2022 年 3 月 31 日
デジタルアーツ株式会社

PRESS RELEASE

【セキュリティレポート】
Emotet の踏み台にされ、攻撃メールを送付した企業・組織は国内で 400 以上
～なぜメールはばらまかれるのか、ばらまかれるメールにはどのように対処するか～

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、Emotet についてのセキュリティレポートを公開したことを発表いたします。

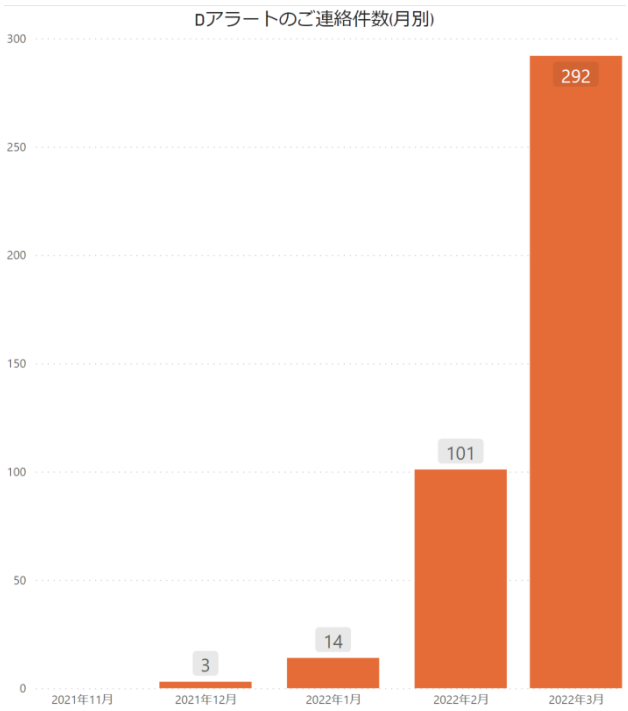
Emotet は 2014 年頃から活動が確認されているマルウェアで、2021 年初頭にテイクダウン（停止措置）されましたが、 2021 年 11 月頃から活動が再開し、今日に至るまで断続的に活発な活動が見られています。Emotet への感染は、メールの添付ファイルなどが発端となり、それらを開いて Office マクロの有効化を行うなどにより始まります。

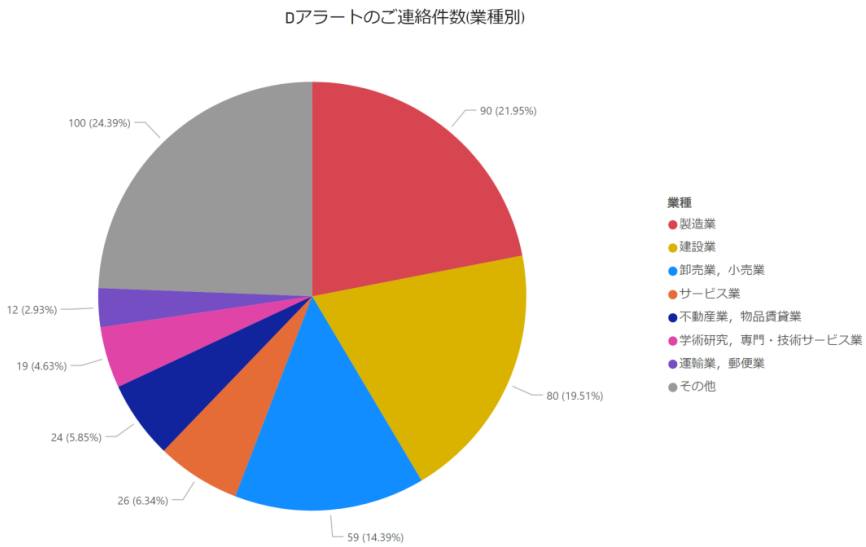
Emotet に踏み台利用された企業・組織は 410 件、 業種は製造業が最多

この Emotet をばらまく攻撃メールは、日本国内の企業・組織から送られているケースも多く、デジタルアーツが確認している限りでも 2021 年 11 月以降で 400 件以上ありました。デジタルアーツは、サイバーリスク情報提供サービス「D アラート」という取り組みを実施しています。「D アラート」は、マルウェア感染やホームページの改ざん、メールサーバーの踏み台利用などが見られる場合、デジタルアーツのお客さまに限らず連絡を行っている CSR 活動の一つです。

今回は、Emotet に感染させる攻撃メールをばらまいている日本の企業・組織に対し連絡を行った件数を用いています。Emotet が復活した 2021 年 11 月から 2022 年 3 月 13 日までの約 5 か月間において、メールサーバーが踏み台利用されている企業・組織への連絡件数は 410 件でした。2021 年 12 月は 3 件、2022 年 1 月は 14 件でしたが、2 月になり 101 件、3 月は 13 日間だけで 292 件と急増しています。前回の Emotet 流行時でも連絡件数は最大 1 か月あたり 39 件でしたので、桁違いの件数といえます。

また、連絡した 410 件の企業・組織について業種別にみると、「製造業」が最多で、次いで「建設業」、「卸売業，小売業」の順に多く、これらの業種で約半数を占めています。ただし、これらの業種は企業数そのものも多いため、母数が多いことに影響を受けているともみられます※。





ばらまかれるメールは巧妙化　最近は正規の企業情報を用いる手口も

2021 年 11 月の活動再開以降、Emotet をばらまく攻撃メールは日々巧妙になっており、直近の 2022 年 3 月ではメーラーから窃取したとみられる正規の企業情報を用いることもわかっています。

時期	特徴
2021年11月頃	・日本語以外の言語が大半
2021年12月頃	・**返信や転送**を装う件名 ・**宛先のメールアドレス**が件名に含まれる ・**活動再開以前に窃取**されたとみられる件名の流用
2022年1月～2月頃	・**活動再開以降に窃取**されたとみられる件名の流用 ・**メーラーから窃取したとみられる情報**を件名やファイル名に用いる
2022年3月頃	・本文が長くなる ・件名やファイル名、署名にメーラーから窃取したとみられる**正規の企業情報**を用いる

Emotet がメール情報や認証情報を窃取　考えられるケースは 3 つ

攻撃者はより感染を広めるため、メールを巧妙にしてきました。その主な要因として、Emotet の機能にメール情報や認証情報などを窃取するというものがあることが挙げられます。考えられるケースのうち、1 つ目は、感染した企業の情報を用いてメールが送付されるケースです。Emotet の機能により、送受信履歴やアドレス帳から、新たに Emotet へ感染させるためのメールを送ります。送信先もメールのやり取りがある中から選ばれることが多いため、精巧になりすますことができます。

2 つ目は、感染した企業の取引先を騙りメールが送付されるケースです。送信元に騙られた企業・組織が、必ずしも Emotet に感染しているとは限らず、感染端末のアドレス帳などから、メールで騙る送信者情報が作られることがあります。3 つ目は、メールサーバーが悪用されるケースです。Emotet に感染した端末より窃取されたメールアカウントの認証情報が悪用されるほか、メールサーバー自体がマルウェアに感染し悪用される事例も報告されています。

自分たちの企業・組織になりすましてばらまかれるメールにはどのように対処するか

ばらまかれるメールに対し、どのように対応すれば良いでしょうか。自分たちの企業・組織になりすまされたメールが出回っていると判明した場合は、まずは内部に Emotet 感染端末がないかを調査することを強く推奨します。メールサーバーのマルウェア感染の可能性もありますので、メールサーバーの調査を行うことも必要です。そして、Emotet への感染が見つからなかったとしても、関係各所に周知する必要があります。

今後、攻撃手法の変化や活発化が見られたとしても、Emotet の攻撃の入り口がメールである限り、窃取した情報からメールをばらまくという手法は利用され続けるとみられます。攻撃メールがばらまかれている現状を把握いただいたうえで、今後も不審なメールへの警戒を怠らず、適切なセキュリティ対策を実施いただくことを強く推奨します。

▼デジタルアーツが提案するセキュリティ対策

■D アラート

デジタルアーツ製品をご利用で、D アラートの通知先をご登録いただいている場合は、Web 通信やメールから、マルウェア感染が疑われる場合にご連絡しております。デジタルアーツ製品をご利用でない場合も、所有している Web サイトの改ざんや、メールサーバーの踏み台利用が見られた場合に連絡しております。

https://www.daj.jp/bs/d-alert/

■「i-FILTER」 Ver.10 と「m-FILTER」 Ver.5 での Emotet 対策について

送信者が普段からやり取りのある企業・組織だとしても、「m-FILTER」の添付ファイル強制検査機能や添付ファイル偽装判定での検知が可能です。また、正規の送信元からだとしても過去 90 日間に交流がなかった場合には、踏み台攻撃である可能性のあるメールとしてメールを無害化する機能があります。

https://www.daj.jp/bs/ifmf/

▶「踏み台にされ Emotet のメールを送付した企業・組織は国内でも 400 以上」についてのレポートはこちら

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　https://www.daj.jp/security_reports/220331_1/

※　総務省・経済産業省「平成 28 年経済センサス-活動調査結果」 によると、「製造業」、「建設業」、「卸売業，小売業」は全企業等数の約 43%を占めています。
今回の D アラートは 3 つの業種で半数以上となっていますが、この傾向はそもそもの母数が多いことに影響を受けているとみられます。
https://www.stat.go.jp/data/e-census/2016/kekka/pdf/k_gaiyo.pdf

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　石井　　TEL　: 080-1555-7254　/ E-mail : press@daj.co.jp
※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は上記とさせていただきます。