関係者各位

株式会社　ダイレクト21

弊社を名乗る「なりすまし迷惑メール」のお詫びとご注意喚起

頭書の件、2月より弊社を名乗るなりすまし迷惑メールが送信され、当該メールを受信された皆様には、多大なご迷惑をお掛けしたことを改めて深くお詫び申し上げます。

なりすましメールを発信しているのは弊社のメールサーバでなくハッカーサーバであるため弊社での抑止ができません。

弊社を名乗り内容が不自然なメールが届きましたら、メールの開封、付属ファイルの　参照、或いはメール本文中の URL のクリック等を行うことなく削除していただきますようお願いいた　します。

弊社の「迷惑メール」への対応

今後、弊社から発信する添付ファイル付きの全てのメールにつき、添付ファイル(Excel,Word,PowerPoint など)を zip 形式(xxxx.zip)に凍結し、拡張子(.zipP)部分を(.zi_)に修正して送付いたします。受信後は(.zi_)部分を(.zip)に変更後、解凍をお願いいたします。　※弊社メールサーバの SPF 設定(ドメイン詐称防止設定)を実施しております。

「なりすまし迷惑メール」関連記事

添付(画像左)3月10日付朝日新聞記事にも指摘されていますが、迷惑メールを発信しているのはロシアや東欧系ハッカーグループのようで活動が活発化しているようです。先日の7時の NHK ニュースでも報じられました。

３月１０日付朝日新聞社会面


朝刊［東京］ 2022/3/10(木)
社会
「最恐」のPCウイルス 再燃
エモテット 企業・行政のメール侵食
消滅のはずが急増
日本標的の見方も
収入印紙貼らず 納付漏れ
ファミマの支払い 10万通超 国税当局

※朝日新聞記事

「最恐」のPCウイルス、再燃　エモテット、企業・行政のメール侵食

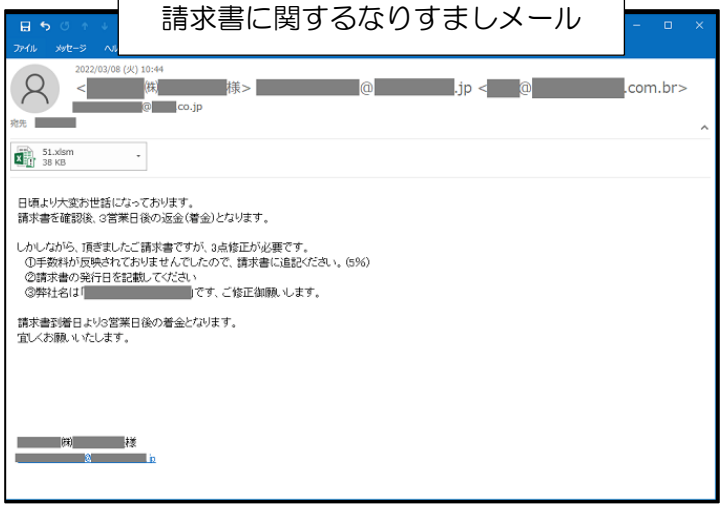
世界規模で感染が広がり、いったんは消滅したはずのコンピューターウイルスが息を吹き返している。メールを介してウイルスをばらまく「Emotet(エモテット)」だ。3月に入り、これまでにない広がりを観測。「感染爆発」とも言える状況が起きている。

※ネットニュース記事

また 3 月 4 日ごろから、下記 URL のネットニュースにありますように、日本語文面(画像右)で請求書に関する具体的な指示が自然な日本語で書かれているメールも発信されています。

https://www.itmedia.co.jp/news/articles/2203/10/news107.html

請求書に関するなりすましメール


2022/03/08 (火) 10:44
51.xlsm
38 KB
日頃より大変お世話になっております。
請求書を確認後、3営業日後の返金(着金)となります。
しかしながら、頂きましたご請求書ですが、3点修正が必要です。
①手数料が反映されておりませんでしたので、請求書に追記ください。(5%)
②請求書の発行日を記載してください
③弊社名は[redacted]です、ご修正御願いします。
請求書到着日より3営業日後の着金となります。
宜しくお願いいたします。

感染が疑われる場合の対応

下記サイトの「2-1.EmoCheck による Emotet 感染有無の確認」を実施にて感染有無確認ができます。

マルウエア Emotet への対応 FAQ - JPCERT/CC Eyes｜JPCERT コーディネーションセンター公式ブログ

https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html