kaspersky bring on the future

O cenário de ameaças em constante evolução dos infostealers:

tendências, estatísticas e estratégias de mitigação

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

Verifique o relatório de 2024 sobre o cenário de ameaças dos infostealers

As estatísticas de anos anteriores podem diferir de publicações anteriores porque credenciais comprometidas mais antigas continuam a surgir na dark web ao longo do tempo, e ajustamos os números desses anos de acordo.

Introdução

O malware infostealer se tornou uma das ameaças cibernéticas mais onipresentes, afetando milhões de dispositivos em todo o mundo e comprometendo dados confidenciais pessoais e corporativos. Esses programas maliciosos são projetados para obter credenciais, cookies, registros financeiros e outras informações valiosas, que então são agrupadas em arquivos de log e disponibilizadas para a rede criminosa da dark web.

A equipe da Kaspersky Digital Footprint Intelligence monitora de perto as atividades dos infostealers para analisar as novas tendências e as táticas desenvolvidas pelos criminosos. No ano passado, nós publicamos um relatório contendo uma análise de dados de arquivos de log de infostealers que haviam sido vazados na dark web e eram datados de 2021 a 2023.

O relatório traz as nossas descobertas mais recentes de 2024, incluindo estatísticas atualizadas, informações novas e existentes sobre variantes de infostealers e estratégias para mitigar riscos.

Ao entender como os infostealers operam e como seus arquivos de log são distribuídos, organizações e indivíduos podem ser proativos e agir para aumentar sua cibersegurança. Esse relatório fornece dados importantes, recomendações práticas e reflexões de especialistas para ajudar as organizações a se prevenir, detectar e lidar com as ameaças relacionadas aos infostealers.

Novidades na Kaspersky Digital Footprint Intelligence em 2024

Os cibercriminosos continuam desenvolvendo seus artifícios, o que levou o malware a evoluir e adquirir novas funcionalidades. Porém, os recursos de defesa também evoluíram. Aprimoramos nossa abordagem de monitoramento dos recursos da dark web, principalmente aqueles nos quais os arquivos de log dos infostealers são publicados com frequência.

O aumento no volume de dados analisados exige atualizações na lógica de análise. Nosso foco foi verificar a exclusividade dos dados adicionados, remover arquivos duplicados e filtrar informações irrelevantes frequentemente encontradas nos arquivos de log.

Nesta pesquisa, considera-se que um arquivo de log exclusivo corresponde a uma infecção em um único dispositivo.

Um arquivo de log é um arquivo compactado que contém dados de usuários roubados. Ele consiste basicamente em arquivos de texto que contêm credenciais de contas, parâmetros de cookies e metadados. No entanto, ele também pode incluir imagens, como capturas de tela da área de trabalho ou fotos da câmera, além de documentos e outros arquivos do usuário, como os que são armazenados na área de trabalho.

7,68%

O número de arquivos de log coletados e processados por nós aumentou em 7,68% em comparação com o ano passado.

Cibercriminosos publicam arquivos de log de infostealer de dispositivos infectados em seções privadas de fóruns clandestinos na dark web. Embora os invasores geralmente vendam esses registros, eles também podem compartilhá-los gratuitamente após obterem todas as informações valiosas para aumentar sua reputação na comunidade cibercriminosa. Analisamos esses arquivos de log para identificar contas que foram comprometidas. A presença de uma conta nesses logs indica que o dispositivo do usuário foi infectado.

50,9

Em média, um arquivo de log inclui 50,9 contas comprometidas. O armazenamento de senhas em arquivos de texto, principalmente na área de trabalho, é extremamente inseguro. É altamente recomendável usar soluções seguras para o gerenciamento de senhas.

Como superamos os obstáculos relativos às análises

O principal obstáculo é identificar a exclusividade dos arquivos de log. Esses arquivos são repostados com frequência em muitas plataformas da dark web, às vezes com algumas alterações:

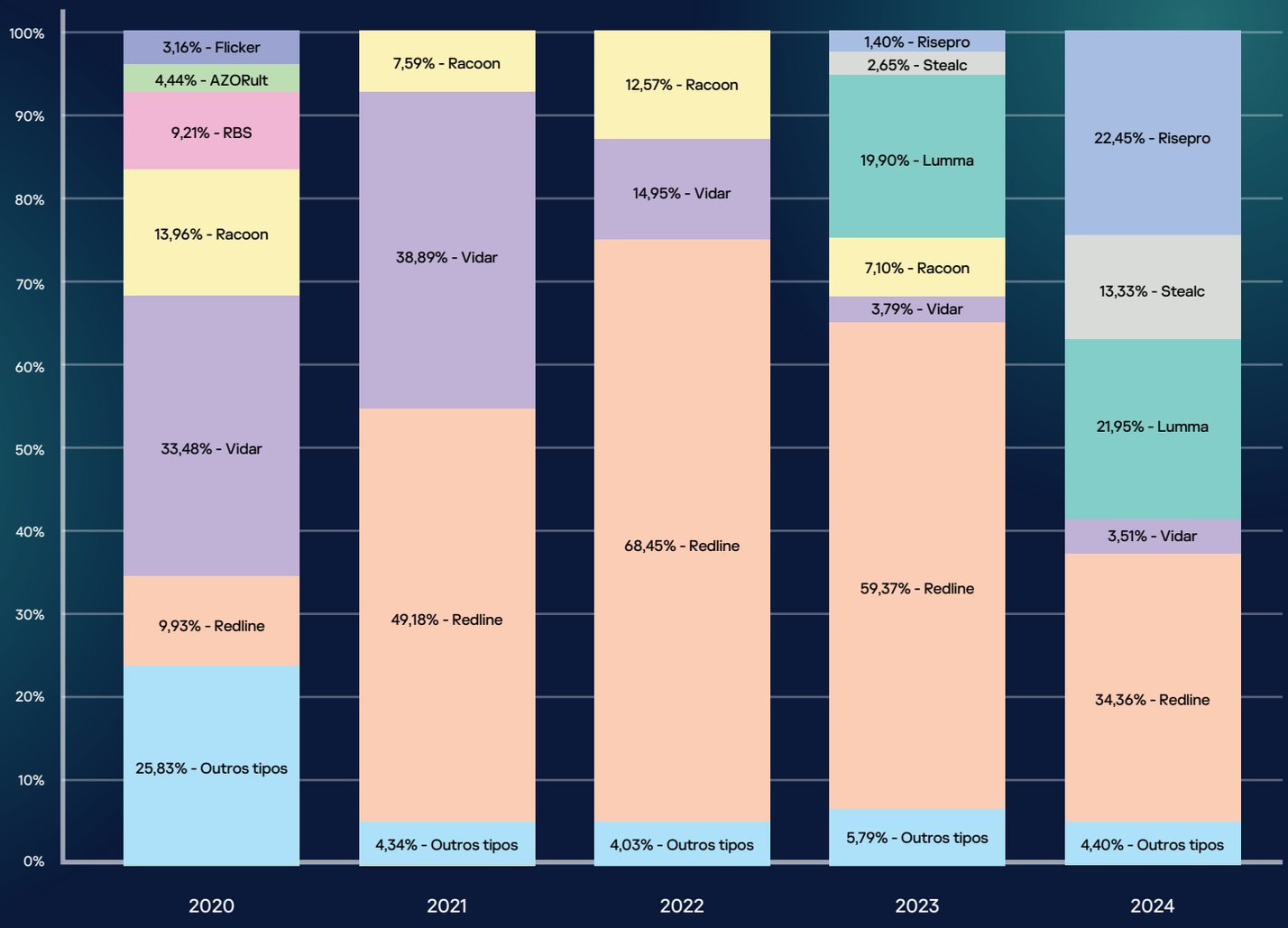
- **Publicidade adicional:** os invasores podem criar arquivos promocionais separados ou adicionar links dentro dos arquivos que já foram publicados, geralmente em arquivos de contas ou de metadados. De vez em quando, a publicidade é embutida nos nomes dos arquivos de log.
- **Remoções parciais:** alguns arquivos, como capturas de tela da área de trabalho ou imagens da câmera, podem ser excluídos do arquivo original para reduzir o tamanho do arquivo de log.
- **Alterações no formato** de arquivos de texto.

Essas alterações afetam o cálculo das somas de verificação usadas para determinar se um arquivo de log é exclusivo ou já foi processado. É essencial evitar a inserção de arquivos duplicados, mas uma filtragem muito agressiva pode levar à exclusão de arquivos que já foram considerados, mas que contêm informações valiosas. Além disso, verificações de exclusividade excessivas podem omitir os logs relacionados a infecções recorrentes, resultando na perda de dados essenciais.

Estatísticas de infecção por tipo de roubo

Uma primeira conclusão resultante da nossa análise é a distribuição de infecções por tipo de infostealer nos últimos cinco anos (2020 a 2024). Esses dados ajudam a rastrear os níveis de atividade e popularidade de diferentes tipos de malware ano após ano.

Em 2024, a maioria das infecções foi causada pelo Redline, seguido pelo Risepro e pelo Lumma.



Infecções por tipo de malware de roubo de dados de 2020 a 2024

Os dados relativos a 2023 sofreram um leve ajuste em comparação com o relatório do ano passado. A causa dessa revisão das estatísticas é que mais arquivos de log do ano de 2023 foram divulgados na dark web ao longo de 2024.

Os cibercriminosos têm o costume de divulgar arquivos de log roubados meses ou até mesmo anos após a infecção ter ocorrido. Por causa disso, nós prestamos atenção tanto na data da divulgação quanto na data em que o comprometimento efetivamente ocorreu. A maior parte das infecções referentes a anos anteriores é observada ao final de cada ano, e não no início. Isso ocorre porque credenciais antigas comprometidas continuam surgindo na dark web ao longo do tempo.

A infecção mais significativa de 2024 foi causada pelo stealer Risepro, cujo número de infecções aumentou de 1,4% em 2023 para 22,45% em 2024, e pelo Stealc, que surgiu pela primeira vez em 2023 e aumentou sua participação de 2,65% para 13,33%. Em 2024, o Redline permaneceu como o infostealer mais prevalente, representando 34,36% das infecções

Tendências de infecção anuais

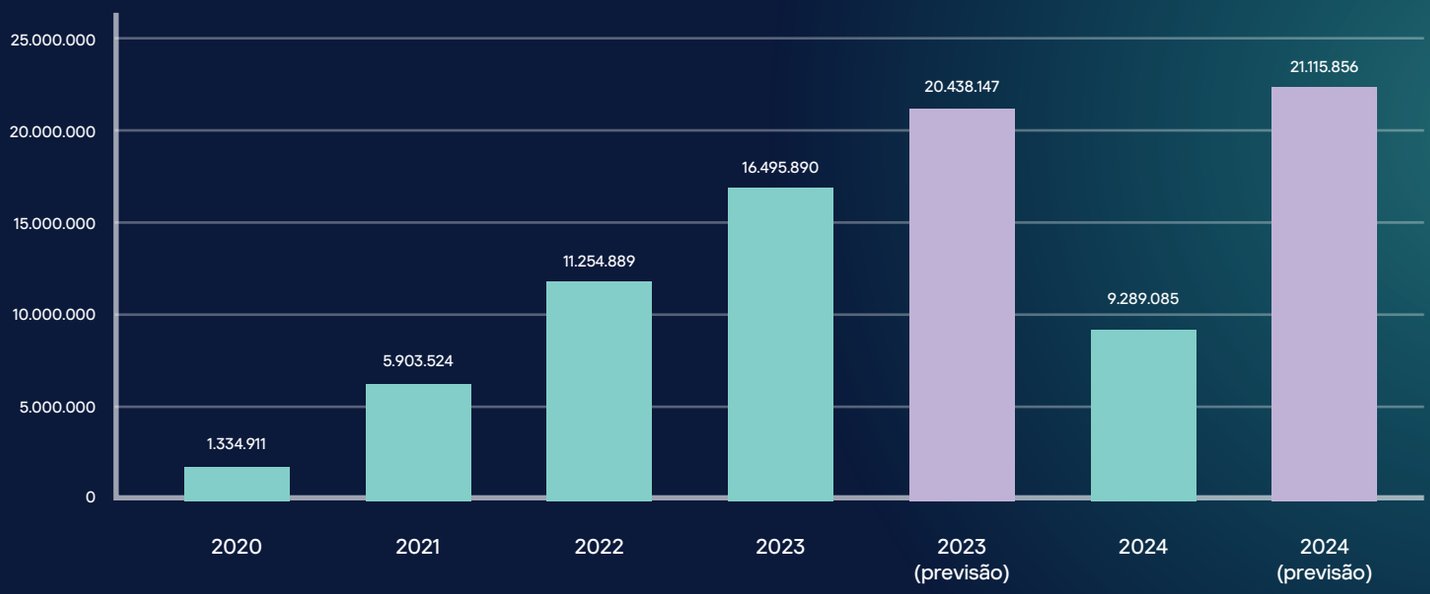
Em agosto de 2024, nós estimamos que 15.908.793 dispositivos haviam sido infectados com infostealers em 2023, com o subsequente vazamento dos logs na dark web.

Revisão das previsões de 2023. Em 2024, fizemos uma previsão do número de infecções ocorridas em 2023, já que alguns arquivos de log daquele ano ainda não haviam sido divulgados nos recursos da dark web. Conforme explicado na seção "Contexto" em "Estatísticas de infecções por tipo de malware de roubo de dados", há um intervalo de tempo entre a data de infecção e a data de divulgação do arquivo de log em uma plataforma da dark web.

Em agosto de 2024, nós estimamos que 15.908.793 dispositivos haviam sido infectados com infostealers em 2023, com o subsequente vazamento dos logs na dark web. Mas, em março de 2025, o número de arquivos de log processados (equivalentes a infecções) datados de 2023 foi de 16.495.890, ultrapassando a nossa previsão em 3,69%.

No início de 2025, observamos que novos arquivos de log de 2023 ainda estavam sendo divulgados, o que indicava que o número total de infecções ocorridas naquele ano era bem maior.

Tendências e previsão de infecções em 2024. Estimamos que o número total de infecções em 2024 será maior do que em 2023, mas ainda permanecerá em um intervalo comparável. Em março de 2025, foram observadas 9.289.085 infecções referentes a 2024.



Estatísticas de infecção anuais, de 2020 a 2024

Nossas previsões de infecções:

- **2023: entre 18 milhões e 22 milhões de infecções.**
- **2024: entre 20 milhões e 25 milhões de infecções.**

Uso de e-mails corporativos em plataformas de terceiros

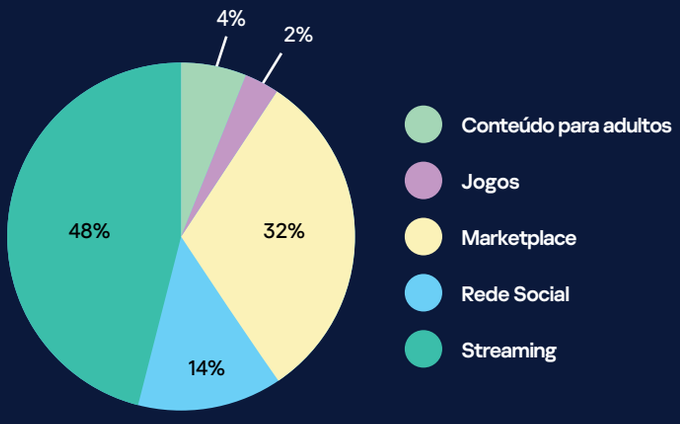
Um e-mail corporativo refere-se a um endereço de e-mail de trabalho fornecido por um empregador para a realização de tarefas profissionais e acesso aos recursos de uma empresa. Usar um e-mail corporativo em plataformas de terceiros é um risco à segurança virtual, pois isso pode ocasionar o roubo da conta do funcionário. Isso é muito importante caso a senha utilizada nos recursos de terceiros corresponda àquela utilizada nos recursos corporativos ou apresente um padrão previsível em diferentes serviços (por exemplo, um usuário pode criar senhas como Word2025!, em que "2025" seja um sufixo recorrente em todas elas). Além do mais, essa prática facilita ataques de engenharia social.

Por mais que algumas políticas de segurança permitam o uso de e-mails corporativos em serviços relacionados ao trabalho (como plataformas de RH e provedores de host), a maioria delas proíbe o seu uso em contas pessoais. Apesar disso, alguns usuários de e-mails corporativos os utilizam para fins pessoais, embora seja difícil saber a proporção exata.

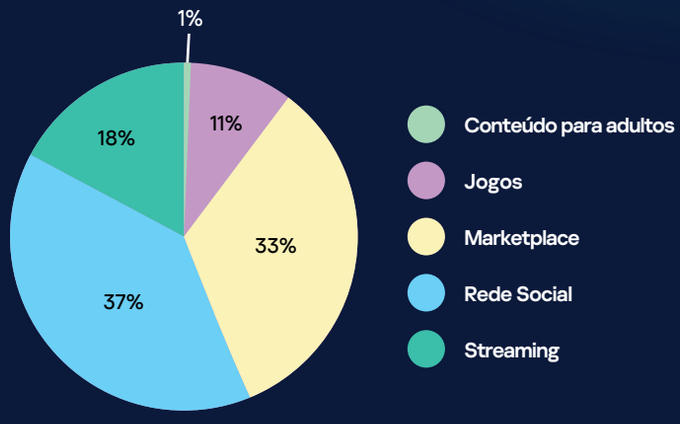
Nosso foco foi estimar a porcentagem de usuários que se registraram em três plataformas populares (Roblox, Discord e Netflix) usando um e-mail corporativo. Para tanto, nós analisamos contas comprometidas desses serviços nos quais um e-mail era utilizado para fazer login. Nossa análise revelou que, em média, **7% dos usuários cujas contas foram vazadas na dark web haviam se registrado nessas plataformas usando um e-mail corporativo.**

Para se aprofundar no assunto, nós compilamos uma amostra de 50 empresas do setor bancário para avaliar os tipos de serviços de entretenimento nos quais os usuários se registraram usando um e-mail corporativo. Analisamos credenciais comprometidas vazadas na dark web, conectadas aos domínios corporativos dessas empresas, em cinco a dez plataformas populares, divididas em cinco categorias: conteúdo adulto, mídias sociais, jogos, marketplaces e streaming.

Nosso estudo revelou que os funcionários utilizavam com frequência os seus e-mails profissionais para se registrar em serviços de streaming, marketplaces e redes sociais. Em alguns casos, e-mails corporativos também foram utilizados como login em plataformas de jogos e sites de conteúdo adulto.



Uso de e-mails corporativos em plataformas de entretenimento: estatísticas de uma amostra de 50 empresas do setor bancário



Uso de e-mails estudantis em plataformas de entretenimento

Para abordar o tema sob outro ângulo, também analisamos com que frequência endereços de e-mail com domínio .edu são usados para registro em serviços de terceiros. Esses domínios estão associados principalmente a instituições educacionais e deveriam ser usados em atividades relacionadas a estudos. No entanto, conforme demonstrado pela nossa pesquisa, algumas pessoas utilizam esses domínios para outros propósitos. Foi detectado um alto número de e-mails .edu comprometidos usados para fazer registro em plataformas de mídia social e marketplaces.

Estatísticas de infecções do SO Windows

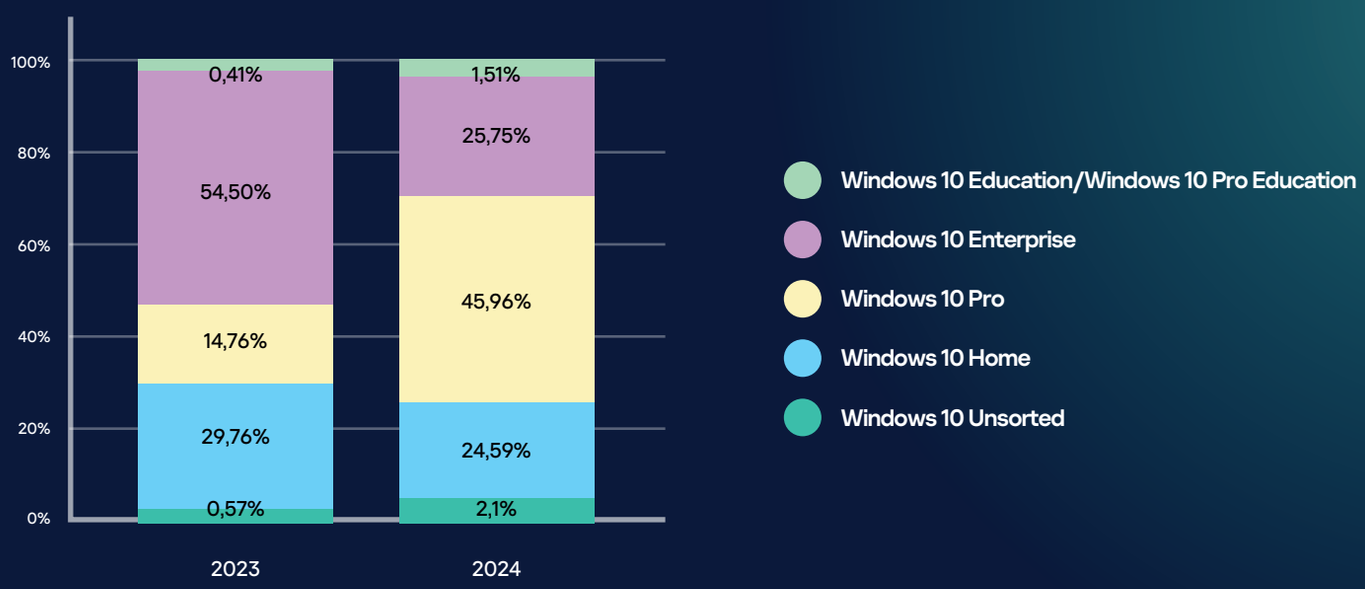
Os metadados dos logs dos infostealers indicam que a maioria dos dispositivos da área de trabalho comprometidos executa o Windows. Isso se deve principalmente ao uso generalizado deste sistema operacional e não a falhas de segurança. O Windows ainda é um dos sistemas operacionais mais utilizados em ambientes corporativos e domésticos.

Para identificar tendências e distinguir usuários corporativos de domésticos, analisamos as estatísticas das infecções por malware de roubo de dados relativas a diferentes versões do Windows. Conforme mencionado acima, elas revelam as tendências de popularidade dos SOs ao longo do tempo.

	2020	2021	2022	2023	2024
Windows 7	14,78%	8,42%	5,62%	3,67%	3,89%
Windows XP	0,02%	0,01%	0,04%	0,01%	0,00%
Windows 8.1	4,36%	2,88%	2,49%	1,96%	1,31%
Windows 8	0,62%	0,32%	0,28%	0,28%	0,17%
Windows 10	80,17%	88,41%	91,19%	92,63%	82,71%
Windows 11	0,10%	0,06%	0,21%	0,56%	↑ 11,81%
Windows Server 2012	0,08%	0,04%	0,04%	0,15%	0,01%
Windows Server 2016	0,02%	0,04%	0,05%	0,08%	0,01%
Windows Server 2019	0,10%	0,06%	0,05%	0,09%	0,03%
Windows Vista	0,03%	0,02%	0,04%	0,12%	0,00%
Windows Server	0,21%	0,14%	0,29%	0,63%	0,09%

Dispositivos infectados pela versão do SO do Windows, de 2020 a 2024

No ano de 2024, observamos o início de uma migração do Windows 10 para o Windows 11, sendo que as infecções deste último aumentaram de 0,56% em 2023 para 11,81% em 2024.



Versões do Windows 10: estatísticas de infecções por infostealers (de 2023 a 2024)

Em 2023, constatamos que um em cada dois dispositivos (55%) infectados por infostealers era corporativo. Essa conclusão se baseou em dados que mostraram que o maior número de infecções ocorreu no Windows 10 Enterprise. Em 2024, a quantidade de infecções no Windows 10 Enterprise diminuiu, o que possivelmente indica que as empresas estão acelerando a migração para um sistema operacional mais recente como parte dos seus esforços de fortalecimento da cibersegurança.

Os dados relativos a outras versões do Windows mostram que, embora o número de infecções na versão não licenciada do Windows 7 permaneça abaixo de 1%, esta plataforma apresentou um leve aumento nas infecções, provavelmente devido à falta ou à fragilidade de mecanismos de segurança nas versões não licenciadas.

	2020	2021	2022	2023	2024
Windows Seven Black Edition	0,09%	0,09%	0,07%	0,08%	0,20%
Windows 7	99,91%	99,91%	99,93%	99,92%	99,80%

Versões do Windows 7: estatísticas de infecções por infostealers (de 2020 a 2024)

Estatísticas do comprometimento de

Analisamos os dados de cartões bancários comprometidos relativos a 44% dos arquivos de log coletados em 2023 e 2024. Embora a proporção de cartões vazados seja muito inferior a 1% dos cartões em circulação no mundo em 2024, constatamos que 95% dos números de cartões bancários contidos nos arquivos de log vazados na dark web parecem ser tecnicamente válidos.

A análise também revelou que, em média, cada arquivo de log contém 0,071 cartões, o que representa aproximadamente um cartão para cada 14 arquivos de log.

Uma em cada 14 infecções por infostealer resulta no roubo de um cartão de crédito.

95%

dos números de cartões bancários contidos nos arquivos de log vazados na dark web parecem ser tecnicamente válidos.

Conclusão

O cenário de ameaças em constante evolução dos infostealers destaca a importância de medidas proativas de cibersegurança. Nosso estudo mostra que os cibercriminosos continuam aperfeiçoando os seus métodos; portanto, as estratégias de detecção e resposta devem ser otimizadas.

O que fazer se sua empresa for mencionada na dark web?

Caso um vazamento por infostealer seja detectado, os seguintes passos devem ser seguidos imediatamente:

- **Altere as senhas das contas comprometidas** e monitore as atividades suspeitas associadas a essas contas.
- **Notifique os usuários afetados** e solicite que eles façam verificações de segurança completas em todos os dispositivos, removendo qualquer malware detectado.
- **Seja proativo e monitore os mercados** da dark web para detectar contas comprometidas antes que elas causem riscos aos clientes e funcionários. Um guia detalhado sobre como configurar uma solução de monitoramento está disponível aqui.
- **Utilize o Kaspersky Digital Footprint Intelligence** para descobrir o que os cibercriminosos sabem sobre os ativos da sua empresa, identificar potenciais vetores de ataque e implementar medidas protetivas em tempo hábil.

Para aumentar a proteção e mitigar os riscos de infecções por infostealers, nós recomendamos:

- **Implementar um programa de conscientização em segurança** para funcionários, incluindo treinamentos frequentes e avaliações de desempenho.
- **Estabelecer uma política de senhas rígida** para todos os recursos corporativos a fim de reduzir vulnerabilidades relacionadas a credenciais.

Ao colocar essas medidas em prática, as organizações poderão fortalecer suas defesas contra os infostealers e minimizar o impacto de vazamentos potenciais, reduzindo, assim, o risco de serem vítimas de ciberameaças relacionadas a credenciais

Guia prático: o que fazer se as contas corporativas tiverem sido comprometidas

Tipo de conta	Recomendações

Conta de domínio do Active Directory
 	
Conta administrativa
 	
Conta de um sistema corporativo
	• Verifique a presença de um usuário com o nome de login especificado.
	• Caso o login tenha sido identificado, inicie os procedimentos de investigação e resposta. Certifique-se de incluir os seguintes passos:
	  ◦ Utilize o antivírus para fazer uma verificação completa nos dispositivos de usuários afetados e nas máquinas corporativas e remova todos os malwares detectados.
	  ◦ Redefina a senha da conta comprometida.
	  ◦ Analise os eventos de logs em busca de atividades suspeitas, como falhas ao fazer login, tentativas de escalar privilégios etc.
	• Ative a MFA (autenticação multifator) para todos os sistemas corporativos caso ela ainda não tenha sido implementada.
	• Fortaleça a política de senhas de acordo com as melhores práticas de segurança, quando aplicável.
	• Melhore a conscientização dos funcionários em cibersegurança para reduzir os riscos causados por infecções por malware.
	• Certifique-se de que a Endpoint Protection Platform (EPP) atual consiga detectar, mitigar e remover malware do tipo infostealer.

Tipo de conta	Recomendações
Conta de funcionário utilizada em recursos de terceiros	• Verifique a presença de um usuário com o nome de login especificado. • Informe ao funcionário afetado que a sua conta foi vazada (o que indica o seu comprometimento). • Solicite que o usuário utilize o antivírus para fazer uma verificação completa nos dispositivos afetados e nas máquinas corporativas e remova todos os malwares detectados. Recomende que o usuário altere suas senhas. • Melhore a conscientização dos funcionários em cibersegurança para reduzir os riscos causados por infecções por malware. • Proíba os usuários de usar e-mails corporativos para fazer autenticações em recursos externos. • Certifique-se de que a Endpoint Protection Platform (EPP) atual consiga detectar, mitigar e remover malware do tipo infostealer.

Conta de cliente	• Verifique se a conta mencionada existe. Determine se a conta pertence a um cliente ou a um funcionário.
	• Informe o usuário afetado sobre o comprometimento.
	• Inicie os procedimentos de investigação e resposta:
	  ◦ Exija a redefinição da senha do usuário afetado.
	  ◦ Verifique os logs de eventos/aplicativos em busca de acessos não autorizados ou atividades suspeitas.
	  ◦ Se for confirmado que a conta pertence a um cliente, solicite que ele realize uma verificação antivírus completa em seus dispositivos.
	  ◦ Se a conta pertencer a um funcionário, execute uma verificação antivírus completa nos dispositivos do usuário afetado e nos equipamentos corporativos e remova qualquer malware identificado.
	• Ative a MFA (autenticação multifator) para o aplicativo afetado caso ela ainda não tenha sido implementada.
	• Fortaleça a política de senhas de acordo com as melhores práticas de segurança, quando aplicável.
	• Melhore a conscientização de funcionários e clientes sobre cibersegurança para mitigar os riscos associados a infecções por malware.

www.kaspersky.com.br

https://dfi.kaspersky.com/br