平成 27 年 12 月 28 日

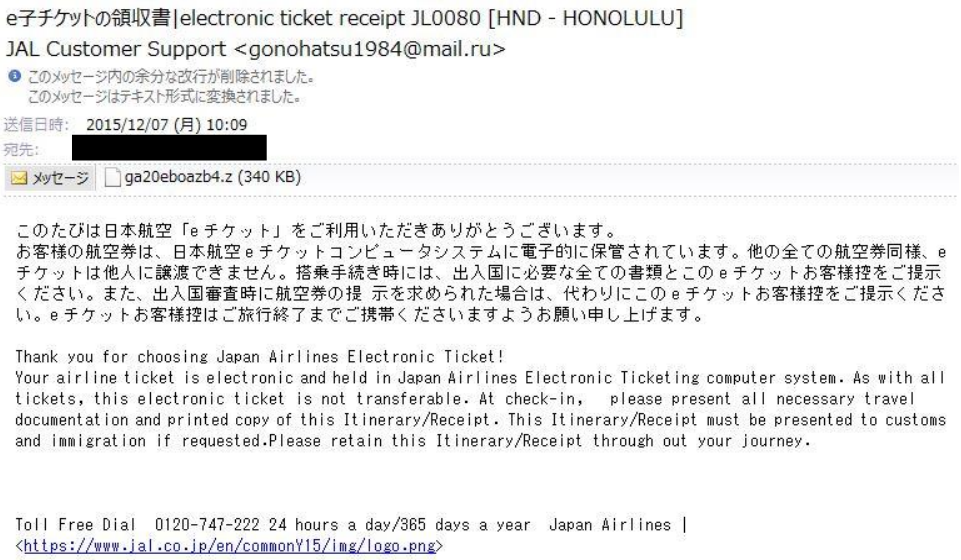
各位

経営企画課 IT 推進担当

【注意喚起】身代金要求型不正プログラムがメールで送られてきています！

感染した PC 上のファイルを勝手に暗号化して『人質』に取り、「復旧して欲しければ『身代金』を支払え」と要求する**「身代金要求型不正プログラム（ランサムウェア）」**が急増しています。本学にもこのようなメールが送られてきたことが確認されたため注意喚起します。

以下は、JAL からの連絡を装ったばらまき型攻撃メールサンプルです。


e子チケットの領収書|electronic ticket receipt JL0080 [HND - HONOLULU]
JAL Customer Support <gonohatsu1984@mail.ru>
このメッセージ内の余分な改行が削除されました。
このメッセージはテキスト形式に変換されました。
送信日時: 2015/12/07 (月) 10:09
宛先: [redacted]
メッセージ ga20eboazb4.z (340 KB)

このたびは日本航空「ｅチケット」をご利用いただきありがとうございます。
お客様の航空券は、日本航空ｅチケットコンピュータシステムに電子的に保管されています。他の全ての航空券同様、ｅチケットは他人に譲渡できません。搭乗手続き時には、出入国に必要な全ての書類とこのｅチケットお客様控をご提示ください。また、出入国審査時に航空券の提 示を求められた場合は、代わりにこのｅチケットお客様控をご提示ください。ｅチケットお客様控はご旅行終了までご携帯くださいますようお願い申し上げます。

Thank you for choosing Japan Airlines Electronic Ticket!
Your airline ticket is electronic and held in Japan Airlines Electronic Ticketing computer system. As with all tickets, this electronic ticket is not transferable. At check-in, please present all necessary travel documentation and printed copy of this Itinerary/Receipt. This Itinerary/Receipt must be presented to customs and immigration if requested.Please retain this Itinerary/Receipt through out your journey.

Toll Free Dial 0120-747-222 24 hours a day/365 days a year Japan Airlines |
<https://www.jal.co.jp/en/common/15/img/logo.png>

図１：JAL からの連絡を装ったばらまき攻撃型メールの例

添付ファイルは「.z」形式（Unix での圧縮形式）で、Lhaplus などの解凍ユーティリティで解凍することが可能な形式となっています。こちらを解凍すると、以下の画像のとおり PDF ファイルがあるように見えますが、実際には exe 形式の実行ファイルでこのファイルを実行すると、インターネットからの指示に基づき PC 内のファイルを暗号化し、身代金を要求するようです。

以下が、PDF ファイルに偽装した.exe ファイルのサンプルです。

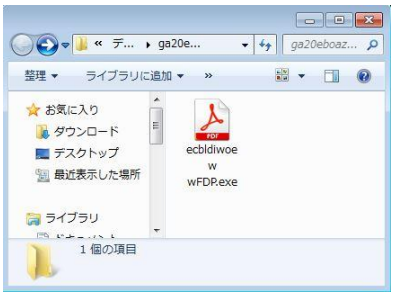
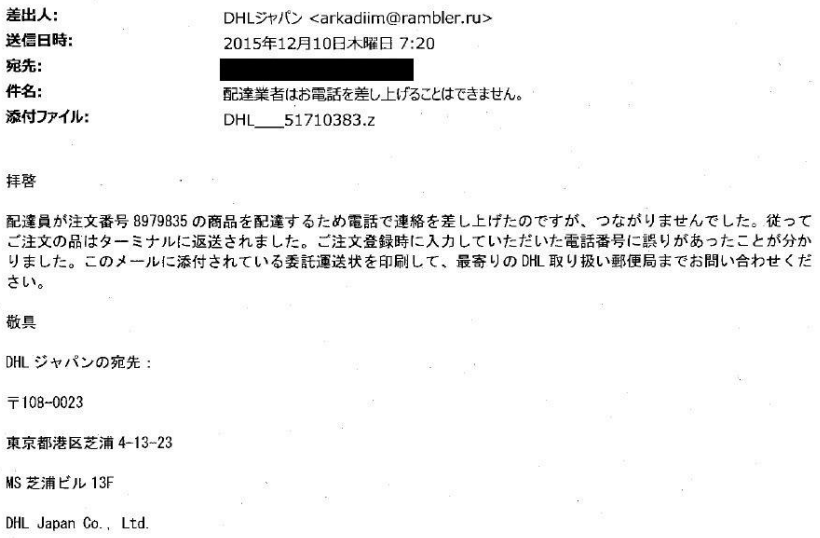


図２：PDF ファイルに偽装した.exe ファイル

また、同様に DHL ジャパンからの連絡を装ったメールが送られてきていることも確認しており、こちらも同様の手法と考えられます。



差出人: DHLジャパン <arkadiim@rambler.ru>
送信日時: 2015年12月10日木曜日 7:20
宛先: [redacted]
件名: 配達業者はお電話を差し上げることはできません。
添付ファイル: DHL___51710383.z

拝啓

配達員が注文番号 8979835 の商品を配達するため電話で連絡を差し上げたのですが、つながりませんでした。従ってご注文の品はターミナルに返送されました。ご注文登録時に入力していただいた電話番号に誤りがあったことが分かりました。このメールに添付されている委託運送状を印刷して、最寄りの DHL 取り扱い郵便局までお問い合わせください。

敬具

DHL ジャパンの宛先：

〒108-0023

東京都港区芝浦 4-13-23

MS 芝浦ビル 13F

DHL Japan Co., Ltd.

図３：DHL からの連絡を装ったばらまき型メールの例

共通する特徴としては、下記が挙げられます。

◆ロシアのドメイン(.ru)が送信元である。
◆添付ファイルの拡張子が「.z」形式の圧縮ファイルである。
◆日本語化されている。

ランサムウェアに感染すると、感染した PC のファイルがすべて暗号化されてしまうだけではなく、同一ネットワーク上のファイルサーバーのファイルも同じく暗号化されてしまうケースが多くみられます。このため、誰かひとりがランサムウェアに感染しただけで、多くの情報が失われてしまう可能性があります。感染しないよう、各自が心がけることはもちろんですが、万が一に備え、バックアップをこまめに採るよう、重ねてお願いします。

※参考

独立行政法人情報処理推進機構(IPA)
2015 年 12 月の呼びかけ「ウイルス感染を目的としたばらまき型メールに引き続き警戒を」
https://www.ipa.go.jp/security/txt/2015/12outline.html

■こちらの内容に関するお問合せ先
八景キャンパス経営企画課IT推進担当
E-mail:center@yokohama-cu.ac.jp
TEL:045-787-2340/2341（平日9:00～17:00）