[S2W LAB] Analysis of Clop Ransomware suspiciously related to the Recent Incident

Archived: 2026-05-05 02:23:56 UTC

Author: TALON (BLKSMTH, HOTSAUCE)

Date: 2020-11-23

Last Modified : 2020-12-02

최근 발생한 침해사고와 관련된 것으로 추정되는 Clop 랜섬웨어를 확보하여 분석 진행하였으며 그 결과에 대한 요약은 아래와 같음

기존 Clop 랜섬웨어의 경우, 암호화된 파일의 내부 컨텐츠와 확장자를 변경하고 암호화키는 파일의 마지막에 저장하였으나 변종 Clop의 경우 암호화된 파일별로 별도 키파일을 생성하여 암호화키를 저장해둠

키파일 확장자 : .cllp

키파일 헤더 : Cllp^_-

랜섬노트 (Ransom Note) 확인결과, 다크웹 상에서 유출 데이터를 공개하는 기존 Clop 랜섬웨어의 유출 사이트에 있는 컨택 포인트(Email)와 동일함을 확인

동일한 서명 정보를 갖는 Clop Ransomware를 Virustotal에서 추가 발견 (Build time: 11월 21일)

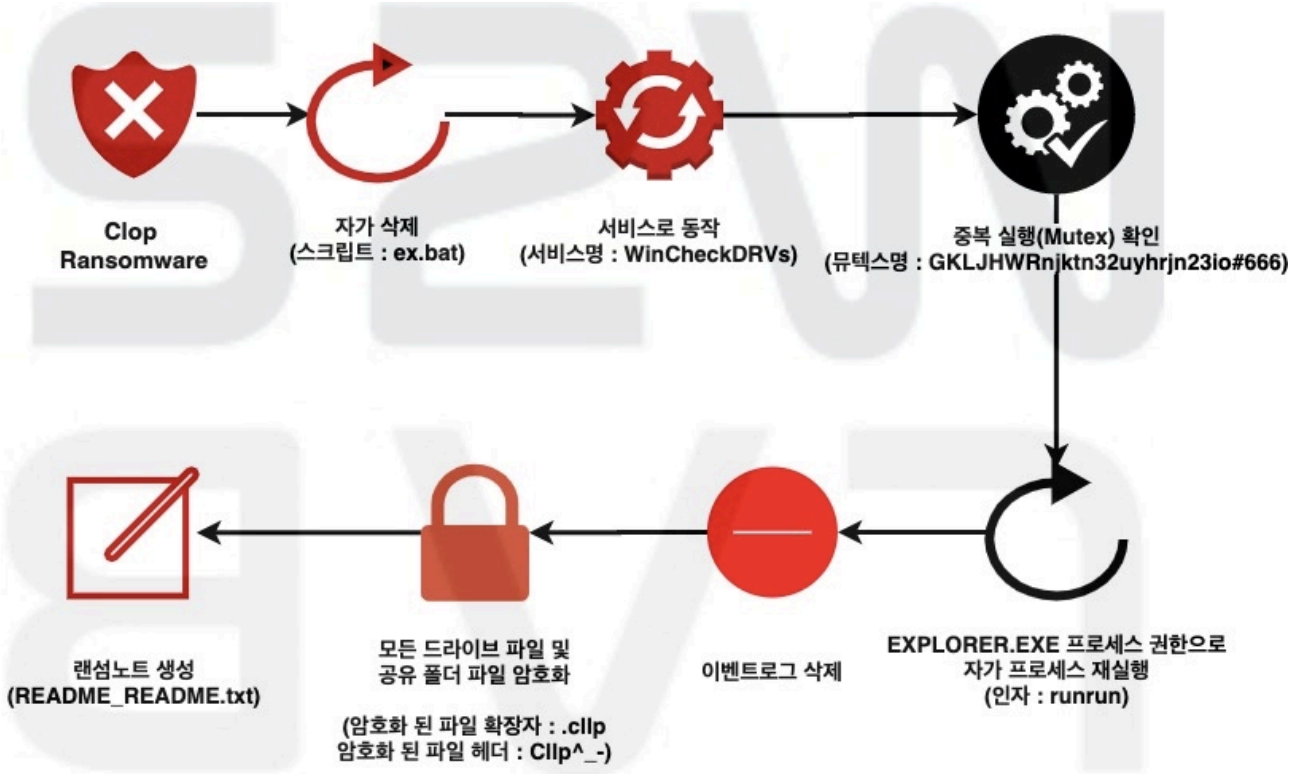
정확한 유포 방식은 현재 조사 중으로 확인된 바 없으나 과거 Clop Ransomware 공격 사례를 통하여 아래와 같은 방식들로 추정

SMB 취약점 등을 이용한 내부 침투

AD (Active Directory) 관리자 계정 유출로 인한 내부 시스템 대규모 전파

스피어피싱 이메일 내 문서형 악성코드 등을 이용한 침투

> MD5 : 8b6c413e2539823ef8f8b85900d19724 SHA-1 : 2d92a9ec1091cb801ff86403374594c74210cd44 SHA-256 : 3d94c4a92382c5c45062d8ea0517be4011be8ba42e9c9a614a99327d0ebdf05b Type : Win32 EXE (PE32 executable for MS Windows (GUI) Intel 80386 32-bit) Build Time : 2020-11-20 18:18:18



외형상으로는 악성코드의 구조를 파악 할 수 없게 메모리에 할당(VirtualAlloc)하여 실행되도록 구성

ex.bat 이라는 파일을 생성하여 자가삭제를 수행

```
strcpy(ex_bat, "ex.bat");
strcpy(CreateFileA_, "CreateFileA");
strcpy(CreateProcessA_, "CreateProcessA");
strcpy(WriteFile_, "WriteFile");
strcpy(CloseHandle_, "CloseHandle");
strcpy(GetModuleFileNameA_, "GetModuleFileNameA");
strcpy(lstrcpyA_, "lstrcpyA");
strcpy(del_, ":R\r\ndel \"");
strcpy(if_exist, "\"\r\nif exist \"");
strcpy(goto_del, "\" goto R\r\ndel \"");
v20[0] = '"';
v20[1] = '\r';
v20[2] = '\n';
v20[3] = 0;
CreateFileA__ = a2(a1, CreateFileA_);
lstrcpyA__ = a2(a1, lstrcpyA_);
GetModuleFileNameA__ = a2(a1, GetModuleFileNameA_);
CloseHandle__ = a2(a1, CloseHandle_);
WriteFile__ = a2(a1, WriteFile_);
CreateProcessA__ = a2(a1, CreateProcessA_);
GetModuleFileNameA__(0, v26, 260);
result = CreateFileA__(ex_bat, 0x40000000, 0, 0, 2, 128, 0);
v16 = result;
if ( result != -1 )
{
  ARG_01_1040(v15, 0, 256);
  lstrcpyA__(v15, del_);
  sub_1080(v15, v26);
  sub_1080(v15, if_exist);
  sub_1080(v15, v26);
  sub_1080(v15, goto_del);
  sub_1080(v15, ex_bat);
  sub_1080(v15, v20);
  v3 = sub_10E0(v15);
  WriteFile__(v16, v15, v3, &goto_del[16], 0);
  CloseHandle__(v16);
  ARG_01_1040(v10, 0, 68);
  ARG_01_1040(v19, 0, 16);
  v10[0] = 68;
  v10[11] = 1;
  v11 = 0;
  result = CreateProcessA__(0, ex_bat, 0, 0, 0, 16, 0, 0, v10, v19);
}
```

MD5 : 14B7069B25B04EBA875F264BE4F140DA

Build Time : 2020-11-20 14:35:08

악성코드 행위 흐름

자기 자신을 서비스로 등록하여 실행

서비스 명 : WinCheckDRVs

뮤텍스를 이용한 중복 실행 여부 체크

뮤텍스 명 : GKLJHWRnjktn32uyhrjn23io#666

RDP 원격 공유 폴더 암호화 시도

실행 중인 EXPLORER.EXE의 권한 토큰 획득

활성화 된 RDP 세션에 로그인 되어있는 유저의 Primary Access Token 수집

획득한 EXPLORER.EXE 토큰의 유저 명과 동일한 계정의 RDP 세션 토큰 수집

유저 명의 길이가 5이하일 경우 활성화된 세션의 토큰 수집

winsta0\default에 “runrun”을 파라미터로 주어 자기 자신 추가 실행

해당 세션의 원격 공유 폴더를 순회하며 암호화 시도

이벤트 로그 삭제 명령어 실행

> Loading PowerShell code…

A~Z까지 모든 드라이브를 순회하며 암호화 시도 (플로피 디스크, CD-ROM 등은 제외)

일부 기능이 추가된 Clop ransomware에는 Restart Manager API를 이용하여 프로세스나 서비스를 강제로 재시작 후 사용 중인 파일에도 암호화를 시도

랜섬웨어 하드코딩되어있는 RSA Public Key

> Loading Plain Text code…

Desktop 경로는 암호화 대상 폴더에서 제외

파일 명을 ROL 연산으로 해시 값 추출 및 비교하여 일부 파일은 암호화 대상에서 제외

Count

특정 확장자 파일 암호화 대상에서 제외

암호화 제외 대상 확장자

.CI0P : 과거 암호화 파일 확장자

.OCX : ActiveX 파일

.DLL : 동적 라이브러리

.EXE : 실행 파일

.SYS : 드라이버 파일

.LNK : 바로가기 파일

.ICO : 아이콘 파일

.INI : 설정파일

.MSI : Installer 파일

.CHM : 도움말 파일

.HLF

.LNG : 언어팩 파일

.TTF : 폰트 파일

.CMD : 배치 파일

.BAT : 배치 파일

.CLLP : 현재 랜섬웨어 암호화 파일

암호화 대상 파일의 크기에 따라 암호화 방식이 다름

sizeof(TargetFile) < 17KB : 암호화 제외

17KB < sizeof(TargetFile) < 2.13MB : 0x4000부터 EOF(End of File)까지 암호화

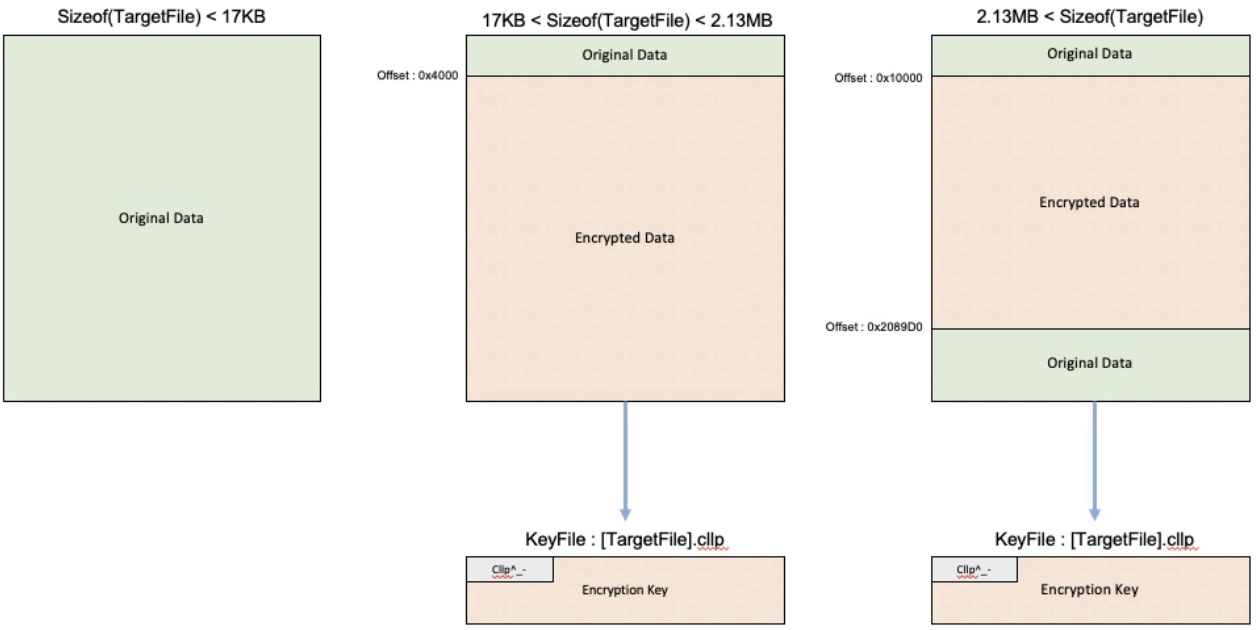
일반 파일 입출력 방식 사용

2.13MB < sizeof(TargetFile) : 0x10000~0x2089D0 오프셋 범위 암호화

대용량 파일 처리시 효율적이고 속도가 빠른 MMF 방식 사용

MMF : Memory Mapped File의 약자이며, 메모리 맵 파일을 통해 프로세스의 가상 메모리 주소 공간에 파일을 맵핑한 뒤 가상 메모리 주소에 직접 접근하는 것으로 파일 읽기/쓰기를 대신함

아래는 Clop 랜섬웨어의 암호화 방식에 대한 도식도



Source: https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-c26daec604da4db6b3c93e26e6c7aa26