## Today's Ransomware – magniber

Jan. 30, 2022

1. Blocked by  $trueEP^{\mathbb{R}}$ 



2. Victim in case trueEP<sup>®</sup> was not installed - All file name's extensions were changed to . yuyevbg.

□   ○ □ =   파일 홈 공유	검색 도구 *.yuye 보기 검색	vbg - 내 PC의 검색 결과			- □ × ^ (3)
한 현재 폴더 한 현재 폴더 14 PC 유 다시 검색할 의 위치	G + Set + S	※ 최근 검색 ▼ E 고급 옵션 ▼ 파일 위7 C 검색 저장 C 검색 저장 C 검색	치 검색 닫기		
$\epsilon \rightarrow \cdot \uparrow \blacksquare $	내 PC의 검색 결과 >			ٽ ~	*.yuyevbg ×
🖈 즐겨찾기	▲ 이름	수정한 날짜	유형	크기	폴더 ^
	이미지_10.png.yuy	2023-01-30 오후 4:00	YUYEVBG 파일	229KB	바탕 화면(C:₩사
■ 바탕 화면 🖈	이미지_08.png.yuy	2023-01-30 오후 4:00	YUYEVBG 파일	25KB	바탕 화면(C:₩사
➡ 다운로드 🖈	이미지_09.png.yuy	2023-01-30 오후 4:00	YUYEVBG 파일	411KB	바탕 화면(C:₩사
🔮 문서 🛛 🖈	이미지_07.jpg.yuye	2023-01-30 오후 4:00	YUYEVBG 파일	141KB	바탕 화면(C:₩사
📰 사진 🛷	이미지_06.jpeg.yuy	2023-01-30 오후 4:00	YUYEVBG 파일	623KB	바탕 화면(C:₩사
LG공유폴더 🖈	이미지_05.jpg.yuye	2023-01-30 오후 4:00	YUYEVBG 파일	100KB	바탕 화면(C:₩사
📑 동영상	이미지_04.jpg.yuye	2023-01-30 오후 4:00	YUYEVBG 파일	66KB	바탕 화면(C:₩사
 _) 음악	이미지_03.bmp.yuy	2023-01-30 오후 4:00	YUYEVBG 파일	242KB	바탕 화면(C:₩사
-	이미지_02.jpg.yuye	2023-01-30 오후 4:00	YUYEVBG 파일	181KB	바탕 화면(C:₩사
lesson one One Drive - Person	이미지_01.jpg.yuye	2023-01-30 오후 4:00	YUYEVBG 파일	6,966KB	바탕 화면(C:₩사
I H PC	🗋 압축파일.zip.yuyev	2023-01-30 오후 4:00	YUYEVBG 파일	13,602KB	바탕 화면(C:₩사
3D 개체	azttu0nr.jpg.yuyevbg	2023-01-30 오후 4:00	YUYEVBG 파일	42KB	문서(C:₩사용자₩.
	skin.jpg.yuyevbg	2023-01-30 오후 4:00	YUYEVBG 파일	42KB	문서(C:₩사용자₩.
➡ 다운로드	📄 atal6km0.jpg.yuyev	2023-01-30 오후 4:00	YUYEVBG 파일	42KB	문서(C:₩사용자₩. ♥
동영상	V (				>
74개 항목					

## 3. Screen of Victim.

README.html × +			$\sim$	_	Ć	7	×			
← → C ③ 파일   C:/README.html	G	Q	Ê	☆		•	:			
🖌 근무일지										
ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!										
Your files are NOT damaged! Your files are modified only. This modification is reversible.										
The only 1 way to decrypt your files is to receive the private key and decryption program.										
Any attempts to restore your files with the third party software will be fatal for your files!										
To receive the private key and decryption program follow the instructions below:										
1. Download 'Tor Browser' from https://www.torproject.org/ and install it.										
2. In the 'Tor Browser' open your personal page here:										
http://f674709874yuyevbg.vbmpkajxyygcqos2luorb5p66yr5wb5v6lj2dy6acqhhuch5ssuq7xqd.onion/yuyevbg										
Notel This page is available via 'Tor Browser' only. 										
http://f674709874yuyevbg.diedsad.info/yuyevbg										
http://f674709874yuyevbg.aresika.info/yuyevbg										
http://f674709874yuyevbg.oldfree.info/yuyevbg										
http://f674709874yuyevbg.rawrow.info/yuyevbg										
Note! There are temporary addresses! They will be available for a limited amount of time!										

ania Brindaty, olukujos.								
이미지 10 문서요.docx 이미지 05					magniber	magniber.msi		
LG공유플터 - 문서삼docx 이미지_00j. 바로 가기								
README NE. 양국파업과, 이미지[07.								
문서D.patiyuy 이미지[01 이미지[03 evbg								
이미지_02 이미지_09								
· · · · · · · · · · · · · · · · · · ·	력하십	H 🐂	<b>Q</b>	O 🜣	🥚 4°C	へ 砲 臣 🖤 A	오후 4:00 2023-01-30	5