ウイルスメール一覧

1．ウイルスメール一覧

ウイルスメール収集対象期間　：　平成28年9月1日～9月30日

No.	受信日時	送信元	件名	添付ファイル	ウイルス検出名
1	2016/9/1	Mueller.66@seriousrenters.com	bank transactions	96c3433d7683.zip	Trojan.Gen.NPE（Symantec） 種類:ランサムウェア／ダウンローダー
2	2016/9/1	Mueller.66@seriousrenters.com	bank transactions	96c3433d7683.zip	JS/Nemucod.nj（McAfee） 種類:ランサムウェア／ダウンローダー
3	2016/9/2	Crawford.74@waghadproject.org	old office facilities	f9a90594421.zip	Trojan.Gen.NPE（Symantec） 種類:ランサムウェア／ダウンローダー
4	2016/9/6	Dominguez.993@BerksCountyElegantWeddings.com	copies	a4d1416830.zip	JS/Nemucod.nj（McAfee） 種類:ランサムウェア／ダウンローダー
5	2016/9/6	Jennings.285@elitemassageacademy.com	copies	72bc6864d9b.zip	Trojan.Gen.NPE（Symantec） 種類:ランサムウェア／ダウンローダー
6	2016/9/12	Riggs.15507@comone.co.zw	Budget report	31733aa99ab.zip	JS/Nemucod.nj（McAfee） 種類:ランサムウェア／ダウンローダー
7	2016/9/13	Battle.6267@static.vnpt.vn	Tax invoice	da4c76eb9914.zip	JS_LOCKY.DLDSAOR（TrendMicro） 種類:ランサムウェア／ダウンローダー
8	2016/9/14	Gross.24871@abotuin.nl	Equipment receipts	3ea33f6c46bd.zip	JS_LOCKY.DLDSAOR（TrendMicro） 種類:ランサムウェア／ダウンローダー
9	2016/9/15	Craig.31067@bufetegarciayasociados.com	Renewed License	d808d46347e1.zip	JS_LOCKY.DLDSAOU（TrendMicro） 種類:ランサムウェア／ダウンローダー
10	2016/9/15	Armstrong.819@ricardcamarena.com	financial report	1b4ddb47090.zip	JS_LOCKY.DLDSAOW（TrendMicro） 種類:ランサムウェア／ダウンローダー
11	2016/9/16	Cole.44768@lightstyleofamerica.com	Booking confirmation	6abab870a009.zip	JS/Nemucod.jt（McAfee） 種類:ランサムウェア／ダウンローダー
12	2016/9/19	Oneal.04302@thoughtube.com	Express Parcel service	5402c536d52a.zip	JS_LOCKY.DLDSAPA（TrendMicro） 種類:ランサムウェア／ダウンローダー
13	2016/9/20	Allen.741@whiterosetattoo.com	Tracking data	bb7474c1d760.zip	JS_LOCKY.DLDSAPB（TrendMicro） 種類:ランサムウェア／ダウンローダー
14	2016/9/20	shoei_ss@oregano.ocn.ne.jp	注文書	n0533979455384(pdf).zip	TSPY_BEBLOH.YMNMY（TrendMicro） 種類:スパイウェア
15	2016/9/21	Munoz.430@maryellenmanning.com	Out of stock	bb28879a6ec0.zip	Trojan.Gen.NPE（Symantec） 種類:ランサムウェア／ダウンローダー
16	2016/9/21	Boyle.93@eurekagarages.com.au	Package	496c5feafa.zip	JS_LOCKY.DLDSAPC（TrendMicro） 種類:ランサムウェア／ダウンローダー
17	2016/9/27	abeckham0325@yahoo.co.jp	ご注文受付メール	XS0.0737711858489 DOC.zip	HEUR_NAMETRICK.A（TrendMicro） 種類:スパイウェア
18	2016/9/28	iis-l2@tenor.ocn.ne.jp	台風対策について	2016.9.28n・220001326doc.zip	HEUR_NAMETRICK.A（TrendMicro） 種類:スパイウェア

2. ウイルスメールの特徴

（1）送信元
送信元は詐称されている場合があります。

（2）件名
英語表記だけでなく日本語表記のメールタイトルが使用されるケースもあります。

①「bank transactions」のような、銀行口座の取引情報を連想させる件名
②「Tax invoices」「Out of stock」「ご注文受付メール」のような、取引にて発生した確認書等の書類送付を連想させるような件名
③「台風対策について」のようなトレンドな話題の件名
④「copies」「old office facilities」のような事務作業を連想させる件名

（3）添付ファイル
①ファイル名
・ランダムな英数字の組合せでつけられた名称
・受信日を含んだ名称
②形式
・ZIP(圧縮)ファイル

（4）本文
「iPhoneから送信」という文言が、本文の最後に書かれているケースが複数件確認されています。

（5）ウイルス検出名
ウイルス検出名は、ウイルス対策ソフトを提供するセキュリティベンダーが、ウイルスに対して付与する名称で、同一のウイルスであってもウイルス対策ソフト毎に表記が異なる場合があります。当一覧では「TrendMicro」、「McAfee」、「Symantec」のいずれかの検出名を記載しています。

①ランサムウェア：感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求するウイルス
②ダウンローダー：攻撃者が用意したサーバーから別のウイルスをダウンロードさせる機能をもつウイルス
③スパイウェア：ユーザーに気づかれずに、コンピュータに不正侵入して、ユーザーの行動や個人情報を収集し送信するウイルス

３．補足事項

上記期間に収集したウイルスメールに添付されたファイルは、ランダムな英数字で付けられたzip形式のファイルでした。ウイルスメールの添付ファイルはzip形式であることが多いため、注意いただいていると思われますが、ドキュメントファイル（拡張子.doc、.docm等）が添付されたウイルスメールが届くケースもあります。

また、ウイルスメールには、英語表記の件名がつけられていましたが、全国的には、「保安検査」、「宅急便お届けのお知らせ」、「商品お届けのご案内」等、不審に感じない日本語表記の件名や本文のウイルスメールも発見され、各セキュリティソフト会社より注意喚起が出ています。送信元のメールアドレスを確認し、身に覚えのないメール、または、万が一メールを開いた場合でも、上記の特徴のような添付ファイルは開かないよう、十分に注意してください。