2025 年 6 月 23 日
デジタルアーツ株式会社

PRESS RELEASE

【セキュリティレポート】ランサムウェア侵入原因の 34%が認証情報 添付ファイル、URL のマルウェア分類ではインフォスティーラーが上位（独自調査）

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下デジタルアーツ、証券コード 2326）は、情報を暗号化、窃取し、その見返りに金銭を要求するランサムウェア被害にあった組織の公表内容をもとに、ランサムウェアの侵入原因の調査、及びメール添付ファイル、URL のマルウェア種別の調査を行い、インフォスティーラーの実態について分析しました。

ランサムウェアの侵入原因を調査

2025 年 3 月に警察庁が公開した調査レポート、「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」※1では、感染経路（侵入経路）の約 9 割が「VPN 機器」と「リモートデスクトップ」とされていました。

この調査を受け、デジタルアーツでは、ランサムウェアによる被害に遭った組織の公表内容をもとに、攻撃者が VPN やリモートデスクトップ用の機器に対して侵入が可能になった原因について（なぜ侵入ができたのか）調査を行った結果、脆弱性や設定不備だけでなく、認証情報をもとに侵入しているケースが一定数存在することがわかりました。

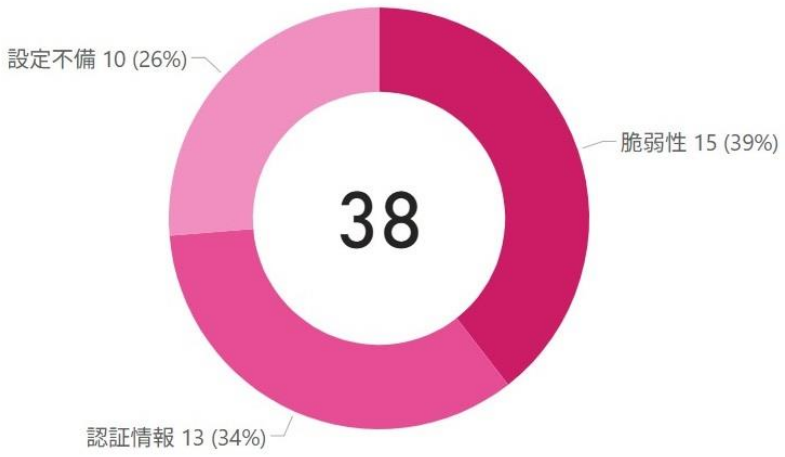
<調査概要>

対象：自組織が直接的な被害にあったランサムウェアインシデント
（業務委託先が侵害され、委託元から預けていたデータに影響を受けたが、委託元への侵害はなかった事例は含まない）

期間：2024 年 1 月～2025 年 5 月（インシデントの初公表日。分類は最新情報を確認。）

総数：126 件／有効回答：38 件（侵入原因に言及があったもの）

国内ランサムウェアインシデントの侵入原因



図において、「脆弱性」はソフトウェアやネットワーク接続機器などの脆弱性をつくもの、「認証情報」は従業員アカウントや管理者アカウントの悪用など、「設定不備」はアクセス制限がなく、ブルートフォースを許して侵入されたものなどを指します。

※1‥警視庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢について」
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/info_security.html

認証情報の流出はなぜ起こる？インフォスティーラーが関係か

認証情報をもとに、攻撃者の侵入を許しているという事実がわかりましたが、「認証情報がそもそもなぜ流出したのか」を探ることは非常に困難です。認証情報が流出する要因としては以下が考えられます。

・フィッシングサイト経由で窃取された
・インフォスティーラーなどのマルウェアにより窃取された

フィッシングというと個人を標的としているイメージが強いものの、業務用の認証情報を狙う攻撃もあります。実際に、認証情報を同期する設定にしていた個人アカウントが窃取された結果、同期していた業務利用の認証情報も窃取され、組織内に侵入されたという事例もあります。

インフォスティーラーの台頭、証券口座不正アクセスの被害拡大。

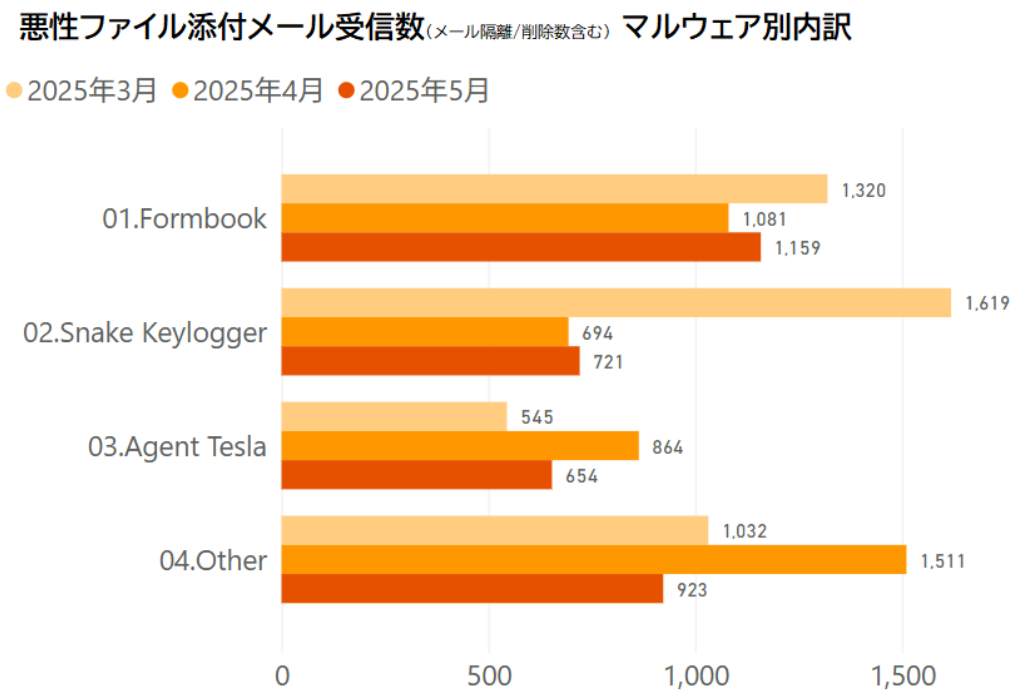
「インフォスティーラー（InfoStealer、情報窃取マルウェア）」は、ユーザーの個人情報や機密データを、Web ブラウザーやメールクライアントなどから不正に収集するマルウェアの一種です。ID・パスワードの認証情報に加え、銀行口座情報、クレジットカード番号、電子メールの内容などの情報が、感染した端末から窃取されます。

近年、ネット証券口座などへの不正アクセスが大きな問題となっていますが、その際に用いられる認証情報はインフォスティーラーにより窃取された可能性も指摘されており、身近に迫った脅威と言えます。

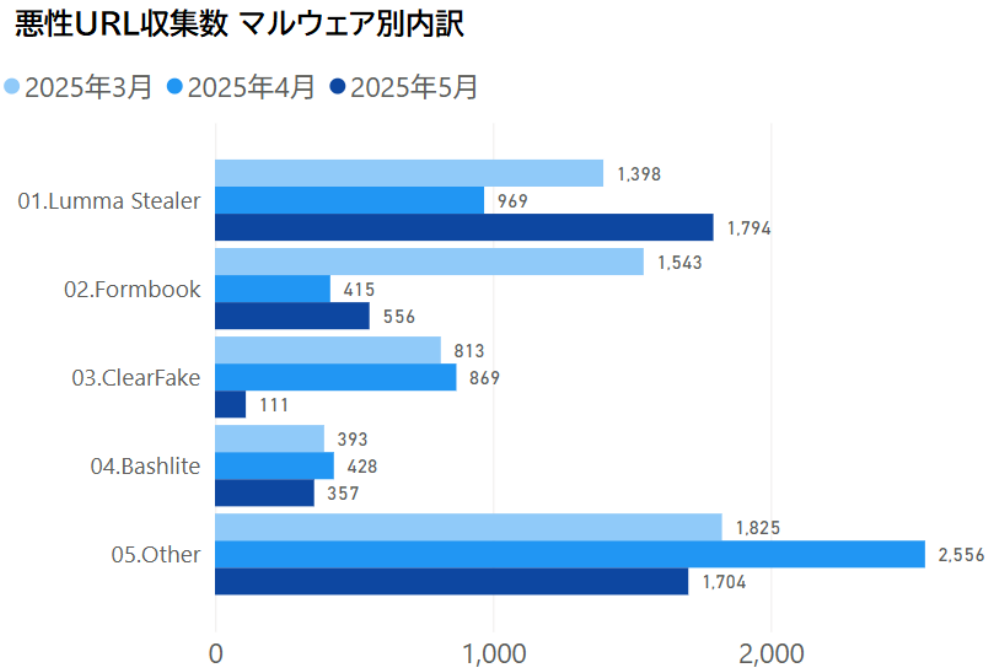
インフォスティーラーは、メールの添付ファイルや悪質な Web サイトなどを通じて拡散され、ユーザーが気付かない間に感染することが多く、また難読化や検出回避技術に長けているため発見が難しく、長期間にわたって情報を盗み続けることが可能です。これらの理由から、サイバー犯罪者にとって非常に人気のツールとなっています。

デジタルアーツによる添付ファイル、URL 調査でも多数のインフォスティーラーを確認

デジタルアーツの提供するメールセキュリティ「m-FILTER」のユーザーが受信した、悪性ファイルが添付されたメール（メール隔離/削除数含む）をマルウェア別に分類したところ、上位3つはいずれもインフォスティーラー感染を狙うものとなっていることがわかりました



また、デジタルアーツが様々なデータソース※2から収集した悪性 URL（フィッシングは含まない）をマルウェア別に分類すると、こちらもインフォスティーラー、もしくはインフォスティーラーをダウンロードさせるためのマルウェアが上位を占めていました。



※2‥自社データベースの「脅威情報サイト」カテゴリに該当する URL、データ提供元、一般公開された悪性 URL 情報を参照

インフォスティーラー対策が、ランサムウェア対策に。

今回の調査では、ランサムウェアの侵入原因（なぜ侵入ができたのか）を調査し、34%が「認証情報」によるものであるとわかりました。これらの認証情報はインフォスティーラーによって窃取され、その認証情報を使って組織内へ侵入を許し、ランサムウェア攻撃が仕掛けられることも少なくありません。また、インフォスティーラーの多くが、メールと Web の両方でマルウェアの上位を占めるほど拡散しており、犯罪者に人気であることが裏付けられました。

インフォスティーラーは感染に気づきにくく、被害が重大になる傾向があります。特に被害が深刻な場合や、法人環境での感染が疑われる場合には、セキュリティの専門家や警察への相談が重要です。

対策としては、メールと Web のセキュリティ対策が必要です。加えて、多要素認証の導入や最小限の権限設定を行うなど、認証認可の適切な設定も重要になります。

インフォスティーラーへの対策を行うことが、同時にランサムウェア対策にもなるといえます。

詳細のセキュリティレポートはこちら

ランサム侵入原因の 34%が認証情報、メールと Web から忍び寄るインフォスティーラーとの関係

https://www.daj.jp/security_reports/47/

■デジタルアーツの Web セキュリティ「i-FILTER」

デジタルアーツでは日々様々な情報をもとにデータの収集を行っています。

「i-FILTER」Ver.10 では、フィッシングサイト URL はフィルターデータベースへと迅速に配信され、

[フィッシング詐欺]や[迷惑メールリンク]や[違法ソフト・反社会行為]カテゴリにてブロックが可能です。

さらに、Web サービス制御機能においても、サービスごとの制御が可能です。

■デジタルアーツのメールセキュリティ「m-FILTER」 Ver.5

メールセキュリティ「m-FILTER（エムフィルター）」 Ver.5 は、電子メールフィルタリング（送受信制御）による誤送信対策、全保存（メールアーカイブ）・検索機能による内部統制・コンプライアンス強化、スパムメール対策・メールセキュリティの推進を実現します。

■安全な Web セキュリティの新定番「ホワイト運用」とは

フィルターデータベースに反映されていない URL についても「ホワイト運用」を行うことで、デジタルアーツが安全を確認した URL にのみアクセスを許可し未知のフィッシングサイトや悪性 URL をブロックすることができます。

■シングルサインオン・ID 管理「StartIn」

「StartIn」は IDaaS 製品です。通常の IDaaS 製品でできる ID 管理やシングルサインオン、多要素認証に加え、位置（GPS）を利用した「位置情報認証」、第三者（上長など）を認証要素に加える「第三者認証」、定期的にアプリケーションでの認証を実施する「定期認証」の独自認証により、強度の高い認証と安心・安全な ID 管理を実現します。

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、情報漏えい対策や標的型攻撃をはじめとするサイバー攻撃対策を実現する最先端の製品を、企業・官公庁・学校・家庭向けに提供しています。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー14F　▶URL: https://www.daj.jp/
＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社　広報課　畑楠・関　　TEL　: 03-5220-1670/ E-mail : press@daj.co.jp