報道関係者各位

2024 年 10 月 21 日

# 盗まれたカード情報はダークウェブで拡散！？
# NordVPN が 60 万件の盗難カードデータをもとに調査を実施
## ～99%のケースで、カード情報に加えて個人情報が流出していることが明らかに～

個人向けセキュリティサービスを展開する NordVPN（本社：Amsterdam, Netherlands、日本代表：小原拓郎）は、自社が運営する情報漏えい管理プラットフォーム「NordStellar」を通じて、ダークウェブ上で取引されるカード情報や、主に使用されているマルウェアの種類、影響を受けたオペレーティングシステムについて調査を実施しました。

**■調査結果**

①マルウェアの種類は多様化し、特に「RedLine」が多く使用されていることが判明

②60%の決済カード情報の漏えいが「RedLine」によるものであることが明らかに

③99%のケースで、カード情報に加えて個人情報が流出

④盗まれたクレジットカード情報の大半が米国のユーザーに関連

⑤盗まれた決済用カードのうち、54%が Visa カード

⑥数時間以内に悪用されるケースが多いことが明らかに

**【調査概要】**

調査対象 ：60 万枚の盗難カードデータ

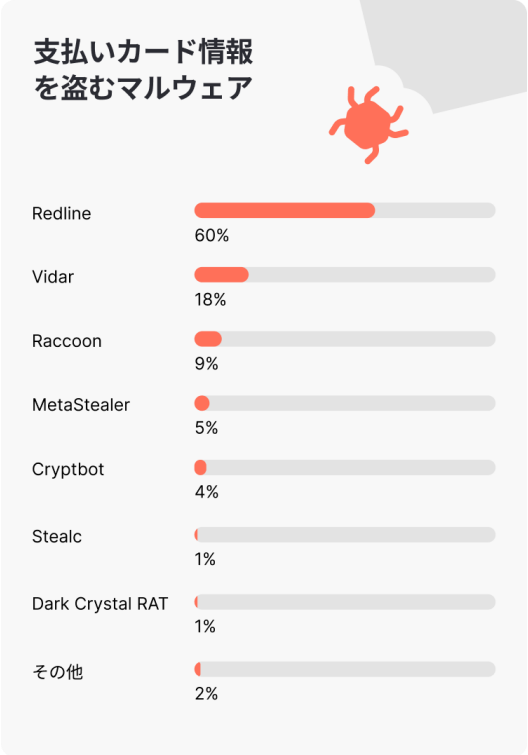
調査手法：NordStellar は、ハッカーが Telegram 上で販売している盗難カードデータを分析し、盗難されたカード情報をハッカーがどのように入手したかについて調査しました。具体的には、カードが盗難された時期、カードのプロバイダー、ペイメントカードと共に漏洩したデータ、使用されたマルウェアの種類、盗難が発生した国、ハッカーの標的となったオペレーティングシステム（OS）など、さまざまなデータを検証しました。

調査時期：2024 年 4 月

昨今、サイバー犯罪者が盗んだ決済カード情報をダークウェブ上で売買する状況が拡大しています。2023 年には、世界で 5,100 万枚以上のカード情報が流出し、消費者の経済的安全が脅かされました。この深刻な状況を受け、NordVPN は、生活者が日常的に直面するマルウェアの脅威を啓発するべく、情報漏えい管理プラットフォーム「NordStellar」を通じて、マルウェアに関する調査を実施。60 万件の盗難カードデータを分析し、カード情報がどのように取引され、被害を拡大させているのかを検証しました。

**①マルウェアの種類は多様化 特に「RedLine」が多く使用されていることが判明**

サイバー犯罪者が使用する「サービスとしてのマルウェア」やサブスクリプション型のマルウェアツールは、情報を盗む手段として普及していることが検証により明らかになりました。これらのツールは月額 150 ドル程度でダークウェブ上で販売され、利用者には豊富なガイダンスやフォーラムも提供されています。また、マルウェアの種類は多様化しており、特に「RedLine」が多く使用されていることがわかりました。

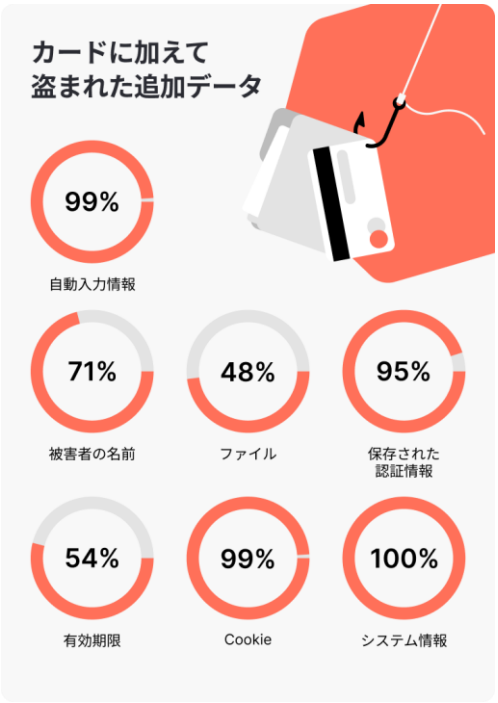



**②60%の決済カード情報の漏えいが「RedLine」によるものであることが明らかに**

「RedLine」は 2020 年 3 月に登場して以来、サイバー犯罪者の間で人気のある情報窃取型マルウェアとして広まりました。本調査によると、漏えいした決済カード情報の 60%が「RedLine」によるものであることが判明しています。「RedLine」は 100 ドルという手頃な価格に加え、効果の高さや配信の容易さ、そして常に進化し続け、検知されにくいことから、利用されやすく危険とされています。さらに、初心者向けのサポートが専用の Telegram チャンネルを通じて提供されていることも特徴です。

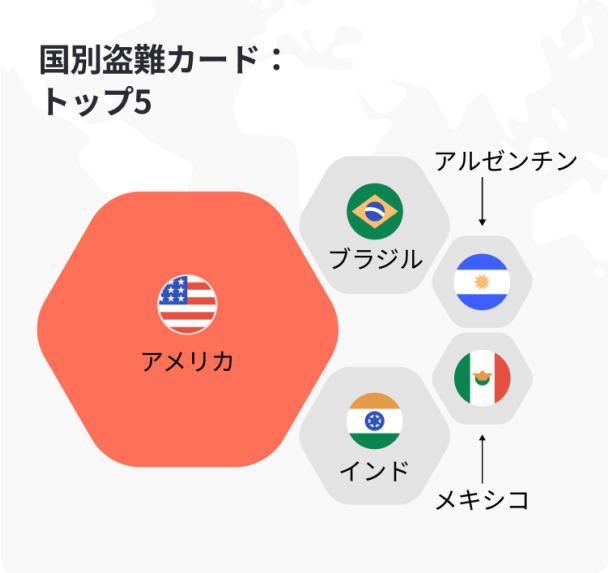
**③99%のケースで、カード情報に加えて個人情報が流出**

マルウェアが決済用カード情報だけでなく、被害者の名前やコンピューター内のファイル、保存された認証情報も漏えいさせることが判明。99%のケースで、カード情報に加えて個人情報が流出しています。これらの膨大なデータは、サイバー犯罪者に個人情報の盗難、オンライン詐欺、恐喝といったサイバー攻撃の機会を提供し、被害のリスクをさらに拡大させる可能性があります。



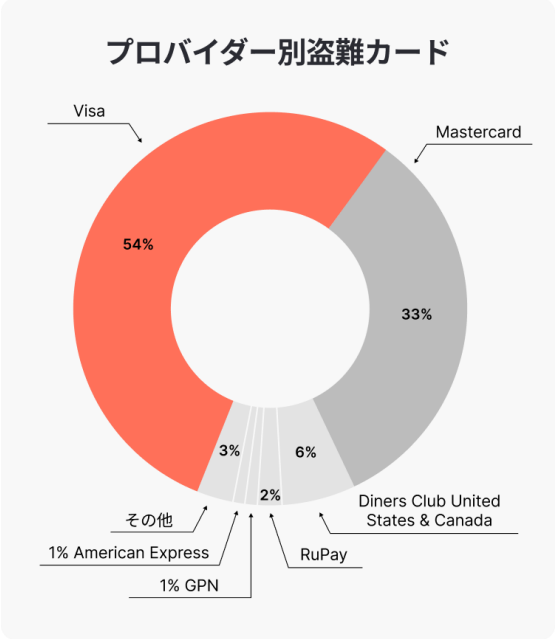
**④盗まれたクレジットカード情報の大半が米国のユーザーに関連**

アメリカでは決済カード情報の漏えいが多発し、盗まれたクレジットカードの大半が米国ユーザーのものであることが確認されました。さらに、ブラジル、インド、メキシコ、アルゼンチンなどの国々でも支払い情報の盗難が深刻な問題となっている上に、サイバー犯罪による個人情報の流出が広範囲に及んでいます。これにより、ユーザーへの経済的被害が拡大し、国際的に重大な影響を及ぼしていることが明らかになりました。




**⑤盗まれた決済用カードのうち、54%が Visa カード**

盗まれた決済用カードのうち、54%が Visa カード、33%が Mastercard であることが明らかになりました。
どのカードでも盗難リスクはありますが、特に利用者が多いブランドほど標的になりやすく、被害が拡大する傾向があります。
この調査結果は、ユーザー数の多い発行会社のカードがサイバー犯罪者に狙われやすいことを示しており、対策の強化が求められています。




**⑥数時間以内に悪用されるケースが多いことが明らかに**

盗まれた決済カード情報は、即座に販売され、数時間以内に悪用されるケースが多いことが確認されました。犯罪者は、盗んだ情報を自身で利用するのではなく、ダークウェブや Telegram などのチャネルを通じて売買しています。
特に、カード情報に加えて個人情報が含まれている場合、その需要が高まり、高額で取引されることが多いです。
こうしたサイバー犯罪のエコシステムにより、盗難データの悪用が急速に進んでいます。

**■NordVPN が提案するマルウェアからの保護方法について**

- フィッシングを見分ける方法を身に付ける

フィッシングメールやテキストは、マルウェア感染の原因となることが多いです。フィッシングの一般的な兆候を知ることが重要です。

- 強力なパスワードを使用する

長く、複雑なパスワードを使用することでアカウントを保護できます。簡単で安全なパスワード管理には、NordPass の使用をご検討ください。

NordPass について：https://nordpass.com/

- 多要素認証（MFA）でアカウントを保護する

アカウントに多要素認証（MFA）を設定することで、セキュリティの層が追加されます。これは第三者があなたの認証情報を入手した場合に非常に役立ちます。

- 怪しいソフトウェアやアプリのダウンロードを避ける

非公式なソースからソフトウェア、アプリをダウンロードすることは避け、代わりにアプリストアや公式ウェブサイトからダウンロードしてください。

- NordVPN のウイルス対策ツール「脅威対策 Pro」の導入

危険なサイトをブロックし、ダウンロード中にファイルをスキャンしてマルウェア感染を防ぎます。

「脅威対策 Pro」について：https://nordvpn.com/ja/features/threat-protection/

- ダークウェブ監視ツールを使用

ダークウェブ監視ツールは、ダークウェブで認証情報を継続的にスキャンし、あなたのメールアドレスが流出データベースに現れた場合にアラートを送信します。

**■NordVPN について**

NordVPN は、世界中で何百万人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。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、最新製品グローバル eSIM サービス「Saily」を展開し、6,400 台以上のサーバーを 111 カ国で提供しています。

【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/