tabela 1 - Papéis no ecossistema RaaS do LockBit. 6

Tabela 2 - Impactos estratégicos de um incidente LockBit. 7

Tabela 3 - Capacidades do criptografador LockBit 5.0 (fontes públicas). 8

Tabela 4 - Mapeamento MITRE ATT&CK do LockBit 5.0. 10

Tabela 5 - Instantâneo da amostra analisada. 10

Tabela 6 - Detecções selecionadas por fornecedor. 13

Tabela 7 - Indicadores de Comprometimento. 15

Tabela 8 - Indicadores comportamentais e de host. 15

LISTA DE FIGURAS

Figura 1 - Evolução do LockBit, de 2019 ao lançamento da versão 5.0. 6

Figura 2 - Cadeia de ataque simplificada observada em operações LockBit. 9

Figura 3 - Registro da amostra no MalwareBazaar (assinatura LockBit, tag lockbit5). 11

Figura 4 - Distribuição de detecções da amostra no VirusTotal. 12

Figura 5 - Resumo da amostra no VirusTotal. 12

Figura 6 - Amostra de detecções por motores antivírus no VirusTotal. 13

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência de ameaças da **ARX CYBER**, tem como objetivo apresentar uma compreensão aprofundada do **LockBit**, um dos grupos de **Ransomware-as-a-Service** (RaaS) mais prolíficos da história recente do cibercrime, e do seu retorno com a versão **LockBit 5.0**.

3	7.000+	57/69	63
PLATAFORMAS ALVO WINDOWS · LINUX · ESXI	ATAQUES CONHECIDOS EM 120 PAÍSES	MOTORES DE AV QUE DETECTAM A AMOSTRA	SERVIÇOS DE SEGURANÇA NA LISTA DE TÉRMINO

2 ESTRATÉGICO

2.1 INTRODUÇÃO SOBRE A AMEAÇA

O **LockBit** opera desde 2019 como um programa de **Ransomware-as-a-Service**: um núcleo de desenvolvedores mantém o código, o painel de afiliados e o site de vazamento, enquanto **afiliados** executam as intrusões e dividem o resgate com o grupo. Esse modelo permitiu escala industrial, com **mais de 7.000 ataques conhecidos em cerca de 120 países**, e fez do LockBit uma referência para o ecossistema de extorsão digital.

SUAS PRINCIPAIS CARACTERÍSTICAS INCLUEM:

- **Dupla extorsão:** além de criptografar os arquivos e exigir pagamento pela chave, o grupo **rouba dados sensíveis** e ameaça publicá-los em seus sites de vazamento caso o resgate não seja pago.
- **Automação e velocidade:** as ferramentas associadas ao grupo são otimizadas para se espalhar rapidamente por redes corporativas (movimento lateral), desativar soluções de segurança e eliminar cópias de sombra (**shadow copies**).
- **Resiliência e evolução de variantes:** LockBit 2.0, 3.0 (“Black”), 4.0 e agora 5.0. A marca seguiu operando por meio de afiliados mesmo após a **Operação Cronos**, a ação internacional de desarticulação conduzida em 2024.

O **LockBit 5.0** surgiu no início de **setembro de 2025** e representa o retorno mais ativo da marca desde a remoção pelas autoridades. O novo criptografador combina uma **cifra de fluxo com troca de chaves de curva elíptica** e é executado em **Windows, Linux e VMware ESXi**, a partir de um **carregador em memória de dois estágios**.

2.2 LINHA DO TEMPO DA AMEAÇA

A trajetória do grupo mostra uma marca que absorve golpes e retorna. A Operação Cronos (liderada pela **National Crime Agency** do Reino Unido, com apoio do FBI) apreendeu infraestrutura, comprometeu painéis de administração e expôs dados de afiliados. Ainda assim, o desenvolvimento continuou e, ao completar seis anos, o grupo anunciou a quinta geração do seu ransomware.

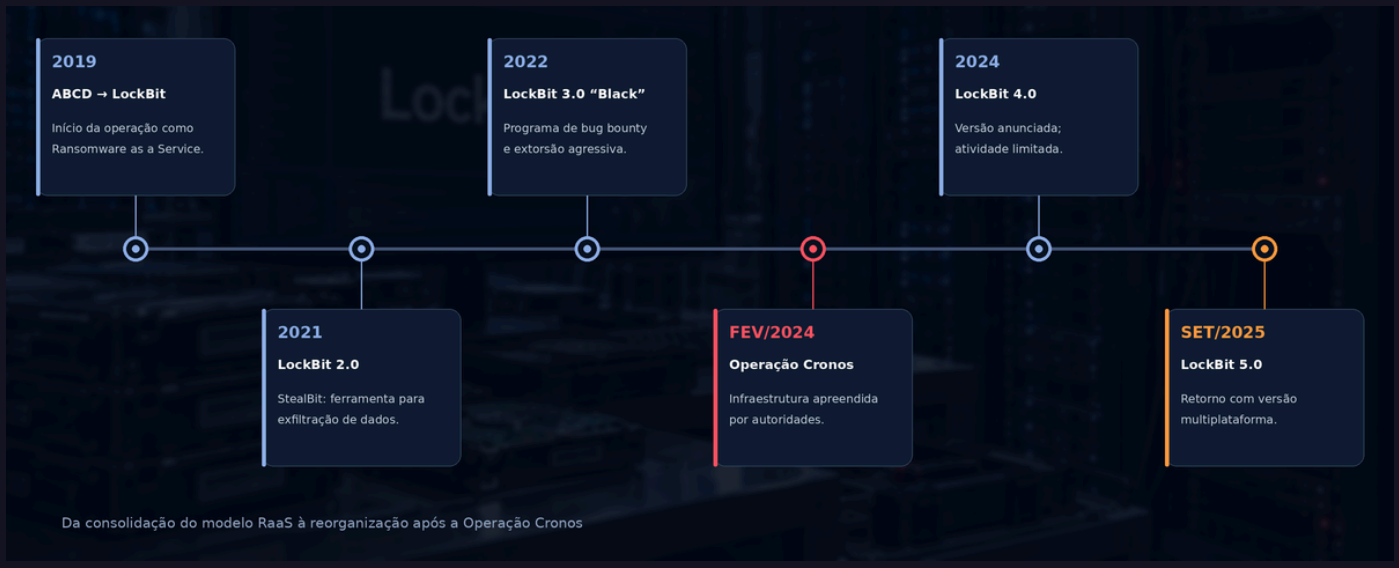


Figura 1 - Evolução do LockBit, de 2019 ao lançamento da versão 5.0.

2.3 MODELO RAAS E DUPLA EXTORSÃO

O valor do LockBit para o crime organizado está menos no código e mais no **modelo de negócio**. Cada papel da cadeia é terceirizado, o que reduz a barreira de entrada e multiplica o número de vítimas.

Papel	Responsabilidade	Observação
Operadores (núcleo)	Desenvolvimento do criptografador, painel de afiliados, site de vazamento e portal de negociação	O portal mantém o "Chat with Support" e suporte a pagamentos em criptomoedas
Afiliados	Acesso inicial, movimento lateral, exfiltração e execução do ransomware	Escolhem alvos e dividem o resgate com o núcleo
Corretores de acesso	Venda de credenciais e acessos a redes comprometidas	Reduzem o tempo entre invasão e impacto
Site de vazamento	Pressão pública: publicação de dados roubados e contagem regressiva	Pesquisadores já apontaram entradas antigas recicladas, sinal de instabilidade operacional

Tabela 1 - Papéis no ecossistema RaaS do LockBit.

ALIANÇA ENTRE GRUPOS

Segundo a SOCRadar, o grupo DragonForce propôs em fórum underground que LockBit e Qilin coordenassem regras em vez de competir, e o LockBit teria concordado publicamente. Não há confirmação de que um cartel formal tenha sido implementado, mas o episódio indica uma tentativa de estabilizar o mercado de afiliados.

2.4 IMPACTO ESTRATÉGICO

Para as organizações, o impacto de um incidente LockBit vai além da perda de dados: há paralisação de sistemas críticos, custos de recuperação, exposição regulatória e dano reputacional. A versão 5.0 amplia o risco ao mirar diretamente **hipervisores VMware ESXi**, onde uma única execução pode cifrar dezenas de máquinas virtuais.

Vetor de impacto	O que acontece na prática	Consequência para o negócio
Parada de operação	Indisponibilidade de servidores, ERP, bancos de dados e ambientes virtualizados	Perdas financeiras imediatas e multas contratuais
Extorsão e vazamento	Roubo de dados antes da criptografia e ameaça de publicação	Impacto reputacional e jurídico (LGPD / contratos)
Perda de visibilidade	Desativação de ETW, término de serviços de segurança e limpeza de logs	Investigação forense dificultada e tempo de contenção maior
Efeito cascata	Ataque a um fornecedor ou provedor afeta clientes	Atrasos sistêmicos e risco na cadeia de suprimentos
Recuperação inviabilizada	Remoção de cópias de sombra e ataque a backups acessíveis	Dependência de backups offline/imutáveis

Tabela 2 - Impactos estratégicos de um incidente LockBit.

No **Brasil**, organizações com Active Directory amplamente integrado, virtualização VMware, acessos remotos expostos e baixa segmentação de rede reúnem exatamente o perfil que o modelo de afiliados explora, independentemente do setor. A ARX CYBER recomenda tratar o LockBit como cenário de referência em exercícios de resposta a incidentes.

3 TÁTICO r

3.1 VISÃO GERAL DO LOCKBIT 5.0

A análise pública da Trend Micro, iniciada em setembro de 2025, classifica o LockBit 5.0 como uma **evolução da versão 4.0**, e não um simples **rebrand**: há reuso extenso de código, incluindo os mesmos algoritmos de **hashing** para resolução de APIs e tratamento de **strings**. As novidades concentram-se em menu de ajuda refinado, modo invisível e reforço de antiforense. O suporte multiplataforma remonta ao LockBit 2.0.

3.2 CAPACIDADES TÉCNICAS

Categoria	Comportamento observado	Relevância defensiva
Plataformas	Builds funcionais para **Windows**, **Linux** e **VMware ESXi**; o build Linux espelha a versão Windows e registra cada etapa	Servidores e hipervisores entram no escopo do impacto, não só estações
Criptografia	Cifra de fluxo com troca de chaves de curva elíptica; extensão aleatória de **16 caracteres** e tamanho original gravado no rodapé do arquivo	Extensão fixa deixa de ser indicador confiável
Execução	Carregador em memória de dois estágios, **DLL reflection**, forte ofuscação e empacotamento	Poucos artefatos em disco; assinaturas estáticas têm baixa eficácia
Evasão	Patch em EtwEventWrite (retorno imediato, 0xC3) para silenciar o ETW; término de serviços por **hash** de nome contra lista de **63 entradas**	Perda de telemetria e queda de EDR podem preceder a criptografia
Antiforense	Limpeza de logs via EvtClearLog após a execução; modo invisível sem extensão nem nota	Detectar o evento de limpeza de logs ganha prioridade
Impacto configurável	Modos local ou rede, **wipe** de espaço livre, seleção e exclusão de diretórios, nota em todos os diretórios, só em C:\ ou nenhuma	Comportamento varia por afiliado e por operação
Geofencing	Evita sistemas com configuração de idioma e geolocalização russas	Característica comum em grupos de língua russa

Tabela 3 - Capacidades do criptografador LockBit 5.0 (fontes públicas).

3.3 CADEIA DE ATAQUE TÍPICA

Como o LockBit é operado por afiliados, o **acesso inicial varia**: credenciais válidas, serviços remotos expostos (VPN e RDP), exploração de vulnerabilidades em dispositivos de borda e **phishing** são os caminhos mais recorrentes. A partir daí, o padrão é consistente: ganhar privilégio no domínio, exfiltrar, desativar defesas e executar o criptografador no maior número possível de hosts e hipervisores.



Figura 2 - Cadeia de ataque simplificada observada em operações LockBit.

3.4 MAPEAMENTO MITRE ATT&CK

A tabela abaixo relaciona as capacidades descritas em fontes públicas e observadas na análise estática às técnicas do **MITRE ATT&CK**. O mapeamento reflete comportamento **reportado pela comunidade** para o LockBit 5.0; a amostra deste relatório passou por análise estática, não por execução.

Tática	Técnica	ID	Contexto
Execução	Reflective Code Loading	T1620	Carregamento do payload em memória via DLL reflection
Evasão de defesa	Obfuscated Files or Information	T1027	Binário empacotado, entropia de .rdata de 7,99
Evasão de defesa	Dynamic API Resolution	T1027.007	Ausência de IAT e resolução por **hash** de API
Evasão de defesa	Indicator Blocking	T1562.006	Patch em EtwEventWrite
Evasão de defesa	Clear Windows Event Logs	T1070.001	Limpeza de logs com EvtClearLog
Descoberta	System Language Discovery	T1614.001	Verificação de idioma e localização (geofencing)

Tática	Técnica	ID	Contexto
Movimento lateral	Remote Services (SMB, RDP)	T1021	Propagação por afiliados em redes corporativas
Exfiltração	Exfiltration Over C2 / Web Service	T1041 / T1567	Roubo de dados para dupla extorsão
Impacto	Service Stop	T1489	Término de serviços de segurança e de aplicações
Impacto	Inhibit System Recovery	T1490	Exclusão de cópias de sombra
Impacto	Data Encrypted for Impact	T1486	Criptografia em Windows, Linux e ESXi

Tabela 4 - Mapeamento MITRE ATT&CK do LockBit 5.0.

4 ANÁLISE DO ARTEFATO

A equipe CTI da ARX CYBER analisou a amostra identificada pelo SHA-256 7ea5afbc166c4e23498a a9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82, obtida do **MalwareBazaar**. A amostra foi registrada em **15/09/2025** pelo repórter **Neiki__** com a assinatura **LockBit** e as **tags** exe , lockbit , lockbit5 , ransomware e signed.

4.1 INSTANTÂNEO DA AMOSTRA

Categoria	Detalhe
Família	LockBit 5.0 (atribuição por assinatura em repositório e consenso de AV)
Formato	PE32 + executável (console), x86-64, Microsoft Windows
Tamanho	710.560 bytes
Primeira ocorrência	15/09/2025 06:07:35 (MalwareBazaar)
Privilégios	Manifesto com requireAdministrator
Metadados do manifesto	Identidade BorgWarner.Blender, descrição “Blender” (disfarce)
Vetor de infecção	Não determinado (requer contexto de entrega)

Tabela 5 - Instantâneo da amostra analisada.

> **NOTA SOBRE CONFIANÇA**
> A análise estática isolada classifica o binário como **empacotado e genérico** (confiança moderada). A atribuição ao **LockBit 5.0** vem do consenso externo: assinatura LockBit no MalwareBazaar e 57 detecções com nomes explícitos de LockBit no VirusTotal. Pelo conjunto, a ARX CYBER trata a amostra como LockBit 5.0 com **confiança moderada a alta**. O nome **BorgWarner** no manifesto é metadado de disfarce e não indica comprometimento dessa empresa.

4.2 ANÁLISE ESTÁTICA

- **Seção .rada:** entropia de **7,9992**, indicando forte compactação ou criptografia de código e dados.
- **Ausência de IAT:** não foi possível mapear chamadas de API na **Import Address Table**, o que sugere empacotador ou resolução dinâmica de APIs (LoadLibrary / GetProcAddress ou **hashing**).
- **Manifesto Win32:** recurso RT_MANIFEST com identidade BorgWarner.Blender e nível de execução requireAdministrator.

Esses achados são **consistentes** com a descrição pública do LockBit 5.0 (ofuscação pesada, carregamento em memória e resolução de API por **hash**). A confirmação do comportamento exige análise dinâmica e **unpacking**, não realizados nesta etapa.

```
sha256_hash:   7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82
sha1_hash:     cdd5717fd3bfd375c1c34237c24073e92ad6dccc
md5_hash:      95daa771a28eaed76eb01e1e8f403f7c
first_seen:    2025-09-15 06:07:35
file_name:     7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82
file_size:     710560 bytes
file_type:     exe
mime_type:     application/x-dosexec
tlsh:          T1D0E4D0ADFD4A8960D553F5BCBE1EB49153017AB80F39A2B7740925E10E738D83AB13C9
reporter:      Neiki__
signature:     LockBit
tags:          exe lockbit lockbit5 Ransomware signed
```

Figura 3 - Registro da amostra no MalwareBazaar (assinatura LockBit, tag lockbit5).

4.3 DETECÇÃO POR MOTORES ANTIVÍRUS

No VirusTotal, a amostra foi submetida **53 vezes**, com última análise em **10/10/2026**. O rótulo de ameaças é ransomware.lockbit/misc.



Figura 4 - Distribuição de detecções da amostra no VirusTotal.

```
MDS hash:            95daa771a28eaed76eb01e1e8f403f7c
SHA1 hash:           cdd5717fd3bfd375c1c34237c24073e92ad6dccc
SHA256 hash:         7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82

Malicious:           57
Undetected:          12

Type Description:    Win32 EXE
Size:                710560
Last Analysis Date:  2026-10-10 20:51:53
Type Tag:            peexe
Times Submitted:     53

Threat Label:        ransomware.lockbit/misc
Classification:
                     popular count: 24
                     label:      ransomware

                     popular count: 20
                     label:      trojan

Trid:
                     file type:     Win64 Executable (generic)
                     probability:   51.9

                     file type:     OS/2 Executable (generic)
                     probability:   16.1

                     file type:     Generic Win/DOS Executable
                     probability:   15.9

                     file type:     DOS Executable (generic)
                     probability:   15.9
```

Figura 5 - Resumo da amostra no VirusTotal.

Fornecedor	Nome da detecção
ClamAV	Win.Ransomware.LockBit5-10058155-1
BitDefender / eScan / GData	Gen:Variant.Ransom.Lockbit.210
ESET NOD32	Win64/Filecoder.Lockbit.F Trojan
Emsisoft	Trojan-Ransom.LockBit.LA (A)
AhnLab-V3	Ransomware/Win.LockBit.C5798524
Arcabit	Trojan.Ransom.Lockbit.210
Elastic	Malicious (high confidence)
CrowdStrike Falcon	Win/malicious_confidence_100%

Tabela 6 - Detecções selecionadas por fornecedor.

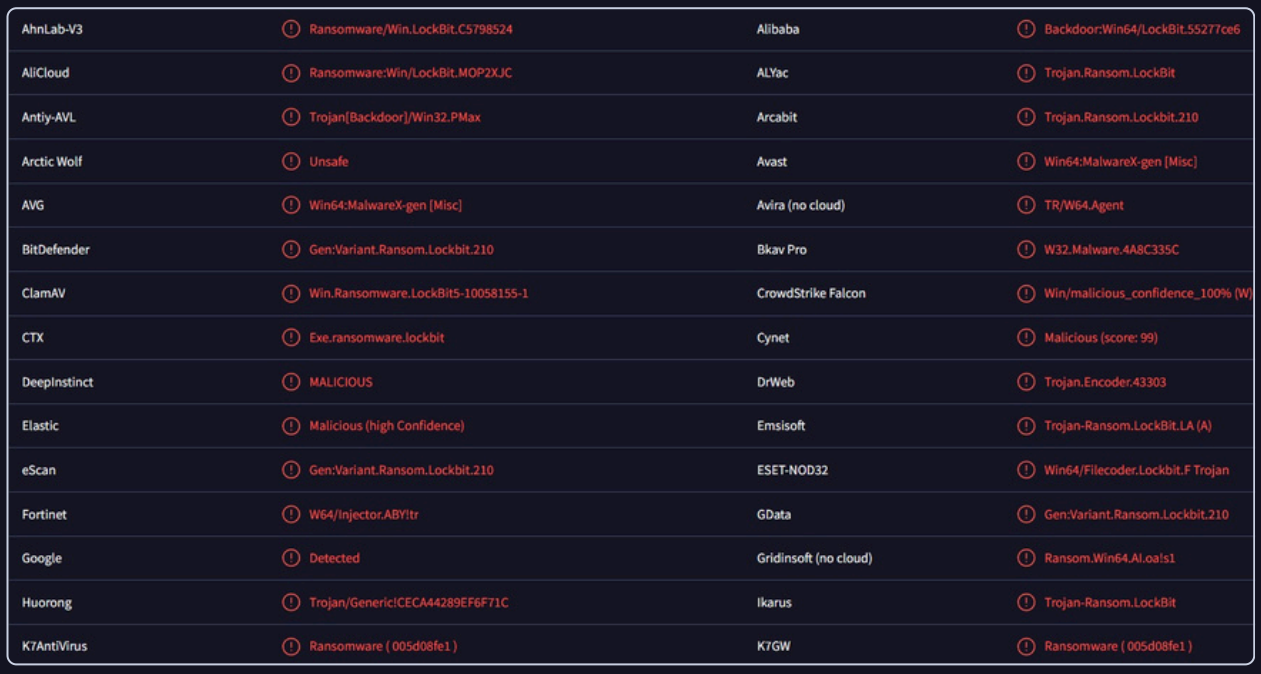


Figura 6 - Amostra de detecções por motores antivírus no VirusTotal.

5 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados pela ARX CYBER recomendam-se as medidas abaixo para reduzir a probabilidade e o impacto de uma infecção por LockBit:

1. **Reduzir a exposição de serviços externos.** VPNs, RDP e dispositivos de borda atualizados, com **hardening** e MFA obrigatório, inclusive para terceiros.

2. **Proteger a camada de virtualização.** Isolar a rede de gerenciamento do ESXi/vCenter, desabilitar SSH quando não necessário, ativar **lockdown mode** e manter backups das VMs fora do domínio.

3. **Fortalecer identidade e acesso.** Menor privilégio, eliminação de contas compartilhadas, camadas de administração e monitoramento de uso anômalo de credenciais válidas.

4. **Backups resilientes e testados.** Cópias offline ou imutáveis 3-2-1-1-0, com restauração testada regularmente, sem depender do pagamento de resgate.

5. **Proteção contra adulteração do EDR.** Ativar **tamper protection**, alertar sobre término de serviços de segurança e sobre lacunas de telemetria (silêncio repentino de um agente).

6. **Detecções comportamentais.** Foco em exclusão de **shadow copies**, limpeza de logs (eventos 1102 e 104), uso de SMB, RDP, PsExec e WMI e grandes volumes de leitura e renomeação de arquivos.

7. **Monitorar exfiltração.** Egresso para serviços de armazenamento em nuvem, uso de ferramentas como **rclone** ou MEGAsync e transferências volumosas fora do horário.

8. **Capacidade contínua de CTI e resposta.** Plano de resposta a ransomware testado, com contatos jurídicos, de seguro e de autoridades definidos.

6 OPERACIONAL

A ARX CYBER realiza o tratamento de indicadores de comprometimento coletados por meio de fontes abertas, fechadas e de análises da sua equipe de segurança. Abaixo listamos os Indicadores de Comprometimento (IoCs) relacionados à análise do artefato deste relatório.

6.1 INDICADORES DE COMPROMETIMENTO (IOC)

6.2 LOCKBIT 5.0 RANSOMWARE

Indicadores do artefato	
md5:	95daa771a28eaed76eb01e1e8f403f7c
sha1:	cdd5717fd3bfd375c1c34237c24073e92ad6dccc
sha256:	7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82
File name:	7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82.exe

Tabela 7 - Indicadores de Comprometimento.

Tipo	Indicador	Contexto
Artefato de host	Manifesto BorgWarner.Blender / descrição Blender	Metadado interno usado para mascarar a aplicação
Artefato de host	Binário PE32+ x86-64 de 710.560 bytes com requireAdministrator	Elevação de privilégio solicitada na execução
Compor tamento	Escrita de 0xC3 em EtwEventWrite	Silenciamento do ETW no processo
Compor tamento	Arquivos com extensão aleatória de 16 caracteres	Indicador por padrão, não por valor fixo
Compor tamento	Eventos 1102 (Security) e 104 (System) de limpeza de logs	Antiforense pós-execução

Tabela 8 - Indicadores comportamentais e de host.

7 REFERÊNCIAS

- ARX CYBER – Threat Intelligence
- CyberInsider – LockBit 5.0 surfaces with support for Windows, Linux and ESXi
- Trend Micro – LockBit 5.0 targets Windows, Linux and ESXi
- SOCRadar – LockBit 5.0 ransomware cartel: what you need to know
- MalwareBazaar (abuse.ch)
- VirusTotal
- MITRE ATT&CK
- CISA – #StopRansomware

8 AUTORES

Equipe CTI - ARX CYBER

Modelo de análise baseado nas diretrizes de Lenny Zeltser (CC BY 4.0). Ambiente de análise: REMnux (Linux x86-64) com pefile, capa e strings. Publicação: 03 de novembro de 2026. Classificação: TLP:CLEAR.

ARX CYBER

BUILT ON TRUST

A equipe de Cyber Threat Intelligence da ARX CYBER acompanha agentes de ameaça, **malwares** e campanhas ativas, e transforma essas informações em indicadores, detecções e recomendações aplicáveis. Este relatório utiliza como base a análise do artefato, dados públicos de pesquisa e referências do setor.

SAIBA MAIS SOBRE A ARX CYBER