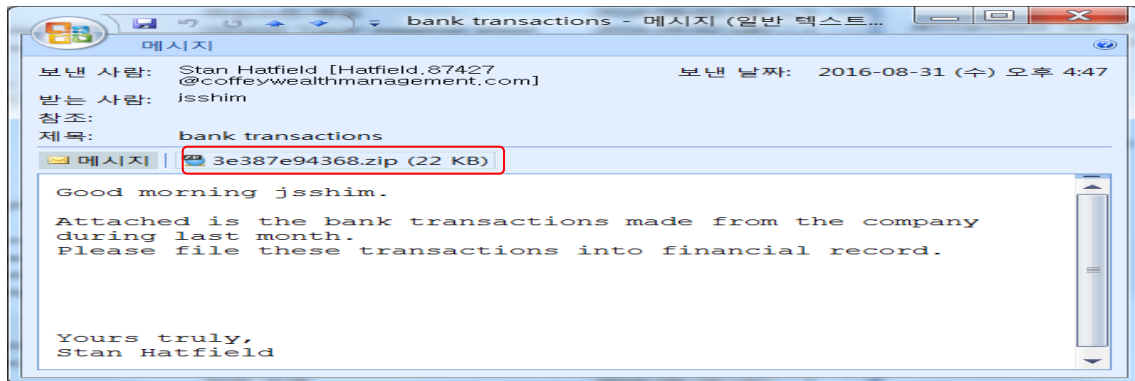


# Today's Ransomware

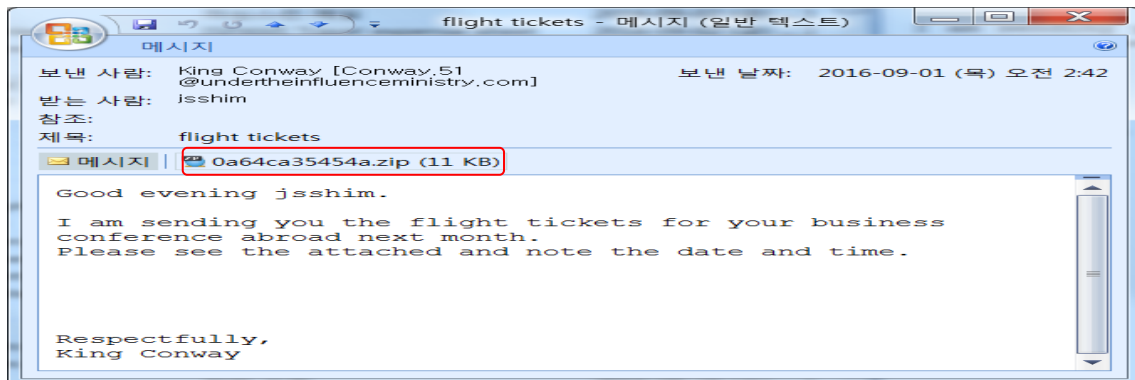
Aug. 31 ~ Sep. 7. 2016

## 1. rundll32 type Ransomware

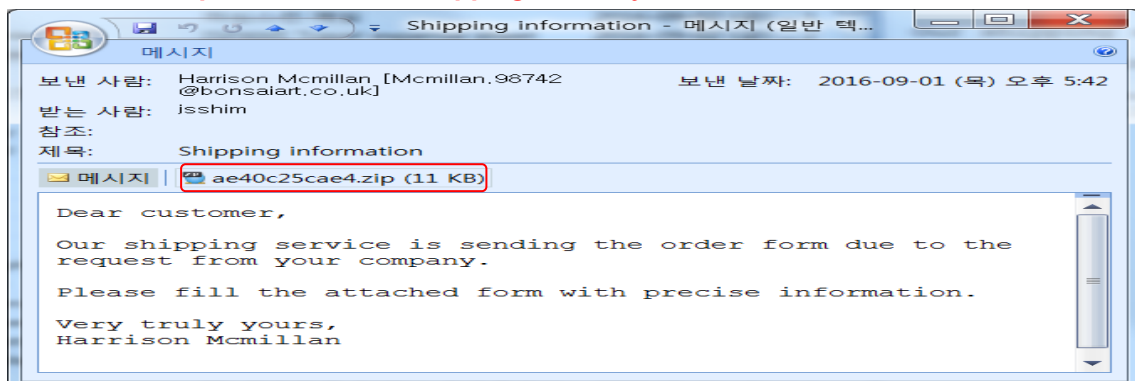
- 3e387e94368.zip => 2DC3CC21\_bank\_transactions.js



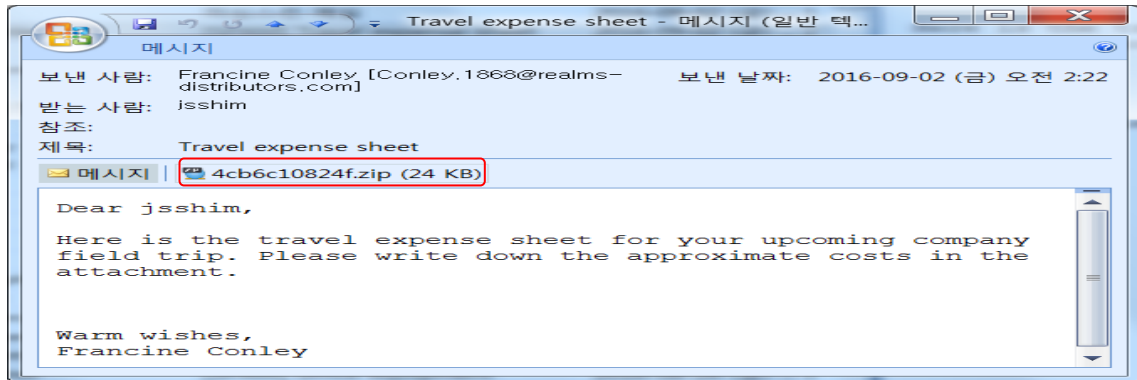
- 0a64ca35454a.zip => 1D05F09E\_flight\_tickets.js



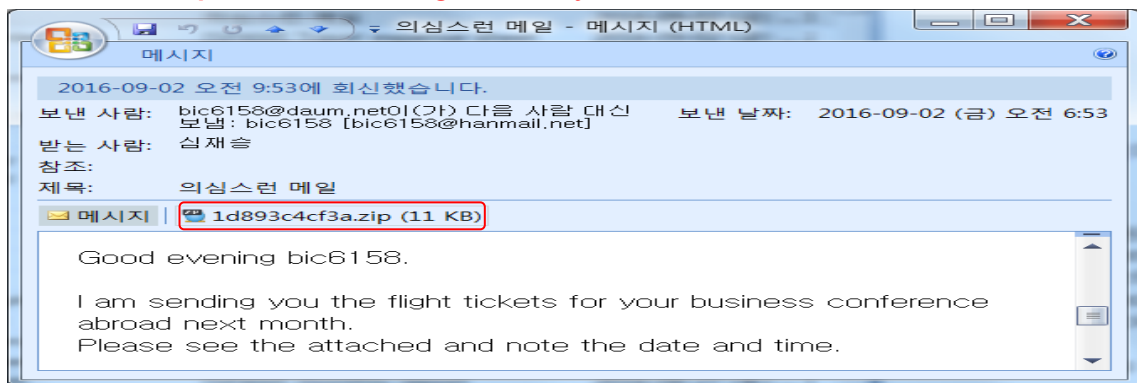
- ae40c25cae4.zip => 2F8D30AD\_shipping\_service.js



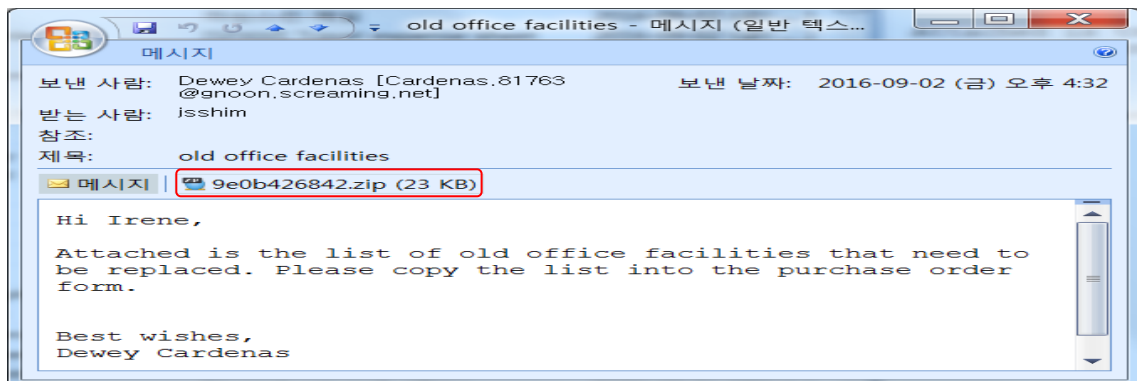
- 4cb6c10824f.zip => Travel\_expense\_sheet\_85C2C83B.js



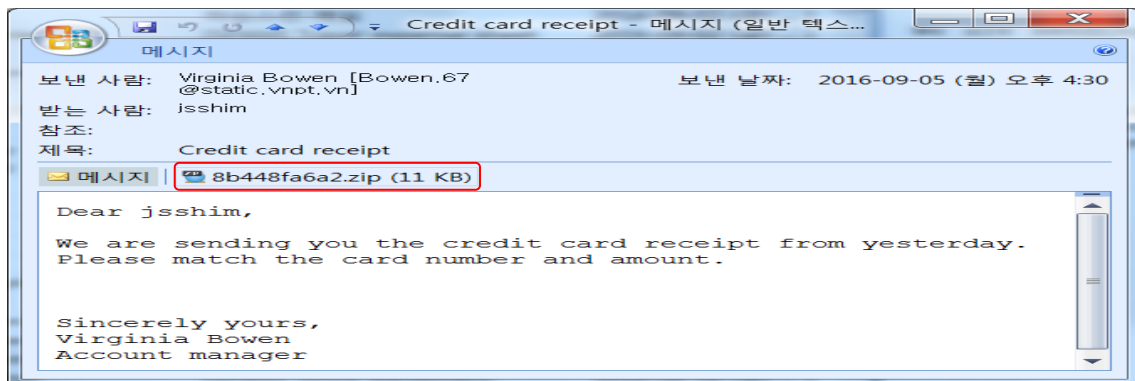
- 1d893c4cf3a.zip => 255B8AF9\_flight\_tickets.js



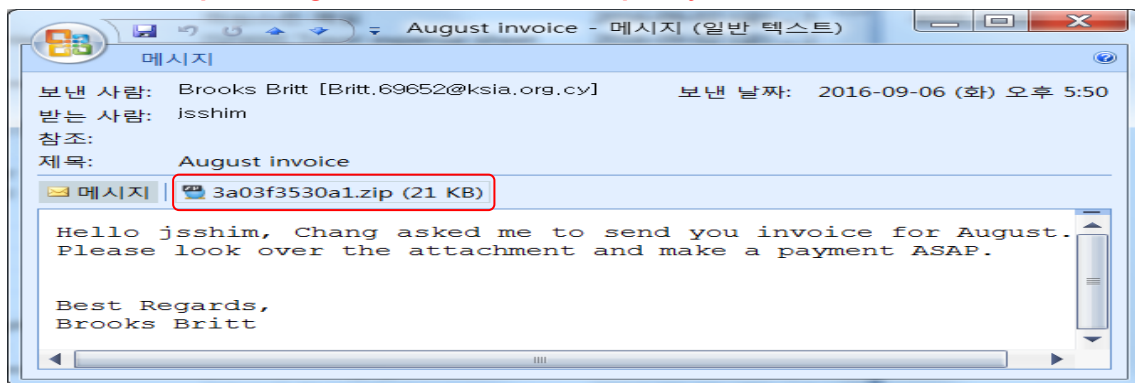
- 9e0b426842.zip => office\_facilities\_0FC93CC1.js



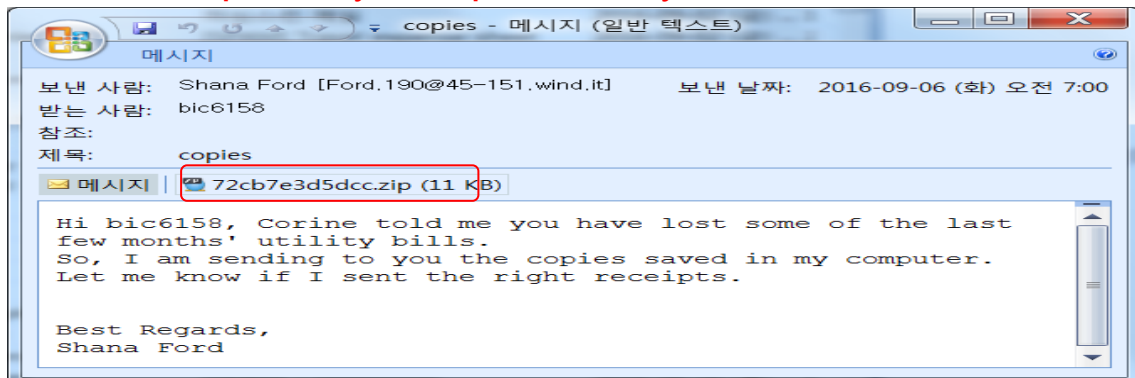
- 8b448fa6a2.zip => credit\_card\_receipt\_C15ADE63.js



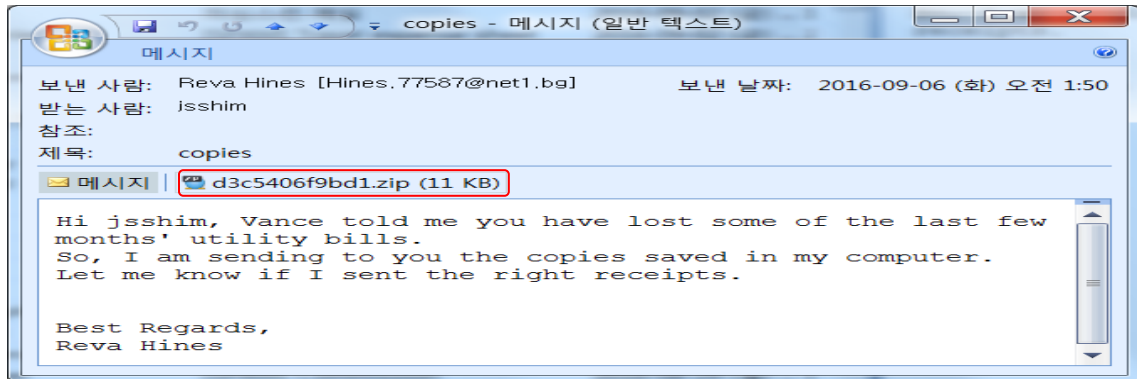
- 3a03f3530a1.zip => August\_invoice 6EAC151A. pdf~.js



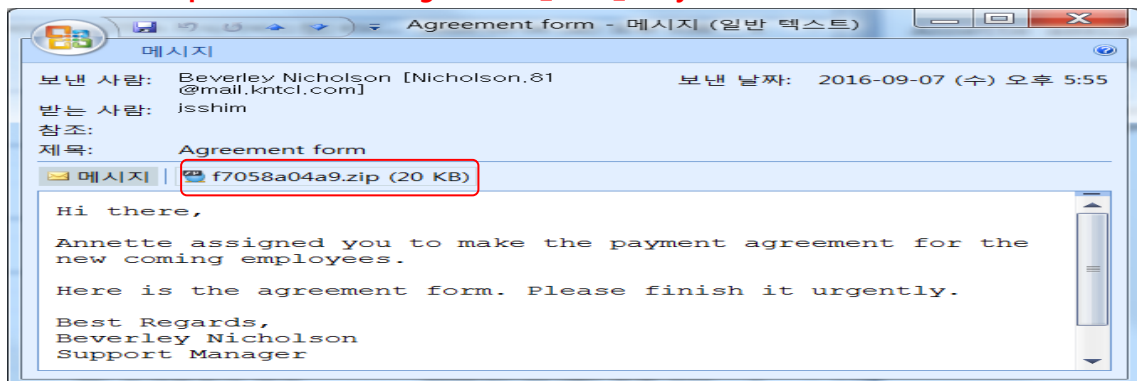
- 72cb7e3d5dcc.zip => utility\_bills\_copies E66A49E2.js



- d3c5406f9bd1.zip => utility\_bills\_copies E66A49E2.js



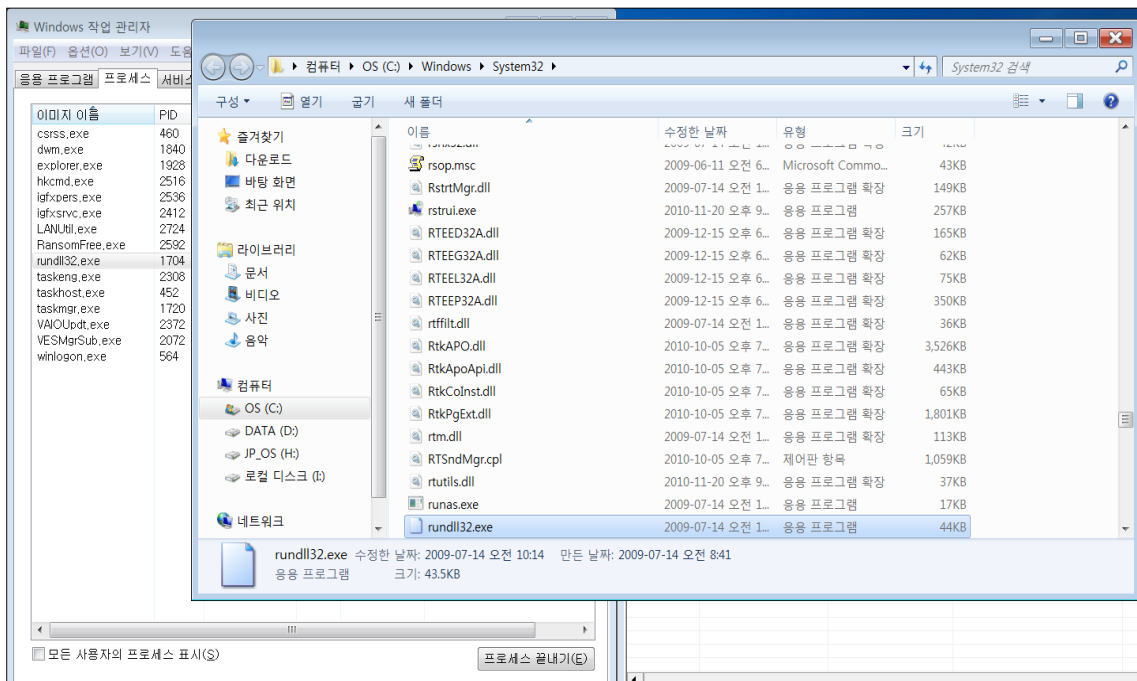
- f7058a04a9.zip => 2DC14A55 agreement\_form\_doc.js



2. Type of Ransomware = zepto

3. Name of process

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



#### 4. Blocked by RansomFree®

The screenshots illustrate the RansomFree64 Monitor application in action. The first image shows a warning dialog box stating '현재 작업이 차단되었습니다. PC전통을 끄고 전문가에게 진단을 의뢰하십시오. 진단없이 PC를 재부팅할 경우 모든 문제가 해결될 수 있습니다.' (Current operation blocked. Turn off PC protection and consult a professional. If you reboot the PC without diagnosis, all problems may be solved.) This dialog is overlaid on the Windows Task Manager window, which lists running processes including RansomFree.exe.

The second screenshot shows the Windows Task Manager window with 'RansomFree.exe' selected. The process list includes:

이미지 이름	사용자	메모리	설명
csrss.exe	ceo	1,892 KB	
dwm.exe	ceo	14,416 KB	태스크바 창 관리자
esif_assist_64.exe	ceo	2,268 KB	
ETDChl.exe	ceo	6,704 KB	ETD Control Center
ETDChlHelper.exe	ceo	3,244 KB	ETD Control Center Helper
explorer.exe	ceo	33,200 KB	Windows 탐색기
lghEM.exe	ceo	4,000 KB	lghEM Module
lghHK.exe	ceo	3,392 KB	lghHK Module
lghTray.exe	ceo	3,844 KB	lghTray.exe
lusb3mon.exe +32	ceo	2,212 KB	lusb3mon
RansomFree.exe	ceo	6,348 KB	RansomFree
RAVCpl64.exe	ceo	4,398 KB	Realtek HD 오디오 관리자
RF_IO32.exe +32	ceo	1,452 KB	RansomFree Monitor
spec.exe +32	ceo	500 KB	NoteBook Application
taskeng.exe	ceo	2,864 KB	작업 스케줄러 엔진
taskhost.exe	ceo	6,016 KB	Windows 작업을 위한 호스트 프로세스
taskmgr.exe	ceo	4,772 KB	Windows 작업 관리자
winlogon.exe	ceo	2,360 KB	

The third screenshot shows the RansomFree64 Monitor application interface. It displays a list of blocked files with columns for '구분' (Category), '일시' (Time), '원시 프로그램명' (Original Program Name), '파일명' (File Name), and '파일 크기' (File Size). The status bar at the bottom indicates 'Blocking ransom attacks' and 'Behavior Blocking - 41021201'.

