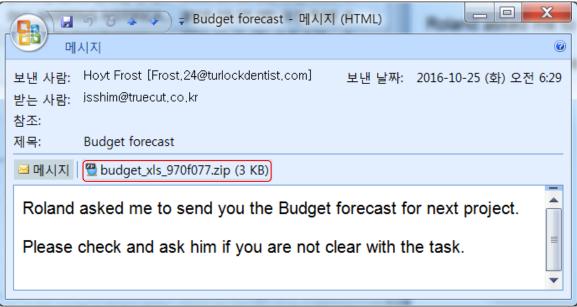
Today's Ransomware - thor ransomware

Oct. 25, 2016

1. I've received a Budget forecast

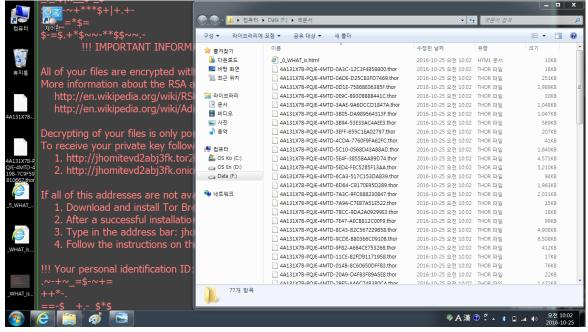


2. Blocked by TrojanCut®

<b>김</b> 퓨터	지어판									
류지동 류지동	scvhost.exe	<ul> <li>♥ Windows 작업 관리자</li> <li>파일(F) 옵션(O) 보기(V)</li> </ul>	도운약(H)							
	<mark>종 백 트로이첫 소개서.pptx</mark>	응용 프로그램 프로세스 사 이미지 이름 Csrss,exe dwm,exe esif_assist_64,exe ETDCtfl.exe ETDCtfl.exe	(비스 성능 네트워킹 / 사용자 C 메모리( 00 1.692 k ceo 03 12.920 k ceo 00 2.436 k	설명 B B 데스크톱 창 관리자 B ETD Control Center						
saved_letter b budget 2C4E6	oudget_xls	explorer, exe igh/EM, exe igh/EM, exe igh/Tray, exe iusb3mon, exe +32 RAVCpI64, exe taskhost, exe taskhost, exe	ceo         00         26.896         H           ceo         00         4.676         H           ceo         00         3.932         H           ceo         00         4.224         H           ceo         00         2.872         H           ceo         00         2.872         H           ceo         00         4.924         H           ceo         00         7.456         H           ceo         00         7.456         H	8 Windows 답석기 8 ight:K Module 8 ight:K Module 8 ight:K Module 8 ight:Stray.exe 8 iusb3mo 8 Realtek HD 오디오 판리자 8 Windows 작업을 위한 호스트 프로 8 Windows 작업 관리자						
2C4E6		TC_I032,exe +32 TC_KB32,exe +32 TrojanCut,exe winlogon,exe	ceo 00 1,608 k ceo 00 684 k ceo 01 10,684 k 00 2,436 k	B TrojanCut Monitor B TrojanCut	<ul> <li>전 TrojanCut64 N</li> <li>자료유출 팀</li> <li>구 분 일</li> <li>랜섬차단 2016</li> </ul>	·지현황 시	DDoS공격 차단현횧 전송프로그램명 rundll32	· 업데이트 파일명 Behavior Blocking	도움말 파일크기 수신처 0 185,102,136,77	×
		< 중 모든 사용자의 프로세 프로세스: 54 CPU 사용:		프로세스 끝내기( <u>E</u> ) 5%			실	N간 악성행위 차단중입니디	ж.	
<b>@</b>	ê 🚞	<i>லூ</i>					9	▶ A 漢 😨 🖁 🔺 📶	券 🔒 .⊪I 🕪 오전 9:21 2016-10-2	25

☞ C&C 서버 IP: 185.102.136.77 (RUSSIA)

3. Victim in case TrojanCut® was not installed



☞ Extension of files were changed to "thor"