Magniber 랜섬웨어 복구툴 (확장자 별 키 정보)

By ATCP

Published: 2018-03-29 · Archived: 2026-04-05 20:46:42 UTC

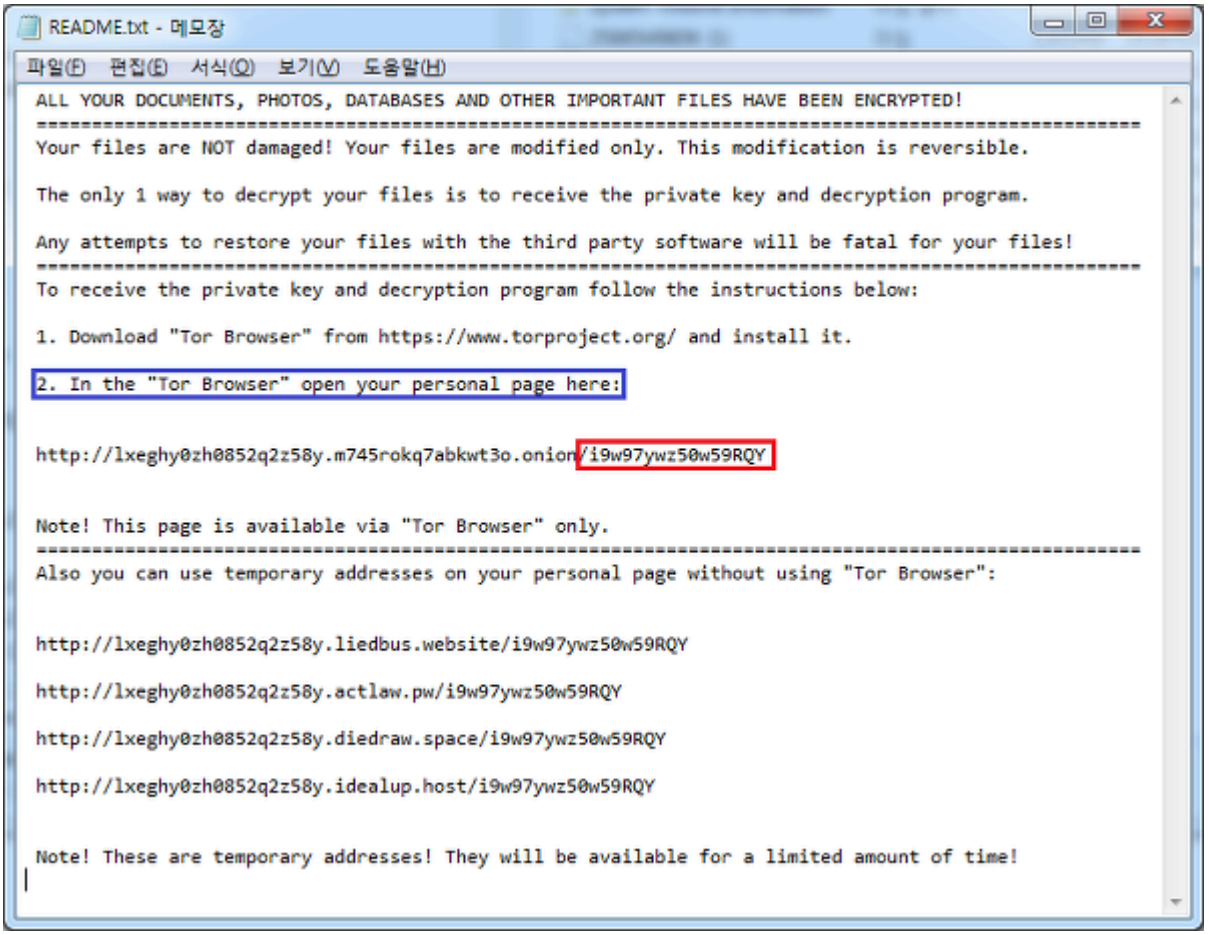
Magniber 랜섬웨어와 외형이 유사한 형태의 랜섬웨어로는 Hermes와 GandCrab 랜섬웨어가 있다. 즉, V3에서 “Trojan/Win32.Magniber”로 진단하는 파일 중에는 실제 Magniber가 아닌 유형이 존재할 수 있다. 각 랜섬웨어 별 랜섬노트를 통해 구분이 가능하다.

§ Hermes : DECRYPT_INFORMATION

§ GandCrab : CRAB-DECRYPT

§ Magniber : README

복구툴에서 복구가 가능한 형태는 README 이름의 랜섬노트를 갖는 Magniber 랜섬웨어이며, 아래와 같은 화면구성을 갖는다. 붉은색 표시부분의 값이 복구 시 사용되는 키 정보 중, 벡터값(IV)에 해당한다.

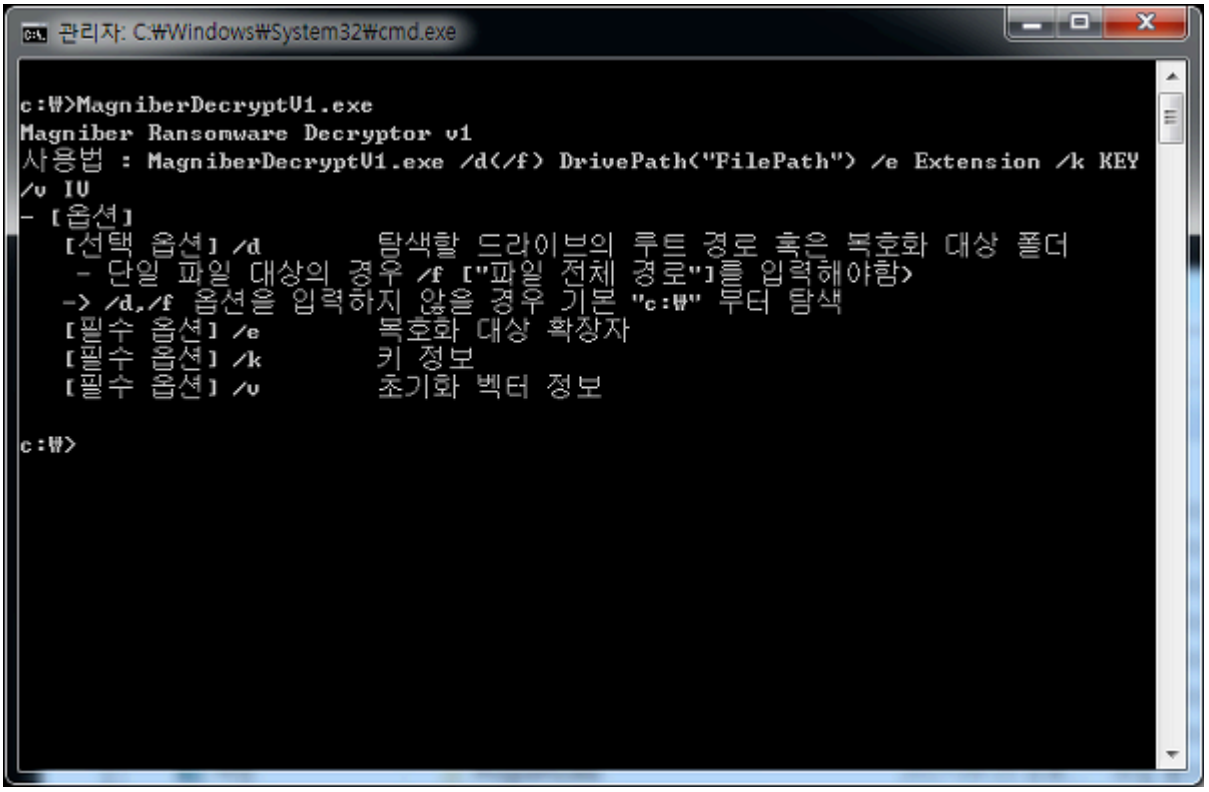


3월 30일 부터 현재까지 확인된 Magniber 랜섬웨어 확장자 별 키, 벡터 정보는 아래의 표와 같다. 이후 추가적으로 확인되는 확장자 별 키, 벡터 정보는 **http://asec.ahnlab.com/1125** 에서 확인 할 수 있다.

날짜	복구가능 확장자	키	벡터	다운로드
3/30	kympzmzw	Jg5jU6J89CUf9C55	i9w97ywz50w59RQY	MagniberDecrypt.zip
3/30	owxpzylj	u4p819wh1464r6J9	mbfRHUlbKJJ7024P	MagniberDecrypt.zip
3/30	prueitfik	EV8n879gAC6080r6	Z123yA89q3m063V9	MagniberDecrypt.zip
3/31	rwighmoz	BF16W5aDYzi751NB	B33hQK9E6Sc7P69B	MagniberDecrypt.zip
3/31	bnxzoucsx	E88SzQ33TRi0P9g6	Bo3AIJyWc7iuOp91	MagniberDecrypt.zip
3/31	tzdbkjry	n9p2n9Io32Br75pN	ir922Y7f83bb7G12	MagniberDecrypt.zip
4/1	iuoqetgb	QEsN9KZXSp61P956	lM174P1e6J24bZt1	MagniberDecrypt.zip
4/1	pgvuuryti	KHp4217jeDx019Uk	A4pTQ6886b401JR5	MagniberDecrypt.zip
4/2	zpnjelt	LyAAS6Ovr647GO65	nS3A41k9pccn03J2	MagniberDecrypt.zip
4/2	gnhnzhu	I0727788KuT5kAqL	sCnHApaa61l5U2R0	MagniberDecrypt.zip
4/3	hssjfbd	u5f1d693LGkEgX07	kV35Z1K3JB7z6P06	MagniberDecrypt.zip
4/3	ldolfoxwu	i24720y16f10qJ21	fX5U9Z6A2j8ZUvkO	MagniberDecrypt.zip
4/3	zskgavp	nuu9WO56Gc0N5hn7	ASY0d6dlyrEH6385	MagniberDecrypt.zip

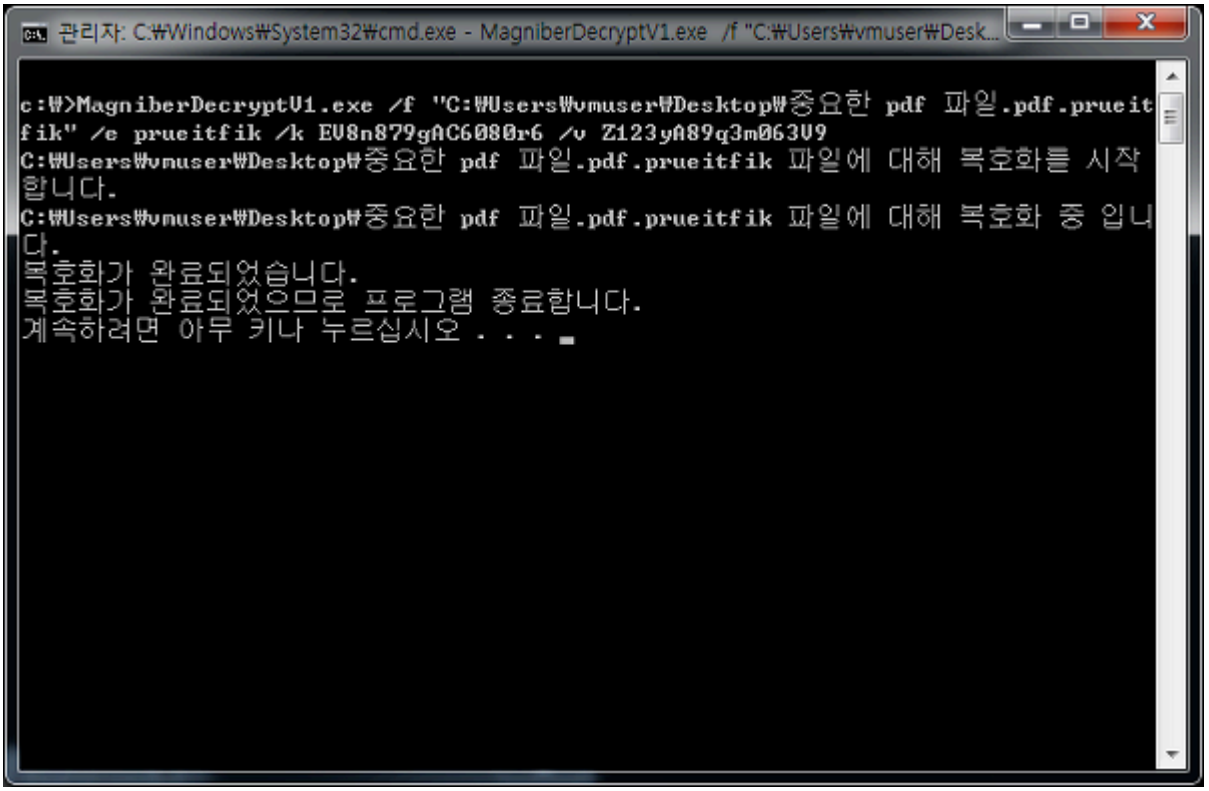
4/3	gwinpyizt	dcQOje3dzW469125	T5438Nl5VI62XxM8	MagniberDecrypt.zip

표에 언급된 예제 중, 3월 30일자의 prueitfik 확장자를 갖는 파일에 대해 복구툴을 이용한 복구 방법은 다음과 같다. **(* cmd.exe 를 관리자 권한으로 실행)**

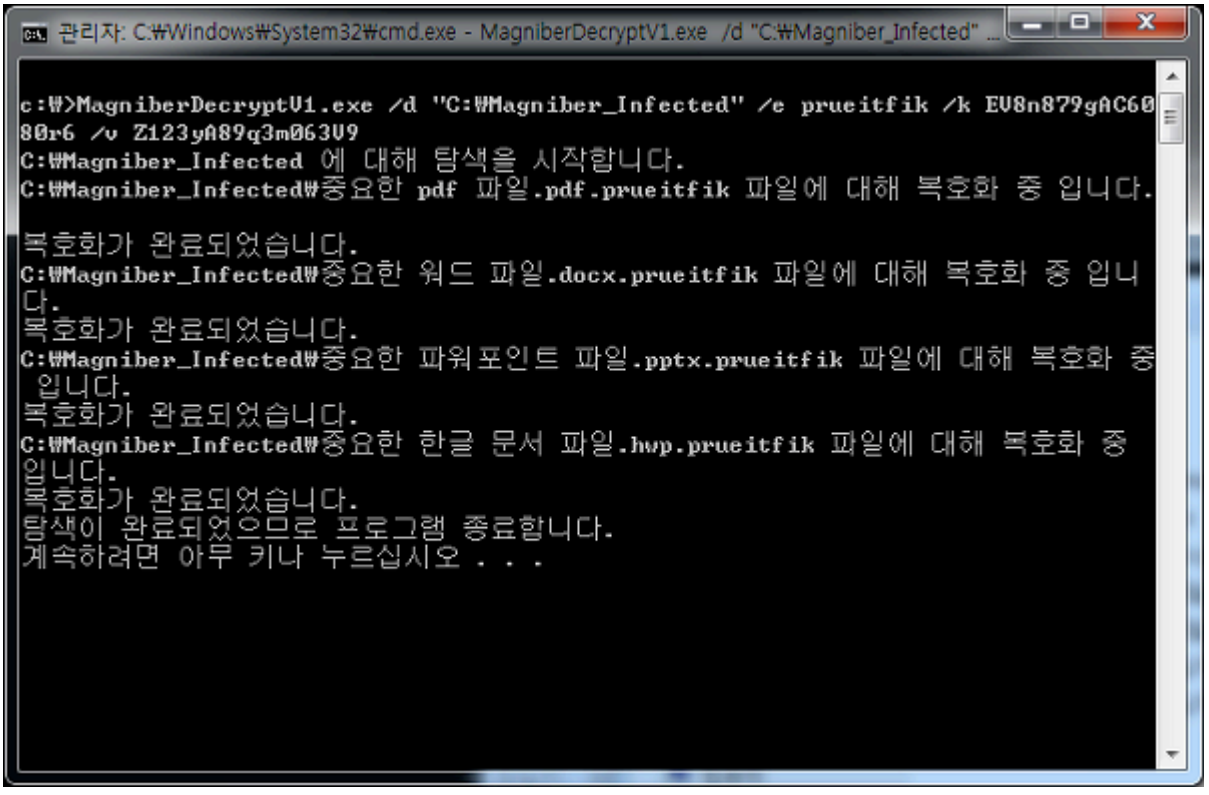


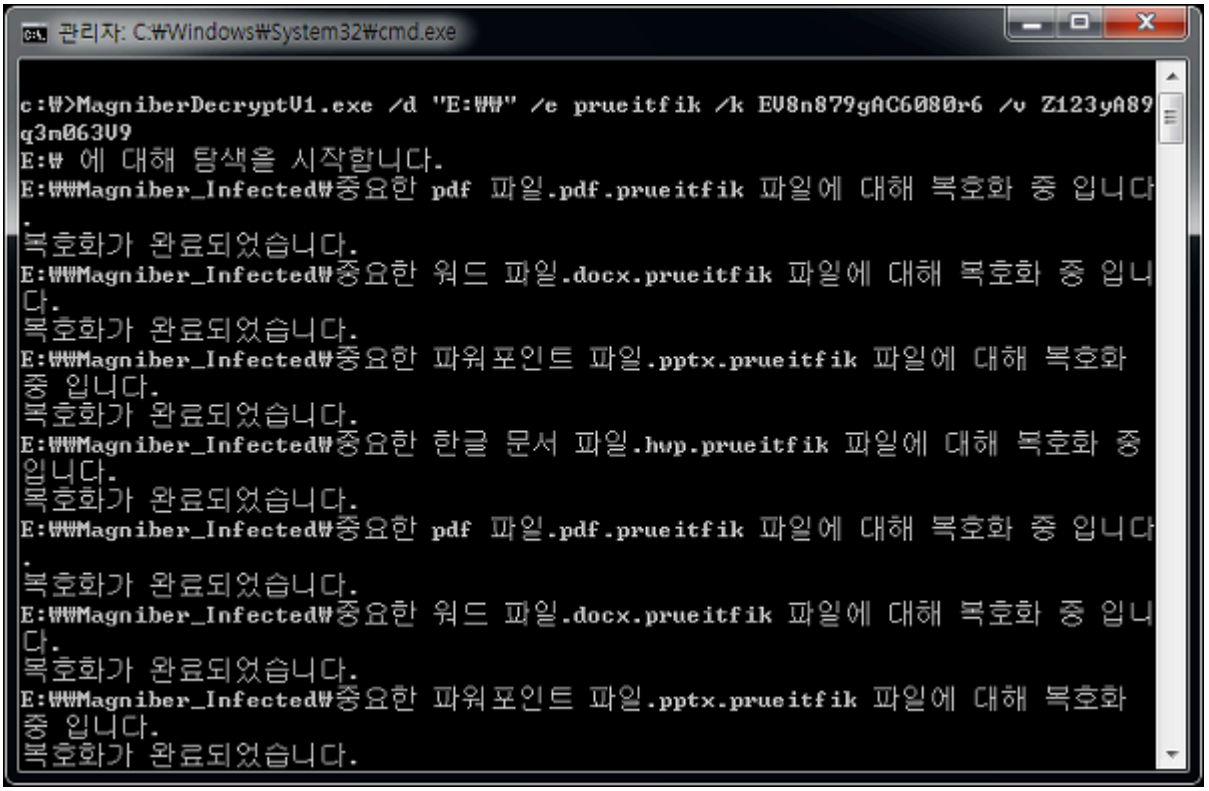
1) 단일 파일에 대해 복구할 경우

/f 옵션에 파일에 대한 경로를 지정한 후 “/e 확장자 /k 키 /v 벡터 값”을 입력한다.



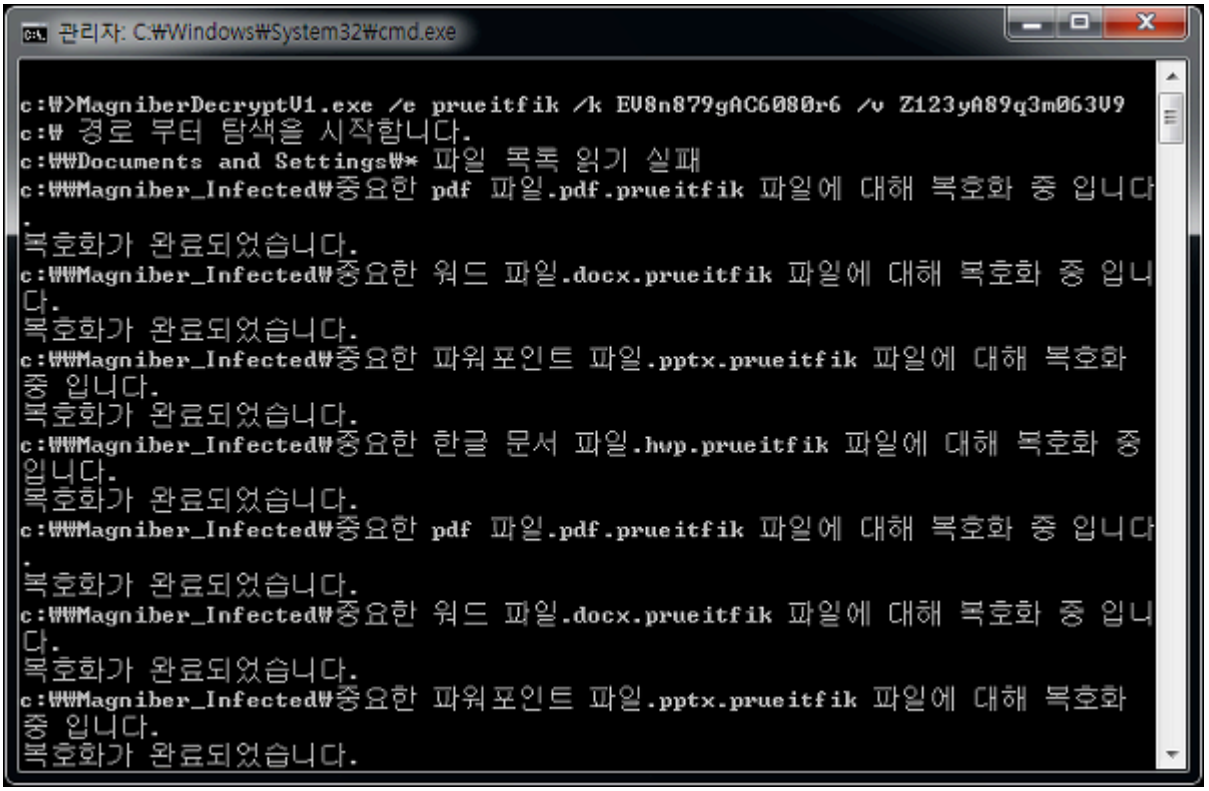
2) 특정 드라이브(이동식 디스크 등) 혹은 폴더에 대해 전체 복구할 경우





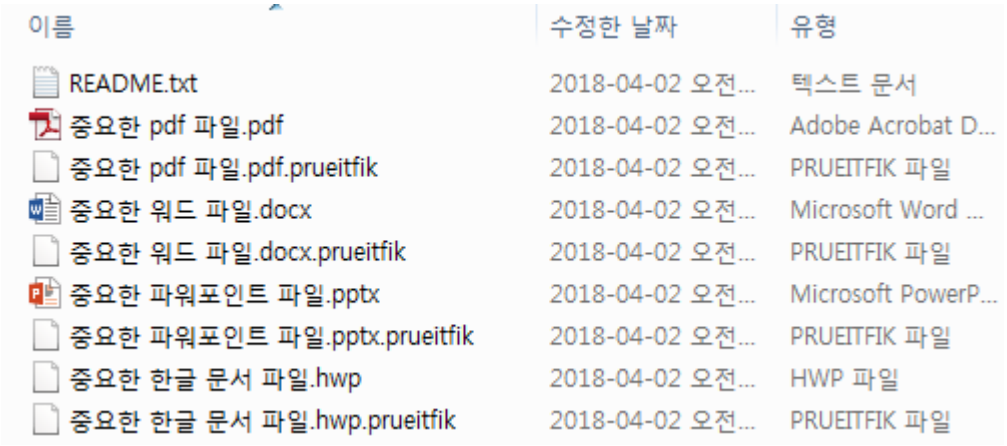
3) “c:” 부터 복구할 경우

특정 폴더 나 드라이브를 지정하지 않더라도, c: 경로 부터 탐색 한다. 이 때는 /f, /d 옵션을 주지 않아도 된다.



※ 암호화된 파일이 존재하는 특정 폴더에 대해서 “파일 목록 읽기 실패”할 경우에는 임의로 새 폴더를 생성하여 해당 폴더에 파일들을 저장하고 /d “새 폴더 경로” 옵션을 통해 복호화 하면된다.

복구가 완료될 경우 아래 그림처럼 “.prueitfik” 확장자가 제거된 상태로 같은 경로에 저장된다.



이름	수정한 날짜	유형
README.txt	2018-04-02 오전...	텍스트 문서
중요한 pdf 파일.pdf	2018-04-02 오전...	Adobe Acrobat D...
중요한 pdf 파일.pdf.prueitfik	2018-04-02 오전...	PRUEITFIK 파일
중요한 워드 파일.docx	2018-04-02 오전...	Microsoft Word ...
중요한 워드 파일.docx.prueitfik	2018-04-02 오전...	PRUEITFIK 파일
중요한 파워포인트 파일.pptx	2018-04-02 오전...	Microsoft PowerP...
중요한 파워포인트 파일.pptx.prueitfik	2018-04-02 오전...	PRUEITFIK 파일
중요한 한글 문서 파일.hwp	2018-04-02 오전...	HWP 파일
중요한 한글 문서 파일.hwp.prueitfik	2018-04-02 오전...	PRUEITFIK 파일

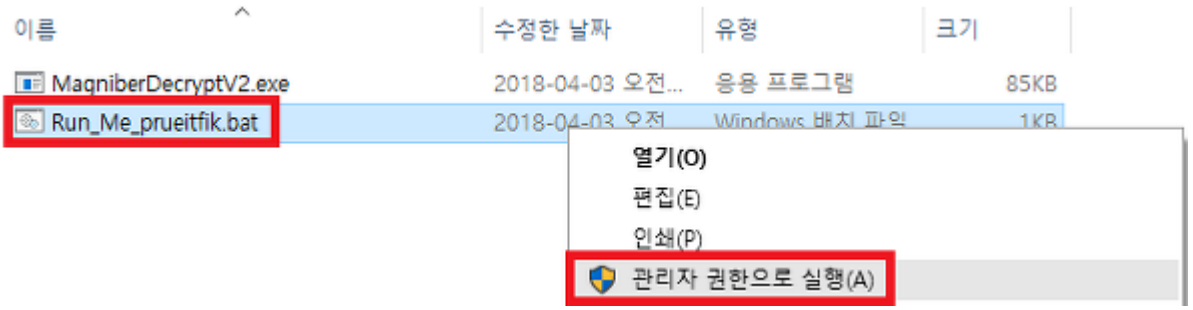
[업데이트 – 2018.04.03]

모든 폴더를 대상으로 **자동**으로 진행하는 bat 파일 추가 업데이트

1. 암호화 확장자에 해당하는 탭의 다운로드 항목의 zip 파일을 다운로드

3월 30일	owxpzylj	u4p819wh1464r6J9	mbfRHUlbKJJ7024P	MagniberDecrypt.zip
3월 30일	prueitfik	EV8n879gAC6080r6	Z123yA89q3m063V9	MagniberDecrypt.zip
3월 31일	rwighmoz	BF16W5aDYzi751NB	B33hQK9E6Sc7P69B	MagniberDecrypt.zip

2. 압축 해제 후 bat 파일을 관리자 권한으로 실행



[복구툴 다운로드]

- MagniberDecryptV1.exe
- md5: 74ebfd6f6d2aa015283880e548826054
- MagniberDecryptV2.exe
- md5: 8949e2d022ee8a7621102f3dfdd964ea

“안랩이 제공하는 전용 백신 및 랜섬웨어 복구툴은 사용자가 비영리 목적으로 다운로드하여 설치 및 이용할 수 있으나 영리적인 목적으로의 사용은 금지되어 있습니다.

만약 영리적인 목적의 이용 · 판매 · 재판매 행위가 확인될 시에는 법적 조치를 취할 수 있음을 밝혀둡니다.”

※ 현재 매그니베르 랜섬웨어에 대한 복구툴 업데이트는 랜섬웨어 암호화 방식 변경 등을 이유로 더 이상 지원되지 않습니다.

Source: http://asec.ahnlab.com/1124