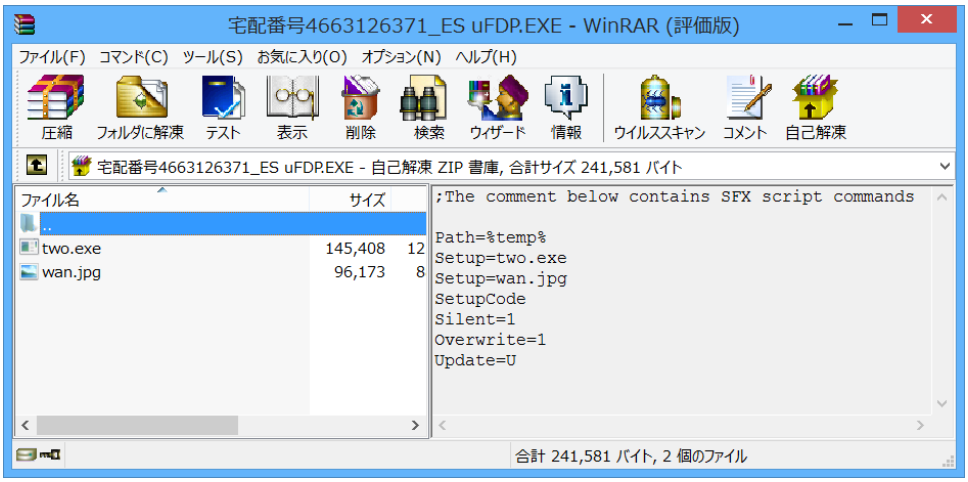
【メール基本情報】

項番	基本情報
1	メールを入手できていないため確認できず。 送信元ドメイン: 現在不明 件名: [件名なし] 添付ファイル名: 現在不明 添付ファイルハッシュ値: MD5: 現在不明 SHA-1: 現在不明
2	送信元ドメイン: rambler.ru 件名: [件名なし] 添付ファイル名: 宅配番号_06012015_EMS^^9514853.zip 添付ファイルハッシュ値: MD5: 1D51E6713DA6A01133E3D714761E196D SHA-1: A156C90452C7D8E0B6151D492EB5EE3856E2B48C
3	送信元ドメイン: rambler.ru 件名: 配達業者はお電話を差し上げることはできません。 添付ファイル名: EMS_59624.zip 添付ファイルハッシュ値: MD5: 1472D27F9CA8BB6D3FED695540D72E99 SHA-1: 6C795214C857617147EF482FEEE5DCBC434A0646

【メール本文】

項番	本文
1	メールを入手できていないため未確認。
2	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 注: *******の部分は 7 桁の数字
3	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: 〒108-7309 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	現在不明	メールを入手できていないため調査できず。
1	宅配番号 4663126371_ES uFDP.EXE	MD5: 04741D2FE07A12AF4F67359B06323128 SHA-1: C93735E655502A35046F45F59CE7875211FF7CB9 ファイル名から恐らくもとは RLO を用いて拡張子が PDF になるようにされていたと考えられる。 このファイルの中には[two.exe]と[wan.jpg] 
1	two.exe	MD5: 02F12EE23202457040B1D972773EF18A SHA-1: 3B7893849CE637EFF75154C0FB06BC192D7DA8F4 ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/4c94b552fe0df0a53857970463e590d52f57002fa78d02ffb78dd3f252730463/analysis/ ■接続先ドメイン castuning.ru mgsmedia.ru textidea.com vintageselects.com pausephone.com hybridtrend.com basislabel.com finehotels.net circlewear.net helloalliance.net seaboy.net

wildclick.net

ninthclub.com

camelcap.com

ideagreens.com

guesstrade.com

■接続先 URL

http://castuning.ru:8080/

http://castuning.ru/rss/feed/stream

http://castuning.ru/rss/feed/stream

http://mgsmedia.ru:8080/

http://mgsmedia.ru/rss/feed/stream

http://textidea.com:8080/

http://textidea.com/rss/feed/stream

http://vintageselects.com:8080/

http://vintageselects.com/rss/feed/stream

http://mgsmedia.ru/rss/feed/stream

http://pausephone.com:8080/

http://pausephone.com/rss/feed/stream

http://textidea.com/rss/feed/stream

http://hybridtrend.com:8080/

http://hybridtrend.com/rss/feed/stream

http://vintageselects.com/rss/feed/stream

http://basislabel.com:8080/

http://basislabel.com/rss/feed/stream

http://pausephone.com/rss/feed/stream

http://finehotels.net:8080/

http://finehotels.net/rss/feed/stream

http://hybridtrend.com/rss/feed/stream

http://circlewear.net:8080/

http://circlewear.net/rss/feed/stream

http://basislabel.com/rss/feed/stream

http://helloalliance.net:8080/

http://helloalliance.net/rss/feed/stream

http://finehotels.net/rss/feed/stream

http://seaboy.net:8080/

http://seaboy.net/rss/feed/stream

http://circlewear.net/rss/feed/stream

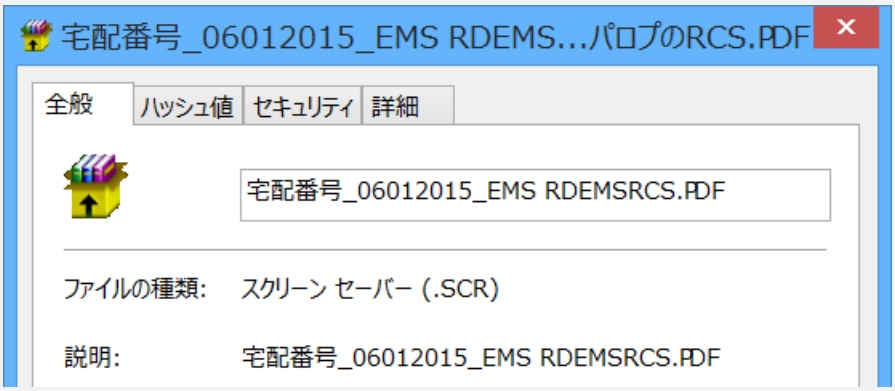
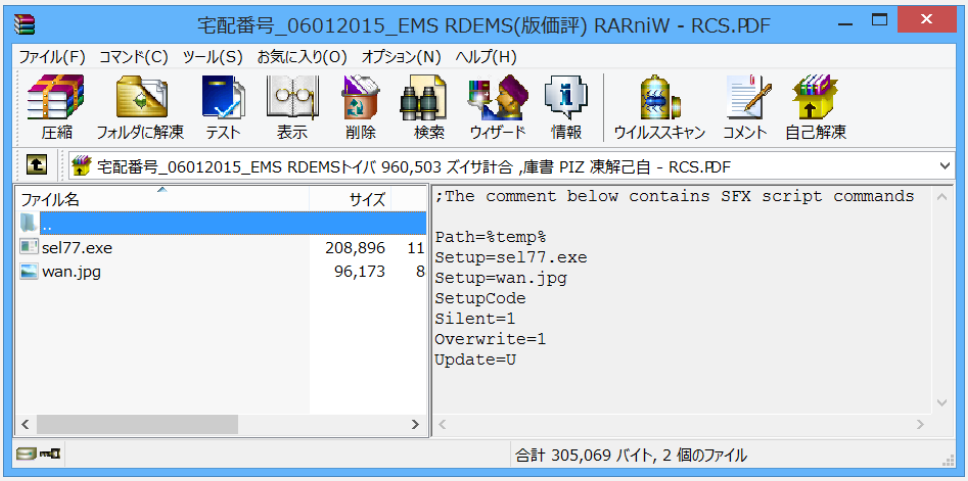
http://wildclick.net:8080/

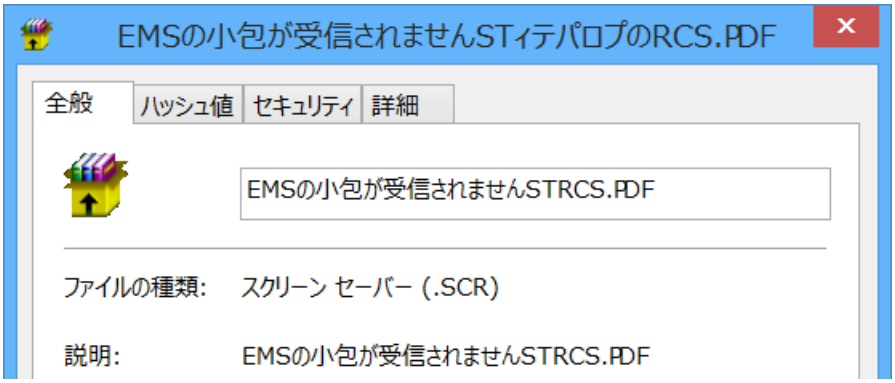
http://wildclick.net/rss/feed/stream

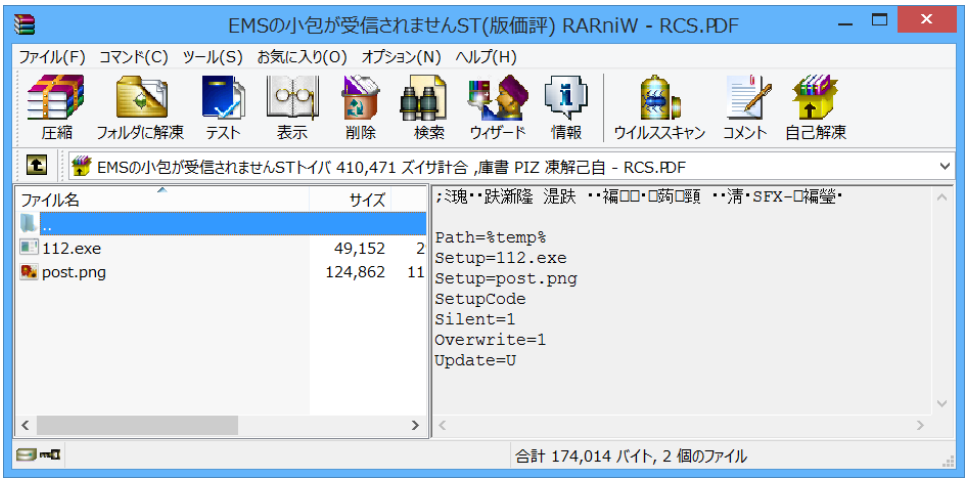
http://helloalliance.net/rss/feed/stream

http://ninthclub.com:8080/

		http://ninthclub.com/rss/feed/stream http://seaboy.net/rss/feed/stream http://camelcap.com:8080/ http://camelcap.com/rss/feed/stream http://ideagreens.com:8080/ http://ideagreens.com/rss/feed/stream http://wildclick.net/rss/feed/stream http://guesstrade.com:8080/ http://guesstrade.com/rss/feed/stream http://ninthclub.com/rss/feed/stream http://camelcap.com/rss/feed/stream http://ideagreens.com/rss/feed/stream http://guesstrade.com/rss/feed/stream 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	wan.jpg	MD5: 86FBC789FE9F0CFD94F4CA64815CC113 SHA-1: AA2108EAC13E930F51B2FFCE5B863AADE9FC9384 ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/8a8f9ab60b84b0e96e9567473dd782a2e09d87d75fa75be4273f5afae6e912b8/analysis/ （ファイルヘッダーを見る限り Jpeg であるため上記結果は誤検出と思われる） 
2	宅配番号 _06012015_EMS^^9514853.zip	MD5: 1D51E6713DA6A01133E3D714761E196D SHA-1: A156C90452C7D8E0B6151D492EB5EE3856E2B48C 展開すると[宅配番号_06012015_EMS_RDEMSRCS.PDF](RLO あり) 正しいファイル名は[宅配番号_06012015_EMS_RDEMSFDP.SRC]

2	宅配番号 _06012015_EMS_RDEMSRCS. PDF	MD5: F48B4682ED887D6D7A04FF12445D9EBC SHA-1: CAFDB14F25658E0FBA14E0997AA7FA0ABB869DE0 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[宅配番号_06012015_EMS_RDEMSFDP.SRC]。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[sel77.exe]と[wan.jpg] 
2	sel77.exe	MD5: 6304AC088AD4FEFD1C00D49F62BF852E SHA-1: 34A144165718F44F1C651DD816EC23381F1324DF ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/c79b7dc7ed9413190bbebef17b13c4506208e27c9b55988b7d711562f1e651d7/analysis/1452079730/ ■接続先ドメイン www.cacetech.com ■通信先 URL 現在不明 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。

2	wan.jpg	MD5: 86FBC789FE9F0CFD94F4CA64815CC113 SHA-1: AA2108EAC13E930F51B2FFCE5B863AADE9FC9384 ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/8a8f9ab60b84b0e96e9567473dd782a2e09d87d75fa75be4273f5afae6e912b8/analysis/ （ファイルヘッダーを見る限り Jpeg であるため上記結果は誤検出と思われる） 
3	EMS_59624.zip	MD5: 1472D27F9CA8BB6D3FED695540D72E99 SHA-1: 6C795214C857617147EF482FEEE5DCBC434A0646 展開すると[EMS の小包が受信されません STRCS.PDF](RLO あり) 正しいファイル名は[EMS の小包が受信されません STFDP.SRC]
3	EMS の小包が受信されません STRCS.PDF	MD5: 84EDC45010DA0D24F00C191A22069385 SHA-1: 8501659B87E5909656BE9E83B18A62781F523F3C 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 の小包が受信されません STRCS.PDF]。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[112.exe]と[post.png]

		
3	112.exe	MD5: B8B1D45EADA01FB29C86C43E58093E68 SHA-1: 7DBE0127F870906F1FFA2E7F4976AF8D74B1E496 ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/5e0d6060ac0989698d5bb8ff68e114b81af226b9616e0a1e6d7bf526090aed96/analysis/1452266935/ ■接続先ドメイン 現在不明 ■通信先 URL 現在不明 ■通信先 IP アドレス 178.126.119.16 17388/udp 77.245.113.167 17388/udp 188.227.20.184 17388/udp 46.201.221.173 17388/udp 2.62.152.103 17388/udp 85.238.100.204 17388/udp 89.178.199.94 17388/udp 94.190.4.6 17388/udp 89.146.92.198 17388/udp 178.167.108.153 17388/udp
3	post.png	MD5: 5D075617E8A9B7F4DA6E4529F2160912 SHA-1: 5A8FF5C9E79C736B161C0CC3A14B92E0573CD3DB ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/8148f496eaed8ca1415af68a63682a3f71c10a2dd6f928192a3e832d71642d62/analysis/1452267342/

日本郵便

あたらしい ふつうをつくる。

FAQs & Inquiries | S

20:24 January 08 ,2011

Detailed International Mail search result

**The item number searched is EC[redacted]
(EMS).**

Date	Status	Details	Office ZIP code	Prefecture
Dec 20 14:58	Posting/Collection		YONAGO Branch 683-8799	Tottori prefecture
Dec 20 15:42	En route		YONAGO Branch 683-8799	Tottori prefecture
Dec 21 3:13	Dispatch from outward office of exchange		OSAKA INTERNATIONAL Branch 549-8799	Osaka prefecture
Dec 22 18:20	Arrival at inward office of exchange		COVENTRY PARCELFORCE	UNITED KINGDOM
Dec 22 18:48	Awaiting presentation to customs commissioner		COVENTRY PARCELFORCE	UNITED KINGDOM
Dec 22 18:49	Awaiting presentation to customs commissioner		COVENTRY PARCELFORCE	UNITED KINGDOM
Dec 30 10:15	Departure from inward office of exchange		COVENTRY PARCELFORCE CONTAINER	UNITED KINGDOM
Dec 30 10:15	Departure from inward office of exchange		PARCELFORCE COVENTRY TRANSIT	UNITED KINGDOM
Dec 31 0:40	Processing at delivery Post Office		O22285	UNITED KINGDOM
Dec 31	Retention			UNITED KINGDOM
Jan 6 18:37	Final delivery			UNITED KINGDOM

【接続先ドメインからの調査】

項番	メモ
1	https://www.virustotal.com/ja/file/f43bf257b30b1dfb54c588c8c098daa9cc0ba073b99db89b14cae925265f2dd3/analysis/ 上記 URL のコメントタブにある別のマルウェアと接続先の URL が重複するものがある。
2	特記事項無し
3	特記事項無し