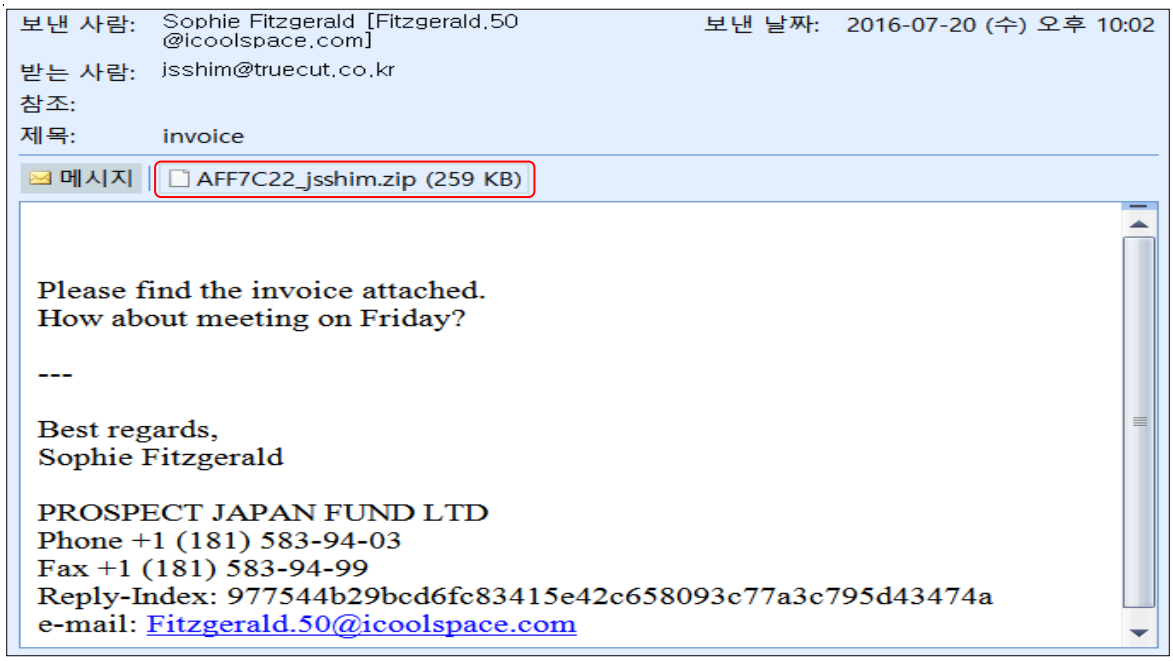
Today's Ransomware

Jul. 21, 2016

1. I received two email which contains ransomware today.

   - **AFF7C22_jsshim.zip =>INV000 1c35.js**
   - **jsshim_DF6FF66.zip =>INV000 0e8.js**



보낸 사람: Sophie Fitzgerald [Fitzgerald.50@icoolspace.com]
보낸 날짜: 2016-07-20 (수) 오후 10:02
받는 사람: jsshim@truecut.co.kr
참조:
제목: invoice
메시지 | AFF7C22_jsshim.zip (259 KB)

Please find the invoice attached.
How about meeting on Friday?

Best regards,
Sophie Fitzgerald

PROSPECT JAPAN FUND LTD
Phone +1 (181) 583-94-03
Fax +1 (181) 583-94-99
Reply-Index: 977544b29bcd6fc83415e42c658093c77a3c795d43474a
e-mail: Fitzgerald.50@icoolspace.com

보낸 사람: Charlene Fox [Fox.76@artisticboxes.com]
보낸 날짜: 2016-07-21 (목) 오전 3:11
받는 사람: jsshim@truecut.co.kr
참조:
제목: invoice
메시지 | jsshim_DF6FF66.zip (259 KB)

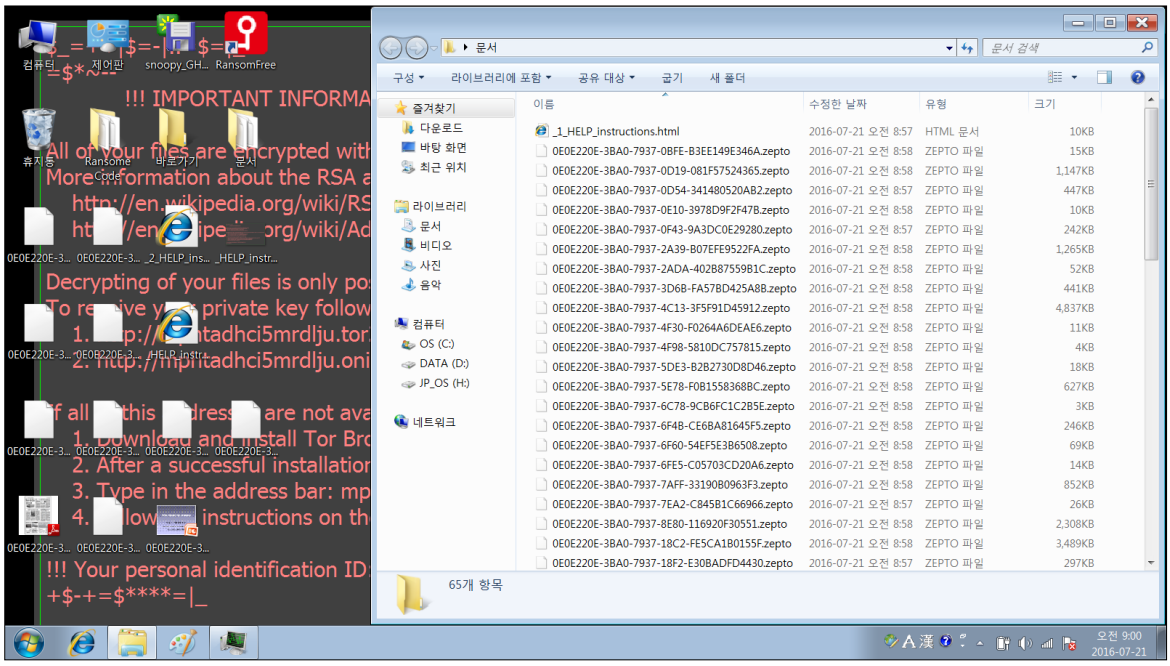
Please find the invoice attached.
How about meeting on Friday?

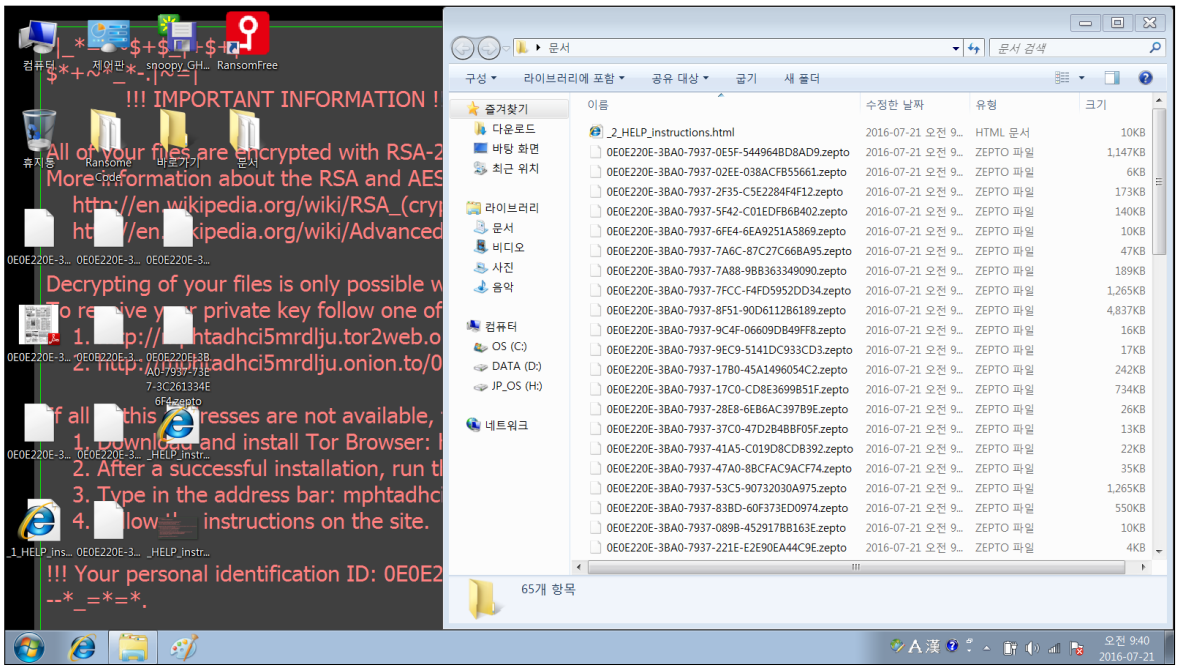
Yours faithfully,
Charlene Fox

AVARAE GLOBAL COINS
Phone +1 (176) 945-02-22
Fax +1 (176) 945-02-74
Reply-Index: 2647a99bd86ec461e1e629758281c8c0076d9e0640a80a
e-mail: Fox.76@artisticboxes.com

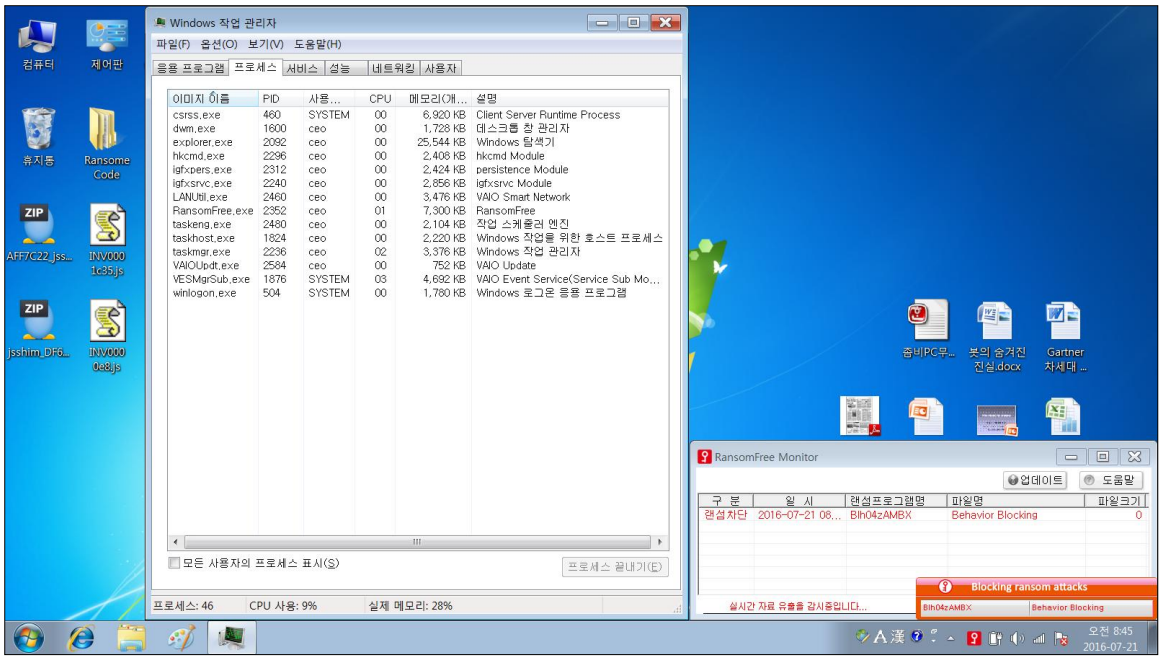
2. Victim under attack

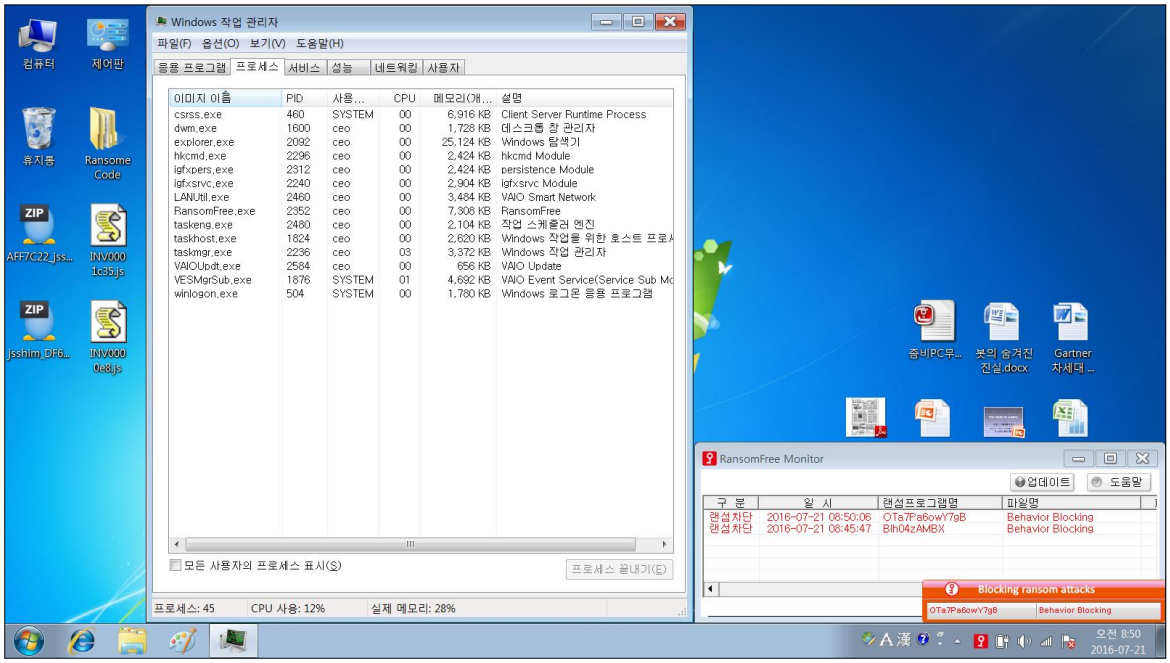
- **Process : C:₩login account₩AppData₩Local₩Temp₩BIh04zAMBX.exe**
- **Process : C:₩login account₩AppData₩Local₩Temp₩Ota7Pa6owY7gB.exe**





3. Blocking by RansomFree®





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