DigitalArts

PRESS RELEASE

2021.03.09

報道関係者各位

デジタルアーツ株式会社

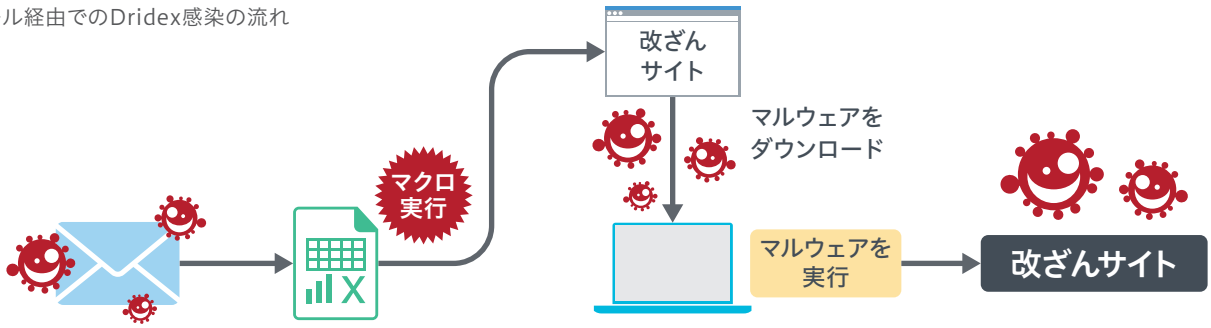
改ざんサイトを大量に悪用するマルウェアDridexに要注意

～「Dアラート」で攻撃キャンペーンを検知　解析レポートを公開～

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、サイバーリスク情報提供サービス「Dアラート」※で、マルウェアDridex（ドライデックス）に感染させるとみられるメール受信を多数検知していること、及びDridexダウンローダーの解析レポートを公開したことを発表いたします。

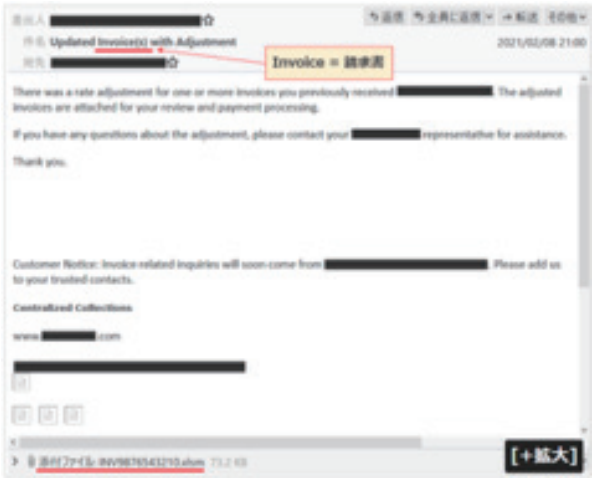
Dridexは情報窃取型のバンキングマルウェアの一種で、感染するとオンラインバンキングなどの認証情報が窃取されます。感染に至るまでの侵入経路にはいくつか報告がされていますが、多くがメールから侵入します。主に海外で攻撃キャンペーンが展開されていますが、デジタルアーツでは、2021年1月から3月にかけてDridexに感染させるとみられるメールを多数確認し、「Dアラート」を発出しました。メールでは、実在の組織を騙って送信元や組織名なども偽装しており、請求書関連のメールを装って、マクロを含むExcelファイルが添付されて送られてくるという手口です。添付ファイルを開いて不正なマクロを実行すると、改ざんサイトからマルウェアをダウンロードして実行し、感染へと繋がります。

【図1】メール経由でのDridex感染の流れ



改ざんサイトを大量に使用し、アンチウイルスやWebプロキシをすり抜ける手口

デジタルアーツでは、実際に検知したメール【図2】で検証しました。Dridexダウンローダーには、Excelファイルの拡張子「xls」または「xlsm」が用いられています。マクロを有効化し、ワークシート上の画像をクリックしてしまうと不正なマクロが実行されます。ワークシート内に予め埋め込まれた文字を用いて約50個のURLを形成し、ランダムでそのいずれか一つを使って改ざんサイトにアクセスさせ、Dridex感染へと至るという手口でした。



【図2】実際のメール

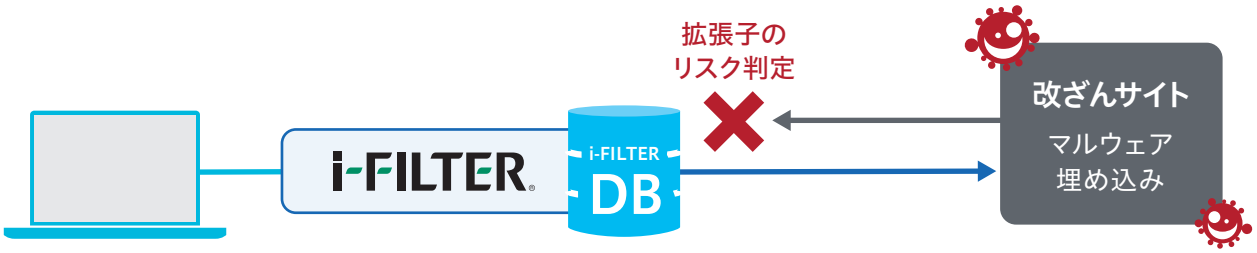
マルウェアダウンロードに用いられるURLは多い時で100を超えることもあり、そのほぼ全てが改ざんサイトでした。企業サイト、個人ブログ、ニュースサイト、ショッピングサイト、などその他様々な言語のWebサイトのURLが悪用され、マルウェアDridexが設置されていました。

改ざんサイトを用いることで、URLブラックリストやアンチウイルスによる発見を遅らせる、といった理由があると考えられます。また、ダウンロードURLが多数の中からランダムで一つ通信する仕組みであるため、サンドボックス等による把握が困難と考えられます。

「i-FILTER」Ver.10のダウンロードフィルター機能でマルウェアDridexのダウンロードをブロック

「i-FILTER」Ver.10は、Webサイトに埋め込まれたマルウェアのダウンロードをブロックする、「ダウンロードフィルター機能」があります。改ざんサイトに埋め込まれたDridexも、本機能でブロックすることが可能です。

▶ Web セキュリティ製品「i-FILTER」Ver.10 のダウンロードフィルター機能



【図3】マルウェアが直接Webサイトに埋め込まれている場合

▶ 製品詳細　https://www.daj.jp/bs/i-filter/

Dridexに感染させる攻撃メールキャンペーンは日本では大規模展開されていないものの、今年に入りメール受信を多数検知し始めています。被害を拡大させたEmotetも、海外圏が主なターゲットであったところ、ある時期から日本で活動が観測され、被害が拡大しました。海外で起こっていることは日本でも起こることが想定されます。こうした攻撃は組織の規模・業種を限定しているものではございませんので、しっかりと製品で対策を取っていただくことをお勧めします。

マルウェアDridexの解析情報レポートはこちら

以下、弊社コーポレートサイト上にて公開しております。

■ セキュリティレポート「メール経由で感染を狙う Dridex キャンペーン 大量の改ざんサイト URL を悪用」
https://www.daj.jp/security_reports/210309_1/

また、以下にてマルウェアDridexに感染させるとみられるメールおよびURLの検知実績について公開しております。

■ サイバーリスク情報提供サービス「D アラート」
https://www.daj.jp/bs/d-alert/archive/

※サイバーリスク情報提供サービス「Dアラート」は「i-FILTER」Ver.10、「m-FILTER」Ver.5、「i-FILTER@Cloud」「m-FILTER@Cloud」の機能を利用して、マルウェア感染の疑いのあるお客様や弊社のお客様以外へも感染情報やホームページの改ざん情報をお知らせする、無償の情報提供サービスです。

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、有害情報の閲覧を制限するWebフィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。
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　広報担当　山田
※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせ先は以下とさせていただきます
TEL : 090-1555-7254 / E-mail : press@daj.co.jp

DigitalArts
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