Today's Ransomware – Zeppelin

Feb 08, 2021

1. Blocked by trueEP®

简									
			타입 랜섬웨어 공격	날짜 2021-02-08 10:51:26	프로세스 zeppelin,exe	파일이름 Behavior Blocking			
	방어			2021-02-08 10:51:25		Behavior Blocking			
ß	스마트 백업								
	검사 제외								
F	토그		백업 로그	찾기	1000개 더	복원 삭제]		
			날짜		파일이름				
G	업데이트								
ŝ	설정								
0	도움말								

2. Victim in case trueEP[®] was not installed - All file name's extensions were changed to Random Extension.

📕 🛃 🗖 🖵 A	ዘ 폴더				- 0	×		
파일 홈 공	공유	보기				~ 🕐		
$\leftrightarrow \rightarrow \cdot \uparrow$	→ < ↑ → 새 폴더 ✓ ♂ 새 폴더 검색							
		이름 ^	수정한 날짜	유형	크기	^		
📌 바로 가기		III ALL YOUR FILES ARE ENCRYPTED !!!		테스트 무서	1KB			
📃 바탕 화면	*	□ 문서1.docx.CC5-413-EBE	2012-10-19 오전		19KB			
👆 다운로드	*	□ 문서1.docx.CC5-413-EBE	2012-10-19 오전					
≝ 문서	*	□ 문서3.docx.CC5-413-EBE	2012-10-19 오전					
🖾 드 ·	*	□ 문서4.xlsx.CC5-413-EBE	2012-10-19 오신 2014-12-11 오후					
	7							
📑 동영상		□ 문서5.pptx.CC5-413-EBE	2011-12-12 오후		-/			
🎝 음악] 문서6.pdf.CC5-413-EBE	2012-10-19 오전		130KB			
OneDrive] 문서7.txt.CC5-413-EBE	2012-08-27 오전					
Olieblive		집 압축.zip.CC5-413-EBE	2019-08-23 오후					
💻 내 PC		집 압축2.zip.CC5-413-EBE	2019-08-23 오후					
		이미지.bmp.CC5-413-EBE	2010-06-24 오전	CC5-413	161KB			
췕 네트워크		이미지.JPG.CC5-413-EBE	2012-12-13 오전	CC5-413	285KB			
		이미지.png.CC5-413-EBE	2013-01-09 오전	CC5-413	25KB			
		🗋 이미지.psd.CC5-413-EBE	2010-06-24 오전	CC5-413	399KB			
		이미지2.jpg.CC5-413-EBE	2009-11-09 오전	CC5-413	197KB			
		이미지3.jpg.CC5-413-EBE	2009-11-09 오전	CC5-413	200KB	~		
16개 항목						:==		

3. Screen of Victim

🧐 !!! ALL YOUR FILES ARE ENCRYPTED !!! - Windows 메모장				_		×
파일(F) 편집(E) 서식(O) 보기(V) 도움말						
!!! ALL YOUR FILES ARE ENCRYPTED !!!						^
All your files, documents, photos, databases and other impo	rtant files are end	rypte	d.			
You are not able to decrypt it by yourself! The only method Only we can give you this key and only we can recover your		es is t	o purchase a	n uniqu	ie priv	ate
To be sure we have the decryptor and it works you can send But this file should be of not valuable!	l an email: uspex	1@co	ck.li and dec	rypt on	e file f	for t
Do you really want to restore your files? Write to email: uspex1@cock.li Reserved email: uspex2@cock.li						
Your personal ID: CC5-413-EBE						
Attention! * Do not rename encrypted files. * Do not try to decrypt your data using third party software * Decryption of your files with the help of third parties may					to our	10 (
						~
	n 1, Col 1	100%	Windows (CRLF)	UTF	0	>
	1,001	100%	windows (CREF)		-0	

ि इ.ग.ह	3	₩X6.pdf -416-898						
III ALL V FILES AS	OUR RE	문서7768.CC5 -413-E86						
문서11.de -413-6) XeX BE	법축 zip.CC5 -413-EBE						
문서2.do -413-8	Jex BE	암국2.ap -413-E8E						
문서B.pc -413-8) iff Ble	새 골의						
문서4.M -413-8) 5X BE	A literosoft Edge						
문서5.pp -413-8)itx Be	Chrome						
	Q	검색하려면 여기에 입력	하십시오.	H C	i		へ 記 🗤 A	오전 11:21 2021-02-08 🔁