K-Shield Jr.

INFOTECT

INFOTECT
- 머신러닝 활용한 DGA 봇넷 C&C 접속 탐지 프로젝트 기획안


Andre


Jack


Airen


Yeny


Jiny


Joony

목차

1. 배경

배경

- BotNet을 이용한 대규모 사이버 공격의 빈도와 규모가 더욱 커지고 있음

배경

- **DGA(Domain Generation Algorithm)를 사용하여 C&C 차단을 우회하는 것으로 보임**

보안뉴스

DNS 이용한 공격, 어디까지 진화했나

멀웨어 감염, DNS 방식으로 진화...90% 이상 DNS 이용

DNS 정보, 다각적인 보안 아키텍처에 통합해 가시성 확보해야

[보안뉴스 김경애 기자] 멀웨어는 DNS를 이용하여 사용자의 PC를 감염시
로드할 때도, 해커가 필요한 정보를 탈취할 때도, C&C(명령제어) 서버와 통
러다 보니 현재 90% 이상의 멀웨어가 DNS를 이용하는 것으로 분석됐다.

C&C 서버는 IP 통신을 시작으로, Fast Flux를 거쳐 DGA(Domain Generation Algorithm)를 사용하는 단계까지 진화했다. 현재 C&C 서버는 Fast Flux와 DGA 기법을 합친 형태로 진화하고 있다. 이렇게 진화하는 해커들의 공격은 분석과 추적이 매우 어렵다.

avast

[보안 사고 공지] 씨클리너 v5.33.6162 버전에서 백도어 삽입 이슈

- IP 주소에 접속할 수 없을 경우에는 DGA(Domain name generator)의 형태의 백업 주소가 활성화되고 다른 곳에 있는 서버로 통신을 시도함. 다행이 생성된 도메인은 공격자의 권한 밖이어서 위협에 노출되지 않음

보안뉴스

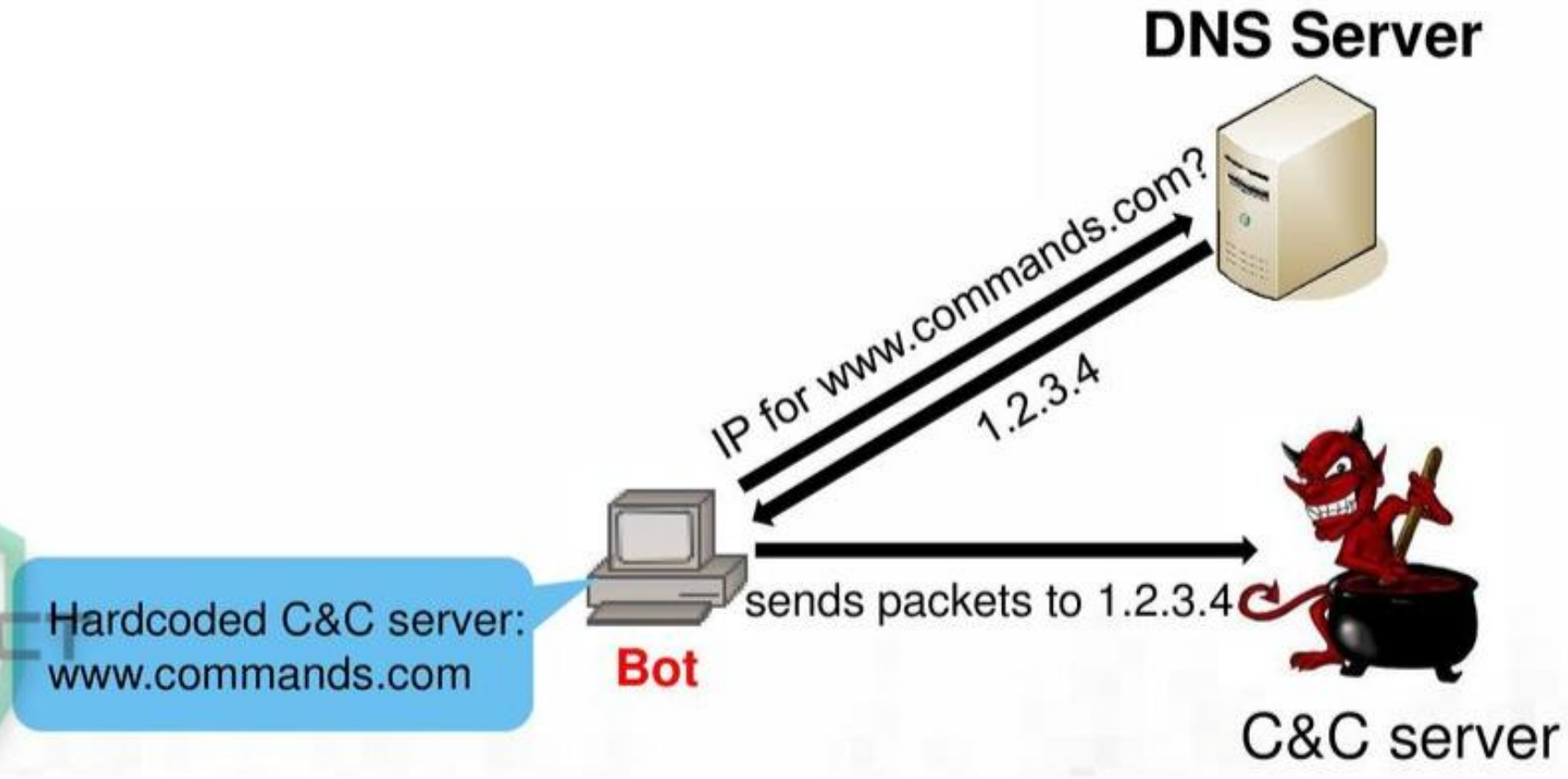
DGA.Changer, "샌드박스 쯤은 우습게 우회해요"

DGA.Changer는 봇넷(botnet) 개념의 공격으로 대규모 시스템이 동시에 명령을 전달받아 클릭 수를 조작하는 클릭사기, 정보 탈취, 트로이 목마 접속, 원격 명령 전송 등과 같은 다양한 기능을 실행할 수 있다. 게다가 DGA.Changer는 이미 상품화되어 있다는 데서 진짜 위력이 발휘된다. 누구든지 마음만 먹으면 얼마든지 구매하여 사용할 수 있기 때문이다.

배경

- 과거의 BotNet의 형태
  - Bot은 C&C Domain으로 접속을 한다.
  - C&C Domain은 바이너리 형태로 하드코딩 되어있다.

  * C&C(Command & Control = C&C, C2): Bot들을 제어하고 명령을 전달하는 서버

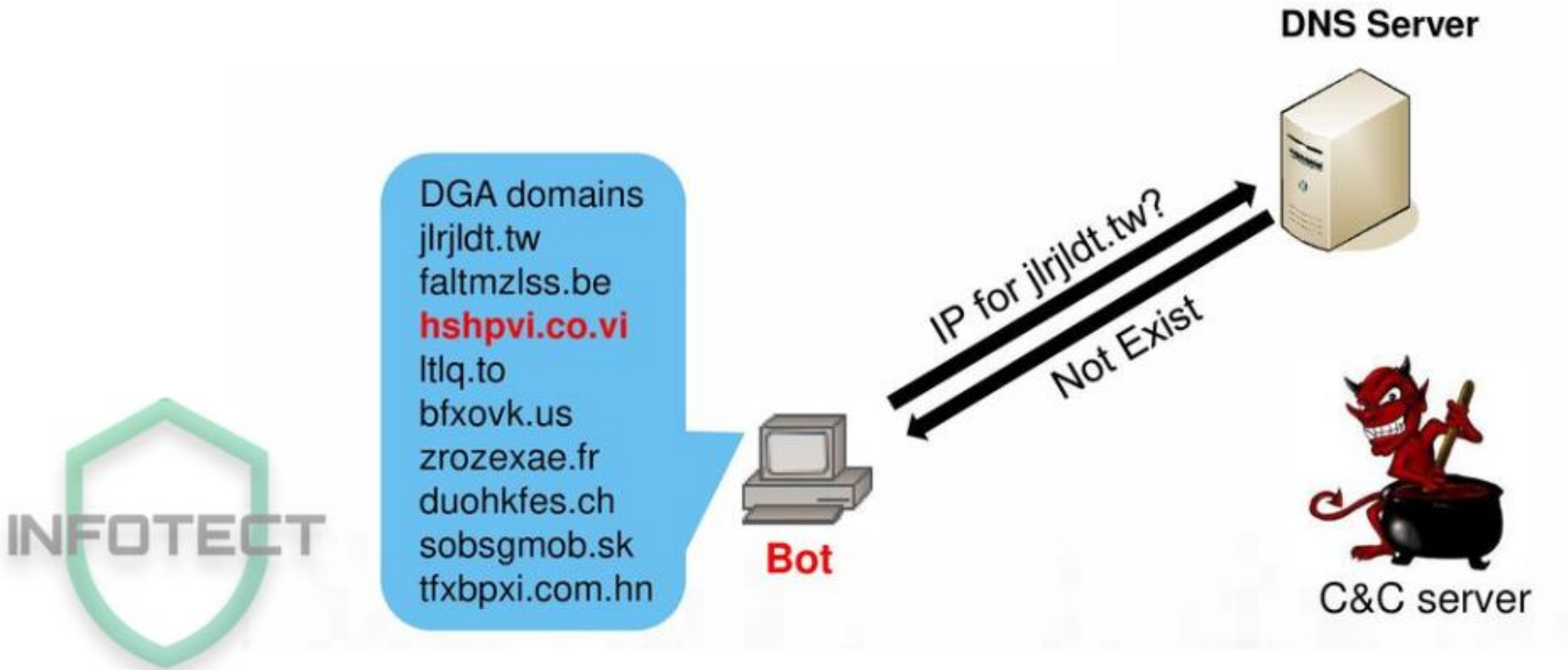


배경

- DGA BotNet의 형태

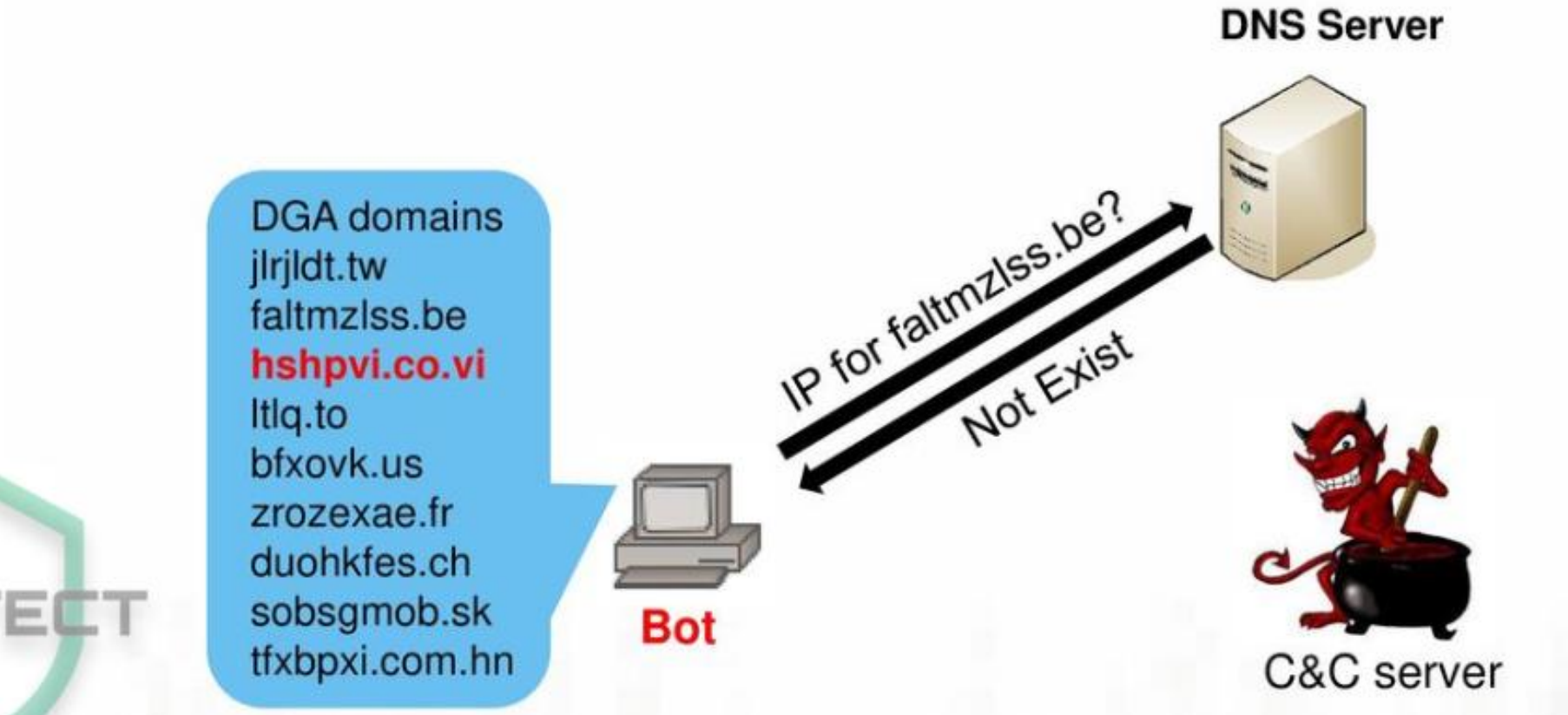
  - 최근의 발전된 Botnet은 DGA를 기반으로 도메인을 계속해서 생성한다.

  * DGA(Domain Genaration Algorithm): 도메인을 생성하는 알고리즘



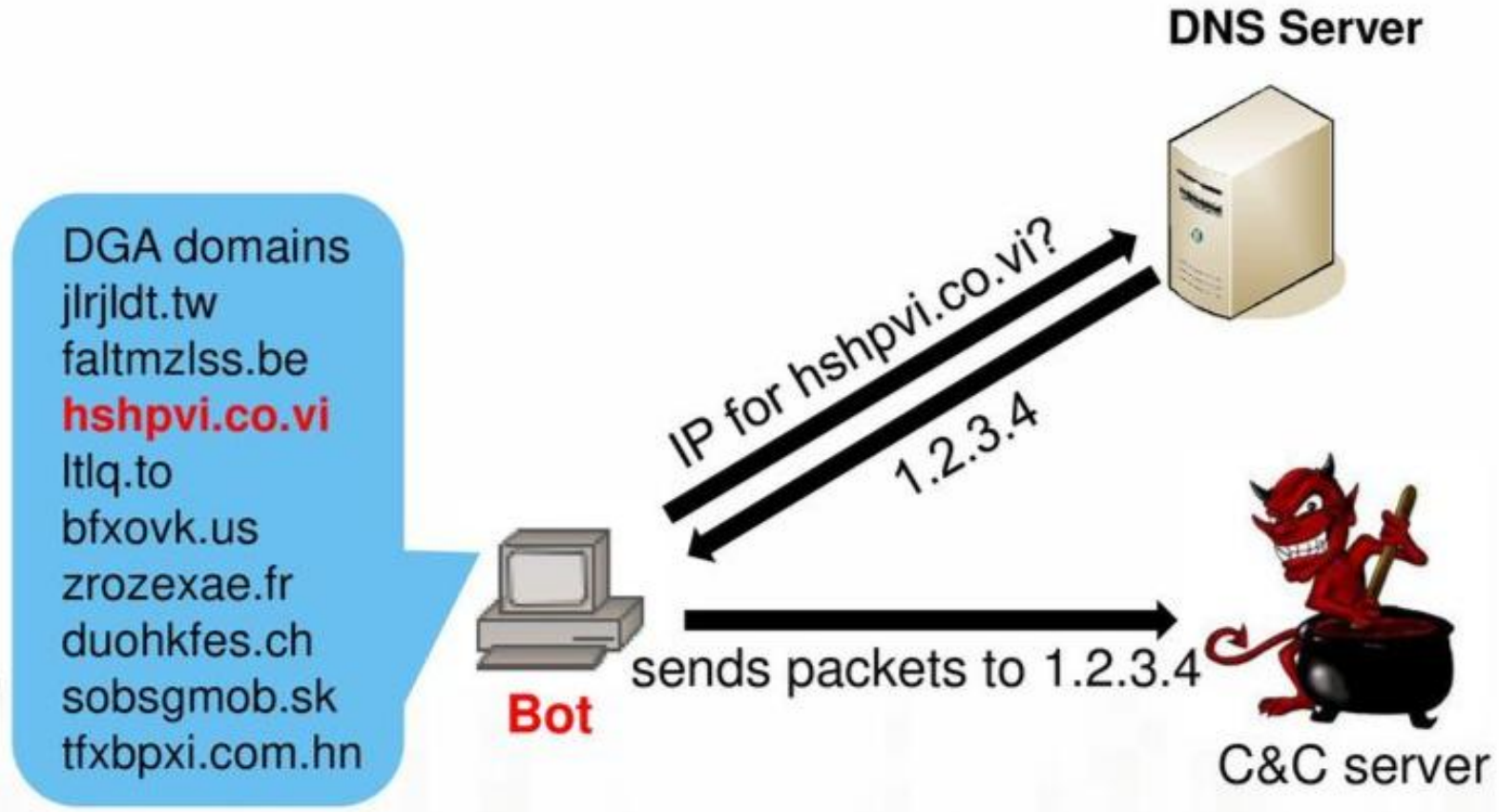
배경

- DGA BotNet의 형태
  - C&C에 접속이 성공할 때까지 생성된 Domain들을 계속해서 DNS에 질의한다.



배경

- DGA BotNet의 형태
  - 아직 차단되지 않은 Domain으로 접속에 성공한다.



배경

- 2019년 7대 사이버 공격 전망 (KISA 발표자료)
  - DGA(Domain Generation Algorithm)를 이용하여 C&C 차단을 회피하는 악성코드가 더욱 증가할 것이라 전망

KISA
Korea Internet & Security Agency

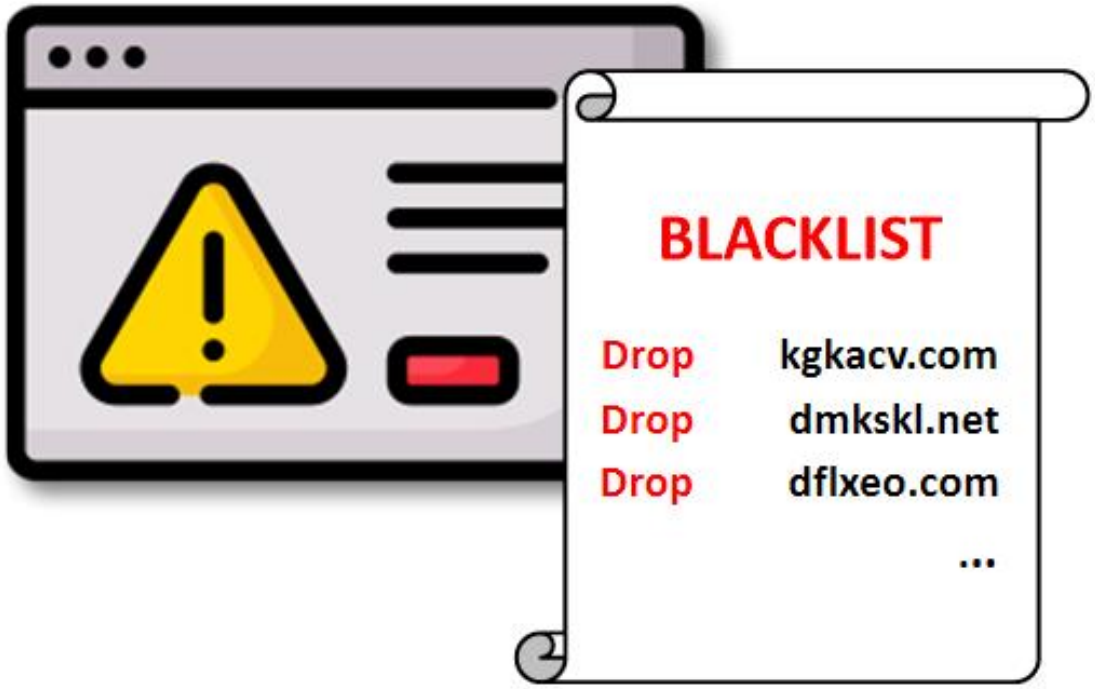
Ⅶ. 악성 행위 탐지를 우회하는 공격 기법의 진화

▮DGA(Domain Generation Algorithm)를 이용하여 C&C 차단을 회피하는 악성코드 증가

2. 목적

목적

- 기본적으로 특정 사이트로의 접속 차단은 BLACKLIST에 Domain을 등록하여 관리



목적

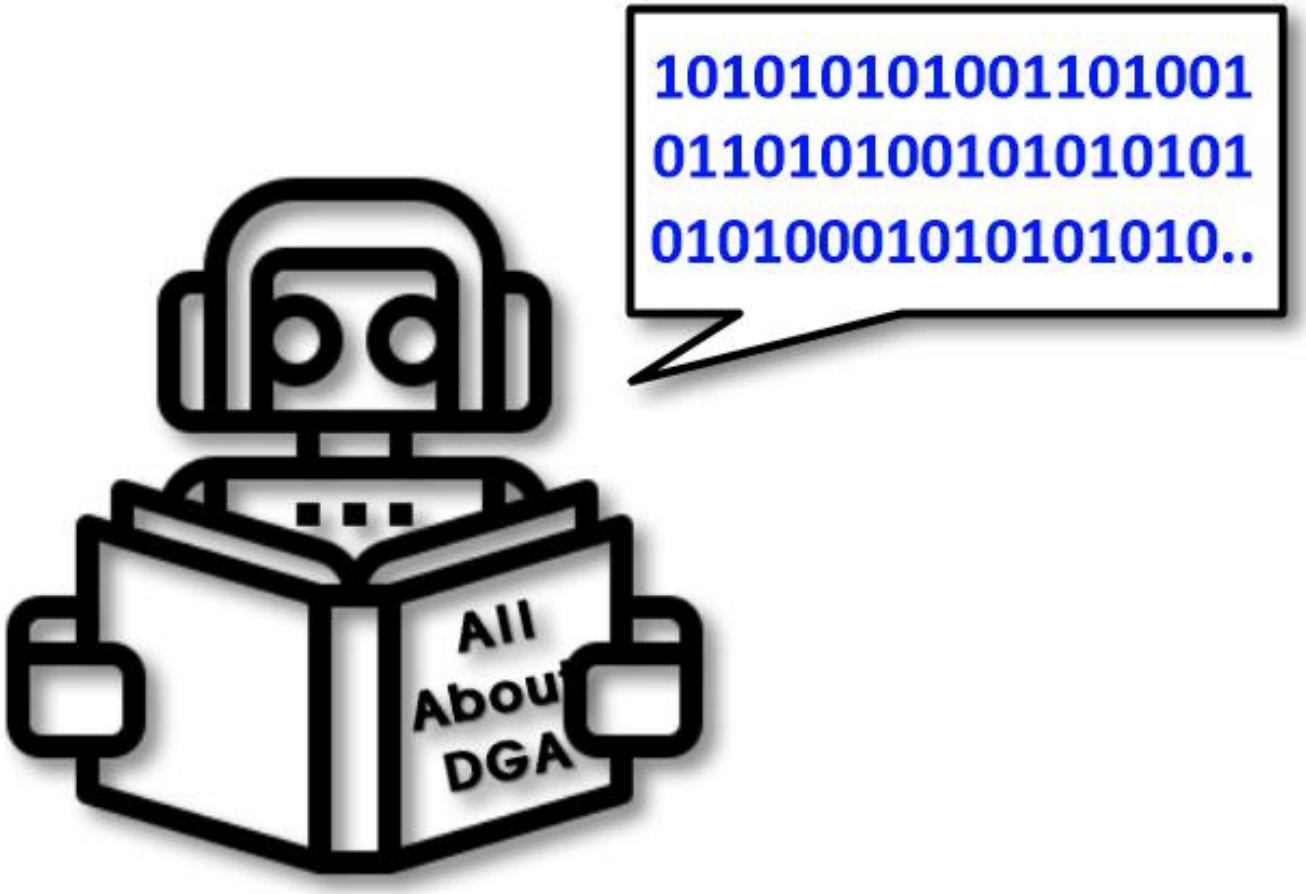
- Network 내에서 발생하는 모든 DNS Query를 감시하여 선별하는 것은 쉽지 않음

목적

- 해당 Domain을 차단했더라도 최근 공격자들은 DGA를 활용해 계속해서 새로운 Domain을 생성하여 차단을 우회함

목적

- 본 프로젝트에서는 Machine Learning을 통해 DGA로 생성된 Domain의 Feature를 학습시켜, DGA Domain인지 아닌지 판별하는 AI모델을 제안함



목적

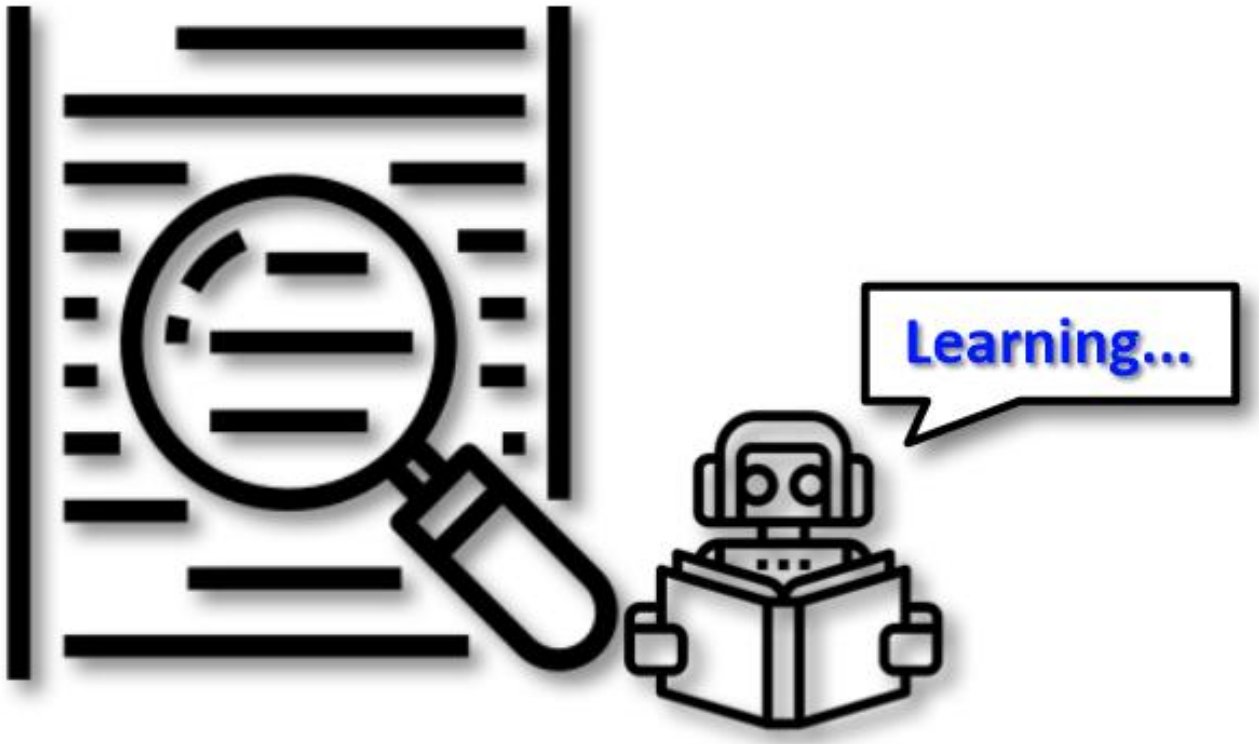
- 이를 활용하여 DGA 봇넷 C&C 접속을 탐지하고 관리자의 업무 효율 증진 방안을 모색함

3. 방법론

방법론

- DGA 봇넷 C&C 접속 탐지/차단 아이디어

  Step1. DGA의 Feature를 Machine Learning으로 학습시킨 AI를 개발

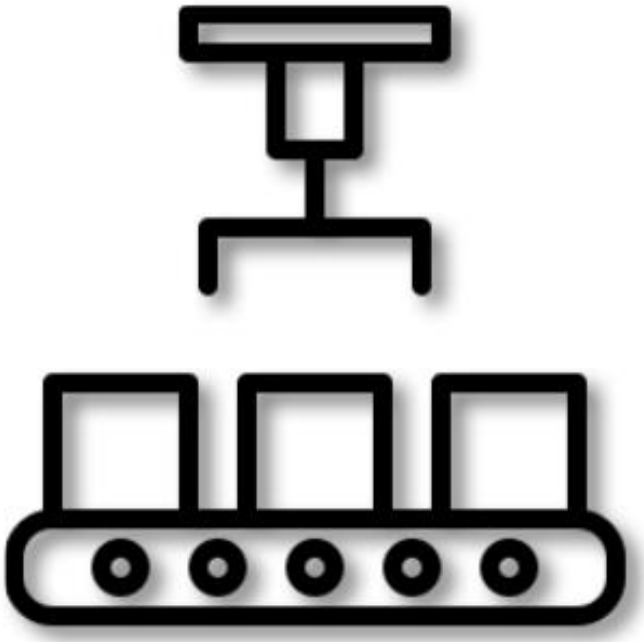


방법론

- DGA 봇넷 C&C 접속 탐지/차단 아이디어

  Step1. DGA의 Feature를 Machine Learning으로 학습시킨 AI를 개발

  Step2. Network 내에서 발생하는 DNS Query Message에서 Domain 추출



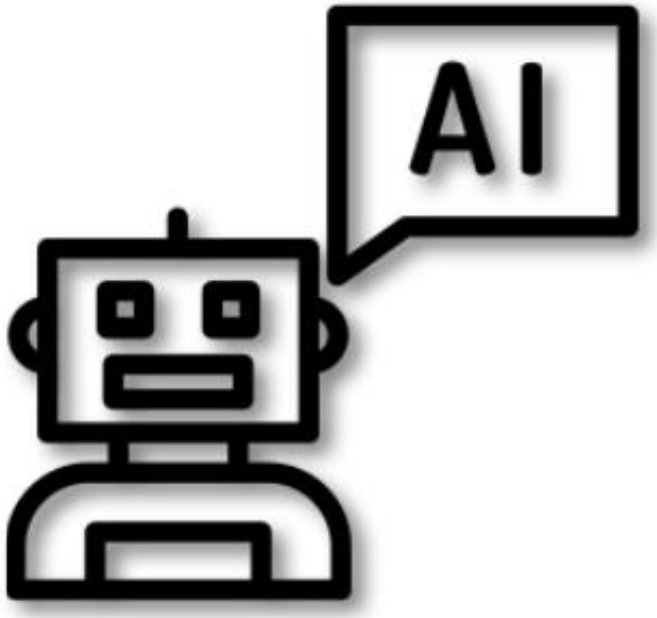
방법론

- DGA 봇넷 C&C 접속 탐지/차단 아이디어

  Step1. DGA의 Feature를 Machine Learning으로 학습시킨 AI를 개발

  Step2. Network 내에서 발생하는 DNS Query Message에서 Domain 추출

  Step3. AI를 통한 DGA Domain 판단



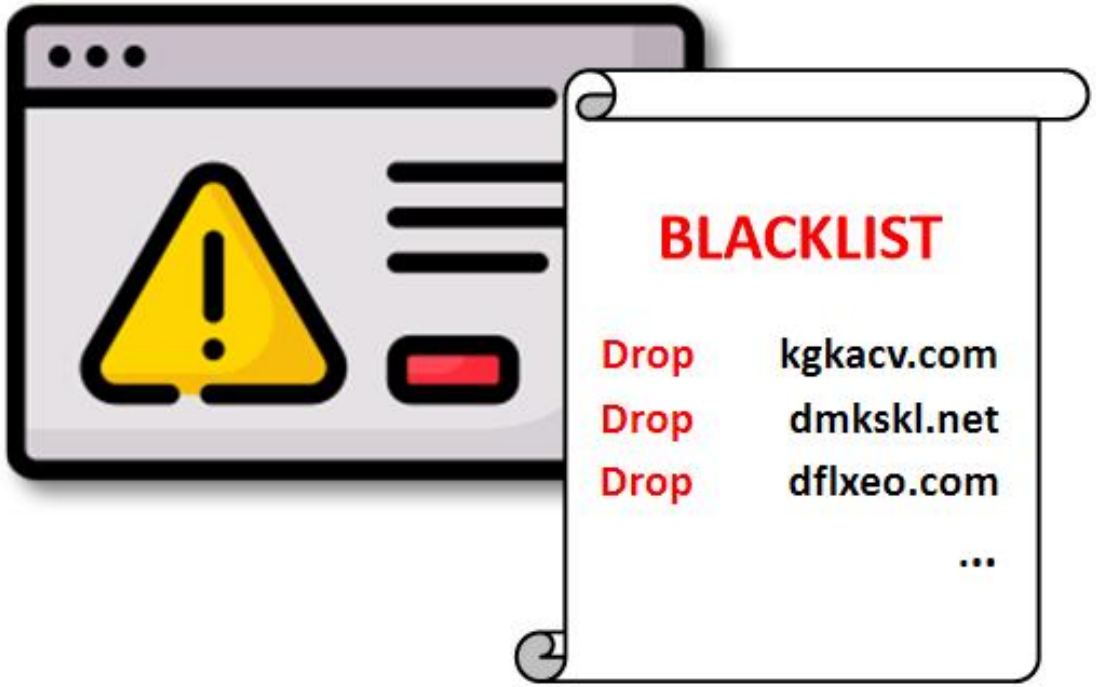
- DGA 봇넷 C&C 접속 탐지/차단 아이디어

  Step1. DGA의 Feature를 Machine Learning으로 학습시킨 AI를 개발

  Step2. Network 내에서 발생하는 DNS Query Message에서 Domain 추출

  Step3. AI를 통한 DGA Domain 판단

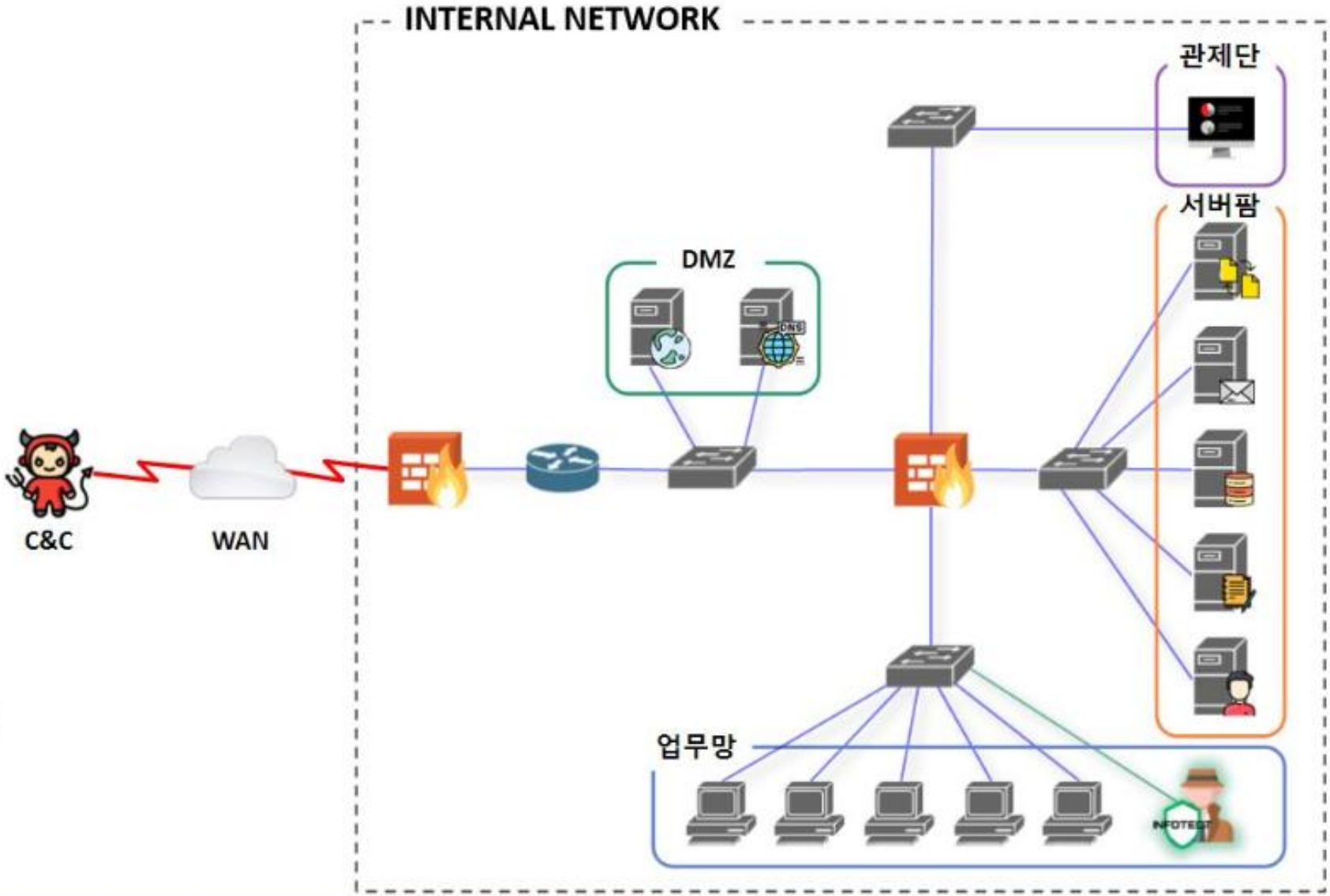
  Step4. 결과가 DGA일 경우, 관리자에게 알림기능을 제공하여 조치할 수 있도록 함



4. 구성도

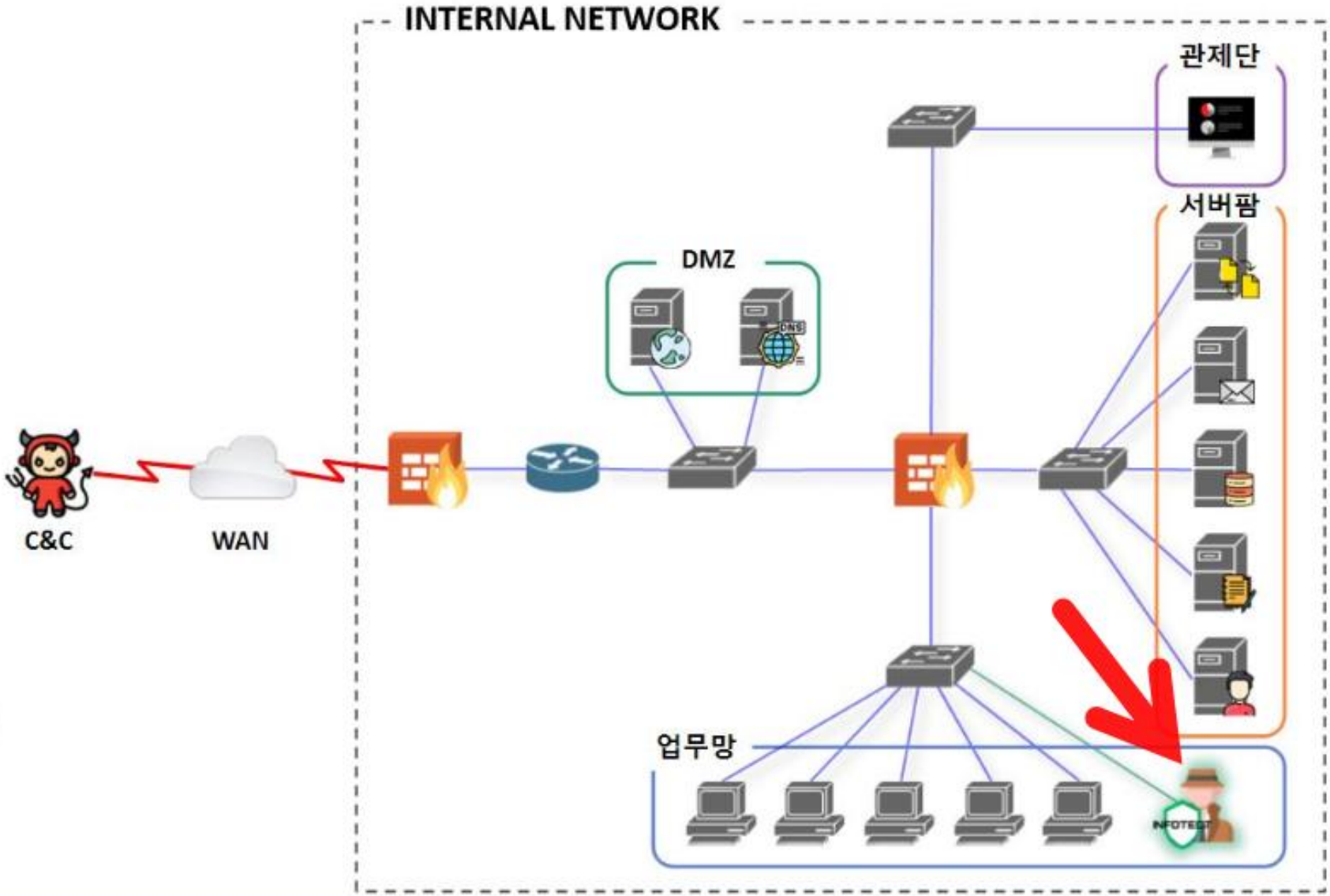
구성도

- DGA 봇넷 C&C 접속 탐지/차단 아이디어
  - 배치도



구성도

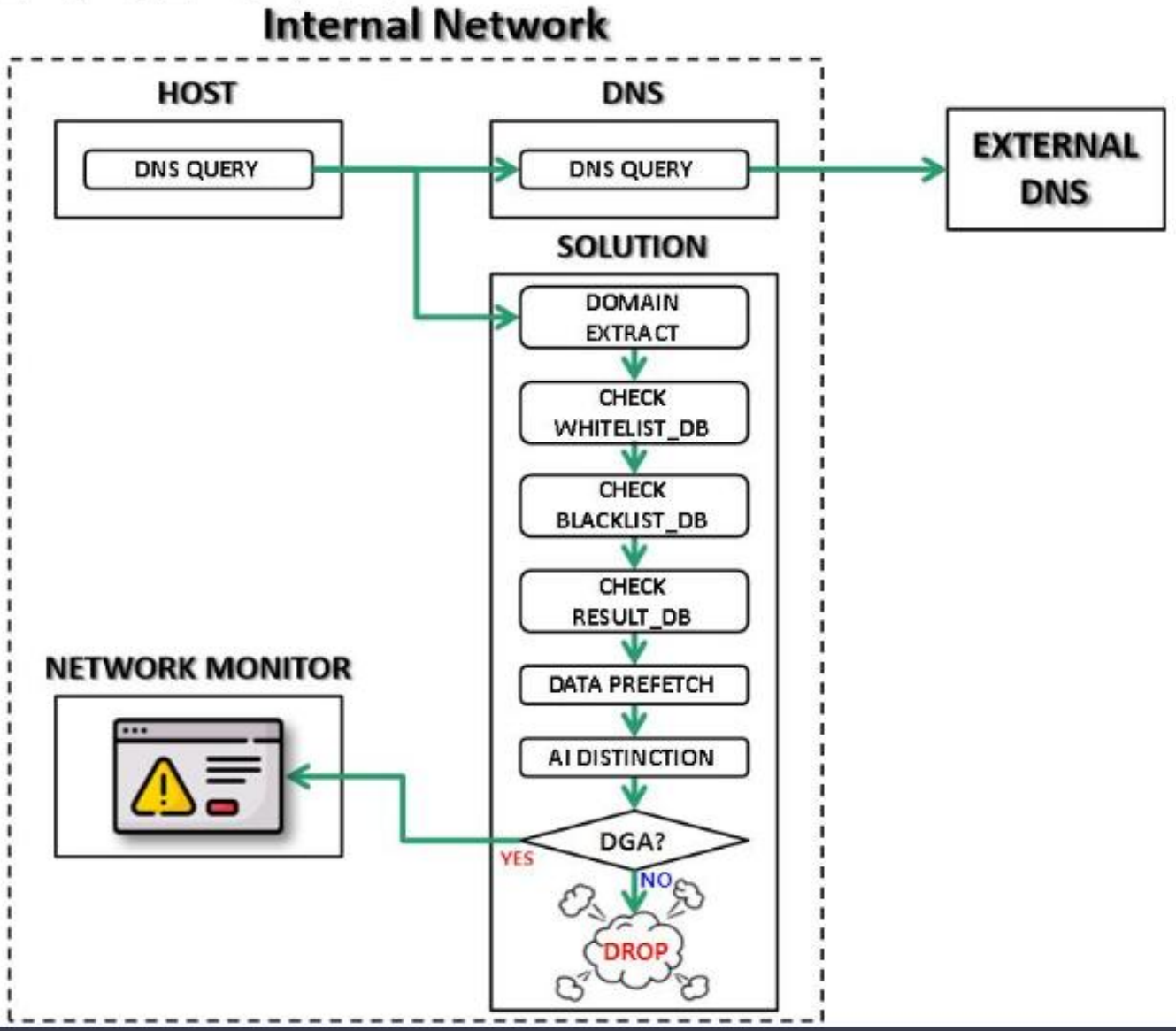
- DGA 봇넷 C&C 접속 탐지/차단 아이디어
  - 배치도



구성도

- DGA 봇넷 C&C 접속 탐지/차단 아이디어

  - 흐름도



5. 최종목표

K-Shield Jr.

“머신러닝을 활용한 DGA 봇넷 C&C 접속 탐지 솔루션”

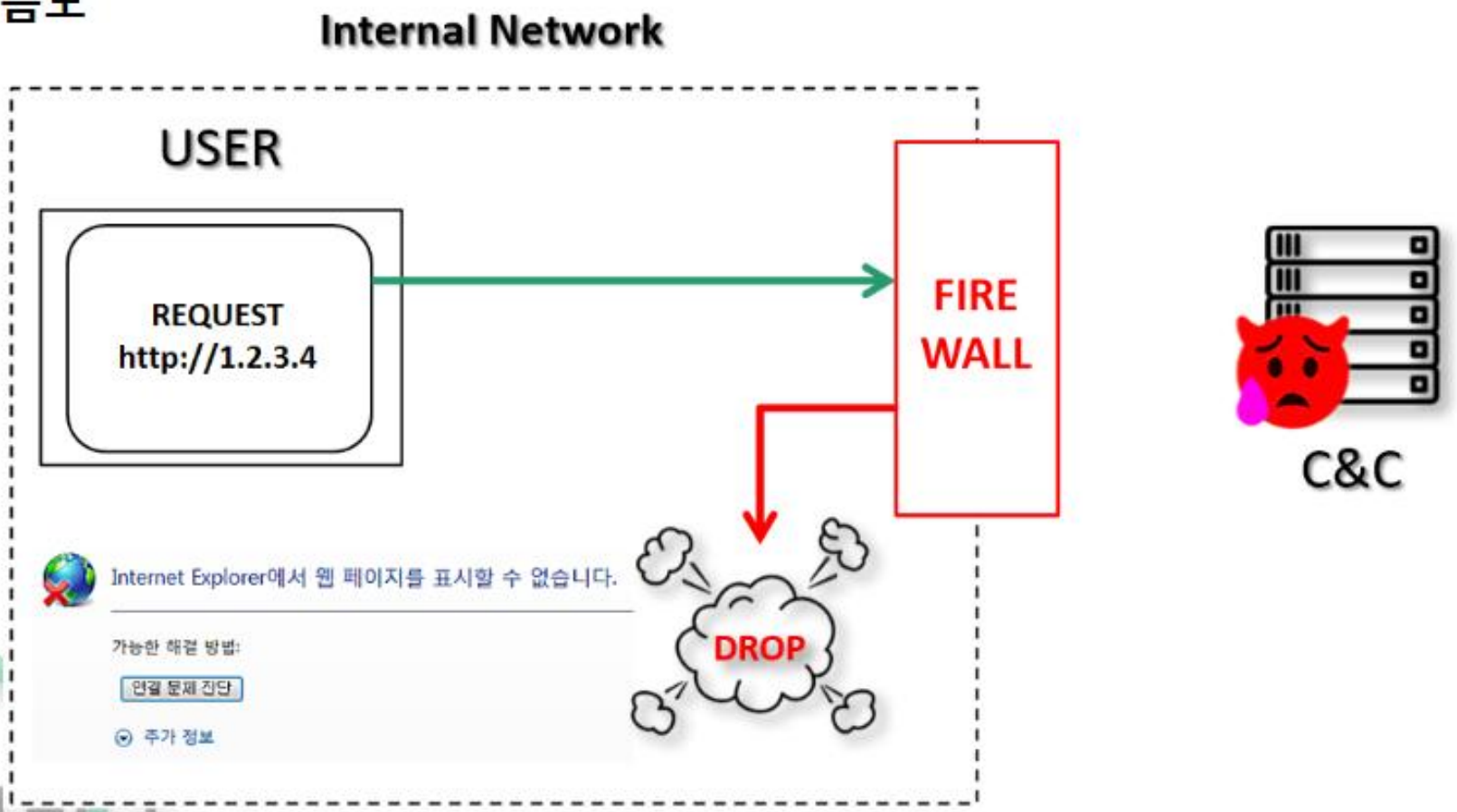
Q&A

최종목표

- **한계점**
  - 현재까지 고안한 것으로는 서버의 Resource 점유율이 저조함
  - AI가 계속해서 학습하고 발전함과 동시에 DGA Domain 탐지도 동시에 수행할 방법을 고안해야 함

구성도

- DGA 봇넷 C&C 접속 탐지/차단 아이디어
  - 흐름도



방법론

- DGA 봇넷 C&C 접속 탐지/차단 아이디어
  - DGA로 생성된 Domain은 모두 악성으로 간주
  - DGA가 생성한 Domain은 언어적으로 고유한 Feature들을 가짐

DGA Bot에 의해 질의 된 NXDomain 예시:

dyayxsgsv.net, yylnfnwjqb.com
wdzitdojre.dyndns.org, svahvjnve.net
mudvpcrwhgj.com, qzudjqxkykxs.com

C&C Domain 예시:

kyqqnrkwijs.dyndns.org

언어적인 속성:

대부분의 Domain:

* 사전적인 단어를 사용하지 않음
* 2LD의 숫자 갯수는 0개
* 2LD의 문자 갯수는 7 - 11개 사이