*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.30, NO.2, Apr. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.2.197

# 악성메일 훈련 모델에 관한 연구

강 영 묵,[1†] 이 상 진[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

# A Study On Malicious Mail Training Model

Young-Mook Kang,[1†] Sang-Jin Lee[2‡]
[1,2]Korea Graduate School of Information Security (Graduate student, Professor)

요 약

가상 화폐와 전자 지갑의 등장으로 익명성을 기반으로 금전적 이득을 취할 수 있는 방법이 생김에 따라, 악성메일을 이용한 피싱과 악성코드의 전파가 지속적으로 증가하고 있다. 이에 대한 피해를 최소화하기 위해서는 인적 요소인 보안인식과 기술적 요소인 대응 능력을 고루 향상시켜야 하며, 이는 실전과 같은 악성메일 대응 훈련을 통해 향상될 수 있다. 본 연구에서는 실전과 같은 악성메일 훈련 수행을 고려한 모델을 제시하였다. 임직원들의 보안인식 향상을 위한 인식 제고 훈련과 악성메일 침투에 대한 대응 능력을 향상시키기 위한 탐지 및 대응 훈련으로 분류하여 목적에 맞는 훈련 시스템, 훈련용 악성코드의 주요 기능, 구현 및 위장 기법, 기술적 대책 우회 기법에 대해 서술하였다. 이 모델을 바탕으로 3년간 수행한 훈련 데이터를 수집하였으며, 훈련횟수, 훈련테마, 위장기법에 따른 결과 분석을 통해 훈련의 효과성을 연구하였다.

ABSTRACT

With the advent of virtual currency and electronic wallets creating a way to make financial gains based on anonymity, malicious code dissemination using malicious mail has continued to increase. In order to minimize the damage, the human factors, security awareness and the ability to respond, which are technical factors, should be improved evenly, which can be improved through malicious mail training. This study presented a model considering the performance of malicious mail training, such as practice. It was classified as a training for enhancing awareness of security for employees and detection and response to improve their ability to respond to malicious mail. A training system suitable for the purpose, the core functions of malware training, implementation and camouflage skills, and bypass techniques were described. Based on the above model, the training data conducted over three years were collected and the effectiveness of the training was studied through analysis of the results according to the number of training sessions, training themes and camouflage techniques.

**Keywords:** Malicious Mail, Malware, Reversing, Training, Security Awareness

## I. 서 론

지능화된 스피어 피싱과 APT 공격이 날로 증가하고 있다. 각종 사회 이슈를 반영하여 더욱 정교하게 진화하고 있으며 피해 규모도 확산되고 있다. 이러한 공격에 가장 많이 활용되는 매개체가 메일이다. 이에 대한 대책으로 스팸메일 차단 솔루션, APT 동적분석 장비, End Point 안티바이러스 등이 사용되고 있지만 모든 공격을 막아내기에는 역부족이다. 공격용 메일 및 첨부되는 악성코드가 지속적으로 지능화되어 기술적 대책들을 우회하기 때문이다. 악성코드 분석 회피 기술, 루트킷 적용, Anti-VM,

Received(02. 13. 2020), Modified(03. 23. 2020), Accepted(03. 27. 2020)
† 주저자, mook1189@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

Anti-SandBox, 실행 압축, 코드 난독화 등의 기법을 사용하여 악성코드를 은닉하거나, 분석을 방해하고 있다.

따라서, 이러한 공격에 대한 피해를 최소화하려면 다음의 두 가지 요소가 향상되어야 한다.

첫째, 악성메일의 열람 및 첨부파일 실행을 하지 않으며, 의심되는 악성메일은 보안조직에 신고하는 등의 보안인식 강화를 통한 인적 대응이다.

둘째, 악성메일을 빠르게 식별하여 탐지 및 차단하며, 실제 악성코드에 감염되었을 때에는 체계적인 대응을 통해 피해 확산을 방지하는 기술적 대응이다.

이 두 가지 요소를 향상하는 방법으로는 실전과 같은 악성메일 훈련이 있다. 다양한 조직에서 악성메일 훈련의 중요성을 인식하여 지속적으로 수행 중이지만 트렌드를 반영한 콘텐츠 부족 및 실제와 같은 악성행위 기법이 적용되지 않은 한계가 있다.

이전의 악성메일에 관한 연구는 설문조사[6]를 인용하거나, 악성메일 발송 후의 결과를 수집[8][9]하여 분석하는 것이 대부분이었으나, 본 연구에서는 실전과 같은 악성메일 훈련을 위한 인적, 기술적 요소를 고려한 모델을 제시하였다. 임직원들의 보안인식 향상을 위한 인식 제고 훈련과 악성메일 침투에 대한 대응 능력을 향상시키기 위한 악성메일 탐지 및 대응 훈련(Table 1)으로 나누어 각각의 목적에 맞는 훈련 모델과 주요 구성요소인 훈련용 악성코드의 기능, 구현 방법, 위장 기법에 대해 서술하였다. 이를 바탕으로 3년간 수행한 훈련 데이터를 수집하였으며, 훈련횟수, 훈련테마, 위장기법에 따른 결과 분석을 통해 훈련의 효과성을 분석하였다. 본 연구에서 제시한 모델을 통해 많은 기관에서 실효성 있는 훈련이 수행되어 악성메일 공격에 의한 피해를 최소화하고, 학술적으로는 악성메일 훈련의 효과성에 관한 검증사례에 기여하고자 한다.

## II. 연구배경 및 선행연구

### 2.1 연구배경

글로벌 보안기업인 마임캐스트에서 1,025명의 IT 의사 결정권자를 대상으로 진행한 2019년 조사에 따르면 피싱 메일 공격이 가장 두드러진 사이버 공격으로 나타났다[1]. 대상자의 94%가 지난 1년간 피싱 및 스피어 피싱 메일을 경험했으며, 55%는 피싱 메일이 증가했다고 응답했다. 또한, 73%는 악성메일에 의해 직간접적인 손실을 입었으며, 이 중 데이터 손실이 40%, 금전 피해가 29%, 고객 손실은 25%로 집계되었다. 또한, 메일은 공격 요소(Vector) 중 1위를 나타내고 있으며, 사이버 범죄자들은 피해자들을 속여 개인 계정, 금융정보 등을 탈취하거나, 심지어 돈을 송금하도록 유도하는 등의 다양한 공격에 사용되고 있다. 가상 화폐와 전자 지갑의 등장으로 익명성을 기반으로 금전적 이득을 취할 수 있는 방법이 생김에 따라, 이와 같은 악성메일을 이용한 피싱과 악성코드 유포는 지속적으로 증가할 것이다[2].

### 2.2 선행연구

기술적 보안대책과 보안인식이 고루 갖추어졌을 때 위와 같은 피해를 최소화할 수 있다. 이를 향상시킬 수 있는 악성메일 훈련에 대한 다양한 연구가 진행되었다.

장인숙[3]은 사이버 위기 상황에서 실질적으로 대응하도록 훈련하기 위해서는 여러 가지 측면이 고려되어야 한다고 역설하였으며, 다양한 공격 유형을 파

Table 1. Classification of Malicious mail training

| Type | Security Awareness Improvement training | Detection and Response Improvement training |
|---|---|---|
| Goal | Security Awareness Improvement of executives and staff members | Improvement ability of Responsiveness aginst malware attack |
| Target | Executives and staff members | IT Security Division |
| Function | Education Page, Screen lock, File Encryption | Infection spread, Concealment, Persistence |
| Evasion Technique | - | Static/Dynamic Analysis evasion, Packing, Source Code Obfuscation |

악하고 공격에 즉시 대응할 수 있도록 실제와 같은 훈련 콘텐츠를 설계하는 것이 중요하다고 주장했다.

Eric Johnson[4]은 무언가를 해킹하는 것보다 사람을 속이는 것이 훨씬 쉬우며, 스피어 피싱의 경우 메일 열람률이나 민감 정보 유출률이 높다고 주장하였다. 이에 대한 대비책으로 실제 의심스러운 메일과 링크를 수신하는 상황을 시뮬레이션 한 훈련이 단순한 온라인 보안교육보다 훨씬 효과적임을 강조하였다. 또한, 악성메일의 열람 및 악성코드의 감염 시 기업의 피해보다는 개인에게 피해가 크다는 것을 강조할수록 훈련의 효과가 높음을 증명하였다.

Stephanou[5]는 기술적 보안만으로는 완벽한 보안을 이룰 수 없다고 주장하였으며 기술을 다루는 사람을 다루는 것도 사람이기에 보안 인식의 중요성을 강조했다. 또한, 조직적 학습 모델을 제시하였으며 해당 모델을 통해 보안 인식 교육의 영향력과 이후의 행동에 대한 분석이 가능함을 보여주었다.

Sheng[6]는 카네기 멜론 대학교의 1,001명 학생을 대상으로 온라인 설문 조사를 통한 정성적인 연구를 진행하였다. 나이와 성별 등으로 분류하여 연구를 진행하였으며 인구 통계학적으로 피싱 메일에 대한 수용성이 다름을 확인하였다. 기술적 훈련이 여성보다는 남성에게 더 많이 되었기 때문에 여성의 수용성이 더 높다고 추정하였다. 또한, 18~25세 구간의 사람은 타 구간의 사람들보다 교육 훈련을 덜 받았으며 리스크에 대한 경계심이 낮아 수용성이 더 높을 것이라고 추정하였다. 이에 대한 교육 훈련을 설계하여 진행한 결과, 40%의 피싱메일 수용성 감소를 확인하였으며 교육의 중요성을 강조하였다.

Caputo[7]는 워싱턴 DC의 한 회사에서 1,359명을 5개의 그룹으로 나누어 각각 3번의 악성메일 훈련을 진행하였다. 5개의 그룹은 피싱 페이지의 링크를 클릭할 경우 스피어 피싱 메일 수신 여부만 안내한 1개의 그룹과 각기 다른 교육 페이지로 안내한 4개의 그룹으로 나누었다. 교육 페이지의 경우, 사용자가 주의 깊게 읽지 않아 실질적인 훈련효과가 미미함을 보였다. 또한, 이메일 열람을 하지 않은 사람이 피싱페이지의 링크를 클릭하지 않을 확률이 높다는 것을 확인하였다. 따라서, 일관되지 않는 선택을 하는 사람들에게 훈련의 효과가 있음을 보였다. 훈련의 효과를 높이기 위해서는 실제와 구분하기 어렵도록 정교하게 만들어진 피싱 메일을 사용해야 하며, 효과를 지속시키기 위해서는 상당기간 반복적으로 진행되어야 한다고 주장했다. 또한, 교육 훈련 페이지와 같은 후속 조치의 경우 훈련대상자가 충분히 숙지하도록 하는 절차가 필요함을 주장하였다.

### 2.3 선행 연구와의 차이점

본 연구는 이전의 연구와 크게 두 가지의 차이점이 있다. 첫째, 이전의 연구가 단순히 악성메일 발송 후의 결과를 수집하여 분석[8][9]하는 것이 대부분이었으며, 악성메일 훈련을 수행하기 위한 모델이나 구현 방법을 제시한 연구는 없었다. 본 연구는 악성메일 훈련 모델을 제시하였으며, 필요 요소들을 분류하여 구현 방법까지 제시하였다. 특히, 구현 요소 중 훈련용 악성코드의 기능과 위장 기법은 최근 해커가 사용하는 기법을 응용 및 분석하여 적용법을 서술하였다. 또한, 기술적 보안 대책을 우회할 수 있는 다양한 안티 기법을 접목하여 실제 공격과 유사하게 구현하였다. 이를 통해 훈련 수행 기관의 악성메일에 대한 대응 및 분석 능력 향상에 기여하였다. 또한, 훈련의 목적에 맞게 실질적인 영향을 줄 수 있는 요소들은 최소화하였고, 보안 인식을 향상시킬 수 있는 교육적 요소들을 추가로 구현하였다.

둘째, 이전의 연구 대부분은 짧은 기간 및 제한된 인원을 대상으로 훈련을 진행하거나 설문조사 결과에 의존[6]하였다. 하지만 본 연구는 3년간 다수의 실제 기관을 대상으로 진행한 신뢰성 있는 데이터를 기반으로 분석을 진행하였다.

## III. 악성메일 훈련 모델

본 연구에서 제안하는 악성메일 훈련 모델은 메일을 발송하는 훈련 주최기관과 악성메일을 수신하는 훈련수행 기관으로 나눈다. 훈련 주최기관은 악성메일의 생성·발송 시스템, 훈련 결과 처리 시스템, 해당 시스템과 연동하여 각종 정보를 제공하는 데이터베이스로 구성하였다. 훈련 수행기관은 스팸메일 솔루션, IPS, APT 동적 분석 장비, End-Point 안티바이스 등으로 구성된 보안대책을 위한 시스템들과 악성메일의 열람, 첨부파일 실행, 피싱페이지 접속 등 악성행위를 하는 인적 요소로 분류하였으며, Fig. 1.와 같이 모델링을 하였다.

### 3.1 악성메일 생성 및 발송

악성메일 생성·발송 시스템의 주요 기능은 훈련

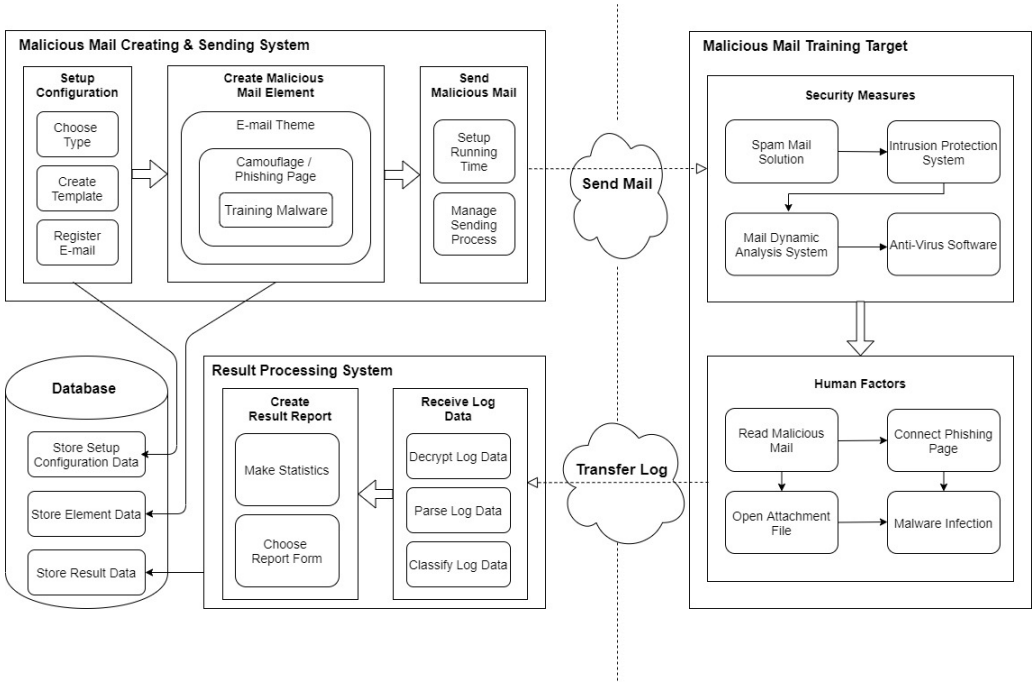


Fig. 1. Malicious Mail Training Model Design

타입 및 템플릿 설정, 훈련 대상자의 이메일을 등록하는 환경설정 기능, 훈련용 악성코드 생성, 위장형태의 첨부파일 생성 및 피싱페이지 생성, 이메일 테마를 씌우는 악성메일 콘텐츠 생성 기능, 악성메일을 발송하고 발송상태를 관리하는 기능으로 분류하였다. 각 기능을 상세하게 살펴보면 다음과 같다.

환경설정 기능에서는 임직원 보안인식 제고 훈련과 탐지 및 대응훈련 여부를 설정한다. 훈련을 수행할 기관과 훈련 기간을 설정하고 훈련 대상 이메일 등록, 발송 방식 등을 등록한다. 이 후 다음 단계에서 생성할 훈련 콘텐츠에 대한 템플릿을 선택한다.

악성메일 콘텐츠 생성기능은 다음과 같다. 명령제어 채널 생성, 정보수집 및 유출, 감염 안내팝업 생성, 화면잠금, 파일암호화 등의 기능을 선택하고 실행파일 형태의 악성코드를 생성한다. 이후, 첨부형의 경우 스크립트, 문서, 윈도우 설치파일 등의 위장형태를 선택하고 공격코드와 훈련용 악성코드를 주입한다. 링크형의 경우 메일 본문에 링크될 피싱페이지의 URL과 입력 정보를 받기 위한 페이지로 구현한다. 최종적으로는 생성한 콘텐츠들에 금전, 위반 등의 사회공학 테마를 추가한다.

악성메일 발송기능은 앞에서 생성한 콘텐츠들과 훈련 대상자의 메일을 매칭하여 발송하는 기능이다. 이외에도 발송성공, 발송실패 등의 진행상황을 가시화하고 발송 일시정지, 재발송 등의 관리기능을 수행한다.

### 3.2 훈련 결과 프로세싱

악성메일이 발송된 이후에는 훈련 종료기간까지 메일 열람, 위장파일 다운로드, 악성코드 실행, 피싱페이지 접속, 개인정보 입력, 치료 등의 단계별 훈련를 수신한다. 로그서버는 수신한 로그를 적절한 형태로 파싱하여 데이터를 가공한다. 이후, 데이터의 내용을 정리 및 분류하여 통계치를 계산하고 문서 형태의 보고서를 생성한다.

## IV. 훈련 모델의 핵심 콘텐츠

본 연구에서 제안하는 훈련 모델의 핵심은 콘텐츠 생성이며, 기존의 연구[4][5][6][7][8][9]에서는 훈련 콘텐츠에 관한 연구가 부족하였다. 이에 따라, 훈련용 악성코드, 기술적 대책 우회기법, 위장기법에 대해 아래에서 비교적 상세하게 서술한다.

### 4.1 훈련용 악성코드

훈련용 악성코드는 단말이나 서버의 파일 암호화, 리소스 고갈, 트래픽 급증, 주요 정보 유출 등의 실질적인 피해를 입혀서는 안 된다. 하지만 실제 악성코드와 유사하게 동작해야 훈련의 효과를 높일 수 있으므로 정교한 설계 및 구현이 필요하다. 훈련용 악성코드는 목적에 따라 두 가지로 나누었다.

첫 번째는 임직원 보안인식 제고를 위한 훈련용 악성코드이다. 감염안내 팝업 생성, 화면 잠금, 파일 암호화 등의 기법을 통해 경각심을 일깨워주는 것을 목적으로 한다.

두 번째는 IT보안 조직의 악성메일에 대한 대응 및 분석 능력 향상을 위한 훈련용 악성코드이다. 해당 악성코드는 침투를 위해 제작되었으므로, 실제 악성코드에서 사용되는 다양한 기술적 보안대책 우회 기술이 적용되어야 한다. 훈련 수행기관은 해당 악성코드의 유입 탐지, 위협 상황 전파, 악성메일 및 악성코드 분석, 감염 단말의 포렌식 진행, 분석 내용을 바탕으로 한 패턴 생성, 행위 추출 등의 후속 조치를 통해 악성메일에 대한 대응 및 분석능력 향상을 목적으로 한다.

본 연구에서 사용한 훈련용 악성코드는 Windows 운영체제에서 동작하며 Windows API를 이용한 C++ 프로그래밍 언어로 구현하였다. 악성코드는 보안인식 제고용 악성코드와 악성메일 탐지 및 대응 훈련용 악성코드로 분리하였으며, 해당 기능 및 수행 흐름은 Fig. 2와 같다.

#### 4.1.1 명령제어 채널 생성

명령제어 채널은 악성코드를 제어하기 위해 생성한다. 보통 공격자가 단말을 장악한 후 원하는 명령을 전달하기 위해 만든 채널이다. 이 채널을 통해 단말의 네트워트 정보, 계정 정보, 주요 정보를 유출하거나, 공격자의 명령을 받아 다음 공격을 수행한다. 훈련 수행 기관은 감염 단말의 네트워크 로그를 다각적으로 분석하여, 해당 명령제어 서버의 URL이나 IP를 탐지하여 차단하는 훈련을 수행한다.

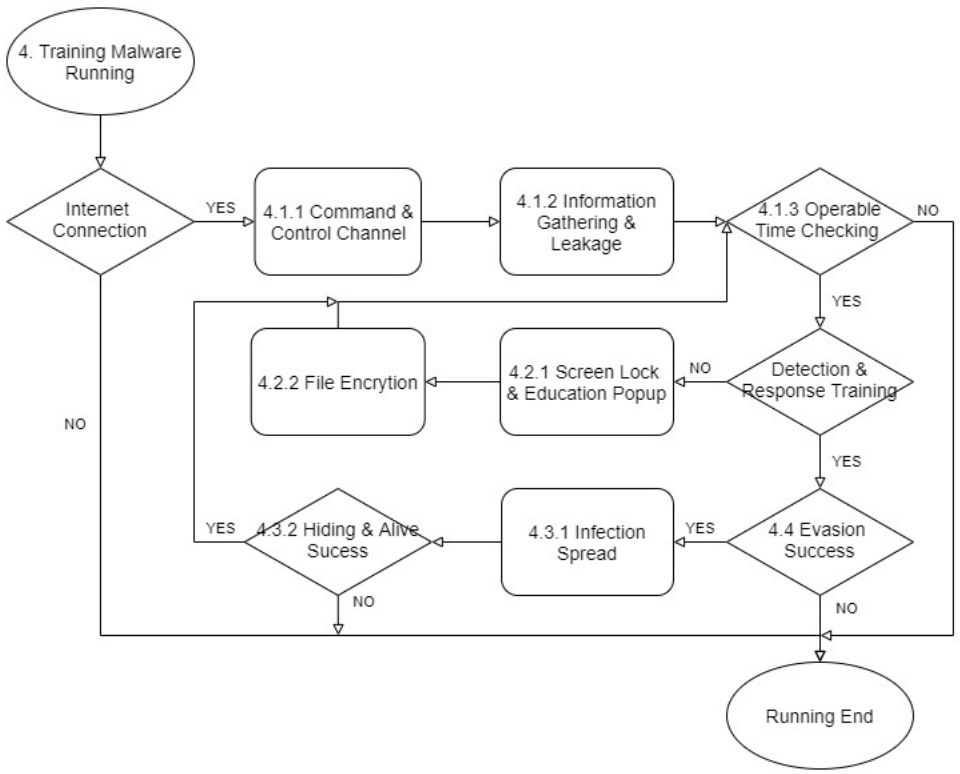


Fig. 2. Training Malware Running Flow

#### 4.1.2 정보수집 및 유출

훈련용 악성코드가 동작할 때에는 다양한 정보 수집 및 유출을 시도한다. 감염 단말의 환경에 최적화된 공격을 수행하기 위해 운영체제 버전, 플랫폼, 컴퓨터 이름 등의 정보를 수집하고, 계정 비밀번호, 연결된 데이터베이스의 계정 비밀번호 등을 알아내기 위한 공격을 수행한다. 수집한 정보는 명령제어 채널을 통해 유출을 시도하고 명령을 전송받아 다음 단계 공격을 진행한다. 유의할 점은 훈련용 악성코드의 경우 비밀번호 유출, 가용성 저해 등의 단말에 영향을 주지 않도록 구현해야 한다. 수집한 정보들은 유출되지 않도록 암호화하여 안전하게 전송한다. 훈련 수행기관은 감염 단말의 이벤트 로그, 행위 분석, 네트워크 트래픽 등을 분석하여 해당 정보 유출 행위를 탐지하여 차단하는 훈련을 수행한다.

#### 4.1.3 동작시간 설정

훈련용 악성코드의 경우 유효 기간에만 동작해야 하며 이후에는 삭제 및 복구하는 조치가 필요하다. 훈련용 악성코드에 유효 기간을 설정해두고 현재의 시간 값과 비교하여 동작 여부를 결정한다. 현재의 시간 값이 설정해 놓은 유효 기간이라면 훈련용 악성코드의 기능을 수행하고, 동작 기간 전이라면 기능을 수행하지 않는다. 또한, 동작 시간으로부터 훈련 유효 기간까지의 시간을 계산하여 만료 기간이 도래하면 자가 삭제 및 복구 기능을 수행한다.

### 4.2 보안인식 제고 악성코드 기능

#### 4.2.1 감염 안내팝업 생성 및 화면잠금

훈련 수행기관의 악성코드 탐지 및 확산 방지와 같은 기술적 방어도 중요하지만 감염자의 빠른 신고/격리/치료 등의 조치도 매우 중요하다. 따라서, 훈련용 악성코드는 감염자에 대한 신고 안내 및 유도를 위한 팝업 생성기능이 필요하다. 이는 감염자에게 주의점을 안내하거나 경각심 고취에 효과적이다. 하지만 단순한 팝업의 안내만으로는 신고에 한계가 있다. 이를 보완하기 위해 키보드의 특정키 입력을 방지하는 등의 방법으로 화면을 잠그거나 악성 이미지 생성 등의 가시적 효과를 줄 수 있는 기능을 추가하여 신고율 및 치료율 높이도록 한다.

#### 4.2.2 파일암호화

훈련용 악성코드의 경우 실제 문서 파일을 암호화하면 업무에 영향을 줄 수 있으므로 특정 경로의 그림 파일을 암호화하거나 악성코드 자체가 생성한 파일을 암호화하는 등의 단말에 실질적인 영향을 주지 않는 방향으로 구현되어야 한다. 또한, 실제와 유사한 랜섬웨어 경고 팝업을 구성하고, 암호화된 파일의 경로를 알려줌으로써 가시성을 확보할 수 있다. 이를 통해 감염자에게 경각심을 주어 훈련효과를 극대화할 수 있다. 훈련 수행기관은 악성코드가 암호화를 시도하는 프로세스를 탐지하고 감염 시의 확산을 방지하는 등의 훈련을 수행한다.

### 4.3 탐지 및 대응 악성코드 기능

#### 4.3.1 감염 확산

악성코드에 감염된 단말의 정보 수집 및 유출 이후 내부 네트워크를 통해 악성코드를 확산하는 기능을 의미한다. 대표적인 유포 사례로는 최근에 유행한 악성코드인 WannaCry, Flawed Ammyy가 있다[10][11]. Wannacry 악성코드의 경우 감염된 단말에서 접속 가능한 IP를 스캔한 이후 Server Message Block 프로토콜의 취약점을 이용하여 네트워크로 전파하였다. Flawed Ammyy 또한, 감염된 단말이 Active Directory 서버에 연결되어 있는지 확인한 후 Server Message Block 프로토콜 취약점을 이용해 파일 생성 및 서비스를 생성하였다. 이를 통해 내부 시스템에 악성코드를 확산시켰다.

최근 사례에서 알 수 있듯이 감염 확산은 네트워크를 통해 이루어지며, 감염 단말이 접근 가능한 네트워크 정보를 스캔하는 절차는 필수적이다. 또한, 감염 단말 간의 네트워크 통신은 치명적인 공격 루트가 될 수 있다. 훈련용 악성코드에는 감염 단말의 네트워크 정보를 스캔하는 기능, 감염 단말 간의 정보를 송수신하는 기능이 구현되어야 한다. 훈련 수행기관은 외부와의 통신뿐만 아니라, 내부 단말과 서버, 내부 단말 간의 특이 네트워크 트래픽의 발생 여부를 모니터링하여 탐지하는 훈련을 수행한다.

#### 4.3.2 지속실행 및 연결유지

명령제어 서버로부터 명령을 받아 지속적으로 악

성행위를 수행하기 위한 기능이다. 실행을 은닉하기 위해 일정기간의 잠복기를 갖도록 구현하며, 시스템의 다양한 인터럽트에도 실행 상태를 유지해야 한다. 훈련용 악성코드의 지속 실행을 구현하는 방법은 Windows API를 이용한 레지스트리 변경 및 등록, 시작 프로그램에 등록, 작업 스케쥴러에 등록, Windows 서비스 등록 등이 있다. 훈련 수행 기관은 감염 단말에 허가 없이 생성된 레지스트리, 시작 프로그램 폴더의 등록, 작업 스케쥴러 생성 등의 윈도우 이벤트 분석 훈련을 수행한다.

### 4.4 탐지 및 대응 악성코드 기술적 대책 우회

본 절에서는 기술적 대책 우회를 정적 및 동적 분석을 통한 악성코드 탐지 및 차단을 무력화하여, 훈련용 악성코드를 동작시키고, 분석을 지연 및 회피하기 위한 방안으로 정의한다. 탐지 및 대응 훈련용 악성코드에 적용된 기술적 대책 우회 기법(Table 2.)은 정적분석 회피, 동적분석 회피, 역분석 방해, 소스코드 난독화이며, 훈련 수행 기관은 해당 악성코드의 공격을 방어하는 과정을 통해 대응 및 분석 능력을 향상시킨다.

#### 4.4.1 정적분석 우회 기법

정적분석 회피를 위한 기법으로 적절한 것은 실행 압축이다. 이를 적용하여 내부 코드와 리소스, 문자

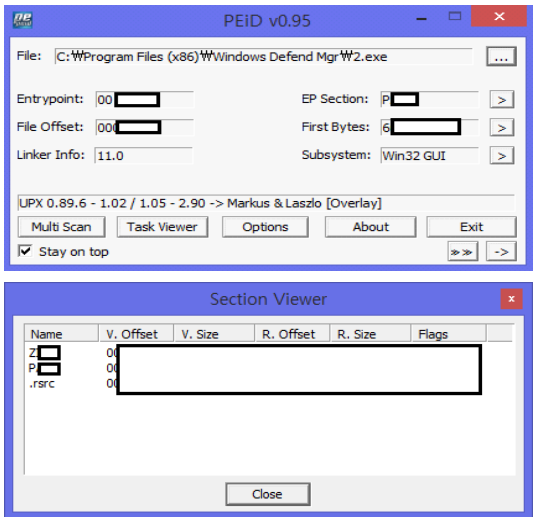


Fig. 3. Training Malware Custom Packing

열, API, Code Flow 등을 숨길 수 있으며 안티바이러스가 정적 분석하는 파일의 특정 위치를 변형할 수 있다. UPX나 ASPack와 같은 상용 패커의 경우 UPX0, UPX1, aspack 등과 같은 섹션명, 압축 알고리즘 안에 특정 Fingerprint, Text 섹션에서 사용되는 코드 시그니처 등이 알려져 있어 탐지가 쉽다. 따라서 훈련용 악성코드는 커스텀 패커를 사용한다. 커스텀 패커는 UPX 패커의 코드를 기반으로 섹션명 및 압축 알고리즘을 변경하여 구현하였다. 해당 커스텀 패커는 기존의 APT 동적 분석 장비와 End-Point 안티바이러스 대부분을 우회하였다. 해당 커스텀 패커는 엔트로피 기반의 탐지, 메모리 포렌식 기법을 통해 언패킹[12][13]이 가능하다.

#### 4.4.2 동적분석 우회 기법

APT 동적 분석 장비들은 피해 방지를 위해 격리된 가상 환경인 가상머신이나 샌드박스를 이용하여 동적 분석을 진행한다. 이러한 동적 분석 장비를 우회하기 위해서는 동작 환경이 가상 환경인지 인지해야 한다. 동작 환경이 가상 환경이라면 악성행위가 아닌 정상 행위를 수행하여 동적 분석을 우회할 수 있다[14]. 물리 단말에서는 악성 명령제어 서버와 통신을 하여 명령어를 받아와 악성행위를 진행하고, 가상 분석 장비에서는 프로세스를 종료하거나 정상적인 기능을 수행하는 것이다.

탐지 및 대응 훈련용 악성코드는 Windows API를 활용해 마우스나 키보드의 움직임을 분석하여 가상 환경임을 탐지하였다. 또한, 가상 환경의 제한된 메모리와 분석 시간이 있다는 점을 이용하여, 불필요하게 많은 메모리 할당, 반복문 삽입, 존재하지 않는 URL 요청, 시간 왜곡을 하는 코드를 삽입하여 동적분석을 우회하였다[15]. 훈련 수행 기관은 동적분석 우회에 자주 사용되는 기법에 대한 분석 및 동적 분석 장비들의 룰 튜닝[16]을 통해 동적분석 우회 기법을 무력화하는 훈련을 수행한다.

#### 4.4.3 역분석 방해 기법

역분석 방해는 악성코드의 분석을 방해하여 탐지 룰을 쉽게 만들지 못하게 하는 기능이다. 탐지 및 대응 훈련용 악성코드에 적용된 역분석 방해기법은 디버깅 방해, 동적 분석 툴의 실행 방지이다. 디버깅 방해를 위해 Windows API를 이용해 Context 구

Table 2. Evasion Tactic/Technique

| Type | Tactic | Technique |
|---|---|---|
| Static Analysis Evasion | Packing | Hiding Source Code, Code Flow, String, EntryPoint |
| | | Using commercial packer (UPX, ASPack) or custom packer |
| Dynamic Analysis Evasion | Detecting Virtualization(Sandbox) Environment | Detecting CPU Instruction(EAX) return value |
| | | Analyzing I/O device(mouse, keyboard) movement |
| | | Detecting virtualization environment signature (file, registry, process) |
| | Insert Dummy Code | Too much memory allocation code |
| | | Useless condition/iteration code |
| | | Time distortion code |
| | | Non-existent URL call |
| Anti-Reversing | Anti-Debugging | Monitoring DebugPort using CheckRemoteDebuggerPresent(), IsDebuggerPresent() API |
| | | Scanning INT 3 instruction |
| | Disturbing Execution of Reversing Tool (OllyDGB, Immnuity Debugger, IDA, Ghidra etc) | Acquiring running process information using CreateToolhelp32Snapshot() API, FindWindow() API and compare to reversing tool information |
| Obfuscation | Virtualization Code Obfuscation | Using virtualization code obfuscation tool like code Virtualizer, VMProtect, Themida |
| | JavaScript/VBScript Obfuscation | String encoding, Eval, Escape function, Array/Variable randomaiztion, Dummy code, Flow flatting, Code spliting |

조체의 디버깅 포트를 검사하여 디버깅 여부를 탐지하였다. 또한, OpenProcess API를 이용하여 PROCESS_ALL_ACCESS 권한을 가진 프로세스의 실행을 시도하고, 해당 프로세스의 실행 성공 여부를 통해 디버깅 중인지 탐지하였다. 프로세스 당 하나의 디버깅만이 가능하다는 특징을 이용하여 자식 프로세스를 생성해 자기 자신을 디버깅하여 타 디버깅을 막는 Self-Debugging 기법과 'INT3' 예외가 발생하기 전에 핸들러를 등록하는 기법을 적용하여 디버깅 중인지 알 수 있도록 구현하였다.

동적분석 툴의 실행 방지를 위해 CreateToolhelp32Snapshot API를 이용하여 실행되고 있는 프로세스 리스트를 얻어 온 후 분석 툴의 프로세스명과 비교하였고, FindWindow API를 이용해 윈도우 창의 타이틀 명을 얻어온 후 분석 툴의 윈도우 창과 비교하였다. 또한, NtQueryInformationProcess API를 이용해 리턴되는 PROCESS_BASIC_INFORMATION 구조체의 특정 필드를 비교하여 분석 툴의 실행을 탐지하였다. 훈련 수행 기관은 탐지한 악성코드의 역분석 방해기법을 무력화하는 프로세스 훈련을 수행한다.[17].

#### 4.4.4 난독화 기법

탐지 및 대응 훈련에서 사용되는 악성코드에는 난독화 기법을 적용하여 소스코드 분석이 어렵도록 하였다. 난독화의 대상은 PE(Portable Executable) 형태의 실행파일, 자바스크립트, VBA(Visual Basic for Application)스크립트이다.

PE(Portable Executable) 형태의 실행 파일에는 가상화 기법[13]이 적용되었다. 가상화 기법 사용 시 보호하고자 하는 코드 영역을 잘 알려지지 않은 기계어로 변환한다. 이를 해석할 수 있는 가상 프로세서를 프로그램 내부에 포함하고 있으며, 구현된 프로세서를 통해 프로그램이 실행된다. 패킹과는 달리 변환된 코드가 원래의 코드로 복원되는 시점이 없어 타 난독화 기법에 비해 분석이 어렵다[18]. Code Virtualizer, VMProtect, Themida 등의 툴을 이

용하여 실행 파일 가상화 난독화 기법 적용이 가능하며, 탐지 및 대응 훈련용 악성코드에는 VMProtect를 적용하였다.

브라우저에서 실행이 가능한 자바스크립트에는 Escape, Eval 등의 내장 함수 사용, 코드의 줄 바꿈 제거, 변수명 치환, 실행 흐름 평탄화, 쓰레기 코드 주입, 문자열을 배열로 만들어 무작위 위치 지정, 문자열 난독화 빈도, 문자열 인코딩(Base64, Base85, Base62, XOR), 콘솔 디버깅 제어 등의 난독화 기법을 적용하였다.

Excel, Word, PPT 등의 프로그램에서 실행이 가능한 VBA 스크립트는 주석과 띄어쓰기 제거, 변수, 모듈, 유저폼, 프로시저의 이름을 임의로 변경, 문자열 암호화, 코드 분할, 쓰레기 코드 주입, 유저폼 컨트롤 난독화 등을 통해 난독화를 구현하였다. 훈련 수행 기관은 API 호출특성, 의미 구조를 이용한 방법을 이용하거나, 메모리 분석, 스택분석 등의 디스어셈블을 수행하여 역난독화 훈련을 수행한다[19][20].

## 4.5 악성코드 위장

### 4.5.1 이메일 첨부형

이메일 첨부형은 신뢰할 만한 파일로 위장하여 사용자가 첨부파일을 열람하도록 유도한다. 첨부파일 열람과 동시에 자신도 모르게 주입된 훈련용 악성코드가 동작하게 된다. 이러한 이유로 사용자는 자신이 악성코드에 감염되었다는 사실을 인지하기 어렵다

본 연구에서 제안한 훈련 모델에서는 스크립트 형태의 HTML/HTA 위장, MS-Office 계열의 문서파일 위장, PDF 위장[21], 한글파일 위장[22], 윈도우 인스톨러 파일 위장[23], LNK(Link)형태의 링크파일을 이용한 압축파일 위장 등의 기법을 구현하여 훈련을 수행하였으며, 주요 구현 기법은 Table 3.과 같다.

### 4.5.2 이메일 링크형

이메일 본문에 피싱페이지로 접속할 수 있는 링크

Table 3. Camouflage Implementation Technique

| Type | Format | Implementation Technique |
|---|---|---|
| SCRIPT | HTML/HTA | Inject exploitable powershell code using javascript |
| | | Download exploitable binary/text using windows ActiveXObject |
| | | Inject encoded malicious binary in html hidden field |
| | | Exploit application(Browser, PDF, SWF) vulnerability (ex. CVE-2017-11882) |
| DOCUMENT | MS-Office | Inject Exploitable VBA(Visual Basic Application) Code |
| | | Malicious payload transfer using DDE(Dynamic Data Exchange) |
| | | Exploit MS-Office vulnerability (ex. Memory Access processing code injection) |
| | PDF | Inject Exploitable javascript/actionscript using PyPdf, Minipdf module |
| | | Inject malicious link in PDF document using Reportab module |
| | HWP | Inject exploitable javascript or postscript |
| | | Exploit hangul processor vulnerability (ex. CVE-2017-8291) |
| | | Inject malicious OLE(Object Linking and Embedding) object |
| INSTALLER | MSI | Make a MSI(Microsoft Installer) file for malware and inject exploit code for using msiexec.exe by wix-tool set |
| COMPRESS | LNK | Compression with malware and LNK(Link) files |

를 삽입하고 접속 시 자동으로 악성코드가 다운로드 되도록 구현하였다. 다운로드 된 악성코드는 보안프로그램으로 위장하여 사용자가 실행할 수 있도록 유도하였으며, 피싱페이지의 경우 개인정보를 입력받을 수 있는 웹페이지로 구현하였다.

## V. 훈련 실시 및 결과 분석

### 5.1 훈련대상 및 환경

본 연구는 국내 161개의 기관을 대상으로 2017년~2019년까지 3년간의 훈련 데이터를 기반으로 작성되었다. 17년에는 144개의 기관, 18년도에는 142개의 기관, 19년도에는 148개의 기관이 각각 훈련에 참여하였다. 17년, 18년 연이어 참가한 기관은 136개의 기관, 18년, 19년에 연이어 기관은 136개의 기관, 3년 연속으로 참여한 기관은 132개 기관이었다. 참여기관의 회사 규모에 따라 훈련 대상 인원은 다양하였으며, 17년도에는 90,491명, 18년도에는 97,808명, 19년도에는 109,717명을 대상으로 훈련이 진행되었으며, 발송 메일건수는 17년도에는 203,089건, 18년도에는 227,093건, 19년도에는 229,936건 이었다.

위와 같이 다수의 기관을 대상으로 연중 실시하는 훈련 환경으로 인해 몇 가지 한계점이 있었다. 참여인원에 대한 개인 식별정보는 훈련기간 이후 즉시 영구 파기하기 때문에 개개인에 대한 보안인식 향상 여부는 확인이 불가능했다. 또한, 매년 신규 콘텐츠를 추가하여 훈련을 수행하였기 때문에 동일 콘텐츠에 대한 반복적인 훈련이 이루어지지 못했다.

하지만 거시적 관점에서 통계치를 기반으로 한 기관의 보안인식 및 악성메일 대응 능력 향상 여부에 관한 분석이 가능했다. 실제 기관의 인프라 환경에서 오랜 기간 많은 양의 훈련 데이터를 수집하였으며, 훈련유형, 훈련횟수, 훈련테마, 위장기법에 따른 결과 분석을 통해 훈련의 효과성을 분석하였다.

### 5.2 훈련 시나리오

훈련 시나리오는 크게 훈련 준비단계와 실시단계로 나눌 수 있다. 준비단계에서 악성메일을 유포하는 훈련 주최기관과 악성메일에 대응하는 훈련 수행기관 간의 훈련 유형, 훈련 진행 방식 등을 협의한다. 협의된 내용을 바탕으로 훈련 진행자는 훈련용 악성코드를 생성한다.

실시단계에서 훈련 진행자는 악성메일 발송을 실시한다. 훈련 시스템에서는 메일 열람, 첨부파일 열람, 훈련용 악성코드 동작, 피싱페이지 접속, 개인정보 유출 등의 훈련 결과를 암호화된 로그형태로 수신한다. 보안인식 제고 훈련은 임직원의 신고를 통해 감염여부 및 개인정보 유출 여부를 파악하고, 감염자 발생 시에는 단말 격리 및 치료를 수행한다. 이후 감염자를 대상으로 별도의 보안인식 교육을 수행한다.

탐지 및 대응 훈련은 악성메일 탐지 및 차단, 악성메일 유입에 따른 위협상황 전파, 보안장비 분석, 유입된 악성코드 분석, 감염 단말의 포렌식 수행, 백신 치료 등의 복구절차를 진행한다. 분석된 내용을 바탕으로 보안정책을 수정하거나 탐지 차단 패턴을 생성하여 등록하는 훈련을 진행한다.

### 5.3 보안인식 제고 훈련결과 분석

17년 보안인식 제고용 악성코드의 주요 특징은 다이얼로그 기반의 감염안내 팝업 생성 기능이며, 주요 훈련 테마는 건강, 직업, 금전 관련 메일이었다. 위장 기법은 HTML/HTA의 스크립트, xls, doc, ppt 등의 MS-Office 문서 파일을 사용하였다. 18년의 특징은 랜섬웨어를 모사한 화면 잠금과 파일암호화 기능이며, 테마는 통신료, 이벤트, 주정차 위반에 관련된 메일이었다. 위장 기법은 HTML/HTA의 스크립트, PDF 문서 파일을 사용하였다. 19년의 특징은 악성 이미지의 복제 기능이며, 테마는 거짓금융경고, 법률 위반, 금전에 관련된 메일이었다. 위장 기법은 HTML의 스크립트, HWP 문서 파일을 사용하였다.

#### 5.3.1 연도별 결과 분석

악성코드 감염률은 감소 추세를 나타내고 있다.(Fig. 4.) 18년도에는 전년 대비 감염률은 2.70% 감소, 감염인원은 24.8% 감소하였으며, 19년도에는 전년 대비 감염률은 2.58% 감소, 감염인원은 42.4% 감소하였으며, 17년도 대비 감염률은 5.28% 감소, 감염인원은 56.7% 감소하였다.

훈련 대상인원이 증가함에도 불구하고 악성코드 인원과 감염률이 동시에 감소한 원인은 반복적인 훈련을 통한 임직원들의 보안인식 향상으로 추정된다. 특히, 19년도의 감염인원이 전년 대비 큰 폭으로 감

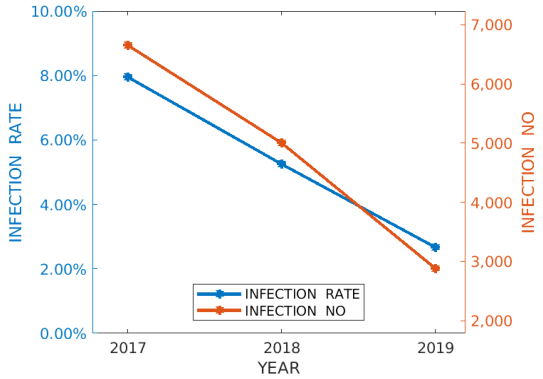


Fig. 4. Infection Result by Awareness Training

소하였는데, 랜섬웨어를 모사한 화면 잠금과 파일암호화 기능이 원인인 것으로 분석된다.

악성코드 치료율은 소폭 증가 추세를 나타내고 있다. 18년도에는 17년도 대비 치료율은 2.46% 감소하였으며, 19년도에는 18년도 대비 4.10% 증가하였으며, 17년도 대비 1.64% 증가하였다. 수치상으로 보았을 때, 치료율의 변화가 크지 않아 보이지만, 감염자의 수가 점차 즐어든 상황을 감안하였을 때, 결코 훈련의 효과가 미비하다고 할 수 없다. 또한, 악성코드에 감염되고도 치료를 하지 않은 미치료자는 심각한 보안 위험 요소라고 할 수 있으며, 19년의 미치료자 수는 2,080명으로 17년의 미치료자 4,885명 대비 57.5% 감소하였다. 이를 보면, 훈련의 효과는 상당하다고 추정할 수 있다.(Fig. 5.)

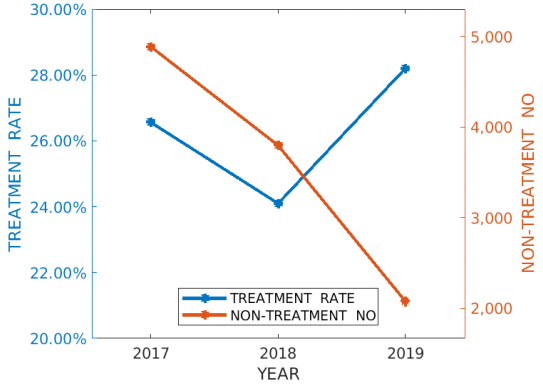


Fig. 5. Treatment by Awareness Training

### 5.3.2 테마별 결과 분석

훈련 테마는 건강, 직업, 금전, 이벤트, 위반, 공지로 대분류하여 훈련 결과를 분석하였으며 결과는 Table 4와 같다. 건강, 금전, 위반에 관한 테마에서 높은 감염률을 보였다. 특히, 건강에 관한 감염률이 상대적으로 높았는데, 건강검진 결과, 소견서 등에 대한 악성메일의 경우 빈번하게 수신하지 않는 형태이기 때문인 것으로 보인다.

Table 4. Classification of Theme

| Theme | Target | Infection | Rate |
|---|---|---|---|
| Health | 57,183 | 4,672 | 8.17% |
| Recruit | 68,645 | 874 | 1.27% |
| Money | 282,379 | 6,688 | 2.36% |
| Event | 91,542 | 747 | 0.81% |
| Violation | 124,286 | 2,608 | 2.10% |
| Notice | 29,817 | 99 | 0.33% |

### 5.3.3 위장기법별 결과 분석

HTA/HTML 스크립트 유형은 3년(17년, 18년, 19년) 간 진행하였으며, MS-Office 문서 유형은 17년에 진행하였다. PDF 문서(17년, 18년) 유형은 2년 간 진행하였다. HWP 문서 유형은 19년에 진행하였으며 그 결과는 Table 5.와 같다.

HTA/HTML 위장기법의 감염률이 압도적으로 높은 것으로 집계되었는데, 그 원인은 감염과정이 비교적 간단하며, 결제대금 안내, 대출이자 안내 메일 등 정기적으로 수신하는 정상 첨부파일의 형태이기 때문인 것으로 추정된다. 그 외의 문서형 위장기법은 뷰어로 실행할 경우 감염 프로세스가 동작하지 않거나, 콘텐츠 실행 클릭 등의 액션이 추가로 필요하므로 상대적으로 낮은 감염률을 보이는 원인으로 분석된다.

Table 5. Classification of Camouflage by Awareness Training

| Format | Target | Infection | Rate |
|---|---|---|---|
| HTA/HTML | 211,299 | 8,820 | 4.21% |
| DOC/XLS | 56,190 | 824 | 1.46% |
| PDF | 88,609 | 723 | 2.36% |
| HWP | 54,465 | 107 | 0.38% |

### 5.4 탐지 및 대응 훈련결과 분석

탐지 및 대응 훈련을 수행한 대부분의 기관은 스팸메일차단 솔루션, 행위 기반의 동적분석 장비, End-Point 안티바이러스 등의 기술적 보안대책을 갖추고 있었다. 또한, 악성메일 및 트래픽에 대한 보안관제, 침해사고 대응 및 분석이 가능한 인적 자원이 확보되어 있었다. 따라서 탐지 및 훈련용 악성코드는 훈련 수행 기관의 기술적 대책을 우회하여 동작할 수 있도록 해야 하며, 쉽게 분석이 되지 않도록 구현되어야 한다. 기존의 악성메일에 관한 연구에서는 메일의 열람여부 만을 확인[9]하거나, 악성코드를 포함하지 않은 안내 형태의 첨부파일[7]을 발송하여 훈련을 진행하였다. 이와 다르게 본 연구에서 수행한 탐지 및 대응훈련은 라자루스, 안다리엘과[24], TA505[23]와 같은 해커 그룹의 최신 공격기법을 적용한 악성코드를 이용하여 훈련을 진행하였다. 문서형태의 파일에 난독화 및 인코딩된 악성코드 주입, 정적분석 회피 기법 등을 적용하여 스팸차단 솔루션 우회를 시도하였으며, 가상화 환경 탐지, 더미코드 삽입 등을 통한 동적분석 장비 우회를 시도하였다. 또한, 시간왜곡, API 간접호출, 인젝션 등의 기법을 통해 End-Point 안티바이러스의 우회를 시도하였다. 이를 통해 악성메일 수신에서부터 단말에서의 악성코드 동작까지 일련의 과정을 실제 악성메일 공격과 유사하게 진행하였다.

#### 5.4.1 연도별 대응률 분석

악성코드 첨부형 악성메일의 대응률은 증가 추세를 나타내고 있다. 18년에는 17년 대비 대응률은 15.62% 증가하였으며, 19년에는 18년 대비 5% 증가하였으며, 17년 대비 대응률은 20.62% 증가하였다.

피싱페이지 링크형 악성메일을 통한 개인정보 유출은 감소 추세를 나타내고 있다. 18년에는 17년 대비 유출률은 20.25% 감소하였으며, 19년에는 18년 대비 7.5% 감소하였으며, 17년 대비 27.75% 감소하였다.(Fig. 6.) 이 결과로 보아, 악성메일에 대한 기관의 전체적인 대응능력이 향상하였음을 추정할 수 있다. 하지만 3년 내내 50% 이상의 기관 침투가 성공한 놀라운 수치가 집계되었다. 이는 탐지 및 대응용 악성코드가 정교하게 제작되었다고 볼 수 있으나, 역으로 말하면 최신 기법을 적용한 악성코드에 대한 기관의 대응능력 향상을 위한 노력이 더욱 필요함을 반증한다.

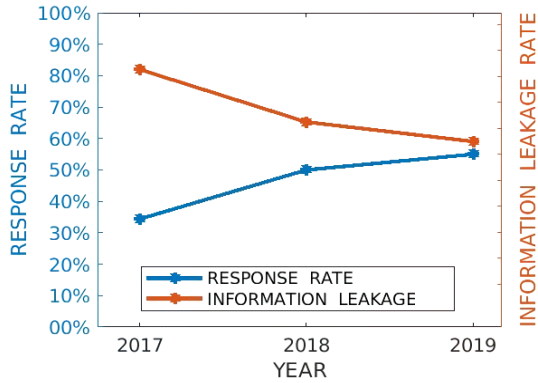


Fig. 6. Detecton & Response Training Defense Rate

#### 5.4.2 위장기법별 대응률 분석

HTA/HTML 스크립트 유형은 3년 간 진행하였으며, MS-Office 문서 유형은 17년에 진행하였다. PDF 문서 유형은 2년(17년, 18년)간 진행하였으며, HWP 문서 유형은 19년에 진행하였다. 피싱페이지와 연계된 보안 프로그램으로 위장한 실행파일 유형은 3년 간 진행하였으며 그 결과는 Table 6.와 같다.

보안 프로그램으로 위장한 PE 형태의 실행파일에 대한 대응률이 상당히 낮은 점이 눈에 띄는데, 피싱페이지와 연계 시, PE 형태의 실행파일이 보안대책 우회에 매우 효과적임을 보여준다. 이는 최근 보안취약점이 많은 ActiveX를 없애고, PE형태의 실행파일을 쉽게 다운받을 수 있게 변경한 것이 원인으로 추정된다.

Table 6. Classification of Camouflage by Detection and Response Training

| Type | Format | Rate |
|---|---|---|
| SCRIPT | HTA/HTML | 52.18% |
| DOCUMENT | DOC/XLS | 70.38% |
| | PDF | 90.32% |
| | HWP | 80% |
| EXECUTABLE | LNK | 52.7% |
| | MSI | |

## VI. 결 론

악성메일을 이용한 공격은 더 이상 사회공학적 요소만으로 성공할 수 없으며, 공격자들은 기관들의 보안 대책 우회기법을 적용하고 있다. 이에 따라, 공격은 정교해지고 있으며, 공격 횟수 및 성공률도 지속

Table 7. Malicious Training Result Summary

| Type | Year | Target | Main function | Theme | Camouflage | Infection | Year on Year | Non Treatment | Year on Year |
|---|---|---|---|---|---|---|---|---|---|
| Security Awareness | 2017 | 116 (83,658) | Education Popup | Health | HTML/HTA | 6,652 (7.95%) | - | 4,885 (73.43%) | - |
| | | | | Recruit | MS-Office | | | | |
| | | | | Violation | | | | | |
| | 2018 | 123 (95,239) | File Encryption | Money | HTML/HTA | 5,004 (5.25%) | -1,648 (-24.78%) | 3,798 (75.89%) | -1,087 (-22.25%) |
| | | | | Event | | | | | |
| | | | Screen Lock | Violation | PDF | | | | |
| | 2019 | 129 (106,964) | Image File Replicate | Money | HTML | 2,885 (2.67%) | -2,119 (-42.35%) | 2,080 (72.09%) | -1,718 (-45.24%) |
| | | | | Notice | HWP | | | | |
| | | | | Violation | | | | | |

| Theme Infection | | | Camouflage Infection | | |
|---|---|---|---|---|---|
| Theme | Target | Infection | Format | Target | Infection |
| Health | 57,183 | 4,672 (8.17%) | HTA/HTML | 211,299 | 8,820 (4.21%) |
| Recruit | 68,645 | 874 (1.27%) | MS-Office | 56,190 | 824 (1.46%) |
| Money | 282,379 | 6,688 (2.36%) | | | |
| Event | 91,542 | 747 (0.81%) | PDF | 88,609 | 723 (2.36%) |
| Violation | 124,286 | 2,608 (2.10%) | HWP | 54,465 | 107 (0.38%) |
| Notice | 29,817 | 99 (0.33%) | | | |

| Type | Year | Main function | Evasion Technique | Camouflage | Response | Year on Year | Information Leakage | Year on Year |
|---|---|---|---|---|---|---|---|---|
| Detection & Response | 2017 | Infection spread | Static | HTML/HTA | 34.38% | - | 82.75% | - |
| | | | | MS-Office | | | | |
| | 2018 | Concealment | Dynamic | PDF | 50.00% | +15.62% | 62.50% | -20.25% |
| | | Persistence | Anti-Reversing | HWP | | | | |
| | 2019 | | | MSI | 55.00% | +5.00% | 55.00% | -7.50% |
| | | Keep-alive | Obfuscation | LNK | | | | |

| Camouflage Response | | | | | |
|---|---|---|---|---|---|
| Attachment | | | | Phishing Page Link | |
| Script | Document | | | PE | |
| HTML/HTA | MS-Office | PDF | HWP | MSI | LNK |
| 52.18% | 70.38% | 90.32% | 80% | 52.7% | |

적으로 증가하고 있다. 본 연구에서는 이에 대한 대응책으로 보안인식 제고와 탐지 및 대응능력 향상을 위한 악성메일 훈련 모델을 제시하였으며, 해당 구성요소들의 구현 방법에 대해 기술하였다. 제시한 모델을 기반으로 3년 간 160여개의 기관을 대상으로 한 훈련 결과(Table 7.)를 다각도로 분석하여 효과성을 확인하였다.

기존의 연구는 설문조사를 인용[6]하거나, 한두 번에 걸친 짧은 기간의 훈련 결과를 분석한 연구가 많았다. 또한, 실제 환경이 아닌 실험실에서 수행한 연구[5][6]가 많았으며, 실제 환경에서 이루어진 훈련의 경우, 악성메일을 보내고 열람 여부만을 확인[9]하여 분석하였다. 하지만 본 연구에서는 오랜 기간, 다수의 기관을 대상으로 훈련을 수행하였으며, 악성코드 감염, 치료, 피싱페이지 접속, 개인정보 유출, 탐지 및 대응 여부 등의 요소들을 종합적으로 고려할 수 있는 훈련 모델을 설계하였다는 것에 의의가 있다. 다만, 설계한 모델을 기반으로 실효성있는 훈련을 수행하기 위해서는 최신 트렌드에 맞는 테마 설정과 공격 기법에 대한 끊임없는 연구와 적용이 필요하다.

향후에는 지속적으로 훈련 효과를 유지할 수 있는 방안에 대한 연구를 진행할 예정이다. 보안인식 제고 훈련은 대상 인원을 직급, 부서, 고용형태 등의 실험군으로 나누어 훈련을 다각화하고, 결과에 대한 인과관계를 명확히 할 수 있는 프로세스에 관한 연구가 진행되어야 할 것이다. 탐지 및 대응 훈련은 도출된 신규 취약 요소들의 즉각적인 공유 및 이전 훈련에서 대응하지 못한 취약 요소에 대한 재훈련 수행 등의 프로세스가 연구되어야 할 것이다. 해당 연구들이 진행되어 훈련의 효과를 보다 향상시킬 수 있는 모델로 발전하기를 기대한다.

## References


[1] Mimecast, "The State of Email Security Report 2019", https://www.mimecast.com/resources/press-releases/dates/2019/5/state-of-email-security-2019, May. 2019.

[2] Financial Security Institute, "2020 Cyber Threat and Prospecting Report", http://www.fsec.or.kr/common/proc/fsec/bbs/41/fileDownLoad/2237.do, Dec. 2019.

[3] In-Sook Jang, "A Study On Cybersecurity Training and Exercise Format", Proceedings of the 2016 KISS conference, pp.1039-1041, Jun. 2016.

[4] Eric Johnson, "Why Training Doesn't Mitigate Phishing", https://www.bankinfosecurity.com/interviews/spear-phishing-training-weaknesses-idd-i-2148, Jan. 2014.

[5] AT Stephanou, "The impact ofinformation security awareness training on information security behaviour: the case for further research", Proceedings of the ISSA 2008 Innovative Minds Conference, pp.309-329, Jul. 2008

[6] S. Sheng, "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp.373-382, Apr. 2010.

[7] Deanna D. Caputo, "Going Spear Phishing: Exploring Embedded Training and Awareness", IEEE security & privacy v.12 no.1, pp.28-38, Aug. 2013.

[8] Duck-sang Yoon, "A Study on the Change of Capability and Behavior against Phishing Attack by Continuous Practical Simulation Training," Journal of the Korea Institute of Information Security &Cryptology 27(2), pp.267-279, Apr. 2017.

[9] Jun-hee Lee, "A Study on Human Vulnerability Factors of Companies :Through Spam Mail Simulation Training Experiments", Journal of the Korea Institute of Information Security & Cryptology 29(4),

pp.847-857, Aug. 2019.
[10] KISA, "Wannacry Analysis Special Report", https://www.boho.or.kr/filedownload.do?attach_file_seq=2235&attach_file_id=EpF2235.pdf, Oct. 2017.
[11] KISA, "Cyber Security Issue Report : Q2 2019", https://www.boho.or.kr/filedownload.do?attach_file_seq=2235&attach_file_id=EpF2235.pdf, Aug. 2019.
[12] Jae-hwi Lee, "A Study on API Wrapping in Themida and Unpacking Technique", Journal of the Korea Institute of Information Security and Cryptology v.27 no.1, pp.67-77, Feb. 2017.
[13] Kyung-Roul Lee, "A New Analysis Method for Packed Malicious Codes", Journal of advanced navigation technology v.16 no.3 = no.54, pp.488-494. Feb. 2012.
[14] Kyeong Sik Lee, "Research on Bypass the malware dynamic analysis and Response method", Proceedings of the 2017 KISS conference, pp.1069-1071, Jul. 2017.
[15] AMIR AFIANIAN, "Malware Dynamic Analysis Evasion Techniques: A Survey", ACM Computing Surveys, Vol. 52, No. 6 Article 126, Nov. 2019.
[16] Woo-Jin Joe, "Method of detecting variant malicious codes using behavior signature", Proceedings of the 2018 KISS conference, pp.1026-1028, Dec. 2018.
[17] Jae Hyuk Suk. "Analysis of Virtualization Obfuscated Executable Files and Implementation of Automatic Analysis Tool", Journal of the Korea Institute of Information Security and Cryptology v.23 no.4, pp.709-720, Aug. 2013.
[18] Seong-Kyun Mok, "Program Slicing for Binary code Deobfuscation", Journal of the Korea Institute of Information Security & Cryptology 27(1), pp.59-66, Feb. 2017.
[19] Lee Kyung-Roul, "A Novel Process Design for Analyzing Malicious Codes That Bypass Analysis Techniques", Informatization policy v.24 no.4 = no.93, pp.68-78, Dec. 2017.
[20] Choi suk-woo, "Method Of Obfuscation Binary Analysis" Communications of the Korean Institute of Information Scientists and Engineers v.36 no.3, pp.26-31, Mar. 2018.
[21] Ah Reum Kang, "Detection of Malicious PDF based on Document Structure Features and Stream Objects", Journal of The Korea Society of Computer and Information Vol. 23 No. 11, pp. 85-93, Nov. 2018.
[22] Financial Security Institute, "Campaign DOKKAIEBI", http://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/1754.do, Aug. 2018.
[23] Financial Security Institute, "TA505 Threat Group Profiling", http://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2297.do, Aug. 2020.
[24] Financial Security Institute, "Campaign RIFLE", http://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/1752.do, Jul. 2017.

## 〈저 자 소 개〉

강 영 묵 (Young-mook Kang) 정회원
2016년 2월: 동국대학교 컴퓨터공학과 졸업
2018년 9월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 악성코드, 디지털포렌식, 침해사고대응, 보안인식

이 상 진 (Sangjin Lee) 종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포헨식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층암호 해시함수