Today's Ransomware – CUBA

Dec. 27, 2022

1. Blocked by trueEP®



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

🗐 🛃 🔜 =	검색 도구 *.cuba	- 로컬 디스크 (C:)의 검색	결과		– 🗆 X
파일 홈 공유 브	보기 검색				~ 🕐
	주정한 및 기타 속성 ▾	 중 최근 검색 ▼ 급 곱급 옵션 ▼ 파일 위기 급 검색 저장 열기 	지 검색 닫기		
위치	구체화	옵션			
← → ▼ ↑ 🗐 > 로컬 디스크 (C:)의 검색 결과 >				ٽ ~	*.cuba ×
🗐 문서 🖈 ^	이름	수정한 날짜	유형	크기 ~	폴더 ^
📰 사진 🛛 🖈	manifest.xml.cuba	2022-12-21 오후 12:50	CUBA 파일	4,913KB	{1A8308C7-90D1
LG공유폴더 🖈	stream.x86.ko-kr.m	2022-12-21 오후 12:50	CUBA 파일	4,622KB	ko-kr.16(C:\Prog.
📕 동영상	nacl_irt_x86_64.nex	2022-12-21 오후 12:50	CUBA 파일	4,227KB	108.0.1462.54(C:.
▲ 888 ▶ 음악	nacl_irt_x86_64.nex	2022-12-21 오후 12:50	CUBA 파일	4,227KB	108.0.5359.125(
	browsermetrics-spa	2022-12-21 오후 12:51	CUBA 파일	4,097KB	User Data(C:₩사
📥 OneDrive - Persoi	browsermetrics-62	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
I HPC	browsermetrics-62	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
	browsermetrics-62	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
🧊 3D 개체	browsermetrics-62	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
🔶 다운로드	browsermetrics-62	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
🐺 동영상	browsermetrics-63	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
🔮 문서	browsermetrics-63	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
바탕 화면	browsermetrics-63	2022-12-21 오후 12:51	CUBA 파일	4,097KB	BrowserMetrics(C:
■ 사진	hxstore.hxd.cuba	2022-12-21 오후 12:51	CUBA 파일	4,097KB	LocalState(C:₩사
	talkuserdb.edb-wal	2022-12-21 오후 12:51	CUBA 파일	4,089KB	003138b3da160f.
♪ 음악	chatlistinfo.edb-wal	2022-12-21 오후 12:51	CUBA 파일	4,025KB	chat_data(C:₩사
🏪 로컬 디스크 (C:)	index.win32.bundle	2022-12-21 오후 12:51	CUBA 파일	3,987KB	PackageResources
🔿 네트워크	📄 microsoftedgeupda	2022-12-21 오후 12:50	CUBA 파일	3,721KB	Log(C:\Program 🗸
6,690개 항목	c				>

3. Screen of Victim.

		~
		×
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)		
Good day. All your files are encrypted. For decryption contact us.		^
Write here mrddnet_support@protonmail.ch	_	
We also inform that your databases, ftp server and file server were downloaded by us to our servers	i.	
* Do not rename encrypted files.		
* Do not try to decrypt your data using third party software,		
it may cause permanent data loss.		
		\sim
		>
Ln 1, Col 1 100% Windows (CRLF) UTF	-8	
· 휴지동 이미지_01 이미지_08		
문서이pdf이미지_02이미지_00		
문서Tigdf 이미지_03 IIFAQ for cubarxe		
Decryption		
문서B.doox 이미지_05		
문서4doex 이미지 to		
암국파일·21 이미지_07		
	0 = 1:00	
📲 🔎 검색하려면 여기에 입력하십 🧕 이 🛱 🐂 💽 🦗 🧔 🗐 🖓 🌙 🍊 2°C ^ 현 🕼 🖫 🐠 A	오루 1:22 2022-12-21	2