바이러스 제작과 취약점 분석(모의침투훈련 경험과 분석)

<<김민규, 심형주, 조영범, 최승혁, 한승희>>

1. 프로젝트 개요

- C&C 서버 구축과 바이러스 제작 연구를 통한 모의침투 훈련 경험
- 보안 취약점 발견 및 이를 활용한 모의침투 훈련 경험

* 본 포트폴리오에는 실제 구현한 바이러스에 대한 내용만을 포함하고 있습니다.

* 보안 및 기밀 유지를 위해 실제 코드와 상세한 구현 내용은 생략하였습니다.

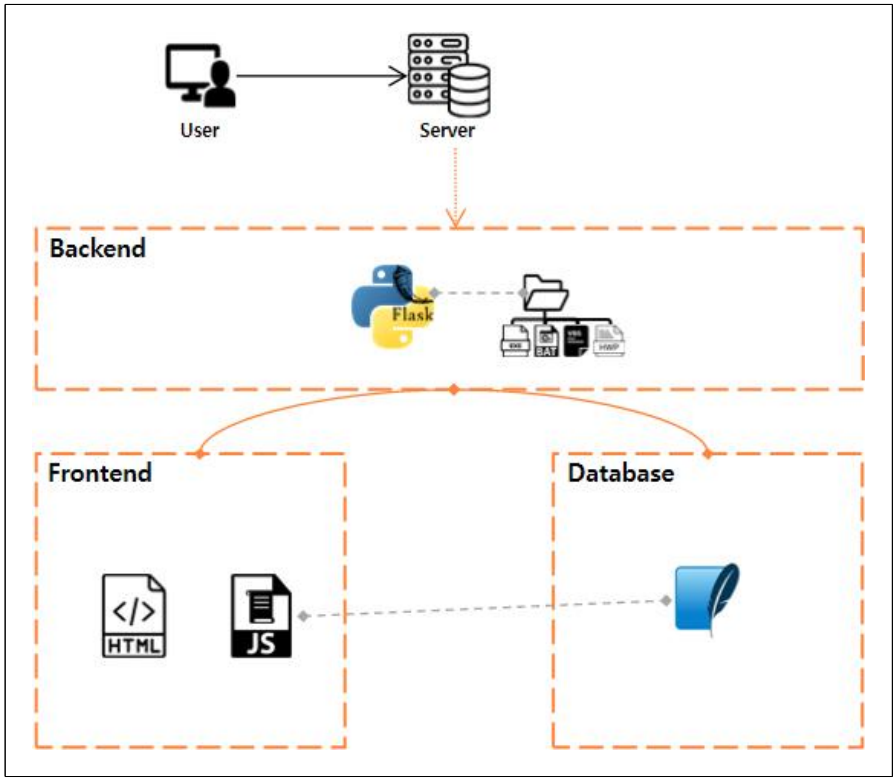
2. 바이러스 제작 경험

2.1 바이러스 제작에 사용한 기술과 도구

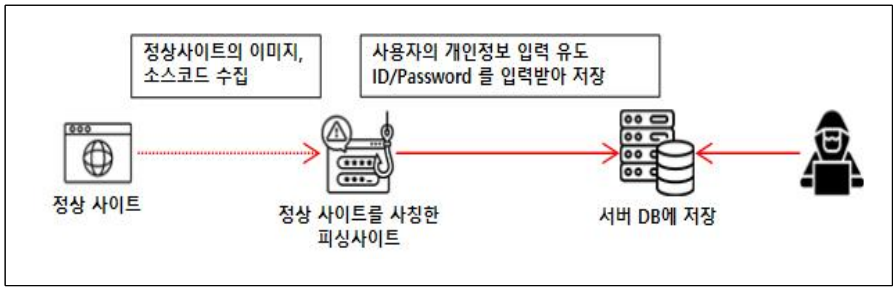
- 도구 : Anaconda3, Js, sqlite, X32dbg, IDA, resource hacker, Vbscript, OS Command
- 기술 : 네트워크/포트 스캐닝, 취약점 분석, C&C 서버 및 악성코드 개발

2.2 바이러스 주요 특징 및 동작 구조

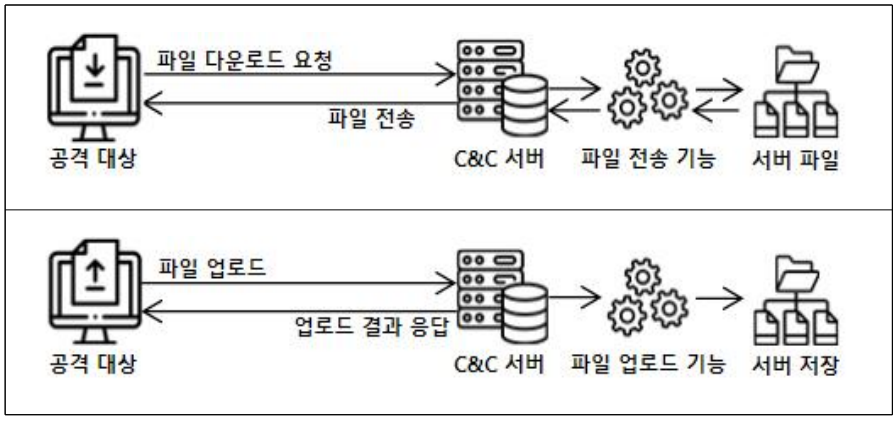
1) C&C 서버 : Python Flask, Js, sqlite를 사용하여 웹, 기능 구현



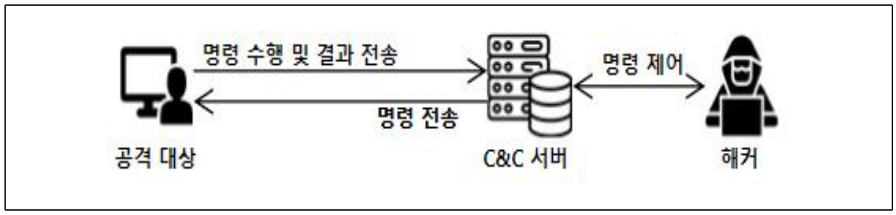
1-1) 피싱 사이트 모의 공격 개발



1-2) C&C 서버 기능 구현 (파일 다운로드/업로드 기능)

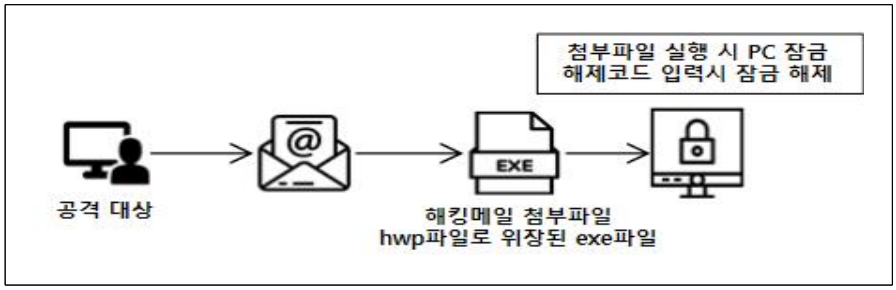


1-3) C&C 서버를 통해 감염단말을 원격으로 조작하는 기능 구현



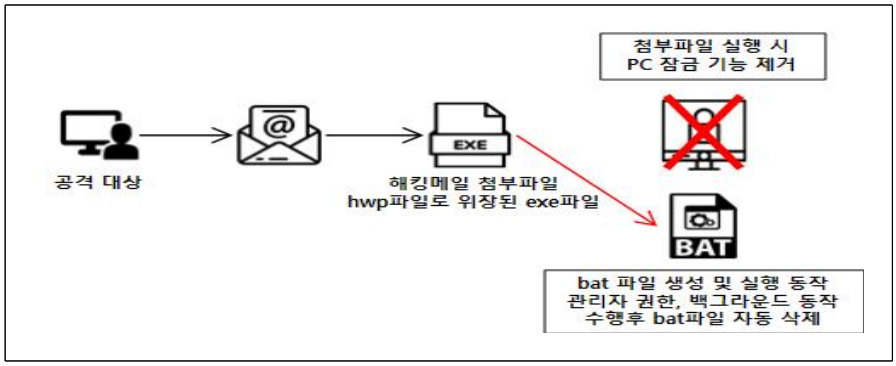
2) 악성코드 : 한글파일을 위장한 악성코드 제작

2-1) 기존 악성코드



2-2) 악성 배치 파일을 생성 및 실행하는 악성코드 제작

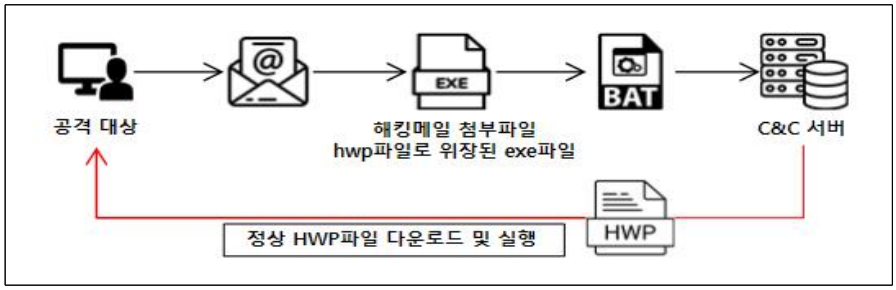
- x32dbg, IDA를 사용하여 기존 악성코드를 리버싱
- bat 파일 생성 및 실행 동작으로 구조 변경



2.3 C&C 서버를 이용하는 악성코드

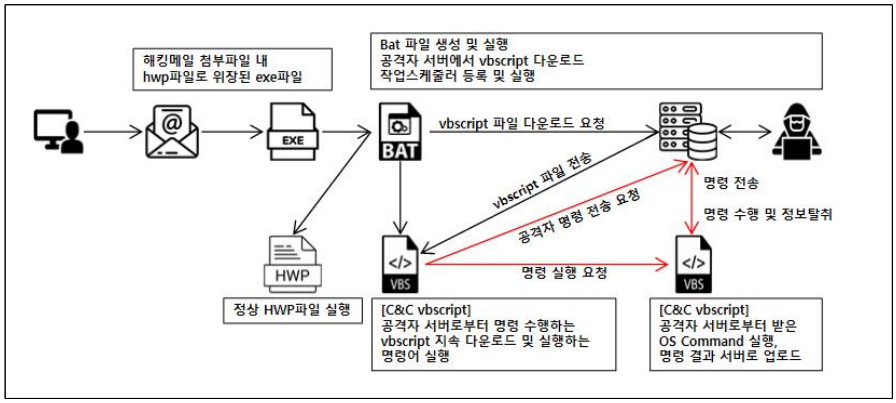
1) 정상파일로 위장하는 악성코드 제작

- bat 파일을 통해 curl 명령 수행
  * C&C 서버로부터 정상파일을 다운로드 및 실행



2) C&C 서버에서 감염단말 제어 악성코드 구현

- bat 파일을 이용하여 OS command 수행
  * curl, schtasks, taskkill, 레지스트리 등록, 파일 생성 등
- vbscript를 이용하여 감염된 좀비 PC와 C&C 서버 간 통신 구현
  * 반복문의 무한 루프를 활용하여 C&C 서버와 주기적 통신 구현
  * 공격자는 C&C 서버에 명령을 생성하면 감염된 좀비 PC가 C&C 서버에 생성된 명령을 가져와 실행하는 형태



3) 자료탈취, 개인정보 탈취 등의 악성 행위 구현

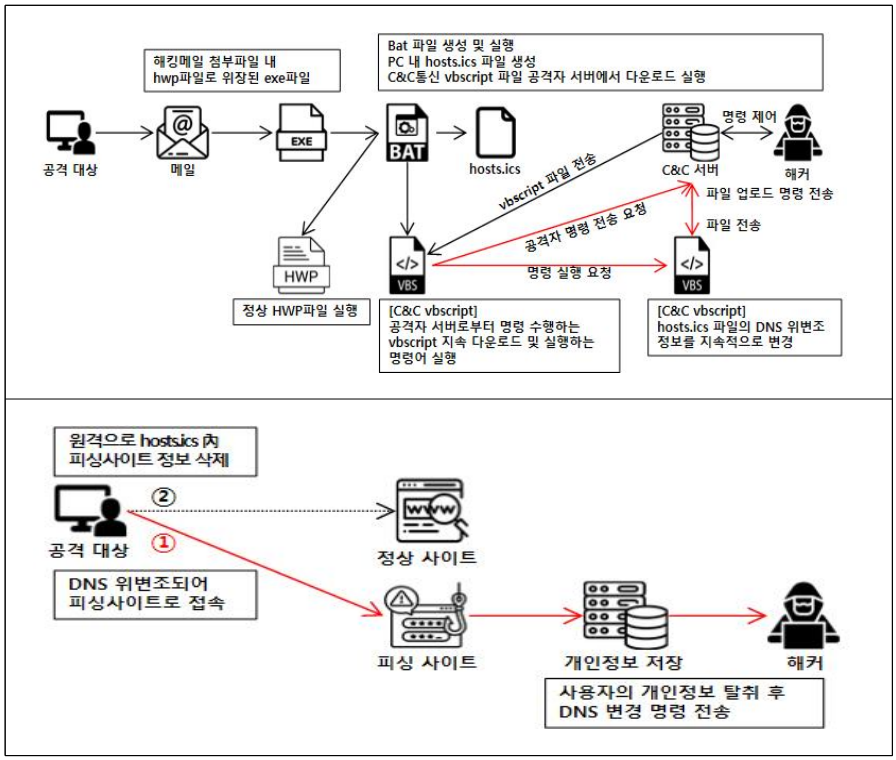
- 감염 단말의 DNS 위변조를 통한 파밍 공격 구현

  * Windows의 DNS 질의 우선순위를 이용한 DNS 위변조

    DNS 질의 우선순위 : DNS cache > hosts.ics > hosts > DNS Query)

  * 피싱 사이트로 접속하여 개인정보 입력을 유도하고 개인정보 탈취

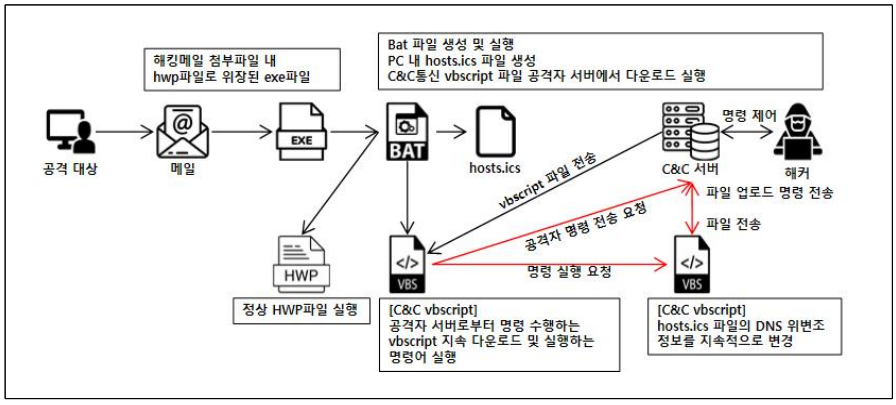
  * 개인정보 탈취 후 원격명령 전송으로 hosts.ics 파일 內 피싱사이트 정보 삭제



- 감염 단말의 자료탈취 기능 구현

  * 첨부파일 실행 시 PC 內 자료 스캔 후 C&C 서버 업로드

  * 대용량 통신 탐지를 우회하기 위해 소량씩 C&C 서버로 전송



3. 취약점 분석 경험

3.1 취약점 분석에 사용한 방법과 도구

• 도구 : nmap, ncat, 취약점 분석 서버

• 기술 : 주요정보통신기반기설 기술적 취약점 분석 평가 상세 가이드,
네트워크/포트 스캐닝, 웹 취약점, 서버 및 네트워크 취약점

3.2 발견한 취약점과 해당 취약점으로부터 얻은 교훈

* 보안 및 기밀 유지를 위해 생략하겠습니다.

4. 모의침투훈련 경험

4.1 모의침투훈련 시나리오

• APT(지능형 지속 공격) 공격 유형의 지속적인 모의침투훈련

- 지속적인 사이버 위협 대응력 강화와 APT 공격 탐지 체계의 구축
- 사용자들의 사이버 위협에 대한 중요성과 대응 방안 교육

• 성과 :

- 실제 침해사고 사례와 유사한 공격에 대한 대비력 강화
- APT 공격 탐지 체계 개선 및 사이버 위협 대응 능력 향상

4.2 공격 구조 및 분석

• 시뮬레이션한 공격 구조 설명

1) 시작 : 웹메일을 통한 악성코드 전파

- 사회공학적 기법을 활용한 메일 열람 유도
  * 관련된 메일 제목 및 본문 작성하여 사용자의 관심 유도
- 개인정보 수집 및 거점 확보, 네트워크 정보 탐색
  * 감염 단말의 개인정보 수집 및 확보된 정보를 기반으로 좀비봇 PC 다량 확보

2) 중간 : 관리자 계정, 서버 권한 탈취

- 웹 서비스의 관리자 계정 탈취 및 서버 취약점 공격
- Backdoor나 좀비봇 PC를 통한 공격자 위치 은닉 및
  동시적 공격으로 혼란 조성
- 대량 감염 및 정보시스템 장악

3) 마무리 : 개인정보 파기 및 사후조치

- 수집한 개인정보 파기 및 바이러스 제거
- 정보시스템 정상화 및 취약점 조치
- 모의침투훈련 산출물 작성

5. 보완 및 개선점

- 더 나은 보안 솔루션을 위해 기존 시스템의 보안 취약점을 지속적으로 점검하고 보완하는 프로세스를 강화할 필요가 있습니다.
- 보다 다양한 보안 취약점 및 해킹 시나리오를 시뮬레이션하는 모의침투 테스트를 통해 대비력을 강화하고자 합니다.
- 보안 교육 및 인식 활동을 통해 조직 구성원들의 보안 인식과 대응 능력을 강화할 계획입니다.

6. 결론

- 이 프로젝트를 통해 보안 분야에서 얻은 경험과 지식은 향후 프로젝트에 적용할 예정입니다.
- 바이러스 제작 및 구현 과정에서 얻은 지식은 이 프로젝트의 핵심이었고, 모의침투훈련과 취약점 보완에 큰 영향을 주었습니다.
- 공격자와 방어팀 시선을 경험함으로써 취약점 파악과 보완에 기여했으며, 이는 보다 강력한 보안 대책 마련에 기여했습니다.
- 이 프로젝트를 통해 복잡한 시스템과 보안적 취약점을 해결하는 방법에 대한 깊은 이해가 가능했습니다.
- 보안 분야에서 얻은 경험과 지식을 다음 프로젝트에 적용하여 보다 효율적인 보안 솔루션을 제공할 계획입니다.
- 마지막으로, 이 프로젝트의 성과는 팀원들의 헌신적인 노력과 협력 덕분입니다. 함께하며 서로의 강점을 발휘하여 프로젝트를 완수하는 과정에서 많은 것을 배웠고, 이는 저에게 소중한 경험이었습니다. 팀원들에게 깊은 감사를 전하며, 함께한 시간이 소중하고 가치있었음을 강조하고 싶습니다.