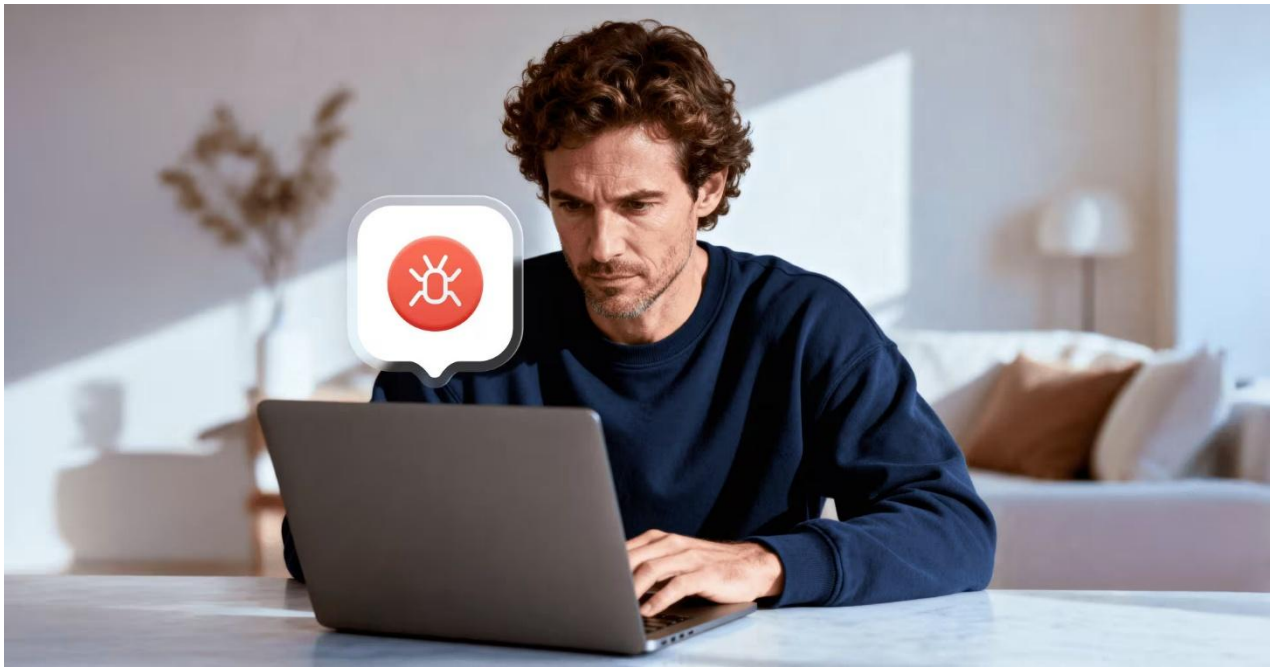
報道関係者各位

2026 年 5 月 27 日

サイバー攻撃の主戦場、企業サーバーから「個人デバイス」へ逆転
インフォスティーラーによるパスワード流出件数はデータ侵害の 18 倍超

個人向けセキュリティサービスを提供する NordVPN（本社：オランダ・アムステルダム、日本代表：小原拓郎）は、脅威インテリジェンスプラットフォーム NordStellar と共同で実施した、データ侵害と「インフォスティーラー（情報窃取型マルウェア）」の動向比較調査の結果を発表しました。
本調査によると、企業や組織のデータベースを標的としたデータ侵害の件数は 2024 年から 2025 年にかけて 36%減少した一方、感染端末から認証情報を密かに収集する「インフォスティーラー（情報窃取型マルウェア）」の感染ログ数は同期間に 35%増加しました。流出パスワード数ではインフォスティーラー経由がデータ侵害経由の 18 倍以上に達しており、サイバー攻撃の主戦場が企業サーバーから個人デバイスへと移行しつつある実態が明らかになりました。



調査概要
本調査は、NordVPN と脅威インテリジェンスプラットフォーム NordStellar が、公開された侵害データベース件数とインフォスティーラー感染ログ数を比較・分析したものです。

調査名称：データ侵害とインフォスティーラー動向比較調査
調査機関：NordVPN・NordStellar
調査期間：2024 年～2025 年
調査方法：公開された侵害データベース件数と、インフォスティーラー感染ログ数の収集・分析
分析内容：データ侵害件数、インフォスティーラー感染ログ数、流出パスワード数、流出メールアドレス数の比較

■ 調査結果
本調査では以下の数値が確認されました。

＜攻撃トレンド（前年比）＞

指標	2024 年	2025 年	増減
侵害データベース件数	4,804 件	3,069 件	36%減
インフォスティーラー感染ログ数	1,950 万件	2,600 万件超	35%増

＜流出規模の比較（手口別）＞

指標	データ侵害経由	インフォスティーラー経由	差・傾向
流出パスワード数	約 3,400 万件	約 6 億 2,400 万件	約 18 倍
流出メールアドレス数	約 5 億 4,200 万件	約 3 億 8,000 万件	侵害が上回るが差は縮小傾向

■ インフォスティーラーが増加する背景

データ侵害件数の減少は、一見するとサイバーセキュリティ環境の改善を示すように見えます。しかし同期間にインフォスティーラーの感染ログが大幅に増加していることは、攻撃者が標的と手法を変えたことを示しています。

この背景には、攻撃者の「費用対効果」重視への転換があります。Cloudflare が発表した「2026 年脅威レポート」は、現代の攻撃者が高度さよりも量と効率を優先する傾向にあると指摘しており、攻撃の成果と労力の比率を意味する「効果測定（MOE：Measure of Effectiveness）」という概念でその行動様式を説明しています。企業サーバーへの正面突破には高価なゼロデイ脆弱性の悪用が必要となる一方、インフォスティーラーで盗んだ認証情報を使えば、はるかに低コストで同等以上の情報を入手できます。企業側のセキュリティ対策が強化されるほど、攻撃者にとっては個人デバイスを経由した侵入の方が「割に合う」手段となっているのです。

NordStellar のシニア脅威インテリジェンスリサーチャー、マンタス・サベキスは、インフォスティーラー1 件の感染で、保存されたパスワード、クッキー、自動入力データ、セッショントークンまで密かに窃取することができ、侵害ほど派手ではないが、個人への被害は同様に深刻になっていると述べています。

■　調査が示す課題──気づけない被害の深刻さ

こうした被害は「気づきにくい」点でも深刻です。データ侵害が発生した場合、被害を受けた企業はユーザーへの通知義務を負い、パスワードリセットなどの対応措置が速やかに講じられます。一方で、インフォスティーラーによる個人デバイスの感染には、こうした通知の仕組みが存在しません。本人が感染に気づかないまま盗み出された認証情報がダークウェブ上に流出し、アカウントの不正利用や SNS アカウントの乗っ取りが発生して初めて被害が判明するケースもあります。

データ侵害件数の減少だけをもってサイバーリスクが低下したと判断することは危険であり、個人端末を起点とした認証情報の窃取にも注意を向ける必要があります。

■インフォスティーラーから身を守るために今すぐできる 3 つの対策

①　ブラウザにパスワードを保存しない

便利な機能ですが、インフォスティーラーが最初に狙う場所の一つです。専用のパスワードマネージャーへ移し、ブラウザの自動保存はオフにしてください。

②　主要アカウントで多要素認証（2FA）を有効にする

パスワードが盗まれても、二要素認証が設定されていれば不正ログインを防ぐ追加の壁になります。

③　非公式サイトからのダウンロードを避け、OS・アプリ・マルウェア対策を最新に保つ

海賊版ソフトや出所不明な無料ツールには、インフォスティーラーが仕込まれていることがあります。公式サイトや正規ストアから入手し、端末を最新の状態に保つことが重要です。

■NordVPN 最高技術責任者（CTO） マリユス・ブリエディスのコメント

「データ侵害は、多くの人にとって比較的イメージしやすいサイバーリスクです。一方で、インフォスティーラーは、感染した端末からパスワードや Cookie、セッショントークンなどを密かに収集するにもかかわらず、まだ十分に認知されていません。攻撃者にとって、企業のシステムへ不正に侵入するよりも、盗み出した認証情報を使って正規ユーザーとしてログインする方が、低コストで成功しやすい手口になっています。デバイスが情報を便利に記憶すればするほど、侵害された際に盗まれる情報も増えてしまいます。まずは、ブラウザにパスワードを保存しないこと、主要なアカウントで多要素認証を有効にすること、非公式サイトからのソフトウェアやファイルのダウンロードを避けることが重要です。インフォスティーラーは、存在を知らなければ対策が遅れやすい脅威です。日常的に使う端末こそ、認証情報の管理を見直す必要があります。」

■ NordVPN について

NordVPN は、世界中で何百万人ものユーザーをもつ先進的な VPN サービスプロバイダーです。8,200 台以上のサーバーを世界 135 カ国 209 都市で提供し、専用 IP や Double VPN、Onion Over VPN サーバーなど、多彩な機能を備え、トラッキングなしでオンラインプライバシーを強化します。主要機能の一つである「脅威対策 Pro」は、悪質なウェブサイトやトラッカー、広告のブロックに加え、マルウェアのスキャンが可能です。さらに、最新の製品であるグローバル eSIM サービス「Saily」を展開しています。「Saily」は海外旅行者向けに設計されており、現地で SIM カードを購入する必要がなく、簡単にデータ通信が利用可能です。

【会社概要】

会社名：NordVPN

本社：Fred. Roeskestraat 115 1076 EE Amsterdam, Netherlands

日本代表：小原拓郎

NordVPN ウェブサイト：https://nordvpn.com/ja/

VPN について：https://nordvpn.com/ja/what-is-a-vpn/

ナショナル・プライバシー・テスト（National Privacy Test）について：https://nationalprivacytest.org/jp