Today's Ransomware–RedEnergy

Aug 28, 2023

1. Blocking screenshot by trueEP[®]



2. Victim in case trueEP[®]wasnot installed - All file name's extensions were changed to <File Name>.FACKOFF!.

🗐 🛃 🔜 =	검색 도구 *.FACK	(OFF! - 로컬 디스크 (C:)의	검색 결과		– 🗆 ×
파일 홈 공유	보기 검색				~ 🕐
← → ~ ↑ 💷 > 로	컬 디스크 (C:)의 검색 결과 >	✓ X *.FA	ACKOFF!		×
★ 즐겨찾기	이름	수정한 날짜	유형	크기	폴더 ^
📃 Desktop 🛛 🖈	desktop.ini.FACKOFF!	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Music(C:\Users\t
🚽 Downloads 🖈	Downloads.Ink.FAC	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Links(C:₩Users₩t
🖹 Documents 🖈	Desktop.ink.FACKO	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Links(C:₩Users₩t
	desktop.ini.FACKOFF!	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Links(C:₩Users₩t
📰 Pictures 🛛 🖈	desktop.ini.FACKOFF!	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Favorites(C:₩User.
Music	desktop.ini.FACKOFF!	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Links(C:\Users\t.
😽 Videos	trueEP_Setup(Ver 2	2023-08-28 오후 4:55	FACKOFF! 파일	12,118KB	trueEP_Setup(C:₩.
lange - Anternal	Windows PowerSh	2023-08-28 오후 4:55	FACKOFF! 파일	3KB	Windows PowerS.
OneDrive - Personal	Windows PowerSh	2023-08-28 오후 4:55	FACKOFF! 파일	3KB	Windows PowerS.
🛄 Ц РС	File Explorer.lnk.FA	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	System Tools(C:₩.
	Run.Ink.FACKOFF!	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	System Tools(C:₩.
🤿 네트워크	Administrative Tool	2023-08-28 오후 4:55	FACKOFF! 파일	2KB	System Tools(C:₩.
	Command Prompt	2023-08-28 오후 4:55	FACKOFF! 파일	2KB	System Tools(C:₩.
	computer.lnk.FACK	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	System Tools(C:₩.
	Control Panel.Ink.F	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	System Tools(C:₩.
	desktop.ini.FACKOFF!	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Startup(C:\Users
	Desktop.ini.FACKO	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	System Tools(C:₩.
	Uninstall.Ink.FACK	2023-08-28 오후 4:55	FACKOFF! 파일	2KB	Oracle VM Virtual
	Desktop.ini.FACKO	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Maintenance(C:\.
	desktop.ini.FACKOFF!	2023-08-28 오후 4:55	FACKOFF! 파일	1KB	Administrative To. 🗸
	<				>
107개 항목					

3. Ransomware Notice.

🤳 read.it.txt - Windows 메모장 \times 파일(F) 편집(E) 서식(O) 보기(V) 도움말(H) YOUR FILES ENCRYPTED VIRUS !!! ANY ATTEMPT THEIR DECRYPT BY, IS ZERO WE HAVE A DECKER, YOU CAN BUY IT FOR --- 100\$--- At Bitcoin WRITE ON MAIL @proton.me), WE WILL ISSUE YOU DECODER (KEY DECRYPTION) BUY OR EXCHANGE Bitcoin CAN HERE OR WHERE THE YET: Coinmama - hxxps://www.coinmama.com, Bitpanda - hxxps://www.bitpanda.com REQUISITES Payment informationAmount : 0.005 BTC Bitcon Address : bc1q MAIL FOR COMMUNICATION : _____@proton.me Ln 10, Col 43 100% Windows (CRLF) UTF-8

4. Victim screen attacked by 'RedEnergy' ransomware.

