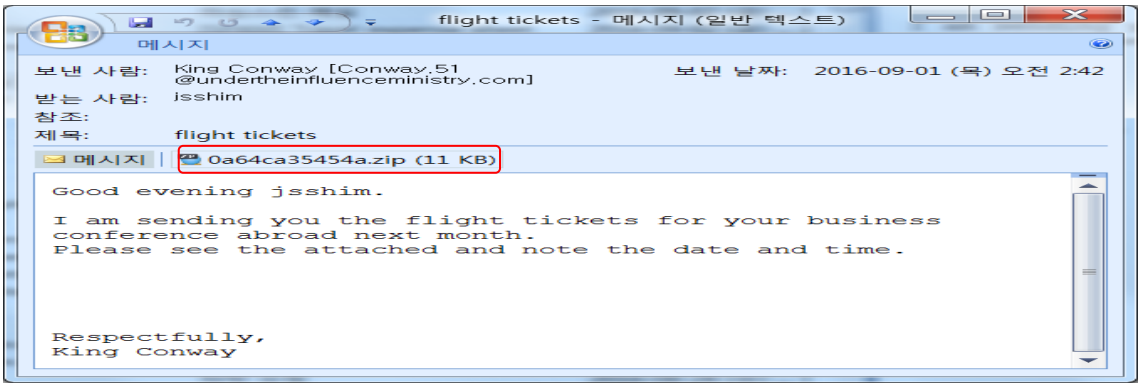
Today's Ransomware

Aug. 31 ~ Sep. 7. 2016

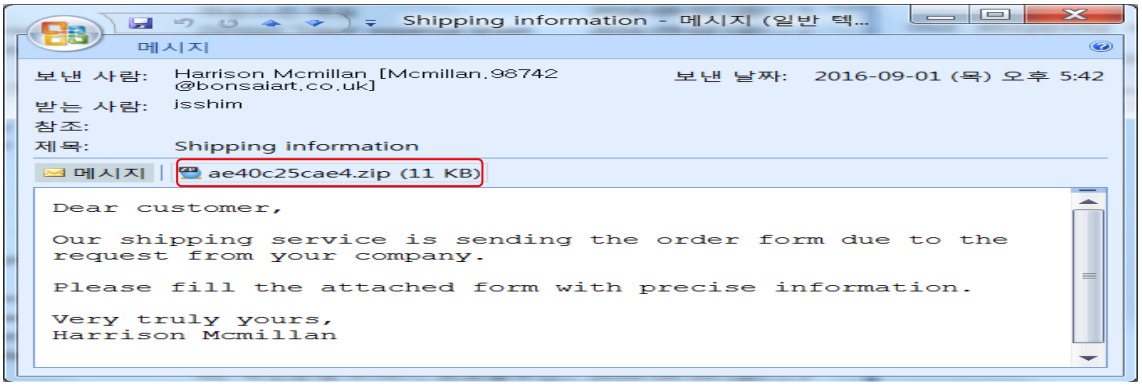
1. rundll32 type Ransomware

- **3e387e94368.zip => 2DC3CC21_bank_transactions.js**

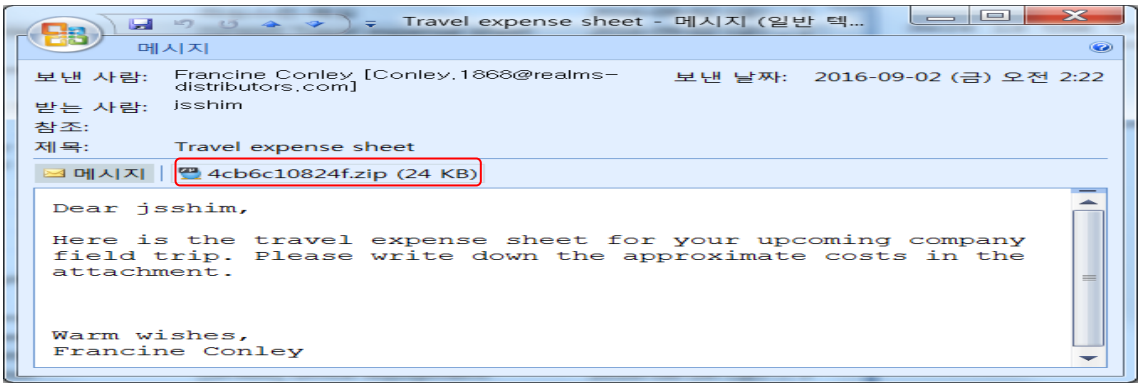
- **0a64ca35454a.zip => 1D05F09E_flight_tickets.js**



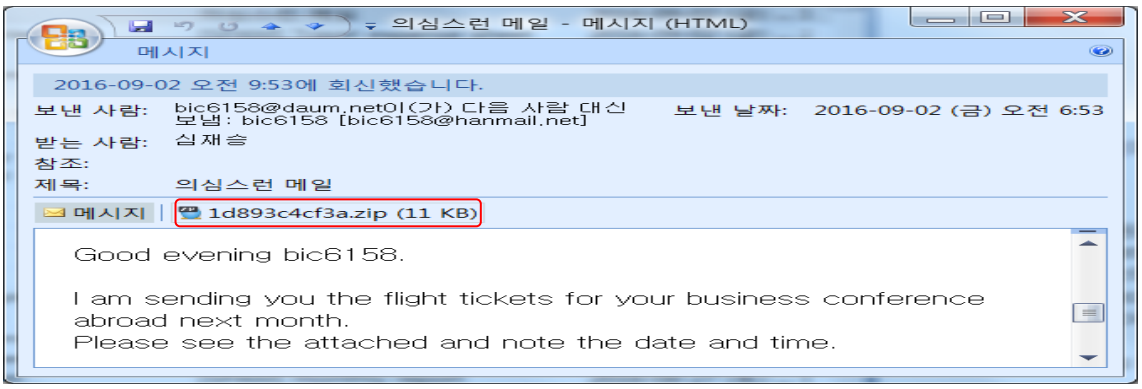
- **ae40c25cae4.zip => 2F8D30AD_shipping_service.js**



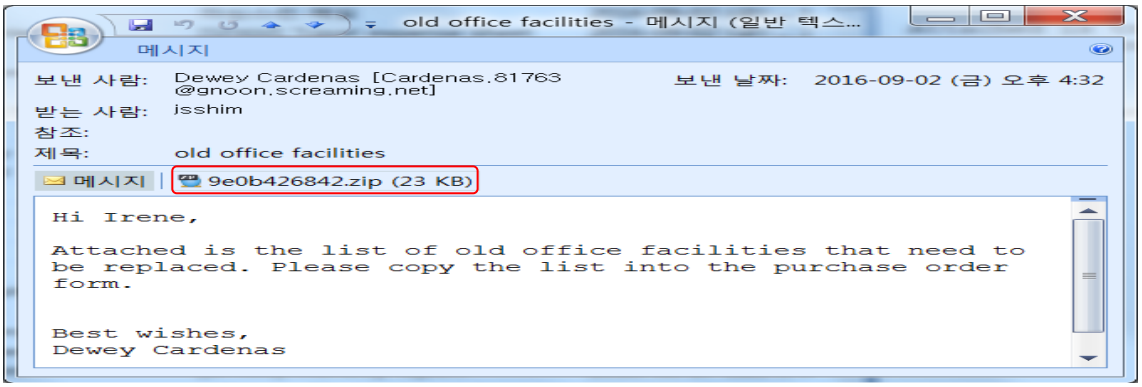
- 4cb6c10824f.zip => Travel_expense_sheet_85C2C83B.js



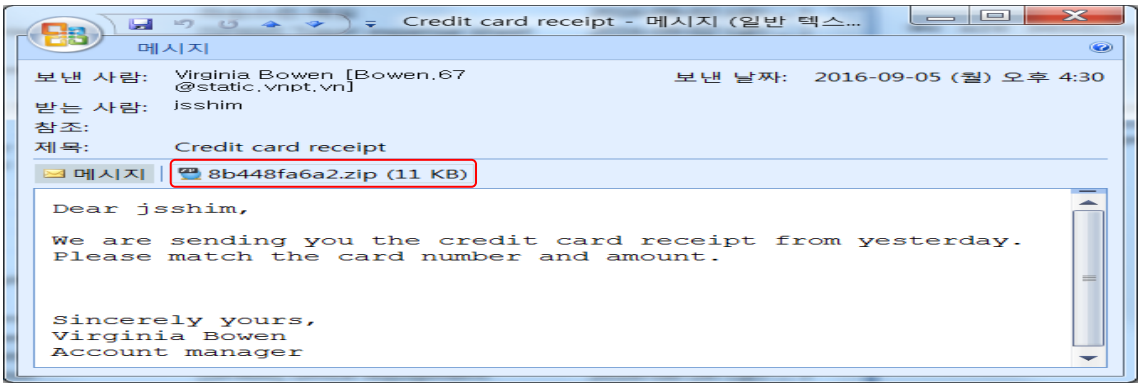
- 1d893c4cf3a.zip => 255B8AF9_flight_tickets.js



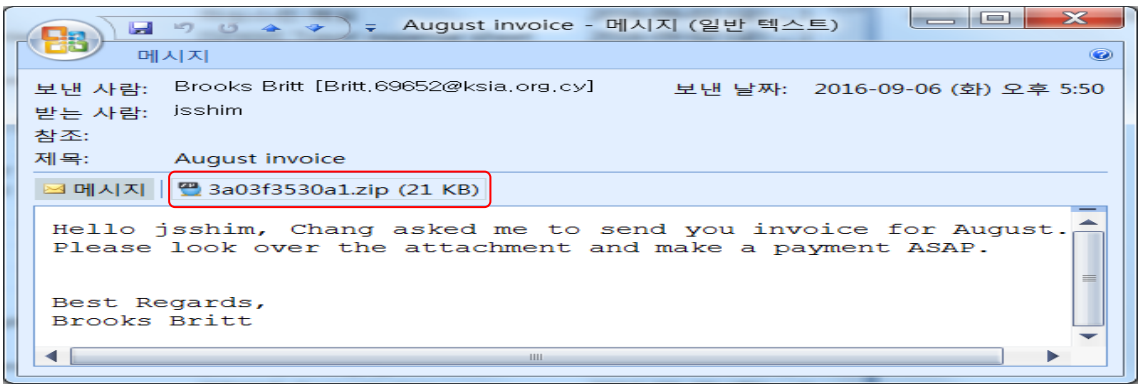
- 9e0b426842.zip => office_facilities_0FC93CC1.js



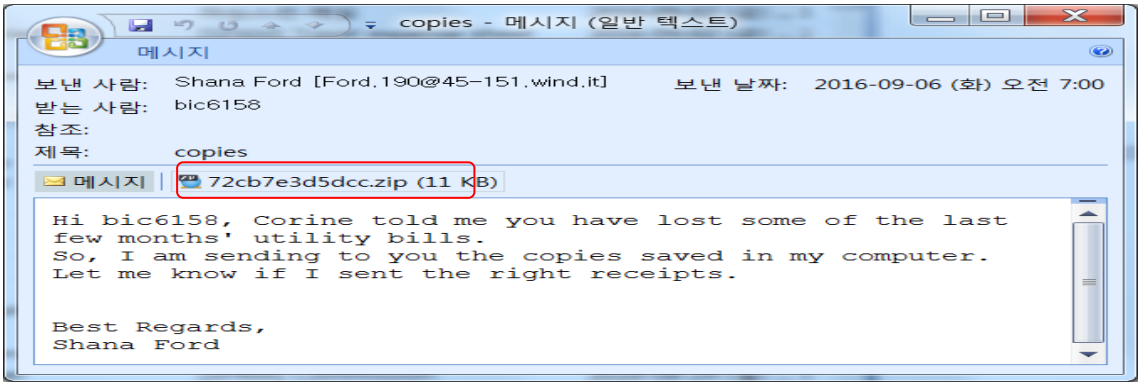
- 8b448fa6a2.zip => credit_card_receipt_C15ADE63.js



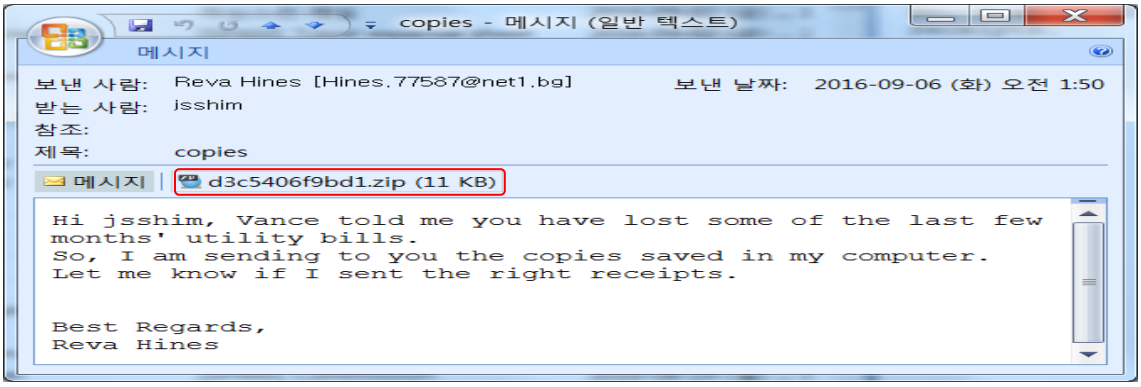
- 3a03f3530a1.zip => August_invoice 6EAC151A. pdf~.js



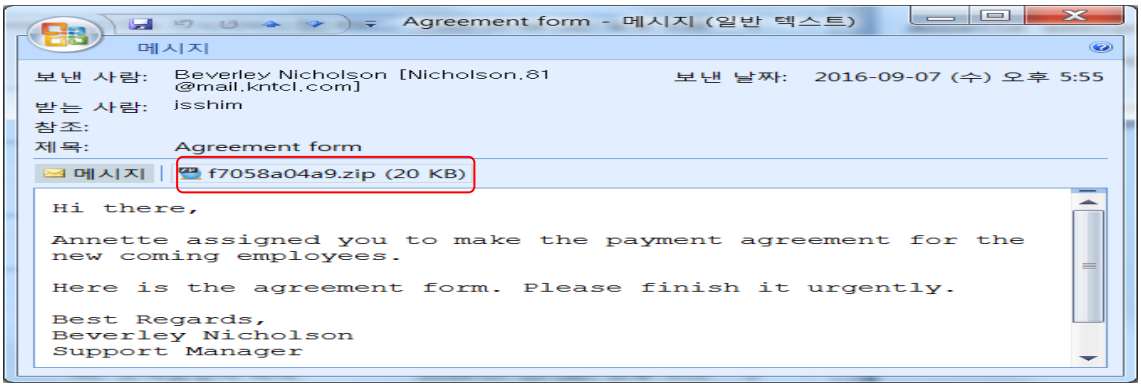
- 72cb7e3d5dcc.zip => utility_bills_copies E66A49E2.js



- **d3c5406f9bd1.zip => utility_bills_copies E66A49E2.js**



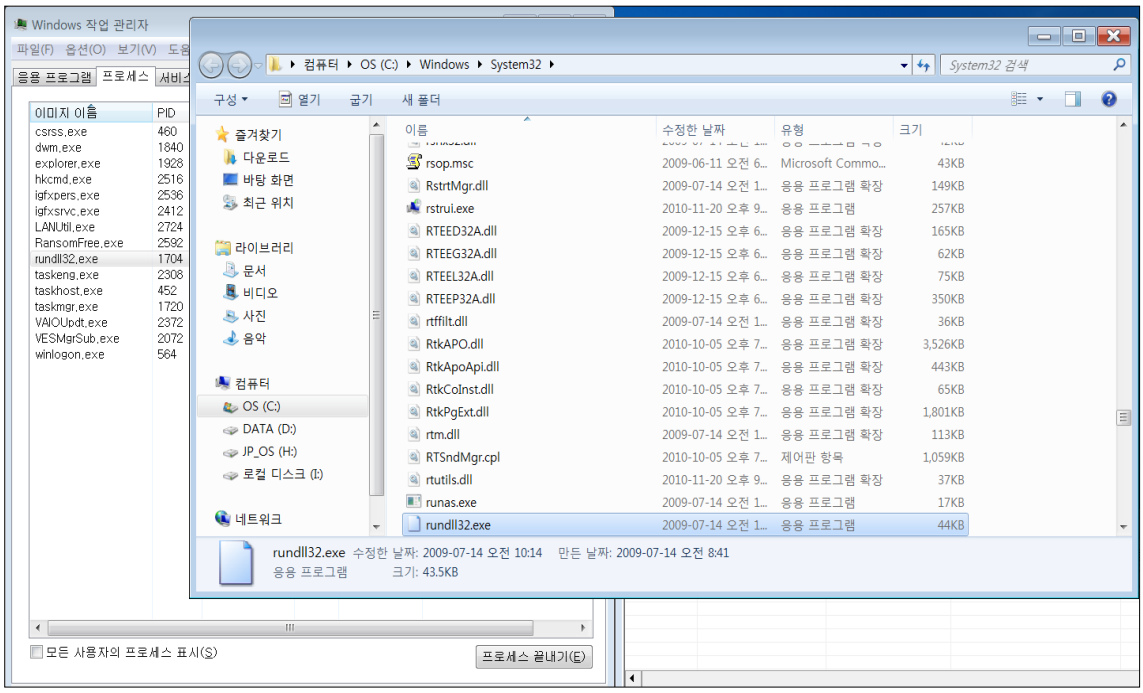
- **f7058a04a9.zip => 2DC14A55 agreement_form_doc.js**



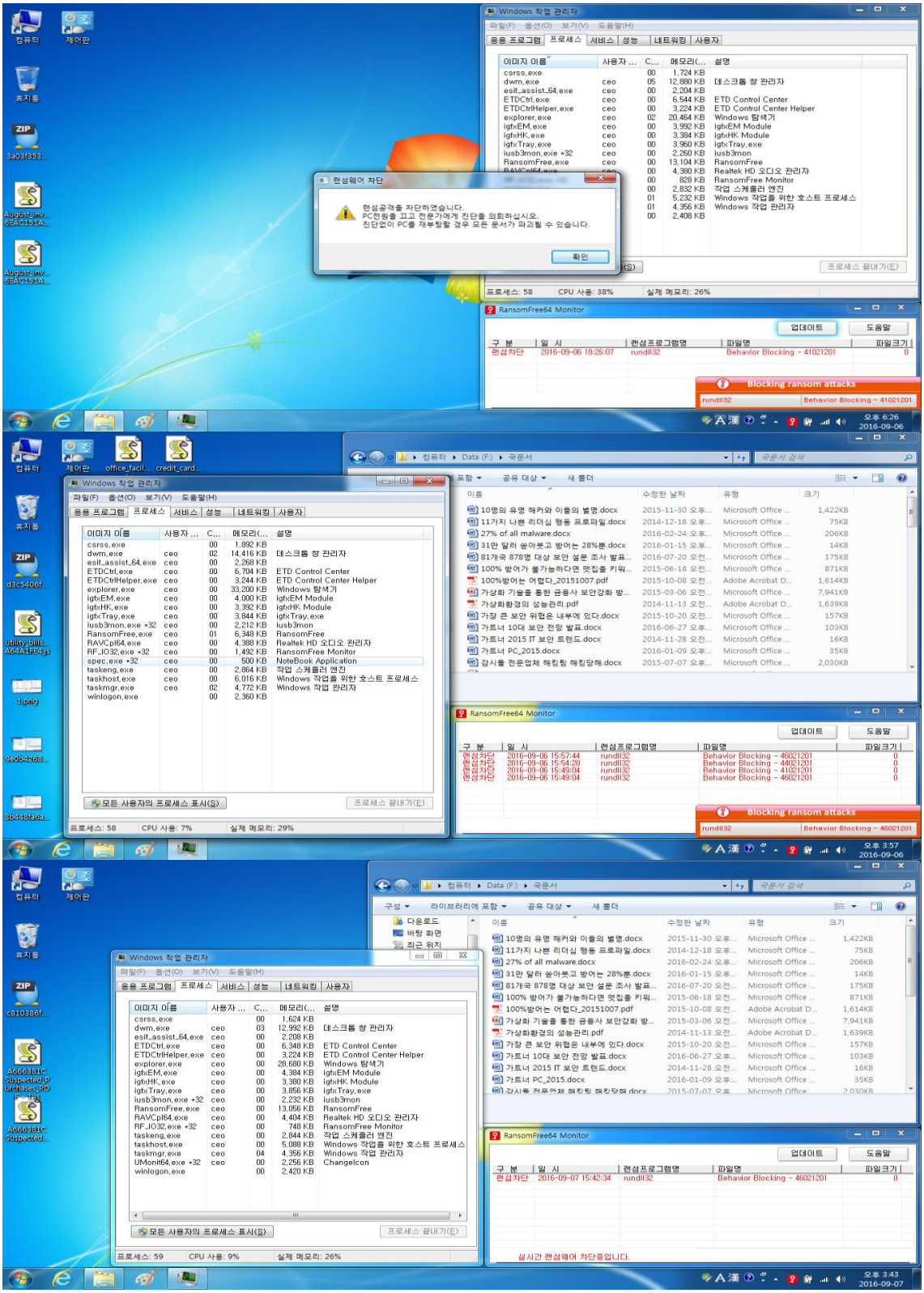
2. Type of Ransomware = zepto

3. Name of process

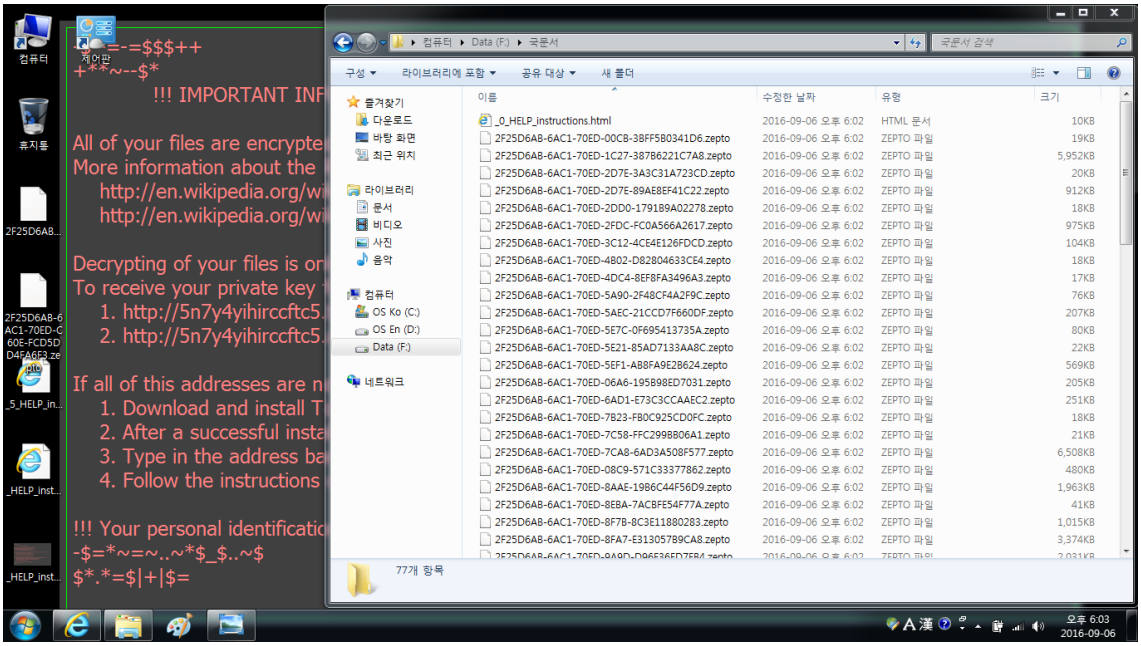
- OS(C:)/Windows/System32/rundll32.exe



4. Blocked by RansomFree®



5. Victim without TrojanCut®



☞ RansomFree® is all blocking in real-time even the unknown ransomware.