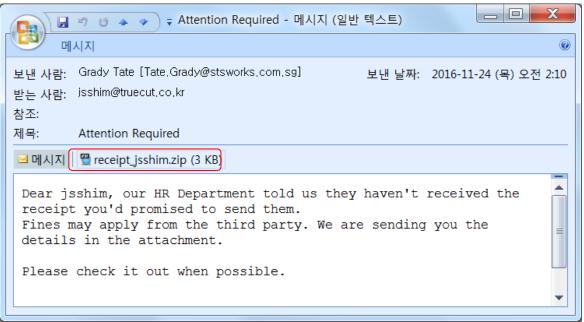
Today's Ransomware - zzzzz ransomware

Nov. 24, 2016

1. The mail which contained a zzzzz ransomeware.



- Filename : B26B44HJ7R2J6BIIV5.js
- 2. Blocked by TrojanCut[®]

					$\left[\right]$						
					(🕘 🛞 → 🚺 → 컴퓨터 →	Data (F:) 🕨 국문서		▼ \$ ₇	국문서 검색	Q
컴퓨터	제어판			ſ	구성 ▼ 라이브러리에 포함 ▼ 공유 대상 ▼ 새 풀더					E • 1 0	
						⁺ ☆ ▼ 다이브더니에:					8== • 🛄 🔮
						쑭 즐겨찾기	이름	수정한 날짜	유형	크기	Â
						🚺 다운로드	🛁 10명의 유명 해커와 이들의 별명.docx	2015-11-30 오후	Microsoft Office	1,422KB	
휴지통	📮 Windows 작업 관리자					📃 바탕 화면	🗐 11가지 나쁜 리더십 행동 프로파일.docx	2014-12-18 오후		75KB	
		·입(F) 옵션(O) 보기(V) 도움말(H)				🗓 최근 위치	27% of all malware.docx	2016-02-24 오후		206KB	
							🗐 31만 달러 쏟아붓고 방어는 28%뿐.docx	2016-01-15 오후		14KB	E
ZIP	응용 프로그램 프로세스 서비스 성능 네트워킹 사용자			H_	📜 라이브러리	1 81개국 878명 대상 보안 설문 조사 발표	2016-07-20 오전	Microsoft Office	175KB		
	OUTUT	o. =^	uon i	0 000000		📑 문서	🗐 100% 방어가 불가능하다면 맷집을 키워		Microsoft Office	871KB	
receipt_jss	이미지		사용자 (38	🛃 비디오	🔁 100%방어는 어렵다_20151007.pdf	2015-10-08 오전	Adobe Acrobat D	1,614KB	
	dwm.ex			00 1,796 KB 04 12,520 KB	9 A	📓 사진	🗐 가상화 기술을 통한 금융사 보안강화 방		Microsoft Office	7,941KB	
				00 2,428 KB	-	■ 랜섬웨어 차단	A CONTRACT DESCRIPTION	11-13 오전	Adobe Acrobat D	1,639KB	
- C	ETDCtr				TO		The second second second second	-10-20 오전	Microsoft Office	157KB	
5					TC 4in			-06-27 오후	Microsoft Office	103KB	
B26B44HJ		explorer,exe ceo 02 26,700 KB Wil igfxEM,exe ceo 00 4,788 KB igf				변섬공격을 차태 PC저워을 11고	건아었습니다. 전문가에게 진단을 의뢰하십시오.	-11-28 오전	Microsoft Office	16KB	
	igfxHK,		090	00 4,152 KB	gfx		재부팅할 경우 모든 문서가 파괴될 수 있습니다.	-01-09 오후	Microsoft Office	35KB	
	igfxTra				gfx			-07-07 오후	Microsoft Office	2,030KB	
					ust Rea			-02-24 오후	Microsoft Office	5,077KB	
	taskeng				약입		확인	-02-24 오후	Microsoft Office	3,088KB	
	taskhos	st,exe c			4in			-02-24 오후	Microsoft Office	4,570KB	
	taskrng TC_AU				4in Fro		🗐 개인정보유출 사고는 왜 자꾸 터질까.docx	: 2016-08-06 오후	Microsoft Office	186KB	
					Fro		🗾 개인정보유출대응현황과시사점.pdf	2011-12-18 오후	Adobe Acrobat D	6,508KB	
		32,exe +32 c	ceo	00 700 KB	Гro		TrojanCut64 Monitor	2010/02/02 02:00	Manual Orac		
	TrojanC winlogo			02 13,548 KB 00 2,376 KB	ro,						
						자료유출 탐지현황 DDoS공격		데이트		도움말	
								동프로그램명 파일 레이아 파일	일명 navior Blocking - 440,		수신처
	< · · · · · · · · · · · · · · · · · · ·					면접자만 2010~11~24 10:04:17 Tun	dli32 Bel	havior blocking - 440,		J	
	프로세스: 57 CPU 사용: 21% 실제 메모리: 26%					76개 항목			실/	시간 자료유출 감시 등	÷
						유충차단 Behavio					1021201
	6	1							◆A漢②	- 👩 🕴 📴	.ul (*) 오전 10:04 2016-11-24

3. Victim in case TrojanCut® was not installed

		▶ Data (F:) ▶ 국문서	- 4	국문서 검색		x
컴퓨터 \$계어판 +=\$-~*+-\$*_ *\$ - ~\$- \$+	구성 ▼ 라이브러리어		<u>/</u>	76787	= - 1	0
	▲☆ 즐겨찾기	이름	수정한 날짜	유형	크기	^
 + \$_\$\$-= \$+ +	┃ 다운로드	_0-INSTRUCTION.html	2016-11-24 오전 10:18	HTML 문서	9KB	
III IMPORTANT INFORM.	🌉 바탕 화면	AA131XAZ-C6JE-4ZZC-0DDB-2EADAAE5B053.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	1.048KB	
휴지통	🗐 최근 위치	4A131XAZ-C6JE-4ZZC-1A3A-D46946E67D5F.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	20KB	
All_of your files are encrypted wit		4A131XAZ-C6JE-4ZZC-02E2-209FC20BFE70.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	2,031KB	E
	4 詞 라이브러리	4A131XAZ-C6JE-4ZZC-2D1C-42B83151AB0A.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	18KB	
N e information about the RSA a	▷ 📑 문서	4A131XAZ-C6JE-4ZZC-2F38-A1F314FF348B.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	36KB	
4A131XAZ. 4A131Attp://en.wikipedia.org/wiki/RS.	🛛 🛃 비디오	4A131XAZ-C6JE-4ZZC-03E1-296EBFFDD554.zzzz	2016-11-24 오전 10:18	ZZZZZ 파일	94KB	
http://en.wikipedia.org/wiki/Ad	▷ 🔛 사진	4A131XAZ-C6JE-4ZZC-3E95-E869ED7DC00F.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	18KB	
http://en.wikipeuia.org/wiki/Au	▷ 👌 음악	4A131XAZ-C6JE-4ZZC-3FB5-42F46547F1F4.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	30KB	
		4A131XAZ-C6JE-4ZZC-4A25-49C3186E4102.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	4,571KB	
ypting of your files is only po	4 🜉 컴퓨터	4A131XAZ-C6JE-4ZZC-4D3F-9BBAAD0831C5.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	4,908KB	
	Þ 💒 OS Ko (C:)	4A131XAZ-C6JE-4ZZC-5B45-CE69F8C86A8B.ZZZZ	2016-11-24 오전 10:18	ZZZZZ 파일	5,952KB	
-5-INSTRUINSTRUCTICE vour private key follow) 👝 OS En (D:)	4A131XAZ-C6JE-4ZZC-5B50-2AB59857B888.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	18KB	
	🛛 🧰 Data (F:)	4A131XAZ-C6JE-4ZZC-6A43-90BFDF369317.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	41KB	
		4A131XAZ-C6JE-4ZZC-6CE3-38DE334F7106.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	111KB	
	▷ 📬 네트워크	4A131XAZ-C6JE-4ZZC-7A14-AEB957E51EB2.ZZZZ	2016-11-24 오전 10:18	ZZZZZ 파일	1,989KB	
If all of this addresses are not ava		4A131XAZ-C6JE-4ZZC-7B3E-289262330130.ZZZZ	2016-11-24 오전 10:18	ZZZZZ 파일	1,504KB	
1. Download and install Tor Bro		4A131XAZ-C6JE-4ZZC-8B59-BF955B50994C.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	80KB	
2. After a successful installation		4A131XAZ-C6JE-4ZZC-8E1E-53D4765BA853.ZZZZ	2016-11-24 오전 10:18	ZZZZZ 파일	3,800KB	
		4A131XAZ-C6JE-4ZZC-9AE5-0D742604A29F.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	18KB	
3. Type in the address bar: mv		4A131XAZ-C6JE-4ZZC-9AED-15C678C02DCE.ZZZZ	2016-11-24 오전 10:18	ZZZZZ 파일	19KB	
4. Follow the instructions on th		4A131XAZ-C6JE-4ZZC-9B23-549110F07E92.ZZZZ	2016-11-24 오전 10:18	ZZZZZ 파일	104KB	
		4A131XAZ-C6JE-4ZZC-46FF-1F08CF242452.zzzz	2016-11-24 오전 10:18	ZZZZZ 파일	21KB	
		4A131XAZ-C6JE-4ZZC-47C7-07F039F22325.zzzz	2016-11-24 오전 10:18	ZZZZZ 파일	872KB	
!!! Your personal identification ID:		4A131XAZ-C6JE-4ZZC-59DD-BB0CB319E176.zzzzz	2016-11-24 오전 10:18	ZZZZZ 파일	17KB	-
.*+*= _~=\$ ~. ~=-	77개 항목	AA131YA7_CAIE_A77C_A752_7958D7E15D37 77777	2016_11_2/ O & 10-19	77777 mLOI	76KR	
📀 🔁 📋 🐗			 ♥A漢(2 🖡 🔺 🎁 .	.nl (*) 오전 10 2016-11	

The file extension of the attacked files were changed to "zzzzz".