報道関係者各位

2026 年 3 月 10 日

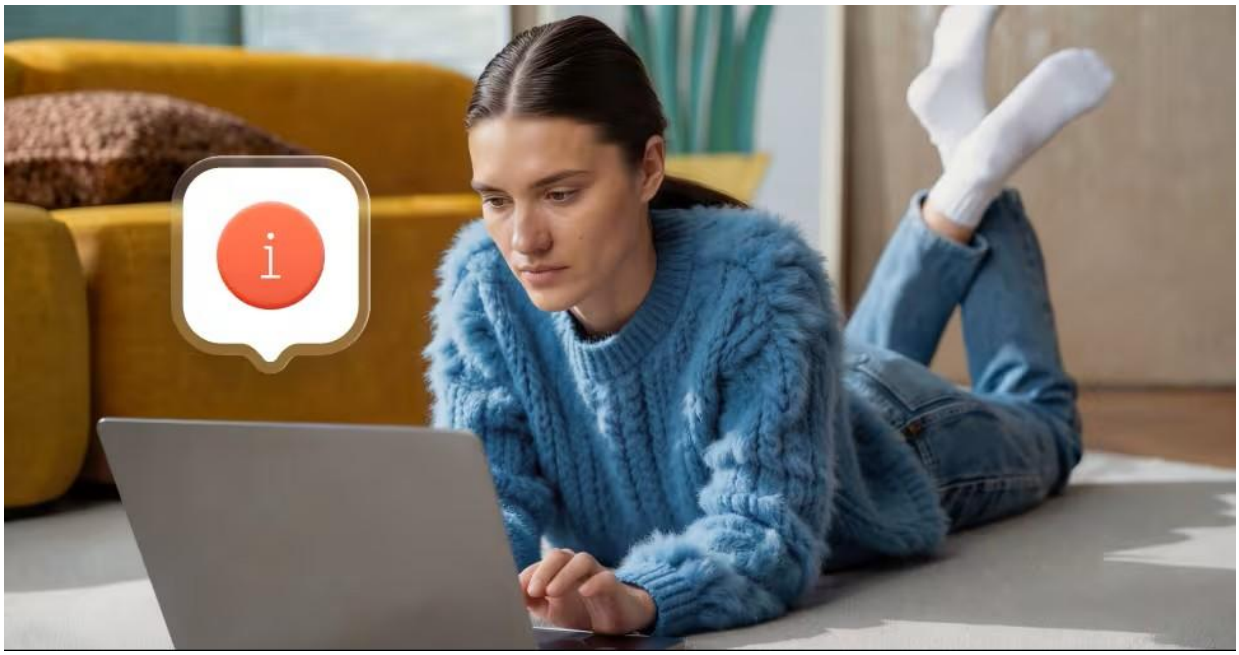
子どものゲームやネット通販が「情報漏洩」の入り口に?

NordVPN が世界 5 億件のデータから見えたマルウェア被害の実態を発表

～SNS ユーザーやゲーマーが最多被害層、家族の PC から情報漏洩のリスクも～

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、同社が運営する脅威エクスポージャー管理プラットフォーム「NordStellar」が 2025 年に実施した、情報窃取型マルウェア「インフォスティーラー（Infostealer）」による被害実態に関する調査の結果を発表しました。

調査の結果、インターネット通販・SNS・子ども向けオンラインゲームなど、現代の家庭に広く普及しているサービスが、サイバー犯罪の主要な標的となっていることが判明しました。なかでも深刻なのが、不審なファイルのダウンロードをきっかけに「家族共有の PC」全体を感染し、決済情報などが抜き取られるリスクです。本調査は、家庭内におけるセキュリティ対策の重要性を改めて示す結果となりました。



調査概要

本調査は、脅威エクスポージャー管理プラットフォーム「NordStellar」の研究チームが、世界中のインフォスティーラーのログデータを統計的に分析したものです。

- **調査対象**：インフォスティーラーのログ内で最も頻繁に検出された上位 1 万件のドメイン
- **分析対象データ**：世界中で特定された約 5 億件のインフォスティーラーログ
- **調査期間**：2025 年 1 月 1 日～2025 年 12 月 31 日

■「インフォスティーラー」とは？その脅威と標的となる 3 つのユーザー層を解説

インフォスティーラーは、感染したデバイスからパスワード、Cookie、金融データなどの機密情報を密かに収集し、サイバー犯罪者に送信するように設計されたマルウェアの一種です。現在、何百種類もの変種が存在し、「マルウェア・アズ・ア・サービス（MaaS）」として犯罪グループ間で取引されています。

今回の調査では、特定された被害者の約 99%が Windows ユーザーであることがわかりました。これは、市場シェアが大きく、標的とするブラウザやゲームに広く対応している Windows 環境が、攻撃者にとって大規模な攻撃を展開しやすいためです。さらに、被害者を「閲覧サイト」や「インストール済みアプリ」で分類した結果、以下の 3 つのユーザー層が標的になっている実態が明らかになりました。

1. ライフスタイル重視の一般インターネットユーザー（最被害層）

最も被害が多いのは、利便性を重視し、日常的に Web サービスを利用する層です。中でも SNS 利用者が最多となり、Facebook、Instagram、X（旧 Twitter）などの SNS 関連で流出された情報件数は約 6,500 万件にのぼり、Netflix などの動画配信サービス関連は約 2,800 万件、そして Amazon などのショッピングサイトなどの EC では約 2,600 万件の流出が確認されています。 ブラウザのセッション情報が盗まれると、パスワードを入力せずにメールや決済サービスへのアクセスが可能になるため、被害が拡大する大きな要因になります。

2. ゲームプラットフォームを利用するゲームユーザー

2 番目に被害が多い層からは、5,300 万件以上の流出が確認されました。PC にゲームランチャーがインストールされ、Steam、Twitch などの主要プラットフォームや、フォートナイト、マインクラフトなどの人気タイトルの利用履歴が確認されています。 主な感染経路は、クラック版（不正改造）ゲーム、チートツール、非公式ランチャーなどの「危険なダウンロード」です。利用者の中では若者も多いため、1 つの不審なファイルが家族共用の PC 全体を感染させ、アカウントに紐付く決済情報などが盗まれるリスクが高まります。

3. 開発・管理ツールを利用するシステム管理者

一般ユーザーとは異なる利用環境を持つ、システム管理者からも、約 2,700 万件の流出が確認されました。企業向け ID 管理ポータル、クラウドプラットフォーム、Zoom などの Web 会議、ルーター管理画面、コード管理ツールなどが標的となっています。エンジニアリングやシステム管理に使用される PC が感染した場合、個人の被害にとどまらず、社内システムや開発環境へ侵入される「サプライチェーン攻撃」へと発展する危険性があります。

■ NordVPN 最高技術責任者（CTO） マリユス・ブリエディスが推奨、インフォスティーラー被害を防ぐ 3 つの防御策

① すべての入口となる「重要アカウント」を最優先で保護する

あらゆるサービスへのログインの鍵となる、主要なメールアドレスや ID 管理用アカウントのセキュリティ対策強化が必要です。これらのアカウントで多要素認証（MFA）を有効化し、パスキー技術を利用した上で、銀行、オンラインショッピング、業務関連のサービスなどのアカウントも順次セキュリティ設定を強化することを推奨します。

② ブラウザの「保存データ」の見直しと、オペレーティングシステムの最新版アップデートを行う

ブラウザの使い方を定期的に見直すことを推奨します。保存されているパスワードを確認して不要なものは削除し、見覚えのないアクティブなセッションからは直ちにログアウトします。また、古いバージョンの OS やブラウザは攻撃者に侵入されやすく、感染後の完全な復旧も困難になるため、常に最新の状態を維持することが必要です。

③ 非公式なダウンロードや「うますぎる話」への警戒を徹底する
インターネット上の無料ツールなど、「うますぎる話」には十分な注意が必要です。セキュリティ保護機能の無効化を求めてきたり、システムの警告を無視させたりするソフトウェア、非公式のランチャーやクラック版（不正改造）ソフトのインストールは、マルウェア感染の直接的な原因となります。

■ NordVPN 最高技術責任者（CTO） マリユス・ブリエディスのコメント
「今回、マルウェア感染に関連するアプリや Web サイトを分析した結果、3 つの明確に狙われやすいユーザー層が浮かび上がりました。いずれも現代のインターネット利用においては一般的な行動であり、IT の専門家であっても被害者になり得ます。インフォスティーラーは特定のユーザー層ではなく、予測可能な行動を標的にしています。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。万が一デバイスが侵害された場合でも、一度に漏洩する情報を最小限に抑えることが、有効な防御策となります。」

■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 127 カ国 165 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/