Today's Ransomware – Revil

1. Blocked by TrojanCut[®]



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

📙 📝 📙 👳 새	폴더			_		
파일 홈 공	유	보기			~ 🧃	
← → < ↑ ↓ · 새 볼더 · · · · · · · · · · · · · · · · · ·						
📌 바로 가기		이름	수정한 날짜	Rġ	크기	
비소 아이	*	dj47898z-readme	2021-07-07 오후 2:33	텍스트 문서	7КВ	
_		📋 iron_man_hd_game-HD.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	309KB	
↓ 다운로드	*	📄 lamborghini-estoque1.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	19KB	
🔮 문서	*	📄 lamborghini-estoque-interior-view1.jpg	2021-07-07 오후 2:33	DJ47898Z 파일	149KB	
📰 사진	*	📄 lamborghini-estoque-rear-view1.jpg.dj4	2021-07-07 오후 2:33	DJ47898Z 파일	70KB	
📑 동영상		📄 mazda-concept-car-1.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	30KB	
 <u>)</u> 음악		📄 mazda-concept-car-8.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	26KB	
• - ·		monster_car1.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	37KB	
loneDrive		monster_car2.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	33KB	
💻 내 PC		monster_car3.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	36KB	
		monster_car4.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	37KB	
💣 네트워크		monster_car5.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	31KB	
		monster_car6.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	36KB	
		monster_car7.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	37KB	
		monster_car8.jpg.dj47898z	2021-07-07 오후 2:33	DJ47898Z 파일	36KB	
		Opel-Flextreme-Concept-Beijing.jpg.dj4	2021-07-07 오후 2:33	DJ47898Z 파일	82KB	
		picture_Citroen_GT_Concept_2008_1.jpg	2021-07-07 오후 2:33	DJ47898Z 파일	146KB	
		Distura Citraan GT Cancant 2009 2 ing	つのつ1 M7 M7 O古 つつつ		170/0	
23개 항목 1개 항목 선택함 6.80KB						

3. Screen of Victim

III dj47898z-readme - Windows 메모장				_		×				
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)										
== Welcome. Again. ===						^				
[-] Whats HapPen? [-]										
Your files are encrypted, and currently unavailable. You can check it: all files on your system has exte By the way, everything is possible to recover (restore), but you need to follow our instructions. Othe										
[+] What guarantees? [+]										
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If w To check the ability of returning files, You should go to our website. There you can decrypt one file If you will not cooperate with our service - for us, its does not matter. But you will lose your time ar										
[+] How to get access on website? [+]										
You have two ways:										
 1) [Recommended] Using a TOR browser! a) Download and install TOR browser from this site: https://torproject.org/ b) Open our website: http://aplebzu47wgazapdgks6vrcv6zcnippkbxbr6wketf56nf6ag2nmvovd.onion/! * 										
	Ln 1, Col 1	100%	Windows (CRLF)	UTF-	16 LE					

