ANÁLISE SEMANAL · 11 A 18 DE NOVEMBRO DE 2026

Trinta e um milhões e meio de credenciais expostas, e a fila de trabalho são 844 mil

O levantamento de exposição de credenciais mais recente mediu 4.824 organizações nos Estados Unidos e na Europa e encontrou 31,5 milhões de credenciais expostas nos doze meses até 1º de setembro de 2026. Dessas, cerca de 30,7 milhões, ou 97%, vieram de vazamentos antigos e listas combinadas. As outras 844 mil, menos de 3%, saíram direto de dispositivos infectados por ladrão de informação. As duas pilhas chegam no mesmo painel, com o mesmo rótulo de credencial exposta, e pedem respostas completamente diferentes. Esta análise propõe separá-las antes de qualquer coisa, e mostra por que trocar a senha resolve a pilha grande e não resolve a pequena.

4.824 organizações medidas · 31,5 milhões de credenciais · 844 mil vindas de infecção · Mediana brasileira: 173 · Janela de 95 dias antes do ataque

Resumo executivo

O problema desta análise: o indicador de credencial exposta virou padrão de painel de segurança e continua sendo lido como um número só. Ele não é um número só. É a soma de duas populações com causas diferentes, urgências diferentes e remédios diferentes, e a maior das duas é a menos urgente.

- A separação por procedência, que é a primeira coisa a fazer e a mais fácil de obter de qualquer fornecedor de monitoramento.
- Por que 41% das organizações têm credencial de e-mail corporativo em registro de infecção, e por que esse recorte, não o total, é a fila de trabalho.
- O que o registro de infecção contém além da senha, com os números de captura de CRM, provedor de identidade, repositório e nuvem.
- A janela de 95 dias que o dado de incidente associa a ataque de resgate, e por que medir por mês perde essa relação.
- O recorte brasileiro, com mediana de 173 contra 32 global, e a leitura honesta desse número.
- O que a vinculação de sessão a hardware resolve, e as cinco coisas que ela não resolve.

Comece pela divisão, porque ela muda tudo que vem depois.

Procedência	Volume	O que indica	Remédio
Vazamento antigo e lista combinada	Cerca de 30,7 milhões, 97%	Que a senha circulou em algum momento, possivelmente anos atrás, possivelmente de serviço pessoal	Higiene de senha, bloqueio de senha conhecida, segundo fator

Procedência	Volume	O que indica	Remédio
Registro de ladrão de informação	Cerca de 844 mil, menos de 3%	Que um dispositivo foi infectado e entregou o que o navegador guardava	Remediação do dispositivo, revogação de sessão, rotação do que o registro mostra

A pilha de cima é crônica. A de baixo é aguda. E a de baixo é a que tem data.

Um registro de ladrão de informação não é uma senha solta. É o conteúdo do navegador de uma máquina específica num momento específico: senhas salvas, cookies de sessão, tokens, histórico, às vezes arquivo. Ele existe porque alguém executou algo. Se o endereço é corporativo, a máquina provavelmente é sua.

O recorte que é a fila de trabalho

No levantamento de 4.824 organizações, 72% tinham pelo menos uma credencial de funcionário ou de cliente exposta por ladrão de informação. Esse número, sozinho, não ajuda ninguém a decidir nada. A divisão dele ajuda:

- **41%** tinham pelo menos uma credencial roubada ligada a um e-mail corporativo. Isso aponta para dispositivo de funcionário infectado.
- **31%** tinham credencial de ladrão de informação ligada somente a conta de cliente. Isso é problema de fraude e de atendimento, não de endpoint seu.

Serviços financeiros ficaram no topo, com 77% das empresas tendo credencial vinda de infecção. Serviços para empresas tiveram 47% com pelo menos um acesso corporativo roubado por malware. Em bens e serviços de consumo o volume é o maior de todos, com a empresa típica em 498 credenciais expostas, e quase todas são conta de cliente. A diferença entre setores foi maior que a diferença entre países.

Guarde essa última frase, porque ela contraria a leitura intuitiva. A média europeia foi de 224 acessos expostos por empresa, 22% acima da média americana de 184. Dentro da Europa, países nórdicos em 358 e Espanha em 133. O grupo mais exposto de todos foi consumo no Benelux, com média de 1.285. Geografia explica menos que modelo de negócio.

O que mais vem no mesmo registro

Trocar a senha do e-mail e encerrar o caso é o erro mais comum, e ele é fácil de demonstrar.

Um painel independente, montado sobre um índice de registros de infecção e medido em 1.856 domínios corporativos de 36 países, mostra o que mais foi capturado junto dos endereços dessas empresas. Foram 145.677 acessos a serviços de terceiros. A distribuição importa mais que o total:

Serviço	Acessos capturados	Empresas afetadas
CRM Salesforce	13.897	204
Provedores de identidade, no conjunto	6.850	129
Okta	4.508	111

Serviço	Acessos capturados	Empresas afetadas
GitHub	3.007	111
AWS	987	77

No setor bancário, 49,8% dos acessos de terceiros capturados eram de CRM. No setor público, 442 acessos a serviço de IA generativa registrados em endereços de governo, distribuídos por 20 órgãos.

Leia a tabela como inventário de alcance, não como lista de senhas. Se um registro trouxe o acesso ao provedor de identidade, a senha do e-mail é o menor dos problemas. E se trouxe o acesso ao repositório de código, o prazo de resposta não é o do próximo ciclo de revisão de acesso.

Há ainda a parte que senha nenhuma resolve. O mesmo painel contabiliza 1,18 bilhão de cookies de sessão associados aos domínios medidos, com 49,3 milhões capturados em um único mês. Uma empresa de recuperação de dado relatou 8,6 bilhões de registros de cookie roubados recapturados do submundo em 2025. Cookie de sessão válido dispensa senha e dispensa segundo fator. Enquanto a sessão não for revogada, a troca de senha não expulsa ninguém.

A janela que o dado de incidente recomenda

Aqui entra o número que justifica tratar a pilha pequena com urgência.

O levantamento anual de investigação de vazamentos de 2026 analisou 31 mil incidentes, dos quais 22 mil foram vazamentos confirmados. A metade das organizações que sofreram ataque de resgate teve um evento de credencial ou de ladrão de informação nos 95 dias anteriores ao ataque. Antes, não depois.

Outros números do mesmo material ajudam a calibrar:

- Credencial roubada como vetor de acesso inicial caiu para 13% dos vazamentos. A queda é mudança de tática do atacante, não melhoria de proteção.
- Considerando qualquer ponto da progressão do ataque, e não só a entrada, o abuso de credencial aparece em 39% dos vazamentos, e credencial roubada como ação em 36%.
- Exploração de vulnerabilidade como acesso inicial subiu para 31%.
- O envolvimento de terceiro cresceu 60% em relação ao conjunto anterior e chegou a 48% dos vazamentos.
- No mercado de acesso, conta de usuário comum sai por cerca de 700 dólares e conta administrativa por cerca de 1.300.

Noventa e cinco dias é a informação operacional. Quase todo painel de exposição de credencial é lido em cadência mensal, e quase toda métrica apresentada a conselho é mensal. Um indicador mensal não mostra uma relação de 95 dias. Ele a corta em três pedaços e perde a forma.

O método, em quatro perguntas

Na ordem em que elas eliminam trabalho.

1. De onde veio este registro?

Lista combinada ou registro de infecção. Qualquer fornecedor de monitoramento sabe responder, e muitos não mostram o campo por padrão. Peça o campo. Sem ele, 97% do volume dilui os 3% que importam, e o seu indicador mede higiene histórica de senha do mercado inteiro, não risco seu.

2. O identificador é corporativo ou de cliente?

Corporativo manda para a fila de endpoint e identidade. De cliente manda para fraude e atendimento. São times diferentes, com prazos diferentes, e misturar os dois é o que faz o número parecer intratável. Lembre que a empresa típica de consumo tem quase 500 credenciais expostas que são todas de cliente.

3. O que mais estava no mesmo registro?

Antes de pedir a troca de senha, pergunte o que foi capturado junto. Acesso a provedor de identidade, a CRM, a repositório e a console de nuvem muda a ordem de resposta, e cada um tem rotação própria. É aqui que a resposta deixa de ser um clique e passa a ser um procedimento.

4. A sessão foi revogada, e o dispositivo foi tratado?

As duas coisas, não uma. Revogar sessão sem tratar a máquina devolve o atacante no dia seguinte, porque o ladrão continua instalado. Tratar a máquina sem revogar sessão deixa a sessão viva até o prazo de expiração, que em alguns provedores é longo: token de atualização de 90 dias por padrão em um deles, e praticamente sem expiração em outro, salvo revogação ou seis meses de inatividade.

O recorte brasileiro, e o que ele não quer dizer

No painel de 1.856 domínios, o Brasil aparece com 61 organizações, taxa de presença de 95,1% e mediana de 173 credenciais por organização. A mediana global do painel é 32. Só dois países ficam acima do Brasil: Estados Unidos com 609 e Índia com 209. Nenhum outro passa de 75. E 77% das organizações brasileiras do painel ganharam pelo menos uma credencial nova em trinta dias, contra 55,5% no conjunto.

A leitura honesta desse número tem três partes.

A primeira é que mediana por organização não é normalizada por número de funcionários. Painel que inclui as maiores empresas de um país grande produz mediana alta por construção. O número americano de 609 é o caso extremo disso.

A segunda é que os três países do topo têm em comum parque grande de dispositivo pessoal usado para trabalho. Isso é hipótese razoável e o próprio material que a publica não a sustenta com dado.

A terceira é a que vale: a taxa de 77% ganhando credencial nova em trinta dias, essa sim é comparável, porque é proporção e não volume. Ela diz que o fluxo de infecção é contínuo, não residual. É um problema de taxa, e problema de taxa não se resolve com mutirão.

O que a vinculação de sessão resolve

A única mudança estrutural recente contra roubo de cookie é vincular a sessão a uma chave privada guardada em hardware do dispositivo, o módulo de plataforma confiável no Windows e o enclave seguro no macOS. O navegador prova periodicamente que tem a chave e renova um cookie de vida curta. Cookie copiado para outra máquina não renova e morre rápido.

Está disponível de forma geral no Chrome 146 no Windows, com o suporte em macOS anunciado para versão futura. E tem limites que precisam ficar claros antes de alguém marcar a caixa no plano:

- O site precisa implementar o lado servidor. Atualizar o navegador, sozinho, não ativa nada.
- Firefox, Safari e Edge ainda não têm. Em dispositivo móvel não há suporte. Máquina sem hardware seguro cai no comportamento antigo, sem vínculo.
- Não cobre roubo de token de atualização, incluindo o fluxo de código de dispositivo, que nunca envolve cookie de sessão.
- Não cobre token primário de atualização, bilhete Kerberos nem token OAuth guardado pelo navegador.
- Não faz nada contra malware que já está rodando na máquina e usa a sessão viva localmente, nem contra aplicativo nativo, ferramenta de linha de comando e cliente dedicado. E não impede phishing: a vítima continua digitando a senha no site falso.

A maioria dos notebooks corporativos de 2018 em diante tem o hardware necessário. A cobertura ampla no parque de consumo, segundo quem acompanha a adoção, deve levar anos.

Como esta análise pode estar errada

Por honestidade com o método, vale listar as fragilidades do dado que a sustenta, porque os próprios autores as listam.

O painel de 1.856 domínios compara duas fotografias, de 13 de outubro e 1º de novembro, cujas janelas de trinta dias se sobrepõem por onze dias. Isso mostra direção e escala, não mês calendário limpo. São dois pontos, e dois pontos não fazem tendência. O índice usado é um só, e nenhum índice vê todos os registros. A composição é curada, não amostra aleatória. E um único despejo grande distorce ranking: um caso documentado no material é o de uma operadora que saltou de 288 para 1.152 credenciais novas em um mês por causa de um lote só.

Vale repetir o que o próprio material repete e que vários resumos esquecem: exposição não é invasão. Registro de infecção vem de dispositivo infectado, muitas vezes pessoal, e a presença dele no índice não prova que alguém entrou no seu ambiente. Prova que existe um caminho pronto e barato, e dá a ele uma data.

É essa data que a janela de 95 dias torna acionável. O resto do número é contexto.

Quatro decisões que cabem nesta semana

01 · DECISÃO

Exigir o campo de procedência do fornecedor de monitoramento

Lista combinada ou registro de infecção, em cada alerta, sem exceção. Sem esse campo o indicador soma 97% de ruído histórico com 3% de evento datado, e nenhuma fila construída sobre ele vai acertar a ordem.

02 · DECISÃO

Separar a fila corporativa da fila de cliente, com donos diferentes

Credencial de e-mail corporativo vai para endpoint e identidade. Credencial de conta de cliente vai para fraude e atendimento. São 41% e 31% das organizações no levantamento, e tratá-las na mesma fila é o que faz o número parecer impossível.

03 · DECISÃO

Trocar o procedimento de redefinição de senha por um de três passos

Revogar sessão, rotacionar o que o registro mostra além da senha e tratar o dispositivo. Nessa ordem e sem pular nenhum. Cookie de sessão válido ignora senha nova e segundo fator até a revogação acontecer.

04 · DECISÃO

Medir a exposição em janela de 95 dias, e não por mês

É a janela em que metade das vítimas de resgate teve evento de credencial antes do ataque. Indicador mensal corta essa relação em três e perde a forma dela. Mude o período do relatório antes de mudar a ferramenta.

Fontes e aprofundamento

eSecurity Planet · Infostealers Expose 72% of Organizations, Why One Login Matters. com a amostra de 4.824 organizações, os 31,5 milhões de credenciais, a fatia de 844 mil vinda de infecção e o recorte de serviços financeiros em 77%.
https://www.esecurityplanet.com/cybersecurity/news-infostealer-credential-exposure-outpost24-report/

The Next Web · Most leaked logins are old, but infostealers reach 72% of firms. com a janela de doze meses até 1º de setembro de 2026, a divisão entre 41% de identificador corporativo e 31% de conta de cliente, e as médias por região.
https://thenextweb.com/news/infostealers-72-percent-organisations-exposed-credentials

Flare · What Security Leaders Need to Know About the 2026 DBIR, 50% of Ransomware Victims Had Credential Exposure Within 95 Days. com os 31 mil incidentes e 22 mil vazamentos confirmados, a janela de 95 dias, os 48% de envolvimento de terceiro e os preços de acesso no mercado criminoso.
https://flare.io/learn/resources/blog/2026-verizon-dbir

RansomNews · Infostealer report November 2026. painel de 1.856 domínios em 36 países, com a mediana brasileira de 173, os acessos de terceiros capturados por serviço, os 1,18 bilhão de cookies e as ressalvas de método declaradas pelos autores.
https://ransomnews.com/infostealer-report-november-2026/

SpyCloud · What You Need to Know About Google DBSC and its Ability to Prevent Session Hijacking. com o funcionamento da vinculação de sessão a hardware, a disponibilidade no Chrome 146 no Windows, os 8,6 bilhões de registros de cookie recapturados em 2025 e a lista do que o mecanismo não cobre.
https://spycloud.com/blog/what-to-know-about-google-chrome-dbsc/

Publicado em 18 de novembro de 2026 em latamsec.com.br/recursos/credenciais-expostas-tres-por-cento/. Conteúdo editorial da LATAMSEC. As afirmações atribuídas a fornecedores e a relatórios mantêm a autoria original e podem ser conferidas nas fontes acima.