



# 악성코드 분석 기초

IT정보공학과 김아은

# INDEX

악성코드 분석 기초

## ■ 악성코드 종류

## ■ 공격 시나리오

- TA505 위협 그룹
- BMP 이미지에 숨겨진 악성코드

# 악성코드(Malware)란?

사용자의 PC에 해를 끼치는, 악의적인 목적으로 만들어진 코드를 모두 통틀어 이른 말

- 랜섬웨어
- 봇넷
- 백도어
- 트로이 목마
- 파일리스
- 루트킷
- ⋮



# 악성코드 종류

## 1. 랜섬웨어(ransomware)

- 컴퓨터 시스템을 감염시켜 접근을 제한하고 데이터를 인질로 일종의 몸값(ransom)을 요구하는 악성 소프트웨어의 한 종류
- 증상 : 몸값을 요구하는 이미지 창이나 텍스트 파일 존재, 특정 파일 열 수 없고 에러메시지, 파일 확장자가 바뀌거나 사라짐

## 2. 봇넷(botnet)

- Robot + Network를 합성한 단어로, 봇에 감염된 좀비PC들로 구성되는 네트워크
- 동일 네트워크상에 있는 취약성한 모든 기기를 감염시켜 특정 기능을 자동으로 수행
- 증상 : 컴퓨터의 동작 및 인터넷 활용 속도가 느려지는 현상



# 악성코드 종류

## 3. 백도어(back door)

- 공격자가 언제든지 시스템에 접속 가능하게 만든 뒷문
- 사용자가 눈치 못채게 작동하며 컴퓨터 데이터를 가져오거나 실행시킬 수 있음
- 증상 : 무증상

## 4. 트로이 목마(trojan horse)

- 정상적인 기능을 하는 것처럼 위장하여 실제로는 다른 기능을 하는 프로그램
- 트로이 목마는 시스템에 대한 재침입을 위한 백도어로 사용되는 경우가 많음
- 증상 : 패스워드 및 키보드 입력 가로채기, 시스템 파일 삭제 및 부팅오류, 백신·방화벽 작동 방해 및 종료, 보안패치 사이트 접속 차단



# 악성코드 종류

## 5. 파일리스(fileless)

- 시스템 내부에 파일 형태로 저장되지 않고 메모리에 바로 실행
- 증상 : 컴퓨터가 봇넷 서버에 연결하는 것과 같은 비정상적인 네트워크 패턴 및 추적, 시스템 메모리의 손상 징후

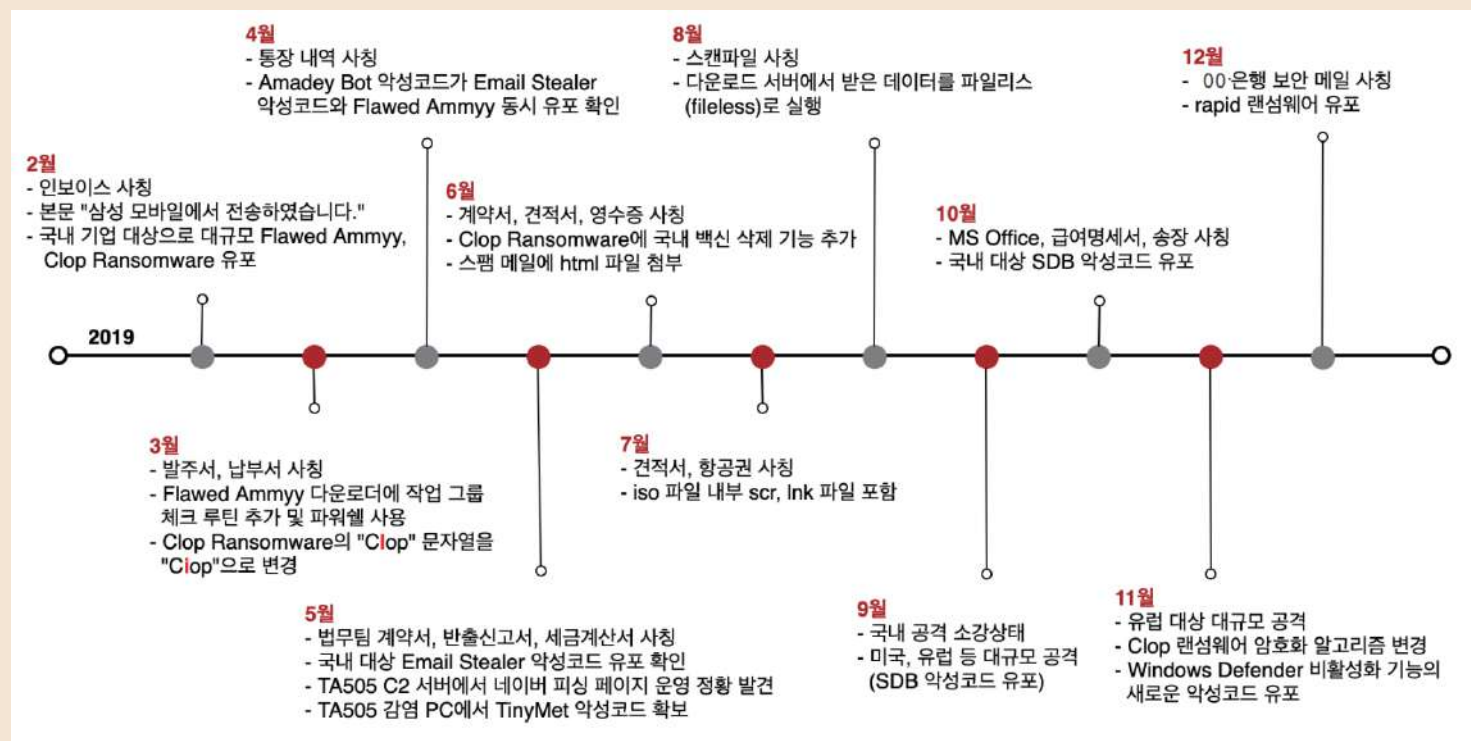
## 6. 루트킷(rootkit)

- 시스템에 전반적으로 접근할 수 있는 루트(Root) 권한을 쉽게 얻게 해주는 도구(Kit)
- 파일이나 레지스트리를 숨기는 것이 루트킷이 하는 대표적인 일
- 증상 : 과도한 CPU 또는 인터넷 대역폭 사용



# 공격 시나리오

## 2019년, 국내를 대상으로 대규모 공격을 한 TA505 위협 그룹



- 국내 기업을 공격 대상
- 신뢰할 수 있는 전송자로 위장하여 메일 전송
- 다양한 악성코드 유포

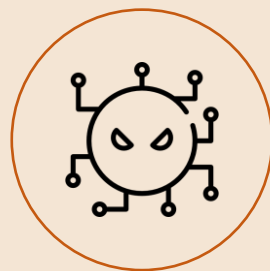


# 공격 시나리오 -TA505 위협 그룹

최초 감염



추가 악성코드 감염



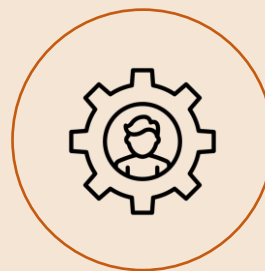
랜섬웨어 감염



정보 탈취



내부망 제어

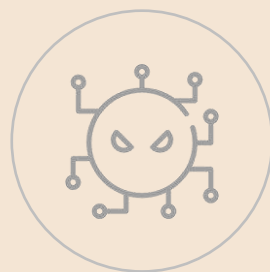




# 공격 시나리오 -TA505 위협 그룹

## 1. 최초 감염

스피어 피싱 메일에 첨부된  
악성 파일 실행



- 스피어 피싱 : 신뢰할 수 있는 전송자로 위장하여 특정 개인 및 기업을 대상으로 시도하는 피싱
- 파일 첨부, 본문 내 링크 형태로 악성 파일 다운로드 유도
- 악성 파일은 악성코드를 다운받을 수 있는 다운로더를 설치
- 본격적인 공격에 사용되는 Flawed Ammyy 원격 제어 악성코드를 다운로드 받기 위한 중간 과정 역할



## 파일을 첨부한 경우

☆ 국세청

2019년 5월 30일 오전 8:14

세청

국세청송장  
받는 사람:

HomeTax 국세청 홈택스

안녕하세요.  
국세청 전자[세금]계산서입니다.  
[전자세금계산서 발급 메일 안내]

본메일은 보안메일입니다.

본 메일은 국세청 홈택스를 이용하여 국일명판사 사업자가 주식회사 현대금형기술.

- 발급일자 : 2019년 05월 30일

- 본 메일이 수신인과 관련없는 경우 수신거부/해제(여기) 를 클릭하시기 바랍니다.

\*메일 내용을 확인하기 위해서는 첨부파일을 클릭하십시오.

전자(세금)계산서 첨부파일이 열리지 않을 시 조치 방법

1. 첨부파일을 사용자PC에 저장

2. 저장한 첨부파일을 오른쪽마우스 클릭 후 연결프로그램에서 [Internet Explorer] 선택

국세청  
National Tax Service

세종특별자치시 국세청로 8-14 국세청(정부세종2청사 국세청동) (우편번호) 30128  
Copyright© National Tax Service. All rights reserved.

☆ KOREAN AIR

2019년 7월 25일 오전 9:12

KA

대한항공 e-티켓 확인증입니다  
받는 사람:  
답장 받는 사람:

KOREAN AIR

www.koreanair.com

e-티켓 이용안내 메일 입니다.

e-티켓 확인증은 첨부된 PDF 파일을 확인해 주시기 바랍니다.

① PC에서 pdf 파일이 보이지 않는다면 Adobe Reader를 다운받으시기 바랍니다.

Adobe Reader 다운로드

더 빠르고 편리한 추천 서비스

키오스크/웹  
/모바일  
체크인

스카이패스  
적립안내

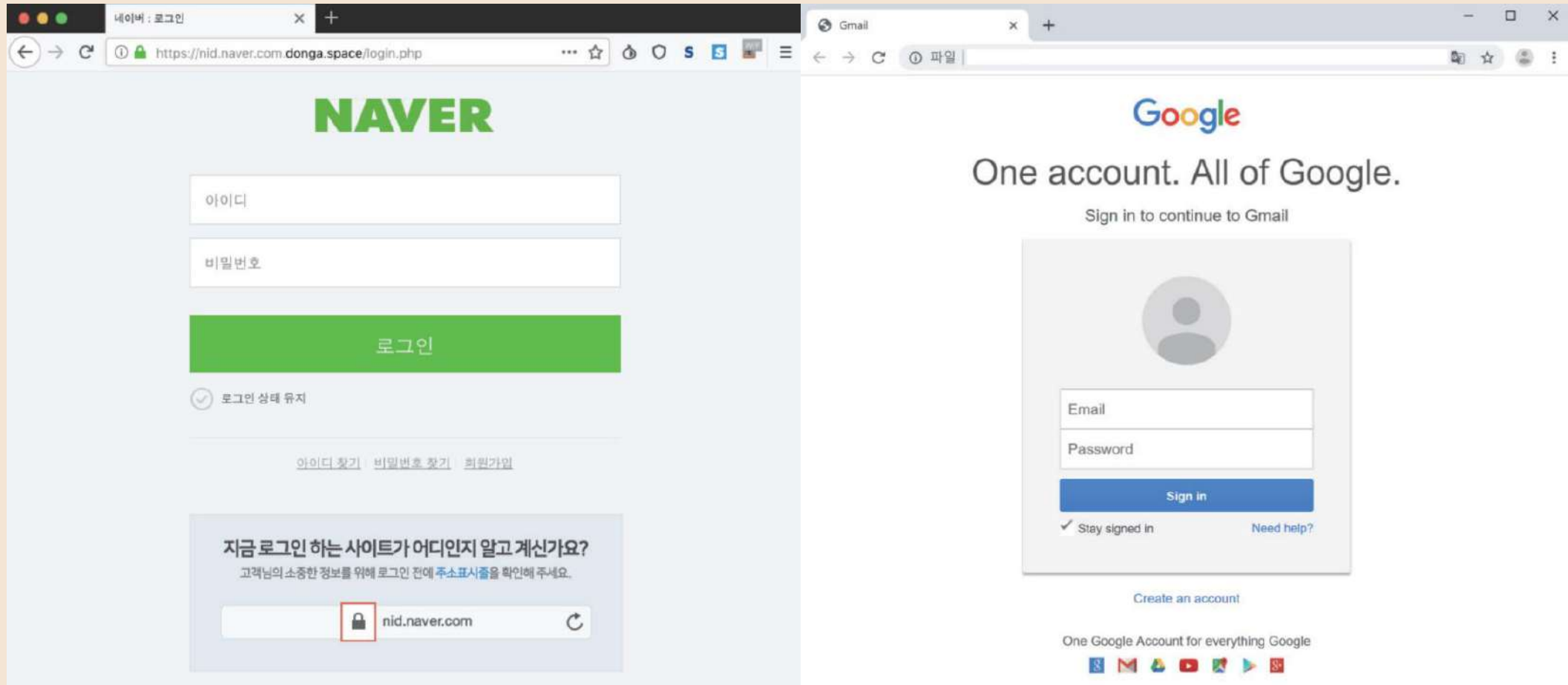
공항가기 전 확인

국내선 운임  
신분 확인 및  
증빙서류

수하물  
제한

기타 안내

## 본문 내 링크로 유도한 경우



# 본문 내 링크로 유도한 경우

☆ 삼덕회계법인 (via Dropbox)

2019년 10월 23일 오전 9:42

회

삼덕회계법인 님이 '송장 N98300 10.21.19' 폴더를 공유했습니다.

받는 사람: \_\_\_\_\_



안녕하세요.

삼덕회계법인님이 Dropbox의 '송장 N98300 10.21.19' 파일을 볼 수 있도록 회원님을 초대했습니다.

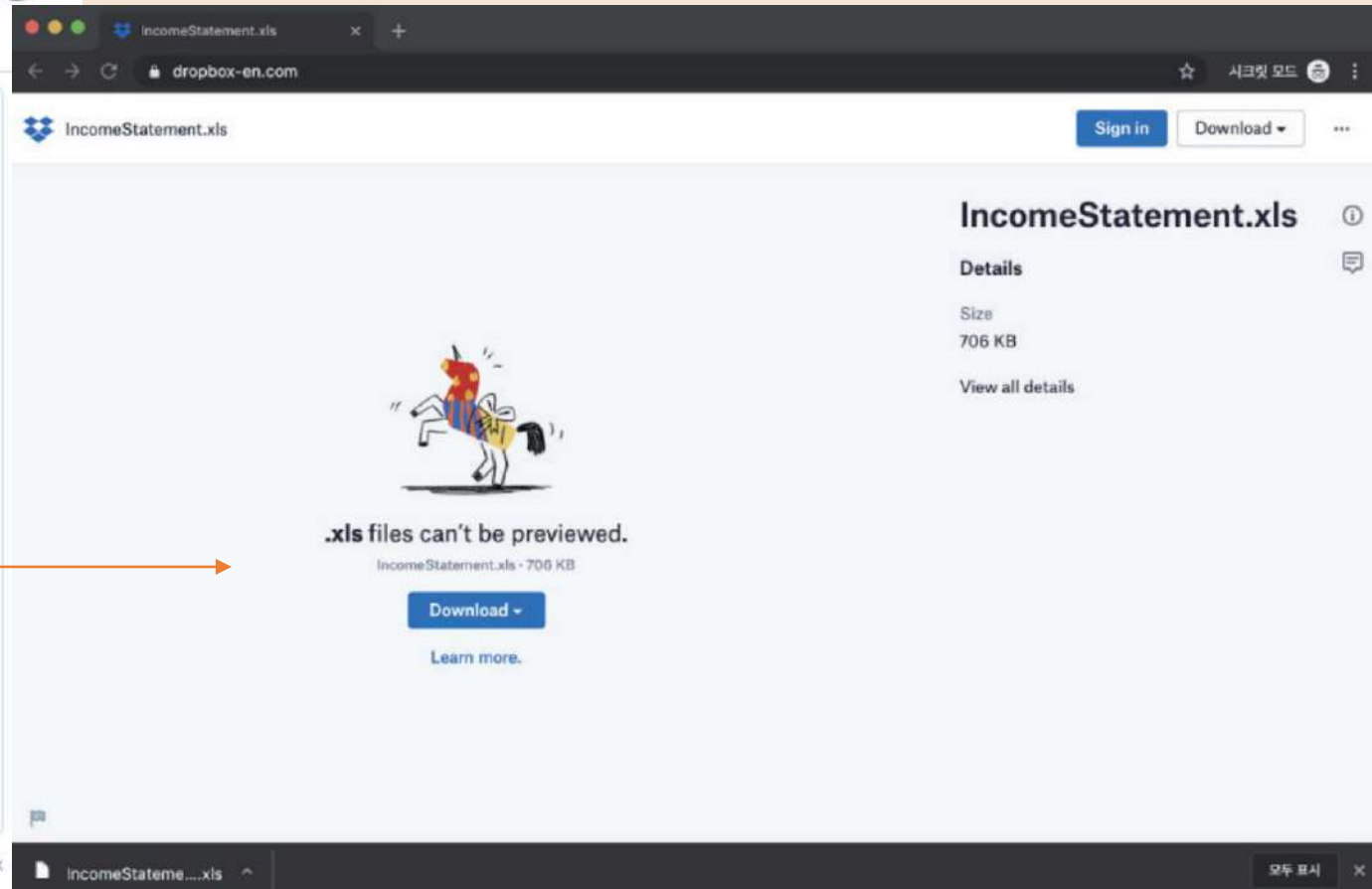
파일 보기

즐겁게 사용하세요!

Dropbox팀 드림

Dropbox에 신고하기

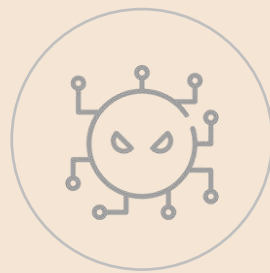
© 2019 Dropbox



# 공격 시나리오 -TA505 위협 그룹

## 2. 정보 탈취

원격 제어 악성 코드를 통한  
PC 정보 탈취

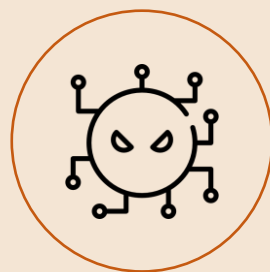


- 다운로드를 통해서 설치된 Flawed Ammyy 원격 제어 악성코드
- 현재 프로세스 목록 중 국내 백신을 포함한 특정 백신 프로세스가 존재할 경우 악성코드를 강제 종료시키고, 백신 프로세스가 존재하지 않을 경우 감염된 PC 정보를 탈취하여 C&C 서버에 전송
- C&C 서버에 전송하는 탈취 정보 : PC 식별 값, OS 정보, 권한(관리자, 유저 등), 백신 제품 명, 악성코드 빌드 시간 등
- C&C 서버로부터 명령 받아 수행하는 기능 : 키보드/마우스 이벤트 수집, 파일 전송/쓰기/읽기, 스크린 샷 정보 수집 등



# 공격 시나리오 -TA505 위협 그룹

## 3. 추가 악성코드 감염 탈취한 정보를 기반으로 추가 악성코드 감염



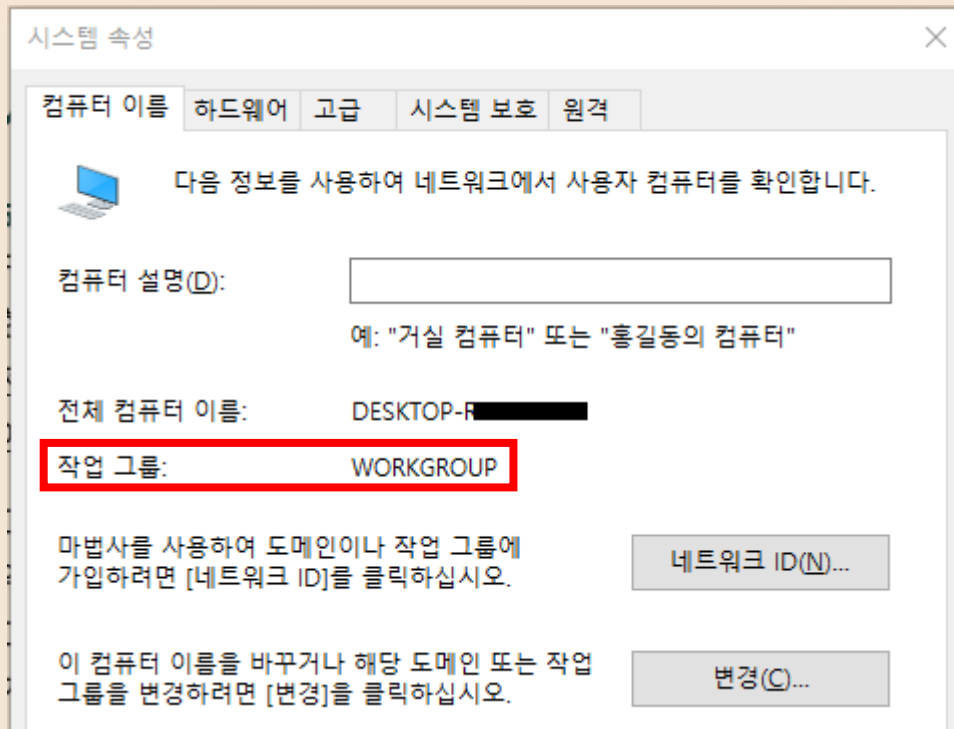
- 감염된 PC의 작업 그룹을 탐색하여 개인 또는 기업 여부를 판별
- 기업 PC일 경우, 다양한 악성코드 감염(Cobalt Strike, TinyMey, Amadey Bot, Email Stealer, SDBbot)



# 공격 시나리오 -TA505 위협 그룹

## 3. 추가 악성코드 감염

감염된 PC의 작업 그룹을 탐색하여 개인 또는 기업 여부를 판별



- 작업 그룹이 기본값인 "WORKGROUP"일 경우  
개인 PC로 판단해 악성 행위를 중지한 후  
자가 삭제하여 흔적을 지움
- AD서버 도메인 값이 반환될 경우  
기업 PC로 판단해 악성 행위를 수행



# 공격 시나리오 -TA505 위협 그룹

## 3. 추가 악성코드 감염

- 1) Cobalt Strike : 내부망을 대상으로 SMB 취약점을 이용해 AD 서버 해킹을 시도  
만약 AD 서버 도메인을 사용한 경우 AD 서버 관리자 계정을 탈취
- 2) TinyMet : 실행되는 옵션에 따라 C&C 서버와 리버스 셸 연결 시도
- 3) Amadey Bot : 감염된 PC 정보 탈취 및 추가 악성코드 다운로드 등의 공격 수행이 가능
- 4) Email Stealer : 감염된 PC에 존재하는 이메일 정보를 탈취
- 5) SDBbot : 정상 서비스에 악성코드를 주입하여 원격 제어 기능을 수행

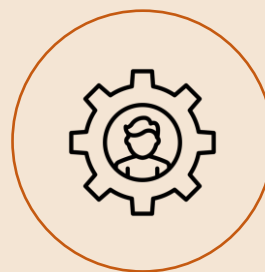
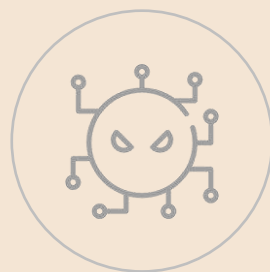




# 공격 시나리오 -TA505 위협 그룹

## 4. 내부망 제어

추가 악성코드를 통해 내부망 탐색  
및 AD서버 관리자 권한 획득



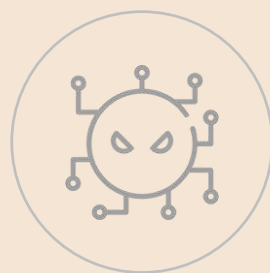
- Cobalt Strike 등의 추가 악성코드로 AD 서버 관리자 계정이 탈취



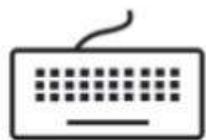
# 공격 시나리오 -TA505 위협 그룹

## 5. 랜섬웨어 감염

획득한 AD 서버 관리자 권한으로  
내부망 PC에 대규모 랜섬웨어 감염



- Clop 랜섬웨어 : 파일을 암호화하고 확장자를 '.Clop'으로 변경하는 랜섬웨어



1. 시스템 언어 확인

2. 백신 탐지 및 우회

3. 윈도우 복원 방지

4. 특정 프로세스 종료

5. 파일 암호화

6. 랜섬노트 생성



# 공격 시나리오 -TA505 위협 그룹

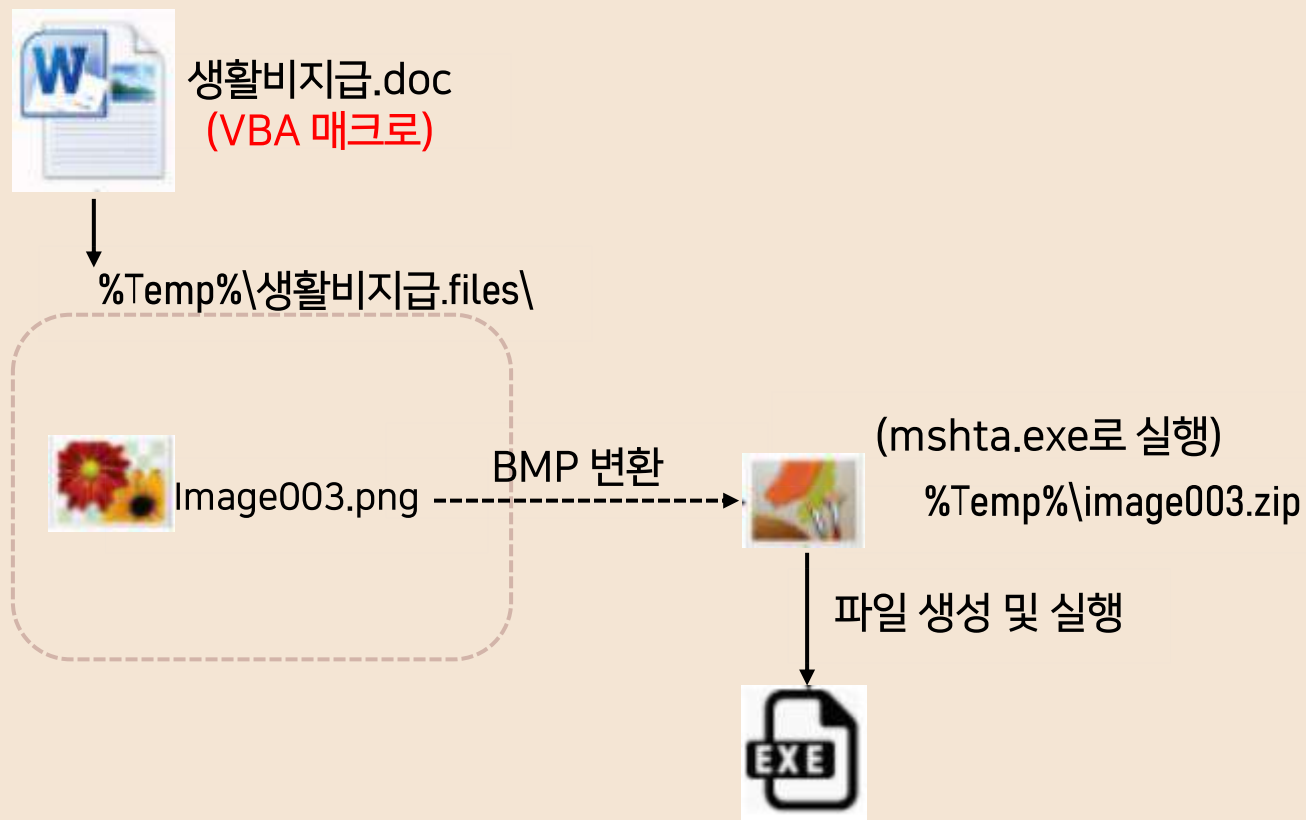
## 유포된 악성코드

- 악성 첨부 문서
- Flawed Ammyy 원격 제어
- Clop 랜섬웨어 : 랜섬웨어
- Cobalt Strike : 루트킷
- Amadey Bot : 봇넷
- Email Stealer : 스파이웨어
- TinyMet : 백도어
- SDBbot : 백도어



# 공격 시나리오

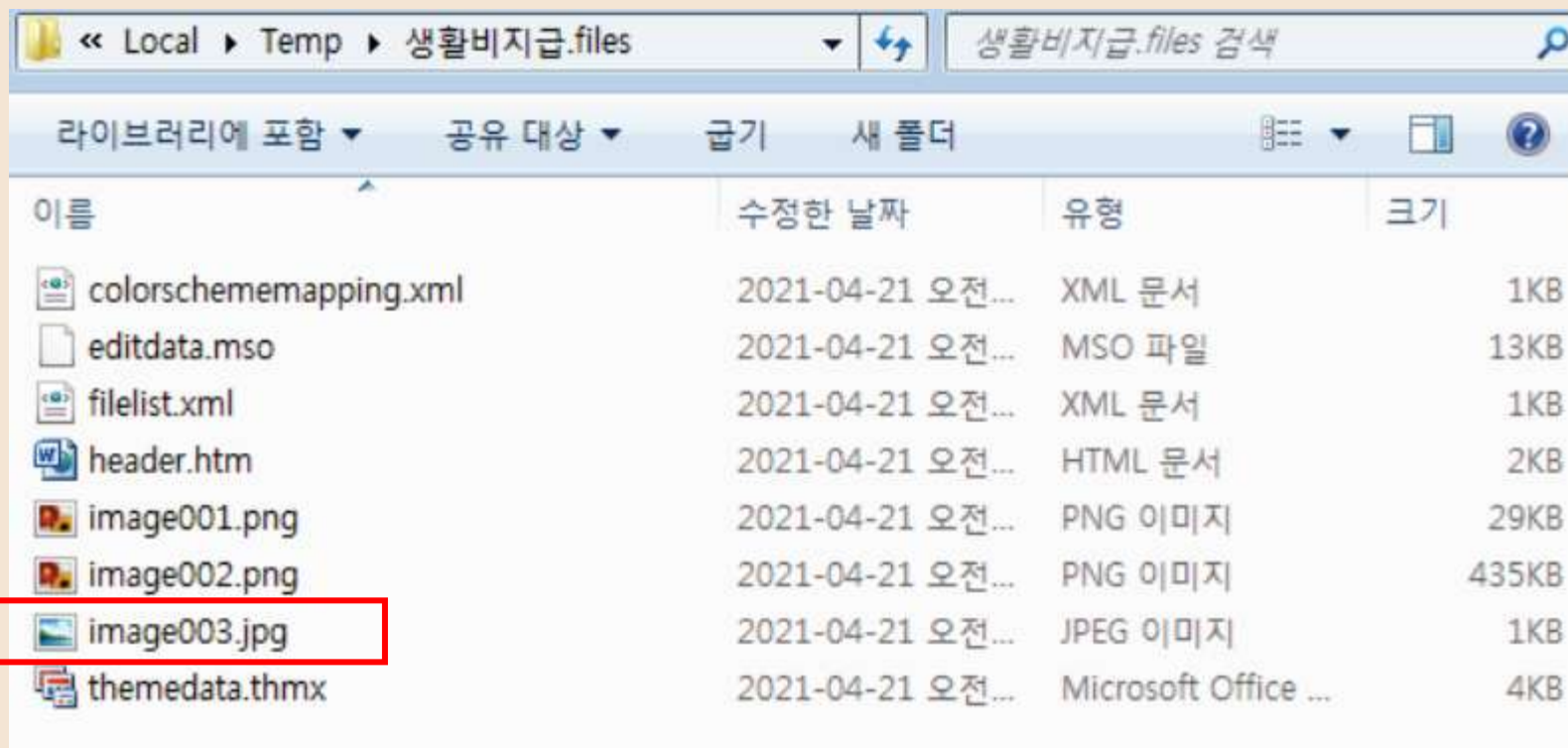
## BMP 이미지에 숨겨진 악성코드



- 신뢰할 수 있는 전송자로 위장하여 메일 전송



# 공격 시나리오 -BMP 이미지에 숨겨진 악성코드



| 이름                     | 수정한 날짜           | 유형                   | 크기    |
|------------------------|------------------|----------------------|-------|
| colorschememapping.xml | 2021-04-21 오전... | XML 문서               | 1KB   |
| editdata.mso           | 2021-04-21 오전... | MSO 파일               | 13KB  |
| filelist.xml           | 2021-04-21 오전... | XML 문서               | 1KB   |
| header.htm             | 2021-04-21 오전... | HTML 문서              | 2KB   |
| image001.png           | 2021-04-21 오전... | PNG 이미지              | 29KB  |
| image002.png           | 2021-04-21 오전... | PNG 이미지              | 435KB |
| image003.jpg           | 2021-04-21 오전... | JPEG 이미지             | 1KB   |
| themedata.thmx         | 2021-04-21 오전... | Microsoft Office ... | 4KB   |

악성코드가 내장된 이미지 파일



# 공격 시나리오 -BMP 이미지에 숨겨진 악성코드

- AlgStore.exe : 정보를 수집하거나 추가 악성코드를 다운로드 받아 실행할 수 있는 백도어 악성코드

| 명령코드 | 기능                     |
|------|------------------------|
| 1111 | 지연 시간에 사용되는 값을 변경한다.   |
| 1234 | 다운로드 받은 셸코드를 실행한다.     |
| 3333 | 자가삭제 배치 파일을 생성하고 실행한다. |
| 4444 | 접속 테스트를 수행한다.          |
| 8877 | 파일을 다운로드 받는다.          |
| 8888 | 파일을 다운로드 받아 실행한다.      |
| 9876 | 프로세스를 종료한다.            |
| 9999 | 특정 명령어 실행 결과를 수집한다.    |
| 기타   | 아무 기능도 수행하지 않는다.       |



# 공격 시나리오 -BMP 이미지에 숨겨진 악성코드

C&C 서버와 접속에 성공하면 일정 시간 지연 후 재 접속을 시도하며,

접속에 실패 시 C&C 서버 주소를 변경하여 접속을 시도한다.

최대 6 번 접속에 실패 시 배치파일을 생성하여 자가삭제 하고 프로그램을 종료한다.



```
@echo off
:L1
del "C:\Users\Public\Libraries\AlgStore.exe"
if exist "C:\Users\Public\Libraries\AlgStore.exe" goto L1
del "C:\Users\john\AppData\Local\Temp\edg89COA.bat"
|
```



# 공격 시나리오

## 두 공격의 공통점

- 메일에 첨부된 악성 파일로 침투 시작
- 악성 파일에 담긴 매크로(VBA) 이용
- 악성코드를 설치/실행할 때 정상적인 프로그램으로 설치(msiexec.exe, mshta.exe)
- C&C 서버와 통신하며 추가 공격 진행(백도어)







감사합니다