Today's Ransomware – Ryuk

Apr 16, 2021

1. Blocked by trueEP®

Y trueEP Ent 2. 0 $-\Box \times$							
^è	▋ 로그						
ि हि	타입 랜섬웨	날짜 2021-04-16 17:28:18	프로세스 xxx,exe	파일이름 Behavior Blockin			
🎧 스마트 백업							
월 검사 제외							
	∎ 백업 로그		찾 <mark>기</mark> 1000개 파일이		삭제		
ତ୍ର ପ୍ରଜ୍ଞାଠାର୍ଚ୍ଚ			- e -				
;;;; ≝≅							
⑦ 도움말							

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

📙 🛃 📙 👳 새 폴더			-	- 🗆 X
파일 홈 공유	보기			~ 🕐
← → ∽ 📴 > 새	폴더	v Q	새 폴더 검색	م
	이름	수정한 날짜	유형	크기
🖈 즐겨찾기	RyukReadMe	2021-04-16 오후	HTML 파일	2KB
📃 바탕 화면 🛛 🖈	☐ 문서1.docx.RYK	2021-04-16 오후	RYK 파일	17KB
🔶 다운로드 🛛 🖈	☐ 문서2.docx.RYK	2021-04-16 오후	RYK 파일	17KB
🔮 문서 🛛 🖈	 문서3.docx.RYK	2021-04-16 오후	RYK 파일	17KB
▶ 사진 🖈	한 문서4.xlsx.RYK	2021-04-16 오후	RYK 파일	18KB
📕 동영상	📄 문서5.pptx.RYK	2021-04-16 오후	RYK 파일	5,526KB
 _) 음악	📄 문서6.pdf.RYK	2021-04-16 오후	RYK 파일	128KB
-	🗋 문서7.txt.RYK	2021-04-16 오후	RYK 파일	1KB
OneDrive	📄 압축.zip.RYK	2021-04-16 오후	RYK 파일	3,488KB
🛄 LH PC	📄 압축2.zip.RYK	2021-04-16 오후	RYK 파일	7,687KB
	📄 이미지.bmp.RYK	2021-04-16 오후	RYK 파일	159KB
🧃 CD 드라이브 (D:) Vir		2021-04-16 오후	RYK 파일	282KB
🔿 네트워크	이미지.png.RYK	2021-04-16 오후	RYK 파일	23KB
	이미지.psd.RYK	2021-04-16 오후	RYK 파일	397KB
	이미지2.jpg.RYK	2021-04-16 오후	RYK 파일	195KB
	이미지3.jpg.RYK	2021-04-16 오후	RYK 파일	198KB
16개 항목				

3. Screen of Victim

ß	€ □ C:\U	sers\Pub	olic\Deskto	x + ~					_		×
\leftarrow	\rightarrow O	ŵ	i file:	///C:/Users/Public/Desktop/RyukReadN	1e.html		□ ☆	չ≜	l_	Ŀ	
	contac			이 사이트의 메시지 INSTRUCTION: 1. Download tor browser. 2. Open link through tor brows rk2zzyh63g5avvii4irkhymha3irb nion	ser: http://	whidkpqd.o					
				 Fill the form, your password: We will contact you shortly. Always send files for test decry 							
					bala	nce of	sha	dow	un	iver	se

