Gli attacchi spam di febbraio sono stati contraddistinti da allegati dannosi arrivati via mail, nel periodo di San Valentino, da parte di donne che fingevano di voler fare nuove amicizie. Alcuni messaggi promettevano foto esplicite in archivi allegati cercando cosi di convincere i destinatari dei messaggi ad aprirli. Oltre a questo tipo di messaggi, ci sono state una serie di mailing di massa più convenzionali che fingevano false notifiche di noti siti di social networking, tra cui Facebook. Lo rende noto un report di Kaspersky.

La percentuale di spam presente nel traffico di posta elettronica a febbraio è aumentata di 4,2 punti rispetto al mese precedente con una media del 69,9% - 1.2 punti percentuali in meno invece rispetto al febbraio 2013. La Cina (23%) è ritornata in cima alla classifica, seguita dagli USA (19,1%) e dalla Corea del Sud (12,8%). Lo spam nocivo di febbraio, che aveva come tema principale l'amore, è stato dominato da Trojan. Infatti i mailing di massa dei cybercriminali che avevano come obiettivo sprovveduti utenti usavano un Trojan-Dropper. Questo Trojan installava due programmi dannosi sul sistema - uno spyware che rubava tutti i file di documenti (*docx, xlsx*, *PDF...) dal computer e li inviava a una mailbox specifica e un altro IRC-bot/worm chiamato Shitstorm che poteva effettuare attacchi DDoS a siti web e diffondere copie di se stesso tramite MSN e servizi P2P. Se i destinatari rispondevano a questo tipo di email, il loro computer poteva facilmente diventare parte di una botnet. Oltre allo spyware Trojan, lo spam nocivo di febbraio includeva ransomware - un tipo di malware che blocca il computer dell'utente per poi chiedere del denaro per sbloccarlo. Le foto esplicite si sono rivelate dei programmi dannosi e tra loro c'era la backdoor Andromeda che permetteva ai criminali informatici di controllare segretamente un computer compromesso. Un altro programma dannoso utilizzato imitava le notifiche dei principali siti di social networking. I messaggi ingannavano il destinatario utilizzando come mittente Facebook e li informavano che dalla loro ultima visita c'erano stati diversi aggiornamenti dei news feed degli amici cosi da essere indotti ad aprire l'archivio in allegato per saperne di più. L'archivio conteneva invece la backdoor appartenente alla famiglia Andromeda. Nel frattempo, i truffatori 'nigeriani' non hanno potuto lasciarsi sfuggire l'occasione di sfruttare la delicata situazione politica che si è venuta a determinare in Ucraina, ed i tragici avvenimenti che si sono verificati, per estorcere del denaro. Citando alcune storie di turisti derubati di tutti i loro soldi a Kiev, richiedevano assistenza finanziaria.
25 marzo 2014