[단독] GandCrab v4.1.2 암호화 차단방법 (Kill-Switch) - Update(v4.1.3) - ASEC

By ATCP

Published: 2018-07-17 · Archived: 2026-04-05 13:21:48 UTC

2018년 7월 9일 보안업체 Fortinet과 7월 13일 안랩에서 GandCrab v4.1.1에 대한 암호화 차단방법을 공유하였다. 이후 7월 17일 아래와 같이 GandCrab 4.1.2 버전이 새롭게 확인되었으며, 악성코드 내부에는 Fortinet과 AhnLab에 대해 조롱하는 듯한 문구가 삽입되었다.

– "#fortinet & #ahnlab, mutex is also kill-switch not only lockfile ;)"

[참고] https://twitter.com/MarceloRivero/status/1019259361259028480?s=09

4.1.2 버전에서는 단순히 해당 문구가 추가된 것 외에 암호화 차단의 핵심이 되는 *.lock 파일이름 생성 알고리즘이 복잡하게 변경되었다. 파일이름의 길이도 기존 8바이트에서 20바이트로 확장되었다. 안랩 ASEC에서는 변경된 파일이름 생성 알고리즘이 알려진 Salsa20 을 일부 수정한 **Custom Salsa20** 으로 확인하였으며, 이러한 정보를 바탕으로 새로운 암호화 차단툴을 제작하였다.

아래의 그림은 새로운 버전 4.1.2에서 *.lock 파일을 생성하는 코드를 나타내며, 붉은색 표시부분이 새롭게 추가된 것으로 기존의 볼륨정보 외에 Salsa20 함수를 통해 lock 파일이름을 생성하는 것을 알 수 있다.

```
if ( SHGetSpecialFolderPathW(0, (LPWSTR)v1 + 256, 35, 1) )
{
  v2 = (WCHAR *)sub_40542D(0xE0Cu);
  v3 = v2;
  if ( v2 )
  {
    GetWindowsDirectoryW(v2, 0x100u);
    v3[3] = 0;
    if ( GetVolumeInformationW(
           v3,
           v3 + 256,
           0x100u,
           (LPDWORD)v3 + 384,
           (LPDWORD)v3 + 386,
           (LPDWORD)v3 + 385,
           v3 + 512,
           0x100u) )
    {
      wsprintfW(
        &v9,
        L"%X fortinet & ahnlab, mutex is also kill-switch not only lockfile ;)",
        *((_DWORD *)v3 + 384) >> 2);
      sub_402152(&v9, (int)&v6, (LPWSTR)&v7);
      v8 = 0;
      wsprintfW((LPWSTR)v1, L"%s\\%s.lock", (char *)v1 + 0x200, &v7);
      v4 = CreateFileW((LPCWSTR)v1, 0x40000000u, 0, 0, 1u, 0x4000000u, 0);
      v10 = (char *)v4 + 1 != 0;
      v8 = (char *)v4 + 1 != 0;
    }
    else
    {
      GetLastError();
    }
```

v4.1.2

Custom Salsa20

[그림-1] GandCrab v4.1.2의 lock 파일생성

Salsa20 암호화 시 사용되는 Key, Vector 정보는 다음과 같다.

- KEY[] (16진수): 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
- VEC[] (16진수): 01 02 03 04 05 06 07 08
- 입력값: “380978EA fortinet & ahnlab, mutex is also kill-switch not only lockfile ;)” (단, 380978EA 값은 드라이브 볼륨을 통해 생성된 정보로 사용자마다 상이)

변경된 파일이름만 특정 경로에 존재하면, 여전히 암호화 차단(Kill-Switch)이 가능함을 확인하였으며, lock 파일의 생성위치 및 사용방법은 기존과 동일하며 아래와 같다.

폴더: CSIDL_COMMON_APPDATA

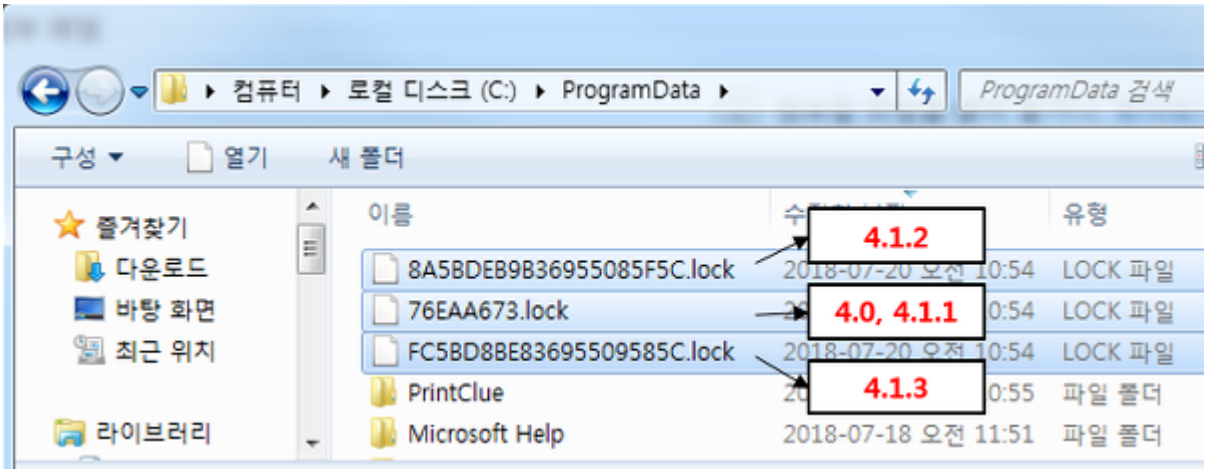
- Win XP: C:Documents and SettingsAll UsersApplication Data
- Win 7, 8, 10: C:ProgramData

파일: 8A5BA4B9C369950A5FEC.lock (예제)

- 파일명은 루트 드라이브의 볼륨정보 + **Custom Salsa20** 알고리즘을 바탕으로 생성
- GandCrab_KillSwitch_(4.0_4.1.1_4.1.2_4.1.3).zip

툴 사용방법

- 첨부한 실행파일을 다운로드 받은 후, 오른쪽 마우스 클릭하여 '관리자 권한으로 실행'
- 아래와 같이 해당 폴더(Common AppData)에 *.lock 파일이 생성됨을 확인



V3제품에서도 현재 유포되는 GandCrab v4.1.2 유형에 대해 아래와 같이 진단/대응하고 있다. 안랩 ASEC은 국내에 유포 중인 GandCrab 랜섬웨어 관련하여 지속적인 모니터링을 수행하고 있으며, 새로운 버전도 V3제품에서는 사전 대응이 가능한 상황이다.

- **행위진단: Malware/MDP.Ransom**
- **파일진단: Win-Trojan/Gandcrab04.Exp (2018.07.17.00)**
- **MD5: f153ac5527a3e0bc3e663b8e953cc529**

국내에 유포되는 GandCrab 랜섬웨어는 이력서 혹은 정상 프로그램으로 위장하여 사용자 클릭을 유도하는 형태임을 확인하였으며, 아래와 같은 파일명들이 사용되고 있다.

– 안녕하세요 입사지원하는 임정연입니다임정연임정연unclej.exe

– micro_office_2010.exe

– 쯔꾸르_게임.exe

– 뿌요뿌요_테트리스.exe

– 포토_리커버리.exe