TLP:GREEN · HACKERS HIVE CTI UNIT · HH-CTI-2026-BR-S1

RELATÓRIO DE INTELIGÊNCIA DE AMEAÇAS

CYBER THREAT INTELLIGENCE — BRASIL

JANEIRO – JUNHO 2026

DOCUMENTO	HH-CTI-2026-BR-S1
UNIDADE PRODUTORA	HACKERS HIVE — CTI INTELLIGENCE UNIT
CLASSIFICAÇÃO TLP	TLP:GREEN
DATA DE EMISSÃO	JULHO DE 2026
PERÍODO ANALISADO	01/JAN/2026 — 30/JUN/2026
TOTAL DE INCIDENTES	92 ataques de ransomware confirmados
GRUPOS IDENTIFICADOS	28 grupos de ameaça distintos
FONTE	RANSOMWARE.LIVE — API PÚBLICA / OSINT

01 SUMÁRIO EXECUTIVO

No 1º semestre de 2026, a Hackers Hive CTI Unit documentou 92 incidentes de ransomware confirmados contra organizações brasileiras, com base em dados coletados diretamente via API do ransomware.live. O período revela um cenário de alta atividade adversarial com distribuição regular de ataques ao longo dos seis meses — sem grandes oscilações, o que indica maturidade e profissionalização dos grupos atuantes no Brasil. Lockbit5 e TheGentlemen dominam amplamente o ranking, respondendo juntos por mais de 34% de todos os ataques. Foram identificados 28 grupos distintos, com destaque para a estreia de novos atores como Exitium, Blackwater e 0day Syndicate. Serviços Profissionais, Indústria e Agronegócio lideraram os setores mais afetados.

92	28	19	19
INCIDENTES TOTAIS	GRUPOS DE AMEAÇA	PICO MENSAL (JAN/26)	ATAQUES LOCKBIT5

02 ANÁLISE GRÁFICA DOS ATAQUES

5 visualizações derivadas dos 92 incidentes confirmados no 1º semestre de 2026, coletados via API do ransomware.live.

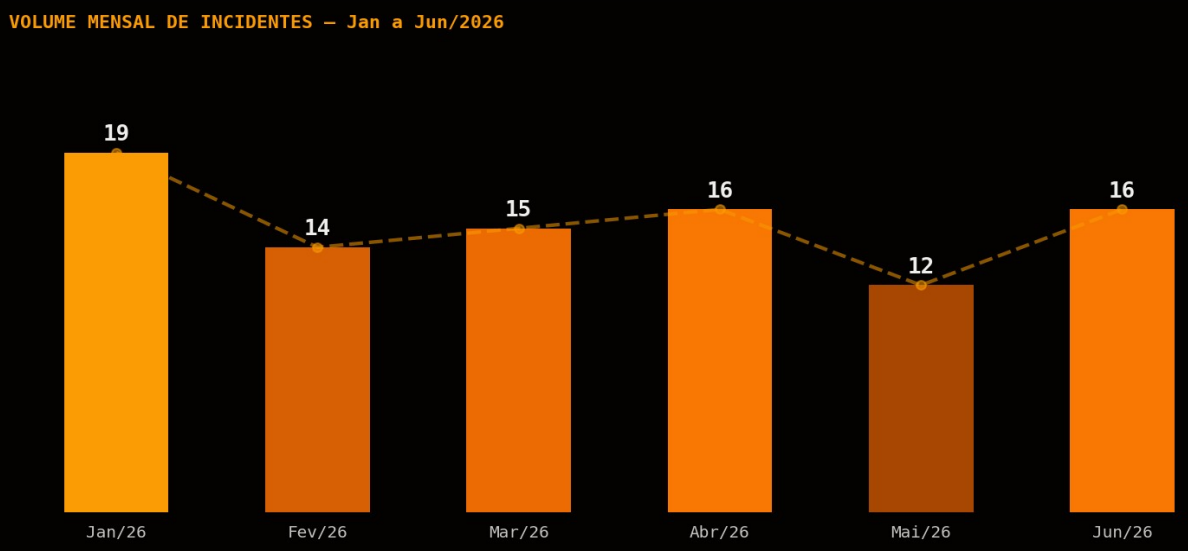

FIG. 01 — *Volume mensal Jan–Jun/2026 — distribuição regular com pico em janeiro.*

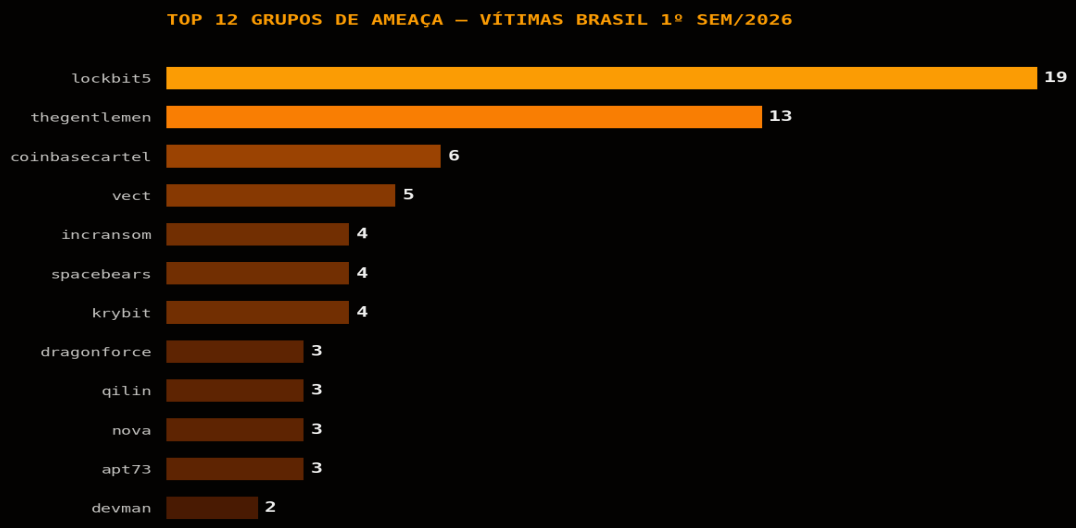

FIG. 02 — *Top 12 grupos de ameaça com vítimas confirmadas no Brasil no período.*

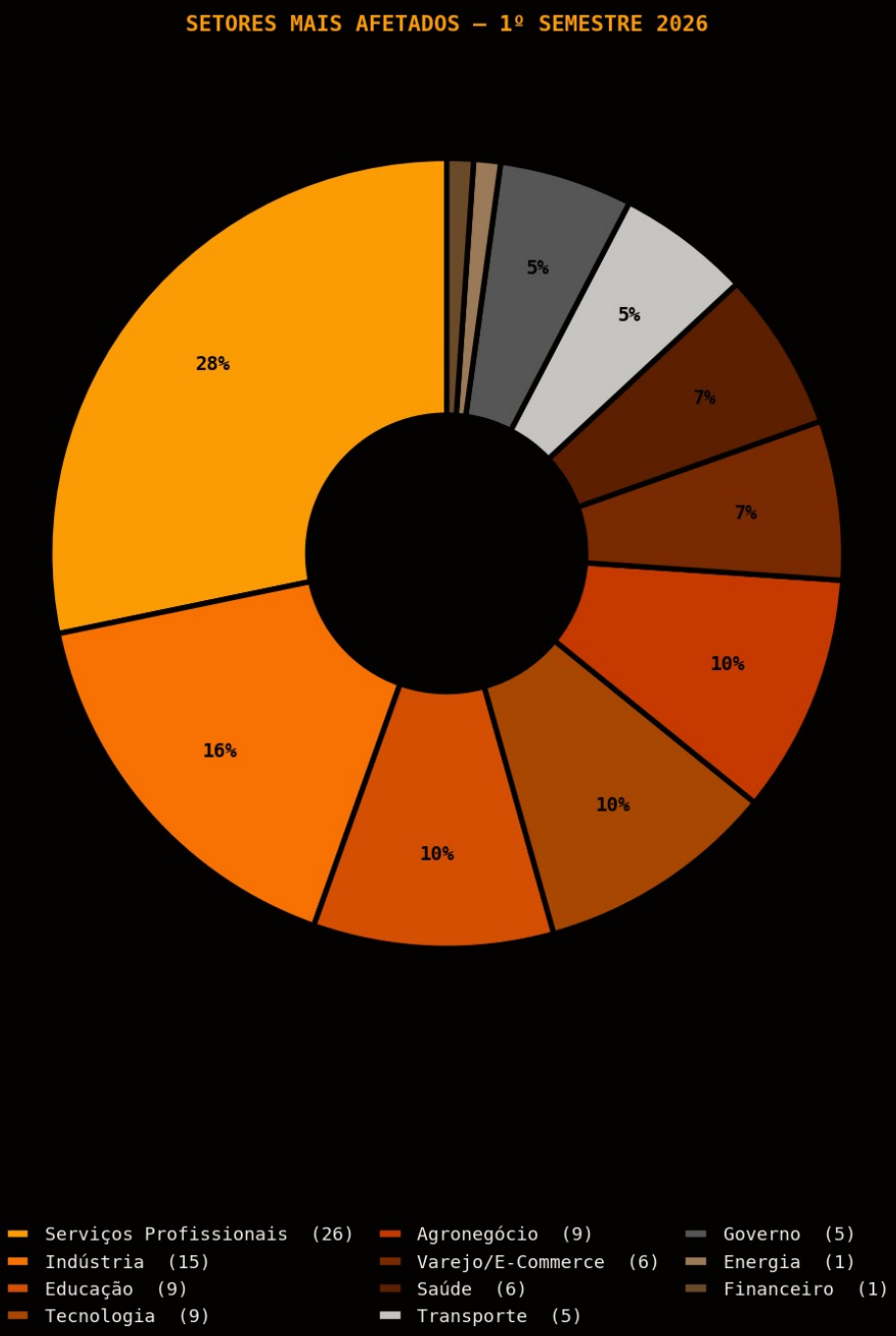

FIG. 03 — *Setores mais afetados — Serviços Profissionais e Indústria lideram.*

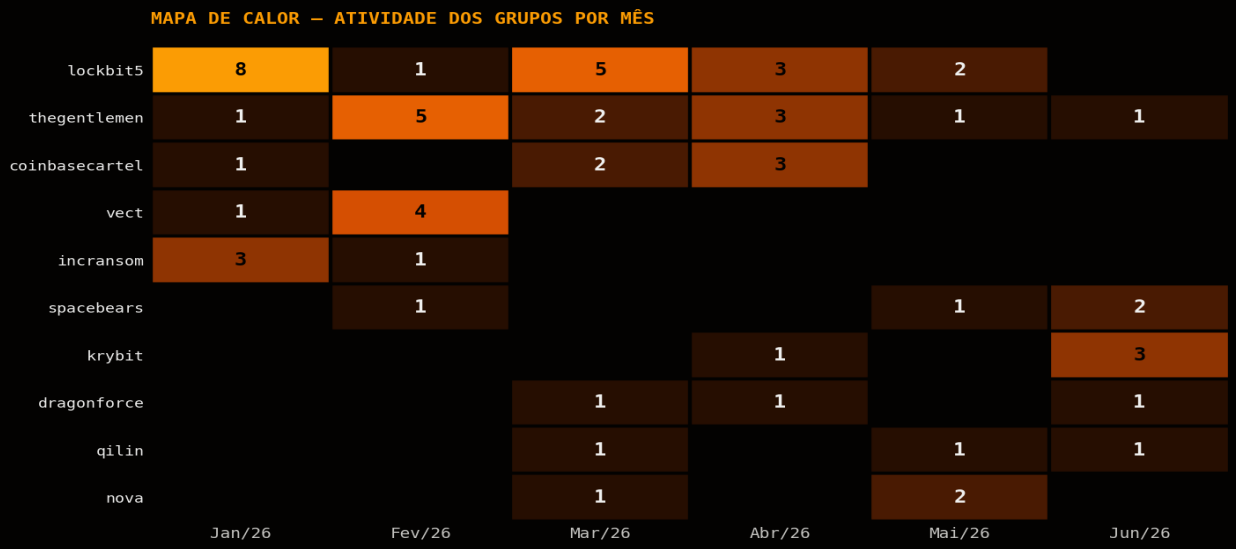

FIG. 04 — *Mapa de calor: intensidade de atividade dos top 10 grupos por mês.*

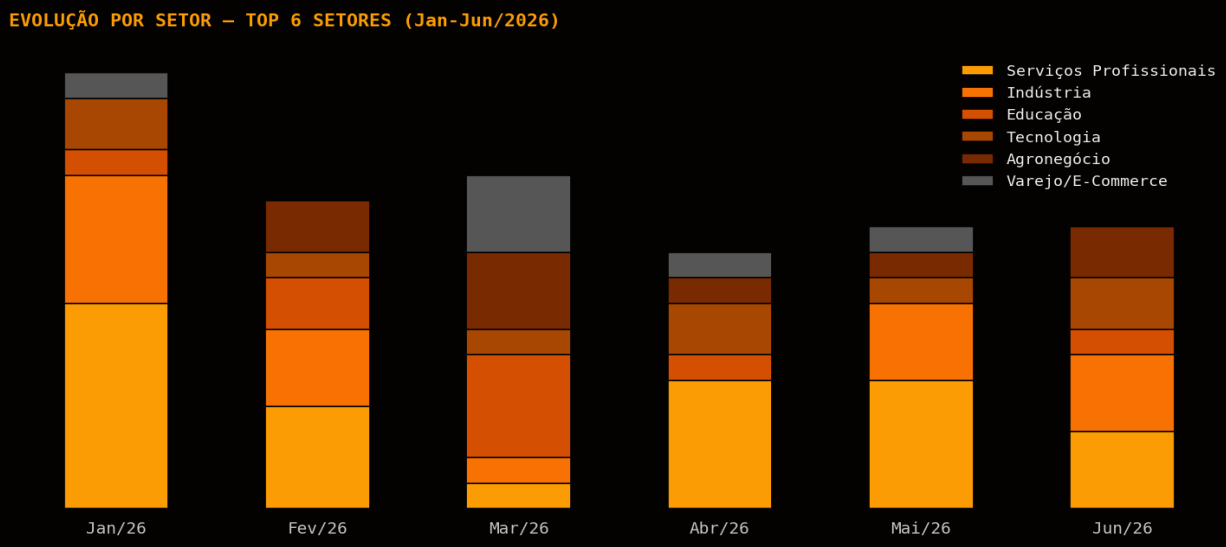

FIG. 05 — *Evolução mensal por setor — top 6 setores empilhados por mês.*

03 PERFIL DOS GRUPOS DE AMEAÇA

Principais agentes identificados com vítimas brasileiras no 1º semestre de 2026.

lockbit5
19 ataques
[CRÍTICO]

TIPO: RaaS — 5ª geração do LockBit
VETOR: VPN vulnerável, RDP exposto, phishing direcionado
Grupo mais ativo do semestre com 19 ataques. Atinge setores variados: jurídico, industrial, educacional e governo. Destacam-se os ataques simultâneos ao Sistema S (SESI, SENAI, FIEPE) em março/2026. Modelo RaaS com afiliados altamente ativos no Brasil.

thegentlemen
13 ataques
[CRÍTICO]

TIPO: Dupla extorsão / site de vazamentos próprio
VETOR: Credenciais comprometidas, serviços expostos
13 ataques com preferência por saúde (Greenpharma, Lab. Santa Luzia, Unimed), educação (UniFil, FGF, Notre Dame) e engenharia. Presença constante mês a mês sem interrupção. Opera site de vazamento próprio com publicação rápida.

coinbasecartel
6 ataques
[CRÍTICO]

TIPO: Extorsão massiva / exfiltração de alto volume
VETOR: Infiltração em redes corporativas, supply chain
6 ataques de alto impacto: JBS Brasil (3 postagens, 3TB reivindicados), Correios (primeira vez), Sea Telecom e CIGAM Software. Padrão de múltiplas publicações sobre a mesma vítima para maximizar pressão de resgate.

vect
5 ataques
[ALTO]

TIPO: Extorsão + exfiltração e publicação de dados
VETOR: Credenciais expostas, acesso remoto
5 ataques em campanha concentrada em janeiro e fevereiro. Comprometeu UFS (dados de estudantes), Was Madeiras, Auvo e duas contabilidades. Publica amostras de dados como prova antes de negociar.

apt73
3 ataques
[CRÍTICO]

TIPO: APT-like / Motivação mista financeira e política
VETOR: Exploração de exposição governamental
3 ataques diretos ao governo federal: siapenet.gov.br (pagamentos de 1,3M de servidores), sella.eng.br e gov.br (domínio raiz do governo federal). Maior ameaça à infraestrutura crítica estatal identificada no semestre.

incransom
4 ataques
[ALTO]

TIPO: Ransomware + extorsão setorial
VETOR: Spear-phishing, engenharia social direcionada
4 ataques com foco no setor jurídico em janeiro (OAB-SP, PK Pinhão, Diehl & Cella) e transporte em fevereiro. Demonstra capacidade de campanhas temáticas por setor com alta eficácia de targeting.

krybit
4 ataques
[MÉDIO]

TIPO: Grupo emergente em expansão
VETOR: Exploração de vulnerabilidades em serviços expostos
4 ataques ao longo do semestre com crescimento progressivo: Secran (abr), schultz.com.br, coemi.com.br e mupras.com (jun). Grupo relativamente novo com presença crescente no Brasil. Monitoramento recomendado.

dragonforce
3 ataques
[ALTO]

TIPO: Ransomware + extorsão / supply chain
VETOR: Acesso via fornecedores e parceiros comprometidos
3 ataques: FGV (mar), Nova FP (abr) e agroprime (jun). Preferência por instituições de ensino e agronegócio. Padrão de targeting estratégico em setores de alto valor de dados.

04 ANÁLISE MENSAL DE INCIDENTES

Detalhamento mês a mês dos 92 incidentes com organização, grupo de ameaça e setor afetado. Dados coletados via API do ransomware.live.

JANEIRO 2026 — 19 INCIDENTES

19 incidentes — maior volume de abertura de semestre já registrado. Lockbit5 domina com 8 ataques concentrados em 30 e 31/jan, incluindo série contra escritórios de advocacia (Guarnera, PK Pinhão, Diehl & Cella) e empresas industriais. Incransom mira setor jurídico: OAB-SP, PK Pinhão e Diehl & Cella no mesmo mês. Coinbasecartel estreia o semestre comprometendo a CIGAM Software — fornecedora de ERP para centenas de empresas brasileiras.

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Jan/26	Aditus BR	lockbit5	Serviços Prof.
Jan/26	Univ. Federal de Sergipe	vect	Educação
Jan/26	Limpebras	lockbit5	Indústria
Jan/26	Consigaz	devman	Energia
Jan/26	Galutti Automotive	sinobi	Indústria
Jan/26	Tvgoiania	devman	Varejo/E-Commerc
Jan/26	Unimed Anápolis	thegentlemen	Saúde
Jan/26	S.Y.L Pastilhas de Freios	nightspire	Indústria
Jan/26	Audicon Contadores	lockbit5	Serviços Prof.
Jan/26	Chiarottino	insomnia	Serviços Prof.
Jan/26	Grupo Ferrosider	lockbit5	Indústria
Jan/26	OAB	incransom	Serviços Prof.
Jan/26	Fast Indústria	lockbit5	Indústria
Jan/26	Grupo Selpe RH	lockbit5	Serviços Prof.
Jan/26	Kenta TI	lockbit5	Tecnologia
Jan/26	PK Pinhão & Koiffman	incransom	Serviços Prof.
Jan/26	Diehl & Cella Advogados	incransom	Serviços Prof.
Jan/26	Guarnera Advogados	lockbit5	Serviços Prof.
Jan/26	CigamSoftware	coinbasecartel	Tecnologia

FEVEREIRO 2026 — 14 INCIDENTES

14 incidentes. TheGentlemen opera em série contra educação (UniFil, FGF Colleges) e engenharia (Agis Civil Engineering). Vect realiza 4 ataques em 12 dias — padrão de campanha concentrada. Lockbit5 atinge o agronegócio com Brassuco. Incransom compromete transportadora Via Pajuçara. Nightspire volta ao radar com ataque à indústria metalúrgica (Fico Ferragens).

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Fev/26	Fico Ferragens	nightspire	Indústria
Fev/26	CENTINELA	clop	Serviços Prof.
Fev/26	UniFil	thegentlemen	Educação
Fev/26	Agis Civil Engineering	thegentlemen	Indústria
Fev/26	FGF Colleges	thegentlemen	Educação
Fev/26	Auvo	vect	Tecnologia

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Fev/26	Was Madeiras	vect	Indústria
Fev/26	Sitran MG	spacebears	Serviços Prof.
Fev/26	Grupo Progresso	thegentlemen	Agronegócio
Fev/26	Brassuco	lockbit5	Agronegócio
Fev/26	MB Contabilidade	vect	Serviços Prof.
Fev/26	Del Rey	vect	Serviços Prof.
Fev/26	Via Pajuçara Transportes	incransom	Transporte
Fev/26	Fundação Para	thegentlemen	Governo

MARÇO 2026 — 15 INCIDENTES

15 incidentes. Mês de alta visibilidade: JBS Brasil reivindica 3TB de dados pelo Coinbasecartel (duas postagens distintas). Lockbit5 ataca SESI, SENAI e FIEPE — três instituições do Sistema S no mesmo mês. FGV comprometida pelo Dragonforce. APT73 ausente, mas o mês registra ataques a governo (Saúde MT) e saúde (Hospital Vet Diadema). Exitium estreia no Brasil com ataque à Marborges Agroindustria.

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Mar/26	FGV	dragonforce	Educação
Mar/26	JBS Brazil (1ª pub.)	coinbasecartel	Agronegócio
Mar/26	SESI	lockbit5	Educação
Mar/26	SENAI	lockbit5	Educação
Mar/26	JBS Brazil (2ª pub.)	coinbasecartel	Agronegócio
Mar/26	Arimex Importadora	qilin	Varejo/E-Commerc
Mar/26	FIEPE	lockbit5	Educação
Mar/26	Hospital Vet Diadema	killsec	Saúde
Mar/26	Saúde MT Gov	lockbit5	Governo
Mar/26	Delta Ducon Engenharia	thegentlemen	Indústria
Mar/26	Marborges Agroindustria	exitium	Agronegócio
Mar/26	Américo Advogados	thegentlemen	Serviços Prof.
Mar/26	5 de Agosto	lockbit5	Varejo/E-Commerc
Mar/26	VX Case	nova	Varejo/E-Commerc
Mar/26	Knewin	ALP-001	Tecnologia

ABRIL 2026 — 16 INCIDENTES

16 incidentes. Coinbasecartel ataca os Correios — primeira vez que a empresa pública de logística nacional é listada. APT73 volta com dois ataques diretos: siapenet.gov.br (sistema de pagamento de 1,3M de servidores federais) e sella.eng.br. TheGentlemen foca em saúde (Greenpharma, Laboratório Santa Luzia). Blackwater estreia no Brasil. Krybit inicia presença com Secran.

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Abr/26	Ipiranga Contábil	gunra	Serviços Prof.
Abr/26	JBS Brazil (amostra)	coinbasecartel	Agronegócio
Abr/26	Correios	coinbasecartel	Transporte
Abr/26	DIME Distribuidora	worldleaks	Transporte

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Abr/26	ERS Transportes	lockbit5	Transporte
Abr/26	Nova FP	dragonforce	Serviços Prof.
Abr/26	Secran	krybit	Serviços Prof.
Abr/26	Greenpharma	thegentlemen	Saúde
Abr/26	Grupo EBD	blackwater	Serviços Prof.
Abr/26	Laboratório Santa Luzia	thegentlemen	Saúde
Abr/26	Sea Telecom Br	coinbasecartel	Tecnologia
Abr/26	Colégio Notre Dame	thegentlemen	Educação
Abr/26	siapenet.gov.br	apt73	Governo
Abr/26	sella.eng.br	apt73	Tecnologia
Abr/26	lbreng.com.br	lockbit5	Serviços Prof.
Abr/26	sweetome.com	lockbit5	Varejo/E-Commerc

MAIO 2026 — 12 INCIDENTES

12 incidentes — menor volume do semestre. Lockbit5 mantém cadência. Nova opera contra governo (SECONT) e tecnologia (BC3). Medusalocker reaparece atacando cadeia alimentar: CEAGESP e Bandeirante Supermercados. 0day Syndicate estreia com ataque a empresa de serviços. TheGentlemen compromete Grupo Alvorada (manufatura).

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Mai/26	santoinacio-rio.com.br	lockbit5	Serviços Prof.
Mai/26	CEAGESP / Netfeirasp	medusalocker	Agronegócio
Mai/26	Bandeirante Supermercados	medusalocker	Varejo/E-Commerc
Mai/26	Complastex	qilin	Indústria
Mai/26	ws.com.br	threeam	Serviços Prof.
Mai/26	Grupo Alvorada	thegentlemen	Indústria
Mai/26	Gerencial Contábil	spacebears	Serviços Prof.
Mai/26	SECONT Secretaria	nova	Governo
Mai/26	grupodetoni.com.br	lockbit5	Serviços Prof.
Mai/26	dxon.com.br	0day Syndicate	Serviços Prof.
Mai/26	BC3 Tecnologia	nova	Tecnologia
Mai/26	Grupo Mauá	bravox	Indústria

JUNHO 2026 — 16 INCIDENTES

16 incidentes. APT73 compromete gov.br — domínio raiz do governo federal brasileiro. Krybit consolida presença com 3 ataques em série. Dragonforce volta ao agronegócio (agroprime). Spacebears realiza dois ataques (Sicol e Chebib). BrainCipher ataca setor farmacêutico (paipharma.com). Direwolf volta ao radar com Clínica Vida. Semestre fecha com 92 incidentes confirmados.

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Jun/26	Sicol	spacebears	Indústria
Jun/26	Eat Salad	qilin	Agronegócio
Jun/26	schultz.com.br	krybit	Serviços Prof.
Jun/26	Silmquinas e Equipamentos	thegentlemen	Indústria

DATA	ORGANIZAÇÃO	GRUPO	SETOR
Jun/26	Clínica Vida	direwolf	Saúde
Jun/26	MHE9 Logística	gunra	Transporte
Jun/26	Chebib Control	spacebears	Serviços Prof.
Jun/26	coemi.com.br	krybit	Financeiro
Jun/26	www.mupras.com	krybit	Serviços Prof.
Jun/26	Super Finishing	worldleaks	Indústria
Jun/26	Editora Irmãos Vitale	payload	Educação
Jun/26	gov.br	apt73	Governo
Jun/26	Meta (metamed)	bravox	Tecnologia
Jun/26	acilab.com	settra	Tecnologia
Jun/26	agroprime	dragonforce	Agronegócio
Jun/26	paipharma.com	BrainCipher	Saúde

05 RECOMENDAÇÕES E MELHORES PRÁTICAS

Baseadas nos padrões identificados nos 92 incidentes. Priorizadas por criticidade e frequência de exploração observada no 1º semestre de 2026.

CRÍTICO	**MFA e Zero Trust em Todos os Acessos Remotos** Lockbit5 e Coinbasecartel exploram ativamente RDP e VPN expostos. MFA obrigatório em todos os pontos de acesso remoto. Implementar modelo Zero Trust com verificação contínua. Desabilitar RDP desnecessário e auditar contas privilegiadas mensalmente.
CRÍTICO	**Proteção de Infraestrutura Governamental** APT73 atacou siapenet.gov.br, gov.br e sella.eng.br no mesmo semestre. Órgãos públicos precisam de segmentação de rede, autenticação reforçada, monitoramento 24x7 e planos de IR testados com exercícios tabletop semestrais.
CRÍTICO	**Backup Offline e Recuperação Validada** JBS, Correios e CIGAM foram alvos de exfiltração massiva. Estratégia 3-2-1-1 (3 cópias, 2 mídias, 1 offsite, 1 imutável). Testar restauração completa trimestralmente. Sem backup válido, o resgate torna-se a única saída.
ALTO	**Monitoramento de Exfiltração (SOC/SIEM/DLP)** Coinbasecartel reivindica 3TB da JBS. Vect exfiltra dados de estudantes da UFS. Implementar alertas para transferências de volume anormal, acessos fora do horário e uso de ferramentas de compressão/staging. A exfiltração precede o ransomware.
ALTO	**Proteção do Setor Jurídico e Serviços Profissionais** 26 ataques em Serviços Profissionais — setor mais visado do semestre. Incransom mira sistematicamente escritórios de advocacia. Implementar segmentação de rede, MFA e treinamento de phishing específico para esse perfil de alvo.
ALTO	**Patch Management — 72h para CVEs Críticos** Vulnerabilidades em VPN Fortinet, Cisco e sistemas de acesso remoto são os principais vetores. Inventário contínuo de ativos expostos à internet. Prioridade máxima para patches de produtos com exploração confirmada in the wild.
MÉDIO	**Monitoramento de Grupos Emergentes** Exitium, Blackwater e 0day Syndicate estrearam no Brasil neste semestre. Grupos novos costumam operar em volumes baixos enquanto mapeiam o ambiente — e então escalam. Incluir esses atores em feeds de CTI e monitoramento de dark web.
MÉDIO	**Threat Intelligence Contínua** A Hackers Hive CTI Unit publica relatórios regulares com base em dados reais da API do ransomware.live. Assinar feeds de CTI focados no Brasil, monitorar Telegram de grupos e participar de grupos ISAC do setor para antecipar campanhas.

CONCLUSÃO E PERSPECTIVAS

O 1º semestre de 2026 confirma o Brasil como alvo consolidado e estratégico do ecossistema global de ransomware. Com 92 incidentes em 6 meses e distribuição regular sem queda expressiva em nenhum mês, o cenário indica operação profissionalizada e contínua dos grupos adversariais. Para o 2º semestre de 2026, a Hackers Hive CTI Unit projeta: intensificação do Lockbit5 que já opera como ator dominante; consolidação do TheGentlemen como maior ameaça aos setores de saúde e educação; crescimento do Coinbasecartel com ataques a alvos de alto valor e visibilidade pública; e expansão dos grupos emergentes Exitium, Blackwater, Krybit e 0day Syndicate. O ataque ao gov.br pelo APT73 em junho é um sinal de alerta para o segundo semestre: grupos com motivação política e financeira mista tendem a escalar

operações em anos de alta tensão. A Hackers Hive CTI Unit continuará publicando inteligência atualizada para a comunidade.