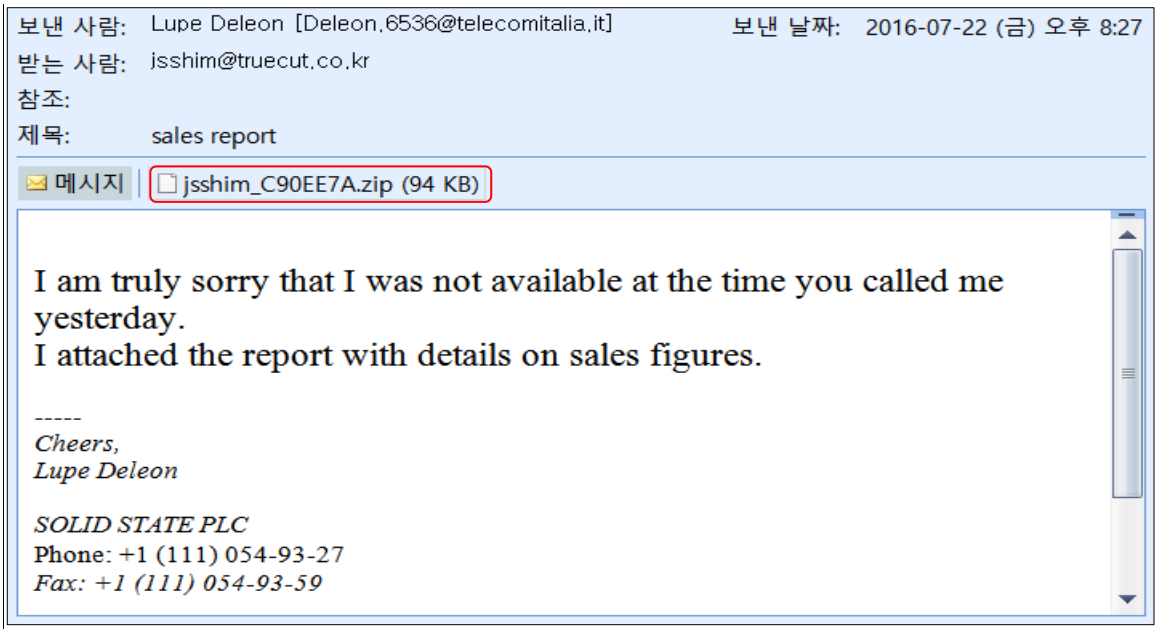
Today's Ransomware

Jul. 25, 2016

1. I've received two ransomware.

- jsshim_C90EE7A.zip => sales report 4c4.wsf

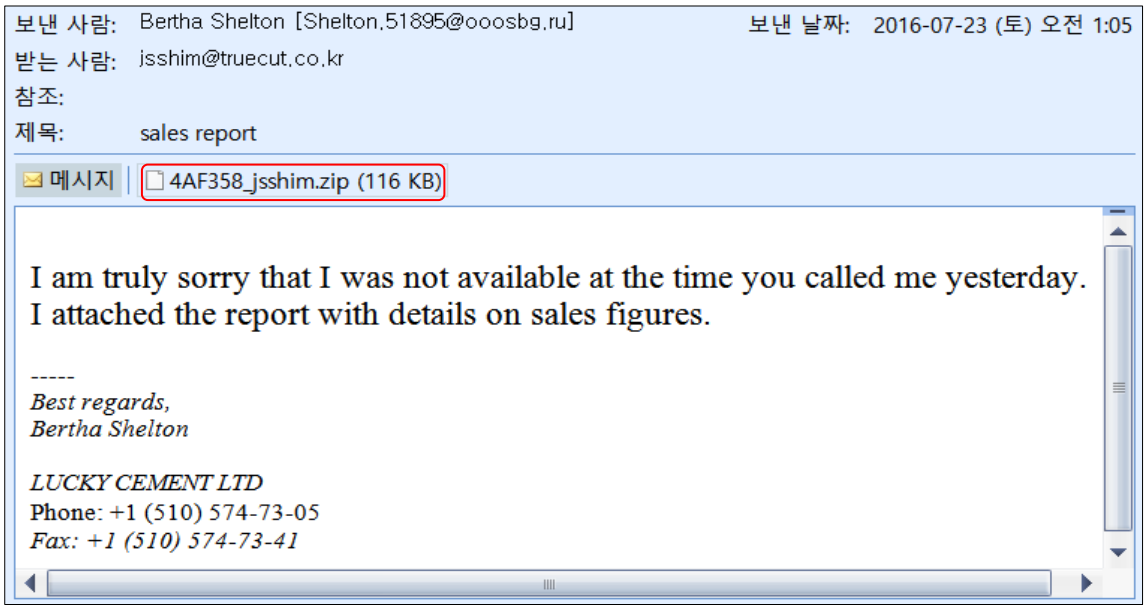

보낸 사람: Lupe Deleon [Deleon.6536@telecomitalia.it] 보낸 날짜: 2016-07-22 (금) 오후 8:27
받는 사람: jsshim@truecut.co.kr
참조:
제목: sales report
메시지 | jsshim_C90EE7A.zip (94 KB)

I am truly sorry that I was not available at the time you called me yesterday.
I attached the report with details on sales figures.

Cheers,
Lupe Deleon

SOLID STATE PLC
Phone: +1 (111) 054-93-27
Fax: +1 (111) 054-93-59

- 4AF358_jsshim.zip => sales report a67.wsf


보낸 사람: Bertha Shelton [Shelton.51895@ooosbg.ru] 보낸 날짜: 2016-07-23 (토) 오전 1:05
받는 사람: jsshim@truecut.co.kr
참조:
제목: sales report
메시지 | 4AF358_jsshim.zip (116 KB)

I am truly sorry that I was not available at the time you called me yesterday.
I attached the report with details on sales figures.

Best regards,
Bertha Shelton

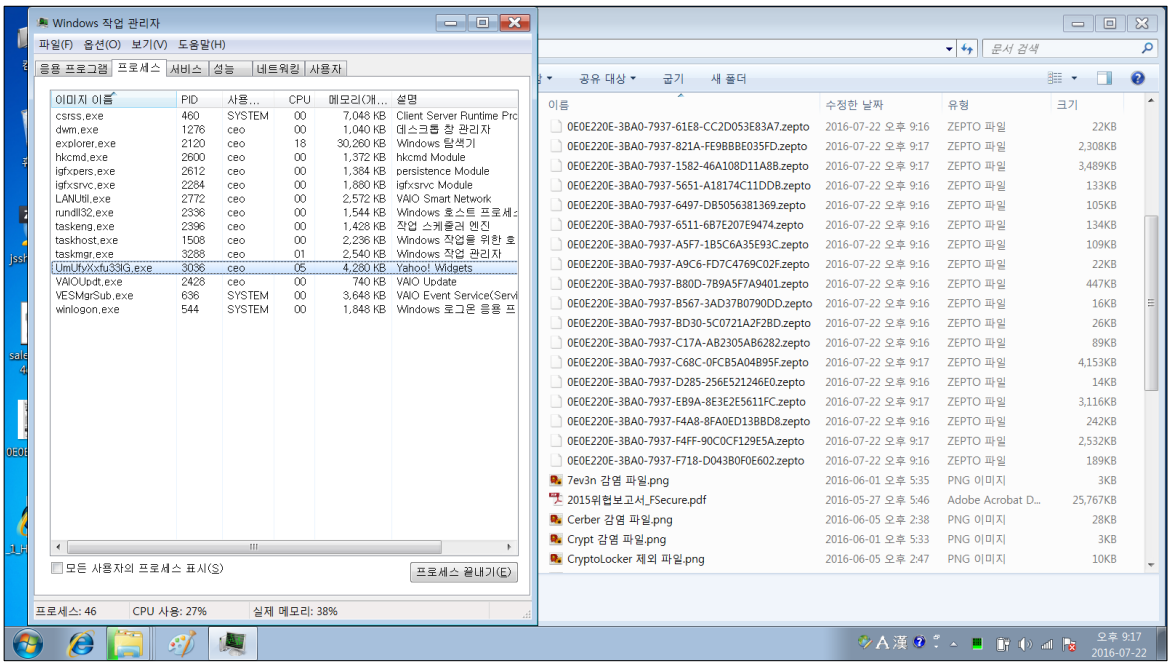
LUCKY CEMENT LTD
Phone: +1 (510) 574-73-05
Fax: +1 (510) 574-73-41

2. Victim under attack

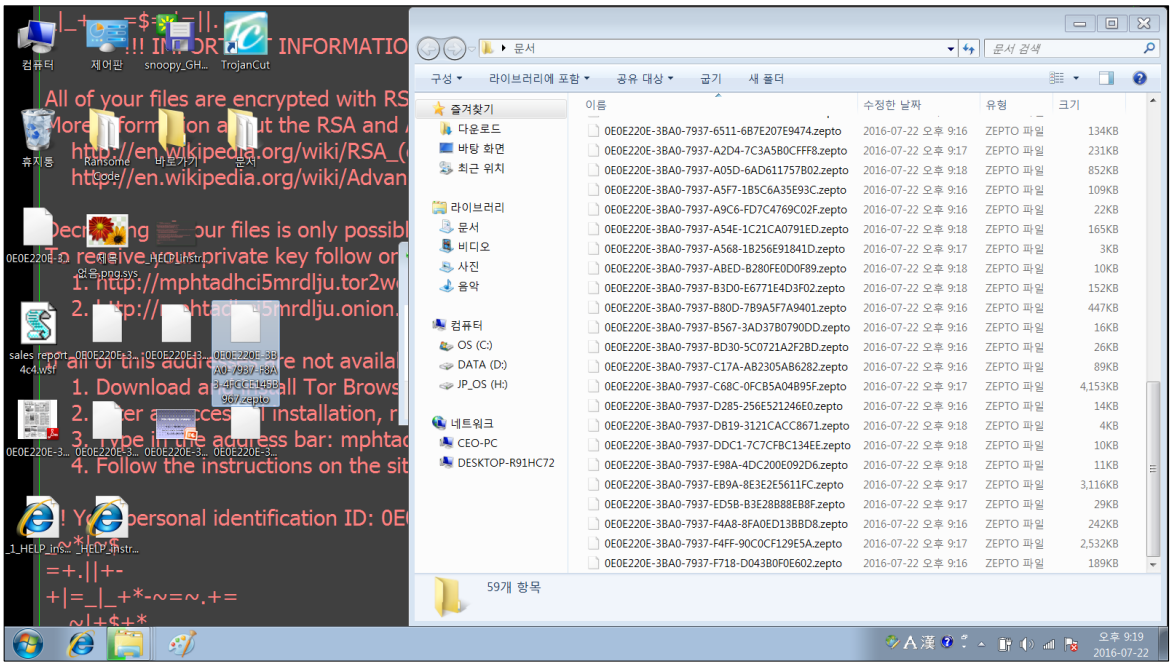
- **jsshim_C90EE7A.zip**

C:₩login account₩AppData₩Local₩Temp₩UmUfyXxfu33IG.exe

Phase 1 : Files are being encrypted under ransom attack.



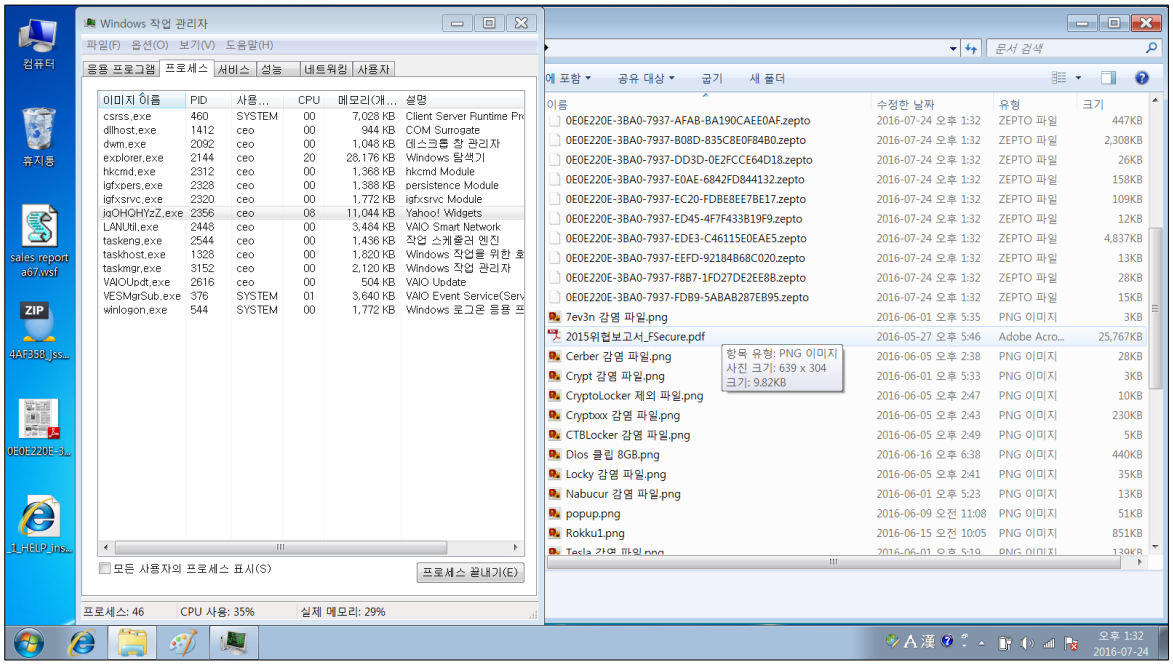
Phase 2 : Attack is over, the screen has changed with the warning message.



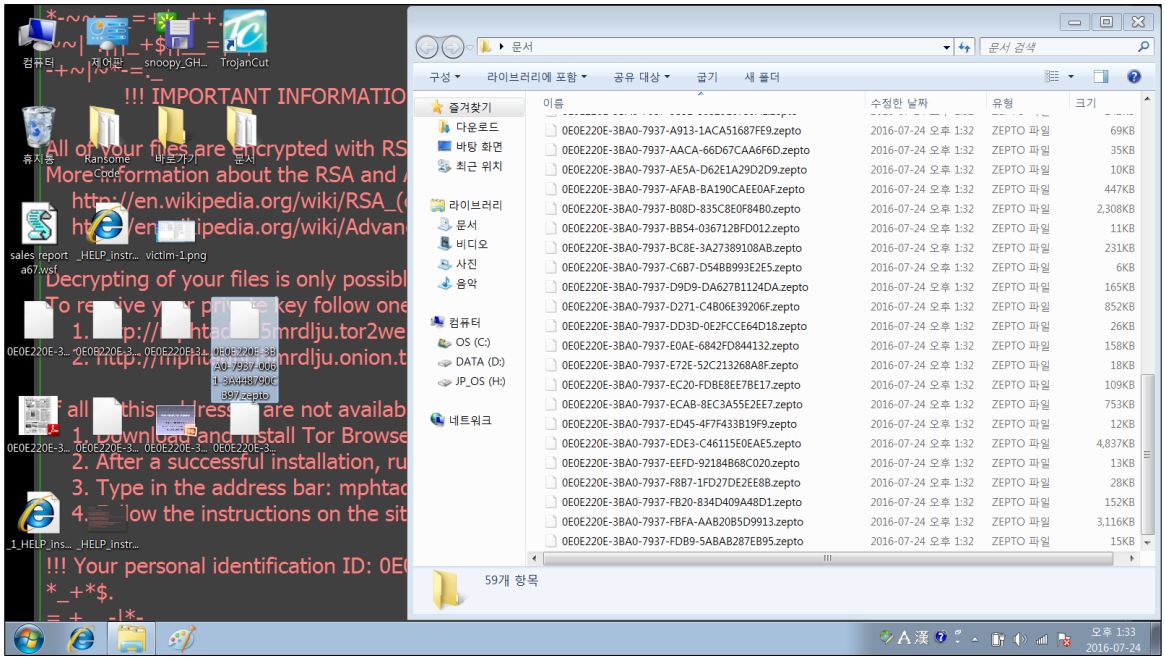
- 4AF358_jsshim.zip

  C:₩login account₩AppData₩Local₩Temp₩jqOHQHYzZ.exe

Phase 1 : Files are being encrypted under ransom attack.

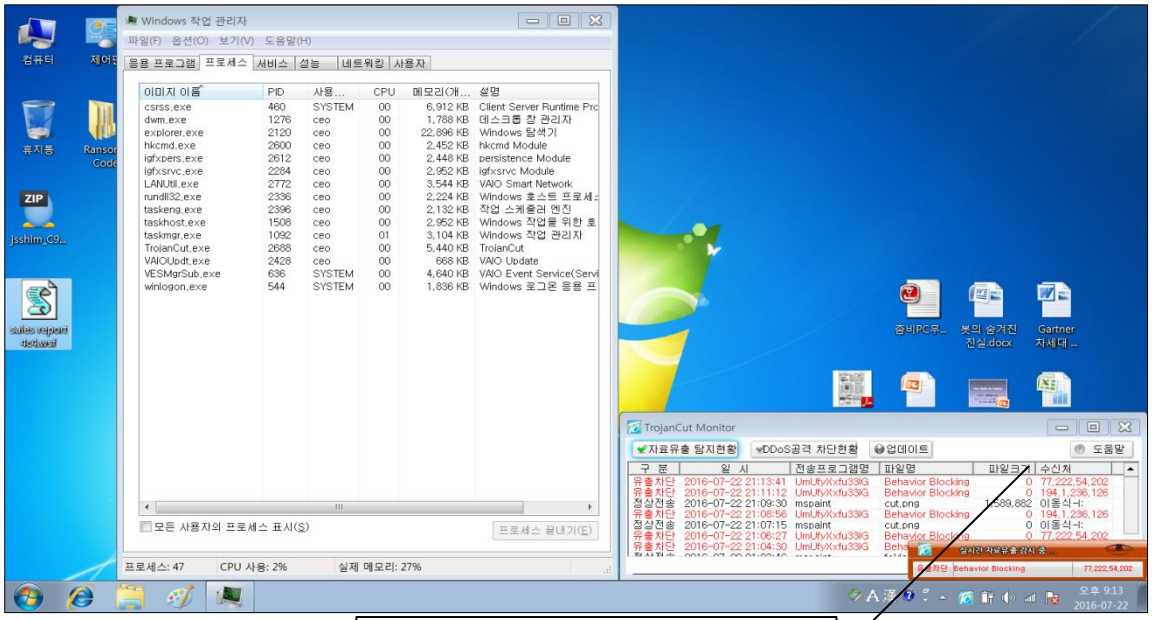


Phase 2 : Attack is over, the screen has changed with the warning message.



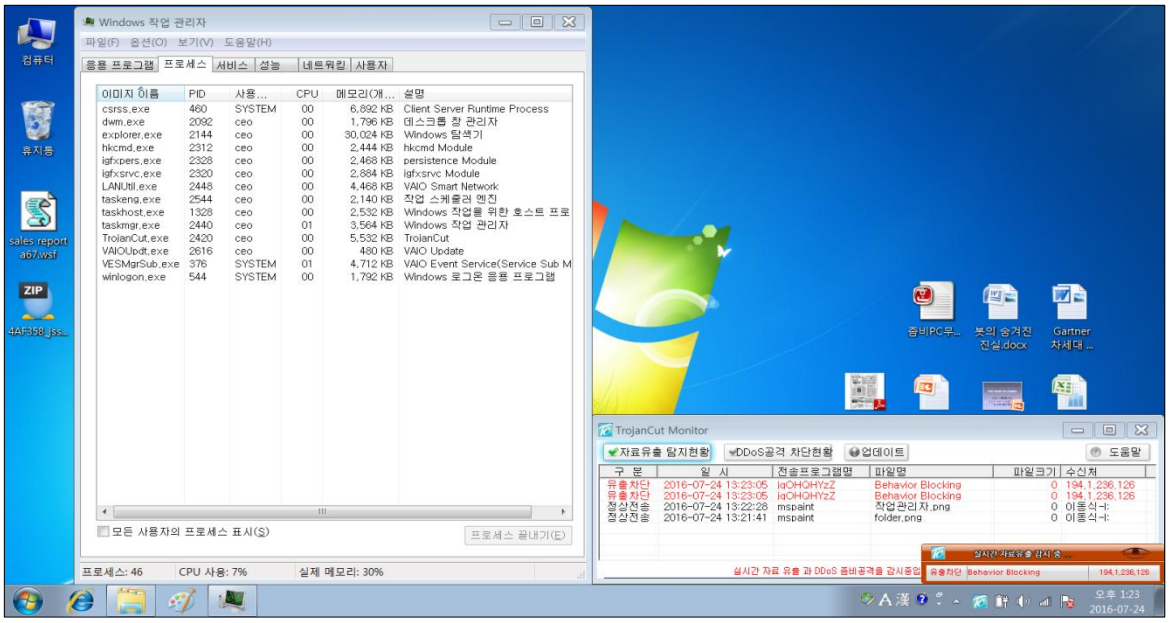
3. Blocking by RansomFree®

- jsshim_C90EE7A.zip



As you see the above,
C&C server is changing all the time.
77.222.54.202 RUSSIA
194.1.236.126 RUSSIA

- 4AF358_jsshim.zip



☞ TrojanCut® is blocking in real-time until the unknown ransomware.