Press Release

Norton PR 事務局
2024 年 12 月

Gen 、2024 年第 3 四半期脅威レポートを発表

Lumma Stealer の急速な拡大により情報窃取のリスク増加
日本はテクニカルサポート詐欺の標的として世界で 1 位は変わらず

デジタルセキュリティのグローバルリーダーである Gen は、2024 年第 2 四半期の脅威レポートを発表しました。本レポートは今まで Avast で公開されていた脅威レポートに代わる、Avast、Norton、AVG、Avira、LifeLock を含む多様なサイバーセキュリティブランドの脅威検知や測定結果を統合した新たなレポートです。

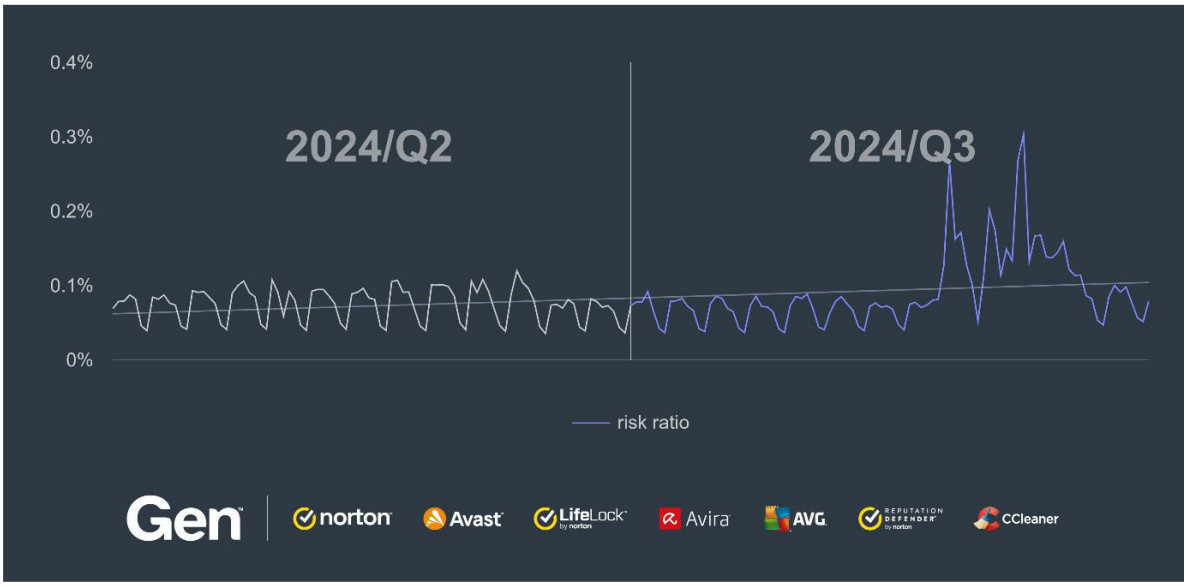
本レポートによると、従来のマルウェアは依然として強大な力を持っているだけでなく、ますます危険度が高くなっていることがわかりました。また、詐欺の脅威は若干減少したものの、不正広告、ランサムウェア、ドロップ型不正プログラム、情報窃取型不正プログラムは急増しました。また最も大きな変化の一つとして、前四半期比で 614%という驚異的な増加率を記録した「自己感染型詐欺」が見られました。

レポートの主なトピックは以下をご覧ください。

情報窃取ツール Lumma Stealer の拡大

情報窃取ツールは、被害者のデバイスから貴重な情報を盗むために使用されます。これには、保存されているログイン情報、暗号通貨の秘密鍵、ブラウザのセッションやクッキー、パスワード、さらにはプライベートな文書などが含まれます。最近、特に「Lumma Stealer」という高度な情報窃取ツールが急速に拡大しており、世界中で広まっています。このツールは、情報窃取マルウェアのシェアを 1154%も増加させ、今後さらに被害が拡大する可能性があります。

2024 年第 3 四半期には、Lumma Stealer によって配信された大規模なキャンペーンにより、情報窃取に感染するリスクが 39%増加しました。2024 年第 3 四半期における情報窃取型不正プログラムのユーザーベースに対する日次リスク比率が、日本は 128%と世界で 2 番目を記録しました。



＜本件に関するお問い合わせ先
Gen PR 事務局（株式会社プラチナム内） 担当：石間、杉原、加藤、宮下
TEL：03-5572-6071（PR 事務局）／Mail：norton-pr@vectorinc.co.jp

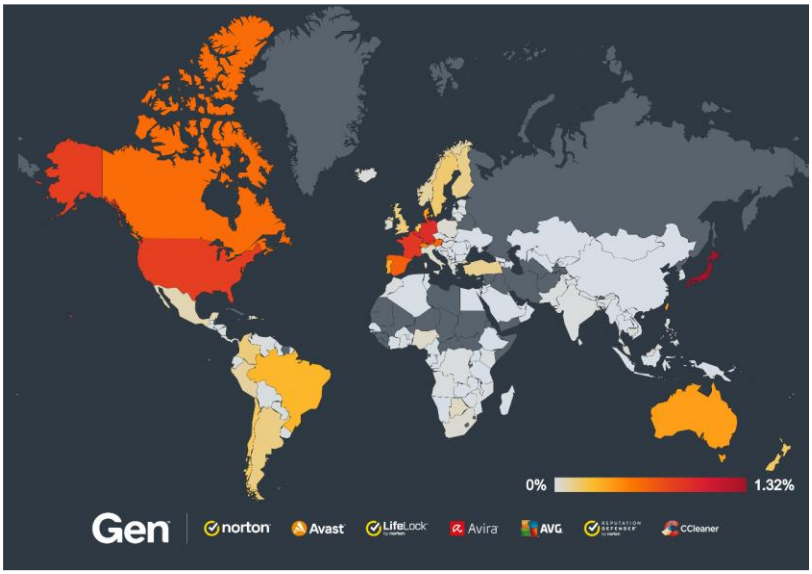
表）2024 年第 3 四半期における情報窃盗犯に関するユーザーベースのリスク比率

国名	リスク比率
フランス	135%
日本	128%
スロバキア	127%
カナダ	48%
スペイン	34%
ブラジル	27%
アメリカ	22%

テクニカルサポート詐欺の標的は変わらず日本が 1 位

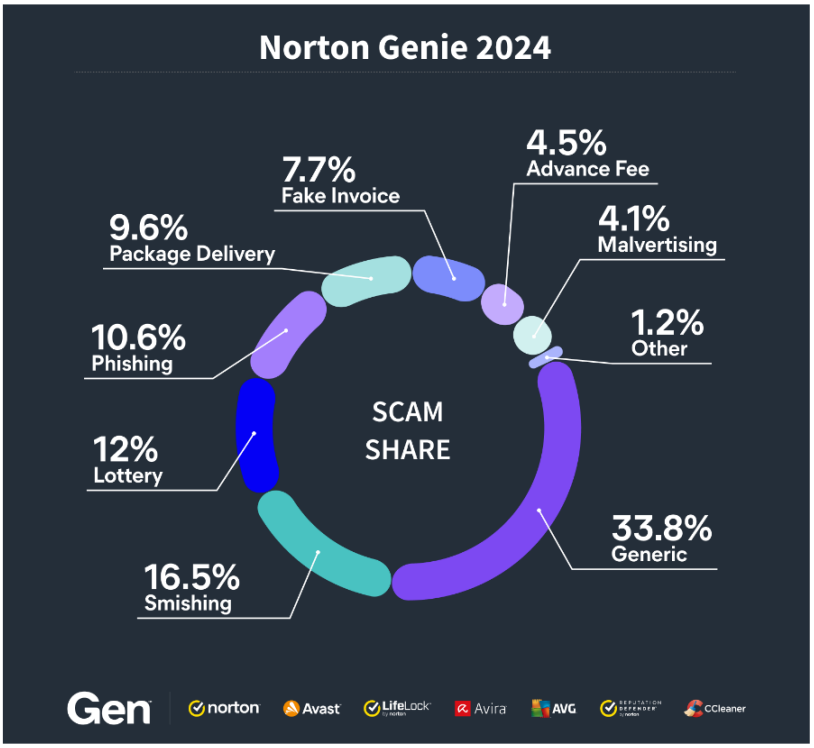
テクニカルサポート詐欺の脅威は、正規のテクニカルサポート担当者を装った詐欺師が被害者のデバイスへのリモートアクセスを試みたり、クレジットカードや銀行口座の詳細情報などの機密性の高い個人情報を取得しようとしたりするものです。

日本（60%）とドイツ（33%）では、前の四半期と比べてテクニカルサポート詐欺のリスクが大幅に減少しました。しかし、これらの国々は依然として詐欺の蔓延率が最も高い国のひとつです。日本はリスク比率が 1.32%で、減少しているものの、依然として世界でトップを維持しており、高い脅威レベルが続いていることを示しています。



2024 年にノートン・ジーニーで確認された主な脅威

Norton Genie（詐欺検出ツール）は、2024 年現在までに検出した脅威を、テレメトリーデータに基づいて発表しました。サイバー犯罪者たちは進化し続けており、消費者を騙す新しい手口を次々に見つけています。これらの脅威は、システムの脆弱性や人間の心理を悪用するなど、さまざまな方法で現れます。以下は、Norton Genie が検出した中で最も多く見られた詐欺の種類についての詳細です。



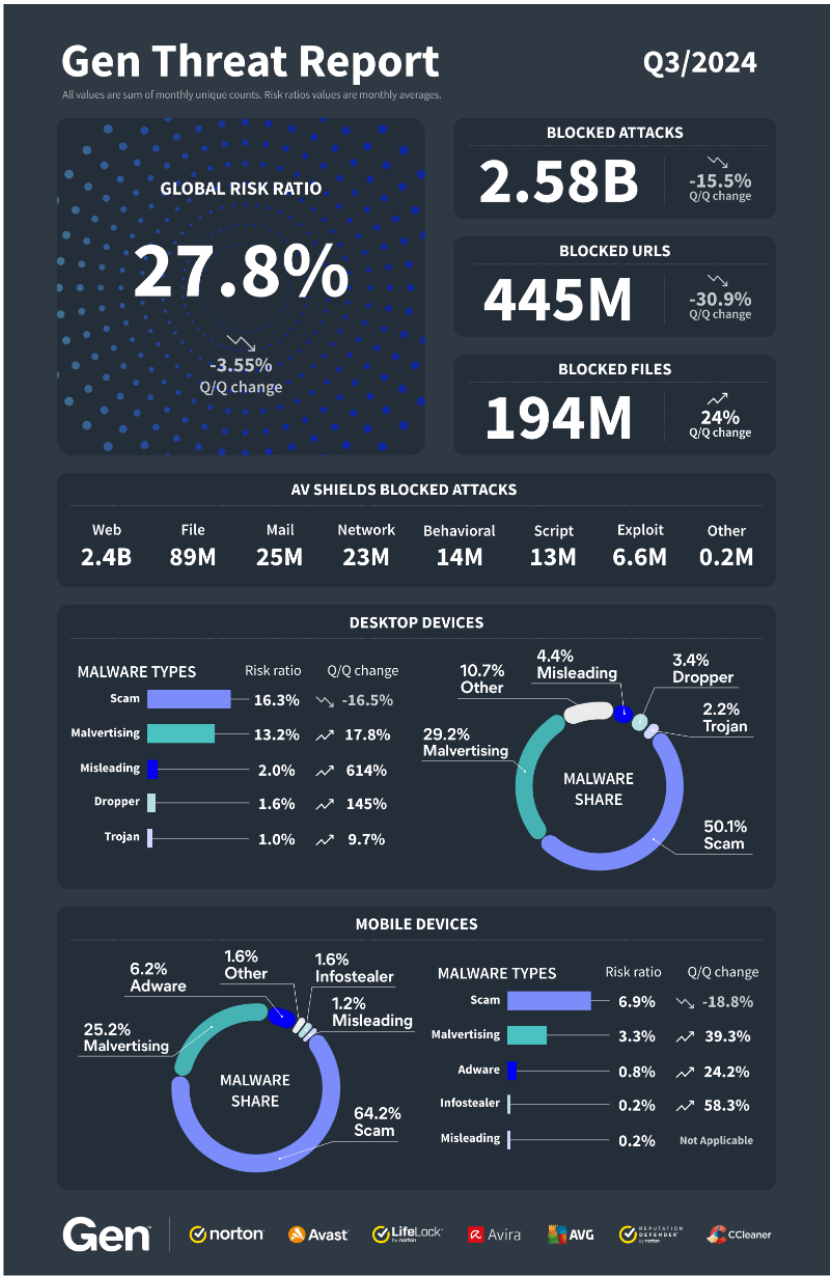
バンカー詐欺が増加する一方、日本で MoqHao のリーチは半減

バンカーは、銀行口座の詳細、暗号通貨のウォレット、即時決済を標的とし、金銭を搾取する目的で設計された高度なモバイルマルウェアです。一般的にフィッシングメッセージや偽のウェブサイトを通じて配布されるバンカーは、スマートフォンのアクセシビリティ（操作）機能を悪用し、被害者のデバイスを乗っ取ります。バンカーがインストールされ有効化されると、SMS メッセージを監視し、ログイン情報を盗むために偽の銀行サイトを表示することがあります。

2024 年第 3 四半期には、バンカーも勢力を増し、保護されたユーザーが大幅に増加し、新たな亜種がモバイルエコシステムに参入しました。ブラジルで、他のバンカーのソースコードを再利用し、Telegram ボットを通じて被害者のデータを外部に送る「ロシナンテ・バンカー」が現れました。

前述の通り、Google サービスアプリを装った TrickMo の新しいバージョンが登場し、被害者のデータを盗んで、一般にアクセス可能な C&C サーバーに保存しています。また、手動で操作されるリモートアクセス型バンカー「BingoMod」はイタリアを標的にし、攻撃後に被害者のデバイスを消去します。最後に、Octo バンカーのソースコードが流出した後、マルウェア開発者は難読化を施し、より安定したリモート操作機能を持つ「Octo2」をリリースしました。

今期、Coper バンカーは影響範囲を 2 倍以上拡大し、バンカー分野で第 1 位となりました。RewardSteal は 2 位に浮上し、モバイルユーザーへの影響力を維持しています。Ermac と Cerberus がそれに続き、両者とも 2024 年第 3 四半期に保護されたユーザー数が増加しました。一方、2024 年第 2 四半期の脅威レポートで言及された MoqHao バンカーは、日本と韓国でのリーチがほぼ半減し、減少傾向にあります。



より詳細な情報については、レポート（英語）をご覧ください：
https://investor.gendigital.com/news/news-details/2024/Gen-Q3-Threat-Report-Millions-Fooled-by-Scam-Yourself-Attacks/default.aspx

Gen について

Gen™ (NASDAQ: GEN) は、信頼性の高いサイバーセキュリティブランドであるノートン、アバスト、ライフロック、Avira、AVG、ReputationDefender、CCleaner を通じてデジタルの自由を推進するグローバル企業です。Gen の消費者向けブランドファミリーは、デジタル世代の安全の確保を第一に考えています。現在、Gen は、人々が今日、そして将来にわたってデジタルライフを安全に、プライバシーを保護しながら、自信を持って送れるようサポートしています。Gen は、サイバーセキュリティ、オンラインプライバシー、ID 保護の分野において、受賞歴のある製品とサービスを 150 か国以上、約 5 億人のユーザーに提供しています。詳細は、GenDigital.com をご覧ください。