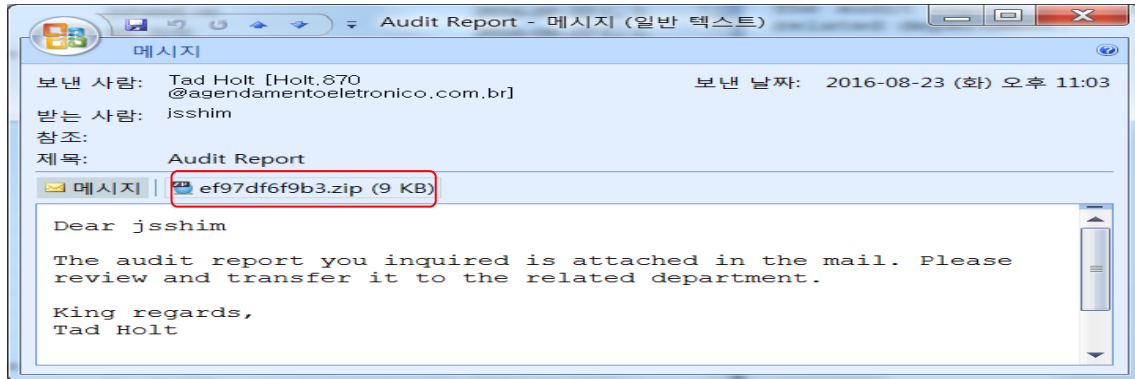


# Today's Ransomware

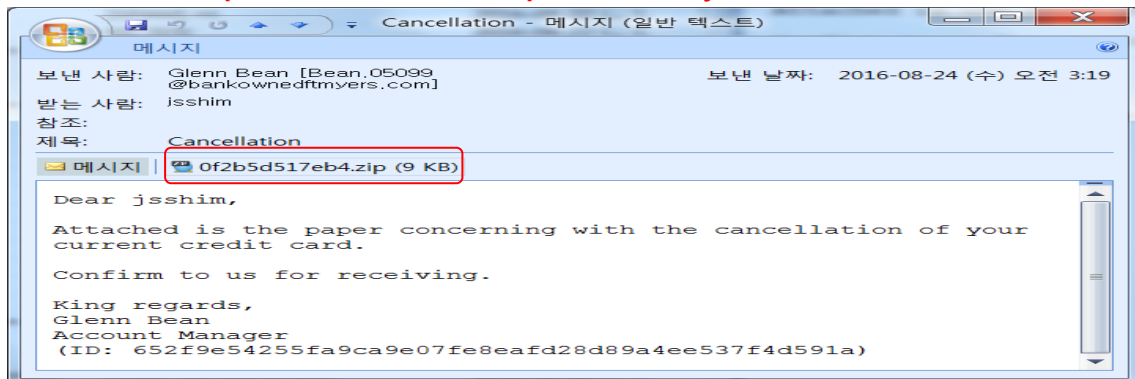
Aug. 30, 2016

## 1. rundll32 type Ransomware

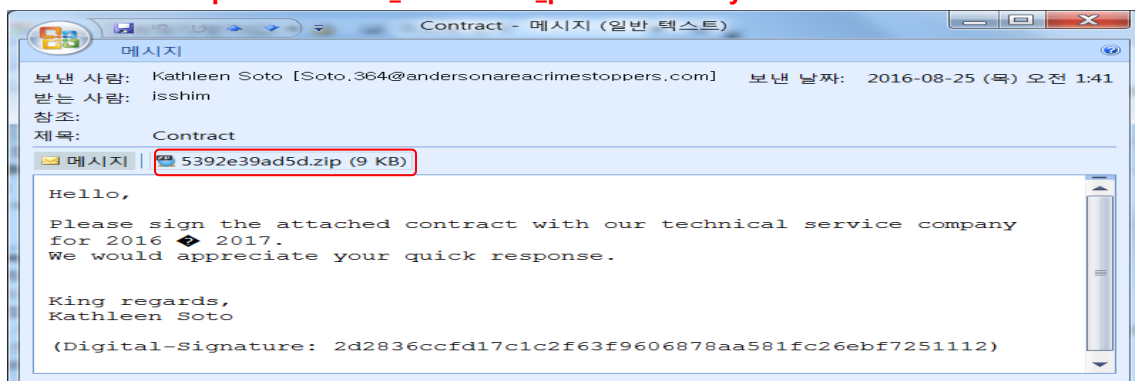
- ef97df6f9b3.zip => audit report 1be2b342.js



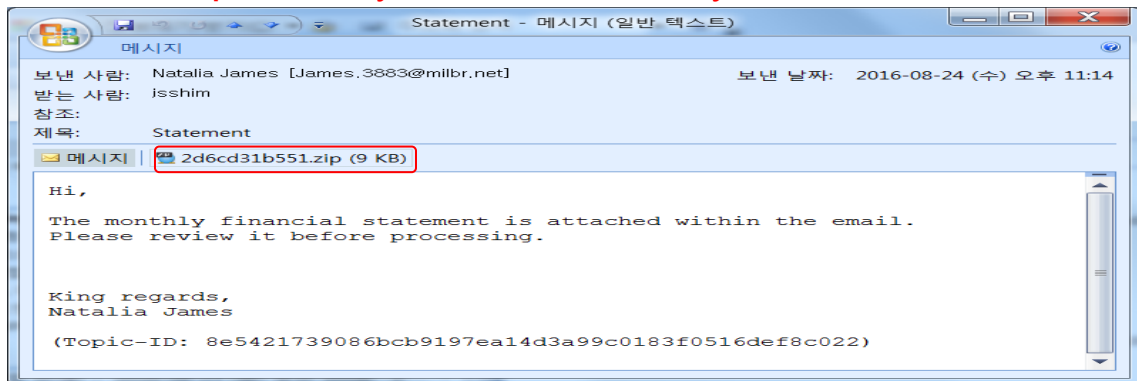
- 0f2b5d517eb4.zip => card\_cancellation\_pdf 3ae5c5d1.js



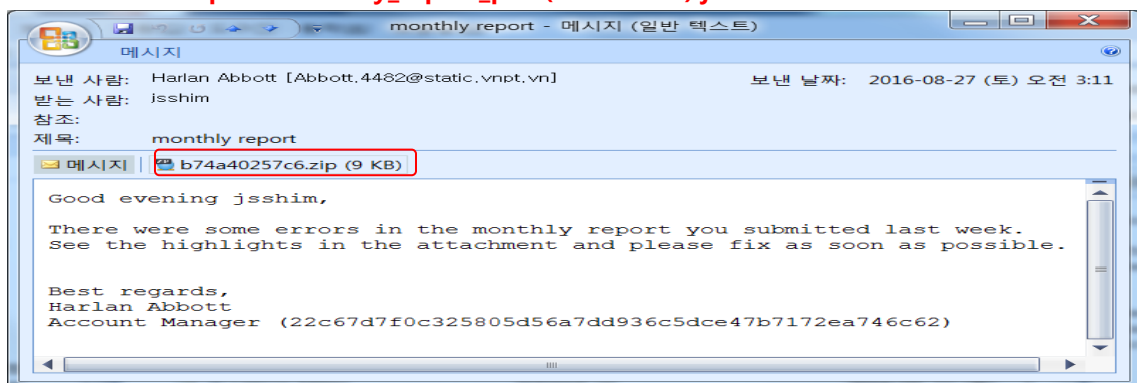
- 5392e39ad5d.zip => contract\_2016-2017\_pdf ~2ffa0f02.js



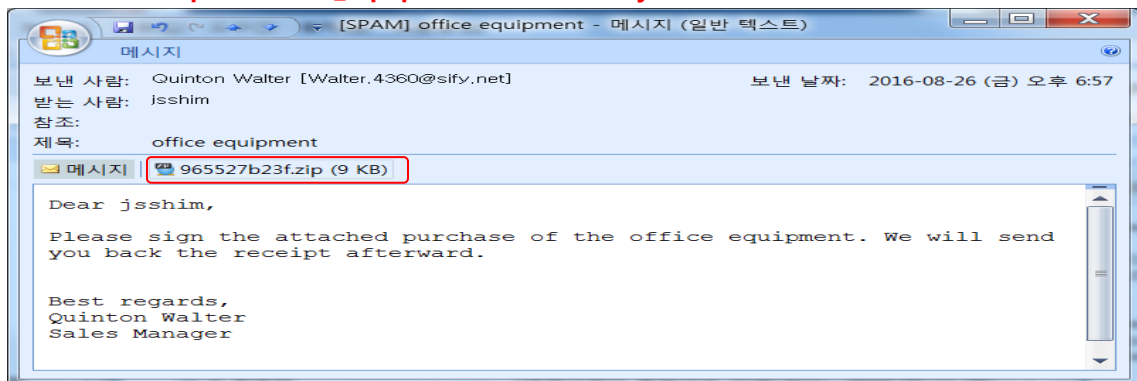
- 2d6cd31b551.zip => monthly\_financial\_scan e546c0d0.js



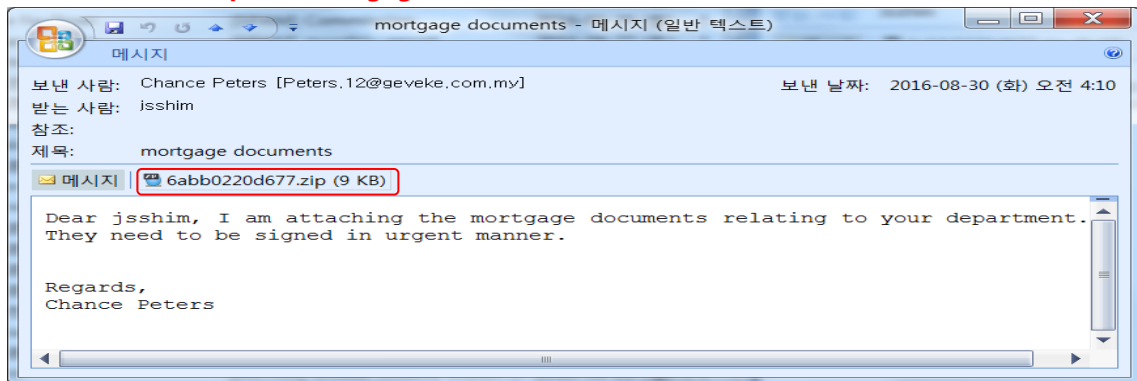
- b74a40257c6.zip => monthly\_report\_pdf (`2c3d1d40).js



- 965527b23f.zip => office\_equipment ~3f50b1b6.js



- 6abb0220d677.zip => mortgage\_documents.b0f3e480.wsf



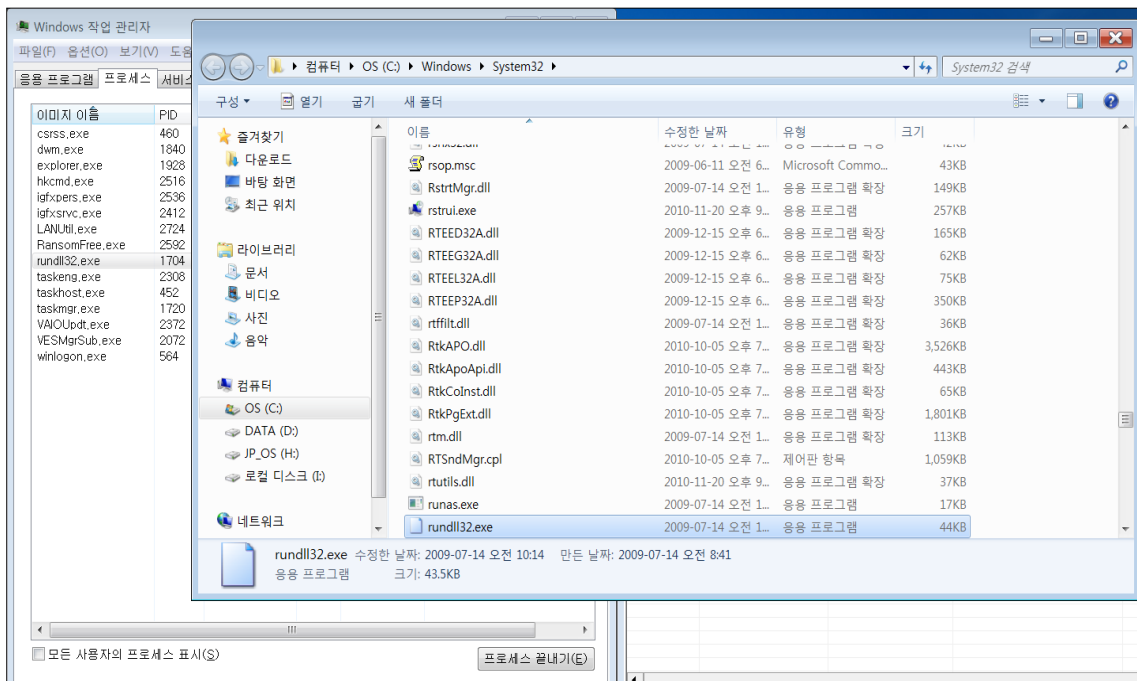
- c94fab15a3.zip => commission\_xls (~98ca4c3d).js



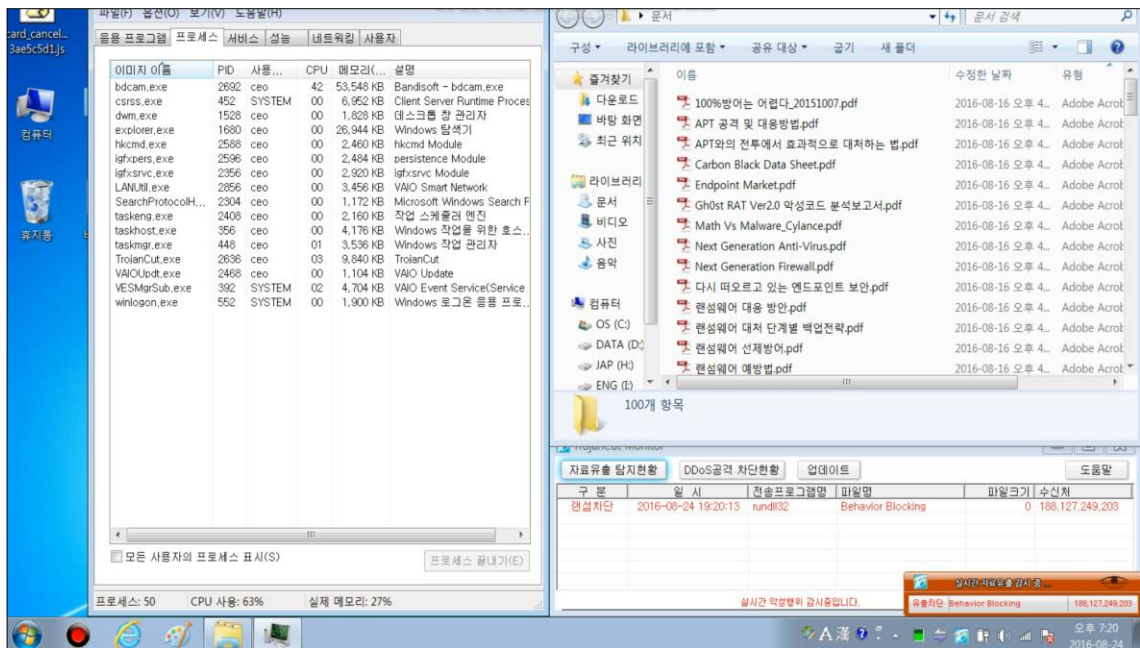
2. Type of Ransomware = zepto

3. Name of process

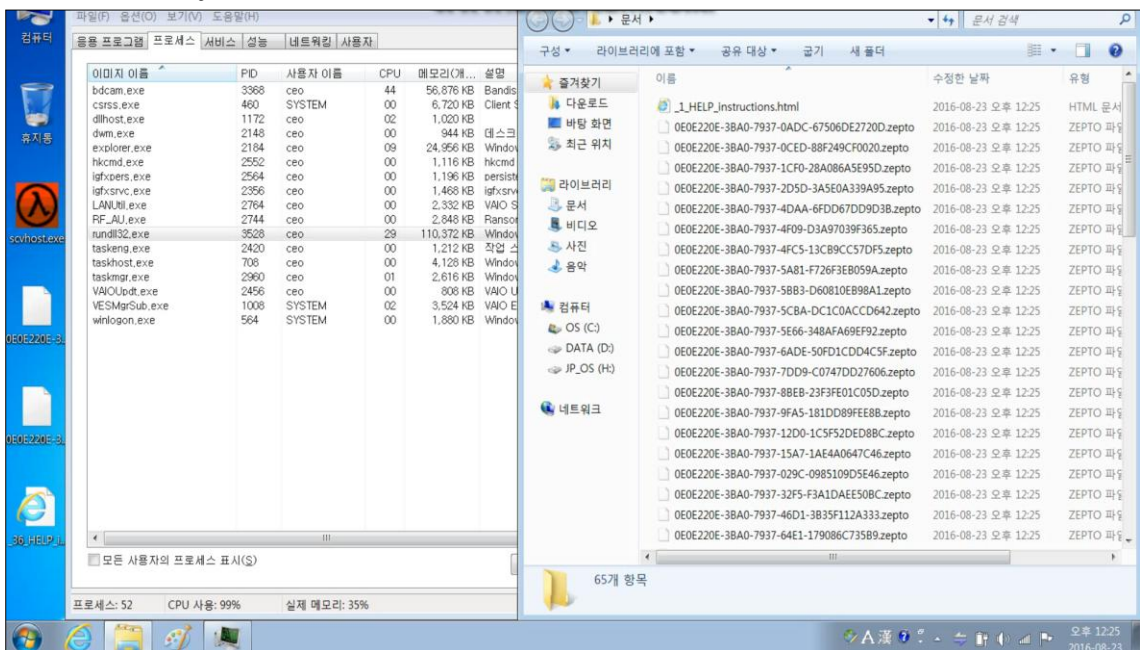
- OS(C:)/Windows/System32/rundll32.exe



#### 4. Blocked by TrojanCut®



#### 5. Victim without TrojanCut®



☞ You can see that TrojanCut® is blocking in real-time even the unknown ransomware.