kaspersky

2025

Relatórios analíticos

Fluindo pela Amazônia

O cenário de ameaças da dark web no Brasil

Conteúdo

Antes da jornada

Antes da jornada

A equipe de Kaspersky Digital Footprint Intelligence preparou um relatório que destaca as ameaças mais graves e proeminentes da dark web comumente enfrentadas por organizações no Brasil. O Brasil não foi escolhido por acaso — com a maior economia em desenvolvimento da América Latina, vastos recursos e ampla variedade de negócios, há anos o país tem sido um alvo apetitoso para cibercriminosos. Nossa pesquisa vai além de simplesmente fornecer uma visão geral do cenário de ameaças da dark web — identifica os possíveis riscos, avalia as respectivas consequências e oferece uma estratégia clara de proteção.

Hoje em dia, gerenciar a segurança de qualquer infraestrutura de TI, seja para governos, empresas ou dispositivos pessoais, exige uma clara compreensão das tendências e ameaças atuais de cibersegurança. Não é segredo algum que agentes maliciosos, de pessoas a grupos organizados que operam em mercados clandestinos, estão constantemente aprimorando suas táticas, ferramentas e procedimentos. Desenvolvem continuamente novos métodos para cada fase do ataque, desde o planejamento inicial e reconhecimento até a obtenção de acesso e manutenção da presença no longo prazo. Esses invasões podem durar anos, com impactos que variam desde violações de dados até destruição parcial ou total de uma infraestrutura.

Por isso, é necessário manter-se informado sobre agentes ativos, abordagens e métodos em evolução e o cenário de ameaças em geral para detectar, interromper ou até mesmo prevenir ataques e fraudes ainda nos estágios iniciais. Com esse conhecimento, acreditamos que este relatório beneficiará organizações de diversos setores, incluindo, entre outros:

- Governo
- Serviços profissionais
- Varejo
- Fabricação
- Serviços de saúde
- Transporte e logística
- Telecomunicações
- Serviços e bens de consumo
- TI e software
- Finanças e seguros
- Educação
- Eletricidade, gás e petróleo, mineração e todos os outros setores industriais
- Construção civil e mercado imobiliário
- Agricultura
- e assim por diante

O que exploramos

No total, analisamos publicações, posts e mensagens em todas as camadas da dark web, inclusive:

- Arquivos de invasões e recursos modificados da Web
- Chats e canais públicos e privados do Telegram
- Fóruns de cibercriminosos, tanto públicos quanto de acesso restrito
- Blogs de agentes de ransomware
- Mercados clandestinos para diversas atividades cibercriminosas.
- Outros recursos onion utilizados por cibercriminosos

Mergulhando no rio traiçoeiro

Algumas palavras sobre a estrutura da dark web

A dark web[1] geralmente se refere a uma parte oculta da Internet que não é indexada por mecanismos de pesquisa (como o Google). De forma mais detalhada, a dark web pode ser comparada a um redemoinho. À medida que você se aprofunda, acaba atravessando diferentes camadas que se distinguem principalmente pelo grau de acessibilidade.

A verdadeira dark web — nas profundezas

Recursos totalmente privados e não indexados que, em geral, exigem verificações e autenticações adicionais pelos administradores antes que o acesso seja concedido

Surface web — fora do redemoinho

Sites, fóruns e canais do Telegram acessíveis na Web 'visível' ou aberta — qualquer usuário da Internet pode acessar e se inscrever nesses recursos

Deep web — o meio do caminho

Chats e canais privados em aplicativos de mensagens instantâneas e recursos com acesso limitado que não são indexados e não podem ser acessados por mecanismos de pesquisa comuns, exceto se ferramentas adicionais (como o Tor) forem utilizadas

1

O que são a deep web e a dark web?

Principais perigos no percurso

Nossa investigação revelou as ameaças mais prevalentes enfrentadas por instituições estatais e empresas brasileiras:

Havia **30 grupos de ransomware** operando no Brasil. As análises de publicações em seus blogs no ano passado mostra que foram executados pelo menos 114 ataques contra 105 empresas, com nove organizações sendo vítimas duas vezes em um ano. As gangues mais ativas foram RansomHub, Arcus Media, Lockbit 3.0, Quilong e Eraleign. Juntas, elas estavam por trás dos ataques a 53% das organizações afetadas. Quanto aos alvos, nossa pesquisa revelou os três principais setores foram saúde (incluindo hospitais), serviços financeiros e serviços profissionais. Entidades públicas também apareceram entre os 10 primeiros colocados.

O mercado de acesso inicial a empresas brasileiras e entidades estatais, incluindo pontos de entrada em redes corporativas e acesso a dispositivos, hosts, serviços ou sistemas corporativos separados, é altamente diversificado e desenvolvido. Apenas em 2024, descobrimos e analisamos mais de 100 anúncios oferecendo acesso a empresas de saúde, governo, construção, agricultura e outros setores. Os agentes de ameaças, de cibercriminosos individuais a gangues de ransomware e grupos de APT, precisam regularmente desses pontos de acesso para o desenvolvimento de seus ataques.

Uma infinidade de vazamentos de bancos de dados (tanto relacionados a empresas quanto aqueles contendo informações sobre indivíduos ou empresas brasileiras) foi descoberto na dark web. No total, no ano passado, os cibercriminosos compartilharam ou comercializaram 309 bancos de dados corporativos supostamente vazados de 185 organizações em vários setores, em que agências governamentais (16% de todas as violações), empresas de telecomunicações e de serviços profissionais foram as mais afetadas[2].

A atividade de ladrão de informações continua crescendo, em que as infecções por malware para roubo de dados disparam ano após ano. Nossa análise de registros publicados por operadores de ladrões de informações na dark web em 2024 revelou 37 milhões de registros de contas de usuários comprometidas vinculadas a recursos brasileiros, com 38% dessas contas comprometidas unicamente em 2024. As famílias de malware mais prevalentes — RedLine, Lumma e RisePro — foram responsáveis por 70% da atividade total.

Quando se trata de setores específicos, nossa pesquisa revelou que setores do governo, de saúde, financeiro e de seguros foram os mais visados. Anteriormente, os cibercriminosos tendiam a evitar atacar determinados alvos "blindados", como hospitais e outras organizações de saúde, devido à conexão com a vida humana que possuem. No entanto, essas regras não escritas aparentemente não se aplicam mais.

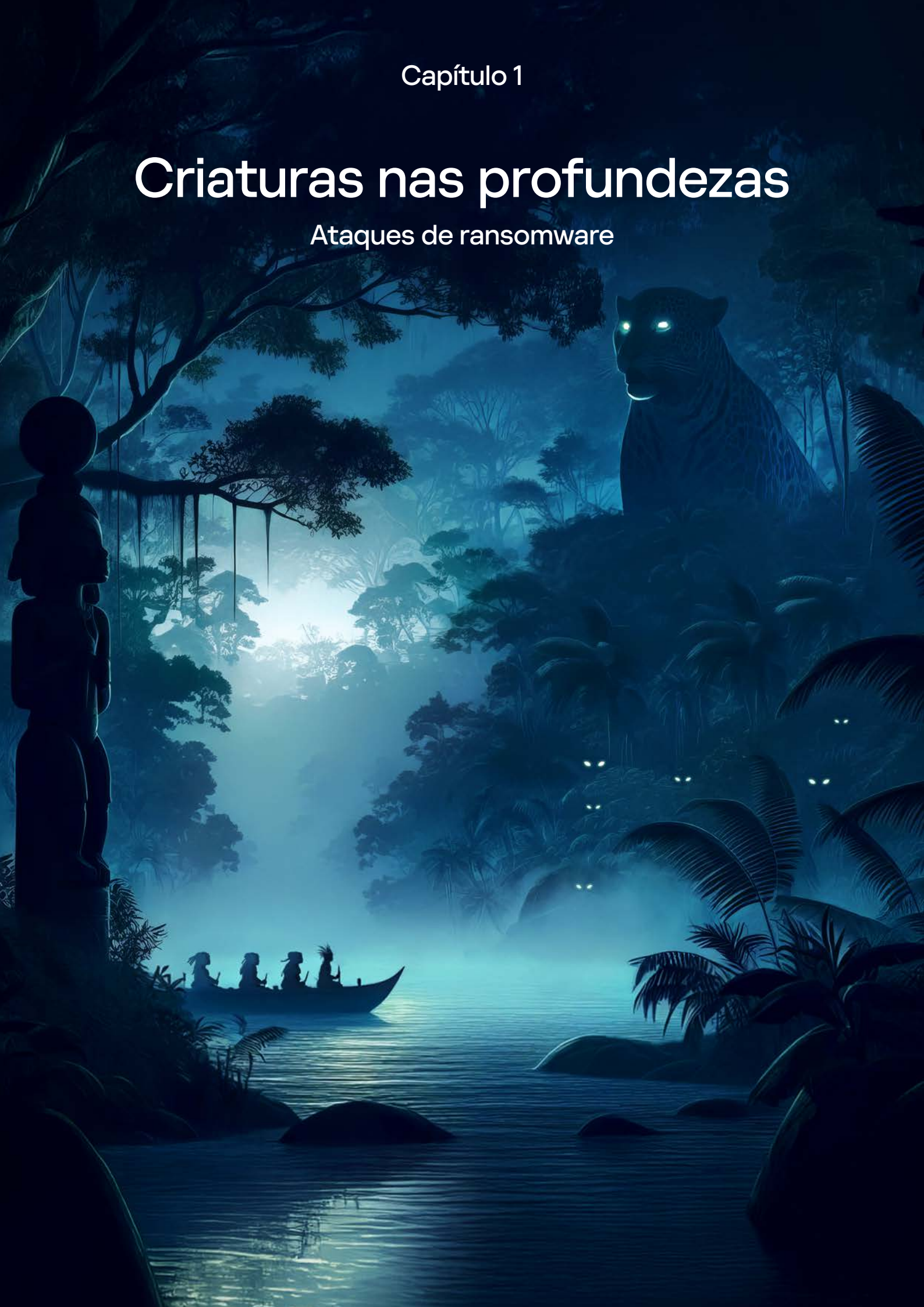
Essas podem ser apenas uma parte da variedade de ameaças que os cibercriminosos da dark web representam para as organizações brasileiras, mas são significativas e estão em evolução. Conhecer tais ameaças é fundamental para reforçar as defesas e proteger proativamente o ambiente de TI.

2 As estatísticas são baseadas em informações de publicações feitas por agentes de ameaças na dark web. Para evitar o acesso não autorizado aos dados das empresas afetadas durante a pesquisa, as informações comprometidas não foram verificadas.

Capítulo 1

Criaturas nas profundezas

Ataques de ransomware



Criaturas nas profundezas

Ataques de ransomware

Os grupos de ransomware estão expandindo suas atividades todos os anos em todo o mundo. Qualquer organização em qualquer setor pode se tornar uma vítima — instituições governamentais, bancos, indústrias, infraestruturas críticas, empresas de todos os tamanhos e até mesmo hospitais e outras organizações de saúde (embora o setor de saúde já tenha sido relativamente protegido contra ataques devido às suas operações de vida ou morte, hoje em dia está cada vez mais visado no Brasil).

Atualmente, os ataques de ransomware estão entre as ameaças mais críticas à integridade operacional e à segurança de qualquer empresa. Sempre levam às consequências mais devastadoras, incluindo roubo de todos os dados confidenciais, o que poderia ser útil para ataques futuros ou valiosos entre outros cibercriminosos, além da criptografia completa dos sistemas de arquivos em todos os hosts na infraestrutura das vítimas. Portanto, é essencial monitorar todos os eventos, alertas e incidentes de segurança da informação para detectar possíveis ataques e se defender deles antes que seja tarde demais ou, pelo menos, minimizar os danos potenciais.

Analisamos blogs de gangues de ransomware em busca de publicações sobre ataques à empresas brasileiras. Esses blogs publicam informações sobre as últimas invasões bem-sucedidas e, caso o resgate não seja pago, os dados roubados passam a ser divulgados.

Nossa análise também confirma que o número de ataques de ransomware no Brasil tem aumentado ano após ano: em 2024, 105 organizações brasileiras sofreram ataques de ransomware, em que nove delas foram vítimas duas vezes, atacadas em meses diferentes ou por grupos distintos de ransomware. Em comparação, em 2023, foram 62 vítimas e, em 2022, 39 (em que novamente algumas foram alvo diversas vezes). Isso mostra que o número de organizações vítimas de ransomware no Brasil quase que dobra a cada ano.

Porém, vale mencionar que o número real de ataques pode ser ainda maior, pois alguns incidentes não são registrados publicamente em blogs de ransomware.

Figura 1 | Ataques de ransomware direcionados ao Brasil em 2022 – 2024

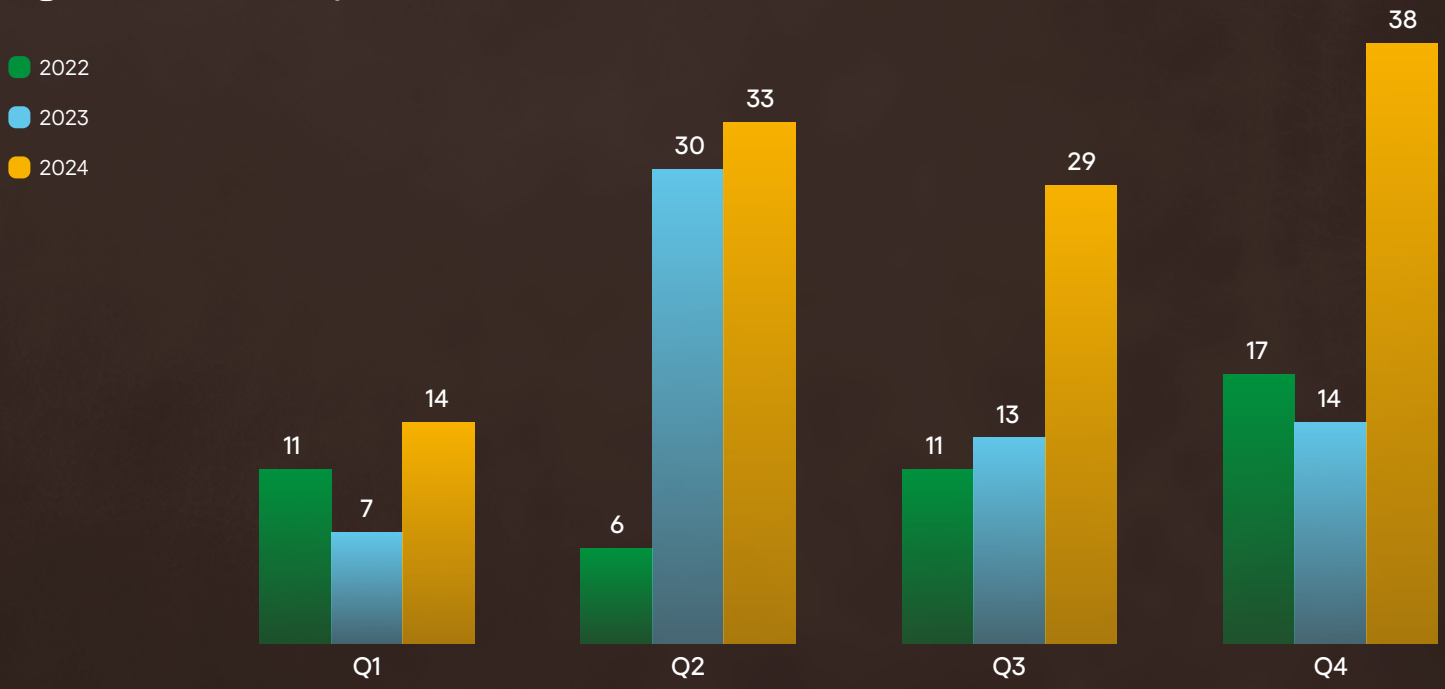
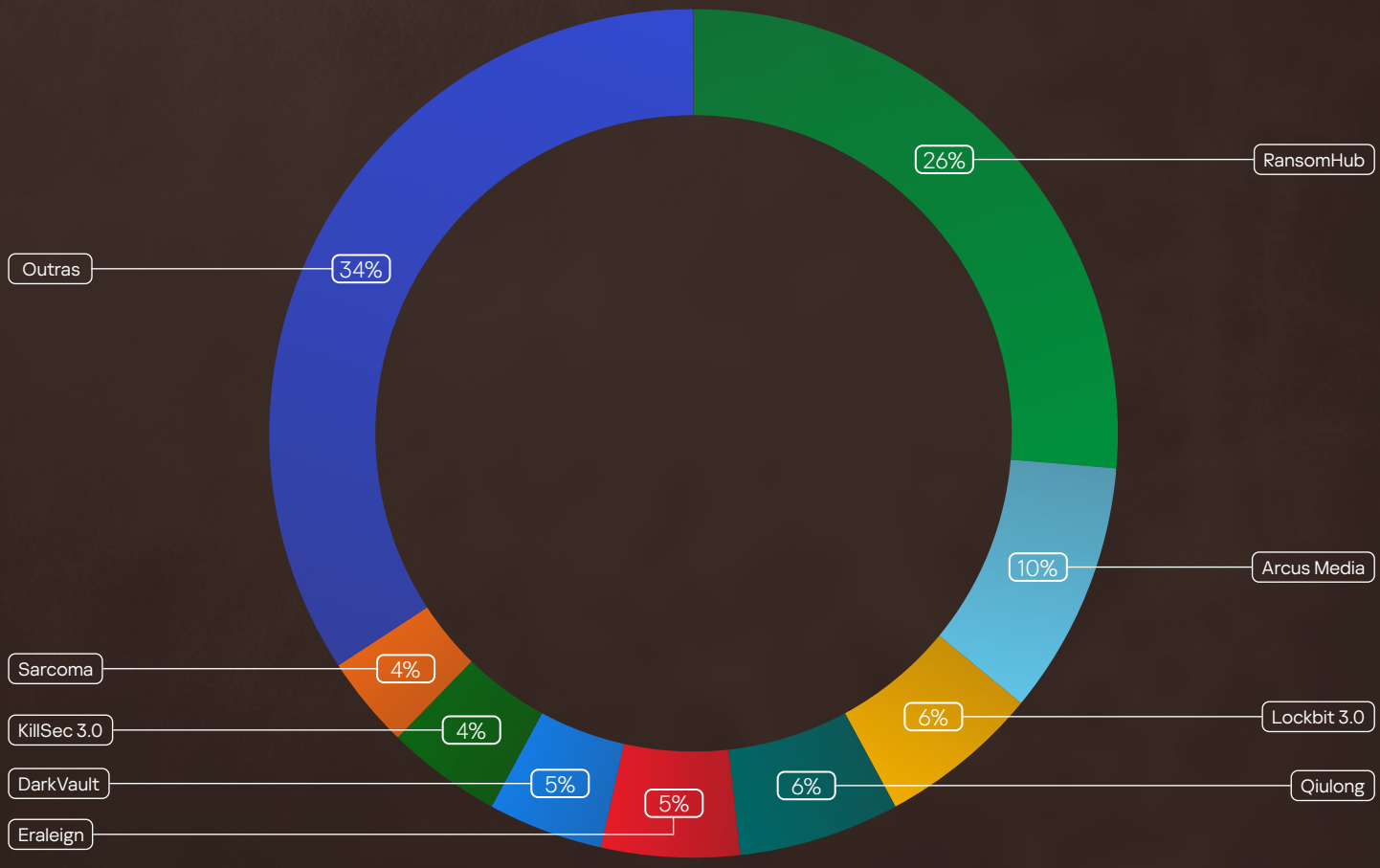


Figura 2 | Ataques de ransomware direcionados a organizações brasileiras em 2024

Cerca de 30 agentes de ransomware atacaram empresas brasileiras em 2024. Os mais ativos foram RansomHub, Arcus Media, Lockbit 3.0, Quilong e Eraleign. Juntos, eles realizaram 53% de todos os ataques daquele ano.

Figura 3 | Agentes de ransomware direcionados ao Brasil em 2024



Cerca de 30 agentes de ransomware atacaram empresas brasileiras em 2024. Os mais ativos foram RansomHub, Arcus Media, Lockbit 3.0, Quilong e Eraleign. Juntos, eles realizaram 53% de todos os ataques daquele ano.

A principal motivação dos agentes de ransomware é o ganho financeiro, seja por meio de pagamentos de resgate ou da venda de dados roubados. Os invasores escolhem alvos com base em uma estimativa de possíveis ganhos, levando em consideração fatores como receita da empresa, setor e assim por diante.

Nossa pesquisa mostra que organizações do setor de saúde (incluindo hospitais) foram as mais atacadas em 2024. Os setores financeiro, varejista e de construção civil, juntamente com prestadores de serviços profissionais e técnicos (como escritórios de contabilidade, marketing, advocacia e consultoria), compuseram o restante dos cinco primeiros colocados. Vale ressaltar que diversas entidades governamentais também ficaram entre os 10 principais alvos.

Figura 4 | Ataques de ransomware no Brasil em 2024. Dez principais setores

Capítulo 2

Erupção vulcânica

Mercado de acesso inicial

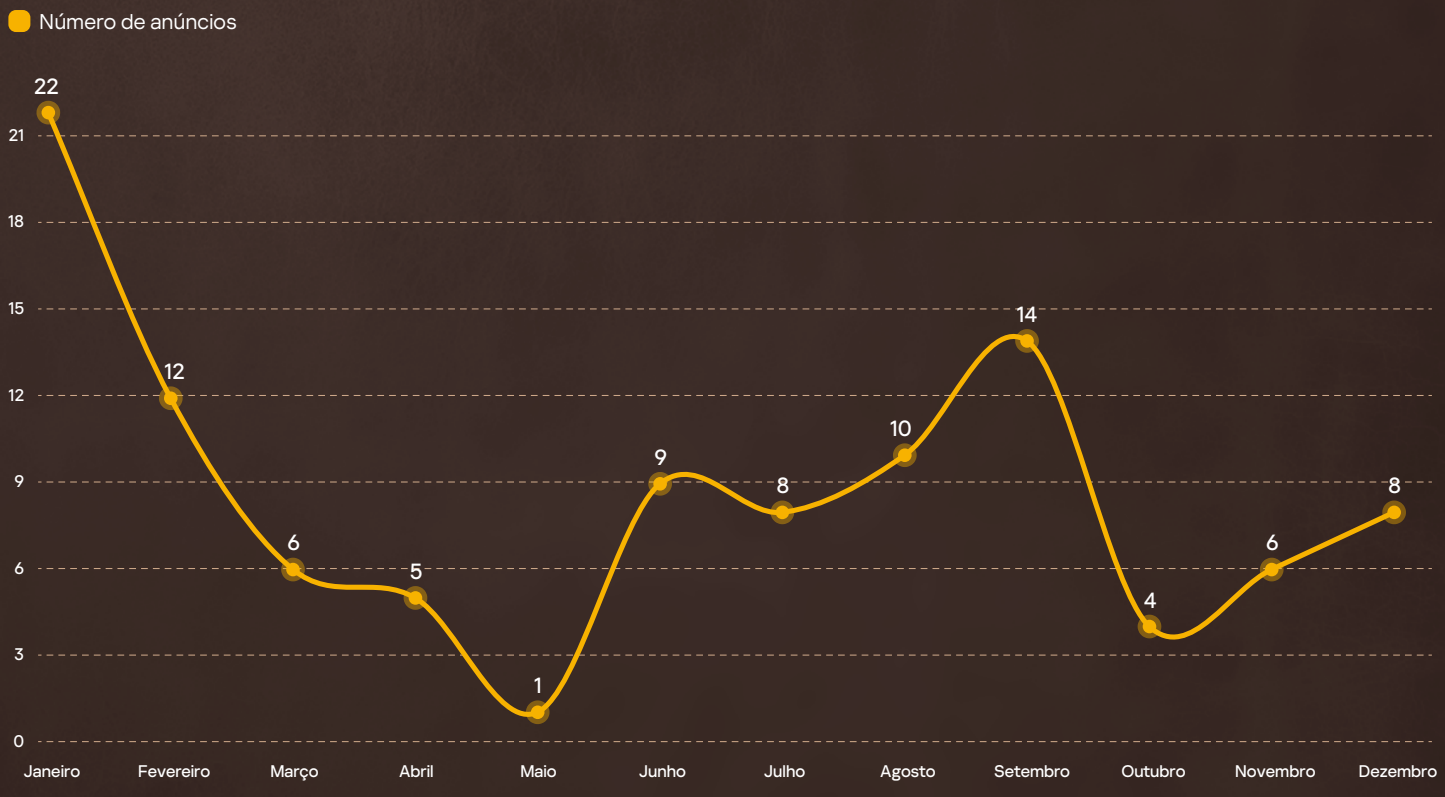
Erupção vulcânica

Mercado de acesso inicial

Outra famosa atividade praticada na comunidade do crime virtual é a venda de acesso inicial — ataques a pontos de entrada em redes internas, sistemas ou dispositivos que pertencem a várias empresas. Cibercriminosos que obtêm e vendem acesso inicial são conhecidos como corretores de desses acessos. Normalmente, esses corretores não desenvolvem ataques direcionados por vários motivos: falta de motivação, habilidades técnicas insuficientes ou crença de que sua função representa um risco legal menor.

No total, descobrimos 105 anúncios oferecendo acesso inicial a empresas e organizações brasileiras. Alguns desses anúncios vendem pacotes de acesso com o fornecimento de pontos de entrada para múltiplos sistemas, servidores, dispositivos (como clientes VPN corporativos ou serviços SSH expostos) ou sites.

Figura 5 | Anúncios sobre acesso inicial no Brasil publicados na dark web em 2024



No entanto, é importante observar que algumas negociações podem ocorrer sem serem publicadas em recursos da dark web. Agentes maliciosos, incluindo gangues de ransomware, frequentemente cooperam com corretores de acesso inicial bem conhecidos e confiáveis dentro da comunidade. Observamos solicitações relacionadas de tempos em tempos.

Figura 6 | Procurando um corretor de acesso inicial para cooperação em ataques de ransomware.

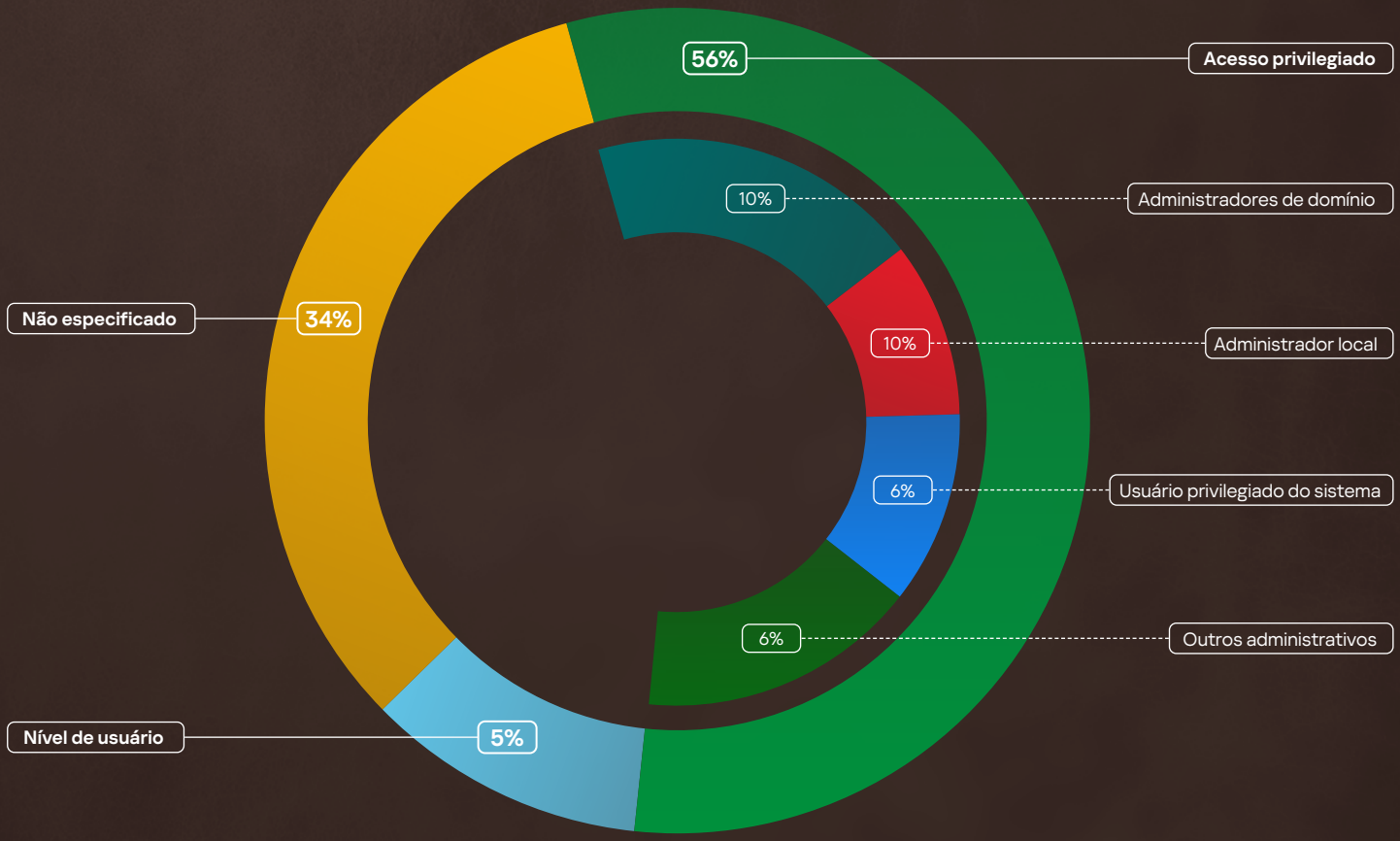
Os tipos comuns de acesso corporativo inicial incluem:

Acesso à rede interna por meio de uma combinação de contas VPN válidas para entrar na rede corporativa, além de interfaces de gerenciamento remoto (por exemplo, RDP, SSH ou software como ScreenConnect, VNC e AnyDesk) para acessar hosts ou dispositivos específicos.

Acesso a dispositivos corporativos individuais, servidores, serviços ou sistemas expostos a redes externas (como painéis de controle, firewalls, bancos de dados, sites e sistemas CRM) usando credenciais válidas, via shells (por exemplo, Web ou reverso) ou explorando vulnerabilidades críticas como execução remota de código (RCE) ou injeção SQL. Mesmo que os invasores não consigam violar a rede interna, eles ainda podem exfiltrar dados confidenciais de recursos de vítimas comprometidas.

Em ambos os casos, o acesso mais privilegiado exige um preço alto, pois permite um maior desenvolvimento do ataque. No entanto, em um terço dos anúncios, os cibercriminosos nem sequer especificam essa informação.

Figura 7 | Nível de acesso inicial comercializado no Brasil em 2024



As informações sobre o acesso inicial são bastante sensíveis para ambos os lados, para cibercriminosos e profissionais de segurança responsáveis por proteger a infraestrutura de TI empresarial, corporativa e do setor público na região. Cibercriminosos evitam revelar informações explícitas em anúncios que possam identificar organizações-alvo e, possivelmente, frustrar ataques futuros. Em vez disso, eles geralmente especificam apenas informações gerais, como o país-sede, setor, receita estimada, número de funcionários, hosts de rede ou software antivírus em uso.

Resumidamente, no mercado de acesso inicial em 2024, organizações brasileiras governamentais e do setor de saúde estiveram entre as mais afetadas. Em um quinto dos anúncios, nenhum setor foi especificado.

Figura 8 | Os dez principais setores por número de ofertas de acesso inicial publicadas na dark web em 2024

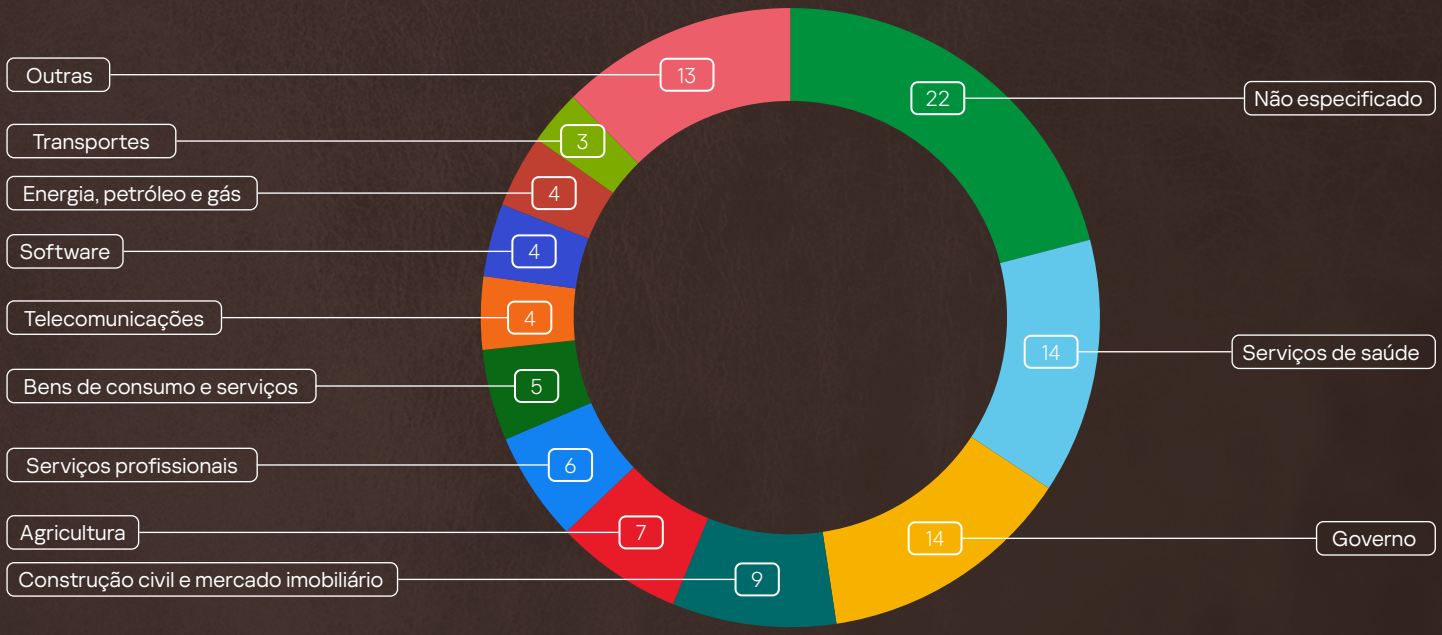


Figura 9 | Exemplo de um anúncio que negocia o acesso corporativo inicial

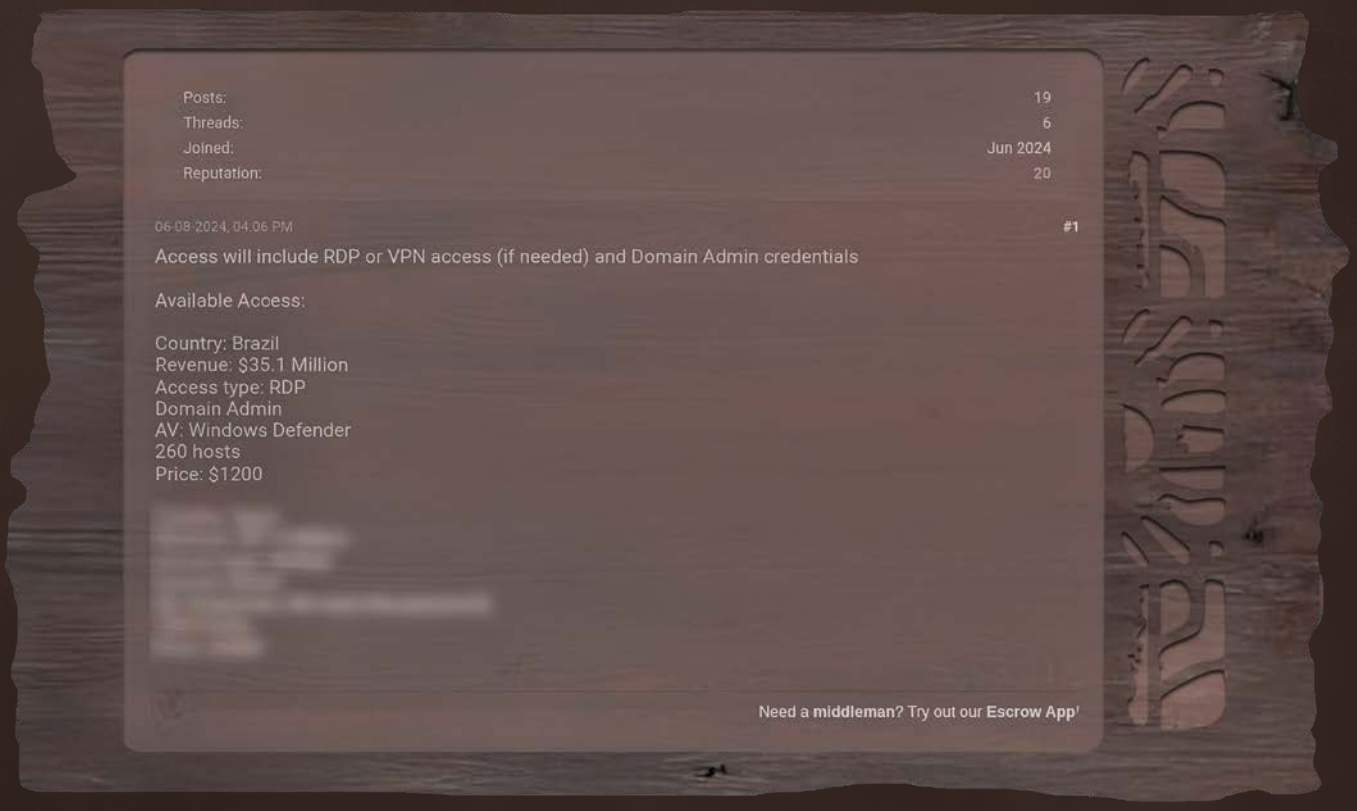
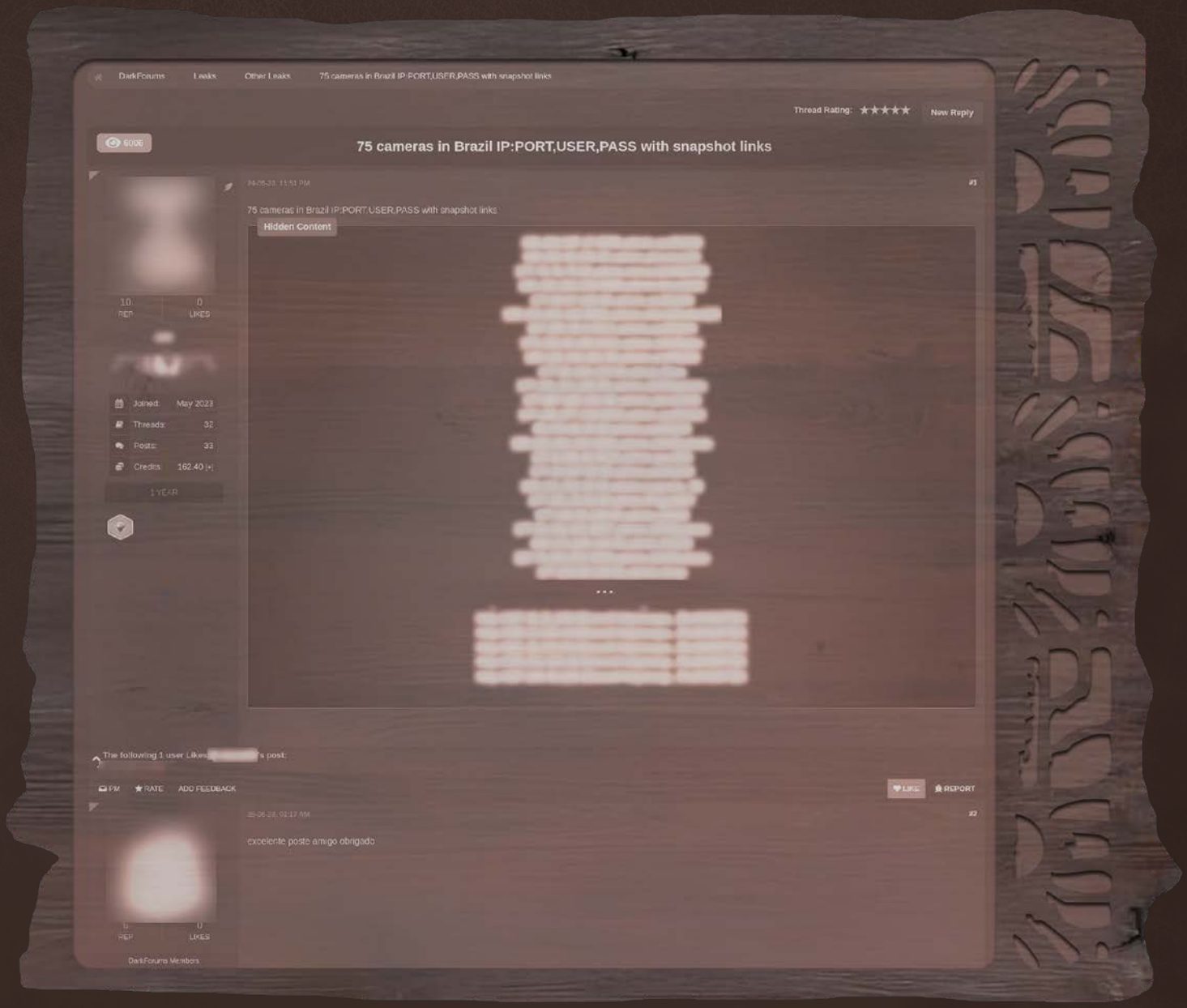


Figura 10 | Venda de acesso a câmeras IP



Capítulo 3

Devastação da aldeia

Violação de dados

Devastação da aldeia

Violação de dados

Analisamos os recursos da dark web em busca de publicações e mensagens relacionadas à distribuição e venda de bancos de dados, documentos, listas de credenciais comprometidas, bem como quaisquer outras informações que possivelmente seriam úteis para cibercriminosos em ataques futuros. Aqui é possível observar três tipos principais de dados em oferta, de acordo com a respectiva relevância e gravidade

Violação de dados

Os dados mais valiosos e confiáveis oferecem mais oportunidades de ataque: bancos de dados ou documentos roubados diretamente de organizações, os respectivos aplicativos ou sistemas como resultado de invasões bem-sucedidas, atividade intencional de funcionários maliciosos — atividades internas ou vazamentos acidentais causados pelo "fator humano" (por exemplo, erros de desenvolvedores ou comportamento desprotegido de funcionários).

Republicações e combinações de vazamentos anteriores

As duas principais razões para tal demanda são:

1. Um banco de dados distribuído pode não ter estado disponível de forma gratuita anteriormente.
2. Os invasores perderam a oportunidade de baixar os dados devido ao curto tempo de expiração dos links para os arquivos compartilhados, geralmente definido após a publicação.

Listas combinadas e de alvos

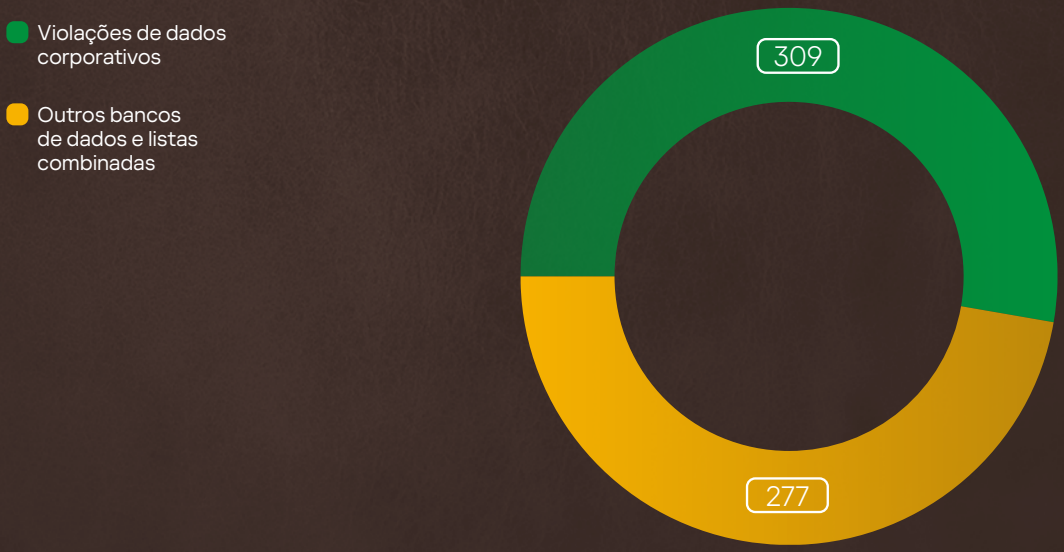
Bancos de dados especialmente elaborados com informações sobre grupos específicos de vítimas — por cidadania, residência, nível de renda, tipo de propriedade, setor de atuação etc. Esses dados são menos valorizados, mas comumente usados para phishing e outras fraudes direcionadas a grupos específicos de vítimas.

Vale mencionar que vazamentos de dados ou documentos representam mais do que apenas riscos de cibersegurança e reputação para a empresa afetada — também aumentam o risco de ataques futuros contra funcionários, parceiros, consumidores, clientes e qualquer pessoa ou organizações afiliada. Os cibercriminosos usam violações para cometer uma ampla gama de fraudes: desde spam e phishing simples até ataques direcionados usando o perfil da vítima, ataques à cadeia de suprimentos e chantagem a funcionários de alto escalão.

Durante todo o ano de 2024, observamos 586 anúncios em diversos fóruns da dark web oferecendo violações de dados ou outros bancos de dados com informações sobre organizações brasileiras, entidades públicas, cidadãos ou usuários. De acordo com as descrições, mais da metade (53%) originou-se de violações de dados corporativos que afetaram 185 empresas ou instituições estatais (alguns bancos de dados foram republicados diversas vezes durante o ano)[3].

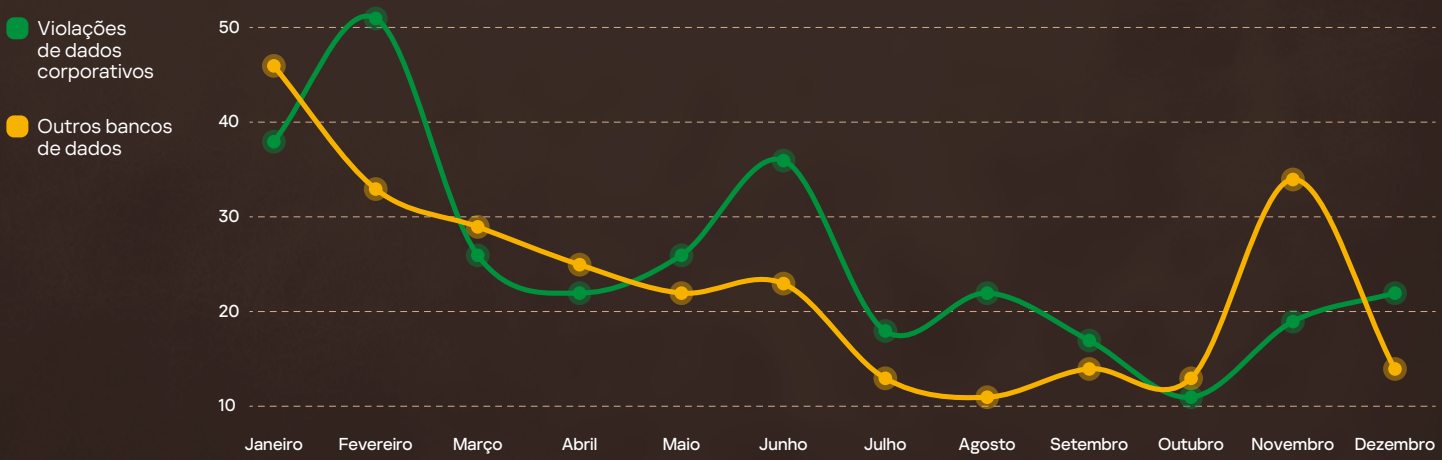
Outros bancos de dados continham informações sobre cidadãos individuais — aqui observamos diversos bancos de dados não especificados com informações pessoais, bem como listas mistas ou direcionadas combinadas de diferentes maneiras. Essa taxa substancial de bancos de dados genéricos (47%) indica que a atividade cibercriminosa ampla e não direcionada no Brasil está em um nível elevado.

Figura 11 | Tipos de bancos de dados distribuídos na dark web em 2024



Em média, houve 49 publicações por mês, sendo 25,5 delas relacionadas a violações de dados corporativos. Curiosamente, no início do ano, houve mais publicações oferecendo bancos de dados relacionados a organizações ou cidadãos brasileiros, embora a atividade geral tenha permanecido relativamente estável ao longo do ano, com uma leve queda no terceiro trimestre.

Figura 12 | Anúncios oferecendo bancos de dados relacionados ao Brasil em 2024



3 As estatísticas são baseadas em informações de publicações feitas por agentes de ameaças na dark web. Para evitar o acesso não autorizado aos dados das empresas afetadas durante a pesquisa, as informações comprometidas não foram verificadas.

Em relação à violações de dados corporativos, observamos que instituições públicas, incluindo diferentes administrações regionais, foram as mais afetadas. Os bancos de dados relacionados ao governo representaram 16% de todos os anúncios nesta categoria. As organizações de telecomunicações e empresas de serviços profissionais completaram as três primeiras posições. Vale destacar também a tendência de ataques a organizações médicas, incluindo hospitais. Conforme mencionado na visão geral de ransomware, organizações de saúde também estão representadas entre os dez setores mais visados.

Figura 13 | Distribuição de violações de dados corporativos no Brasil em 2024. Dez principais setores

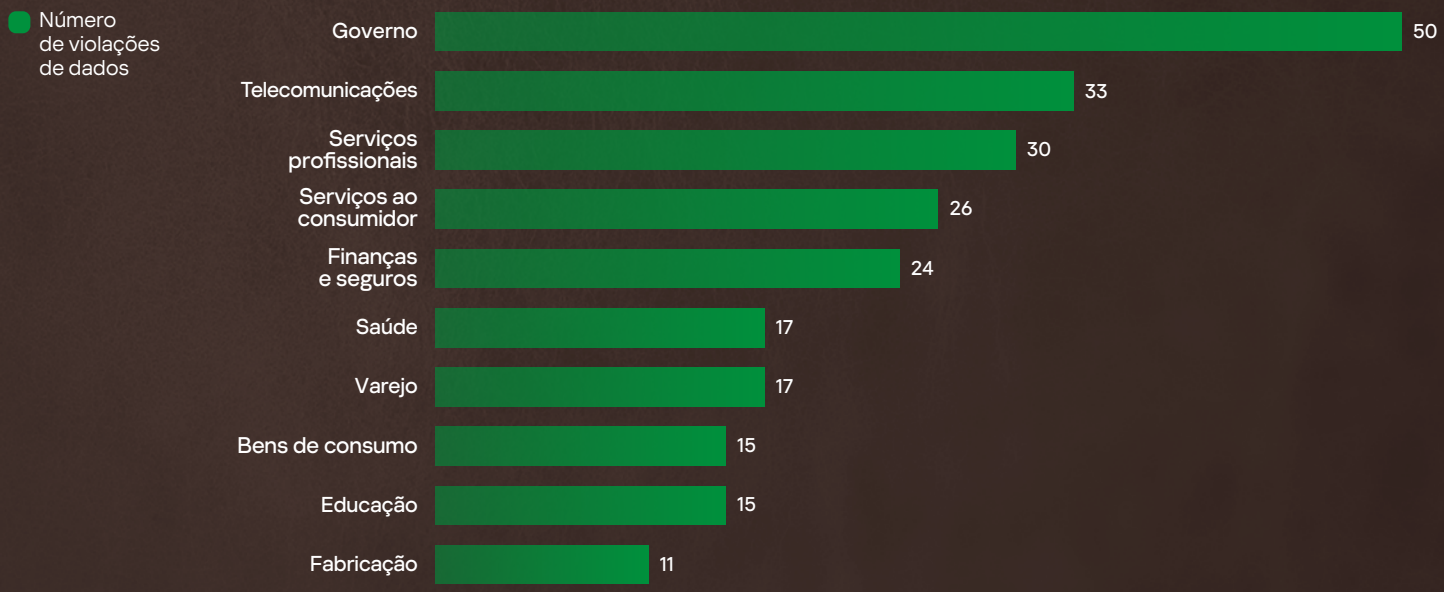
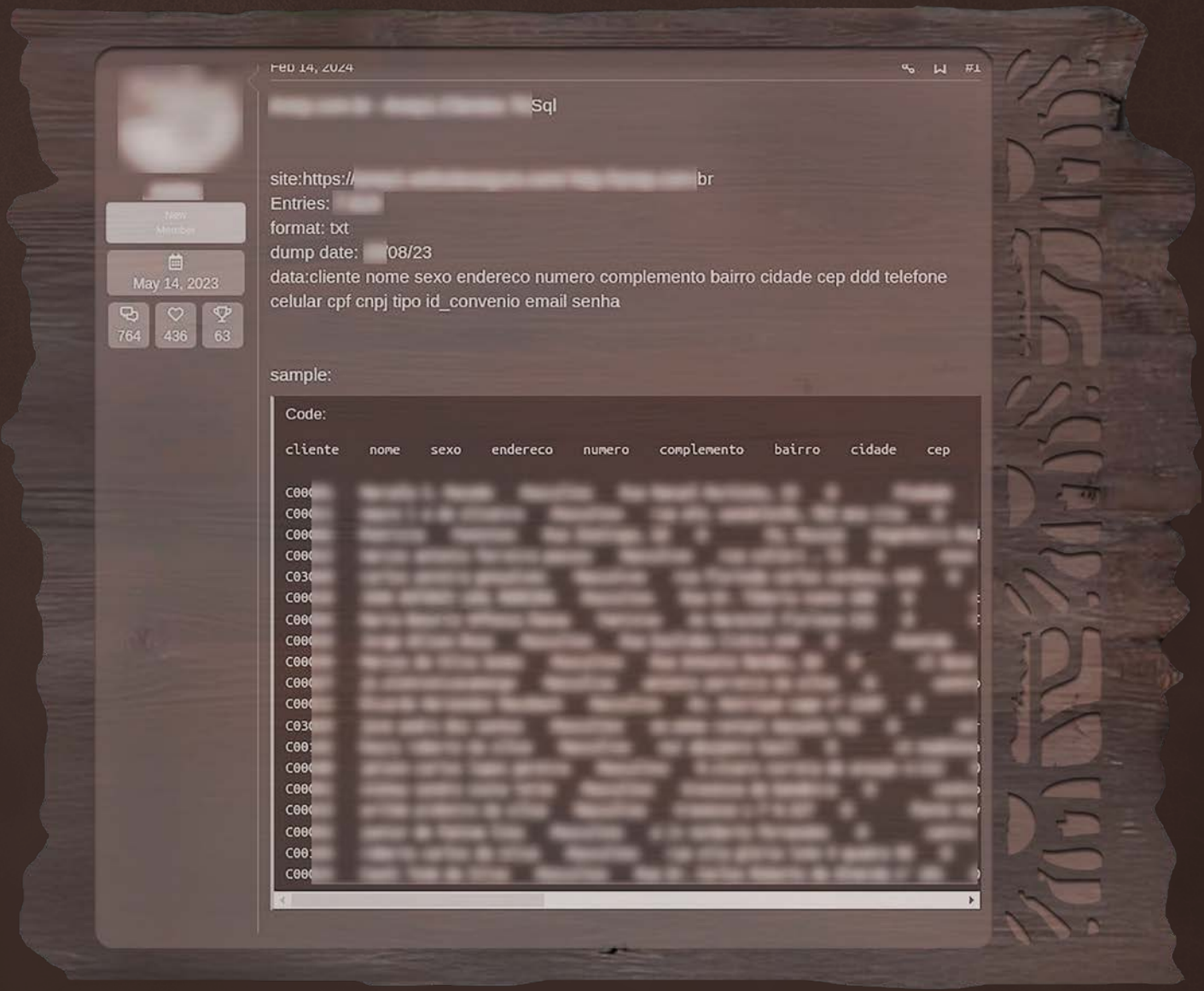


Figura 14 | Exemplo de um anúncio no Telegram compartilhando o vazamento de dados de um recurso governamental (fonte: Threat Lookup do portal Kaspersky Threat Intelligence).

Figura 15 | Exemplo de um anúncio em um fórum da dark web compartilhando uma violação de dados corporativos.



Capítulo 4

Ameaças onipresentes

Atividade de ladrões de informações

Ameaças onipresentes

Atividade de ladrões de informações

A cada ano, milhões de dispositivos em todo o mundo são comprometidos por diversos tipos de malware projetados para roubar secretamente dados confidenciais e sensíveis. Dependendo de sua funcionalidade, esses programas coletam informações armazenadas no dispositivo (como histórico do navegador e senhas salvas), interceptam dados introduzidos, incluindo credenciais de usuário, informações de cartões bancários ou carteiras digitais, coletam cookies, tokens, chaves de API, fazem capturas de tela e assim por diante.

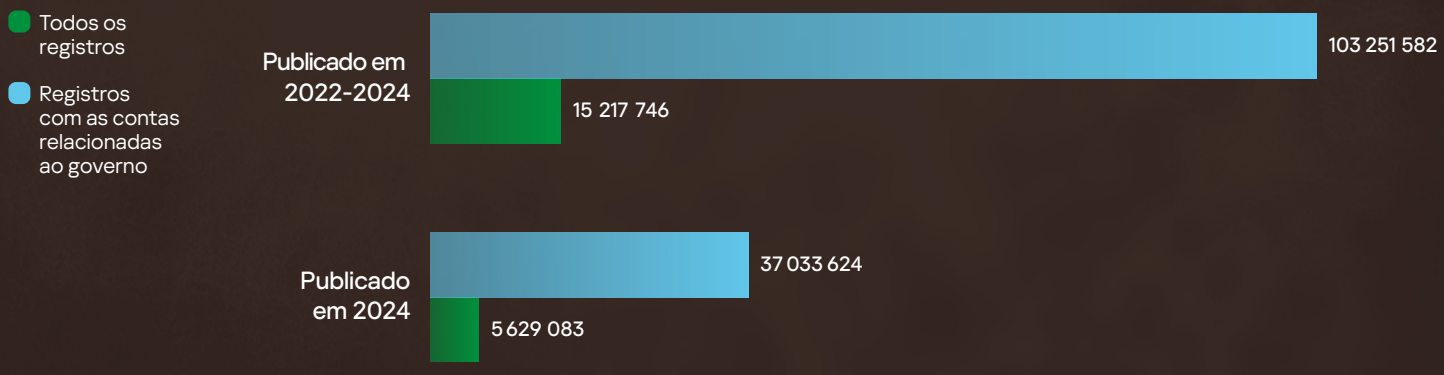
Todos os dados roubados são consolidados em arquivos de log e enviados para servidores de controle gerenciados por operadores de malware. Na verdade, há um atraso entre o momento em que a informação é roubada e o momento em que ela aparece na dark web. É comum observar um vazamento de dados que aconteceu em 2022 ou anteriormente aparecer apenas em logs publicados em 2024. Isso ocorre porque os operadores de malware primeiro analisam as informações recuperadas para extrair qualquer coisa particularmente útil para suas atividades — como contas válidas para sistemas e serviços corporativos, dados financeiros — antes de vender ou compartilhar os logs a outros cibercriminosos por meio de mercados da darknet ou outros canais da dark web.

Analisamos logs de ladrões de informações para identificar registros contendo contas comprometidas relacionadas ao domínio de nível superior regional brasileiro (.br). O número total de tais registros publicados em logs de malware nos últimos quatro anos é superior a 103 milhões, com mais de um terço (cerca de 37 milhões de linhas) publicado unicamente em 2024.

Também preparamos um relatório de pesquisa detalhado, "Tormenta de roubo de dados", no qual exploramos o mercado da dark web de credenciais comprometidas publicadas em logs de ladrões de informações em 2024. Isso acompanha nosso relatório anterior, que analisou dados de logs de ladrões de informações publicados entre 2021 e 2023. Entre outras descobertas, a análise revelou que recursos brasileiros lideraram as infecções por ladrões de informações em 2023.

Uma análise especial dos registros de importantes entidades governamentais mostra que 15% de todos os registros em logs — representando 5,6 milhões de linhas publicadas em 2024 e mais de 15 milhões nos últimos três anos — contêm contas pertencentes a funcionários de importantes órgãos estatais brasileiros ou aquelas usadas por cidadãos e empresas para acessar diversos serviços públicos.

Figura 16 | Registros de logs de ladrões de informações. Estatísticas gerais

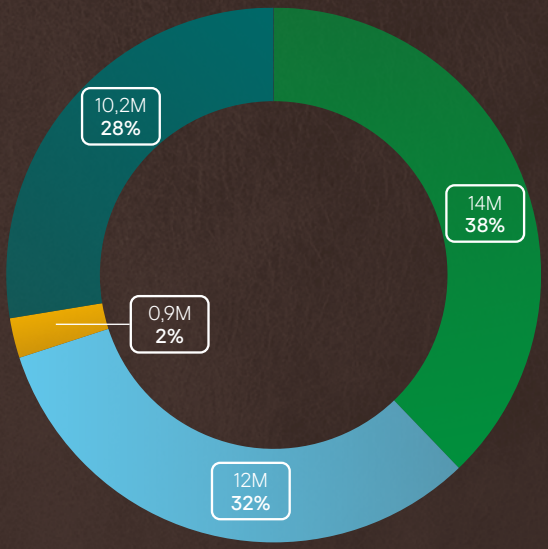


Os diagramas a seguir mostram que 38% de todos os registros publicados em logs de malware em 2024 contêm contas que foram vazadas naquele ano, enquanto um terço corresponde a 2023 e uma parcela menor data de 2022, 2021 ou anteriormente.

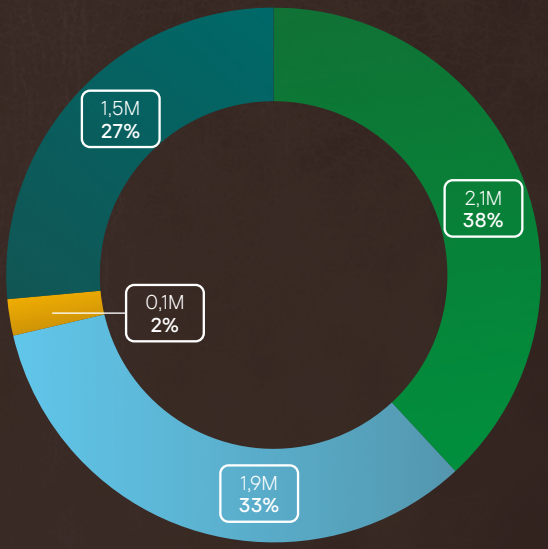
Figura 17 | Estatísticas sobre os anos de comprometimento das contas. Registros publicados em 2024*

2024
2023
2022 ou anterior
Não determinado

*Os diagramas exibem números arredondados.



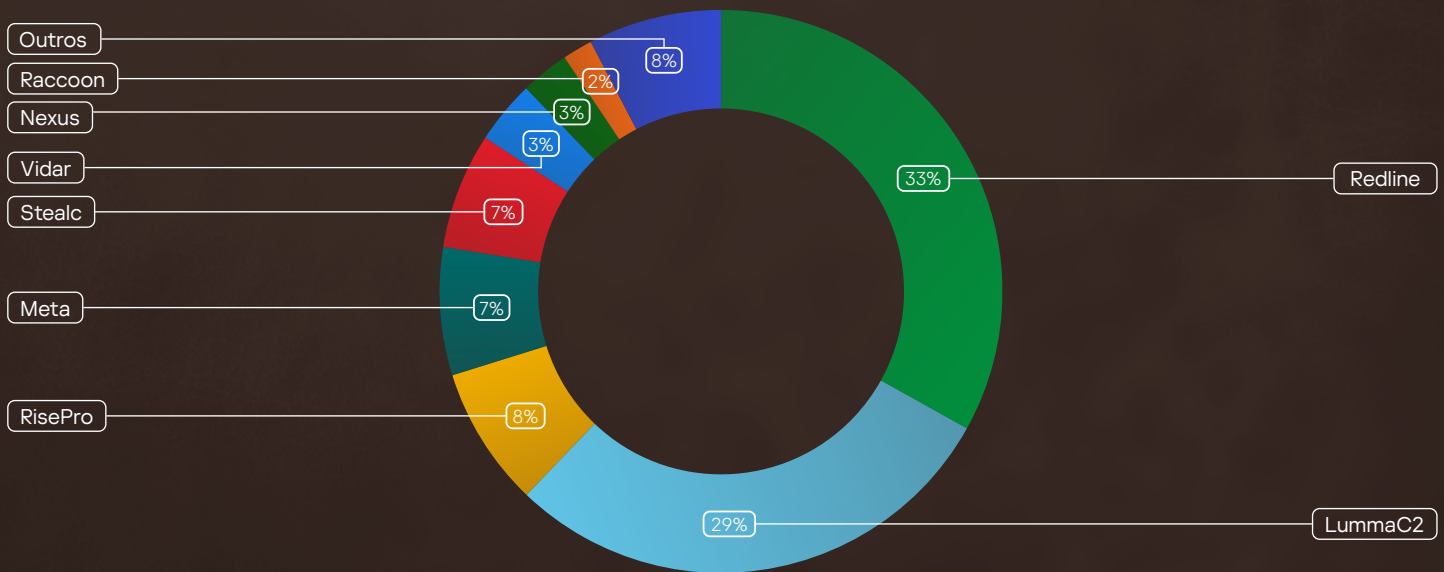
Todos os registros publicados em 2024



Registros com contas relacionadas ao governo

No Brasil, mais de 60% de toda a atividade de ladrões de informações envolve os malwares RedLine e LummaC2 (ou apenas Lumma). RisePro, Meta (uma versão "aprimorada" do RedLine que surgiu em 2022) e Stealc também figuram entre os cinco principais com base no número de contas comprometidas publicadas na dark web em 2024.

Figura 18 | Atividade de ladrões de informações no Brasil em 2024



Resultados da jornada:

Resultados da jornada

O cenário completo de ameaças representadas por cibercriminosos da dark web para empresas e instituições públicas brasileiras não pode ser totalmente coberto em um único relatório, pois as atividades variam amplamente entre os setores e evoluíram significativamente nos últimos anos. Entre outros fatores, a implementação mais ampla e o desenvolvimento constante de modelos de malware como serviço e ransomware como serviço impulsionaram um aumento acentuado na atividade e nos ataques maliciosos relacionados. Esses modelos permitem que uma gama muito maior de cibercriminosos sem habilidades técnicas avançadas realize ataques contra cada vez mais alvos.

O Brasil está na mira dos cibercriminosos mais do que muitos outros países por uma série de razões, incluindo sua grande população, crescimento econômico e cenário comercial diversificado. O volume de ataques e a atividade de crimes virtuais em geral são intensos. Dessa forma, é necessário apoiar o crescimento econômico na região fortalecendo a TI e a cibersegurança. Assim, governos, empresas e outras organizações podem se proteger contra ciberataques e ameaças em constante evolução que emergem da dark web.

Portanto, é cada vez mais importante adotar uma abordagem proativa e rápida para se defender contra ameaças virtuais, ataques e outros incidentes de cibersegurança — em outras palavras, manter-se um passo à frente de possíveis adversários. Isso é, sem dúvida, desafiador, mas crucial. Recomendamos uma estratégia de segurança clara para proteger a infraestrutura de TI corporativa e os ambientes digitais.

Para obter informações sobre serviços de monitoramento de ameaças para sua organização, entre em contato conosco por meio do site do **Kaspersky Digital Footprint Intelligence** ou diretamente pelo e-mail dfi@kaspersky.com.

Digital Footprint Intelligence

Se já estiver enfrentando um incidente, nosso serviço **Kaspersky Incident Response** ajudará você a responder e minimizar as consequências, principalmente identificando nós comprometidos e protegendo sua infraestrutura contra ataques semelhantes no futuro.

Incident Response

Para descobrir ciberataques ocultos ou garantir que seu ambiente não seja comprometido, considere nosso serviço **Kaspersky Compromise Assessment**.

Avaliação de comprometimento

Se você planeja avaliar e aprimorar a postura de segurança da sua organização, o **Kaspersky Security Assessment** inclui uma variedade de serviços, além de testes de penetração e red teaming.

Security Assessment

Estratégia de proteção

Inventário de ativos de TI e gerenciamento de correções

Primeiramente, identifique todos os ativos que você precisa proteger, implemente atualizações frequentes de software e garanta que os invasores não tenham chance de explorar vulnerabilidades conhecidas.

Soluções abrangentes de segurança

Utilize controles de segurança multicamadas em todos os componentes da sua infraestrutura de rede para obter melhor visibilidade de todo o seu ambiente e possibilitar a detecção e prevenção oportunas de vários tipos de ataques.

Mantenha a conscientização sobre segurança entre os membros da equipe

Independentemente dos controles de segurança utilizados, o fator humano continua sendo uma das vulnerabilidades mais sérias e comuns que levam a violações de segurança.

Monitoramento e avaliação contínuos

Monitore de perto todos os dispositivos, servidores, sistemas, serviços, aplicativos e tráfego em busca de qualquer atividade suspeita — a detecção precoce de uma atividade maliciosa é fundamental.

Inteligência de ameaças (IA) atualizada

Revise regularmente os dados de TI para entender táticas, técnicas e procedimentos mais recentes usados por invasores e adapte suas defesas de acordo.

Monitoramento da dark web

Informe-se sempre sobre possíveis vetores de ataques, interesses e planos de cibercriminosos e ameaças emergentes. Conhecimento é poder — reforça suas defesas e permite respostas proativas e reativas oportunas.

kaspersky

Relatórios analíticos

Fluindo pela Amazônia

O cenário de ameaças da dark web no Brasil

www.kaspersky.com.br

#kaspersky
#bringonthefuture