SpyUSB

내부망 침투 및 정보 유출 시나리오

강지혁
권승원*
고은이
서동민

목차

팀원 소개

강지혁

- Payload 제작
- Privilege Escalation
- 내부망 구축
- loader & module 구조 설계
- 키로깅 제작

고은이

- schtasks 지속성 기법 구현
- Registry Run key 지속성 기법 구현
- 코드 구조 설계 및 통합

권승원

- 라즈베리파이 구축
- HTTPS 전송로직 구현
- Fastapi 서버 구축
- 이벤트로그 중지 및 로그 삭제

서동민

- Flask 기반 C&C 웹 대시보드 구축
- 양방향 C&C 채널을 통한 원격 코드 실행 (RCE) 구현
- Go 기반 DNS C&C 서버 구축
- 다기능 C&C 에이전트 개발

선정 이유

내부자에 의한 정보 유출

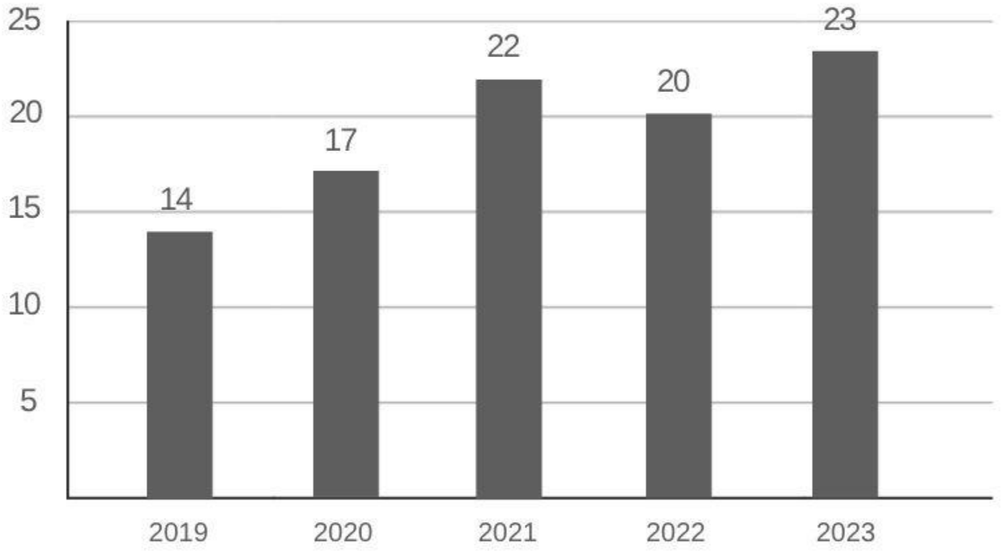
국가정보원 통계에 따르면 최근 수년간 내부자에 의한
정보 유출 사례가 지속적으로 증가하는 추세

기존 보안 체계의 내부 위협 탐지 한계

내부자가 보유한 권한을 활용한 비정상 행위는 기존 보안 체계로는
탐지 및 대응이 어려운 구조적 한계를 지님

기술 기반 시나리오 구현의 필요성 대두

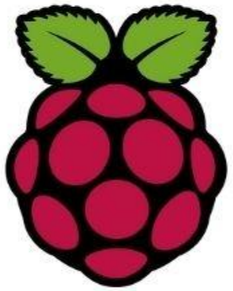
현실과 동떨어진 대응 방식의 한계를 극복하기 위해
실제 내부자 공격 시나리오를 기술적으로 구현하는 접근이
더욱 중요해지고 있음



내부자 유출 사례 연도별 변화

자료 출처: https://www.hankyung.com/article/202402273629i

기술 스택



프로그램

C - payload

python - 웹 대시보드/API/Flask

go - DNS C&C 서버

bash - 서버 관리 및 자동화, 라즈베리파이 구축

hid - 키보드 입력 자동화

환경

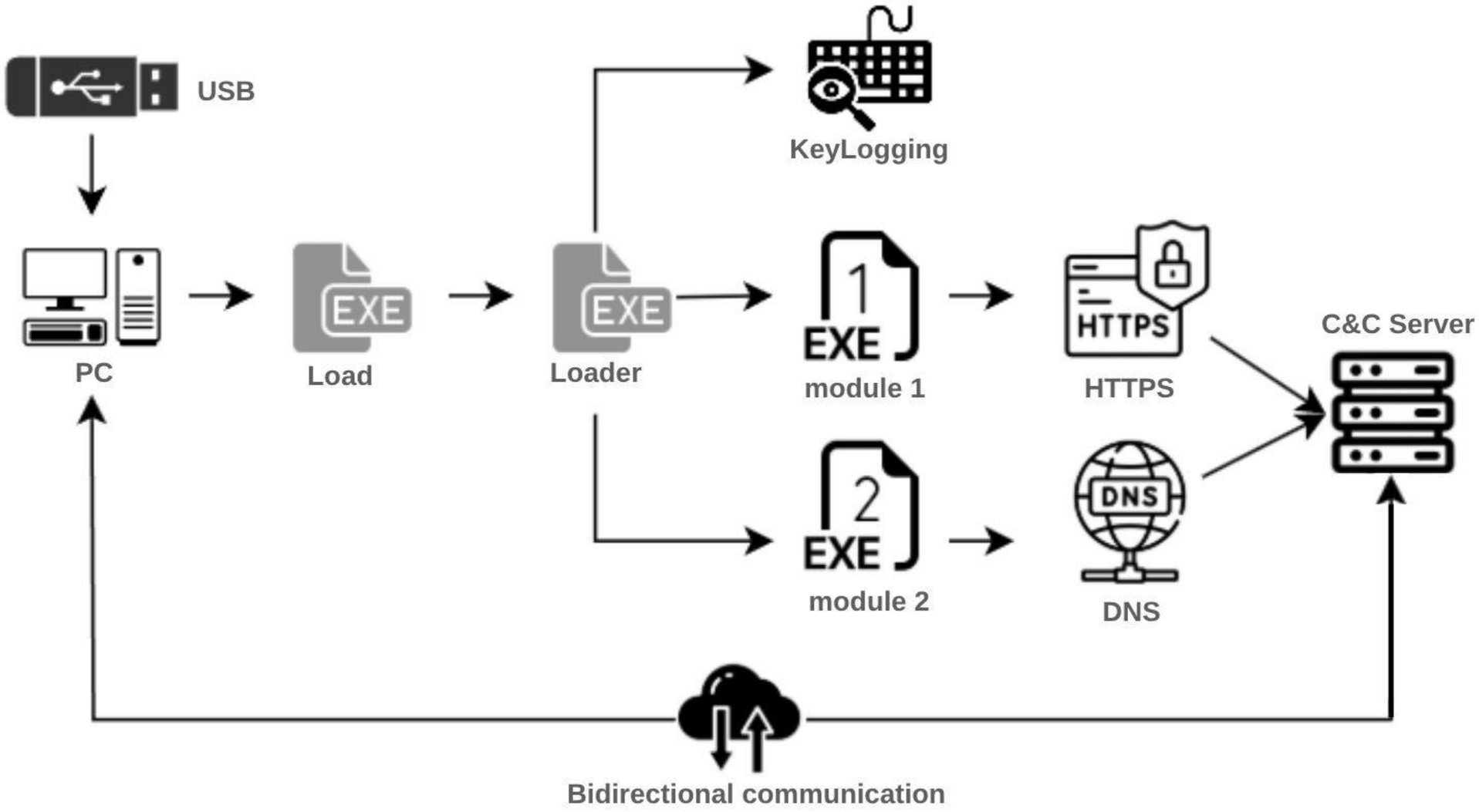
Windows 11(OS 26100.4061) - Internal Client Node

라즈베리파이 - Raspberry Pi zero 2w

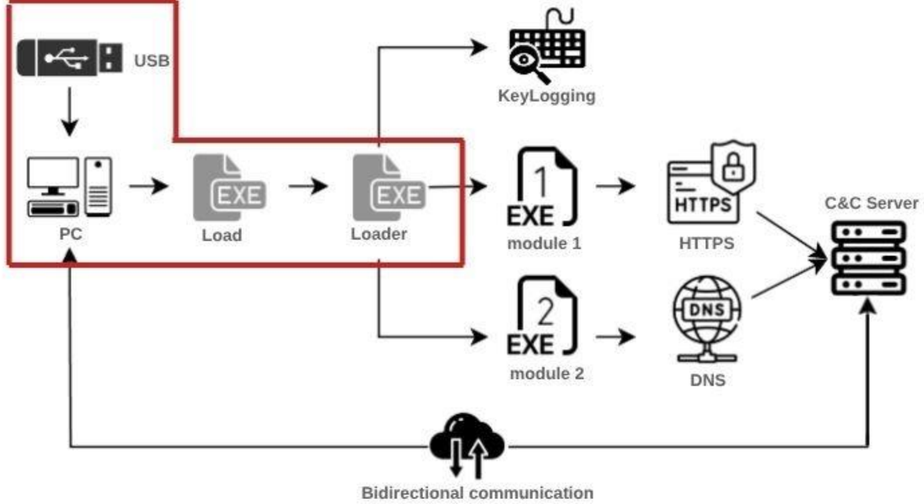
VPS(서버) - Ubuntu22.04(LTS) x64

리눅스 - Fedora 39 (64bit), Raspberry Pi OS Lite (32bit)

시나리오


USB
KeyLogging
PC
Load
EXE
Loader
EXE
1
EXE
module 1
HTTPS
HTTPS
C&C Server
2
EXE
module 2
DNS
DNS
Bidirectional communication

구현 결과



USB HID 공격

PC에 USB를 삽입된 순간 HID 공격으로 CMD창에 악성코드 실행

UAC(User Account Control) 우회

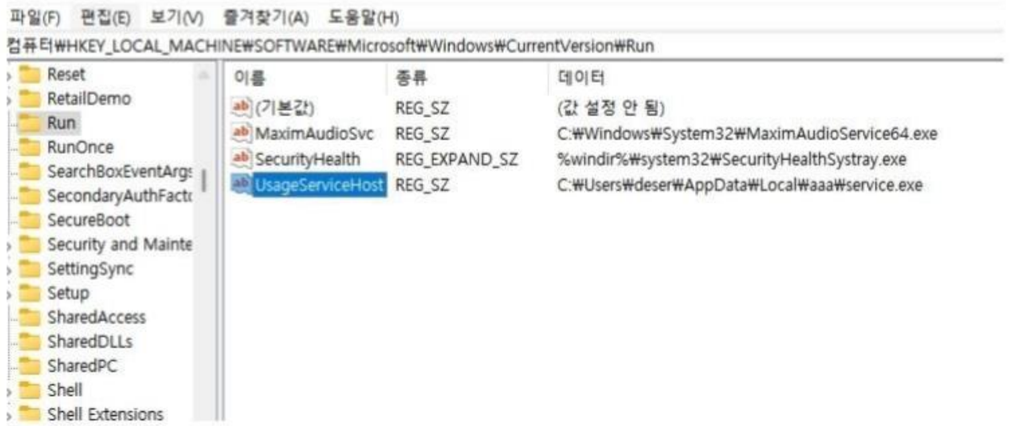
UAC 우회를 통해 초기 악성 프로그램 실행(Loader)

악성 행위 수행

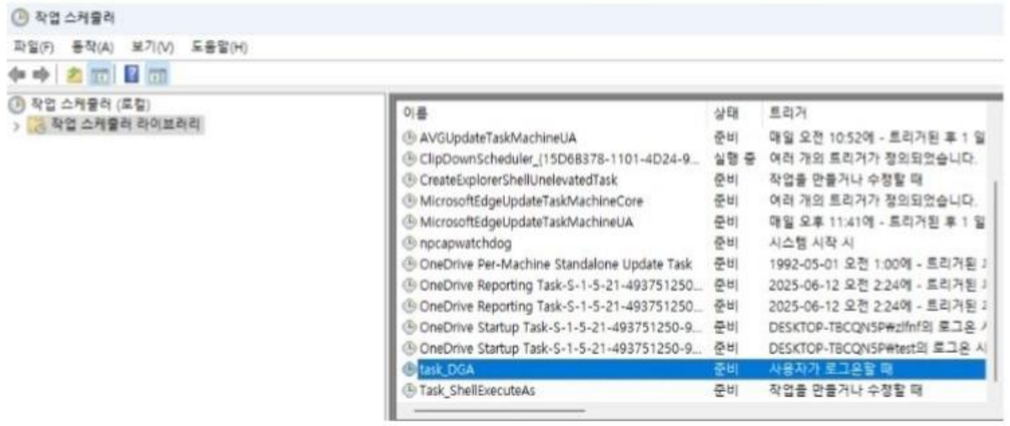
초기 실행된 프로그램은 보안 우회 및 지속성 확보 후 권한 상승을 거쳐 파일 수집 모듈 구동

구현 결과

지속성



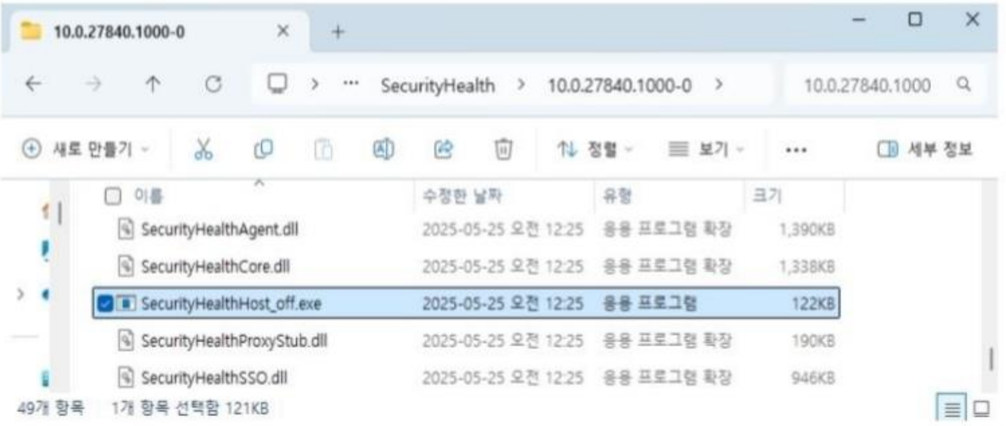
레지스트리 Run 키 등록



작업 스케줄러 등록

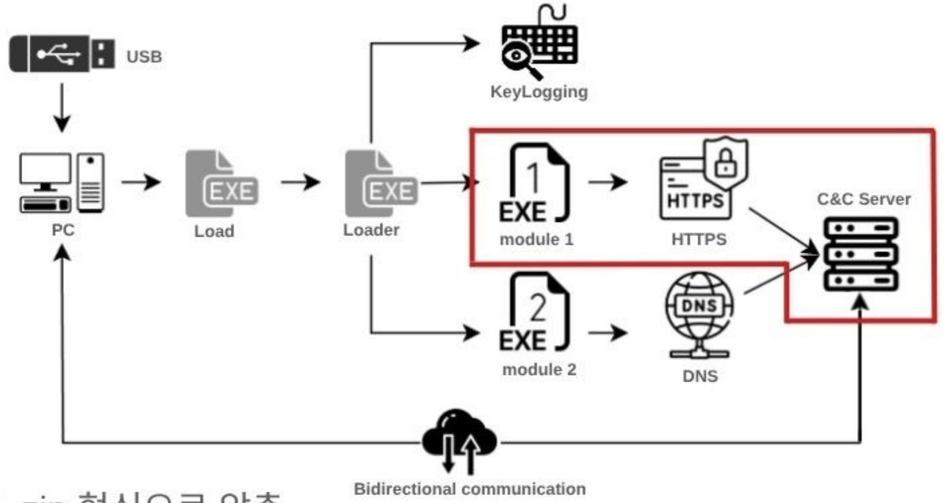
탐지 우회

Defender 예외 처리 등록



SecurityHealthHost 종료

구현 결과



module 1

PDF, HWP 등 특정 확장자를 대상으로 한 번에 대용량 파일을 수집하고 .zip 형식으로 압축

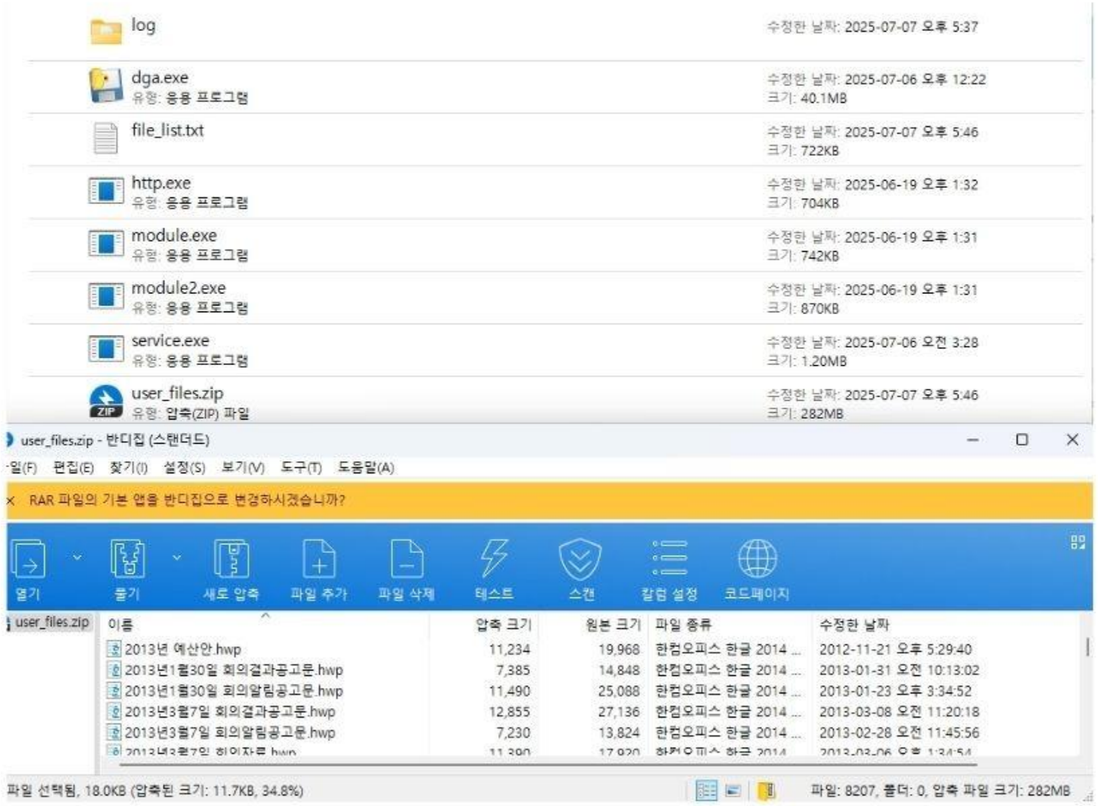
HTTPS 기반 정보유출

암호화한 후, 청크 단위로 나눠 HTTPS를 통해 FastAPI 서버로 전송

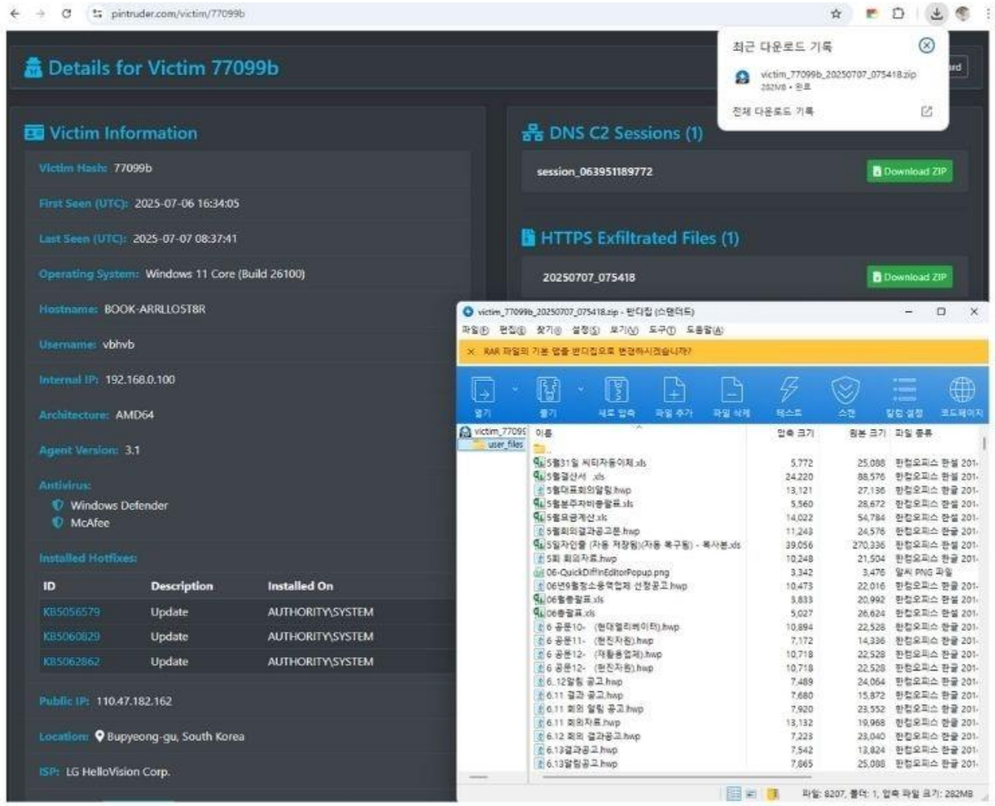
C&C 서버 수신 및 자동 복원

암호화된 데이터는 프록시 서버로 사용된 FastAPI에서 자동으로 복호화 및 재조립 한 후
C&C 서버로 전달

구현 결과

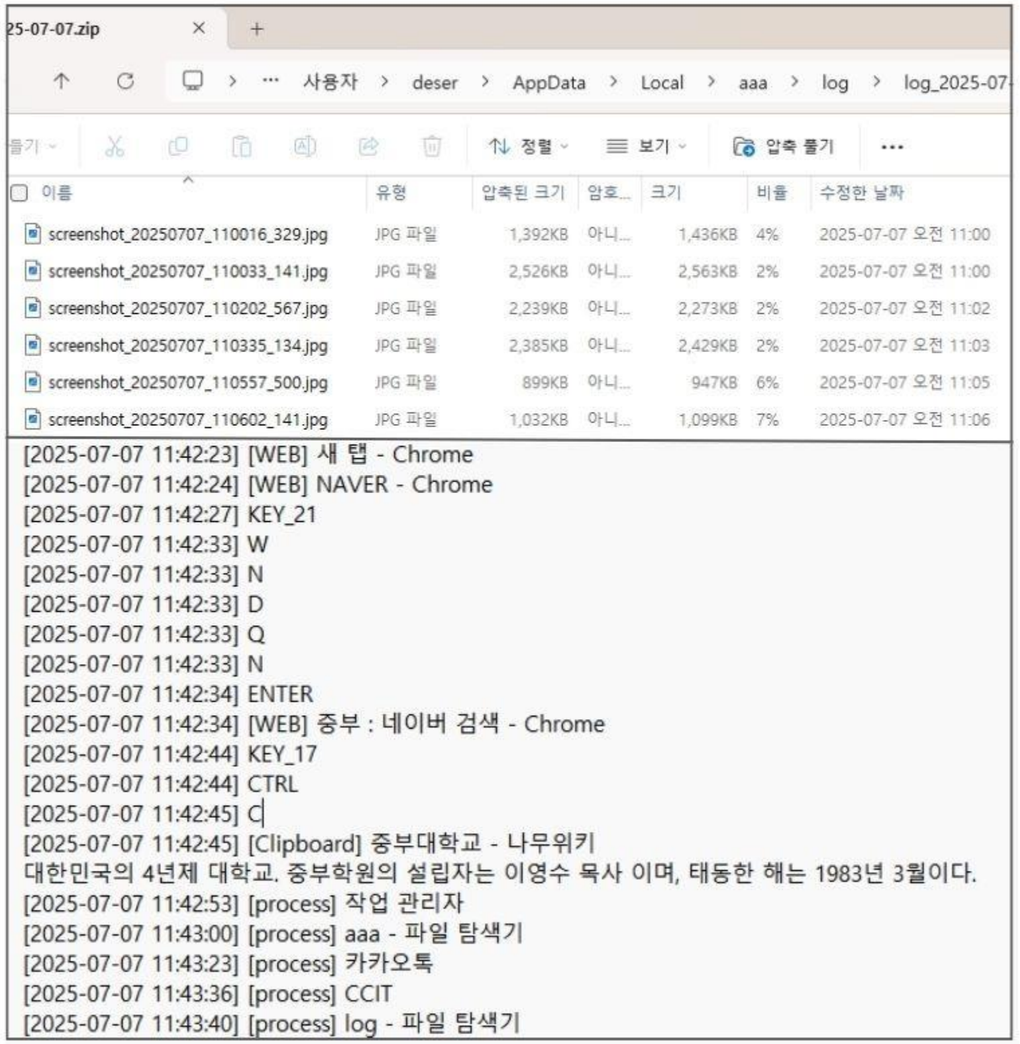


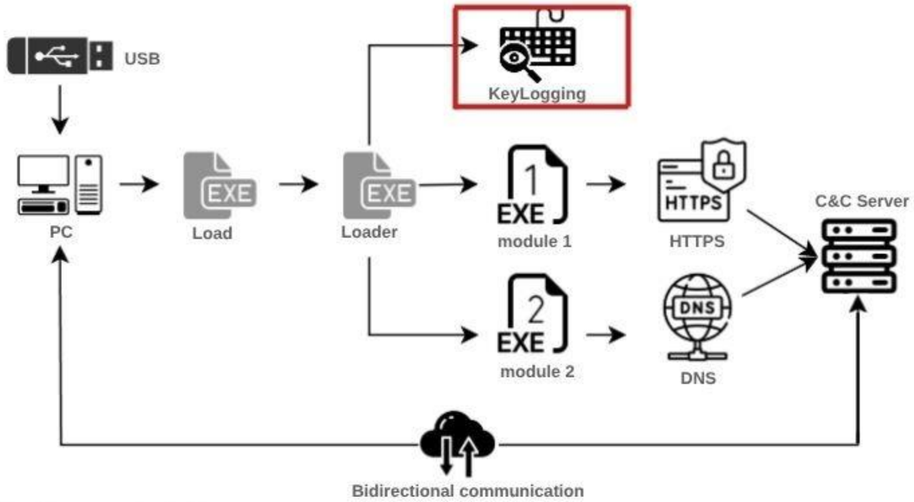
피해자 PC에서 수집된 파일의 압축 결과



C&C 서버에서 수신된 압축 파일의 복원 결과

구현 결과





스크린샷 압축 파일

스크린샷 이름: 날짜 + 시간 + 난수

ZIP 파일 이름: log_YYYY-MM-DD.zip

윈도우 타이틀 변경 시 자동 캡처 및 저장

키로깅 텍스트 파일

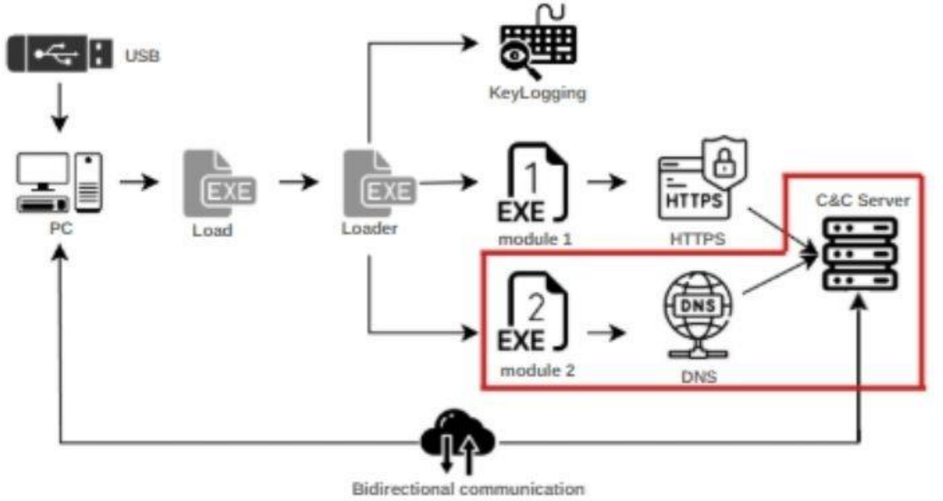
키 입력, 클립보드 내용 기록

사용 중인 프로그램명 구분 (웹브라우저, 카카오톡, 작업 관리자 등)

파일 보관

수집된 모든 파일은 C2 서버로 전송이 완료되면 원본은 자동 삭제

구현 결과



module 2

수정된 날짜 및 module 1 이후에 생성된 파일들 대상으로
특정확장자 파일을 탐색 해 .zip 형식으로 압축

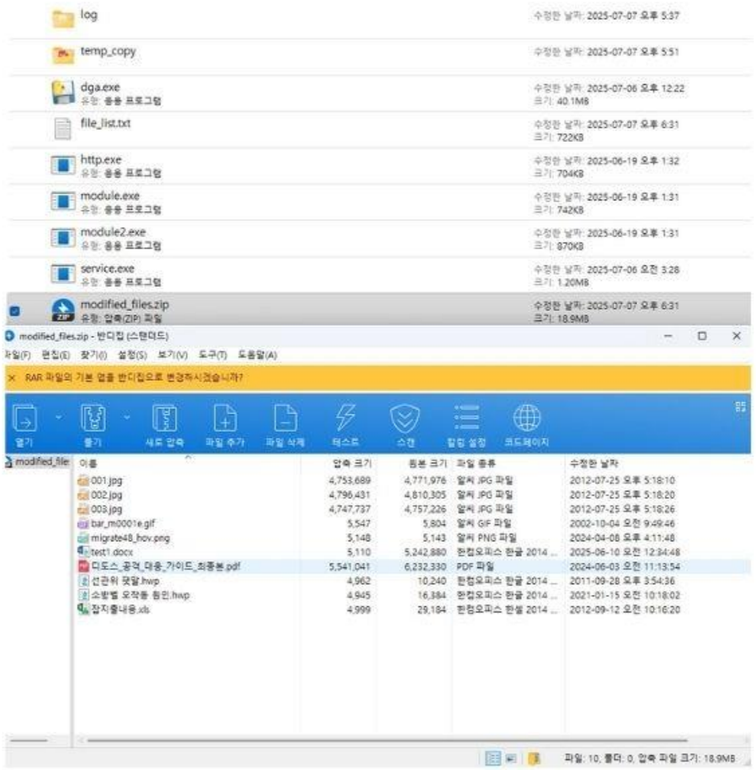
DGA 기반 DNS 정보 유출

DGA로 생성한 도메인에 데이터를 전송, 실패 시 고정 도메인으로 우회하여 유출

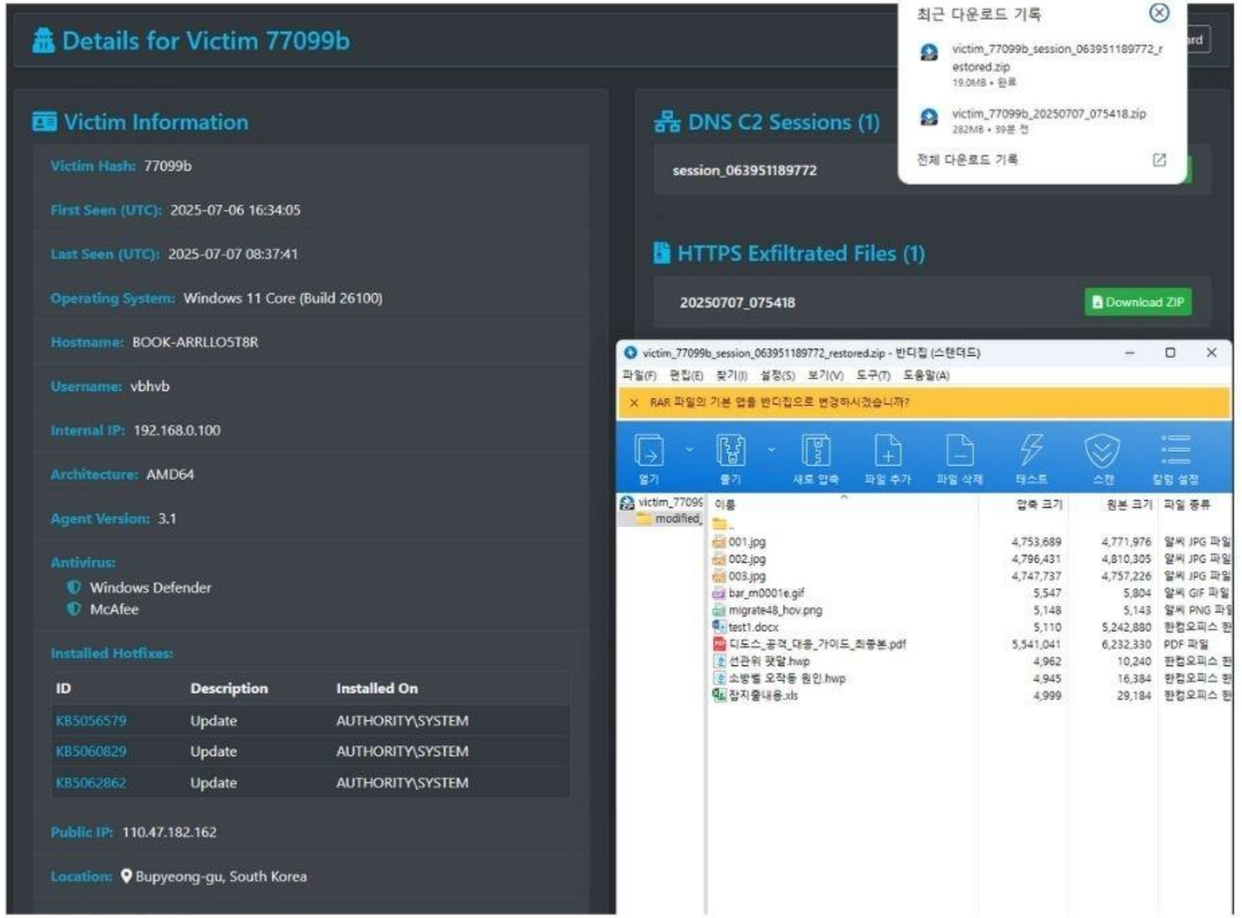
C&C 서버 수신 및 자동 복원

전송된 암호화 데이터를 C&C 서버에서 수신한 뒤, 자동 복호화 및 압축 해제를 통해 파일 복원

구현 결과

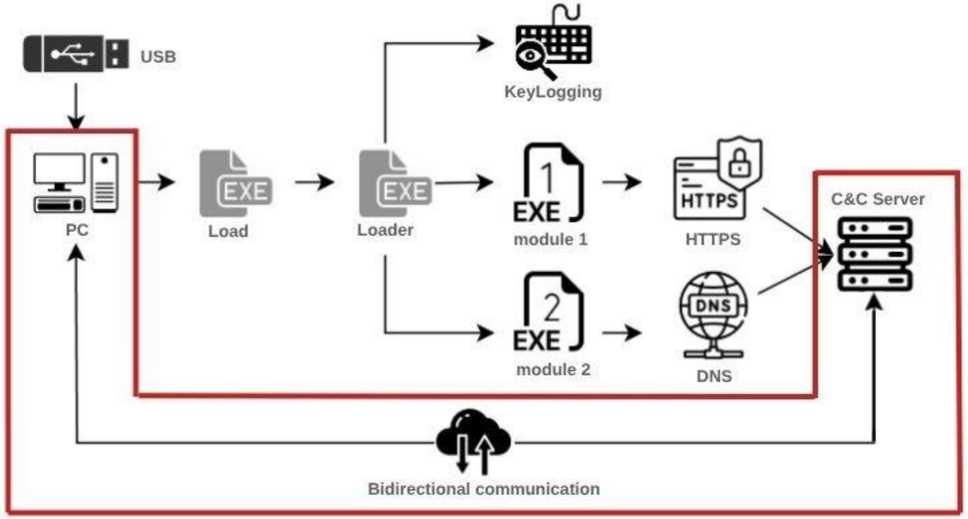


피해자 PC에서 수집된 파일의 압축 결과



C&C 서버에서 수신된 압축 파일의 복원 결과

구현 결과



명령 수신(Inbound)

피해자PC는 일정 주기로 C2 서버에 접속하여 피해자 고유 식별자와 시스템 정보를 포함한 명령 요청을 보냄

웹 페이지에 입력한 명령어를 암호화된 형태로 응답에 포함하여 전달함

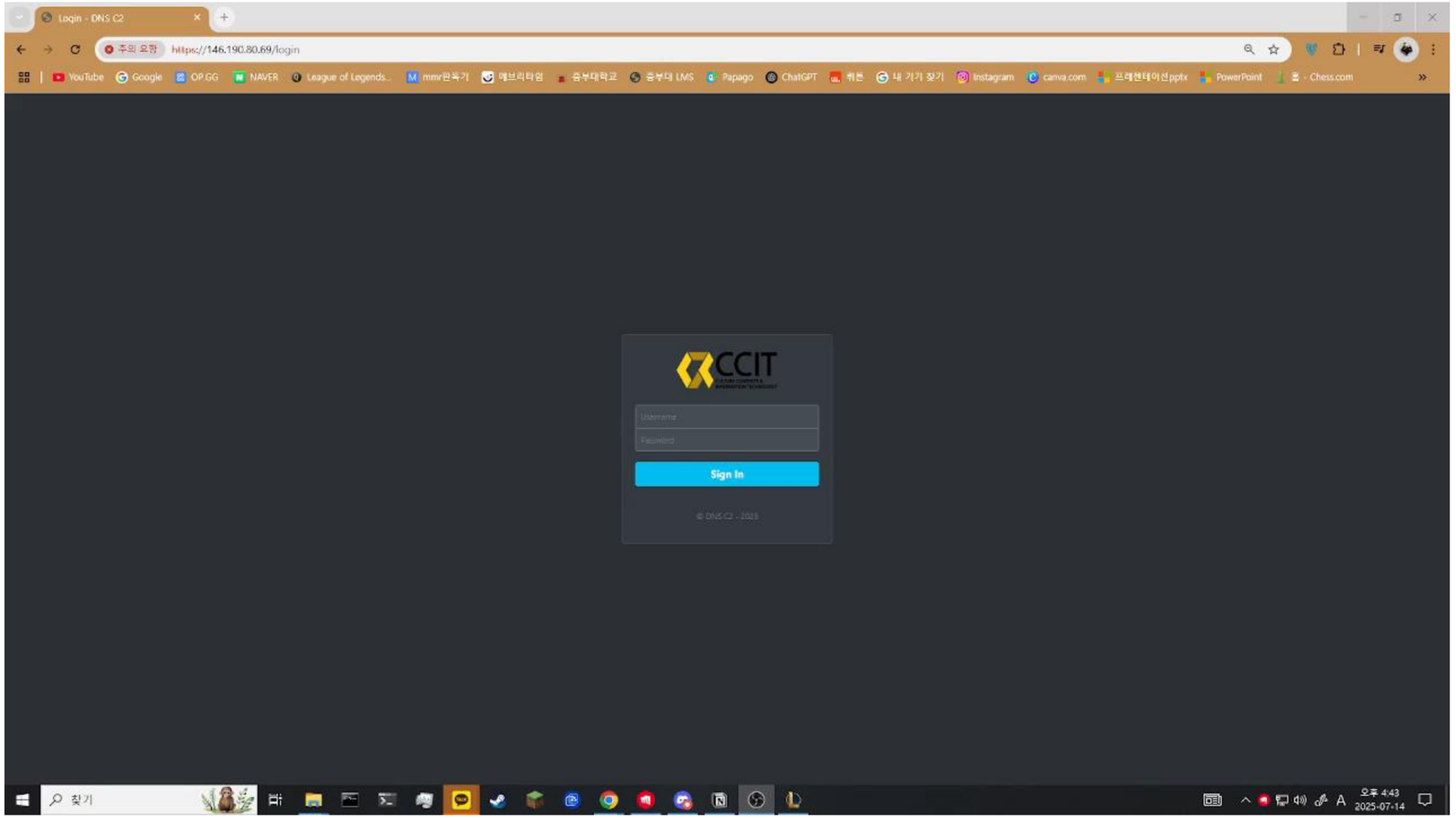
클라이언트는 사전에 공유된 세션 키를 사용해 암호화된 명령을 복호화한 뒤, 명령 프롬프트 통해 해당 명령을 실행

결과 전송(Outbound)

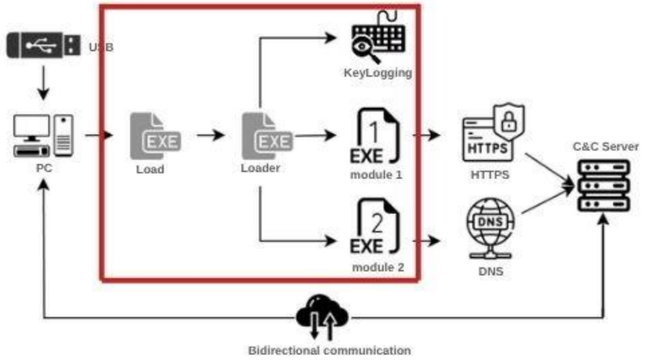
명령 실행 결과는 텍스트 출력 또는 오류 메시지를 포함하며, 세션 키를 사용해 암호화된 형태로 서버에 전송

서버는 전달받은 결과를 복호화 실시간으로 웹 페이지에 출력하여 명령 수행 여부와 내용을 즉시 확인 가능

DEMO



대응방안 - 정책

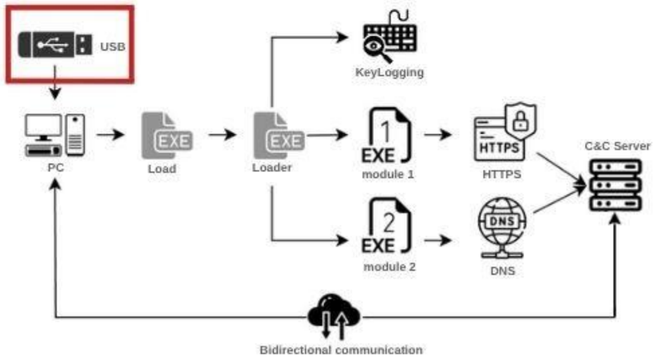


시스템 정책 설정

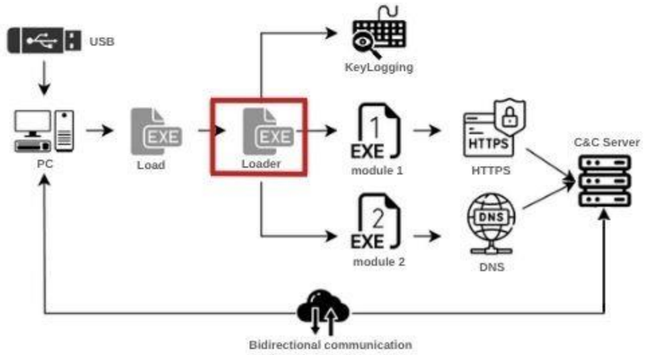
- UAC 감도 설정
- PowerShell 실행 정책
- 보안 이벤트 로그 설정
- 현재 사용자 그룹
- 응용프로그램 제어 정책 사용
- 로그온 자동 실행 제한
- CMD 실행 파일 권한 제한

이동식 저장매체 정책

- 이동식 디스크 접근 차단 정책
- 인가된 디스크 필터링 정책

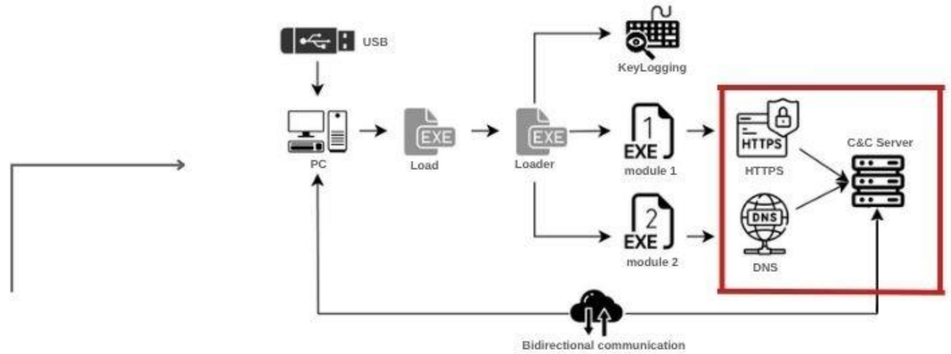


대응방안 - 정책



Defender 예외 관리

- 등록된 예외 항목 주기 점검
- 의심 경로(AppData, Temp 등) 예외 등록 감시 및 차단 정책 수립



네트워크 설정

- 텍스트 DNS 외부 통신
- DNS 서버 설정
- HTTP/HTTPS 통신
- PowerShell DNS/HTTP 질의
- 방화벽 아웃바운드 정책
- 브라우저 외 HTTPS 사용 프로그램 점검

대응방안 - 기술

대응 기술

허니청크(Honey Chunk)를 이용해 프록시 서버에서
DNS 터널링을 탐지 및 차단하는 방법

WDAC 정책으로 디펜더 예외등록 차단하기

USB 포트 사용 감지 시, 사용자에게 알림 전송

공격 기반 보안 점검 체계에 대한 후속 연구 및 적용 사례 확산 가능

개선 방향

잠금화면시 작동 불가

win + L 잠금화면시, hid 공격이 실행이 안되는 점

네트워크 공격으로 발전

물리적 공격이 아닌 네트워크를 통해 원격으로 초기 접근하도록 개선

사용자 권한 제한

관리자(Admin) 권한 사용자만 대상이며,
일반 사용자(User 그룹)에 대한 권한 상승(LPE)이 미비함

일반 사용자 대상 LPE 기법 적용

취약점 기반 권한 상승을 통해 User 그룹에서도
SYSTEM 권한 획득 가능하게 개선

디스크 기반 악성코드 실행

악성 모듈이 디스크에 저장되어 탐지 가능성이 높고,
고급 악성코드 대비 탐지 회피력이 부족함

메모리 기반 실행 구조로 전환

스크립트리스 & Fileless 방식으로 탐지 우회 및 흔적 최소화
우회 기술 고도화
BYOVD, 메모리 주입 등 최신 탐지 우회 트렌드 적용

개선 방향

지속성 유지 방식의 단조로움

작업 스케줄러 기반 등록은 흔히 사용되는 기법으로
탐지될 가능성이 높음

은밀한 지속성 확보

WMI 이벤트 구독, COM/CLSID 하이재킹, BITS 등
고급 은폐 기법 도입

C2 서버의 불안정성

저사양 VPS 환경에서 간헐적으로 응답 중단 현상 발생

서버 최적화 및 모니터링 도입

Nginx/Gunicorn 튜닝, Prometheus 기반 헬스 체크 시스템 구축

DGA 도메인 수동 운영

도메인을 수동으로 구매하고 설정해야 하므로
관리 효율성이 떨어짐

DGA 도메인 자동화 시스템 구축

예측 스크립트 + 등록업체 API 연동으로 자동 구매 및 설정 수행

Q&A

Question & Answer

감사합니다

Thank you for watching