GandCrab, Nemty에 이어 동일 외형의 DEATHRansom 국내 발견 - ASEC

By ATCP

Published: 2019-11-20 · Archived: 2026-04-05 20:11:36 UTC

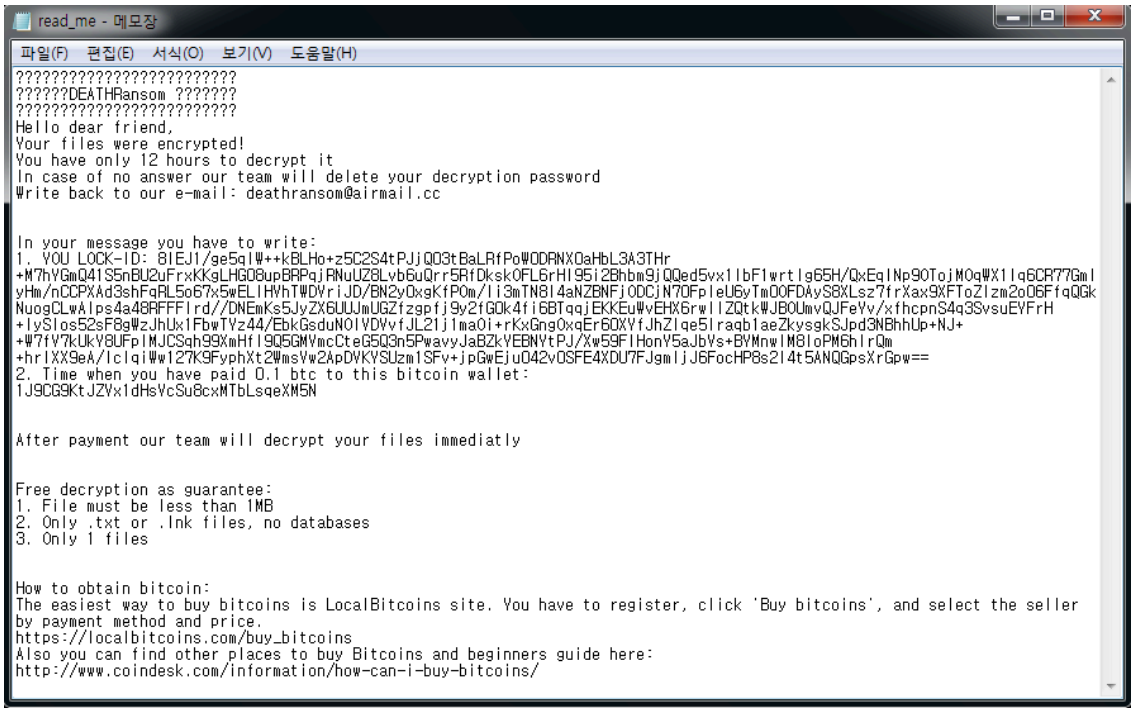
2019년 11월 20일 안랩 ASEC 분석팀은 국내에 유포된 DEATHRansom이라는 새로운 랜섬웨어를 발견하였다. 해당 랜섬웨어는 GandCrab, BlueCrab(=Sodinokibi), Nemty와 동일한 패커를 사용하고 있다.

이 패커(Packer)는 작년에 활발히 유포한 GandCrab부터 BlueCrab과 2019년 9월에 발견 된 Nemty 랜섬웨어, 이번에 발견된 DEATHRansom 까지 다양한 랜섬웨어에 사용되고 있다. 이러한 패커형태는 랜섬웨어 뿐만 아니라 사용자 정보탈취 악성코드와 암호화폐 채굴형 악성코드까지 다양하게 사용하고 있어 사용자의 주의가 필요하다.

DEATHRanom 랜섬웨어는 아래 폴더와 파일을 제외하고 모두 감염 대상이다. 감염 후 확장자 변경은 하지 않고, 감염을 한 폴더마다 랜섬노트인 “read_me.txt” 파일을 생성한다.

	감염 제외 목록
폴더	Programdata, $recycle bin, program files, windows, all users, appdata

파일	read_me.txt, autoexec.bat, desktop.ini, autorun.inf, ntuser.dat, iconcache.db, bootsect.back, boot.ini, ntuser.dat, thumbs.db



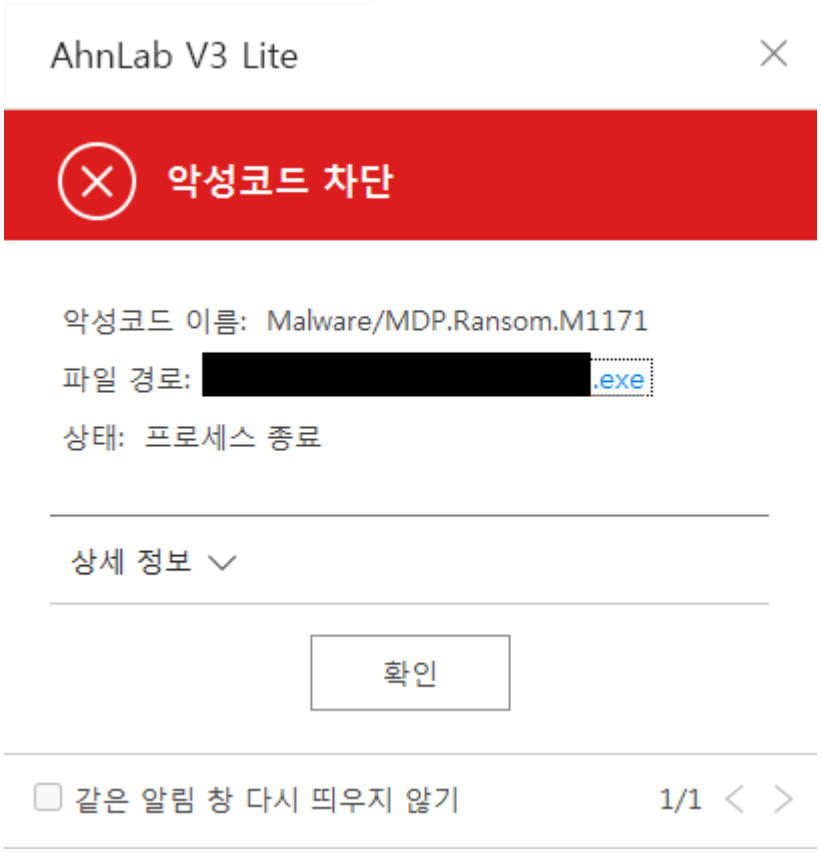
DEATHRansom 랜섬노트

현재 V3에서는 DEATHRansom 랜섬웨어를 다음과 같은 진단명으로 진단하고 있다.

[파일 진단]

- Trojan/Win32.MalPe.R300037 (2019.11.20.03)
- Win-Trojan/MalPeU.mexp (2019.11.21.00)

[행위 진단]



V3 행위탐지 화면

Source: https://asec.ahnlab.com/1269