

MIND THE SEC

Conscientização Orientada a Adversário com Threat Intelligence

Por que o programa de conscientização
começa muito antes do primeiro
treinamento

Fernando Andreazi

Enterprise Account Manager | Kaspersky Brasil



O PONTO DE PARTIDA

Três perguntas que a maioria dos programas nunca fez

Se você não sabe responder, o conteúdo do treinamento está sendo escolhido no escuro.



1 Quais credenciais corporativas já estão circulando?

Logs de infostealer, combolists, mercados de acesso inicial
Não é hipótese. É inventário.

2 Qual é a superfície de ataque externa hoje?

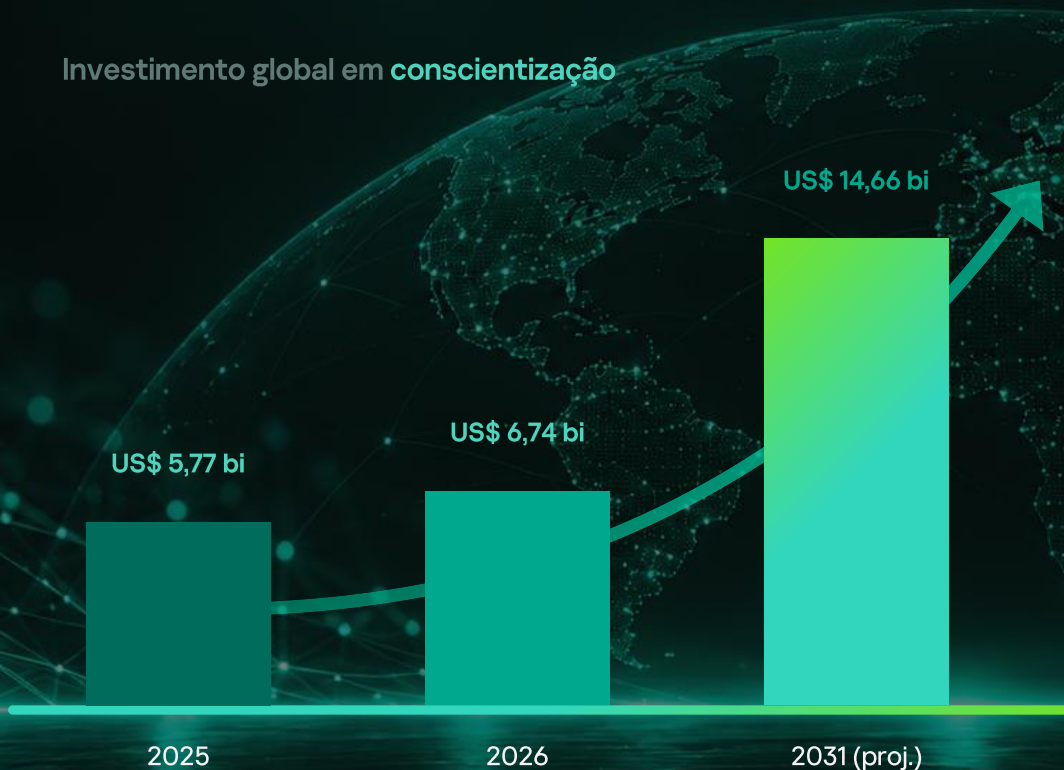
Portais de VPN, RDP exposto, subdomínios esquecidos, appliances de borda sem patch.

3 Quem está falando da minha empresa, setor ou região?

Fórums, canais de Telegram, blogs de vazamento, corretores de acesso inicial.

O mercado de Security Awareness nunca esteve tão aquecido

Investimento global em conscientização



16,8%

CAGR projetado de 2026 a 2031



US\$ 10 bi

Patamar anual esperado já em 2027



2.700+

Profissionais em 70 países ouvidos pelo SANS



Engenharia social segue como **risco humano número 1**, agora amplificada por deepfake e clonagem de voz.

Mais investimento, mesmo vetor

O que melhorou

- ✓ Plataformas **maduras**, conteúdo em português e **simulação automatizada**
- ✓ **Conscientização** virou exigência de cliente grande e de seguradora
- ✓ **Tema entrou na pauta** de conselho e de comitê executivo
- ✓ Taxa de **clique em simulação** cai de forma consistente com cadência

O que não mudou

- **Elemento humano presente** em mais de 60% das violações, pelo quinto ano seguido
- **Credencial comprometida** segue como a técnica mais difundida em toda a cadeia de ataque
- **Mudar comportamento** leva de 6 a 12 meses. Enraizar cultura leva de 3 a 10 anos
- A maior parte dos programas ainda mede conclusão de curso, não **redução de risco**



Cinco falhas estruturais que se repetem



As cinco têm a mesma raiz: o programa é desenhado a partir do que se pode ensinar, não do que o adversário já tem em mãos.



O programa de conscientização não começa no primeiro treinamento.

Começa na análise da **exposição externa** da organização, que é exatamente o material com que o adversário já está trabalhando.

A mudança de frase, do ponto de vista do usuário:



de “proteja a sua senha” para “a sua credencial já vazou, e é assim que vão usá-la”



Duas formas de desenhar o mesmo programa

Orientado a conteúdo



Ponto de partida: catálogo de trilhas da plataforma



Público: todo mundo, mesma trilha



Simulação: modelo genérico de prêmio ou boleto



Gatilho: calendário



Métrica: conclusão e taxa de clique



Conversa com a diretoria: percentual treinado



Orientado a adversário



Ponto de partida: exposição medida da organização



Público: priorizado por exposição real e por privilégio



Simulação: reproduz o modus operandi do grupo que ataca o setor



Gatilho: evento de inteligência, como credencial detectada em log



Métrica: tempo entre detecção do vazamento e remediação



Conversa com a diretoria: risco evitado, em reais

Mesma plataforma. Mesmo orçamento. **Ponto de partida diferente.**

A EVIDÊNCIA

O que os dados dizem sobre credencial e ransomware

O DBIR 2026 foi publicado em maio e mudou a leitura do vetor inicial. A conclusão sobre credencial ficou mais forte, não mais fraca.

DBIR 2025

22%

das violações tiveram credencial comprometida como vetor de acesso inicial

54%

das vítimas de ransomware tinham domínio em dumps de credencial antes do ataque

DBIR 2026

13%

credencial como vetor inicial. Exploração de vulnerabilidade assume o topo com 31%

39%

quando a credencial é contada em qualquer ponto da cadeia. Segue a técnica mais difundida

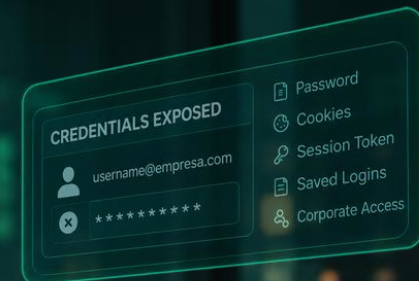
O achado que muda o jogo

73%

das vítimas de ransomware tiveram infecção por infostealer ou evento de vazamento de credencial no ano anterior ao ataque

50%

desses casos ocorreram dentro de 95 dias antes do ataque



O SLIDE ÂNCORA

A janela de 95 dias

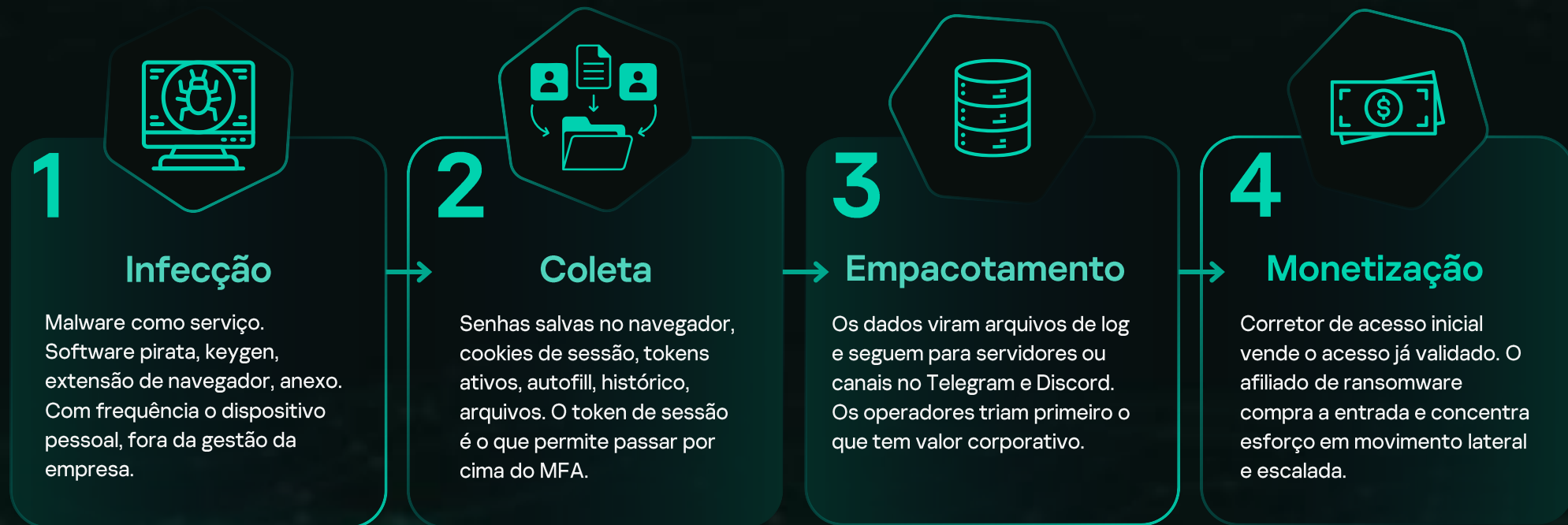
*Entre o vazamento da credencial e a detonação do ransomware existe um intervalo mensurável.
É nele que a conscientização precisa acontecer.*



A pergunta operacional:

quanto tempo a sua organização leva hoje, do vazamento à troca de senha e à revogação de sessão?

A economia do infostealer, em quatro etapas



Consequência para o programa de conscientização:

o comprometimento acontece com frequência fora do notebook corporativo e fora do e-mail. Não existe um clique para simular.

O tamanho da **exposição** na nossa praça



37 milhões

de registros de pessoas físicas e jurídicas do Brasil publicados na dark web somente em 2024, dos quais 5,6 milhões ligados a contas de governo



+54%

de crescimento nas detecções de infostealer na região e +56% no volume de credenciais expostas, comparando 2025 e 2026



50% / 15%

participação de RedLine e Lumma nas infecções da região. O Lumma tem foco declarado em credencial corporativa e alta capacidade de evasão

Por que isso importa para o desenho do programa



O Brasil é o principal alvo de infostealer da região. Governo, educação e saúde estão entre os setores mais atingidos



Vazamento de credencial pessoal e corporativa se misturam no mesmo log, porque o dispositivo é o mesmo



A orientação ao colaborador precisa cobrir a vida digital dele, não apenas o crachá. Esse é o ponto que os CISOs entrevistados mais repetem

Qilin: o adversário que praticamente não precisa do seu usuário clicar



Perfil operacional

- Ransomware como serviço, ativo desde 2022, antes conhecido como Agenda
- Afiliado retém de 80% a 85% do resgate. O operador entrega payload, infraestrutura, site de vazamento e portal de negociação
- Dupla extorsão. Exfiltra primeiro, criptografa depois, publica se não houver pagamento
- Grupo mais ativo do primeiro semestre de 2026, com 370 ataques na América do Norte, 158 na Europa e Reino Unido e 40 na América do Sul

Como entra

- Rota primária: VPN de perímetro com credencial válida. SSL VPN de Fortinet, SonicWall, Cisco e RDP exposto
- Na maioria dos casos investigados, o appliance estava com patch em dia. O que faltava era MFA e bloqueio de conta
- Também explora falhas de autenticação em borda quando disponíveis, como PAN-OS e Check Point em 2026
- Movimento lateral com ferramentas nativas do sistema. Permanência curta, de 3 a 5 dias até a detonação



O padrão temporal que aparece nas investigações

Sequência recorrente observada por equipes de resposta a incidentes em casos atribuídos ao grupo.

- 1 Credencial administrativa aparece exposta**
Log de infostealer ou anúncio em fórum. Neste momento nada acontece no ambiente da vítima. Nenhum alerta dispara.
- 2 Cerca de duas semanas depois**
Volume anômalo de tentativas de autenticação NTLM contra o portal de VPN. Muitos ambientes não monitoram isso.
- 3 Autenticação bem-sucedida**
A VPN envolvida não tinha MFA configurado. Do ponto de vista do log, é um usuário legítimo entrando.



O único momento em que o usuário poderia ter sido alcançado por um programa de conscientização foi na etapa 1. E ele não sabia de nada.

A CONSEQUÊNCIA

Por que o **treinamento genérico** não endereça esse risco



Não houve clique

O acesso inicial é uma autenticação válida. Não existe e-mail suspeito para reportar nem link para não clicar.



O comprometimento aconteceu fora do perímetro

Notebook de casa, celular pessoal, conta pessoal com senha reutilizada. Nada disso aparece nos controles corporativos.



O tempo de exposição é invisível para o usuário

A pessoa não sabe que a credencial dela está circulando. Sem essa informação, a recomendação genérica é ruído.



O MFA sozinho não fecha a porta

Cookie e token de sessão roubados permitem retomar sessão autenticada. E boa parte dos acessos remotos ainda não tem MFA.



A trilha anual chega tarde

Se a janela mediana é de 95 dias, um ciclo de treinamento anual perde a janela em três de cada quatro casos.



Não é que o treinamento seja inútil. É que ele está começando no lugar errado da linha do tempo.

kaspersky

O MODELO

Conscientização Orientada a Adversário

Quatro camadas. A camada zero é a que quase nunca existe.



0 Inteligência

Vazamento de credenciais, superfície de ataque externa e monitoramento de dark web. Responde às três perguntas do início.

1 Priorização

Quem está exposto, com qual privilégio, em qual processo crítico. Define público e urgência, não o calendário.

2

Intervenção dirigida

Conteúdo e simulação que reproduzem o modus operandi do adversário do setor. Notificação individual como gatilho.

3

Medição comportamental

Tempo de remediação, taxa de reporte, cobertura de MFA e redução de exposição. Traduzido em risco financeiro.

*A ordem importa. Bruno Guerreiro resume assim: pessoas primeiro, processos em seguida, tecnologia por último. Aqui vale acrescentar **inteligência** antes de tudo.*

O que a **inteligência** entrega para o programa

1 Vazamento de credenciais

Credenciais de colaboradores, parceiros e clientes. Contas corporativas comprometidas, dados de cartão, telefones.

O que isso decide no programa

Define quem é notificado hoje e quem entra em trilha reforçada.

2 Superfície de ataque externa

Ativos expostos na internet, serviços mal configurados, vulnerabilidades em borda, recursos modificados ou comprometidos.

O que isso decide no programa

Define quais equipes de TI e quais processos entram no escopo do programa.

3 Monitoramento de dark web

Fóruns, blogs de ransomware, mensageiros e sites tor. Campanhas ativas ou em planejamento contra a empresa, o setor ou a região.

O que isso decide no programa

Define o modus operandi que a simulação vai reproduzir.

Sem essa camada, o programa escolhe conteúdo por intuição e simula ataque por catálogo.

Da inteligência para o público-alvo

Personas definidas por exposição medida e por privilégio, não por organograma.



Credencial detectada em log

Crítico

Notificação individual em até 24 horas, reset, revogação de sessão e verificação do dispositivo de origem



Usuários de VPN e acesso remoto

Alto

Trilha sobre reautenticação, portal falso, fadiga de MFA e reconexão fora do processo



TI, administradores e contas privilegiadas

Alto

Credencial-alvo, cofre de senhas, sessão gravada, separação de conta administrativa



Financeiro, compras e contas a pagar

Alto

Fraude de troca bancária, dupla checagem fora de banda, pretexting por telefone



Executivos e liderança

Alto

Higiene digital fora do trabalho, exposição pública, whaling e clonagem de voz



Terceiros com acesso ao ambiente

Médio

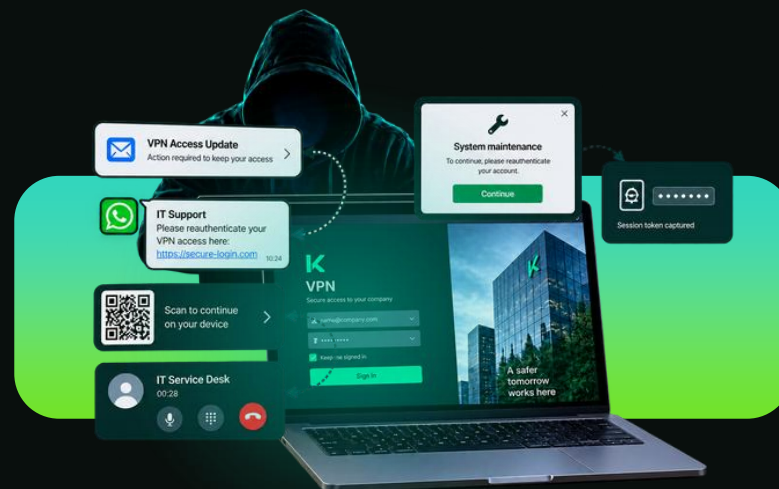
Mesma régua de identidade, expiração automática, conta separada por contrato

A **simulação** precisa parecer com **quem ataca** o seu setor



Simulação de catálogo

- Prêmio, sorteio ou cartão presente
- Boleto genérico de fornecedor desconhecido
- Atualização de senha de serviço que a empresa não usa
- Canal único: e-mail corporativo
- Resultado: taxa de clique cai, risco real não muda



Simulação orientada a adversário

- Página de reconexão de VPN idêntica ao portal que a empresa usa
- Aviso de janela de manutenção pedindo reautenticação
- Fadiga de MFA e captura de token de sessão
- Pretexting para o service desk pedindo reset de senha
- Multicanal: e-mail, WhatsApp, QR code, ligação

O gatilho de maior aprendizado que um programa pode ter



A notificação individual de credencial vazada



*Sua credencial corporativa foi identificada em um log de infostealer em 12 de março. O dispositivo de origem provavelmente é pessoal. Vamos trocar a senha, encerrar as sessões ativas e verificar o seu equipamento. Você não está em apuros. **Você está sendo avisado antes que alguém use isso.***

Por que funciona

No modelo de BJ Fogg, comportamento nasce de **motivação**, **habilidade** e **gatilho**. A notificação entrega os três de uma vez: o risco é pessoal, a ação é simples e o momento é agora.



Tom

Acolhimento, nunca punição. Segurança psicológica é pré-requisito para reporte espontâneo.



Ação

Reset, revogação de sessão, verificação do dispositivo e microaula de 3 minutos no mesmo fluxo.



LGPD

Metadado corporativo e escopo definido. Nada de inspeção de conteúdo pessoal sem base legal e política publicada.



Cadência

Fluxo contínuo, não campanha. O evento define o momento, não o calendário.

Métricas que decidem, não que decoram



Indicadores que levam medem preparo

- Tempo médio entre detecção do vazamento e reset com revogação de sessão
- Percentual de credenciais expostas remediadas em até 7 dias
- Cobertura de MFA em acesso remoto e em contas privilegiadas
- Redução de ativos expostos na superfície externa
- Taxa de reporte espontâneo, medida em conjunto com a de clique

Indicadores que chegam medem realidade

- Incidentes com origem em credencial válida
- Tentativas anômalas de autenticação em portais de acesso remoto
- Taxa de clique em simulação que reproduz o modus operandi real do setor
- Tempo de detecção, contenção e recuperação
- Reincidência por causa raiz não tratada

*Para a diretoria, converta em RONI, o risco de não investir:
quanto custa uma hora parada, multiplicado pela probabilidade que a exposição medida indica.*



COMO COMEÇAR

Duas ações combinadas, sem compromisso de compra



1 Assessment de Threat Intelligence

Responde às três perguntas do início da sessão com dados da sua organização.

-  Credenciais corporativas identificadas em vazamentos e logs
-  Superfície de ataque externa e ativos expostos
-  Menções à empresa, ao setor e à região em dark web



2 Avaliação do KASAP por 30 dias

Transforma o diagnóstico em programa executável, com público e conteúdo já definidos.

-  Trilhas por nível de risco e simulador de phishing
-  Conteúdo ajustável às políticas internas da organização
-  Painel de comportamento por grupo, área e evolução no tempo

Por que as duas juntas

O assessment define quem treinar, sobre o que e com que urgência. A plataforma executa, mede e sustenta a cadência. Uma sem a outra é diagnóstico sem tratamento, ou tratamento sem diagnóstico.

O que você tem em mãos ao final de 30 dias

1 Inventário de exposição

Lista de credenciais corporativas identificadas em vazamentos, com data, origem e criticidade por usuário.



2 Mapa de superfície externa

Ativos expostos, serviços mal configurados e vulnerabilidades de borda priorizadas por risco de negócio.



3 Perfil do adversário do setor

Quais grupos atuam na sua vertical e na sua região, e qual é o modus operandi que a simulação precisa reproduzir.



4 Matriz de personas priorizadas

Quem entra em trilha reforçada, quem entra em notificação imediata e quem segue na trilha padrão.



5 Primeira campanha rodada

Simulação com modus operandi real, mais a trilha correspondente, com linha de base de comportamento medida.



6 Caso de negócio para a diretoria

Exposição medida traduzida em RONI, com metas de remediação e cadência proposta para os 60 dias seguintes.



O adversário já fez a **pesquisa sobre a** **sua empresa.**

A pergunta é se o seu programa
de conscientização vai usar a
mesma pesquisa.



OBRIGADO! OBRIGADO!

Perguntas?

Fernando Andreazi

Enterprise Account Manager | Kaspersky Brasil

kaspersky

