【メール基本情報】

項番	基本情報
1	送信元アドレスドメイン： paikane.com （送信元アドレスドメインが偽装されている可能性あり。送信に利用されたと思われる IP アドレスはスパム送信リストに登録されていた） 件名： 裁判所への通知 添付ファイル名： invoice_id1518959921.doc.zip 添付ファイルハッシュ値： MD5: 5EE68F4C62AC298CEC73DAE1A01157BE SHA-1: B69202DF135090A6806A78FEC32BAEF5BD7EF43E

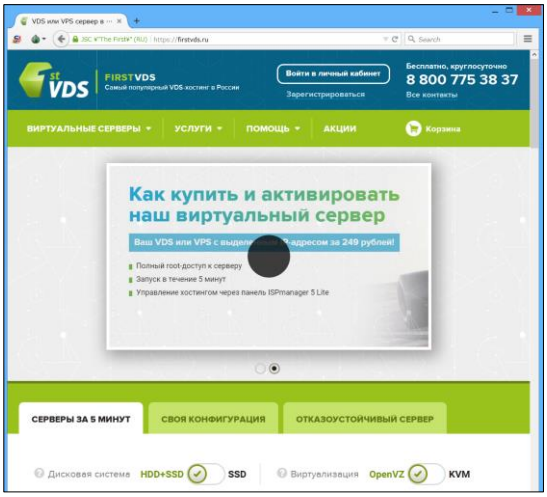
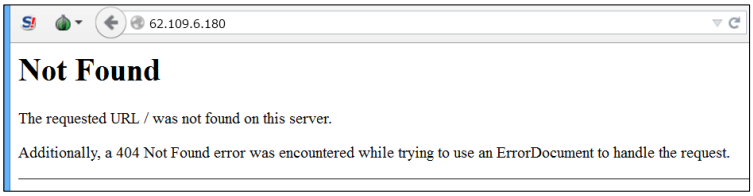
【メール本文】

項番	本文
1	拝啓 注意 – お知らせします: あなたは 2 月 20 日に裁判に出席しなければなりません。 アドレス : 〒102-8651 東京、千代田、隼町 4—2。 指定された裁判日付までに、ケースに関連する全ての書類をご用意下さい。 備考: “裁判の司法予告”は添付書類にお探しできます。 敬具 最高裁判所の書記官

【添付ファイル調査】

項番	添付ファイル	調査情報
1	DHL_44991.zip	MD5: 5EE68F4C62AC298CEC73DAE1A01157BE SHA-1: B69202DF135090A6806A78FEC32BAEF5BD7EF43E 展開すると[invoice_id1518959921.doc.js]という二重拡張子の JavaScript ファイル。
1	invoice_id1518959921.doc.js	MD5: C657D1953D6BDFD4C385081261FB1245 SHA-1: 3DD7749B01FE45842ECD9AD9B4EBF63837A80C4D ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/24c3f521b39e7246fd5988eab3f0286d4f755f950172e52a0ebe7d7bd54b76dc/analysis/1455388656/ このファイルは難読化が施されている。  上記ファイルを実行すると HTTP リクエストを送信し、マルウェアと思われるファイルをダウンロードし実行する。 HTTP リクエスト先 http://62.109.6.180/down/invoice%200000102.exe
1	invoice 0000102.exe	MD5: CC5A97E3CCD9944A9872F6F842FA3073 SHA-1: 8D54BCC02FEB5223193136509459FD475A9611E7 ■VirusTotal（検出あり） https://www.virustotal.com/ja/file/31ac87b9e1e2b0299c4f04ec81d870e87216206a5666bc98a0469e668db6054f/analysis/1455389981/ 通信先ドメイン 不明 HTTP リクエスト先 不明

【通信先 IP アドレスからの調査】

項番	メモ
1	 上記 IP アドレスはロシアの IP アドレスであること判明。 ホスト名のドメインにアクセスしたところ下記のサイトへとリダイレクトされた。  通信先である IP アドレスに接続したところ下図のようにトップページは存在しなかった。  また、Javascript ファイルの通信先 URL のディレクトにアクセスしたところ下図にようにマルウェアと思われるファイルの最終更新日時が判明した。