## Today's Ransomware – Sugar

Feb. 08, 2022

NEWS related to Sugar Ransomware

https://medium.com/walmartglobaltech/sugar-ransomware-a-new-raas-a5d94d58d9fb https://www.boannews.com/media/view.asp?idx=104529&kind=

1. Blocked by trueEP®

💡 trueEP Ent 2. 0					- 🗆 ×
°≊					
	타입	날짜	프로세스	파일이름	
WH 🕅	랜섬웨 202	2-02-08 11:28:04	sugar,exe	Behavior Blocking	
🏠 스마트 백업					
갑사 제외					
	백업 로그	찾	<b>7 </b> 10007#	더 복원 (	삭제
	날짜		파일이	음	
<b>;;;;</b> 설정					
? 도움말					

2. Victim in case trueEP<sup>®</sup> was not installed - All files were encrypted and extensions ware changed to encoded01.

📙   🔽 📑 🚽   새 출						_		×
파일 홈 공유	유 보기						^	?
★ 다 바로 가기에 복사 붙 고정	[1] 🔏 <sup>[</sup> 여넣기 🚺	및 이동 위치 ∽     ★ 삭제 ▾       [] 복사 위치 ∽     ■ 이름 바꾸기	- 새 폴더	¶ù• 1]•	<ul> <li>✓</li> <li>✓</li> <li>4d</li> <li>✓</li> </ul>			
클립보드		구성	새로	만들기	열기	선택		
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	›새 폴더	~	Ō	ر م	내 폴더 검색			
🚁 바로 가기	이름	÷ ^		수정한	날짜	유형	크기	
바탕 화면	*	BackFiles_encoded01		2022-0	2-08 오후 1:08	텍스트 문서	5K	В
	-	문서1.docx.encoded01		2022-0	2-08 오후 1:08	ENCODED01 파일	12K	В
↓ 다운로드	*	<ul> <li>문서1.xlsx.encoded01</li> <li>문서2.docx.encoded01</li> <li>문서2.xlsx.encoded01</li> <li>문서3.xlsx.encoded01</li> <li>문서3.xlsx.encoded01</li> <li>이미지.gif.encoded01</li> </ul>			2-08 오후 1:08	ENCODED01 파일	9K	В
💼 문서	*				2022-02-08 오후 1:08 ENCODED01 프		12K	В
▶ 사진	*				022-02-08 오후 1:08 ENCC	ENCODED01 파일	9K	В
server	*				2-08 오후 1:08	ENCODED01 파일	12K	В
🖵 cst	*				2-08 오후 1:08	ENCODED01 파일	9K	В
📕 동영상					2-08 오후 1:08	ENCODED01 파일	678K	В
▶ 음악		이미지1.png.encoded01			02-08 오후 1:08	ENCODED01 파일	262K	
-		이미지2.png.encoded01		2022-0	2-08 오후 1:08	ENCODED01 파일	30K	В
<ul> <li>OneDrive</li> </ul>								
💻 내 PC								
💣 네트워크								
10711 51-12	<							>
10개 항목								

## 3. Screen of Victim

I BackFiles_encoded01 - Windows 메모장				_		Х		
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)								
[+] Whats Happen? [+]						^		
Your files are encrypted, and currently unavailable. You can check it: all files on your system has extens By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherw return your data (NEVER).								
[+] What guarantees? [+]								
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we work and liabilities - nobody will not cooperate with us. Its not in our interests.								
To check the ability of returning files, You should go to our website. There you can decrypt 1-5 files f is								
our guarantee.								
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and just we have the private key. In practise - time is much more valuable than money.								
[+] How to get access on website? [+]								
You can open our site by the shortcut "SUPPORT (TOR_BROWSER)" created on the desktor								
Also as the second option you can install the tor	browser:					~		
<	La di Cali di	1000/	Windows (CDLD)	1175.0		>		
	Ln 1, Col 1	100%	Windows (CRLF)	UTF-8	5			

