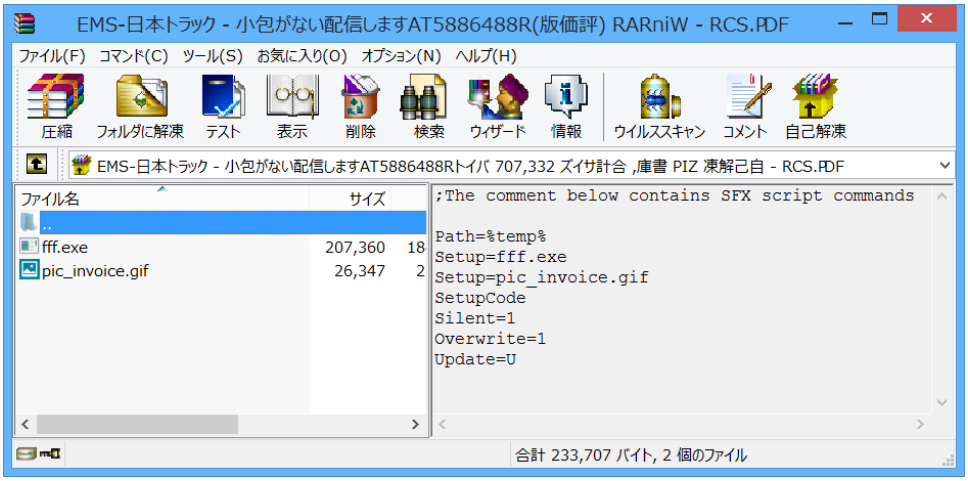
【メール基本情報】

項番	基本情報
1	送信元ドメイン: rambler.ru 件名: 件名なし 添付ファイル名: EMS_1302015_35143.zip 添付ファイルハッシュ値: MD5: 29A2B91C3E5232FEFA62FD7E4CE79D62 SHA-1: AA56BB8C43D549EB52160DC5A226F5D40621C15B

【メール本文】

項番	本文
1	拝啓 配達員が注文番号**********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 EMS 取り扱い郵便局までお問い合わせください。 敬具 EMS ジャパンの宛先 : 〒108-5205 東京都港区芝浦 4-13-23 MS 芝浦ビル 13F EMS Japan Co., Ltd. 注: *******の部分は 12 桁の数字

【添付ファイル調査】

項番	添付ファイル	調査情報
1	EMS_1302015_35143.zip	MD5: 29A2B91C3E5232FEFA62FD7E4CE79D62 SHA-1: AA56BB8C43D549EB52160DC5A226F5D40621C15B 展開すると[MS-日本トラック － 小包がない配信します AT5886488RRCS.PDF](RLO あり)正しいファイル名は[E EMS-日本トラック － 小包がない配信します AT5886488RFDP.SCR]
1	EMS-日本トラック － 小包がない配信します AT5886488RRCS.PDF	MD5: 9293F0E8713A366CB2DD8DF74D61F36E SHA-1: 12C9B1B715AA0E8E828EF3087800CD5D74284445 ファイル名には RLO が使われており正しい拡張子は、[scr]。正しいファイル名は[EMS-日本トラック － 小包がない配信します AT5886488RFDP.SCR]。ファイルの種類はスクリーンセーバー。 このファイルの中には[fff.exe]と[pic_invoice.gif]  ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/32f108c46cea0500e06b60b8de981a5c15f0c42db948b1bf89e032030fa048c8/analysis/
1	fff.exe	MD5: 4394DDC1B24159B1DB0E17EF30CC6402 SHA-1: 11715FCD3D4316033B92FC1061F957EEEB0E902D ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/2fbfca44a0ff56fdd36cb266821ada35cadec4017d9bb918f3bdf5dadbe4c609/analysis/1452790421/ ■接続先ドメイン tdf.in.ua hosenherren.de

optionwin.tk

emilysworld.us

novingostar.net

expertiza.info

design.3dstyle.in.ua

e-minunat.ro

portalmaismidia.com.br

sigareta.by

torsh.in

eurotend.it

noye.pl

dravram.ro

iceshow.kz

cheyn.us

wicaksanajayaabadi.com

medmo.net

becar.net

efespastanesi.com.tr

kancelaria-ostrowska.pl

gmc2015.tk

babylicious.ie

naturalpraxis.es

bktrade.kiev.ua

evanetwork.ro

bichngocshop.tk

mundomuvi.com.br

idealmarket.kz

savethesummit.com

patrianossa.com.br

bootsvermietung-moisl.de

kostenlose-erstberatung.de

fineeyecolor.com

mjfotos.de

mjakobs.nl

tra.su

dalihome.cn

■接続先 URL

http://tdf.in.ua/ZBVi09.php?a=3pr5a23nsp1n54

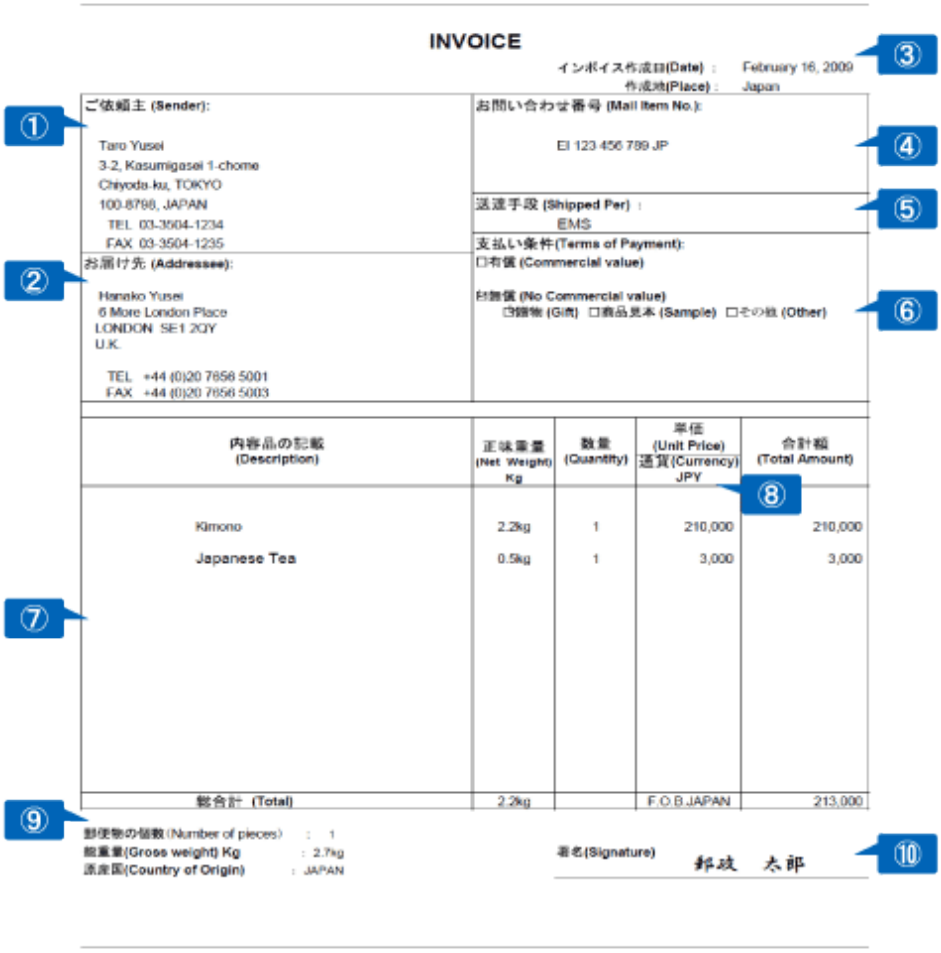
http://hosenherren.de/kFIy3A.php?z=3pr5a23nsp1n54

http://optionwin.tk/HtluAy.php?j=3pr5a23nsp1n54

http://emilysworld.us/Pd3MDR.php?h=3pr5a23nsp1n54

		http://novingostar.net/mxRrUj.php?l=3pr5a23nsp1n54 http://expertiza.info/FNCul0.php?z=3pr5a23nsp1n54 http://design.3dstyle.in.ua/i34zIW.php?i=3pr5a23nsp1n54 http://e-minunat.ro/i28emH.php?z=3pr5a23nsp1n54 http://portalmaismidia.com.br/tnSmIb.php?s=3pr5a23nsp1n54 http://sigareta.by/gROnmV.php?q=3pr5a23nsp1n54 http://torsh.in/TFWoqw.php?l=3pr5a23nsp1n54 http://eurotend.it/G5DSbw.php?u=3pr5a23nsp1n54 http://noye.pl/C4uRnf.php?s=3pr5a23nsp1n54 http://dravram.ro/CcT8oy.php?p=3pr5a23nsp1n54 http://iceshow.kz/4vMNJt.php?e=3pr5a23nsp1n54 http://cheyn.us/CxMcud.php?m=3pr5a23nsp1n54 http://wicaksanajayaabadi.com/mkYJHW.php?l=3pr5a23nsp1n54 http://medmo.net/m2_P0E.php?p=3pr5a23nsp1n54 http://becar.net/y48WzV.php?o=3pr5a23nsp1n54 http://efespastanesi.com.tr/Miwa0O.php?e=3pr5a23nsp1n54 http://kancelaria-ostrowska.pl/SGs6i_.php?w=3pr5a23nsp1n54 http://gmc2015.tk/kidr5Q.php?y=3pr5a23nsp1n54 http://babylicious.ie/s1GHUZ.php?x=3pr5a23nsp1n54 http://naturalpraxis.es/mrXjtb.php?w=3pr5a23nsp1n54 http://bktrade.kiev.ua/76b3ZQ.php?n=3pr5a23nsp1n54 http://evanetwork.ro/0XO231.php?x=3pr5a23nsp1n54 http://bichngocshop.tk/4vSAGh.php?g=3pr5a23nsp1n54 http://mundomuvi.com.br/mfv2TI.php?c=3pr5a23nsp1n54 http://idealmarket.kz/czDqxo.php?x=3pr5a23nsp1n54 http://savethesummit.com/8AqU4l.php?f=3pr5a23nsp1n54 http://patrianossa.com.br/Gv9UNy.php?o=3pr5a23nsp1n54 http://bootsvermietung-moisl.de/Y8GEZ_.php?d=3pr5a23nsp1n54 http://kostenlose-erstberatung.de/OLvfWS.php?i=3pr5a23nsp1n54 http://fineeyecolor.com/JxtfPn.php?l=3pr5a23nsp1n54 http://mjfotos.de/yoAM3Z.php?l=3pr5a23nsp1n54 http://mjakobs.nl/ksi7qV.php?z=3pr5a23nsp1n54 http://tra.su/fN1iuE.php?l=3pr5a23nsp1n54 http://dalihome.cn/1LSUpq.php?i=3pr5a23nsp1n54 注：上記、接続先ドメイン、接続先 URL はサンドボックスによる解析によるものですのでこちらがすべての接続先ではない可能性があります。また、マルウェアの通信先ではなく接続確認を行うためだけのものと思われるものは排除しております。
1	pic_invoice.gif	MD5: B216F5A82604394F46F9870853E97B18 SHA-1: A78ED451C20E1B793D67EB4B6B6F589C0FA5976D ■VirusTotal（検出なし）

https://www.virustotal.com/ja/file/e4808a018d2485d8468e211b7cc4038097022b80a677d133b3397f5454403e9a/analysis/1452790623/



INVOICE

インボイス作成日(Date) : February 16, 2009
作成地(Place) : Japan

③

①

ご依頼主 (Sender):

Taro Yusei
3-2, Kasumigasei 1-chome
Chiyoda-ku, TOKYO
100-8798, JAPAN
TEL 03-3504-1234
FAX 03-3504-1235

お問い合わせ番号 (Mail Item No.):

EI 123 456 789 JP

④

送達手段 (Shipped Per) :
EMS

⑤

②

お届け先 (Addressee):

Hanako Yusei
6 More London Place
LONDON SE1 2QY
U.K.

TEL +44 (0)20 7856 5001
FAX +44 (0)20 7856 5003

支払い条件(Terms of Payment):
□有償 (Commercial value)

⑥

□無償 (No Commercial value)
□贈物 (Gift) □商品見本 (Sample) □その他 (Other)

内容品の記載 (Description)	正味重量 (Net Weight) Kg	数量 (Quantity)	単価 (Unit Price) 通貨(Currency) JPY	合計額 (Total Amount)
Kimono	2.2kg	1	210,000	210,000
Japanese Tea	0.5kg	1	3,000	3,000
総合計 (Total)	2.7kg		F.O.B.JAPAN	213,000

⑧

⑦

⑨

郵便物の個数(Number of pieces) : 1
総重量(Gross weight) Kg : 2.7kg
原産国(Country of Origin) : JAPAN

署名(Signature) 郵政 太郎

⑩

【接続先ドメインからの調査】

項番	メモ
1	現時点で特筆すべき事項無し。