Relatório Anual de Ameaças 2025

Panorama executivo e técnico sobre campanhas observadas na América Latina, com foco em ransomware, exposição de superfícies públicas e abuso de credenciais.

Organização	OceanSec Labs - Threat Intelligence
Período	Janeiro a Dezembro de 2025
Classificação	Uso externo - material de imprensa
Revisão técnica	David Chang, Sarah Jenkins
Revisão editorial	Lúcia Mendes

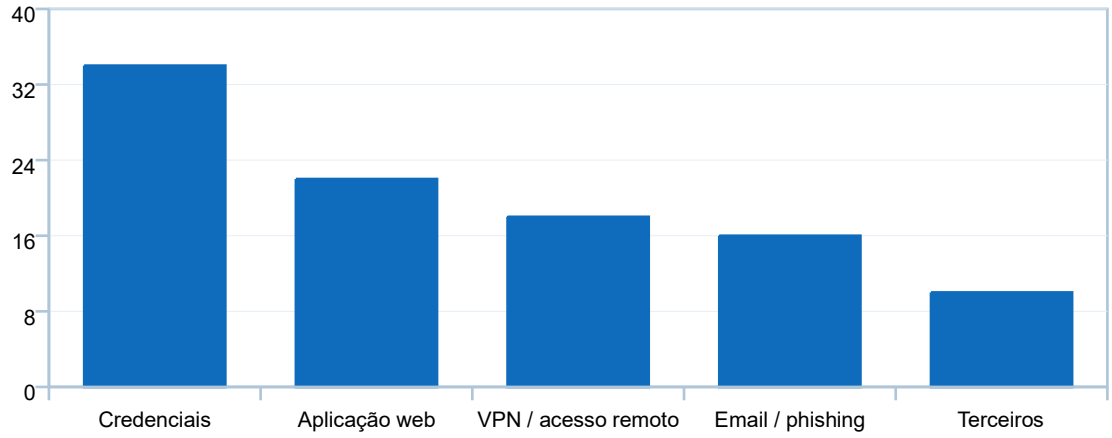
Resumo executivo: em 2025, observamos aumento consistente do uso de credenciais válidas como vetor inicial, crescimento de campanhas de ransomware com dupla extorsão e maior aproveitamento de ambientes de homologação, painéis expostos e repositórios com segredos operacionais.

1. Principais tendências observadas

A maior parte dos incidentes acompanhados pela OceanSec em 2025 apresentou uma combinação de vetores previsíveis e execução disciplinada. Em vez de depender apenas de exploits complexos, grupos oportunistas e atores mais maduros priorizaram ativos expostos, acessos reutilizados e cadeias de credenciais distribuídas entre aplicações, VPNs, painéis administrativos e serviços de terceiros.

No recorte regional, os setores mais afetados foram serviços financeiros, logística, saúde suplementar e varejo. Em todos eles, a disponibilidade operacional teve peso semelhante - ou superior - ao impacto de confidencialidade.

Incidentes observados por vetor inicial (amostra consolidada)



2. Destaques do ano

- Acesso inicial por credenciais válidas continuou sendo o padrão dominante em ambientes com MFA parcial ou mal aplicado.
- Ambientes de homologação e painéis administrativos permaneceram como fontes recorrentes de exposição por DNS público, reuso de segredos e ausência de segmentação.
- Ransomware com dupla extorsão ampliou o uso de tempo de permanência curto, com exfiltração seletiva antes do impacto operacional.
- Ataques a fornecedores e integrações passaram a ser tratados com prioridade por organizações maduras, mas ainda com baixa maturidade contratual em monitoramento contínuo.

Distribuição estimada de impacto em incidentes acompanhados

Campanha / padrão	Setor mais afetado	Tática recorrente	Observação
Silent Ledger	Financeiro	Exposição de credenciais e painéi	s legados
North Dock	Logística	VPN desatualizada e movimentação lateral	
Amber Ward	Saúde	Aplicações legadas de telemedici	ıa
Paper Route	Varejo	Repositórios com segredos e inte	ração CI/CD

3. Campanhas e padrões recorrentes

Uso de infraestrutura terceirizada e abuso de contas

Tempo de permanência curto e foco em interrupção operacional.

Forte aproveitamento de segmentação insuficiente entre Credenciais reaproveitadas em APIs e storage exposto.

4. Recomendações prioritárias

1. Mapear e revisar ativos de homologação, painéis administrativos e subdomínios pouco utilizados.
2. Centralizar segredos fora do código e reduzir reuso entre aplicações, automações e ambientes.
3. Aprimorar correlação entre eventos de autenticação, telemetria de endpoint e mudanças em infraestrutura.

4 Expandir due diligence de terceiros com foco em acessos, integrações e processos de atualização.

Contato de imprensa: press@oceansec.com | Assessoria: Lúcia Mendes | Atualizado em 05/01/2026